

McAfee®

Internet Security Suite 2008

Kullanıcı Kılavuzu

İçindekiler

McAfee Internet Security	3
McAfee SecurityCenter	5
SecurityCenter özellikleri	6
SecurityCenter'ı kullanma	7
SecurityCenter'ı güncelleştirme	13
Koruma sorunlarını onarma veya yok sayma	17
Uyarılarla çalışma	21
Olayları görüntüleme	27
McAfee VirusScan	29
VirusScan özellikleri	30
Gerçek zamanlı virüsten korumayı başlatma	31
Ek korumayı başlatma	33
Virüsten korumayı ayarlama	37
Bilgisayarınızı tarama	55
Tarama sonuçlarıyla çalışma	59
McAfee Personal Firewall	63
Personal Firewall özellikleri	64
Firewall'u başlatma	67
Uyarılarla çalışma	69
Bilgi uyarılarını yönetme	71
Firewall korumasını yapılandırma	73
Programları ve izinleri yönetme	85
Sistem hizmetlerini yönetme	93
Bilgisayar bağlantılarını yönetme	99
Günlüğe kaydetme, izleme ve analiz	107
İnternet güvenliği hakkında bilgi alma	117
McAfee Anti-Spam	119
Anti-Spam özellikleri	121
Web posta hesaplarınızı ayarlama	123
Arkadaşları ayarlama	127
Spam algılamayı yapılandırma	133
E-posta filtreleme	141
Filtrelenen e-posta ile çalışma	145
Phishing korumasını yapılandırma	147
McAfee Privacy Service	149
Privacy Service özellikleri	150
Ebeveyn Denetimleri'ni ayarlama	151
Web'de bilgileri koruma	167
Parolaları koruma	169
McAfee Data Backup	173
Özellikler	174
Dosyaları arşivleme	175
Arşivlenen dosyalarla çalışma	183
McAfee QuickClean	189
QuickClean özellikleri	190
Bilgisayarınızı temizleme	191
Bilgisayarınızı birleştirme	194

Görev zamanlama	195
McAfee Shredder	201
Shredder özellikleri	202
Dosyaları, klasörleri ve diskleri parçalama	203
McAfee Network Manager.....	205
Network Manager özellikleri.....	206
Network Manager simgeleri hakkında bilgi	207
Yönetilen bir ağ kurma	209
Ağı uzaktan yönetme	215
McAfee EasyNetwork.....	219
EasyNetwork özellikleri.....	220
EasyNetwork'ü ayarlama	221
Dosyaları paylaşma ve gönderme	227
Yazıcıları paylaşma	233
Başvuru	235
 Sözlük	 236
 McAfee Hakkında	 251
Telif Hakkı	251
Lisans	252
Müşteri Desteği ve Teknik Destek.....	253
McAfee Virtual Technician'ı kullanma	254
Destek ve Yüklemeler	255
 Dizin	 263

B Ö L Ü M 1

McAfee Internet Security

SiteAdvisor ile birlikte McAfee Internet Security Suite, değer verdiğiniz şeyleri, kimliğinizi ve bilgisayarınızı virüslerden, casus yazılımlardan, e-posta ve anlık ileti aldatmacalarından, korsanlardan ve çevrimiçi yağmacılardan koruyan, önemli dosyalarınızı otomatik olarak yedekleyen, her zaman güncelleştirme yapan etkin onu bir arada güvenlik ürün grubudur. Web'de güven içinde gezinin, alışveriş ve bankacılık işlemleri yapın, e-posta ve anlık ileti gönderip alın, dosyalar yükleyin. McAfee SiteAdvisor ve Ebeveyn Denetimleri, sizin ve ailenizin güvenli olmayan Web sitelerinden uzak durmanıza yardımcı olur. McAfee'nin güvenlik hizmeti, sürekli ve otomatik olarak en güncel özellikleri, geliştirmeleri ve tehdit verilerini aktarır. Ayrıca otomatikleştirilmiş bilgisayar ayarları, tam bilgisayar performansı için gereksiz dosyaları kaldırır.

Bu bölümde

McAfee SecurityCenter	5
McAfee VirusScan	29
McAfee Personal Firewall	63
McAfee Anti-Spam	119
McAfee Privacy Service	149
McAfee Data Backup	173
McAfee QuickClean	189
McAfee Shredder	201
McAfee Network Manager	205
McAfee EasyNetwork	219
Başvuru	235
McAfee Hakkında	251
Müşteri Desteği ve Teknik Destek	253

B Ö L Ü M 2

McAfee SecurityCenter

McAfee SecurityCenter, bilgisayarınızın güvenlik durumunu izlemenize, bilgisayarınızdaki virüs, casus yazılım, e-posta ve güvenlik duvarı koruma hizmetlerinin güncel olup olmadığını anında öğrenmenize, olası güvenlik açıklarını düzeltmenize olanak verir. Bilgisayarınızda tüm koruma alanlarını koordine etmek ve yönetmek için gereksinim duyduğunuz gezinti araçlarını ve denetimlerini sağlar.

Bilgisayarınızın korumasını yapılandırmaya ve yönetmeye başlamadan önce, SecurityCenter arabirimini inceleyin ve korunma durumu, korunma kategorileri ve korunma hizmetleri arasındaki farkı bildiğinizden emin olun. Sonra McAfee tarafından sunulan en son korumaya sahip olmak için SecurityCenter'ı güncelleştirin.

Başlangıç yapılandırması görevlerini tamamlayınca, bilgisayarınızın korunma durumunu izlemek için SecurityCenter'ı kullanın. SecurityCenter bir sorun algıladığında, sorunu çözmeniz veya yok saymanız (önem düzeyine göre) için sizi uyarır. Ayrıca olay günlüğünde, virüs taraması yapılandırma değişiklikleri gibi SecurityCenter olaylarını da inceleyebilirsiniz.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

SecurityCenter özellikleri	6
SecurityCenter'ı kullanma	7
SecurityCenter'ı güncelleştirme	13
Koruma sorunlarını onarma veya yok sayma	17
Uyarılarla çalışma	21
Olayları görüntüleme	27

SecurityCenter özellikleri

SecurityCenter şu özellikleri sunar:

Basitleştirilmiş koruma durumu

Kolayca bilgisayarınızın korunma durumunu inceleyin, güncelleştirmeleri denetleyin ve olası korunma sorunlarını düzeltin.

Otomatik güncelleştirmeler ve yükseltmeler

Kayıtlı programlarınız için güncelleştirmeleri otomatik olarak yükleyip kurun. Kayıtlı McAfee programının yeni bir sürümü çıktığında, aboneliğiniz geçerli olduğu sürece bunu ücretsiz olarak edinerek, her zaman en güncel korumaya sahip olduğunuzdan emin olursunuz.

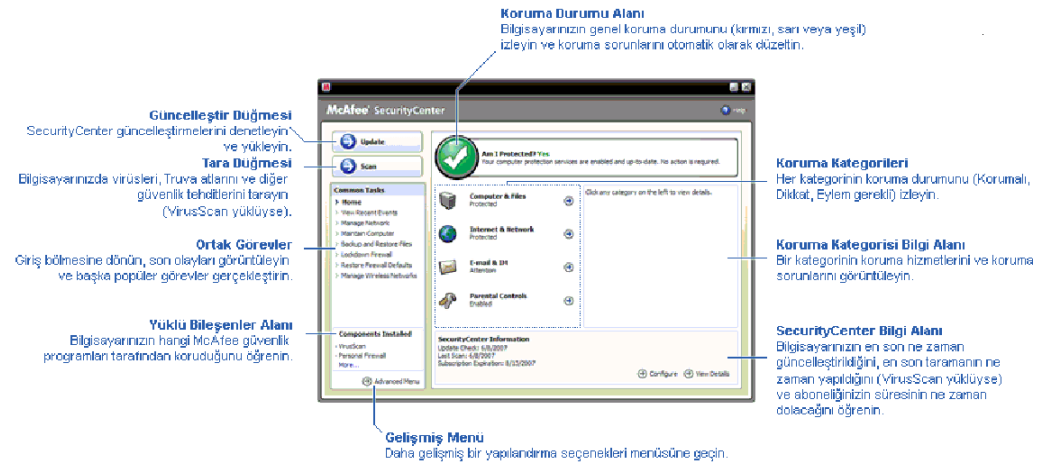
Gerçek zamanlı uyarılar

Güvenlik uyarıları, size acil virüs saldırılarını ve güvenlik tehditlerini bildirir; tehdidi ortadan kaldırmak, etkisiz hale getirmek veya bununla ilgili ayrıntılı bilgi almak için seçenekler sunar.

B Ö L Ü M 3

SecurityCenter'i kullanma

SecurityCenter'i kullanmaya başlamadan önce, bilgisayarınızın korunma durumunu yönetmek için kullanacağınız bileşenleri ve yapılandırma alanlarını inceleyin. Bu görüntüde kullanılan terminoloji hakkında ayrıntılı bilgi için bkz. Koruma durumu hakkında bilgi (sayfa 8) ve Koruma kategorileri hakkında bilgi (sayfa 9). Sonra, McAfee hesabı bilgilerinizi inceleyebilir ve aboneliğinizin geçerliliğini doğrulayabilirsiniz.



Bu bölümde

Koruma durumu hakkında bilgi	8
Koruma kategorileri hakkında bilgi	9
Koruma hizmetleri hakkında bilgi	10
McAfee hesabınızı yönetme	11

Koruma durumu hakkında bilgi

Bilgisayarınızın koruma durumu, SecurityCenter Giriş bölümündeki koruma durumu alanında gösterilir. Burada, bilgisayarınızın en son güvenlik tehditlerinden tam olarak korunup korunmadığı ve dış güvenlik saldırıları, diğer güvenlik programları ve Internet'e erişebilen programlar gibi etkilere açık olup olmadığı belirtilir.

Bilgisayarınızın koruma durumu kırmızı, sarı veya yeşil olabilir.

Koruma Durumu	Açıklama
Kırmızı	Bilgisayarınız korunmuyor. SecurityCenter Giriş bölümündeki koruma durumu alanı kırmızıdır ve korunmadığınızı belirtir. SecurityCenter, en az bir kritik güvenlik sorunu bildirir. Tam korumaya ulaşmak için her bir koruma kategorisindeki tüm kritik güvenlik sorunlarını düzeltmeniz gerekir (sorun kategorisinin durumu yine kırmızı renkte Eylem Gerekli seçeneğine ayarlıdır). Koruma sorunlarını düzeltme hakkında bilgi için bkz. Koruma sorunlarını onarma (sayfa 18).
Sarı	Bilgisayarınız kısmen korunuyor. SecurityCenter Giriş bölümündeki koruma durumu alanı sarıdır ve korunmadığınızı belirtir. SecurityCenter, en az bir kritik olmayan güvenlik sorunu bildirir. Tam korumaya ulaşmak için her bir koruma kategorisiyle ilişkili kritik olmayan güvenlik sorunlarını düzeltmeniz veya yok saymanız gerekir. Koruma sorunlarını düzeltme veya yok sayma hakkında bilgi için bkz. Koruma sorunlarını onarma veya yok sayma (sayfa 17).
Yeşil	Bilgisayarınız tam olarak korunuyor. SecurityCenter Giriş bölümündeki koruma durumu alanı yeşildir ve korunduğunuzu belirtir. SecurityCenter, kritik veya kritik olmayan güvenlik sorunu bildirmez. Her koruma kategorisinde, bilgisayarınızı koruyan hizmetler listelenir.

Koruma kategorileri hakkında bilgi

SecurityCenter'in koruma hizmetleri dört kategoriye ayrılır: Bilgisayar ve Dosyalar, Internet ve Ağ, E-posta ve Anlık İletişim, Ebeveyn Denetimleri. Bu kategoriler, bilgisayarınızı koruyan güvenlik hizmetlerine göz atmanıza ve bunları yapılandırmanıza yardımcı olur.

Koruma hizmetlerini yapılandırmak için bir kategori adını tıklatır ve varsa bu hizmetlerle ilgili algılanan güvenlik sorunlarını görüntülersiniz. Bilgisayarınızın koruma durumu kırmızı veya sarı ise, bir veya birkaç kategoride *Eylem Gerekli* veya *Dikkat* uyarısı görüntülenir; bu, SecurityCenter'in bu kategori içinde bir sorun algıladığını gösterir. Koruma durumu hakkında ayrıntılı bilgi için bkz. Koruma durumu hakkında bilgi (sayfa 8).

Koruma Kategorisi	Açıklama
Bilgisayar ve Dosyalar	Bilgisayar ve Dosyalar kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: - Virüsten Koruma - PUP Koruması - Sistem Monitörleri - Windows Koruması
Internet ve Ağ	Internet ve Ağ kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: - Güvenlik Duvarı Koruması - Kimlik Koruma
E-posta ve Anlık İletişim	E-posta ve Anlık İletişim kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: - E-posta Koruması - Spam'den Korunma
Ebeveyn Denetimleri	Ebeveyn Denetimleri kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: İçerik Engelleme

Koruma hizmetleri hakkında bilgi

Koruma hizmetleri, bilgisayarınızı korumak için yapılandırıđınız temel SecurityCenter bileşenleridir. Koruma hizmetleri, doğrudan McAfee programlarıyla ilişkilidir. Örneđin VirusScan yüklediđinizde, řu koruma hizmetlerini kullanabilirsiniz: Virüsten Koruma, PUP Koruması, Sistem Monitörleri ve Windows Koruması. Bu özel koruma hizmetleri hakkında ayrıntılı bilgi için VirusScan yardımına bakın.

Varsayılan olarak, bir programı yüklediđinizde bu programla ilişkili tüm koruma hizmetleri etkindir; ancak istediđiniz zaman koruma hizmetini devre dışı bırakabilirsiniz. Örneđin Privacy Service yüklerseniz, İçerik Engelleme ve Kimlik Koruma etkindir. İçerik Engelleme koruma hizmetini kullanmayı düşünmüyorsanız, bunu tamamen devre dışı bırakabilirsiniz. Ayrıca ayar veya bakım görevleri gerçekleştirirken de bir koruma hizmetini geçici olarak devre dışı bırakabilirsiniz.

McAfee hesabınızı yönetme

Hesap bilgilerinize kolayca erişip bunları inceleyerek ve geçerli abonelik durumunuzu doğrulayarak, SecurityCenter'dan McAfee hesabınızı yönetin.

Not: McAfee programlarınızı CD'den yüklediyseniz, McAfee hesabınızı ayarlamak veya güncelleştirmek için bunları McAfee Web sitesinden kaydettirmelisiniz. Ancak bundan sonra düzenli ve otomatik program güncelleştirmeleri yapabilirsiniz.

McAfee hesabınızı yönetme

McAfee hesap bilgilerinize (Hesabım), SecurityCenter'dan kolayca erişebilirsiniz.

- 1 **Ortak Görevler** altında **Hesabım**'ı tıklayın.
- 2 McAfee hesabınızda oturumu açın.

Aboneliğinizi doğrulama

Süresinin sona ermediğinden emin olmak için aboneliğinizi doğrularsınız.

- Görev çubuğunun sağ ucundaki bildirim alanında bulunan SecurityCenter simgesini  sağ tıklayın ve sonra **Aboneliği Doğrula**'yı tıklayın.

B Ö L Ü M 4

SecurityCenter'ı güncelleştirme

SecurityCenter, dört saatte bir çevrimiçi güncelleştirmeleri denetleyip yükleyerek, kayıtlı McAfee programlarınızın güncel olmasını sağlar. yüklediğiniz veya kaydettirdiğiniz programlara bağlı olarak, çevrimiçi güncelleştirmeler en son virüs tanımlarını ve korsan, spam, casus yazılım veya gizlilik koruması yükseltmelerini içerebilir. Varsayılan dört saatlik süre içinde güncelleştirmeleri denetlemek istiyorsanız, bunu istediğiniz zaman yapabilirsiniz. SecurityCenter güncelleştirmeleri denetlerken, siz başka görevler gerçekleştirmeye devam edebilirsiniz.

Bu önerilme de, SecurityCenter'ın güncelleştirmeleri denetleme ve yükleme biçimini değiştirebilirsiniz. Örneğin, SecurityCenter'ı güncelleştirmeleri yükleyecek ancak kurmayacak ya da güncelleştirmeleri yüklemeyen veya kurmadan önce size bildirecek şekilde yapılandırabilirsiniz. Ayrıca otomatik güncelleştirmeyi devre dışı bırakabilirsiniz.

Not: McAfee programlarınızı CD'den yüklediyseniz, McAfee Web sitesinden bunları kaydettirene kadar, bu programlar için düzenli ve otomatik güncelleştirmeleri alamazsınız.

Bu bölümde

Güncelleştirmeleri denetleme	13
Otomatik güncelleştirmeleri yapılandırma.....	14
Otomatik güncelleştirmeleri devre dışı bırakma.....	14

Güncelleştirmeleri denetleme

Varsayılan olarak, bilgisayarınız Internet'e bağlı olduğunda, SecurityCenter dört saatte bir güncelleştirmeleri otomatik olarak denetler; ancak dört saatlik süre içinde güncelleştirmeleri denetlemek isterseniz, bunu yapabilirsiniz. Otomatik güncelleştirmeleri devre dışı bıraktıysanız, güncelleştirmeleri düzenli olarak denetlemek sizin sorumluluğunuzdadır.

- SecurityCenter Giriş bölümünde **Güncelleştir**'i tıklayın.

İpucu: Görev çubuğunun sağ ucundaki bildirim alanında bulunan SecurityCenter simgesini  sağ tıklayıp, ardından **Güncelleştirmeler**'i tıklayarak, SecurityCenter'ı başlatmadan güncelleştirmeleri denetleyebilirsiniz.

Otomatik güncelleştirmeleri yapılandırma

Varsayılan olarak, bilgisayarınız Internet'e bağlı olduğunda, SecurityCenter dört saatte bir güncelleştirmeleri otomatik olarak denetler ve yükler. Bu varsayılan davranışı değiştirmek isterseniz, güncelleştirmeleri otomatik olarak yükleyip ardından güncelleştirmeler kurulmak üzere hazır olunca size bunu bildirecek veya güncelleştirmeleri yüklemekten önce bildirecek şekilde SecurityCenter'ı yapılandırabilirsiniz.

Not: Güncelleştirmeler karşıdan yüklenmek veya kurulmak üzere hazır olunca, SecurityCenter uyarıları kullanarak bunu size bildirir. Uyarılardan güncelleştirmeleri yükleyebilir veya kurabilir ya da güncelleştirmeleri erteleyebilirsiniz. Programlarınızı uyarıdan güncelleştirince, güncelleştirmeyi yükleyip kurmadan önce aboneliğinizi doğrulamanız istenebilir. Ayrıntılı bilgi için bkz. Uyarılarla çalışma (sayfa 21).

- 1 SecurityCenter Yapılandırma bölümünü açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
- 2 SecurityCenter Yapılandırma bölümünde, **Otomatik güncelleştirmeler devre dışı** altında **Açık**'ı ve sonra **Gelişmiş**'i tıklatın.
- 3 Aşağıdaki düğmelerden birini tıklatın:
 - **Güncelleştirmeler otomatik olarak yükle ve hizmetlerim güncelleştirildiğinde bana bildir (önerilir)**
 - **Güncelleştirmeleri otomatik olarak karşıdan yükle ve yüklemeye hazır olduğunda bana bildir**
 - **Güncelleştirmeleri karşıdan yüklemekten önce bana bildir**
- 4 **Tamam**'ı tıklatın.

Otomatik güncelleştirmeleri devre dışı bırakma

Otomatik güncelleştirmeleri devre dışı bırakırsanız, güncelleştirmeleri düzenli olarak denetlemek sizin sorumluluğunuzdadır; aksi halde, bilgisayarınızda en son güvenlik koruması olmaz. Güncelleştirmeleri el ile denetleme hakkında ayrıntılı bilgi için bkz. Güncelleştirmeleri denetleme (sayfa 13).

- 1 SecurityCenter Yapılandırma bölümünü açın.
Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
- 2** SecurityCenter Yapılandırma bölümünde, **Otomatik güncelleştirmeler etkin** altında **Kapalı**'yı tıklatın.

İpucu: **Açık** düğmesini tıklatarak veya Güncelleştirme Seçenekleri bölümünde **Otomatik güncelleştirmeyi devreden çıkar ve güncelleştirmeleri el ile denetlememe izin ver**'in işaretini kaldırarak otomatik güncelleştirmeleri etkinleştirirsiniz.

B Ö L Ü M 5

Koruma sorunlarını onarma veya yok sayma

SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Kritik sorunlarla hemen ilgilenilmesi gerekir ve bunlar koruma durumunuzu tehlikeye atar (rengi kırmızıya döner). Kritik olmayan sorunlarla hemen ilgilenilmesi gerekmez ve bunlar koruma durumunuzu tehlikeye atabilir veya atmayabilir (sorunun türüne göre). Yeşil koruma durumuna ulaşmak için tüm kritik sorunları düzeltmeniz ve tüm kritik olmayan sorunları düzeltmeniz veya yok saymanız gerekir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz. McAfee Virtual Technician hakkında ayrıntılı bilgi için McAfee Virtual Technician yardımına bakın.

Bu bölümde

Koruma sorunlarını onarma	18
Koruma sorunlarını yok sayma	20

Koruma sorunlarını onarma

Güvenlik sorunlarının çoğu otomatik olarak düzeltilebilir; ancak bazı sorunlarla sizin ilgilenmeniz gerekebilir. Örneğin Güvenlik Duvarı Koruması devre dışıysa, SecurityCenter bunu otomatik olarak etkinleştirebilir; ancak Güvenlik Duvarı Koruması yüklü değilse bunu yüklemeniz gerekir. Aşağıdaki tabloda, koruma sorunlarını el ile düzeltirken gerçekleştirebileceğiniz diğer bazı eylemler açıklanmaktadır:

Sorun	Eylem
Son 30 gün içinde bilgisayarınızda tam tarama yapılmadı.	Bilgisayarınızı el ile tarayın. Ayrıntılı bilgi için VirusScan yardımına bakın.
Algılama imza dosyalarınız (DAT) eski.	Korumanızı el ile güncelleştirin. Ayrıntılı bilgi için VirusScan yardımına bakın.
Bir program yüklü değil.	Programı McAfee Web sitesinden veya CD'den yükleyin.
Bir programın bileşenleri eksik.	Programı McAfee Web sitesinden veya CD'den yeniden yükleyin.
Bir program kayıtlı değil ve tam koruma alamıyor.	Programı McAfee Web sitesinde kaydettirin.
Programın süresi geçmiş.	Hesap durumunuzu McAfee Web sitesinde denetleyin.

Not: Genellikle bir tek koruma sorunu birden çok koruma kategorisini etkiler. Bu durumda, sorunu bir kategoride düzelttiğinizde, bu sorun diğer tüm kategorilerden silinir.

Koruma sorunlarını otomatik olarak onarma

SecurityCenter, koruma sorunlarının çoğunu otomatik olarak düzeltebilir. SecurityCenter'ın koruma sorunlarını otomatik olarak düzeltirken yaptığı yapılandırma değişiklikleri, olay günlüğüne kaydedilmez. Olaylar hakkında ayrıntılı bilgi için bkz. Olayları görüntüleme (sayfa 27).

- Ortak Görevler** bölümünde **Giriş**'i tıklatın.
- SecurityCenter Giriş bölümünde, koruma durumu alanında **Onar**'ı tıklatın.

Koruma sorunlarını el ile onarma

Otomatik olarak düzeltmeyi denedikten sonra bir veya birkaç koruma sorunu devam ederse, bunları el ile düzeltebilirsiniz.

- 1 Ortak Görevler** bölümünde **Giriş**'i tıklatın.
- 2** SecurityCenter Giriş bölümünde, SecurityCenter'ın sorunu bildirdiği koruma kategorisini tıklatın.
- 3** Sorun açıklamasının yanındaki bağlantıyı tıklatın.

Koruma sorunlarını yok sayma

SecurityCenter kritik olmayan bir sorun algılsa, bunu düzeltebilir veya yok sayabilirsiniz. Diğer kritik olmayan sorunlar (örneğin, Anti-Spam veya Privacy Service yüklü değilse) otomatik olarak yok sayılır. Bilgisayarınızın koruma durumu yeşil olmadığı sürece, yok sayılan sorunlar SecurityCenter Giriş bölümündeki koruma kategorisi alanında gösterilmez. Bir sorunu önce yok sayıp, daha sonra bilgisayarınızın koruma durumu yeşil olmasa bile bunun koruma kategorisi bilgi alanında görüntülenmesini istediğinize karar vererseniz, yok sayılan sorunu gösterebilirsiniz.

Koruma sorununu yok sayma

SecurityCenter kritik olmayan bir sorun algılsa ve bunu düzeltmeyi düşünmüyorsanız yok sayabilirsiniz. Yok saydığınızda, sorun SecurityCenter'da koruma kategorisi bilgi alanından kaldırılır.

- 1 **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
- 2 SecurityCenter Giriş bölümünde, sorunun bildirildiği koruma kategorisini tıklatın.
- 3 Koruma sorununun yanındaki **Yoksay** bağlantısını tıklatın.

Yok sayılan sorunları gösterme veya gizleme

Önem düzeyine bağlı olarak, yok sayılan koruma sorununu gösterebilir veya gizleyebilirsiniz.

- 1 Uyarı Seçenekleri bölümünü açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
 3. **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 2 SecurityCenter Yapılandırma bölümünde **Yoksayılan Sorunlar**'ı tıklatın.
- 3 Yoksayılan Sorunlar bölümünde aşağıdakileri yapın:
 - Bir sorunu yok saymak için onay kutusunu işaretleyin.
 - Koruma kategorisi bilgi alanında bir sorunu bildirmek için onay kutusunun işaretini kaldırın.
- 4 **Tamam**'ı tıklatın.

İpucu: Koruma kategorisi bilgi alanında bildirilen sorunun yanındaki **Yoksay** bağlantısını tıklayarak da sorunu yok sayabilirsiniz.

B Ö L Ü M 6

Uyarılarla çalışma

Uyarılar, belirli SecurityCenter olayları gerçekleştiğinde, ekranınızın sağ alt köşesinde açılan küçük iletişim kutularıdır. Uyarı, olay hakkında ayrıntılı bilgilerin yanı sıra, olayla ilişkili olabilecek sorunları çözmeye yönelik öneriler ve seçenekler de sağlar. Bazı uyarılar, olayla ilgili ek bilgilere bağlantılar da içerir. Bu bağlantılar, McAfee'nin genel Web sitesini açmanızı veya sorunu gidermek için McAfee'ye bilgi göndermenizi sağlar.

Üç tür uyarı vardır: kırmızı, sarı ve yeşil.

Uyarı Türü	Açıklama
Kırmızı	Kırmızı uyarı, sizden yanıt vermenizi isteyen kritik bir bildirimdir. SecurityCenter koruma sorununun otomatik olarak nasıl çözüleceğini belirleyemediği zaman kırmızı uyarılar oluşur.
Sarı	Sarı uyarı, genellikle sizden yanıt vermenizi isteyen kritik olmayan bir bildirimdir.
Yeşil	Yeşil uyarı, genellikle sizden yanıt vermenizi istemeyen kritik olmayan bir bildirimdir. Yeşil uyarılar, olayla ilgili temel bilgiler verir.

Uyarılar koruma durumunuzun izlenmesi ve yönetilmesinde çok önemli bir rol oynadığı için bunları devre dışı bırakamazsınız. Ancak belirli bilgi uyarılarının görüntülenip görüntülenmemesini kontrol edebilir ve diğer bazı uyarı seçeneklerini yapılandırabilirsiniz (SecurityCenter'ın uyarıyla birlikte ses çıkarıp çıkarmayacağı veya başlangıçta McAfee giriş ekranını görüntüleyip görüntülemeyeceği gibi).

Bu bölümde

Bilgi uyarılarını gösterme ve gizleme.....	22
Uyarı seçeneklerini yapılandırma	24

Bilgi uyarılarını gösterme ve gizleme

Bilgi uyarıları, bilgisayarınızın güvenliğini tehdit etmeyen olaylar olduğunda bunu size bildirir. Örneğin, Güvenlik Duvarı korumasını ayarladıysanız, bilgisayarınızdaki bir programa Internet erişimi verildiğinde varsayılan olarak bilgi uyarısı görüntülenir. Belirli bir bilgi uyarısı türünün görüntülenmesini istemiyorsanız bunu gizleyebilirsiniz. Hiçbir bilgi uyarısının görüntülenmesini istemiyorsanız tümünü gizleyebilirsiniz. Bilgisayarınızda tam ekran modunda oyun oynarken de tüm bilgi uyarılarını gizleyebilirsiniz. Oyununuz bitince tam ekran modundan çıktığınızda, SecurityCenter bilgi uyarılarını yeniden görüntülemeye başlar.

Bir bilgi uyarısını yanlışlıkla gizlediyseniz, bunu istediğiniz zaman yeniden gösterebilirsiniz. Varsayılan olarak, SecurityCenter tüm bilgi uyarılarını gösterir.

Bilgi uyarılarını gösterme veya gizleme

SecurityCenter'ı, bazı bilgi uyarılarını gösterecek veya gizleyecek ya da tüm bilgi uyarılarını gizleyecek şekilde yapılandırabilirsiniz.

- 1 Uyarı Seçenekleri bölümünü açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
 3. **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 2 SecurityCenter Yapılandırma bölümünde **Bilgi Uyarıları**'nı tıklatın.
- 3 Bilgi Uyarıları bölümünde aşağıdakileri yapın:
 - Bir bilgi uyarısını göstermek için onay kutusunu temizleyin.
 - Bir bilgi uyarısını gizlemek için onay kutusunu işaretleyin.
 - Tüm bilgi uyarılarını gizlemek için **Bilgi uyarılarını gösterme** onay kutusunu işaretleyin.
- 4 **Tamam**'ı tıklatın.

İpucu: Uyarının içinden **Bu uyarıyı bir daha gösterme** onay kutusunu işaretleyerek de bilgi uyarısını gizleyebilirsiniz. Bunu yaptığınızda, Bilgi Uyarıları bölümünde uygun onay kutusunun işaretini kaldırarak, bilgi uyarısını yeniden gösterebilirsiniz.

Oyun oynarken bilgi uyarılarını gösterme veya gizleme

Bilgisayarınızda tam ekran modunda oyun oynarken de bilgi uyarılarını gizleyebilirsiniz. Oyununuz bitince tam ekran modundan çıktığınızda, SecurityCenter bilgi uyarılarını yeniden görüntülemeye başlar.

- 1 Uyarı Seçenekleri bölmesini açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
 3. **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 2 Uyarı Seçenekleri bölmesinde **Oyun modu algılandığında bilgilendirme uyarılarını göster** onay kutusunu işaretleyin veya işaretini kaldırın.
- 3 **Tamam**'ı tıklatın.

Uyarı seçeneklerini yapılandırma

Uyarıların görünümü ve sıklığı, SecurityCenter tarafından yapılandırılır; ancak bazı temel uyarı seçeneklerini ayarlayabilirsiniz. Örneğin, uyarılarla birlikte sesi açabilir veya Windows başlatıldığında giriş ekranı uyarısının görüntülenmesini engelleyebilirsiniz. Size çevrimiçi topluluktaki virüs saldırılarını ve diğer güvenlik tehditlerini bildiren uyarıları da gizleyebilirsiniz.

Uyarılarla birlikte sesi açma

Uyarının size sesle birlikte bildirilmesini istiyorsanız, her uyarıyla birlikte ses çıkarması için SecurityCenter'ı yapılandırabilirsiniz.

- 1 Uyarı Seçenekleri bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklayın.
2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklayın.
3. **Uyarılar** altında **Gelişmiş**'i tıklayın.

- 2 Uyarı Seçenekleri bölümünde, **Ses** altında **Bir uyarı oluştuğunda ses çal** onay kutusunu işaretleyin.

Başlangıçta giriş ekranını gizleme

Varsayılan olarak, Windows başlatıldığında, SecurityCenter'ın bilgisayarınızı koruduğunu size bildiren McAfee giriş ekranı kısaca görüntülenir. Ancak bunun görüntülenmesini istemiyorsanız giriş ekranını gizleyebilirsiniz.

- 1 Uyarı Seçenekleri bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklayın.
2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklayın.
3. **Uyarılar** altında **Gelişmiş**'i tıklayın.

- 2 Uyarı Seçenekleri bölümünde, **Giriş Ekranı** altında **Windows başlangıcında McAfee giriş ekranını göster** onay kutusunun işaretini kaldırın.

İpucu: Windows başlangıcında McAfee giriş ekranını göster onay kutusunu işaretleyerek, istediğiniz zaman giriş ekranını yeniden gösterebilirsiniz.

Virüs saldırısı uyarılarını gizleme

Size çevrimiçi topluluktaki virüs saldırılarını ve diğer güvenlik tehditlerini bildiren uyarıları gizleyebilirsiniz.

- 1 Uyarı Seçenekleri bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
 3. **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 2** Uyarı Seçenekleri bölümünde **Virüs veya güvenlik tehdidi oluştuğunda beni uyar** onay kutusunun işaretini kaldırın.

İpucu: **Virüs veya güvenlik tehdidi oluştuğunda beni uyar** onay kutusunu işaretleyerek, istediğiniz zaman virüs saldırısı uyarılarını yeniden gösterebilirsiniz.

B Ö L Ü M 7

Olayları görüntüleme

Olay, koruma kategorisinde ve ilişkili koruma hizmetlerinde gerçekleşen eylem veya yapılandırma değişikliğidir. Farklı koruma hizmetleri, farklı türde olayları kaydeder. Örneğin, bir koruma hizmeti etkinleştirilir veya devre dışı bırakılırsa, SecurityCenter olay kaydeder; Virus Protection, virüs algılandığında ve kaldırıldığında olay kaydeder; Firewall Protection ise, Internet'e bağlanma denemesi engellendiğinde olay kaydeder. Koruma kategorileri hakkında ayrıntılı bilgi için bkz. Koruma kategorileri hakkında bilgi (sayfa 9).

Yapılandırma sorunlarını giderirken ve başka kullanıcılar tarafından gerçekleştirilen işlemleri incelerken olayları görüntüleyebilirsiniz. Pek çok ebeveyn, çocuklarının Internet'teki davranış biçimini izlemek için olay günlüğünü kullanır. Yalnızca gerçekleşen en son 30 olayı incelemek istiyorsanız son olayları görüntülersiniz. Gerçekleşen tüm olayların kapsamlı listesini incelemek istiyorsanız tüm olayları görüntülersiniz. Tüm olayları görüntülediğinizde, SecurityCenter olayları gerçekleştikleri koruma kategorisine göre sıralayan olay günlüğünü başlatır.

Bu bölümde

Son olayları görüntüleme	27
Tüm olayları görüntüleme	27

Son olayları görüntüleme

Yalnızca gerçekleşen en son 30 olayı incelemek istiyorsanız son olayları görüntülersiniz.

- **Ortak Görevler** altında **Son Olayları Görüntüle**'yi tıklatın.

Tüm olayları görüntüleme

Gerçekleşen tüm olayların kapsamlı listesini incelemek istiyorsanız tüm olayları görüntülersiniz.

- 1 **Ortak Görevler** altında **Son Olayları Görüntüle**'yi tıklatın.
- 2 Son Olaylar bölümünde **Günlüğü Görüntüle**'yi tıklatın.
- 3 Olay günlüğünün soldaki bölümünde, görüntülemek istediğiniz olay türlerini tıklatın.

B Ö L Ü M 8

McAfee VirusScan

VirusScan'ın gelişmiş algılama ve koruma hizmetleri, sizi ve bilgisayarınızı virüsler, Truva atları, izleme tanımlama bilgileri, casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar gibi en son güvenlik tehditlerinden korur. Koruma, masaüstü bilgisayarınızdaki dosya ve klasörlerin ötesine geçerek, e-posta, anlık iletiler ve Web gibi farklı giriş noktalarından gelen tehditleri hedefler.

VirusScan ile bilgisayarınızda anında ve sürekli koruma sağlanır (zahmetli yönetim gerekmez). Siz çalışırken, oyun oynarken, Web'de gezinirken veya e-postanızı kontrol ederken, program arka planda çalışır ve olası zararları gerçek zamanlı izler, tarar ve algılar. Kapsamlı taramalar zamanlamaya göre çalışır ve birtakım gelişmiş seçenekler kullanarak bilgisayarınızı düzenli olarak denetler. VirusScan, isterseniz size bu davranışı özelleştirme esnekliği sağlar; ancak özelleştirme yapmasanız da bilgisayarınız korunur.

Normal bilgisayar kullanımı sırasında virüsler, solucanlar ve diğer olası tehditler bilgisayarınıza sızabilir. VirusScan, bu durumda size tehdidi bildirir ve genellikle bunu sizin için ele alarak herhangi bir zarara yol açmadan virüs bulaşan öğeleri temizler veya karantinaya alır. Nadiren daha fazla işlem gerekebilir. VirusScan, bu tür durumlarda ne yapılması gerektiğine (bilgisayarınızı bir daha başlattığınızda yeniden tarama yapmak, algılanan öğeyi saklamak veya algılanan öğeyi kaldırmak) karar vermenize olanak tanır.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

VirusScan özellikleri.....	30
Gerçek zamanlı virüsten korumayı başlatma.....	31
Ek korumayı başlatma	33
Virüsten korumayı ayarlama	37
Bilgisayarınızı tarama	55
Tarama sonuçlarıyla çalışma.....	59

VirusScan özellikleri

VirusScan aşağıdaki özellikleri sunar.

Kapsamlı virüsten koruma

VirusScan'ın gelişmiş algılama ve koruma hizmetleri, sizi ve bilgisayarınızı virüsler, Truva atları, izleme tanımlama bilgileri, casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar gibi en son güvenlik tehditlerinden korur. Koruma, masaüstü bilgisayarınızdaki dosya ve klasörlerin ötesine geçerek, e-posta, anlık iletiler ve Web gibi farklı giriş noktalarından gelen tehditleri hedefler. Zahmetli yönetim gerektirmez.

Kaynakları bilen tarama seçenekleri

Tarama hızı yavaşlarsa, minimum bilgisayar kaynağının kullanılması için seçeneği devre dışı bırakabilirsiniz; ancak virüs korumasına diğer görevlerden daha fazla öncelik tanınacağını unutmayın. VirusScan, isterseniz size gerçek zamanlı ve el ile tarama seçeneklerini özelleştirme esnekliği sağlar; ancak özelleştirme yapmasanız da bilgisayarınız korunur.

Otomatik düzeltmeler

VirusScan gerçek zamanlı veya el ile tarama çalıştırırken bir güvenlik tehdidi algılırsa, tehdit türüne göre tehdidi otomatik olarak ele almayı dener. Bu yolla, pek çok tehdit algılanabilir ve sizin müdahaleniz olmadan etkisiz hale getirilebilir. Nadiren VirusScan tehdidi kendi başına etkisiz hale getiremeyebilir. VirusScan, bu tür durumlarda ne yapılması gerektiğine (bilgisayarınızı bir daha başlattığınızda yeniden tarama yapmak, algılanan öğeyi saklamak veya algılanan öğeyi kaldırmak) karar vermenize olanak tanır.

Tam ekran modunda görevleri duraklatma

Film izlemek, bilgisayarınızda oyun oynamak gibi şeylerin veya bilgisayar ekranınızın tamamını kaplayan herhangi bir etkinliğin keyfini çıkarırken, VirusScan otomatik güncelleştirmeler ve el ile taramalar gibi çeşitli görevleri duraklatır.

Gerçek zamanlı virüsten korumayı başlatma

VirusScan iki tür virüsten koruma sağlar: gerçek zamanlı ve el ile. Gerçek zamanlı virüsten koruma, siz veya bilgisayarınız dosyalara erişince bunları tarayarak, bilgisayarınızda virüs etkinliğini sürekli izler. El ile virüsten koruma, istediğinizde dosyaları sizin taramanıza olanak verir. Bilgisayarınızın en son güvenlik tehditlerine karşı korunduğundan emin olmak için gerçek zamanlı virüsten korumayı açık bırakın ve düzenli, daha kapsamlı el ile taramalar için zamanlama yapın. Varsayılan olarak, VirusScan haftada bir kez zamanlanan tarama gerçekleştirir. Gerçek zamanlı ve el ile tarama hakkında ayrıntılı bilgi için bkz. Bilgisayarınızı tarama (sayfa 55).

Nadiren gerçek zamanlı taramayı geçici olarak durdurmak isteyebilirsiniz (örneğin bazı tarama seçeneklerini değiştirmek veya bir performans sorununu gidermek için). Gerçek zamanlı virüsten koruma deve dışı bırakıldığında, bilgisayarınız korunmaz ve SecurityCenter koruma durumunuz kırmızı olur. Koruma durumu hakkında ayrıntılı bilgi için SecurityCenter yardımında bkz. "Koruma durumu hakkında bilgi".

Gerçek zamanlı virüsten korumayı başlatma

Varsayılan olarak, gerçek zamanlı virüsten koruma açıktır ve bilgisayarınızı virüslerden, Truva atlarından ve diğer güvenlik tehditlerinden korur. Gerçek zamanlı virüsten korumayı kapattığınızda, korunmak için bunu yeniden açmanız gerekir.

- 1 Bilgisayar ve Dosyalar Yapılandırma bölmesini açın.
Nasıl?
 1. Soldaki bölmede **Gelişmiş Menü**'yü tıklayın.
 2. **Yapılandır**'ı tıklayın.
 3. Yapılandır bölmesinde **Bilgisayar ve Dosyalar**'ı tıklayın.
- 2 **Virüsten koruma** altında **Açık**'ı tıklayın.

Gerçek zamanlı virüsten korumayı durdurma

Gerçek zamanlı virüsten korumayı kapatabilir ve sonra yeniden devam edeceği zamanı belirtebilirsiniz. Bilgisayarınız yeniden başlatıldıktan 15, 30, 45 veya 60 dakika sonra korumayı otomatik olarak devam ettirebilir veya hiçbir zaman devam ettirmeyebilirsiniz.

- 1 Bilgisayar ve Dosyalar Yapılandırma bölmesini açın.
Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
2. **Yapılandır**'ı tıklatın.
3. Yapılandır bölmesinde **Bilgisayar ve Dosyalar**'ı tıklatın.
- 2 **Virüsten koruma** altında **Kapalı**'yı tıklatın.
- 3 İletişim kutusunda, gerçek zamanlı taramanın devam edeceği zamanı seçin.
- 4 **Tamam**'ı tıklatın.

B Ö L Ü M 9

Ek korumayı başlatma

VirusScan, gerçek zamanlı virüsten korumanın yanı sıra, komut dosyalarına, casus yazılımlara ve olası zararlı e-posta ve anlık ileti eklerine karşı gelişmiş koruma sağlar. Varsayılan olarak, komut dosyası tarama özelliği, casus yazılım, e-posta ve anlık ileti koruması açıktır ve bilgisayarınızı korur.

Komut dosyası tarama

Komut dosyası tarama koruması, olası zararlı komut dosyalarını algılar ve bunların bilgisayarınızda çalışmasını engeller. Bilgisayarınızda, dosyalar oluşturan, kopyalayan veya silen ya da Windows kayıt defterini açan komut dosyaları gibi şüpheli komut dosyası etkinliklerini izler ve herhangi bir zarar oluşmadan sizi uyarır.

Casus yazılım koruması

Casus yazılım koruması, casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programları algılar. Casus yazılım, davranışınızı izlemek, kişisel bilgilerinizi toplamak ve hatta ek yazılımlar yükleyerek veya tarayıcı etkinliğinizin yönünü değiştirerek bilgisayarınızın kontrolünü ele geçirmek için gizlice bilgisayarınıza yüklenebilen yazılımdır.

E-posta koruması

E-posta koruması, gönderdiğiniz ve aldığınız e-posta iletileri ve eklerindeki şüpheli etkinliği algılar.

Anlık ileti koruması

Anlık ileti koruması, aldığınız anlık ileti eklerindeki olası güvenlik tehditlerini algılar. Ayrıca, anlık ileti programlarının kişisel bilgileri paylaşmasını engeller.

Bu bölümde

Komut dosyası tarama korumasını başlatma	34
Casus yazılım korumasını başlatma	34
E-posta korumasını başlatma	34
Anlık ileti korumasını başlatma	35

Komut dosyası tarama korumasını başlatma

Olası zararlı komut dosyalarını algılaması ve bunların bilgisayarınızda çalışmasını engellemesi için komut dosyası tarama korumasını açın. Komut dosyası tarama koruması, bir komut dosyası bilgisayarınızda dosyalar oluşturmaya, kopyalamaya veya silmeye ya da Windows kayıt defterinde değişiklik yapmaya çalıştığında bunu size bildirir.

- 1 Bilgisayar ve Dosyalar Yapılandırma bölümünü açın.
Nasıl?
 1. Soldaki bölmede **Gelişmiş Menü**'yü tıklayın.
 2. **Yapılandır**'ı tıklayın.
 3. Yapılandır bölümünde **Bilgisayar ve Dosyalar**'ı tıklayın.

- 2 **Komut dosyası tarama koruması** altında **Açık**'ı tıklayın.

Not: İstediğiniz zaman komut dosyası tarama korumasını kapatabilmenize karşın, bunu yaparsanız bilgisayarınız zararlı komut dosyalarına karşı korumasız kalır.

Casus yazılım korumasını başlatma

Casus yazılımları, reklam yazılımları ve sizin bilginiz veya izniniz olmadan bilgi toplayan ve ileten diğer olası istenmeyen programları algılaması ve kaldırması için casus yazılım korumasını açın.

- 1 Bilgisayar ve Dosyalar Yapılandırma bölümünü açın.
Nasıl?
 1. Soldaki bölmede **Gelişmiş Menü**'yü tıklayın.
 2. **Yapılandır**'ı tıklayın.
 3. Yapılandır bölümünde **Bilgisayar ve Dosyalar**'ı tıklayın.

- 2 **Komut dosyası tarama koruması** altında **Açık**'ı tıklayın.

Not: İstediğiniz zaman casus yazılım korumasını kapatabilmenize karşın, bunu yaparsanız bilgisayarınız olası istenmeyen programlara karşı korumasız kalır.

E-posta korumasını başlatma

Solucanların yanı sıra giden (SMTP) ve gelen (POP3) e-posta iletileri ve eklerindeki olası tehditleri algılaması için e-posta korumasını açın.

- 1 E-posta ve Anlık İleti Yapılandırma bölümünü açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
2. **Yapılandır**'ı tıklatın.
3. Yapılandır bölümünde **E-posta ve Anlık İleti**'yi tıklatın.

2 E-posta koruması altında Açık'ı tıklatın.

Not: İsteddiğiniz zaman e-posta korumasını kapatabilmenize karşın, bunu yaparsanız bilgisayarınız e-posta tehditlerine karşı korumasız kalır.

Anlık ileti korumasını başlatma

Gelen anlık ileti eklerinde bulunabilen güvenlik tehditlerini algılaması için anlık ileti korumasını açın.

1 E-posta ve Anlık İleti Yapılandırma bölümünü açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
2. **Yapılandır**'ı tıklatın.
3. Yapılandır bölümünde **E-posta ve Anlık İleti**'yi tıklatın.

2 Anlık İleti koruması altında Açık'ı tıklatın.

Not: İsteddiğiniz zaman anlık ileti korumasını kapatabilmenize karşın, bunu yaparsanız bilgisayarınız zararlı anlık ileti eklerine karşı korumasız kalır.

B Ö L Ü M 1 0

Virüsten korumayı ayarlama

VirusScan iki tür virüsten koruma sağlar: gerçek zamanlı ve el ile. Gerçek zamanlı virüsten koruma, siz veya bilgisayarınız dosyalara erişince bunları tarar. El ile virüsten koruma, istediğinizde dosyaları sizin taramanıza olanak verir. Her koruma türü için farklı seçenekler ayarlayabilirsiniz. Örneğin, gerçek zamanlı koruma bilgisayarınızı sürekli izlediği için isteğe bağlı el ile korumaya yönelik daha kapsamlı tarama seçeneklerini ayırarak, temel tarama seçeneklerinden oluşan bir grubu seçebilirsiniz.

Bu bölümde

Gerçek zamanlı tarama seçeneklerini ayarlama.....	38
El ile tarama seçeneklerini ayarlama	40
Sistem Koruması seçeneklerini kullanma	44
Güvenilenler listelerini kullanma	51

Gerçek zamanlı tarama seçeneklerini ayarlama

Gerçek zamanlı virüsten korumayı başlattığınızda, VirusScan dosyaları taramak için varsayılan birtakım seçenekler kullanır; ancak varsayılan seçenekleri gereksinimlerinize uygun şekilde değiştirebilirsiniz.

Gerçek zamanlı tarama seçeneklerini değiştirmek için tarama sırasında VirusScan'ın neleri denetleyeceğini, tarayacağı konumları ve dosya türlerini belirlemeniz gerekir. Örneğin, VirusScan'ın davranışınızı izlemek için Web siteleri tarafından kullanılan bilinmeyen virüsleri veya tanımlama bilgilerini denetleyip denetlemeyeceğini ve bilgisayarınızla veya yalnızca yerel sürücülerle eşleştirilen ağ sürücülerini tarayıp taramayacağını belirleyebilirsiniz. Hangi dosya türlerinin (tüm dosyalar veya yalnızca çoğu virüsün algılandığı yer olan program dosyaları ve belgeler) taranacağını da belirleyebilirsiniz.

Gerçek zamanlı tarama seçeneklerini değiştirirken, bilgisayarınızda arabellek taşıması koruması olmasının önemli olup olmadığını da belirlemeniz gerekir. Arabellek, bilgisayar bilgilerini geçici olarak tutmak için kullanılan bellek bölümüdür. Arabellek taşmaları, şüpheli programların ve işlemlerin arabellekte depoladığı bilgi miktarı arabellek kapasitesini aştığı zaman gerçekleşebilir. Bu olursa, bilgisayarınız güvenlik saldırılarına açık hale gelir.

Gerçek zamanlı tarama seçeneklerini ayarlama

Gerçek zamanlı tarama sırasında VirusScan'ın neleri arayacağını, tarayacağı konumları ve dosya türlerini özelleştirmek için gerçek zamanlı tarama seçeneklerini ayarlarsınız. Seçenekler, bilinmeyen virüsleri ve tanımlama bilgilerini taramanın yanı sıra, arabellek taşıma koruması sağlamayı içerir. Gerçek zamanlı taramayı, bilgisayarınızla eşleştirilen ağ sürücülerini denetlemesi için de yapılandırabilirsiniz.

1 Gerçek Zamanlı Tarama bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'ı tıklatın.
 3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklatın.
 4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, virüsten korumanın etkin olduğundan emin olun ve sonra **Gelişmiş**'i tıklatın.
- 2 Gerçek zamanlı tarama seçeneklerinizi belirtin ve sonra **Tamam**'ı tıklatın.

Bunu yapmak için...	Bunu yapın...
Bilinmeyen virüsleri ve bilinen virüslerin yeni türevlerini algılamak	Sezgisel yöntem kullanarak bilinmeyen virüsleri tara onay kutusunu işaretleyin.
Tanımlama bilgilerini algılamak	İzleme tanımlama bilgilerini tara ve temizle onay kutusunu işaretleyin.
Ağınıza bağlı sürücülerde virüsleri ve diğer olası tehditleri algılamak	Ağ sürücülerini tara onay kutusunu işaretleyin.
Bilgisayarınızı arabellek taşmalarından korumak	Arabellek taşması korumasını etkinleştir onay kutusunu işaretleyin.
Hangi dosya türlerinin taranacağını belirtmek	Tüm dosyalar (önerilir) veya Yalnızca program dosyaları ve belgeler 'i tıklatın.

El ile tarama seçeneklerini ayarlama

El ile virüsten koruma, istediğinizde dosyaları sizin taramanıza olanak verir. El ile taramayı başlattığınızda, VirusScan daha kapsamlı birtakım tarama seçenekleri kullanarak bilgisayarınızda virüsleri ve diğer olası zararlı öğeleri denetler. El ile tarama seçeneklerini değiştirmek için VirusScan'ın tarama sırasında neleri denetleyeceğini belirlemeniz gerekir. Örneğin, VirusScan'ın virüsleri, casus yazılım veya reklam yazılım gibi olası istenmeyen programları, bilgisayarınıza yetkisiz erişim verebilen köke inme programları gibi hayalet programları ve Web sitelerinin davranışınızı izlemek için kullanabileceği tanımlama bilgilerini arayıp aramayacağını belirleyebilirsiniz. Denetlenen dosya türlerini de belirlemeniz gerekir. Örneğin, VirusScan'ın tüm dosyaları mı yoksa yalnızca program dosyaları ve belgeleri mi (burası çoğu virüsün algılandığı yer olduğu için) belirleyebilirsiniz. Taramaya arşiv dosyalarının (örneğin .zip dosyaları) eklenip eklenmeyeceğini de belirtebilirsiniz.

Varsayılan olarak, VirusScan her el ile tarama çalıştırdığında, bilgisayarınızdaki tüm sürücüler ve klasörleri denetler; ancak varsayılan konumları, gereksinimlerinize uygun olarak değiştirebilirsiniz. Örneğin, yalnızca kritik sistem dosyalarını, masaüstünüzdeki öğeleri veya Program Files klasöründeki öğeleri tarayabilirsiniz. Her el ile taramayı kendiniz başlatmak istemiyorsanız, taramalar için düzenli zamanlama ayarlayabilirsiniz. Zamanlanan taramalar, her zaman varsayılan tarama seçeneklerini kullanarak tüm bilgisayarınızı denetler. Varsayılan olarak, VirusScan haftada bir kez zamanlanan tarama gerçekleştirir.

Tarama hızının yavaşladığını fark ederseniz, minimum bilgisayar kaynağının kullanılması için seçeneği devre dışı bırakmayı düşünün; ancak virüs korumasına diğer görevlerden daha fazla öncelik tanınacağını unutmayın.

Not: Film izlemek, bilgisayarınızda oyun oynamak gibi şeylerin veya bilgisayar ekranınızın tamamını kaplayan herhangi bir etkinliğin keyfini çıkarırken, VirusScan otomatik güncelleştirmeler ve el ile taramalar gibi çeşitli görevleri duraklatır.

El ile tarama seçeneklerini ayarlama

El ile tarama sırasında VirusScan'ın neleri arayacağını, tarayacağı konumları ve dosya türlerini özelleştirmek için el ile tarama seçeneklerini ayarlarsınız. Seçenekler; bilinmeyen virüsleri, dosya arşivlerini, casus yazılımları ve olası istenmeyen programları, izleme tanımlama bilgilerini, köke inme programlarını ve hayalet programları içerir.

1 El İle Tarama bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'ı tıklatın.
 3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklatın.
 4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, virüsten korumanın etkin olduğundan emin olun ve **Gelişmiş**'i tıklatın.
 5. Virüsten Koruma bölümünde **El ile Tarama**'yı tıklatın.
- 2 El ile tarama seçeneklerinizi belirtin ve sonra **Tamam**'ı tıklatın.

Bunu yapmak için...	Bunu yapın...
Bilinmeyen virüsleri ve bilinen virüslerin yeni türevlerini algılamak	Sezgisel yöntem kullanarak bilinmeyen virüsleri tara onay kutusunu işaretleyin.
.Zip ve diğer arşiv dosyalarındaki virüsleri algılamak ve kaldırmak	.zip ve diğer arşiv dosyalarını tara onay kutusunu işaretleyin.
Casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programları algılamak	Casus yazılım ve olası istenmeyen programları tara onay kutusunu işaretleyin.
Tanımlama bilgilerini algılamak	İzleme tanımlama bilgilerini tara ve temizle onay kutusunu işaretleyin.
Varolan Windows sistem dosyalarını değiştirebilen ve kullanabilen köke inme programlarını ve hayalet programları algılamak	Köke inme programları ve diğer hayalet programları tara onay kutusunu işaretleyin.
Taramalar için daha az işlemci gücü kullanmak diğer görevlere (Web'de gezinme veya dosyalar açma gibi) daha yüksek öncelik tanımak	En az bilgisayar kaynağı kullanarak tara onay kutusunu işaretleyin.
Hangi dosya türlerinin taranacağını belirtmek	Tüm dosyalar (önerilir) veya Yalnızca program dosyaları ve belgeler 'i tıklatın.

El ile tarama konumunu ayarlama

El ile tarama sırasında VirusScan'ın virüsleri ve diğer zararlı öğeleri nerede arayacağını belirlemek için el ile tarama konumunu ayarlarsınız. Bilgisayarınızdaki tüm dosyalar, klasörler ve sürücüler tarayabilir veya tarama işlemini belirli klasörler ve sürücülerle sınırlandırabilirsiniz.

1 El İle Tarama bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklayın.
2. SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'ı tıklayın.
3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklayın.
4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, virüsten korumanın etkin olduğundan emin olun ve **Gelişmiş**'i tıklayın.
5. Virüsten Koruma bölümünde **El İle Tarama**'yı tıklayın.

2 Taranacak Varsayılan Konum'u tıklayın.

3 El ile tarama konumunu belirtin ve sonra **Tamam**'ı tıklayın.

Bunu yapmak için...	Bunu yapın...
Bilgisayarınızdaki tüm dosya ve klasörleri taramak	Bilgisayarım onay kutusunu işaretleyin.
Bilgisayarınızdaki belirli dosyalar, klasörler ve sürücüler taramak	Bilgisayarım onay kutusunun işaretini kaldırın ve bir veya birkaç klasör veya sürücü seçin.
Kritik sistem dosyalarını taramak	Bilgisayarım onay kutusunun işaretini kaldırın ve sonra Kritik Sistem Dosyaları onay kutusunu işaretleyin.

Bir tarama zamanlama

Haftanın herhangi bir gününde ve saatinde bilgisayarınızda virüsleri ve diğer tehditleri kapsamlı olarak denetlemek için taramalar zamanlayın. Zamanlanan taramalar, her zaman varsayılan tarama seçeneklerini kullanarak tüm bilgisayarınızı denetler. Varsayılan olarak, VirusScan haftada bir kez zamanlanan tarama gerçekleştirir. Tarama hızının yavaşladığını fark ederseniz, minimum bilgisayar kaynağının kullanılması için seçeneği devre dışı bırakmayı düşünün; ancak virüs korumasına diğer görevlerden daha fazla öncelik tanınacağını unutmayın.

1 Zamanlanan Tarama bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'ı tıklatın.
3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklatın.
4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, virüsten korumanın etkin olduğundan emin olun ve **Gelişmiş**'i tıklatın.
5. Virüsten Koruma bölümünde **Zamanlanan Tarama**'yı tıklatın.

2 Zamanlanan taramayı etkinleştir'i seçin.

3 Normalde tarama işlemi için kullanılan işlemci miktarını azaltmak için **En az bilgisayar kaynağı kullanarak tara**'yı seçin.

4 Bir veya birkaç gün seçin.

5 Başlangıç zamanını belirtin.

6 **Tamam**'ı tıklatın.

İpucu: **Sıfırla**'yı tıklatarak varsayılan zamanlamayı geri yükleyebilirsiniz.

Sistem Koruması seçeneklerini kullanma

Sistem Koruması, bilgisayarınızda Windows kayıt defterinde veya kritik sistem dosyalarında yapılan olası yetkisiz değişiklikleri izler, günlüğe kaydeder, bildirir ve yönetir. Yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınıza zarar verebilir, güvenliğini tehlikeye atabilir ve değerli sistem dosyalarını bozabilir.

Kayıt defteri ve dosya değişiklikleri yaygındır ve bilgisayarınızda düzenli olarak gerçekleşebilir. Değişikliklerin pek çoğu zararsız olduğu için Sistem Koruması'nın varsayılan ayarları, önemli zarar olasılığı bulunan yetkisiz değişikliklere karşı güvenilir, akıllı ve somut koruma sağlamak üzere yapılandırılmıştır. Örneğin, Sistem Koruması yaygın olmayan ve önemli bir tehdit oluşturma olasılığı bulunan değişiklikler algıladığında, etkinlik hemen bildirilir ve günlüğe kaydedilir. Daha yaygın olan ancak yine de zarar verme olasılığı bulunan değişiklikler yalnızca günlüğe kaydedilir. Ancak standart ve düşük riskli değişikliklerin izlenmesi varsayılan olarak devre dışıdır. Sistem Koruması teknolojisinin korumasını, istediğiniz herhangi bir ortamı kapsayacak şekilde yapılandırabilirsiniz.

Üç tür Sistem Koruması vardır: Program Sistem Koruması, Windows Sistem Koruması ve Tarayıcı Sistem Koruması.

Program Sistem Koruması

Program Sistem Koruması, bilgisayarınızın kayıt defterindeki ve Windows tarafından kullanılan diğer kritik dosyalardaki olası yetkisiz değişiklikleri algılar. Bu önemli kayıt defteri öğeleri ve dosyaları; ActiveX yüklemelerini, başlangıç öğelerini, Windows kabuk yürütme kancalarını ve kabuk hizmeti nesne gecikme yüklemelerini içerir. Program Sistem Koruması teknolojisi, bunları izleyerek şüpheli ActiveX programlarının (İnternet'ten yüklenen) yanı sıra casus yazılımları ve Windows başlatıldığında otomatik olarak açılabilen olası istenmeyen programları durdurur.

Windows Sistem Koruması

Windows Sistem Koruması da bilgisayarınızın kayıt defterindeki ve Windows tarafından kullanılan diğer kritik dosyalardaki olası yetkisiz değişiklikleri algılar. Bu önemli kayıt defteri öğeleri ve dosyalar; içerik menüsü işleyicileri, applnit DLL dosyaları ve Windows hosts dosyasını içerir. Windows Sistem Koruması teknolojisi, bunları izleyerek bilgisayarınızın İnternet üzerinden yetkisiz veya kişisel bilgileri gönderip almasını engellemeye yardımcı olur. Ayrıca siz ve aileniz için önemli olan programların görünümünde ve davranışında istenmeyen değişiklikler yapabilen şüpheli programları durdurmaya yardımcı olur.

Tarayıcı Sistem Koruması

Program ve Windows Sistem Koruması gibi Sistem Koruması da bilgisayarınızın kayıt defterindeki ve Windows tarafından kullanılan diğer kritik dosyalardaki olası yetkisiz değişiklikleri algılar. Ancak Tarayıcı Sistem Koruması; Internet Explorer eklentileri, Internet Explorer URL'leri ve Internet Explorer güvenlik bölgeleri gibi önemli kayıt defteri öğeleri ve dosyalarındaki değişiklikleri izler. Tarayıcı Sistem Koruması teknolojisi, bunları izleyerek şüpheli Web sitelerine yeniden yönlendirme, tarayıcı ayarlarında ve seçeneklerinde habersiz değişiklik yapma ve şüpheli Web sitelerine istenmeyen şekilde güvenme gibi yetkisiz tarayıcı etkinliğini engellemeye yardımcı olur.

Sistem Koruması'nı etkinleştirme

Bilgisayarınızda olası istenmeyen Windows kayıt defteri ve dosya değişikliklerini algılayıp size bildirmesi için Sistem Koruması'nı etkinleştirin. Yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınıza zarar verebilir, güvenliğini tehlikeye atabilir ve değerli sistem dosyalarını bozabilir.

1 Bilgisayar ve Dosyalar Yapılandırma bölümünü açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklayın.
2. **Yapılandır**'ı tıklayın.
3. Yapılandır bölümünde **Bilgisayar ve Dosyalar**'ı tıklayın.

2 Sistem Koruması altında **Açık**'ı tıklayın.

Not: **Kapalı**'yı tıklayarak Sistem Koruması'nı devre dışı bırakabilirsiniz.

Sistem Koruması seçeneklerini yapılandırma

Windows dosyaları, programları ve Internet Explorer ile ilişkili yetkisiz kayıt defteri ve dosya değişikliklerine karşı koruma, günlüğe kaydetme ve uyarı seçeneklerini yapılandırmak için Sistem Koruması bölümünü kullanın. Yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınıza zarar verebilir, güvenliğini tehlikeye atabilir ve değerli sistem dosyalarını bozabilir.

1 Sistem Koruması bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'ı tıklatın.
3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklatın.
4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, Sistem Koruması'nın etkin olduğundan emin olun ve **Gelişmiş**'i tıklatın.

2 Listedeki Sistem Koruması türünü seçin.

- **Program Sistem Koruması**
- **Windows Sistem Koruması**
- **Tarayıcı Sistem Koruması**

3 **Şunu yapmak istiyorum** altında aşağıdakilerden birini gerçekleştirin:

- Program, Windows ve Tarayıcı Sistem Koruması ile ilişkili yetkisiz kayıt defteri ve dosya değişikliklerini algılamak, günlüğe kaydetmek ve bildirmek için **Uyarıları göster**'i tıklatın.
- Program, Windows ve Tarayıcı Sistem Koruması ile ilişkili yetkisiz kayıt defteri ve dosya değişikliklerini algılamak ve günlüğe kaydetmek için **Değişiklikleri yalnızca günlüğe kaydet**'i tıklatın.
- Program, Windows ve Tarayıcı Sistem Koruması ile ilişkili yetkisiz kayıt defteri ve dosya değişikliklerini algılama özelliğini devre dışı bırakmak için **Bu Sistem Koruması'nı devre dışı bırak**'ı tıklatın.

Not: Sistem Koruması türleri hakkında ayrıntılı bilgi için bkz. Sistem Koruması türleri hakkında (sayfa 47).

Sistem Koruması türleri hakkında

Sistem Koruması, bilgisayarınızın kayıt defterindeki ve Windows tarafından kullanılan diğer kritik dosyalardaki olası yetkisiz değişiklikleri algılar. Üç tür Sistem Koruması vardır: Program Sistem Koruması, Windows Sistem Koruması ve Tarayıcı Sistem Koruması

Program Sistem Koruması

Program Sistem Koruması teknolojisi, şüpheli ActiveX programlarının (İnternet'ten yüklenen) yanı sıra casus yazılımları ve Windows başlatıldığında otomatik olarak açılabilen olası istenmeyen programları durdurur.

Sistem Koruması	Şunları algılar...
ActiveX Yüklemeleri	Bilgisayarınıza zarar verebilen, güvenliğini tehlikeye atabilen ve değerli sistem dosyalarını bozabilen ActiveX yüklemelerinde yapılan yetkisiz kayıt defteri değişiklikleri.
Başlangıç Öğeleri	Başlangıç öğelerine dosya değişiklikleri yükleyerek, bilgisayarınızı başlattığınızda şüpheli programların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar.
Windows Kabuk Yürütme Kancaları	Güvenlik programlarının düzgün şekilde çalışmasını engellemek için Windows kabuk yürütme kancaları yükleyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Kabuk Hizmeti Nesne Gecikme Yükleme	Kabuk hizmeti nesne gecikme yüklemesi üzerinde kayıt defteri değişiklikleri yaparak, bilgisayarınızı başlattığınızda zararlı dosyaların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.

Windows Sistem Koruması

Windows Sistem Koruması teknolojisi, bilgisayarınızın Internet üzerinden yetkisiz veya kişisel bilgileri gönderip almasını engellemeye yardımcı olur. Ayrıca siz ve aileniz için önemli olan programların görünümünde ve davranışında istenmeyen değişiklikler yapabilen şüpheli programları durdurmaya yardımcı olur.

Sistem Koruması	Şunları algılar...
İçerik Menüsü İşleyicileri	Windows menülerinin görünümünü ve davranışını etkileyebilen Windows içerik menüsü işleyicilerinde yapılan yetkisiz kayıt defteri değişiklikleri. İçerik menüleri, bilgisayarınızda dosyaları sağ tıklatmak gibi eylemler gerçekleştirmenize izin verir.
AppInit DLL'ler	Bilgisayarınızı başlattığınızda olası zararlı dosyaların çalışmasına izin verebilen Windows appinit DLL dosyalarında yapılan yetkisiz kayıt defteri değişiklikleri.
Windows Hosts Dosyası	Windows Hosts dosyanızda yetkisiz değişiklikler yaparak, tarayıcınızın şüpheli Web sitelerine yönlendirilmesine ve yazılım güncelleştirmelerinin engellenmesine izin verebilen casus yazılımlar, reklam yazılımlar ve olası istenmeyen programlar.
Winlogon Kabuğu	Winlogon kabuğu üzerinde kayıt defteri değişiklikleri yaparak, diğer programların Windows Explorer yerine geçmesine izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Winlogon Kullanıcı Başlatma	Winlogon kullanıcı başlatma üzerinde kayıt defteri değişiklikleri yaparak, Windows oturumu açtığınızda şüpheli programların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Windows Protokolleri	Windows protokolleri üzerinde kayıt defteri değişiklikleri yaparak, bilgisayarınızın Internet'te bilgi gönderme ve alma biçimini etkileyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Winsock Katmanlı Hizmet Sağlayıcıları	Internet'te gönderip aldığınız bilgileri ele geçirmek ve değiştirmek için Winsock Katmanlı Hizmet Sağlayıcıları (LSP) üzerine kayıt defteri değişiklikleri yükleyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Windows Kabuk Açma Komutları	Solucanların ve diğer zararlı programların bilgisayarınızda çalışmasına izin verebilen Windows kabuk açma komutları üzerinde yapılan yetkisiz değişiklikler.

Paylaşılan Görev Zamanlayıcı	Paylaşılan görev zamanlayıcı üzerinde kayıt defteri ve dosya değişiklikleri yaparak, bilgisayarınızı başlattığınızda olası zararlı dosyaların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Windows Messenger Hizmeti	Windows messenger hizmeti üzerinde kayıt defteri değişiklikleri yaparak, bilgisayarınızda istenmeyen reklamlara ve uzaktan çalıştırılan programlara izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Windows Win.ini Dosyası	Win.ini dosyasında değişiklikler yaparak, bilgisayarınızı başlattığınızda şüpheli programların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar.

Tarayıcı Sistem Koruması

Tarayıcı Sistem Koruması teknolojisi, şüpheli Web sitelerine yeniden yönlendirme, tarayıcı ayarlarında ve seçeneklerinde habersiz değişiklik yapma ve şüpheli Web sitelerine istenmeyen şekilde güvenme gibi yetkisiz tarayıcı etkinliğini engellemeye yardımcı olur.

Sistem Koruması	Şunları algılar...
Tarayıcı Yardımcı Nesneleri	Web'de gezinmeyi izlemek ve istenmeyen reklamları göstermek için tarayıcı yardımcı nesneleri kullanabilen casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar.
Internet Explorer Çubukları	Internet Explorer'ın görünümünü ve davranışını etkileyebilen Ara ve Sık Kullanılanlar gibi Internet Explorer Çubuğu programlarında yapılan yetkisiz kayıt defteri değişiklikleri.
Internet Explorer Eklentileri	Web'de gezinmeyi izlemek ve istenmeyen reklamları göstermek için Internet Explorer eklentileri yükleyebilen casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar.
Internet Explorer ShellBrowser	Web tarayıcınızın görünümünü ve davranışını etkileyebilen Internet Explorer shell browser üzerinde yapılan yetkisiz kayıt defteri değişiklikleri.
Internet Explorer Web Tarayıcısı	Tarayıcınızın görünümünü ve davranışını etkileyebilen Internet Explorer Web tarayıcısı üzerinde yapılan yetkisiz kayıt defteri değişiklikleri.

Internet Explorer URL Arama Kancaları	Internet Explorer URL arama kancalarında kayıt defteri değişiklikleri yaparak, tarayıcınızın Web'de arama yaparken şüpheli Web sitelerine yönlendirilmesine izin verebilen casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar.
Internet Explorer URL'leri	Internet Explorer URL'lerinde kayıt defteri değişiklikleri yaparak tarayıcı ayarlarını etkileyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Internet Explorer Kısıtlamaları	Internet Explorer kısıtlamaları üzerinde kayıt defteri değişiklikleri yaparak, tarayıcı ayarlarını ve seçeneklerini etkileyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Internet Explorer Güvenlik Bölgeleri	Internet Explorer güvenlik bölgeleri üzerinde kayıt defteri değişiklikleri yaparak, bilgisayarınızı başlattığınızda olası zararlı dosyaların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Internet Explorer Güvenilir Siteleri	Internet Explorer güvenilir siteleri üzerinde kayıt defteri değişiklikleri yaparak, tarayıcınızın şüpheli Web sitelerine güvenmesine izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Internet Explorer İlkesi	Internet Explorer ilkelerinde kayıt defteri değişiklikleri yaparak, tarayıcınızın görünümünü ve davranışını etkileyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.

Güvenilenler listelerini kullanma

VirusScan bir dosya veya kayıt defteri değişikliği (Sistem Koruması), program veya arabellek taşması algıladığında, buna güvenmenizi veya bunu kaldırmanızı ister. Öğe güvenir ve bu etkinlik hakkında başka bildirim almak istemediğinizi belirtirseniz, öğe güvenilenler listesine eklenir ve VirusScan artık bunu algılamaz ve etkinliği hakkında size bildirimde bulunmaz. Bir öğeyi güvenilenler listesine ekledikten sonra etkinliğini engellemek istediğinize karar verirsiniz bunu yapabilirsiniz. Engellendiğinde, öğenin çalışması veya her girişimde bulunduğu size bildirmeden bilgisayarınızda değişiklik yapması önlenir. Bir öğeyi güvenilenler listesinden de kaldırabilirsiniz. Kaldırıldığında, VirusScan öğenin etkinliğini yeniden algılayabilir.

Güvenilenler listelerini yönetme

Önceden algılanan ve güvenilen öğelere güvenmek veya bunları engellemek için Güvenilenler Listeleri bölmesini kullanın. Bir öğeyi VirusScan'ın yeniden algılaması için güvenilenler listesinden de kaldırabilirsiniz.

1 Güvenilenler Listeleri bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklayın.
2. SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'ı tıklayın.
3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklayın.
4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, virüsten korumanın etkin olduğundan emin olun ve **Gelişmiş**'i tıklayın.
5. Virüsten Koruma bölümünde **Güvenilenler Listeleri**'ni tıklayın.

2 Aşağıdaki güvenilenler listesi türlerinden birini seçin:

- **Program Sistem Koruması**
- **Windows Sistem Koruması**
- **Tarayıcı Sistem Koruması**
- **Güvenilen Programlar**
- **Güvenilen Arabellek Taşmaları**

3 Şunu yapmak istiyorum altında aşağıdakilerden birini gerçekleştirin:

- Algılanan öğenin Windows kayıt defterinde veya bilgisayarınızdaki kritik sistem dosyalarında size bildirmeden değişiklik yapmasına izin vermek için **Güven**'i tıklayın.

- Algılanan öğenin Windows kayıt defterinde veya bilgisayarınızdaki kritik sistem dosyalarında size bildirmeden değişiklik yapmasını engellemek için **Engelle**'yi tıklatın.
- Algılanan öğeyi güvenilenler listelerinden kaldırmak için **Kaldır**'ı tıklatın.

4 Tamam'ı tıklatın.

Not: Güvenilenler listesi türleri hakkında ayrıntılı bilgi için bkz. Güvenilenler listesi türleri hakkında (sayfa 52).

Güvenilenler listesi türleri hakkında

Güvenilenler Listeleri bölmesindeki Sistem Koruması, VirusScan tarafından önceden algılanan ancak sizin uyarıdan veya Tarama sonuçları bölmesinden izin vermeyi seçtiğiniz, yetkisiz kayıt defteri ve dosya değişikliklerini yansıtır. Güvenilenler Listeleri bölmesinden yönetebileceğiniz beş tür güvenilenler listesi türü vardır: Program Sistem Koruması, Windows Sistem Koruması, Tarayıcı Sistem Koruması, Güvenilen Programlar ve Güvenilen Arabellek Taşmaları.

Seçenek	Açıklama
Program Sistem Koruması	Güvenilenler Listeleri bölmesindeki Program Sistem Koruması, önceden VirusScan tarafından algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölmesinden izin vermeyi seçtiğiniz, yetkisiz kayıt defteri ve dosya değişikliklerini yansıtır. Program Sistem Koruması; ActiveX yüklemeleri, başlangıç öğeleri, Windows kabuk yürütme kancaları ve kabuk hizmeti nesne gecikme yükleme etkinliğiyle ilişkili yetkisiz kayıt defteri ve dosya değişikliklerini algılar. Bu türde yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınıza zarar verebilir, güvenliğini tehlikeye atabilir ve değerli sistem dosyalarını bozabilir.

Windows Sistem Koruması	Güvenilenler Listeleri bölümündeki Windows Sistem Koruması, VirusScan tarafından önceden algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölümünden izin vermeyi seçtiğiniz, yetkisiz kayıt defteri ve dosya değişikliklerini yansıtır. Windows Sistem Koruması; içerik menüsü işleyicileri, applnit DLL dosyaları, Windows hosts dosyası, Winlogon kabuğu, Winsock Katmanlı Hizmet Sağlayıcıları (LSP) vb. ile ilişkili yetkisiz kayıt defteri ve dosya değişikliklerini algılar. Bu türde yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınızın Internet'te bilgi gönderme ve alma biçimini etkileyebilir, programların görünümünü ve davranışını değiştirebilir ve şüpheli programların bilgisayarınızda çalışmasına izin verebilir.
Tarayıcı Sistem Koruması	Güvenilenler Listeleri bölümündeki Tarayıcı Sistem Koruması, VirusScan tarafından önceden algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölümünden izin vermeyi seçtiğiniz, yetkisiz kayıt defteri ve dosya değişikliklerini yansıtır. Tarayıcı Sistem Koruması; Tarayıcı yardımcı nesneleri, Internet Explorer eklentileri, Internet Explorer URL'leri, Internet Explorer güvenlik bölgeleri vb. ile ilişkili yetkisiz kayıt defteri değişikliklerini ve diğer istenmeyen davranışları algılar. Bu türde yetkisiz kayıt defteri değişiklikleri, şüpheli Web sitelerine yeniden yönlendirme, tarayıcı ayarlarında ve seçeneklerinde değişiklikler ve şüpheli Web sitelerine güvenme gibi istenmeyen tarayıcı etkinliğine neden olabilir.
Güvenilen Programlar	Güvenilen programlar, VirusScan tarafından önceden algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölümünden izin vermeyi seçtiğiniz olası istenmeyen programlardır.
Güvenilen Arabellek Taşmaları	Güvenilen arabellek taşmaları, VirusScan tarafından algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölümünden izin vermeyi seçtiğiniz istenmeyen etkinliği yansıtır. Arabellek taşmaları bilgisayarınıza zarar verebilir ve dosyalarınızı bozabilir. Arabellek taşmaları, şüpheli programların ve işlemlerin arabellekte depoladığı bilgi miktarı arabellek kapasitesini aştığı zaman gerçekleşir.

B Ö L Ü M 1 1

Bilgisayarınızı tarama

SecurityCenter'ı ilk kez başlattığınızda, VirusScan'in gerçek zamanlı virüsten koruması, bilgisayarınızı olası zararlı virüslerden, Truva atlarından ve diğer güvenlik tehditlerinden korumaya başlar. Gerçek zamanlı virüsten korumayı devre dışı bırakmadığınız sürece, VirusScan ayarladığınız gerçek zamanlı tarama seçeneklerini kullanarak, siz veya bilgisayarınız dosyalara erişince bunları tarar ve bilgisayarınızda virüs etkinliğini sürekli izler. Bilgisayarınızın en son güvenlik tehditlerine karşı korunduğundan emin olmak için gerçek zamanlı virüsten korumayı açık bırakın ve düzenli, daha kapsamlı el ile taramalar için zamanlama yapın. Gerçek zamanlı ve el ile tarama seçeneklerini ayarlama hakkında ayrıntılı bilgi için bkz. Virüsten korumayı ayarlama (sayfa 37).

VirusScan, düzenli aralıklarla daha kapsamlı taramalar çalıştırmanıza olanak vererek, el ile virüsten korumaya yönelik daha ayrıntılı tarama seçenekleri sunar. SecurityCenter'dan, ayarlı zamanlamaya göre belirli konumları hedefleyen el ile taramalar çalıştırabilirsiniz. Ancak el ile taramaları, çalıştığınız sırada doğrudan Windows Gezgini'nden de çalıştırabilirsiniz. SecurityCenter'da tarama yapmak, tarama seçeneklerini anında değiştirme avantajı sağlar. Windows Gezgini'nden tarama yapmak ise bilgisayar güvenliği açısından rahat bir yaklaşım sunar.

El ile taramayı ister SecurityCenter'dan isterseniz Windows Gezgini'nden çalıştırın, işlem tamamlandığında tarama sonuçlarını görüntüleyebilirsiniz. VirusScan'in virüs, truva atı, casus yazılım, reklam yazılım, tanımlama bilgisi ve başka olası istenmeyen program algılayıp algılamadığını, onarıp onarmadığını veya karantinaya alıp almadığını belirlemek için tarama sonuçlarını görüntülersiniz. Tarama sonuçları farklı yollarla görüntülenebilir. Örneğin, tarama sonuçlarının temel özetini veya virüs bulaşma durumu ve türü gibi ayrıntılı bilgileri görüntüleyebilirsiniz. Ayrıca, genel tarama ve algılama istatistiklerini de görüntüleyebilirsiniz.

Bu bölümde

Bilgisayarınızı tarama	56
Tarama sonuçlarını görüntüleme	56

Bilgisayarınızı tarama

SecurityCenter'da Gelişmiş veya Temel menüden el ile tarama çalıştırabilirsiniz. Gelişmiş menüden tarama çalıştırırsanız, tarama öncesinde el ile tarama seçeneklerinizi onaylayabilirsiniz. Temel menüden tarama çalıştırırsanız, VirusScan varolan tarama seçeneklerini kullanarak hemen taramayı başlatır. Ayrıca, varolan tarama seçeneklerini kullanarak Windows Gezgini'nden de tarama çalıştırabilirsiniz.

- Aşağıdakilerden birini gerçekleştirin:

SecurityCenter'da tarama

Bunu yapmak için...	Bunu yapın...
Varolan ayarları kullanarak tarama yapmak	Temel menüde Tara 'yı tıklatın.
Değiştirilen ayarları kullanarak tarama yapmak	Gelişmiş menüde Tara 'yı tıklatın, taranacak konumları seçin, tarama seçeneklerini belirleyin ve sonra Şimdi Tara 'yı tıklatın.

Windows Gezgini'nde tarama

- Windows Gezgini'ni açın.
- Dosyayı, klasörü veya sürücüyü sağ tıklatın ve sonra **Tara**'yı tıklatın.

Not: Tarama sonuçları, Tarama tamamlandı uyarısında görüntülenir. Sonuçlar; taranan, algılanan, onarılan, karantinaya alınan ve kaldırılan öğelerin sayısını içerir. Tarama sonuçları hakkında ayrıntılı bilgi almak veya virüslü öğeler üzerinde çalışmak için **Tarama ayrıntılarını görüntüle**'yi tıklatın.

Tarama sonuçlarını görüntüleme

El ile tarama bitince, taramada neler bulunduğunu belirlemek ve bilgisayarınızın geçerli koruma durumunu analiz etmek için sonuçları görüntülersiniz. Tarama sonuçları size VirusScan'ın virüs, truva atı, casus yazılım, reklam yazılım, tanımlama bilgisi ve başka olası istenmeyen program algılayıp algılamadığını, onarıp onarmadığını veya karantinaya alıp almadığını söyler.

- Temel veya Gelişmiş menüde **Tara**'yı tıklatın ve sonra aşağıdakilerden birini yapın:

Bunu yapmak için...	Bunu yapın...
Tarama sonuçlarını uyarıda görüntülemek	Tarama sonuçlarını, Tarama tamamlandı uyarısında görüntüleyin.

Tarama sonuçları hakkında ayrıntılı bilgi görüntülemek	Tarama tamamlandı uyarısında Tarama ayrıntılarını görüntüle 'yi tıklatın.
Tarama sonuçlarının hızlı özetini görüntülemek	Görev çubuğunuzdaki bildirim alanında Tarama tamamlandı simgesi 'ne gidin.
Tarama ve algılama istatistiklerini görüntülemek	Görev çubuğunuzdaki bildirim alanında Tarama tamamlandı simgesini çift tıklatın.
Algılanan öğeler, bulaşma durumu ve türü hakkında ayrıntılı bilgi görüntülemek	Görev çubuğunuzdaki bildirim alanında Tarama tamamlandı simgesini çift tıklatın ve sonra Tarama İlerleyişi: El İle Tarama bölümünde Sonuçları Görüntüle 'yi tıklatın.

B Ö L Ü M 1 2

Tarama sonuçlarıyla çalışma

VirusScan gerçek zamanlı veya el ile tarama çalıştırırken bir güvenlik tehdidi algılsa, tehdit türüne göre tehdidi otomatik olarak ele almayı dener. Örneğin, VirusScan bilgisayarınızda bir virüs, Truva atı veya izleme tanımlama bilgisi algılsa, virüslü dosyayı temizlemeyi dener. VirusScan dosyayı temizleyemezse karantinaya alır.

Bazı güvenlik tehditlerinde, VirusScan dosyayı başarıyla temizleyemeyebilir veya karantinaya alamayabilir. Bu durumda, VirusScan sizden güvenlik tehdidini ele almanızı ister. Tehdit türüne bağlı olarak farklı eylemler gerçekleştirebilirsiniz. Örneğin bir dosyada virüs algılanırsa ancak VirusScan dosyayı başarıyla temizleyemez veya karantinaya alamazsa, buna erişimi reddeder. Tanımlama bilgileri algılanırsa ancak VirusScan tanımlama bilgilerini başarıyla temizleyemez veya karantinaya alamazsa, bunları kaldırma veya bunlara güvenme kararını siz verebilirsiniz. Olası istenmeyen programlar algılanırsa, VirusScan otomatik eylem gerçekleştirmez; bunun yerine, programı karantinaya alma veya programa güvenme kararını size bırakır.

VirusScan öğeleri karantinaya alınca, bunları şifreler ve sonra dosyaların, programların veya tanımlama bilgilerinin bilgisayarınıza zarar vermesini engellemek için bunları bir klasörde izole eder. Karantinadaki öğeleri geri yükleyebilir veya kaldırabilirsiniz. Genellikle karantinadaki bir tanımlama bilgisini bilgisayarınızı etkilemeden silebilirsiniz; ancak VirusScan bildiğiniz ve kullandığınız bir programı karantinaya almışsa bunu geri yüklemeyi düşünün.

Bu bölümde

Virüsler ve Truva atlarıyla çalışma.....	59
Olası istenmeyen programlarla çalışma	60
Karantinadaki dosyalarla çalışma	60
Karantinadaki programlar ve tanımlama bilgileriyle çalışma	61

Virüsler ve Truva atlarıyla çalışma

VirusScan gerçek zamanlı tarama veya el ile tarama sırasında bilgisayarınızdaki bir dosyada virüs veya Truva atı algılsa, dosyayı temizlemeyi dener. VirusScan dosyayı temizleyemezse karantinaya almayı dener. Bu da başarısız olursa, dosyaya erişim reddedilir (yalnızca gerçek zamanlı taramalarda).

1 Tarama Sonuçları bölmesini açın.

Nasıl?

1. Görev çubuğunuzun en sağındaki bildirim alanında **Tarama tamamlandı** simgesini çift tıklatın.
2. Tarama ilerleyişi: El ile Tarama bölümünde **Sonuçları Görüntüle**'yi tıklatın.

2 Tarama sonuçları listesinde **Virüsler ve Truva Atları**'nı tıklatın.

Not: VirusScan'ın karantinaya aldığı dosyalarla çalışmak için bkz. Karantinadaki dosyalarla çalışma (sayfa 60).

Olası istenmeyen programlarla çalışma

VirusScan gerçek zamanlı tarama veya el ile tarama sırasında bilgisayarınızda olası istenmeyen bir program algıarsa, programı kaldırabilir veya programa güvenebilirsiniz. Olası istenmeyen program kaldırıldığında, gerçekte sisteminizden silinmez. Kaldırma işlemi, programı karantinaya alarak bilgisayarınıza veya dosyalarınıza daha fazla zarar vermesini engeller.

- 1 Tarama Sonuçları bölümünü açın.
Nasıl?
 1. Görev çubuğunuzun en sağındaki bildirim alanında **Tarama tamamlandı** simgesini çift tıklatın.
 2. Tarama ilerleyişi: El ile Tarama bölümünde **Sonuçları Görüntüle**'yi tıklatın.
- 2 Tarama sonuçları listesinde **Olası İstenmeyen Programlar**'ı tıklatın.
- 3 Olası istenmeyen programı seçin.
- 4 **Şunu yapmak istiyorum** altında **Kaldır**'ı veya **Güven**'i tıklatın.
- 5 Belirlediğiniz seçeneği onaylayın.

Karantinadaki dosyalarla çalışma

VirusScan virüslü dosyaları karantinaya alınca, bunları şifreler ve sonra dosyaların bilgisayarınıza zarar vermesini engellemek için bunları bir klasöre taşır. Daha sonra karantinadaki dosyaları geri yükleyebilir veya kaldırabilirsiniz.

- 1 Karantinadaki Dosyalar bölümünü açın.
Nasıl?
 1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
 2. **Geri Yükle**'yi tıklatın.
 3. **Dosyalar**'ı tıklatın.
- 2 Karantinadaki bir dosyayı seçin.
- 3 Aşağıdakilerden birini gerçekleştirin:
 - Virüslü dosyayı onarıp bilgisayarınızdaki özgün konumuna döndürmek için **Geri Yükle**'yi tıklatın.

- Virüslü dosyayı bilgisayarınızdan kaldırmak için **Kaldır**'ı tıklatın.

4 Belirlediğiniz seçimi onaylamak için **Evet**'i tıklatın.

İpucu: Birden çok dosyayı aynı anda geri yükleyebilir veya kaldırabilirsiniz.

Karantinadaki programlar ve tanımlama bilgileriyle çalışma

VirusScan olası istenmeyen programları veya izleme tanımlama bilgilerini karantinaya alınca, bunları şifreler ve sonra programların veya tanımlama bilgilerinin bilgisayarınıza zarar vermesini engellemek için bunları korunan bir klasöre taşır. Daha sonra karantinadaki öğeleri geri yükleyebilir veya kaldırabilirsiniz. Genellikle karantinadaki öğeyi sisteminizi etkilemeden silebilirsiniz.

1 Karantinadaki Programlar ve İzleme Tanımlama Bilgileri bölümünü açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
2. **Geri Yükle**'yi tıklatın.
3. **Programlar ve Tanımlama Bilgileri**'ni tıklatın.

2 Karantinadaki bir programı veya tanımlama bilgisini seçin.

3 Aşağıdakilerden birini gerçekleştirin:

- Virüslü dosyayı onarıp bilgisayarınızdaki özgün konumuna döndürmek için **Geri Yükle**'yi tıklatın.
- Virüslü dosyayı bilgisayarınızdan kaldırmak için **Kaldır**'ı tıklatın.

4 İşlemi onaylamak için **Evet**'i tıklatın.

İpucu: Birden çok programı ve tanımlama bilgisini aynı anda geri yükleyebilir veya kaldırabilirsiniz.

B Ö L Ü M 13

McAfee Personal Firewall

Personal Firewall, bilgisayarınız ve kişisel verileriniz için gelişmiş koruma sağlar. Personal Firewall, bilgisayarınızla Internet arasında bir engel oluşturarak, şüpheli etkinliklere karşı Internet trafiğini sessizce izler.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Personal Firewall özellikleri	64
Firewall'u başlatma	67
Uyarılarla çalışma	69
Bilgi uyarılarını yönetme	71
Firewall korumasını yapılandırma.....	73
Programları ve izinleri yönetme	85
Sistem hizmetlerini yönetme.....	93
Bilgisayar bağlantılarını yönetme.....	99
Günlüğe kaydetme, izleme ve analiz	107
Internet güvenliği hakkında bilgi alma.....	117

Personal Firewall özellikleri

Personal Firewall aşağıdaki özellikleri sunar.

Standart ve özel koruma düzeyleri

Firewall'un varsayılan veya özelleştirilebilir koruma ayarlarını kullanarak, izinsiz girişlerden ve şüpheli etkinliklerden korunun.

Gerçek zamanlı öneriler

Programlara Internet erişim izni vermeniz veya ağ trafiğine güvenmeniz gerekip gerekmediğini belirlemenize yardımcı olan dinamik öneriler alın.

Programlar için akıllı erişim yönetimi

Uyarılar ve Olay Günlükleri ile programların Internet erişimini yönetin ve belirli programların erişim izinlerini yapılandırın.

Oyun koruması

İzinsiz giriş denemeleri ve şüpheli etkinliklerle ilgili uyarıların, tam ekranda oyun oynarken dikkatinizi dağıtmasını engeller.

Bilgisayar başlangıç koruması

Windows® başlar başlamaz, Firewall bilgisayarınızı izinsiz giriş denemelerinden, istenmeyen programlardan ve ağ trafiğinden korur.

Sistem hizmeti portunu kontrol etme

Bazı programlar için gereken açık ve kapalı sistem hizmeti portlarını yönetin.

Bilgisayar bağlantılarını yönetme

Başka bilgisayarlarla kendi bilgisayarınız arasında uzak bağlantılara izin verin ve bunları engelleyin.

HackerWatch bilgi tümleşmesi

Bilgisayarınızdaki programlar hakkında güncel güvenlik bilgilerinin yanı sıra genel güvenlik olayları ve Internet port istatistikleri de veren HackerWatch'un Web sitesi aracılığıyla, genel korsanlık hareketlerini ve izinsiz giriş desenlerini izleyin.

Firewall'u kilitleme

Bilgisayarınız ve Internet arasındaki tüm gelen ve giden trafiği anında engelleyin.

Firewall'u geri yükleme

Firewall'un özgün koruma ayarlarını anında geri yükleyin.

Gelişmiş Truva atı algılama

Truva atları gibi olası zararlı uygulamaları algılayıp, bunların kişisel verilerinizi Internet'e göndermesini engelleyin.

Olay günlüğü kaydetme

En son gelen ve giden Internet trafiğini, izinsiz giriş olaylarını izleyin.

Internet trafiğini izleme

Saldırıların kaynağını ve trafiği gösteren dünya haritalarını inceleyin. Bunun yanı sıra, IP adreslerinin kaynağını bulmak için ayrıntılı kullanıcı bilgilerine ve coğrafi verilere ulaşın. Ayrıca, gelen ve giden trafiği analiz edin; program bant genişliğini ve program etkinliğini izleyin.

İzinsiz girişleri engelleme

Gizliliğinizi olası Internet tehditlerinden koruyun. McAfee, sezgisel işlevler kullanarak saldırı belirtileri veya korsanlık girişimi özellikleri sergileyen öğeleri engelleyip, üçüncü bir koruma katmanı sağlar.

Karmaşık trafik analizi

Açık bağlantıları etkin şekilde dinleyenler de dahil, gelen ve giden Internet trafiğini ve program bağlantılarını inceleyin. Bu özellik, izinsiz girişlere karşı hassas olan programları görmenize ve gerekeni yapmanıza olanak verir.

B Ö L Ü M 14

Firewall'u başlatma

Firewall yüklendikten sonra, bilgisayarınız izinsiz girişlerden ve istenmeyen ağ trafiğinden korunur. Ayrıca uyarıları işleyebilir; bilinen ve bilinmeyen programların gelen ve giden Internet erişimini yönetebilirsiniz. Akıllı Öneriler ve Güvenilen güvenlik düzeyi (programların yalnızca giden Internet erişimine izin verme seçeneği belirlenmiş) otomatik olarak etkinleştirilir.

Internet ve Ağ Yapılandırması bölümünden Firewall'u devre dışı bırakabilirsiniz; ancak bu durumda bilgisayarınız izinsiz girişlerden ve istenmeyen ağ trafiğinden korunmaz ve siz gelen ve giden Internet bağlantılarını etkili şekilde yönetemezsiniz. Güvenlik duvarı korumasını kaldırmanız gerekirse, bunu yalnızca zorunlu durumlarda ve geçici olarak yapın. Firewall'u aynı zamanda Internet ve Ağ Yapılandırması panelinden de etkinleştirebilirsiniz.

Firewall, Windows® Güvenlik Duvarı'nı otomatik olarak devre dışı bırakır ve kendisini varsayılan güvenlik duvarı olarak ayarlar.

Not: Firewall'u yapılandırmak için, Internet ve Ağ Yapılandırması bölümünü açın.

Bu bölümde

Güvenlik duvarı korumasını başlatma	67
Güvenlik duvarı korumasını durdurma.....	68

Güvenlik duvarı korumasını başlatma

Bilgisayarınızı izinsiz girişlerden ve istenmeyen ağ trafiğinden korumak, gelen ve giden Internet bağlantılarını yönetmek için Firewall'u etkinleştirebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı ve sonra **Yapılandır**'ı tıklayın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruması devre dışı** altında **Açık**'ı tıklayın.

Güvenlik duvarı korumasını durdurma

Bilgisayarınızı izinsiz girişlerden ve istenmeyen ağ trafiğinden korumak istemiyorsanız Firewall'u devre dışı bırakabilirsiniz. Firewall devre dışı bırakıldığında, gelen ve giden Internet bağlantılarını yönetemezsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı ve sonra **Yapılandır**'ı tıklayın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Kapalı**'yı tıklayın.

B Ö L Ü M 1 5

Uyarılarla çalışma

Firewall, güvenliğinizi yönetmenize yardımcı olmak için birtakım uyarılar yapar. Bu uyarılar, üç temel gruba ayrılabilir:

- Kırmızı uyarı
- Sarı uyarı
- Yeşil uyarı

Uyarılar, uyarıları nasıl işleyeceğinize karar vermenize veya bilgisayarınızda çalışan programlar hakkında bilgi almanıza yardımcı olan bilgiler de içerebilir.

Bu bölümde

Uyarılar hakkında.....70

Uyarılar hakkında

Firewall'da üç temel uyarı türü vardır. Ayrıca, bazı uyarılar bilgisayarınızda çalışan programları öğrenmenize veya bunlarla ilgili bilgi almanıza yardımcı olan bilgiler içerir.

Kırmızı uyarı

Firewall bilgisayarınızda bir Truva atı algılayıp engellediğinde, ek tehditlere karşı tarama yapmanızı öneren bir kırmızı uyarı görüntülenir. Truva atı yasal program gibi görünür ancak bilgisayarınızı bozabilir, ona zarar verebilir ve yetkisiz erişim sağlayabilir. Bu uyarı, Açık seçeneği dışındaki tüm güvenlik düzeylerinde gerçekleşir.

Sarı uyarı

En yaygın uyarı türü, Firewall tarafından algılanan bir program etkinliğini veya ağ olayını size bildiren sarı uyarıdır. Bu oluştuğunda, uyarı program etkinliğini veya ağ olayını açıklar ve sonra size yanıt vermenizi gerektiren bir veya birkaç seçenek sunar. Örneğin, Firewall yüklü bir bilgisayar yeni bir ağa bağlandığında, **Yeni Ağ Algılandı** uyarısı görüntülenir. Ağa güvenmeyi veya onu engellemeyi seçebilirsiniz. Ağa güvenmeyi seçerseniz, Firewall bu ağ üzerindeki tüm bilgisayarlardan gelen trafiğe izin verir ve ağı Güvenilen IP Adresleri arasına ekler. Akıllı Öneriler etkinse, programlar Program İzinleri bölümüne eklenir.

Yeşil uyarı

Pek çok durumda, yeşil uyarı bir olayla ilgili temel bilgiler verir ve sizden yanıt vermenizi istemez. Yeşil uyarılar varsayılan olarak devre dışıdır ve genellikle Standart, Güvenilen, Sıkı ve Gizli güvenlik düzeyleri ayarlandığında gerçekleşir.

Kullanıcı Yardımı

Pek çok Firewall uyarısı, bilgisayarınızın güvenliğini yönetmenize yardım etmek için aşağıdaki gibi ek bilgiler içerir:

- **Bu program hakkında ek bilgi al:** Firewall'un bilgisayarınızda algıladığı bir program hakkında bilgi almak için, McAfee'nin genel güvenlik Web sitesini başlatın.
- **Bu program hakkında McAfee'yi bilgilendir:** Firewall'un bilgisayarınızda algıladığı bilinmeyen bir dosya hakkında McAfee'ye bilgi gönderin.
- **McAfee önerisi:** Uyarıların işlenmesiyle ilgili önerilerdir. Örneğin, uyarı size programa erişim izni vermenizi önerebilir.

B Ö L Ü M 1 6

Bilgi uyarılarını yönetme

Firewall, örneğin tam ekranda oyun gibi belirli olaylar sırasında izinsiz giriş denemeleri veya şüpheli etkinlik algılsa, bilgi uyarılarını görüntülemenize veya gizlemenize olanak verir.

Bu bölümde

Oyun sırasında uyarıları görüntüleme	71
Bilgi uyarılarını gizleme.....	71

Oyun sırasında uyarıları görüntüleme

Tam ekranda oyun oynarken Firewall tarafından izinsiz giriş denemeleri veya şüpheli etkinlik algılandığında, bilgi uyarılarının görüntülenmesine izin verebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Gelişmiş Menü**'yü tıklatın.
- 2 **Yapılandır**'ı tıklatın.
- 3 SecurityCenter Yapılandırma bölmesinde, **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 4 Uyarı Seçenekleri bölmesinde **Oyun modu algılandığında bilgilendirme uyarılarını göster**'i seçin.
- 5 **Tamam**'ı tıklatın.

Bilgi uyarılarını gizleme

Firewall tarafından izinsiz giriş denemeleri veya şüpheli etkinlik algılandığında, bilgi uyarılarının görüntülenmesini engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Gelişmiş Menü**'yü tıklatın.
- 2 **Yapılandır**'ı tıklatın.
- 3 SecurityCenter Yapılandırma bölmesinde, **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 4 SecurityCenter Yapılandırma bölmesinde **Bilgi Uyarıları**'nı tıklatın.
- 5 Bilgi Uyarıları bölmesinde, aşağıdakilerden birini gerçekleştirin:
 - Tüm bilgi uyarılarını gizlemek için **Bilgi uyarılarını gösterme**'yi seçin.
 - Gizlemek için uyarının işaretini temizleyin.
- 6 **Tamam**'ı tıklatın.

B Ö L Ü M 17

Firewall korumasını yapılandırma

Firewall, güvenliğinizi yönetmek, güvenlik olayları ve uyarılara yanıt verme biçiminizi istediğiniz gibi değiştirmek için çeşitli yöntemler sunar.

Firewall'u ilk kez yüklediğinizde, bilgisayarınızın koruma düzeyi Güvenilen seçeneğine ayarlıdır ve programlarınızın yalnızca giden Internet erişimine izin verilir. Ancak Firewall, kısıtlayıcı ile açık arasında değişen başka düzeyler de sunar.

Firewall, size uyarılar ve programların Internet erişimi hakkında öneriler alma fırsatı da sunar.

Bu bölümde

Firewall güvenlik düzeylerini yönetme	74
Akıllı Önerileri uyarılar için yapılandırma	78
Firewall güvenliğini iyileştirme	80
Firewall'u kilitleme ve geri yükleme	83

Firewall güvenlik düzeylerini yönetme

Firewall'un güvenlik düzeyleri, uyarıları ne düzeyde yönetmek ve bunlara ne kadar yanıt vermek istediğinizi kontrol eder. Program istenmeyen ağ trafiği, gelen ve giden Internet bağlantıları algıladığında bu uyarılar görüntülenir. Varsayılan olarak, Firewall'un güvenlik düzeyi yalnızca giden erişimine izin veren Güvenilen seçeneğine ayarlıdır.

Güvenilen güvenlik düzeyi ayarlıysa ve Akıllı Öneriler etkinse, sarı uyarılar gelen erişimi gerektiren bilinmeyen programlara erişim izni vermek veya erişimi engellemek için seçenek sunar. Bilinen programlar algılandığında, yeşil bilgi uyarıları görüntülenir ve otomatik olarak erişim izni verilir. Erişim izni verilmesi, programın giden bağlantılar oluşturmaya ve istenmeyen gelen bağlantıları dinlemesine olanak verir.

Genel olarak, güvenlik düzeyi ne kadar kısıtlayıcıysa (Gizli ve Sıkı), görüntülenen ve dolayısıyla sizin tarafınızdan işlenmesi gereken seçeneklerin ve uyarıların sayısı o kadar artar.

Aşağıdaki tabloda, en kısıtlayıcı olandan en az kısıtlayıcı olana kadar, Firewall'un altı güvenlik düzeyi açıklanmaktadır:

Düzye	Açıklama
Kilitli	Web sitelerine, e-postalara ve güvenlik güncelleştirmelerine erişim dahil olmak üzere tüm gelen ve giden ağ bağlantılarını engeller. Bu güvenlik düzeyi, Internet bağlantınızın kaldırılmasıyla aynı sonucu verir. Bu ayarı kullanarak, Sistem Hizmetleri bölmesinde açık olarak ayarladığınız portları engelleyebilirsiniz.
Gizli	Açık portlar dışında tüm gelen Internet bağlantılarını engeller ve bilgisayarınızın Internet'teki varlığını gizler. Güvenlik duvarı, yeni programlar giden Internet bağlantıları denediğinde veya gelen bağlantı istekleri aldığında sizi uyarır. Engellenen ve eklenen programlar, Program İzinleri bölümünde görüntülenir.
Sıkı	Yeni programlar giden Internet bağlantıları denediğinde veya gelen bağlantı istekleri aldığında sizi uyarır. Engellenen ve eklenen programlar, Program İzinleri bölümünde görüntülenir. Güvenlik düzeyi Sıkı seçeneğine ayarlandığında, program yalnızca o sırada gerekli olan erişim türünü ister (örneğin yalnızca giden erişimi); buna izin verilebilir veya engelleyebilirsiniz. Daha sonra program hem gelen hem de giden bağlantısı kurmak isterse, Program İzinleri bölümünden bu programa tam erişim izni verilebilir.
Standart	Gelen ve giden bağlantıları izler ve yeni programlar Internet'e erişmeye çalıştığında sizi uyarır. Engellenen ve eklenen programlar, Program İzinleri bölümünde görüntülenir.

Güvenilen	Programlara gelen ve giden (tam) veya yalnızca giden Internet erişimi izni verir. Varsayılan güvenlik düzeyi, programların yalnızca giden erişimine izin verme seçeneği belirlenmiş durumda Güvenilen olarak ayarlıdır. Bir programa tam erişim izni verilirse, Firewall programa otomatik olarak güvenir ve bunu Program İzinleri bölümünde izin verilen programlar listesine ekler. Bir programa yalnızca giden erişim izni verilirse, Firewall yalnızca giden Internet bağlantısı yaparken programa otomatik olarak güvenir. Gelen bağlantıya otomatik olarak güvenir.
Aç	Tüm gelen ve giden Internet bağlantılarına izin verir.

Firewall, aynı zamanda Güvenlik Duvarı Koruması Varsayılanlarını Geri Yükle bölümünden, güvenlik düzeyinizi anında Güvenilen seçeneğine sıfırlamanıza (ve yalnızca giden erişimine izin vermenize) olanak verir.

Güvenlik düzeyini Kilitle seçeneğine ayarlama

Tüm gelen ve giden ağ bağlantılarını engellemek için Firewall'un güvenlik düzeyini Kilitle seçeneğine ayarlayabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Kilitle** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
- 4 **Tamam**'ı tıklatın.

Güvenlik düzeyini Gizli seçeneğine ayarlama

Açık portlar dışında tüm gelen ağ bağlantılarını engellemek ve bilgisayarınızın Internet'teki varlığını gizlemek için Firewall'un güvenlik düzeyini Gizli seçeneğine ayarlayabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Gizli** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
- 4 **Tamam**'ı tıklatın.

Not: Gizli modunda, yeni programlar giden Internet bağlantısı istediğinde veya gelen bağlantı istekleri aldığı anda Firewall sizi uyarır.

Güvenlik düzeyini Sıkı seçeneğine ayarlama

Yeni programlar giden Internet bağlantıları kurmaya çalıştığında veya gelen bağlantı istekleri aldığında uyarı almak için Firewall'un güvenlik düzeyini Sıkı seçeneğine ayarlayabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Sıkı** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
- 4 **Tamam**'ı tıklatın.

Not: Sıkı modunda, program yalnızca o sırada gerekli olan erişim türünü ister (örneğin yalnızca giden erişimi); buna izin verebilir veya engelleyebilirsiniz. Program daha sonra hem gelen hem de giden bağlantısı kurmak isterse, Program İzinleri bölümünden bu programa tam erişim izni verebilirsiniz.

Güvenlik düzeyini Standart seçeneğine ayarlama

Gelen ve giden bağlantıları izlemek ve yeni programlar Internet'e erişmeye çalıştığında uyarı almak için güvenlik düzeyini Standart seçeneğine ayarlayabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Standart** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
- 4 **Tamam**'ı tıklatın.

Güvenlik düzeyini Güvenilen seçeneğine ayarlama

Tam erişim veya yalnızca giden ağ erişimi izni vermek için Firewall'un güvenlik düzeyini Güvenilen seçeneğine ayarlayabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Güvenilen** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
- 4 Aşağıdakilerden birini gerçekleştirin:
 - Tam gelen ve giden ağ erişimi izni vermek için **Tam Erişime İzin Ver**'i seçin.

- Yalnızca giden ağ erişimi izni vermek için **Yalnızca Giden Erişimine İzin Ver**'i seçin.

5 Tamam'ı tıklatın.

Not: Yalnızca Giden Erişimine İzin Ver, varsayılan seçenektir.

Güvenlik düzeyini Açık seçeneğine ayarlama

Tüm gelen ve giden ağ bağlantılarına izin vermek için Firewall'un güvenlik düzeyini Aç seçeneğine ayarlayabilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölmesinde, **Açık** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
- 4 **Tamam**'ı tıklatın.

Akıllı Önerileri uyarılar için yapılandırma

Herhangi bir program Internet'e erişmeye çalıştığında, uyarılara öneriler eklemesi, eklememesi veya görüntülemesi için Firewall'u yapılandırabilirsiniz. Akıllı Önerilerin etkinleştirilmesi, uyarıları nasıl işleyeceğinize karar vermenize yardımcı olur.

Akıllı Öneriler etkinleştirildiğinde (ve güvenlik düzeyi yalnızca giden erişimi etkin olarak Güvenilen seçeneğine ayarlandığında), Firewall bilinen programlara otomatik olarak izin verir veya engeller; olası tehlikeli programlar algılandığında, uyarının içinde bir öneri görüntüler.

Akıllı Öneriler devre dışı bırakıldığında, Firewall Internet erişimine izin vermez veya engellemez; uyarının içinde bir eylem planı önermez.

Akıllı Öneriler Yalnızca Görüntüle seçeneğine ayarlandığında, uyarıyla erişime izin vermeniz veya engellemeniz istenir, ancak uyarının içinde bir eylem planı da önerilir.

Akıllı Önerileri etkinleştirme

Firewall'un otomatik olarak programlara erişim izni vermesi veya engellemesi ve tanınmayan ve tehlikeli olması olası programlar hakkında sizi uyarması için Akıllı Öneriler'i etkinleştirebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Akıllı Öneriler**'in altında **Akıllı Önerileri Etkinleştir**'i seçin.
- 4 **Tamam**'ı tıklatın.

Akıllı Önerileri devre dışı bırakma

Firewall'un programlara erişim izni vermesi veya engellemesi ve tanınmayan ve tehlikeli olması olası programlar hakkında sizi uyarması için Akıllı Öneriler'i devre dışı bırakabilirsiniz. Ancak uyarılar, programlara erişim izni verme hakkında herhangi bir öneri içermez. Firewall şüpheli veya tehdit olasılığı olduğu bilinen yeni bir program algılsa, programın Internet'e erişmesini otomatik olarak engeller.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Akıllı Öneriler**'in altında **Akıllı Önerileri Devre Dışı Bırak**'ı seçin.
- 4 **Tamam**'ı tıklatın.

Akıllı Önerileri yalnızca görüntüleme

Uyarıların yalnızca eylem planı önerilerinde bulunması ve böylece tanınmayan ve tehlikeli olması olası programlara izin verme veya engelleme kararını verebilmeniz için Akıllı Öneriler'i görüntüleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Akıllı Öneriler**'in altında **Yalnızca Görüntüle**'yi seçin.
- 4 **Tamam**'ı tıklatın.

Firewall güvenliğini iyileştirme

Bilgisayarınızın güvenliği çeşitli şekillerde tehlikeye girebilir. Örneğin, bazı programlar Windows® başlamadan Internet'e bağlanmaya çalışabilir. Ayrıca deneyimli bilgisayar kullanıcıları, bilgisayarınızın ağa bağlı olup olmadığını belirlemek için onu izleyebilirler (ping işlemi yapabilirler). Firewall, başlangıç korumasını etkinleştirmenize ve ping isteklerini engellenize olanak vererek, her iki izinsiz giriş türüne karşı sizi korur. Birinci ayar Windows başlarken programların Internet'e erişmelerini engeller; ikinci ayar ise başka kullanıcıların ağ üzerinde bilgisayarınızı algılamalarına yardımcı olan ping isteklerini engeller.

Standart yükleme ayarları, Hizmet Reddi saldırıları veya suiistimaller gibi en yaygın saldırı denemelerine karşı otomatik algılama özelliği içerir. Standart yükleme ayarlarının kullanılması, bu saldırılara ve taramalara karşı korunmanızı sağlar; ancak İzinsiz Giriş Tespiti bölmesinde, bir veya daha fazla saldırı ya da tarama için otomatik algılamayı devre dışı bırakabilirsiniz.

Başlatma sırasında bilgisayarınızı koruma

Başlangıçta Internet erişimi bulunmayan ve şimdi buna gerek duyan yeni programları engellemek için Windows başlarken bilgisayarınızı koruyabilirsiniz. Firewall, Internet'e erişmek isteyen programlar için uygun uyarılar görüntülenir; böylece bunlara izin verebilir veya engelleyebilirsiniz. Bu seçeneği kullanabilmeniz için, güvenlik düzeyiniz Açık veya Kilitle seçeneğine ayarlı olmamalıdır.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Güvenlik Ayarları** altında **Başlangıç korumasını etkinleştir**'i seçin.
- 4 **Tamam**'ı tıklatın.

Not: Başlangıç koruması etkinleştirildiğinde, engellenen bağlantılar ve izinsiz girişler günlüğe kaydedilmez.

Ping isteği ayarlarını yapılandırma

Ağ üzerinde bilgisayarınızın diğer bilgisayar kullanıcıları tarafından tespit edilmesine izin verebilir veya engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölmesinde, **Güvenlik Ayarları**'nın altında aşağıdakilerden birini gerçekleştirin:
 - Ping istekleri kullanarak bilgisayarınızın ağ üzerinde algılanmasına izin vermek için **ICMP ping isteklerine izin ver**'i seçin.
 - Ping istekleri kullanarak bilgisayarınızın ağ üzerinde algılanmasını önlemek için **ICMP ping isteklerine izin ver**'i temizleyin.
- 4 **Tamam**'i tıklatın.

İzinsiz giriş tespitini yapılandırma

Bilgisayarınızı saldırılardan ve yetkisiz taramalardan korumak için izinsiz giriş denemelerini tespit edebilirsiniz. Standart Firewall ayarı, Hizmet Reddi saldırıları veya suiistimaller gibi en yaygın saldırı denemelerine karşı otomatik algılama özelliği içerir; ancak bir veya daha çok saldırı veya tarama için otomatik algılamayı devre dışı bırakabilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölmesinde **İzinsiz Giriş Tespiti**'ni tıklatın.
- 4 **İzinsiz Giriş Denemelerini Tespit Et** altında, aşağıdakilerden birini gerçekleştirin:
 - Otomatik olarak algılanacak saldırı veya taramanın adını seçin.
 - Saldırı veya taramanın otomatik olarak algılanmasını devre dışı bırakmak için adını temizleyin.
- 5 **Tamam**'i tıklatın.

Firewall Koruma Durumu ayarlarını yapılandırma

Firewall'u, bilgisayarınızda ortaya çıkan ve SecurityCenter'a bildirilmeyen belirli sorunları yok sayması için yapılandırabilirsiniz.

- 1 McAfee SecurityCenter bölmesinde, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
- 2 SecurityCenter Yapılandırma bölmesinde, **Koruma Durumu** altında **Gelişmiş**'i tıklatın.
- 3 Yoksayılan Sorunlar bölmesinde, aşağıdaki seçeneklerden birini veya birkaçını belirleyin:
 - **Güvenlik Duvarı koruması devre dışı.**
 - **Güvenlik duvarı Açık güvenlik düzeyine ayarlı.**
 - **Güvenlik duvarı hizmeti çalışmıyor.**
 - **Güvenlik Duvarı Koruması bilgisayarınızda yüklü değil.**
 - **Windows Güvenlik Duvarı devre dışı.**
 - **Giden güvenlik duvarı bilgisayarınızda yüklü değil.**
- 4 **Tamam**'ı tıklatın.

Firewall'u kilitleme ve geri yükleme

Kilitleme işlemi, tüm gelen ve giden ağ trafiğini anında engelleyerek, bilgisayarınızdaki bir sorunu izole etmenize ve gidermenize yardımcı olur.

Firewall'u anında kilitleme

Bilgisayarınız ve Internet arasındaki tüm ağ trafiğini anında engellemek için Firewall'u kilitleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde, **Ortak Görevler** altında **Güvenlik Duvarını Kilitle**'yi tıklayın.
- 2 Güvenlik Duvarını Kilitle bölümünde **Kilitle**'yi tıklayın.
- 3 Onaylamak için **Evet**'i tıklayın.

İpucu: Görev çubuğunun sağ ucundaki bildirim alanında bulunan SecurityCenter simgesini  sağ tıklayıp, ardından **Hızlı Bağlantılar**'ı ve sonra **Güvenlik Duvarını Kilitle**'yi tıklayarak da Firewall'u kilitleyebilirsiniz.

Firewall'un kilidini anında açma

Bilgisayarınız ve Internet arasındaki tüm ağ trafiğine anında izin vermek için Firewall'un kilidini açabilirsiniz.

- 1 McAfee SecurityCenter bölümünde, **Ortak Görevler** altında **Güvenlik Duvarını Kilitle**'yi tıklayın.
- 2 Kilit Etkin bölümünde **Kilidi Aç**'ı tıklayın.
- 3 Onaylamak için **Evet**'i tıklayın.

Firewall ayarlarını geri yükleme

Firewall'u hızla özgün koruma ayarlarına geri yükleyebilirsiniz. Bu geri yükleme işlemi, güvenlik düzeyinizi Güvenilen seçeneğine sıfırlar ve yalnızca giden ağ erişimi izni verir, Akıllı Öneriler'i etkinleştirir, varsayılan programların ve izinlerinin listesini Program İzinleri bölümünde geri yükler, güvenilen ve yasaklı IP adreslerini kaldırır ve sistem hizmetlerini, olay günlüğü ayarlarını ve izinsiz giriş tespitini geri yükler.

- 1 McAfee SecurityCenter bölümünde **Güvenlik Duvarı Varsayılanlarını Geri Yükle**'yi tıklayın.
- 2 Güvenlik Duvarı Koruması Varsayılanlarını Geri Yükle bölümünde **Varsayılanları Geri Yükle**'yi tıklayın.
- 3 Onaylamak için **Evet**'i tıklayın.

İpucu: Görev çubuğunun sağ ucundaki bildirim alanında bulunan SecurityCenter simgesini  sağ tıklayıp, ardından **Hızlı Bağlantılar**'ı ve sonra **Güvenlik Duvarı Varsayılanlarını Geri Yükle**'yi tıklayarak da Firewall'un varsayılan ayarlarını geri yükleyebilirsiniz.

B Ö L Ü M 1 8

Programları ve izinleri yönetme

Firewall, gelen ve giden Internet erişimi isteyen mevcut ve yeni programları yönetmenize ve bunlar için erişim izinleri oluşturmanıza olanak verir. Firewall, programların tam erişim veya yalnızca giden erişimini kontrol etmenizi sağlar. Ayrıca, programların erişimini engelleyebilirsiniz.

Bu bölümde

Programlara Internet erişim izni verme	86
Programlara yalnızca giden erişim izni verme	88
Programların Internet erişimini engelleme	89
Programların erişim izinlerini kaldırma.....	91
Programlar hakkında bilgi alma	92

Programlara Internet erişim izni verme

Internet tarayıcıları gibi bazı programların düzgün çalışabilmesi için Internet'e erişimleri gerekir.

Firewall, Program İzinleri sayfasını kullanarak aşağıdakileri yapmanıza olanak verir:

- Programlara erişim izni vermek
- Programlara yalnızca giden erişim izni vermek
- Programların erişimini engellemek

Bir programa Giden Olaylar ve Son Olaylar günlüğünden tam ve yalnızca giden Internet erişim izni de verebilirsiniz.

Bir programa tam erişim izni verme

Bilgisayarınızdaki engellenen bir programa tam gelen ve giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölmesinde **Program İzinleri**'ni tıklatın.
- 4 **Program İzinleri**'nin altında, **Engellenen** veya **Yalnızca Giden Erişimi** seçeneğine ayarlı bir program seçin.
- 5 **Eylem** altında **Erişime İzin Ver**'i tıklatın.
- 6 **Tamam**'ı tıklatın.

Yeni bir programa tam erişim izni verme

Bilgisayarınızdaki yeni bir programa tam gelen ve giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölmesinde **Program İzinleri**'ni tıklatın.
- 4 **Program İzinleri** altında **İzin Verilen Program Ekle**'yi tıklatın.
- 5 **Program Ekle** iletişim kutusunda, eklemek istediğiniz programa gidip seçin ve sonra **Aç**'ı tıklatın.

Not: Yeni eklenen programın izinlerini, mevcut bir programın izinleri gibi değiştirebilirsiniz; bunun için programı seçin ve sonra **Eylem** altında **Yalnızca Giden Erişimine İzin Ver**'i veya **Erişimi Engelle**'yi tıklatın.

Son Olaylar günlüğünden tam erişim izni verme

Son Olaylar günlüğünde görüntülenen engellenen bir programa tam gelen ve giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Gelişmiş Menü**'yü tıklayın.
- 2 **Raporlar ve Günlükler**'i tıklayın.
- 3 **Son Olaylar** altında, olay açıklamasını seçin ve ardından **Erişime İzin Ver**'i tıklayın.
- 4 Onaylamak için Program İzinleri iletişim kutusunda **Evet**'i tıklayın.

İlgili konular

- Giden olayları görüntüleme (sayfa 109)

Giden Olaylar günlüğünden tam erişim izni verme

Giden Olaylar günlüğünde görüntülenen engellenen bir programa tam gelen ve giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Gelişmiş Menü**'yü tıklayın.
- 2 **Raporlar ve Günlükler**'i tıklayın.
- 3 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 4 **Internet ve Ağ**'ı tıklayın ve sonra **Giden Olaylar**'ı tıklayın.
- 5 Bir program seçin ve **Şunu yapmak istiyorum** altında **Erişime İzin Ver**'i tıklayın.
- 6 Onaylamak için Program İzinleri iletişim kutusunda **Evet**'i tıklayın.

Programlara yalnızca giden erişim izni verme

Bilgisayarınızda bulunan bazı programlar, giden Internet erişim izni ister. Firewall, programı yalnızca giden Internet erişim izni verecek şekilde yapılandırmanızı sağlar.

Bir programa yalnızca giden erişim izni verme

Bir programa yalnızca giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklayın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklayın.
- 3 Güvenlik Duvarı bölümünde **Program İzinleri**'ni tıklayın.
- 4 **Program İzinleri** altında, **Engellenen** veya **Tam Erişim** seçeneğine ayarlı bir program seçin.
- 5 **Eylem** altında **Yalnızca Giden Erişimine İzin Ver**'i tıklayın.
- 6 **Tamam**'ı tıklayın.

Son Olaylar günlüğünden yalnızca giden erişim izni verme

Son Olaylar günlüğünde görüntülenen engellenen bir programa yalnızca giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Gelişmiş Menü**'yü tıklayın.
- 2 **Raporlar ve Günlükler**'i tıklayın.
- 3 **Son Olaylar** altında olay açıklamasını seçin ve sonra **Yalnızca Giden Erişimine İzin Ver**'i tıklayın.
- 4 Onaylamak için Program İzinleri iletişim kutusunda **Evet**'i tıklayın.

Giden Olaylar günlüğünden yalnızca giden erişim izni verme

Giden Olaylar günlüğünde görüntülenen engellenen bir programa yalnızca giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Gelişmiş Menü**'yü tıklayın.
- 2 **Raporlar ve Günlükler**'i tıklayın.
- 3 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 4 **Internet ve Ağ**'ı tıklayın ve sonra **Giden Olaylar**'ı tıklayın.
- 5 Bir program seçin ve **Şunu yapmak istiyorum** altında **Yalnızca Giden Erişimine İzin Ver**'i tıklayın.
- 6 Onaylamak için Program İzinleri iletişim kutusunda **Evet**'i tıklayın.

Programların Internet erişimini engelleme

Firewall, programların Internet'e erişmesini engellemenize olanak verir. Bir programı engellediğinizde, bunun ağ bağlantınıza veya düzgün çalışabilmesi için Internet erişimine gereksinim duyan başka bir programa engel olmayacağından emin olun.

Bir programın erişimini engelleme

Bir programın gelen ve giden Internet erişimini engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde **Program İzinleri**'ni tıklatın.
- 4 **Program İzinleri** altında, **Tam Erişim** veya **Yalnızca Giden Erişimi** seçeneğine ayarlı bir program seçin.
- 5 **Eylem** altında **Erişimi Engelle**'yi tıklatın.
- 6 **Tamam**'ı tıklatın.

Yeni bir programın erişimini engelleme

Yeni bir programın gelen ve giden Internet erişimini engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde **Program İzinleri**'ni tıklatın.
- 4 **Program İzinleri** altında **Engellenen Program Ekle**'yi tıklatın.
- 5 Program Ekle iletişim kutusunda, eklemek istediğiniz programa gidip seçin ve sonra **Aç**'ı tıklatın.

Not: Yeni eklenen programın izinlerini değiştirebilirsiniz; bunun için programı seçin ve sonra **Eylem** altında **Yalnızca Giden Erişimine İzin Ver**'i veya **Erişime İzin Ver**'i tıklatın.

Son Olaylar günlüğünden erişimi engelleme

Son Olaylar günlüğünde görüntülenen bir programın gelen ve giden Internet erişimini engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Gelişmiş Menü**'yü tıklatın.
- 2 **Raporlar ve Günlükler**'i tıklatın.
- 3 **Son Olaylar** altında olay açıklamasını seçin ve sonra **Erişimi Engelle**'yi tıklatın.
- 4 Onaylamak için Program İzinleri iletişim kutusunda **Evet**'i tıklatın.

Programların erişim izinlerini kaldırma

Bir program iznini kaldırmadan önce, izin kaldırılınca bilgisayarınızın işlevlerinin veya ağ bağlantınızın etkilenmeyeceğinden emin olun.

Program iznini kaldırma

Bir programın gelen ve giden Internet erişimini kaldırabilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklayın.
- 2 Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklayın.
- 3 Güvenlik Duvarı bölmesinde **Program İzinleri**'ni tıklayın.
- 4 **Program İzinleri** altında bir program seçin.
- 5 **Eylem** altında **Program İznini Kaldır**'ı tıklayın.
- 6 **Tamam**'ı tıklayın.

Not: Firewall, belirli eylemleri karartarak veya devre dışı bırakarak, bazı programları değiştirmenizi önler.

Programlar hakkında bilgi alma

Hangi program iznini uygulamanız gerektiğinden emin olamıyorsanız, McAfee'nin HackerWatch Web sitesinden programla ilgili bilgi alabilirsiniz.

Program bilgilerini alma

Gelen ve giden Internet erişimine izin verme veya engelleme kararı verebilmek için McAfee'nin HackerWatch Web sitesinden program bilgileri alabilirsiniz.

Not: Tarayıcınızın, McAfee'nin programlar, Internet erişimi gereksinimleri ve güvenlik tehditleri hakkında güncel bilgiler sunan HackerWatch Web sitesini açabilmesi için Internet'e bağlandığınızdan emin olun.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde **Program İzinleri**'ni tıklatın.
- 4 **Program İzinleri** altında bir program seçin.
- 5 **Eylem** altında **Ek Bilgi**'yi tıklatın.

Giden Olaylar günlüğünden program bilgilerini alma

Giden Olaylar günlüğünde, hangi programların gelen ve giden Internet erişimine izin vereceğinize karar verebilmek için McAfee'nin HackerWatch Web sitesinden program bilgileri alabilirsiniz.

Not: Tarayıcınızın, McAfee'nin programlar, Internet erişimi gereksinimleri ve güvenlik tehditleri hakkında güncel bilgiler sunan HackerWatch Web sitesini açabilmesi için Internet'e bağlandığınızdan emin olun.

- 1 McAfee SecurityCenter bölümünde **Gelişmiş Menü**'yü tıklatın.
- 2 **Raporlar ve Günlükler**'i tıklatın.
- 3 Son Olaylar altında bir olay seçin ve sonra **Günlük Görüntüle**'yi tıklatın.
- 4 **Internet ve Ağ**'ı tıklatın ve sonra **Giden Olaylar**'ı tıklatın.
- 5 Bir IP adresi seçin ve sonra **Ek bilgi**'yi tıklatın.

B Ö L Ü M 19

Sistem hizmetlerini yönetme

Düzgün çalışabilmeleri için, bazı programların (Web sunucuları ve dosya paylaşımı sunucu programları dahil) atanmış sistem hizmeti portları aracılığıyla, başka bilgisayarlardan istenmeyen bağlantıları kabul etmeleri gerekir. Sisteminizde güvenli olmama olasılığı bulunan kaynakları temsil ettikleri için, Firewall genellikle bu sistem hizmeti portlarını kapatır. Ancak uzak bilgisayarlardan bağlantıları kabul etmek için, sistem hizmeti portları açık olmalıdır.

Bu bölümde

Sistem hizmeti portlarını yapılandırma94

Sistem hizmeti portlarını yapılandırma

Sistem hizmeti portları, bilgisayarınızda bir hizmete uzak ağ erişimi izni verecek veya engelleyecek şekilde yapılandırılabilir.

Aşağıdaki listede, yaygın sistem hizmetleri ve ilişkili portları gösterilmektedir:

- Dosya Aktarım Protokolü (FTP) Portları 20-21
- Posta Sunucusu (IMAP) Portu 143
- Posta Sunucusu (POP3) Portu 110
- Posta Sunucusu (SMTP) Portu 25
- Microsoft Directory Server (MSFT DS) Portu 445
- Microsoft SQL Server (MSFT SQL) Portu 1433
- Ağ Saati Protokolü Portu 123
- Uzak Masaüstü / Uzaktan Yardım / Terminal Server (RDP) Portu 3389
- Uzaktan Yordam Çağrılar (RPC) Portu 135
- Güvenli Web Sunucusu (HTTPS) Portu 443
- Evrensel Tak ve Kullan (UPNP) Portu 5000
- Web Sunucusu (HTTP) Portu 80
- Windows Dosya Paylaşımı (NETBIOS) Portları 137-139

Sistem hizmeti portları, bilgisayarın Internet bağlantısını aynı ağ aracılığıyla kendisine bağlı başka bilgisayarlarla paylaşmasına izin verecek şekilde de yapılandırılabilir. Internet Bağlantısı Paylaşımı (ICS) olarak adlandırılan bu bağlantı, bağlantıyı paylaşan bilgisayarın ağ üzerindeki diğer bilgisayarlar için Internet'e açılan bir ağ geçidi görevi görmesine olanak verir.

Not: Bilgisayarınızda Web veya FTP sunucusu bağlantılarını kabul eden bir uygulama varsa, bağlantıyı paylaşan bilgisayarın ilişkili sistem hizmeti portunu açması ve bu portlar için gelen bağlantıların iletilmesine izin vermesi gerekebilir.

Mevcut sistem hizmeti portuna erişim izni verme

Mevcut bir portu, bilgisayarınızda bir ağ hizmetine uzak erişim izni vermesi için açabilirsiniz.

Not: Açık sistem hizmeti portu, bilgisayarınızı Internet güvenliği tehditlerine açabilir; bu nedenle yalnızca gerekli olursa bir port açın.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklayın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklayın.
- 3 Güvenlik Duvarı bölümünde **Sistem Hizmetleri**'ni tıklayın.
- 4 **Sistem Hizmeti Portu Aç** altında portunu açmak için bir sistem hizmeti seçin.
- 5 **Tamam**'ı tıklayın.

Mevcut sistem hizmeti portuna erişimi engelleme

Mevcut bir portu, bilgisayarınızda bir hizmete uzak ağ erişimini engellemesi için kapatabilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklayın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklayın.
- 3 Güvenlik Duvarı bölümünde **Sistem Hizmetleri**'ni tıklayın.
- 4 **Sistem Hizmeti Portu Aç** altında, portunu kapatmak için sistem hizmetinin işaretini temizleyin.
- 5 **Tamam**'ı tıklayın.

Yeni bir sistem hizmeti portunu yapılandırma

Bilgisayarınızda, bilgisayarınızdan uzaktan erişime izin vermeyi veya engellemeyi açıp kapatabileceğiniz yeni bir ağ hizmet portu yapılandırabilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklayın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklayın.
- 3 Güvenlik Duvarı bölümünde **Sistem Hizmetleri**'ni tıklayın.
- 4 **Ekle**'yi tıklayın.
- 5 Sistem Hizmetleri bölümünde, **Bağlantı Noktaları ve Sistem Hizmetleri** altında şunları girin:
 - Program adı
 - Gelen TCP/IP portları

- Giden TCP/IP portları
 - Gelen UDP portları
 - Giden UDP portları
- 6** Bu portun etkinlik bilgilerini, ağda Internet bağlantınızı paylaşan başka bir Windows bilgisayarına göndermek isterseniz, **Bu bağlantı noktası üzerindeki ağ etkinliğini Internet Bağlantısı Paylaşımı kullanan ağ kullanıcılarına iletin** seçeneğini belirleyin.
- 7** İsterseniz, yeni yapılandırmaya açıklama ekleyebilirsiniz.
- 8** **Tamam'ı** tıklatın.

Not: Bilgisayarınızda Web veya FTP sunucusu bağlantılarını kabul eden bir uygulama varsa, bağlantıyı paylaşan bilgisayarın ilişkili sistem hizmeti portunu açması ve bu portlar için gelen bağlantıların iletilmesine izin vermesi gerekebilir. Internet Bağlantısı Paylaşımı (ICS) özelliğini kullanıyorsanız, Güvenilen IP Adresleri listesine güvenilen bilgisayar bağlantısı da eklemeniz gerekebilir. Ayrıntılı bilgi için bkz. Güvenilen bilgisayar bağlantısı ekleme

Sistem hizmeti portunu değiştirme

Mevcut sistem hizmeti portuyla ilgili gelen ve giden ağ erişimi bilgilerini değiştirebilirsiniz.

Not: Port bilgisi yanlış girilirse, sistem hizmeti başarısız olur.

- 1** McAfee SecurityCenter bölmesinde **Internet ve Ağ'ı**, ardından **Yapılandır'ı** tıklatın.
- 2** Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıklatın.
- 3** Güvenlik Duvarı bölmesinde **Sistem Hizmetleri'ni** tıklatın.
- 4** Bir sistem hizmeti seçin ve sonra **Düzenle'yi** tıklatın.
- 5** Sistem Hizmetleri bölmesinde, **Bağlantı Noktaları ve Sistem Hizmetleri** altında şunları girin:
 - Program adı
 - Gelen TCP/IP portları
 - Giden TCP/IP portları
 - Gelen UDP portları
 - Giden UDP portları

- 6 Bu portun etkinlik bilgilerini, ağda Internet bağlantınızı paylaşan başka bir Windows bilgisayarına göndermek isterseniz, **Bu bağlantı noktası üzerindeki ağ etkinliğini Internet Bağlantısı Paylaşımı** kullanan ağ kullanıcılarına iletin seçeneğini belirleyin.
- 7 İsterseniz, değiştirilen yapılandırmaya açıklama ekleyebilirsiniz.
- 8 **Tamam**'ı tıklatın.

Sistem hizmeti portunu kaldırma

Mevcut bir sistem hizmeti portunu bilgisayarınızdan kaldırabilirsiniz. Kaldırdıktan sonra, uzak bilgisayarlar artık bilgisayarınızdaki ağ hizmetine erişemez.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde **Sistem Hizmetleri**'ni tıklatın.
- 4 Bir sistem hizmeti seçin ve **Kaldır**'ı tıklatın.
- 5 Onaylamak için açılan sorgu penceresinde **Evet**'i tıklatın.

B Ö L Ü M 2 0

Bilgisayar bağlantılarını yönetme

Uzak bilgisayarlarla ilişkili Internet Protokolü (IP) adreslerini temel alan kurallar oluşturarak, bilgisayarınıza yapılan belirli uzak bağlantıları yönetmek üzere Firewall'u yapılandırabilirsiniz. Güvenilen IP adresleriyle ilişkili bilgisayarların bilgisayarınıza bağlanmasına izin verilirken; bilinmeyen, şüpheli veya güvenilmeyen IP'lerin bilgisayarınıza bağlanması yasaklanabilir.

Bir bağlantıya izin verirken, güvendiğiniz bilgisayarın güvenli olduğundan emin olun. Güvendiğiniz bir bilgisayara solucan veya başka bir mekanizma bulaşmışsa, bilgisayarınız etkilere açık olabilir. Ayrıca, McAfee güvendiğiniz bilgisayarların güvenlik duvarının yanı sıra güncel bir virüsten korunma programıyla da korunmasını önerir. Firewall, Güvenilen IP Adresleri listesinde bulunan IP adreslerinin trafiğini günlüğe kaydetmez veya bunlardan olay uyarıları üretmez.

Bilinmeyen, şüpheli veya güvenilmeyen IP adresleriyle ilişkili bilgisayarların, sizin bilgisayarınıza bağlanması yasaklanabilir.

Firewall tüm istenmeyen trafiği engellediği için, genellikle bir IP adresini yasaklamanız gerekmez. Bir IP adresini ancak Internet bağlantısının belirli bir tehdit oluşturduğundan eminseniz yasaklamalısınız. DNS veya DHCP sunucunuz ya da diğer ISS ile ilişkili sunucular gibi önemli IP adreslerini engellemediğinizden emin olun. Güvenlik ayarlarınıza bağlı olarak, Firewall yasaklanan bir bilgisayardan olay algıladığında sizi uyarabilir.

Bu bölümde

Bilgisayar bağlantılarına güvenme.....	100
Bilgisayar bağlantılarını yasaklama	103

Bilgisayar bağlantılarına güvenme

Güvenilen ve Yasaklı IP'ler bölümünde, **Güvenilen IP Adresleri** altında güvenilen IP adresleri ekleyebilir, düzenleyebilir ve kaldırabilirsiniz.

Güvenilen ve Yasaklı IP'ler bölümündeki **Güvenilen IP Adresleri** listesi, belirli bir bilgisayarın sizin bilgisayarınıza ulaşmak için gerçekleştirdiği tüm trafiğe izin verir. Firewall, **Güvenilen IP Adresleri** listesinde görüntülenen IP adreslerinin trafiğini günlüğe kaydetmez veya bunlardan olay uyarıları üretmez.

Firewall, listede işaretli olan IP adreslerine güvenir ve herhangi bir port üzerinde güvenlik duvarı aracılığıyla güvenilir IP'nin trafiğine her zaman izin verir. Güvenilen bir IP adresiyle ilişkili bilgisayar ve sizin bilgisayarınız arasındaki etkinlik, Firewall tarafından filtrelenmez veya analiz edilmez. Varsayılan olarak, Güvenilen IP Adresleri'nde Firewall'un bulduğu ilk özel ağ listelenir.

Bir bağlantıya izin verirken, güvendiğiniz bilgisayarın güvenli olduğundan emin olun. Güvendiğiniz bir bilgisayara solucan veya başka bir mekanizma bulaşmışsa, bilgisayarınız etkilere açık olabilir. Ayrıca, McAfee güvendiğiniz bilgisayarların güvenlik duvarının yanı sıra güncel bir virüsten korunma programıyla da korunmasını önerir.

Güvenilen bilgisayar bağlantısı ekleme

Güvenilen bir bilgisayar bağlantısı ve bununla ilişkili IP adresi ekleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklayın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklayın.
- 3 Güvenlik Duvarı bölümünde, **Güvenilen ve Yasaklı IP'ler** seçeneğini tıklayın.
- 4 Güvenilen ve Yasaklı IP'ler bölümünde **Güvenilen IP Adresleri**'ni seçin ve sonra **Ekle**'yi tıklayın.
- 5 **Güvenilen IP Adresi Kuralı Ekle** altında, aşağıdakilerden birini gerçekleştirin:
 - **Tek IP Adresi**'ni seçin ve sonra IP adresini girin.
 - **IP Adresi Aralığı**'nı seçin ve sonra **IP Adreslerinden** ve **IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin.

- 6 Sistem hizmeti Internet Bağlantısı Paylaşımı (ICS) kullanıyorsa, şu IP adresi aralığını ekleyebilirsiniz: 192.168.0.1 - 192.168.0.255.
- 7 İsterseniz, **Kuralın geçerlilik süresi**'ni seçip, kuralın geçerli olacağı gün sayısını girebilirsiniz.
- 8 Ayrıca, kural için bir açıklama da yazabilirsiniz.
- 9 **Tamam**'ı tıklayın.
- 10 Onaylamak için **Güvenilen ve Yasaklı IP'ler** iletişim kutusunda **Evet**'i tıklayın.

Not: Internet Bağlantısı Paylaşımı (ICS) hakkında ayrıntılı bilgi için bkz. Yeni bir sistem hizmeti yapılandırma.

Gelen Olaylar günlüğünden güvenilen bir bilgisayar ekleme

Gelen Olaylar günlüğünden güvenilen bir bilgisayar bağlantısını ve onunla ilişkili IP adresini ekleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde, Ortak Görevler bölümünde **Gelişmiş Menü**'yü tıklayın.
- 2 **Raporlar ve Günlükler**'i tıklayın.
- 3 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 4 **Internet ve Ağ**'ı tıklayın ve sonra **Gelen Olaylar**'ı tıklayın.
- 5 Kaynak IP adresini seçin ve **Şunu yapmak istiyorum** altında **Bu Adrese Güven**'i tıklayın.
- 6 Onaylamak için **Evet**'i tıklayın.

Güvenilen bilgisayar bağlantısını düzenleme

Güvenilen bir bilgisayar bağlantısını ve bununla ilişkili IP adresini düzenleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklayın.
- 2 **Internet ve Ağ Yapılandırması** bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklayın.
- 3 **Güvenlik Duvarı** bölümünde, **Güvenilen ve Yasaklı IP'ler** seçeneğini tıklayın.
- 4 **Güvenilen ve Yasaklı IP'ler** bölümünde **Güvenilen IP Adresleri**'ni seçin.
- 5 Bir IP adresi seçin ve ardından **Düzenle**'yi tıklayın.
- 6 **Güvenilen IP Adresi Düzenle** altında, aşağıdakilerden birini gerçekleştirin:
 - **Tek IP Adresi**'ni seçin ve sonra IP adresini girin.
 - **IP Adresi Aralığı**'ni seçin ve sonra **IP Adreslerinden ve IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin.

- 7 İsterseniz **Kuralın geçerlilik süresi**'ni işaretleyip, kuralın geçerli olacağı gün sayısını girebilirsiniz.
- 8 Ayrıca, kural için bir açıklama da yazabilirsiniz.
- 9 **Tamam**'ı tıklayın.

Not: Firewall'un güvenilen özel ağdan otomatik olarak eklediği varsayılan bilgisayar bağlantılarını düzenleyemezsiniz.

Güvenilen bilgisayar bağlantısını kaldırma

Güvenilen bir bilgisayar bağlantısını ve bununla ilişkili IP adresini kaldırabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklayın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklayın.
- 3 Güvenlik Duvarı bölümünde, **Güvenilen ve Yasaklı IP'ler** seçeneğini tıklayın.
- 4 Güvenilen ve Yasaklı IP'ler bölümünde **Güvenilen IP Adresleri**'ni seçin.
- 5 Bir IP adresi seçin ve ardından **Kaldır**'ı tıklayın.
- 6 Onaylamak için **Güvenilen ve Yasaklı IP'ler** iletişim kutusunda **Evet**'i tıklayın.

Bilgisayar bağlantılarını yasaklama

Güvenilen ve Yasaklı IP'ler bölümünde, **Yasaklanan IP Adresleri** altında yasaklı IP adresleri ekleyebilir, düzenleyebilir ve kaldırabilirsiniz.

Bilinmeyen, şüpheli veya güvenilmeyen IP adresleriyle ilişkili bilgisayarların, sizin bilgisayarınıza bağlanması yasaklanabilir.

Firewall tüm istenmeyen trafiği engellediği için, genellikle bir IP adresini yasaklamanız gerekmez. Bir IP adresini ancak Internet bağlantısının belirli bir tehdit oluşturduğundan eminseniz yasaklamalısınız. DNS veya DHCP sunucunuz ya da diğer ISS ile ilişkili sunucular gibi önemli IP adreslerini engellemediğinizden emin olun. Güvenlik ayarlarınıza bağlı olarak, Firewall yasaklanan bir bilgisayardan olay algıladığında sizi uyarabilir.

Yasaklanan bilgisayar bağlantısı ekleme

Yasaklanan bir bilgisayar bağlantısı ve bununla ilişkili IP adresi ekleyebilirsiniz.

Not: DNS veya DHCP sunucunuz ya da diğer ISS ile ilişkili sunucular gibi önemli IP adreslerini engellemediğinizden emin olun.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde, **Güvenilen ve Yasaklı IP'ler** seçeneğini tıklatın.
- 4 Güvenilen ve Yasaklı IP'ler bölümünde **Yasaklanan IP Adresleri**'ni seçin ve sonra **Ekle**'yi tıklatın.
- 5 **Yasaklanan IP Adresi Kuralı Ekle** altında, aşağıdakilerden birini gerçekleştirin:
 - **Tek IP Adresi**'ni seçin ve sonra IP adresini girin.
 - **IP Adresi Aralığı**'nı seçin ve sonra **IP Adreslerinden ve IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin.
- 6 İsterseniz, **Kuralın geçerlilik süresi**'ni seçip, kuralın geçerli olacağı gün sayısını girebilirsiniz.
- 7 Ayrıca, kural için bir açıklama da yazabilirsiniz.
- 8 **Tamam**'ı tıklatın.
- 9 Onaylamak için **Güvenilen ve Yasaklı IP'ler** iletişim kutusunda **Evet**'i tıklatın.

Yasaklanan bilgisayar bağlantısını düzenleme

Yasaklanan bir bilgisayar bağlantısını ve bununla ilişkili IP adresini düzenleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde, **Güvenilen ve Yasaklı IP'ler** seçeneğini tıklatın.
- 4 Güvenilen ve Yasaklı IP'ler bölümünde **Yasaklanan IP Adresleri**'ni seçin ve sonra **Düzenle**'yi tıklatın.
- 5 **Yasaklanan IP Adresi Düzenle** altında, aşağıdakilerden birini gerçekleştirin:
 - **Tek IP Adresi**'ni seçin ve sonra IP adresini girin.
 - **IP Adresi Aralığı**'ni seçin ve sonra **IP Adreslerinden** ve **IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin.
- 6 İsterseniz, **Kuralın geçerlilik süresi**'ni seçip, kuralın geçerli olacağı gün sayısını girebilirsiniz.
- 7 Ayrıca, kural için bir açıklama da yazabilirsiniz.
- 8 **Tamam**'ı tıklatın.

Yasaklanan bilgisayar bağlantısını kaldırma

Yasaklanan bir bilgisayar bağlantısını ve bununla ilişkili IP adresini kaldırabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde, **Güvenilen ve Yasaklı IP'ler** seçeneğini tıklatın.
- 4 Güvenilen ve Yasaklı IP'ler bölümünde **Yasaklanan IP Adresleri**'ni seçin.
- 5 Bir IP adresi seçin ve ardından **Kaldır**'ı tıklatın.
- 6 Onaylamak için **Güvenilen ve Yasaklı IP'ler** iletişim kutusunda **Evet**'i tıklatın.

Gelen Olaylar günlüğünden bir bilgisayarı yasaklama

Gelen Olaylar günlüğünden bir bilgisayar bağlantısını ve onunla ilişkili IP adresini yasaklayabilirsiniz.

Gelen Olaylar günlüğünde görüntülenen IP adresleri engellenir. Bu nedenle, bilgisayarınız özellikle açılan portlar kullanmıyorsa veya Internet erişim izni verilen bir program içermiyorsa, adresin yasaklanması ek koruma sağlamaz.

Yalnızca bir veya daha fazla bilerek açılmış portunuz varsa ve bu adresin açık portlara erişiminin engellenmesi gerektiğine inanmak için yeterli nedeniniz varsa, **Yasaklanan IP Adresleri** listesine bir IP adresi ekleyin.

Şüpheli veya istenmeyen Internet etkinliğinin kaynağı olduğundan şüphelendiğiniz bir IP adresini yasaklamak için, tüm gelen Internet trafiğinin IP adreslerini listeleyen Gelen Olaylar sayfasını kullanabilirsiniz.

- 1 McAfee SecurityCenter bölümünde, **Ortak Görevler** altında, **Gelişmiş Menü**'yü tıklayın.
- 2 **Raporlar ve Günlükler**'i tıklayın.
- 3 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 4 **Internet ve Ağ**'ı tıklayın ve sonra **Gelen Olaylar**'ı tıklayın.
- 5 Kaynak IP adresini seçin ve **Şunu yapmak istiyorum** altında **Bu Adresi Yasakla**'yı tıklayın.
- 6 Onaylamak için **Yasaklanan IP Adresi Kuralı Ekle** iletişim kutusunda **Evet**'i tıklayın.

İzinsiz Giriş Tespiti Olayları günlüğünden bir bilgisayarı yasaklama

İzinsiz Giriş Tespiti Olayları günlüğünden, bir bilgisayar bağlantısını ve onunla ilişkili IP adresini yasaklayabilirsiniz.

- 1 McAfee SecurityCenter bölümünde, **Ortak Görevler** altında, **Gelişmiş Menü**'yü tıklayın.
- 2 **Raporlar ve Günlükler**'i tıklayın.
- 3 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 4 **Internet ve Ağ**'ı ve sonra **İzinsiz Giriş Tespiti Olayları**'nı tıklayın.
- 5 Kaynak IP adresini seçin ve **Şunu yapmak istiyorum** altında **Bu Adresi Yasakla**'yı tıklayın.
- 6 Onaylamak için **Yasaklanan IP Adresi Kuralı Ekle** iletişim kutusunda **Evet**'i tıklayın.

B Ö L Ü M 2 1

Günlüğe kaydetme, izleme ve analiz

Firewall, Internet olayları ve trafiğinin kapsamlı ve okunması kolay bir biçimde günlüğe kaydedilmesini, izlenmesini ve analizini sağlar. Internet trafiğini ve olayları anlamak, Internet bağlantılarınızı yönetmenize yardımcı olur.

Bu bölümde

Olay Günlüğü Kaydetme.....	108
İstatistiklerle Çalışma.....	110
Internet trafiğini izleme.....	111
Internet trafiğini izleme.....	114

Olay Günlüğü Kaydetme

Firewall, olay günlüğü kaydetmeyi etkinleştirmenize veya devre dışı bırakmanıza ve etkinleştirildiğinde hangi olay türlerinin günlüğe kaydedileceğini belirlemenize olanak verir. Olay günlüğüne kaydetme, en son gelen ve giden olayları görüntülemenizi sağlar.

Olay günlüğü ayarlarını yapılandırma

Günlüğe kaydedilecek Firewall olaylarının türlerini belirtebilir ve bunları yapılandırabilirsiniz. Varsayılan olarak, olay günlüğü kaydetme tüm olaylar ve etkinlikler için etkindir.

- 1 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 2 Güvenlik Duvarı bölümünde **Olay Günlüğü Ayarları**'nı tıklatın.
- 3 Zaten seçili değilse, **Olay Günlüğü Kaydetmeyi Etkinleştir**'i seçin.
- 4 **Olay Günlüğü Kaydetmeyi Etkinleştir** altında günlüğe kaydedilmesini istediğiniz veya istemediğiniz olay türlerini seçin veya seçimini kaldırın. Olay türleri aşağıdakileri içerir:
 - Engellenen Programlar
 - ICMP Pingleri
 - Yasaklı IP Adreslerinden Gelen Trafik
 - Sistem Hizmet Portları İle İlgili Olaylar
 - Bilinmeyen Portları İle İlgili Olaylar
 - İzinsiz Giriş Tespiti (IDS) olayları
- 5 Belirli portlarda günlük kaydını engellemek için, **Aşağıdaki portlarla ilgili olayları günlüğe kaydetme**'yi seçin ve ardından tek port numaralarını virgüllerle, port aralıklarını tirelerle ayırarak girin. Örnek: 137-139, 445, 400-5000.
- 6 **Tamam**'ı tıklatın.

Son olayları görüntüleme

Günlük kaydı etkinse, son olayları görüntüleyebilirsiniz. Son Olaylar bölümünde, olayın tarihi ve açıklaması görüntülenir. Bu bölme, Internet erişimi açıkça engellenmiş olan programların etkinliğini görüntüler.

- **Gelişmiş Menü**'de, Ortak Görevler bölümünde **Raporlar ve Günlükler**'i veya **Son Olayları Görüntüle**'yi tıklatın. İsterseniz Temel Menü'de, Ortak Görevler bölümünde **Son Olayları Görüntüle**'yi tıklatabilirsiniz.

Gelen olayları görüntüleme

Günlük kaydı etkinse, gelen olayları görüntüleyebilirsiniz. Gelen Olaylar; tarih ve saati, kaynak IP adresini, ana bilgisayar adını, bilgi ve olay türünü içerir.

- 1 Gelişmiş menünün etkin olduğundan emin olun. Ortak Görevler bölümünde **Raporlar ve Günlükler**'i tıklayın.
- 2 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 3 **Internet ve Ağ**'ı tıklayın ve sonra **Gelen Olaylar**'ı tıklayın.

Not: Gelen Olay günlüğünde bir IP adresini güvenilen, yasaklanan veya izlenen olarak belirleyebilirsiniz.

Giden olayları görüntüleme

Günlük kaydı etkinse, giden olayları görüntüleyebilirsiniz. Giden Olaylar, giden erişim sağlamaya çalışan programın adını, olay tarihi ve saatini, programın bilgisayarınızdaki konumunu içerir.

- 1 Ortak Görevler bölümünde **Raporlar ve Günlükler**'i tıklayın.
- 2 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 3 **Internet ve Ağ**'ı tıklayın ve sonra **Giden Olaylar**'ı tıklayın.

Not: Giden Olaylar günlüğünden, bir programa tam erişim veya yalnızca giden erişim izni verebilirsiniz. Ayrıca, programla ilgili ek bilgiler de bulabilirsiniz.

İzinsiz giriş tespiti olaylarını görüntüleme

Günlük kaydı etkinse, gelen izinsiz giriş olaylarını görüntüleyebilirsiniz. İzinsiz Giriş Tespiti olayları; olayın tarih ve saatini, kaynak IP'sini, ana bilgisayar adını ve türünü görüntüler.

- 1 Ortak Görevler bölümünde **Raporlar ve Günlükler**'i tıklayın.
- 2 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 3 **Internet ve Ağ**'ı ve sonra **İzinsiz Giriş Tespiti Olayları**'nı tıklayın.

Not: İzinsiz Giriş Tespiti Olayları günlüğünde, bir IP adresini yasaklanan ve izlenen olarak belirleyebilirsiniz.

İstatistiklerle Çalışma

Firewall, size genel Internet güvenliği olayları ve port etkinliği hakkında istatistikler sunmak için, McAfee'nin HackerWatch güvenlik Web sitesini destekler.

Genel güvenlik olayı istatistiklerini görüntüleme

HackerWatch, SecurityCenter'da görüntüleyebileceğiniz dünya çapındaki Internet güvenliği olaylarını izler. İzleme bilgilerinde son 24 saat, 7 gün ve 30 gün içinde HackerWatch'a raporlanan olaylar listelenir.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **HackerWatch**'u tıklatın.
- 3 Olay İzleme altında güvenlik olayı istatistiklerini görüntüleyin.

Genel Internet port etkinliğini görüntüleme

HackerWatch, SecurityCenter'da görüntüleyebileceğiniz dünya çapındaki Internet güvenliği olaylarını izler. Görüntülenen bilgiler, son yedi gün içinde HackerWatch'a rapor edilen en son olay portlarını içerir. Genellikle HTTP, TCP ve UDP port bilgileri görüntülenir.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **HackerWatch**'u tıklatın.
- 3 **En Son Port Etkinliği** altında en son olay portlarını görüntüleyin.

İnternet trafiğini izleme

Firewall, İnternet trafiğini izlemek için çeşitli seçenekler sunar. Bu seçenekler, bir ağ bilgisayarının coğrafi konumunu izlemenize, etki alanı ve ağ bilgilerini elde etmenize, Gelen Olaylar ve İzinsiz Giriş Tespiti Olayları günlüklerinden bilgisayarları izlemenize olanak verir.

Bir ağ bilgisayarının coğrafi konumunu izleme

Görsel İzleyici kullanarak, bilgisayarınıza bağlanan veya bağlanmaya çalışan bir bilgisayarın coğrafi konumunu, adı veya IP adresi ile bulabilirsiniz. Ayrıca, Görsel İzleyici ile ağ ve kayıt bilgilerine de erişebilirsiniz. Görsel İzleyici çalıştırıldığında, kaynak bilgisayardan sizin bilgisayarınıza alınan veriler için en olası yolu gösteren bir dünya haritası görüntülenir.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **Görsel İzleyici**'yi tıklatın.
- 3 Bilgisayarın IP adresini yazın ve **İzle**'yi tıklatın.
- 4 **Görsel İzleyici** altında **Harita Görünümü**'nü seçin.

Not: Döngüsel, özel veya geçersiz IP adresi olaylarını izleyemezsiniz.

Bilgisayar kayıt bilgilerini elde etme

Visual Trace kullanarak, SecurityCenter'dan bir bilgisayarın kayıt bilgilerini elde edebilirsiniz. Bu bilgiler etki alanı adını, kayıt adı ve adresini, yönetici iletişim bilgilerini içerir.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **Görsel İzleyici**'yi tıklatın.
- 3 Bilgisayarın IP adresini yazın ve ardından **İzle**'yi tıklatın.
- 4 **Görsel İzleyici** altında **Kayıt Görünümü**'nü seçin.

Bilgisayar ağ bilgilerini elde etme

Visual Trace kullanarak, SecurityCenter'dan bir bilgisayarın ağ bilgilerini elde edebilirsiniz. Ağ bilgileri, etki alanının bulunduğu ağ ile ilgili ayrıntıları içerir.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **Görsel İzleyici**'yi tıklatın.
- 3 Bilgisayarın IP adresini yazın ve ardından **İzle**'yi tıklatın.
- 4 **Görsel İzleyici** altında **Ağ Görünümü**'nü seçin.

Gelen Olaylar günlüğünden bir bilgisayarı izleme

Gelen Olaylar bölmesinden, Gelen Olaylar günlüğünde görüntülenen bir IP adresini izleyebilirsiniz.

- 1 Gelişmiş menünün etkin olduğundan emin olun. Ortak Görevler bölümünde **Raporlar ve Günlükler**'i tıklatın.
- 2 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklatın.
- 3 **Internet ve Ağ**'ı tıklatın ve sonra **Gelen Olaylar**'ı tıklatın.
- 4 Gelen Olaylar bölümünde, bir kaynak IP adresi seçin ve ardından **Bu adresi izle**'yi tıklatın.
- 5 Görsel İzleyici bölümünde, aşağıdakilerden birini tıklatın:
 - **Harita Görünümü**: Seçili IP adresini kullanarak bilgisayarın coğrafi konumunu bulun.
 - **Kayıt Görünümü**: Seçili IP adresini kullanarak etki alanı bilgilerini bulun.
 - **Ağ Görünümü**: Seçili IP adresini kullanarak ağ bilgilerini bulun.
- 6 **Bitti**'yi tıklatın.

İzinsiz Giriş Tespiti Olayları günlüğünden bir bilgisayarı izleme

İzinsiz Giriş Tespiti Olayları bölmesinden, İzinsiz Giriş Tespiti Olayları günlüğünde görüntülenen bir IP adresini izleyebilirsiniz.

- 1 Ortak Görevler bölümünde **Raporlar ve Günlükler**'i tıklatın.
- 2 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklatın.
- 3 **Internet ve Ağ**'ı ve sonra **İzinsiz Giriş Tespiti Olayları**'nı tıklatın. İzinsiz Giriş Tespiti Olayları bölümünde, bir kaynak IP adresi seçin ve sonra **Bu adresi izle**'yi tıklatın.
- 4 Görsel İzleyici bölümünde, aşağıdakilerden birini tıklatın:
 - **Harita Görünümü**: Seçili IP adresini kullanarak bilgisayarın coğrafi konumunu bulun.
 - **Kayıt Görünümü**: Seçili IP adresini kullanarak etki alanı bilgilerini bulun.
 - **Ağ Görünümü**: Seçili IP adresini kullanarak ağ bilgilerini bulun.
- 5 **Bitti**'yi tıklatın.

İzlenen bir IP adresini izleme

Kaynak bilgisayardan sizin bilgisayarınıza alınan veriler için en olası yolu gösteren coğrafi görünümü elde etmek üzere, izlenen bir IP adresini izleyebilirsiniz. Ayrıca, IP adresiyle ilgili kayıt ve ağ bilgilerini de elde edebilirsiniz.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **Trafik Monitörü**'nü tıklatın.
- 3 **Trafik Monitörü** altında **Etkin Programlar**'ı tıklatın.
- 4 Bir program seçin ve ardından program adının altında görüntülenen IP adresini belirleyin.
- 5 **Program Etkinliği** altında **Bu IP'yi İzle**'yi tıklatın.
- 6 **Görsel İzleyici** altında, kaynak bilgisayardan sizin bilgisayarınıza alınan veriler için en olası yolu gösteren bir harita görüntüleyebilirsiniz. Ayrıca, IP adresiyle ilgili kayıt ve ağ bilgilerini de elde edebilirsiniz.

Not: En güncel istatistikleri görüntülemek için, **Görsel İzleyici** altında **Yenile**'yi tıklatın.

Internet trafiğini izleme

Firewall, aşağıdakileri içeren Internet trafiğinizi izlemek için çeşitli yöntemler sunar:

- **Trafik Analizi grafiği:** En son gelen ve giden Internet trafiğini görüntüler.
- **Trafik Kullanımı grafiği:** Son 24 saatte en etkin programlar tarafından kullanılan bant genişliği yüzdesini görüntüler.
- **Etkin Programlar:** Bilgisayarınızda ağ bağlantılarının büyük bir bölümünü kullanan programları ve bu programların eriştikleri IP adreslerini görüntüler.

Trafik Analizi grafiği hakkında

Trafik Analizi grafiği, gelen ve giden Internet trafiğinin sayısal ve grafiksel anlatımıdır. Ayrıca Trafik Monitörü, bilgisayarınızda en büyük ağ bağlantısı sayısını ve programın eriştiği IP adreslerini kullanarak programları görüntüler.

Trafik Analizi bölümünde, en son gelen ve giden Internet trafiğinin yanı sıra geçerli, ortalama ve en yüksek aktarım hızlarını görüntüleyebilirsiniz. Ayrıca, Firewall'u başlattıktan sonra gerçekleşen trafiğin miktarını içeren trafik hacmini, geçerli ve önceki aylara ait toplam trafiği de görüntüleyebilirsiniz.

Trafik Analizi bölümü, bilgisayarınızda son gelen ve giden Internet trafiğinin hacmi ve hızı, bağlantı hızı ve Internet üzerinden aktarılan toplam baytı içeren bilgisayarınızın gerçek zamanlı Internet etkinliğini görüntüler.

Düz yeşil çizgi, gelen trafiğin geçerli aktarım hızını temsil eder. Kesik yeşil çizgi, gelen trafiğin ortalama aktarım hızını temsil eder. Geçerli aktarım hızı ve ortalama aktarım hızı aynıysa, grafikte kesik çizgi görüntülenmez. Bu durumda, düz çizgi hem ortalama hem de geçerli aktarım hızını temsil eder.

Düz kırmızı çizgi, giden trafiğin geçerli aktarım hızını temsil eder. Kesik kırmızı çizgi, giden trafiğin ortalama aktarım hızını temsil eder. Geçerli aktarım hızı ve ortalama aktarım hızı aynıysa, grafikte kesik çizgi görüntülenmez. Bu durumda, düz çizgi hem ortalama hem de geçerli aktarım hızını temsil eder.

Gelen ve giden trafiği analiz etme

Trafik Analizi grafiği, gelen ve giden Internet trafiğinin sayısal ve grafiksel anlatımıdır. Ayrıca Trafik Monitörü, bilgisayarınızda en büyük ağ bağlantısı sayısını ve programın eriştiği IP adreslerini kullanarak programları görüntüler.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklayın.
- 2 Araçlar bölümünde **Trafik Monitörü**'nü tıklayın.
- 3 **Trafik Monitörü** altında **Trafik Analizi**'ni tıklayın.

İpucu: En güncel istatistikleri görüntülemek için, **Trafik Analizi** altında **Yenile**'yi tıklayın.

Program bant genişliğini izleme

Son yirmi dört saat içinde bilgisayarınızdaki en etkin programlar tarafından kullanılan bant genişliğinin yaklaşık yüzdesini gösteren pasta grafiği görüntüleyebilirsiniz. Pasta grafik, programlar tarafından kullanılan göreceli bant genişliği miktarlarının görsel anlatımını sunar.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklayın.
- 2 Araçlar bölümünde **Trafik Monitörü**'nü tıklayın.
- 3 **Trafik Monitörü** altında **Trafik Kullanımı**'ni tıklayın.

İpucu: En güncel istatistikleri görüntülemek için, **Trafik Kullanımı** altında **Yenile**'yi tıklayın.

Program etkinliğini izleme

Uzak bilgisayar bağlantılarını ve portları gösteren, gelen ve giden program etkinliğini görüntüleyebilirsiniz.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklayın.
- 2 Araçlar bölümünde **Trafik Monitörü**'nü tıklayın.
- 3 **Trafik Monitörü** altında **Etkin Programlar**'ı tıklayın.
- 4 Aşağıdaki bilgileri görüntüleyebilirsiniz:
 - Program Etkinliği grafiği: Etkinlik grafiğini görüntüleyeceğiniz programı seçin.
 - Dinleme bağlantısı: Program adı altında bir Dinleme ögesi seçin.
 - Bilgisayar bağlantısı: Program adı, sistem işlemi veya hizmet altında bir IP adresi seçin.

Not: En güncel istatistikleri görüntülemek için, **Etkin Programlar** altında **Yenile**'yi tıklayın.

B Ö L Ü M 2 2

İnternet güvenliđi hakkında bilgi alma

Firewall, size programlar ve genel İnternet etkinliđi hakkında güncel bilgiler sunmak için McAfee'nin güvenlik Web sitesi HackerWatch'u destekler. HackerWatch, Firewall hakkında bir HTML dersi de sağlar.

Bu bölümde

HackerWatch dersini başlatma 118

HackerWatch dersini başlatma

Firewall hakkında bilgi almak için, SecurityCenter'dan HackerWatch dersine erişebilirsiniz.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklayın.
- 2 Araçlar bölümünde **HackerWatch**'u tıklayın.
- 3 **HackerWatch Kaynakları** altında **Dersi Görüntüle**'yi tıklayın.

B Ö L Ü M 23

McAfee Anti-Spam

Anti-Spam (eski adıyla SpamKiller), gelen e-postalarınızı inceleyip, istenmeyen e-postaları spam (sizin bir şey satın almanıza yetki veren e-posta) veya phishing (kişisel bilgilerinizi hileli olma olasılığı bulunan Web sitelerine sağlamanıza yetki veren e-posta) olarak işaretler ve böylece bunların Gelen Kutusu'na girişini durdurur. Anti-Spam, daha sonra spam e-postaları filtreler ve McAfee Anti-Spam klasörüne taşır.

Arkadaşlarınız bazen size spam gibi görünen yasal e-postalar gönderirlerse, bu adresleri Anti-Spam'in arkadaş listesine ekleyerek bunların filtrelenmemesini sağlayabilirsiniz. Ayrıca, spam iletilerin algılanma biçimini de özelleştirebilirsiniz. Örneğin, iletileri daha kararlı bir şekilde filtreleyebilir, ileti içinde nelerin aranacağını belirtebilir ve kendi filtrelerinizi oluşturabilirsiniz.

E-posta iletisinin içindeki bir bağlantı aracılığıyla hileli olma olasılığı bulunan bir Web sitesine erişmeye çalıştığınızda da Anti-Spam sizi korur. Hileli olma olasılığı bulunan bir Web sitesinin bağlantısını tıklattığınızda, Phishing filtresinin güvenli sayfasına yönlendirilirsiniz. Filtrelenmesini istemediğiniz Web siteleri varsa, bunları beyaz listeye ekleyebilirsiniz (bu listedeki Web siteleri filtrelenmez).

Anti-Spam; POP3, POP3 Web postası, Yahoo®, MSN®/Hotmail®, Windows® Live™ Mail ve MAPI (Microsoft Exchange Server) hesapları gibi çeşitli e-posta programlarıyla çalışır. E-postanızı okumak için tarayıcı kullanıyorsanız, Web posta hesabınızı Anti-Spam'e eklemeniz gerekir. Diğer tüm hesaplar otomatik olarak yapılandırılır ve bunları Anti-Spam'e eklemeniz gerekmez.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Anti-Spam özellikleri	121
Web posta hesaplarınızı ayarlama	123
Arkadaşları ayarlama	127
Spam algılamayı yapılandırma	133
E-posta filtreleme	141
Filtrelenen e-posta ile çalışma	145
Phishing korumasını yapılandırma	147

Anti-Spam özellikleri

Anti-Spam aşağıdaki özellikleri sunar.

Spam filtreleme

Anti-Spam'in gelişmiş filtreleri, istenmeyen e-postaların Gelen Kutusu'na girişini engeller ve tüm e-posta hesaplarınız için otomatik olarak güncelleştirilir. Ayrıca, tüm spam iletilerin filtrelendiğinden emin olmak için özel filtreler oluşturabilir ve spam iletileri analiz için McAfee'ye bildirebilirsiniz.

Phishing filtreleme

Phishing filtresi, kişisel bilgileri ele geçiren olası phishing (hileli) Web sitelerini tanımlar.

Özelleştirilmiş spam ileti işleme

İstenmeyen e-postaları spam olarak işaretleyip McAfee Anti-Spam klasörünüze taşıyın veya yasal e-postaları spam değil olarak işaretleyip Gelen Kutusu'na taşıyın.

Arkadaşlar

Arkadaşlarınızdan gelen e-postaların filtrelenmemesi için e-posta adreslerini arkadaş listesine alın.

Liste öğelerini konuyla ilgisine göre sıralama

Kişisel filtrelerinizi, arkadaşlarınızı, adres defterlerinizi ve Web posta hesaplarınızı konuyla ilgisine göre sıralayabilirsiniz (uygun sütun adını tıklatmanız yeterlidir).

Ek destek

Anti-Spam Mozilla® Thunderbird™ 1.5 ve 2.0'yi destekler ve Windows Mail için Windows Vista™ 64 bit desteği sağlar. Ayrıca yeni oyun modu özelliği, siz video oyunları oynarken veya DVD izlerken bilgisayarınızın yavaşlamaması için Anti-Spam'in arka plan işlemlerini durdurur. Anti-Spam, SSL (Güvenli Yuva Katmanı) portları dahil tüm portlarda Microsoft® Outlook®, Outlook Express veya Windows Mail hesaplarını da filtreler.

B Ö L Ü M 2 4

Web posta hesaplarınızı ayarlama

E-posta iletilerinizi okumak için tarayıcı kullanıyorsanız, hesabınıza bağlanması ve iletilerinizi filtrelemesi için Anti-Spam'i yapılandırmanız gerekir. Web posta hesabınızı Anti-Spam'e eklemek için e-posta sağlayıcınız tarafından verilen hesap bilgilerini eklemeniz yeterlidir.

Web posta hesabını ekledikten sonra, hesap bilgilerinizi düzenleyebilir ve filtrelenen Web postası hakkında ayrıntılı bilgi alabilirsiniz. Artık Web posta hesabı kullanmıyorsanız veya hesabın filtrelenmesini istemiyorsanız, bunu kaldırabilirsiniz.

Anti-Spam; POP3, POP3 Web postası, Yahoo®, MSN/Hotmail, Windows Live Mail ve MAPI hesapları gibi çeşitli e-posta programlarıyla çalışır. POP3, en yaygın hesap türüdür ve Internet e-postasında standarttır. POP3 hesabınız varsa, Anti-Spam doğrudan e-posta sunucusuna bağlanır ve iletileri e-posta programınız tarafından alınmadan önce filtreler. POP3 Web postası, Yahoo, MSN/Hotmail ve Windows Mail hesapları Web tabanlıdır. POP3 Web posta hesaplarını filtrelemek, POP3 hesaplarını filtrelemeye benzer. MAPI; Internet e-postası, faks ve Exchange Server iletileri dahil çok çeşitli ileti türlerini destekleyen ve Microsoft tarafından tasarlanmış olan bir sistemdir. Şu anda yalnızca Microsoft Outlook doğrudan MAPI hesaplarıyla çalışabilmektedir.

Not: Anti-Spam MAPI hesaplarına erişebilir ancak iletilerinizi Microsoft Outlook ile almadığınız sürece e-postanızı filtrelemez.

Bu bölümde

Web posta hesabı ekleme	123
Web posta hesabını düzenleme	124
Web posta hesabını kaldırma	125
Web posta hesabı bilgilerini anlama	125

Web posta hesabı ekleme

Hesabınızdaki iletilere spam filtresi uygulamak istiyorsanız, bir POP3 (örneğin Yahoo), MSN/Hotmail veya Windows Mail (yalnızca ücretli sürümler tam olarak desteklenir) Web posta hesabı ekleyin.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.
- 2 Spam'den Korunma bölümünde **Web Posta Hesapları**'nı tıklayın.
- 3 Web Posta Hesapları bölümünde **Ekle**'yi tıklayın.
- 4 Hesap bilgileri (sayfa 125)'ni belirtin ve sonra **İleri**'yi tıklayın.
- 5 **Denetleme Seçenekleri** altında Anti-Spam'in hesabınızda spam denetleyeceği zamanı (sayfa 125) belirtin.
- 6 Çevirmeli bağlantı kullanıyorsanız, Anti-Spam'in Internet'e nasıl bağlanacağını (sayfa 125) belirtin.
- 7 **Son**'u tıklayın.

Web posta hesabını düzenleme

Hesabınızda değişiklikler olduğu zaman Web posta hesabınızı düzenlemeniz gerekir. Örneğin, parolanızı değiştirirseniz veya Anti-Spam'in daha sık spam denetimi yapmasını isterseniz, Web posta hesabınızı düzenleyin.

- 1 Spam'den Korunma bölümünü açın.
Nasıl?
 1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
 2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
 3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.
- 2 Spam'den Korunma bölümünde **Web Posta Hesapları**'nı tıklayın.
- 3 Değiştirmek istediğiniz hesabı seçin ve ardından **Düzenle**'yi tıklayın.
- 4 Hesap bilgileri (sayfa 125)'ni belirtin ve sonra **İleri**'yi tıklayın.
- 5 **Denetleme Seçenekleri** altında Anti-Spam'in hesabınızda spam denetleyeceği zamanı (sayfa 125) belirtin.
- 6 Çevirmeli bağlantı kullanıyorsanız, Anti-Spam'in Internet'e nasıl bağlanacağını (sayfa 125) belirtin.
- 7 **Son**'u tıklayın.

Web posta hesabını kaldırma

Artık e-postalarınıza spam filtresi uygulamak istemediğiniz Web posta hesabını kaldırın. Örneğin, hesabınız artık etkin değilse veya sorun yaşıyorsanız, sorunu giderirken hesabı kaldırabilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Web Posta Hesapları**'nı tıklatın.

3 Kaldırmak istediğiniz hesabı seçin ve ardından **Kaldır**'ı tıklatın.

Web posta hesabı bilgilerini anlama

Aşağıdaki tabloda, Web posta hesabı eklerken veya düzenlerken belirtmeniz gereken bilgiler açıklanmaktadır.

Hesap bilgisi

Bilgi	Açıklama
Açıklama	Kendiniz başvurmak üzere hesaba açıklama ekleyin. Bu kutuya her türde bilgiyi yazabilirsiniz.
E-posta Adresi	Bu e-posta hesabıyla ilişkili e-posta adresini belirtin.
Hesap Türü	Eklemekte olduğunuz e-posta hesabının türünü belirtin. (Örneğin, POP3 Web postası veya MSN/Hotmail).
Sunucu	Bu hesabı barındıran posta sunucusunun adını belirtin. Sunucunuzun adını bilmiyorsanız, Internet Servis Sağlayıcınız (ISS) tarafından verilen bilgilere bakın.
Kullanıcı Adı	Bu e-posta hesabının kullanıcı adını belirtin. Örneğin, e-posta adresiniz <i>kullanıcıadı@hotmail.com</i> ise, kullanıcı adınız büyük olasılıkla <i>kullanıcıadı</i> 'dir.
Parola	Bu e-posta hesabının parolasını belirtin.
Parolayı Onayla	Bu e-posta hesabının parolasını doğrulayın.

Denetleme seçenekleri

Seenek	Aıklama
Her	Anti-Spam, belirttiėiniz sıklıkta (dakika) bu hesapta spam denetler. Aralık 5-3600 dakika arasında olmalıdır.
Başlangıta denetle	Anti-Spam, bilgisayarını her başlattığınızda bu hesabı denetler.

Baėlantı seçenekleri

Seenek	Aıklama
Asla baėlantı numarası evirme	Anti-Spam sizin iin otomatik olarak baėlantı numarası evirmez. evirmeli baėlantınızı el ile başlatmanız gerekir.
Baėlantı yoksa baėlantı numarası evir	İnternet baėlantısı yoksa, Anti-Spam sizin belirttiėiniz evirmeli baėlantıyı kullanarak baėlanmaya alışır.
Her zaman belirtilen baėlantıyı evir	Anti-Spam, sizin belirttiėiniz evirmeli baėlantıyı kullanarak baėlanmaya alışır. Belirtiėiniz evirmeli baėlantıdan farklı bir baėlantıyla baėlı olduėunuzda, baėlantınız kesilir.
Bu baėlantıyı evir	Anti-Spam'ın İnternet'e baėlanmak iin kullandıėı evirmeli baėlantıyı belirtin.
Filtreleme tamamlandıktan sonra baėlı kal	Filtreleme tamamlandıktan sonra, bilgisayarınız İnternet'e baėlı kalır.

B Ö L Ü M 2 5

Arkadaşları ayarlama

Anti-Spam'in arkadaşlarınızdan gelen yasal e-posta iletilerini filtrelemediğinden emin olmak için arkadaşlarınızın adreslerini Anti-Spam'in arkadaş listesine ekleyebilirsiniz.

Arkadaş listenizi güncelleştirmenin en kolay yolu, adres defterlerinizi Anti-Spam'e eklemektir; böylece, tüm arkadaşlarınızın e-posta adresleri alınır. Bir adres defterini ekledikten sonra, arkadaş listenizin güncelliğini yitirmesini önlemek için defterin içerikleri zamanlanan aralıklarla (günlük, haftalık veya aylık) otomatik olarak alınır.

Anti-Spam'in arkadaş listesini el ile de güncelleştirebilirsiniz veya etki alanı üzerindeki tüm kullanıcıların arkadaş listenize eklenmesini istiyorsanız tüm etki alanını ekleyebilirsiniz. Örneğin, şirket.com etki alanını eklerseniz, bu kuruluştan gelen hiçbir e-posta filtrelenmez.

Bu bölümde

Arkadaşları otomatik olarak ayarlama	128
Arkadaşları el ile ayarlama	130

Arkadaşları otomatik olarak ayarlama

Adres defterlerinizi Anti-Spam'e ekleyerek, arkadaş listenizi otomatik olarak güncelleştirirsiniz. Adres defteri eklemek, Anti-Spam'in ilişkili e-posta adreslerini almasına ve arkadaş listesini bunlarla doldurmasına olanak verir.

Adres defterini ekledikten sonra, içeriklerinin arkadaş listenize alınma sıklığını değiştirebilirsiniz. Ayrıca, artık içeriklerini almak istemediğiniz adres defterini kaldırabilirsiniz.

Adres defteri ekleme

Anti-Spam'in tüm e-posta adreslerinizi otomatik olarak alabilmesi ve arkadaş listenizi güncelleştirmesi için adres defterlerinizi ekleyin. Bu işlem, arkadaş listenizin her zaman güncel kalmasını sağlar.

- 1 Spam'den Korunma bölümünü açın.
Nasıl?
 1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
 2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
 3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.
- 2 Spam'den Korunma bölümünde **Adres Defterleri**'ni tıklayın.
- 3 Adres Defterleri bölümünde **Ekle**'yi tıklayın.
- 4 Almak istediğiniz adres defteri türünü, **Türü** listesinde tıklayın.
- 5 **Kaynak** listesi doluysa, adres defteri kaynağını seçin. Örneğin Outlook adres defterleriniz varsa, bu listeden Outlook'u seçmeniz gerekir.
- 6 Anti-Spam'in adres defterinizde yeni adresleri denetleyeceği zamanı belirlemek için **Zamanla** listesinde **Günlük**, **Haftalık** veya **Aylık** seçeneğini tıklayın.
- 7 **Tamam**'ı tıklayın.

Adres defterini düzenleme

Adres defterleri ekledikten sonra, bunların alma bilgilerini ve zamanlamasını değiştirebilirsiniz. Örneğin, Anti-Spam'in yeni adresleri daha sık denetlemesini isterseniz, adres defterlerinizi düzenleyin.

- 1 Spam'den Korunma bölümünü açın.
Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.
- 2 Spam'den Korunma bölümünde **Adres Defterleri**'ni tıklatın.
- 3 Düzenlemek istediğiniz adres defterini seçin ve ardından **Düzenle**'yi tıklatın.
- 4 Almak istediğiniz adres defteri türünü, **Türü** listesinde tıklatın.
- 5 **Kaynak** listesi doluysa, adres defteri kaynağını seçin. Örneğin Outlook adres defterleriniz varsa, bu listeden Outlook'u seçmeniz gerekir.
- 6 Anti-Spam'in adres defterinizde yeni adresleri denetleyeceği zamanı belirlemek için **Zamanla** listesinde **Günlük**, **Haftalık** veya **Aylık** seçeneğini tıklatın.
- 7 **Tamam**'ı tıklatın.

Adres defterini kaldırma

Anti-Spam'in artık adresleri içinden otomatik olarak almasını istemediğiniz adres defterini kaldırın (örneğin adres defteri güncelliğini yitirmişse ve bunu artık kullanmak istemiyorsanız).

- 1 Spam'den Korunma bölümünü açın.
Nasıl?
 1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
 2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
 3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.
- 2 Spam'den Korunma bölümünde **Adres Defterleri**'ni tıklatın.
- 3 Kaldırmak istediğiniz adres defterini seçin ve ardından **Kaldır**'ı tıklatın.

Arkadaşları el ile ayarlama

Girişleri tek tek düzenleyerek arkadaş listenizi el ile güncelleyebilirsiniz. Örneğin, adresi adres defterinizde olmayan bir arkadaşınızdan e-posta alırsanız, e-posta adresini hemen el ile ekleyebilirsiniz. Bunu yapmanın en kolay yolu, Anti-Spam araç çubuğunu kullanmaktır. Anti-Spam araç çubuğunu kullanmazsanız, arkadaşınızın bilgilerini belirtmeniz gerekir.

Anti-Spam araç çubuğundan arkadaş ekleme

Outlook, Outlook Express, Windows Mail, Eudora™ veya Thunderbird e-posta programlarını kullanıyorsanız, doğrudan Anti-Spam araç çubuğunu kullanarak arkadaşlarınızı ekleyebilirsiniz.

Bu programa arkadaş eklemek için...	Bir iletiyi seçin ve sonra...
Outlook, Outlook Express, Windows Mail	Arkadaş Ekle 'yi tıklatın.
Eudora, Thunderbird	Anti-Spam menüsünde Arkadaş Ekle 'yi tıklatın.

Arkadaşınızı el ile ekleme

Arkadaşınızı doğrudan araç çubuğundan eklemek istemiyorsanız veya e-posta iletisini aldığınızda bunu yapmayı unuttuysanız, Anti-Spam'in adres defterinizi otomatik olarak almasını beklemek zorunda kalmadan, arkadaşınızı arkadaş listesine ekleyebilirsiniz.

- 1 Spam'den Korunma bölmesini açın.
Nasıl?
 1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
 2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
 3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.
- 2 Spam'den Korunma bölümünde **Arkadaşlar**'ı tıklatın.
- 3 Arkadaşlar bölümünde **Ekle**'yi tıklatın.
- 4 **Ad** kutusuna arkadaşınızın adını yazın.
- 5 **Tür** listesinde **Tek e-posta adresi**'ni seçin.
- 6 Arkadaşınızın e-posta adresini **E-posta Adresi** kutusuna yazın.
- 7 **Tamam**'i tıklatın.

Etki alanı ekleme

Bir etki alanı üzerindeki tüm kullanıcıları arkadaş listenize eklemek istiyorsanız tüm etki alanını ekleyin. Örneğin, şirket.com etki alanını eklerseniz, bu kuruluştan gelen hiçbir e-posta filtrelenmez.

- 1 Spam'den Korunma bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.
- 2 Spam'den Korunma bölümünde **Arkadaşlar**'ı tıklayın.
- 3 Arkadaşlar bölümünde **Ekle**'yi tıklayın.
- 4 **Ad** kutusuna kuruluşun veya grubun adını yazın.
- 5 **Tür** listesinde **Tüm etki alanı**'nı seçin.
- 6 Etki alanı adını **E-posta Adresi** kutusuna yazın.
- 7 **Tamam**'i tıklayın.

Arkadaşınızı düzenleme

Bir arkadaşınızın bilgileri değişirse, Anti-Spam'in ondan gelen iletileri spam olarak işaretlememesi için arkadaş listenizi güncelleştirebilirsiniz.

- 1 Spam'den Korunma bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.
- 2 Spam'den Korunma bölümünde **Arkadaşlar**'ı tıklayın.
- 3 Düzenlemek istediğiniz arkadaşınızı seçin ve ardından **Düzenle**'yi tıklayın.
- 4 **Ad** kutusunda arkadaşınızın adını değiştirin.
- 5 Arkadaşınızın e-posta adresini **E-posta Adresi** kutusunda değiştirin.
- 6 **Tamam**'i tıklayın.

Etki alanını düzenleme

Bir etki alanının bilgileri değişirse, Anti-Spam'in bu etki alanından gelen iletileri spam olarak işaretlememesi için arkadaş listenizi güncelleştirebilirsiniz.

1 Spam'den Korunma bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.

2 Spam'den Korunma bölümünde **Arkadaşlar**'ı tıklayın.

3 Arkadaşlar bölümünde **Ekle**'yi tıklayın.

4 **Ad** kutusunda kuruluşun veya grubun adını değiştirin.

5 **Tür** listesinde **Tüm etki alanı**'nı seçin.

6 Etki alanı adını **E-posta Adresi** kutusunda değiştirin.

7 **Tamam**'ı tıklayın.

Arkadaşınızı kaldırma

Arkadaş listenizdeki bir kişi veya etki alanı size spam gönderirse, bunu Anti-Spam'in arkadaş listesinden kaldırarak, buradan gelen e-posta iletilerinin yeniden filtrelenmesini sağlayın.

1 Spam'den Korunma bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.

2 Spam'den Korunma bölümünde **Arkadaşlar**'ı tıklayın.

3 Kaldırmak istediğiniz arkadaşınızı seçin ve ardından **Kaldır**'ı tıklayın.

B Ö L Ü M 2 6

Spam algılamayı yapılandırma

Anti-Spam, spam iletilerin algılanma biçimini özelleştirmenize olanak verir. İletileri daha kararlı bir şekilde filtreleyebilir, ileti içinde nelerin aranacağını belirtebilir ve spam'i analiz ederken özel karakter kümeleri arayabilirsiniz. Ayrıca, Anti-Spam'in hangi iletileri spam olarak tanımlayacağını ayarlamak için kişisel filtreler oluşturabilirsiniz. Örneğin, ipotek sözcüğünü içeren istenmeyen e-posta filtrelenmiyorsa, ipotek sözcüğünü içeren bir filtre ekleyebilirsiniz.

E-postanızla ilgili sorunlar yaşıyorsanız, sorun giderme stratejiniz kapsamında spam korumasını devre dışı bırakabilirsiniz.

Bu bölümde

Spam korumasını devre dışı bırakma.....	133
Filtreleme seçeneklerini ayarlama	134
Kişisel filtreleri kullanma	137

Spam korumasını devre dışı bırakma

Anti-Spam'in e-postaları filtrelemesini önlemek için spam korumasını devre dışı bırakabilirsiniz.

- 1 Gelişmiş Menü'de **Yapılandır**'ı tıklatın.
- 2 Yapılandır bölmesinde **E-posta ve Anlık İleti**'yi tıklatın.
- 3 **Spam'den korunma** bölümünde **Kapalı**'yı tıklatın.

İpucu: Spam'den korunmak için **Spam'den korunma** altında **Açık**'ı tıklatmayı unutmayın.

Filtreleme seçeneklerini ayarlama

İletileri daha kararlı bir şekilde filtrelemek, ileti içinde nelerin aranacağını belirtmek ve spam'i analiz ederken özel karakter kümeleri aramak isterseniz, Anti-Spam'in filtreleme seçeneklerini ayarlayın.

Filtreleme düzeyi

Filtreleme düzeyi, e-postanızın ne kadar kararlı bir düzeyde filtreleneceğini belirler. Örneğin, spam filtrelenmezse ve filtreleme düzeyiniz Orta seçeneğine ayarlıysa, bunu Yüksek olarak değiştirebilirsiniz. Ancak, filtreleme düzeyiniz Yüksek olarak ayarlıysa, yalnızca arkadaş listenizdeki göndericilerden gelen e-posta iletileri kabul edilir: Diğer tüm iletiler filtrelenir.

Özel filtreler

Filtre, Anti-Spam'in alınan bir e-postada neleri arayacağını belirtir. Özel filtreler; gizli metin, katıştırılmış görüntüler, amaçlı HTML biçimlendirme hataları ve spam gönderenler tarafından yaygın olarak kullanılan diğer teknikleri içeren e-posta iletilerini algılar. Bu özniteliklere sahip e-posta iletileri genellikle spam olduğu için özel filtreler varsayılan olarak etkindir. Örneğin, katıştırılmış görüntüler içeren e-posta iletilerini almak isterseniz, özel görüntü filtresini devre dışı bırakmanız gerekebilir.

Karakter Kümeleri

Anti-Spam, spam analizi yaparken özel karakter kümelerini arayabilir. Karakter kümeleri; dilin alfabesi, rakamlar ve diğer simgeleri de kapsayan bir dili temsil etmek üzere kullanılır. Yunanca spam alıyorsanız, Yunanca karakter kümesi içeren tüm iletileri filtreleyebilirsiniz.

Yasal e-posta aldığınız dillerin karakter kümelerini filtrelememeye dikkat edin. Örneğin, yalnızca İtalyanca iletileri filtrelemek istiyorsanız, İtalya Batı Avrupa'da olduğu için Batı Avrupa'yı seçebilirsiniz. Ancak İngilizce yasal e-posta alıyorsanız, Batı Avrupa'yı seçtiğinizde, İngilizce iletiler ve Batı Avrupa karakter kümesindeki diğer diller de filtrelenir. Bu durumda, yalnızca İtalyanca iletileri filtreleyemezsiniz.

Not: Belirli bir karakter kümesinden karakterler içeren iletileri filtrelemek, deneyimli kullanıcılara yönelik bir işlemdir.

Filtreleme düzeyini değiştirme

E-postanızı filtrelemek istediğiniz etkinlik düzeyini değiştirebilirsiniz. Örneğin, yasal iletiler filtreleniyorsa, filtreleme düzeyini düşürebilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.
- 2 Spam'den Korunma bölümünde **Filtreleme Seçenekleri**'ni tıklayın.
- 3 **Filtreleme Seçenekleri** altında kaydırma çubuğunu uygun düzeye götürün ve sonra **Tamam**'ı tıklayın.

Düzy	Açıklama
Düşük	Çoğu e-posta kabul edilir.
Orta-Düşük	Yalnızca spam olduğu belli olan iletiler filtrelendir.
Orta	E-posta önerilen düzeyde filtrelendir.
Orta-Yüksek	Spam'e benzeyen tüm e-postalar filtrelendir.
Yüksek	Yalnızca arkadaş listenizdeki gönderenlerden iletiler kabul edilir.

Özel filtreyi devre dışı bırakma

Genellikle spam gönderenler tarafından gönderilen iletileri filtreledikleri için özel filtreler varsayılan olarak etkindir. Örneğin, katıştırılmış görüntüler içeren e-posta iletileri genellikle spam'dir; ancak sık sık katıştırılmış görüntüler içeren yasal e-posta alıyorsanız, özel görüntü filtresini devre dışı bırakın.

- 1 Spam'den Korunma bölümünü açın.
Nasıl?
 1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
 2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
 3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.
- 2 Spam'den Korunma bölümünde **Filtreleme Seçenekleri**'ni tıklayın.
- 3 **Özel Filtreler** altında uygun onay kutularını işaretleyin veya işaretini kaldırın ve sonra **Tamam**'ı tıklayın.

Filtre	Açıklama
Gizli metin içeren iletileri filtrele	Gizli metin içeren iletiler algılanmaktan kaçınan spam gönderenler tarafından sık sık kullanıldığı için gizli metin arar.

Metne göre belirli bir oranda resim içeren iletileri filtrele	Katıştırılmış görüntüler içeren iletiler genellikle spam olduğu için katıştırılmış görüntüleri arar.
Amaçlı HTML biçimlendirme hataları içeren iletileri filtrele	Geçersiz biçimlendirme filtrelerin spam filtrelemesini engellemede kullanıldığı için geçersiz biçimlendirme içeren iletileri arar.
Şundan büyük iletileri filtreleme	Büyük iletiler spam olmayabileceği için belirtilen boyuttan büyük iletileri aramaz. İleti boyutunu artırabilir veya azaltabilirsiniz (geçerli aralık 0-250 KB'dir).

Karakter kümesi filtrelerini uygulama

Not: Belirli bir karakter kümesinden karakterler içeren iletileri filtrelemek, deneyimli kullanıcılara yönelik bir işlemdir.

Belirli dillerin karakter kümelerini filtreleyebilirsiniz; ancak yasal e-posta aldığınız dillerin karakter kümelerini filtrelemeyin.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Karakter Kümeleri**'ni tıklatın.

3 Filtrelemek istediğiniz karakter kümelerinin yanındaki onay kutularını seçin.

4 **Tamam**'ı tıklatın.

Kişisel filtreleri kullanma

Filtre, Anti-Spam'ın alınan bir e-postada neleri arayacağını belirtir. Spam bulunduğunda, ileti spam olarak işaretlenir ve Gelen Kutusu'nda bırakılır veya McAfee Anti-Spam klasörüne taşınır. Spam'in işleme biçimi hakkında ayrıntılı bilgi için bkz. İletinin işleme ve işaretlenme biçimini değiştirme (sayfa 142).

Varsayılan olarak, Anti-Spam çok çeşitli filtreler kullanır; ancak hangi iletilerin Anti-Spam tarafından spam olarak tanımlanacağını ayarlamak için yeni filtreler oluşturabilir veya geçerli filtreleri düzenleyebilirsiniz. Örneğin, ipotek sözcüğünü içeren bir filtre eklerseniz, Anti-Spam ipotek sözcüğünü içeren iletileri filtreler. Yasal e-posta iletilerinde yaygın olarak bulunan sözcükler için filtreler oluşturmayın çünkü bu durumda spam olmayan e-postalar da filtrelendir. Bir filtre oluşturduktan sonra, filtrenin bazı spam iletileri algılamadığını fark ederseniz bunu düzenleyebilirsiniz. Örneğin, iletinin konusunda viagra sözcüğünü arayacak bir filtre oluşturduysanız ancak iletinin gövdesinde geçtiği için viagra sözcüğünü içeren iletileri almaya devam ediyorsanız, filtreyi ileti konusu yerine ileti gövdesinde viagra sözcüğünü arayacak şekilde değiştirin.

Düzenli ifadeler (RegEx) de kişisel filtrelerde kullanılabilen özel karakterler ve sıralardır; ancak McAfee, düzenli ifadelerin yalnızca deneyimli kullanıcılar tarafından kullanılmasını önerir. Düzenli ifadeleri tanıımıyorsanız veya bunların kullanımı hakkında ayrıntılı bilgi almak isterseniz, Web'de düzenli ifadelerle ilgili araştırma yapabilirsiniz (örneğin, http://en.wikipedia.org/wiki/Regular_expression adresine gidin).

Kişisel filtre ekleme

Anti-Spam'ın hangi iletileri spam olarak tanımlayacağını ayarlamak için filtreler ekleyebilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölmesinde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Kişisel Filtreler**'i tıklatın.

3 Ekle'yi tıklatın.

4 E-posta iletisinde kişisel filtrenin neyi arayacağını belirtin (sayfa 138).

5 Tamam'ı tıklatın.

Kişisel filtreyi düzenleme

Hangi iletilerin spam olarak tanımlanacağını ayarlamak için mevcut filtreleri düzenleyin.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.

2 Spam'den Korunma bölümünde **Kişisel Filtreler**'i tıklayın.

3 Düzenlemek istediğiniz filtreyi seçin ve ardından **Düzenle**'yi tıklayın.

4 E-posta iletilerinde kişisel filtrenin neyi arayacağını belirtin (sayfa 138).

5 **Tamam**'i tıklayın.

Kişisel filtreyi kaldırma

Artık kullanmak istemediğiniz filtreleri kalıcı olarak kaldırabilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.

2 Spam'den Korunma bölümünde **Kişisel Filtreler**'i tıklayın.

3 Kaldırmak istediğiniz filtreyi seçin ve ardından **Kaldır**'ı tıklayın.

4 **Tamam**'i tıklayın.

Kişisel filtreyi belirtme

Aşağıdaki tabloda, e-posta iletilerinde kişisel filtrenin neyi arayacağı açıklanmaktadır.

Bilgi	Açıklama
Öge	Filtrenin sözcükleri veya tümcecikleri ileti konusu, gövde, başlıklar veya ileti gönderen seçeneklerinde arayıp aramayacağını belirlemek için bir girişi tıklayın.
Koşul	Filtrenin belirlediğiniz sözcükleri veya tümcecikleri içeren ya da içermeyen bir iletiyi arayıp aramayacağını belirlemek için bir girişi tıklayın.

Sözcük veya tümcecik	İletide neyin aranacağını yazın. Örneğin ipotek sözcüğünü belirtirseniz, bu sözcüğü içeren tüm iletiler filtrelenir.
Bu filtre normal ifadeleri kullanır (RegEx)	Filtre koşullarında kullanılan karakter desenlerini belirtin. Bir karakter desenini test etmek için Test 'i tıklayın.

B Ö L Ü M 2 7

E-posta filtreleme

Anti-Spam gelen e-postanızı inceler ve bunu spam (sizden bir şey satın almanızı isteyen e-postalar) veya phishing (olası bir hileli Web sitesine kişisel bilgi sağlamanızı isteyen e-postalar) olarak sınıflandırır. Varsayılan olarak, Anti-Spam daha sonra tüm istenmeyen e-posta iletilerini spam veya phishing (iletinin konu satırında [SPAM] veya [PHISH] etiketi görüntülenir) olarak işaretler ve iletileri McAfee Anti-Spam klasörüne taşır.

Anti-Spam'in e-posta iletilerinizi filtreleme biçimini özelleştirmek için Anti-Spam araç çubuğundan e-postayı spam olarak veya spam değil olarak işaretleyebilir, spam iletilerin taşındığı konumu değiştirebilir ve konu satırında görüntülenen etiketi değiştirebilirsiniz.

Spam'in işleme ve işaretleme biçimini değiştirmek için spam ve phishing e-posta iletilerinin taşındığı konumu ve konu satırında görüntülenen etiketin adını özelleştirebilirsiniz.

E-posta programınızla ilgili sorunlar yaşarsanız, sorun giderme stratejiniz kapsamında Anti-Spam araç çubuklarını da devre dışı bırakabilirsiniz.

Bu bölümde

Anti-Spam araç çubuğundan bir iletiyi işaretleme..... 141
İletin işleme ve işaretleme biçimini değiştirme 142
Anti-Spam araç çubuğunu devre dışı bırakma 142

Anti-Spam araç çubuğundan bir iletiyi işaretleme

Bir iletiyi spam olarak işaretlediğinizde, iletinin konusuna [SPAM] etiketi veya sizin seçtiğiniz bir etiket eklenir ve Gelen Kutusu'nda, McAfee Anti-Spam klasörünüzde (Outlook, Outlook Express, Windows Mail, Thunderbird) veya Önemsiz Posta klasörünüzde (Eudora®) bırakılır. Bir iletiyi spam değil olarak işaretlediğinizde, ileti etiketi kaldırılır ve ileti Gelen Kutusu'na taşınır.

Bu programda bir iletiyi işaretleme için...	Bir iletiyi seçin ve sonra...
Outlook, Outlook Express, Windows Mail	Spam Olarak İşaretle 'yi veya Spam Değil Olarak İşaretle 'yi tıklatın.
Eudora, Thunderbird	Anti-Spam menüsünde Spam Olarak İşaretle 'yi veya Spam Değil Olarak İşaretle 'yi tıklatın.

İletinin işlenme ve işaretlenme biçimini değiştirme

Spam'in işlenme ve işaretlenme biçimini değiştirebilirsiniz. Örneğin, e-posta iletisinin Gelen Kutusu'nda mı yoksa McAfee Anti-Spam klasöründe mi bırakılacağına karar verebilir ve iletinin konu satırında görüntülenen [SPAM] veya [PHISH] etiketini değiştirebilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.

2 Spam'den Korunma bölümünde **İşleme**'yi tıklayın.

3 Uygun onay kutularını işaretleyin veya işaretini kaldırın ve sonra **Tamam**'i tıklayın.

Seçenek	Açıklama
Spam olarak işaretle ve McAfee Anti-Spam klasörüne taşı	Bu varsayılan ayardır. Spam iletiler McAfee Anti-Spam klasörünüze taşınır.
Spam olarak işaretle ve Gelen Kutusu'nda bırak	Spam iletiler Gelen Kutusu'nda bırakılır.
Bu özelleştirilebilir etiketi spam iletilerin konusuna ekle	Belirttiğiniz etiket, spam iletilerin e-posta konu satırına eklenir.
Bu özelleştirilebilir etiketi phishing iletilerinin konusuna ekle	Belirttiğiniz etiket, phishing iletilerin e-posta konu satırına eklenir.

Anti-Spam araç çubuğunu devre dışı bırakma

Outlook, Outlook Express, Windows Mail, Eudora veya Thunderbird kullanıyorsanız, Anti-Spam araç çubuğunu devre dışı bırakabilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.
- 2 Spam'den Korunma bölümünde **E-Posta Araç Çubukları**'nı tıklatın.
- 3 Devre dışı bırakmak istediğiniz araç çubuğunun yanındaki onay kutusunu temizleyin.
- 4 **Tamam**'ı tıklatın.

İpucu: İsteddiğiniz zaman onay kutularını işaretleyerek Anti-Spam araç çubuklarınızı yeniden etkinleştirebilirsiniz.

B Ö L Ü M 2 8

Filtrelenen e-posta ile çalışma

Bazen bazı spam iletiler algılanmayabilir. Bu durumda, McAfee'ye spam raporlayabilirsiniz; bunlar filtre güncelleştirmeleri oluşturmak üzere analiz edilir.

Web posta hesabı kullanıyorsanız, filtrelenen e-posta iletilerinizi kopyalayabilir, silebilir ve bunlar hakkında ayrıntılı bilgi alabilirsiniz. Yasal bir iletinin filtreleneip filtrelenmediğinden emin olamıyorsanız veya iletinin ne zaman filtrelendiğini bilmek istiyorsanız bu kullanışlı bir özelliktir.

Bu bölümde

McAfee'ye spam raporlama	145
Filtrelenen Web posta iletilerini kopyalama veya silme	146
Filtrelenen Web postasında olay görüntüleme	146

McAfee'ye spam raporlama

McAfee'ye spam raporlayabilirsiniz; bunlar filtre güncelleştirmeleri oluşturmak üzere analiz edilir.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'i tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **McAfee'ye Raporlama** seçeneğini tıklatın.

3 Uygun onay kutularını işaretleyin ve sonra **Tamam**'i tıklatın.

Seçenek	Açıklama
Spam olarak İşaretle'yi tıklattığınızda raporlamayı etkinleştir	Spam olarak işaretlediğiniz her iletiyi McAfee'ye raporlar.
Spam Değil olarak İşaretle'yi tıklattığınızda raporlamayı etkinleştir	Spam değil olarak işaretlediğiniz her iletiyi McAfee'ye raporlar.

Tüm iletiyi gönder (yalnızca üstbilgileri değil)	McAfee'ye bir ileti raporladığınızda, yalnızca üstbilgileri değil, tüm iletiyi gönderir.
--	--

Filtrelenen Web posta iletisini kopyalama veya silme

Web posta hesabınızda filtrelenen iletileri kopyalayabilir veya silebilirsiniz.

- 1 **Ortak Görevler** altında **Son Olayları Görüntüle**'yi tıklatın.
- 2 Son Olaylar bölümünde **Günlüğü Görüntüle**'yi tıklatın.
- 3 Soldaki bölmede **E-posta ve Anlık İleti** listesini genişletin ve sonra **Web Postası Filtreleme Olayları**'nı tıklatın.
- 4 Bir ileti seçin.
- 5 **Şunu yapmak istiyorum** altında aşağıdakilerden birini gerçekleştirin:
 - İletiyi Pano'ya kopyalamak için **Kopyala**'yı tıklatın.
 - İletiyi silmek için **Sil**'i tıklatın.

Filtrelenen Web postasında olay görüntüleme

E-posta iletilerinin filtrelendiği tarih ve saati ve bunları alan hesabı görüntüleyebilirsiniz.

- 1 **Ortak Görevler** altında **Son Olayları Görüntüle**'yi tıklatın.
- 2 Son Olaylar bölümünde **Günlüğü Görüntüle**'yi tıklatın.
- 3 Soldaki bölmede **E-posta ve Anlık İleti** listesini genişletin ve sonra **Web Postası Filtreleme Olayları**'nı tıklatın.
- 4 Görüntülemek istediğiniz günlüğü seçin.

B Ö L Ü M 2 9

Phishing korumasını yapılandırma

Anti-Spam, istenmeyen e-postaları, spam (sizden bir şey satın almanızı isteyen e-postalar) veya phishing (bilinen veya olası bir hileli Web sitesine kişisel bilgi sağlamanızı isteyen e-postalar) olarak sınıflandırır. Phishing koruması, sizi hileli Web sitelerine erişmekten korur. Bir e-posta iletilirken hileli olduğu bilinen veya olma olasılığı bulunan bir Web sitesinin bağlantısını tıklarızsanız, Anti-Spam sizi Phishing filtresinin güvenli sayfasına yönlendirir.

Filtrelemek istemediğiniz Web siteleri varsa, bunları Phishing beyaz listesine ekleyin. Ayrıca beyaz listedeki Web sitelerini düzenleyebilir ve kaldırabilirsiniz. Google®, Yahoo veya McAfee gibi siteleri eklemenize gerek yoktur çünkü bu Web siteleri hileli olarak değerlendirilmez.

Not: Bilgisayarınızda SiteAdvisor yüklüyse, SiteAdvisor'da Anti-Spam'in phishing korumasına benzer bir koruma olduğu için Anti-Spam'in phishing korumasını almazsınız.

Bu bölümde

Beyaz listeye Web sitesi ekleme	147
Beyaz listenizdeki siteleri düzenleme	148
Beyaz listeden Web sitesini kaldırma	148
Phishing korumasını devre dışı bırakma	148

Beyaz listeye Web sitesi ekleme

Filtrelemek istemediğiniz Web siteleri varsa, bunları beyaz listeye ekleyin.

- 1 Phishing Koruması bölmesini açın.
Nasıl?
 1. SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklatın.
 2. Internet ve Ağ bilgi alanında **Yapılandır**'ı tıklatın.
- 2 Phishing Koruması bölümünde **Gelişmiş**'i tıklatın.
- 3 **Beyaz Liste** altında **Ekle**'yi tıklatın.
- 4 Web sitesinin adresini yazın ve sonra **Tamam**'i tıklatın.

Beyaz listenizdeki siteleri düzenleme

Bir Web sitesini beyaz listeye eklediyseniz ve Web sitesinin adresi değiştiyse, her zaman bunu güncelleştirebilirsiniz.

- 1 Phishing Koruması bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklayın.
2. Internet ve Ağ bilgi alanında **Yapılandır**'ı tıklayın.
- 2 Phishing Koruması bölümünde **Gelişmiş**'i tıklayın.
- 3 **Beyaz Liste** altında güncelleştirmek istediğiniz Web sitesini seçin ve sonra **Düzenle**'yi tıklayın.
- 4 Web sitesinin adresini düzenleyin ve sonra **Tamam**'ı tıklayın.

Beyaz listeden Web sitesini kaldırma

Erişmek istediğiniz bir Web sitesini beyaz listeye eklediyseniz ancak artık siteyi filtrelemek istiyorsanız, bunu beyaz listeden kaldırın.

- 1 Phishing Koruması bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklayın.
2. Internet ve Ağ bilgi alanında **Yapılandır**'ı tıklayın.
- 2 Phishing Koruması bölümünde **Gelişmiş**'i tıklayın.
- 3 **Beyaz Liste** altında kaldırmak istediğiniz Web sitesini seçin ve sonra **Kaldır**'ı tıklayın.

Phishing korumasını devre dışı bırakma

McAfee olmayan bir phishing yazılımınız varsa ve bunlar çakışıyorsa, Anti-Spam phishing korumasını devre dışı bırakabilirsiniz.

- 1 SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklayın.
- 2 Internet ve Ağ bilgi alanında **Yapılandır**'ı tıklayın.
- 3 **Phishing koruması** altında **Kapalı**'yı tıklayın.

İpucu: İşiniz bitince, hileli Web sitelerinden korunmak için **Phishing koruması** altında **Açık**'ı tıklatmayı unutmayın.

B Ö L Ü M 3 0

McAfee Privacy Service

Privacy Service, siz, aileniz, kişisel dosyalarınız ve bilgisayarınız için gelişmiş koruma sunar. Çevrimiçi kimlik hırsızlığından korunmanıza, kişisel bilgilerin iletilmesini engellemenize, olası zararlı çevrimiçi içeriği (görüntüler dahil) filtrelemenize yardımcı olur. Ayrıca, bazı yetkisiz Web'de gezinme alışkanlıklarının yetişkinler tarafından izlenmesine, denetlenmesine ve günlüğe kaydedilmesine olanak veren gelişmiş Ebeveyn Denetimleri'nin yanı sıra, kişisel parolalar için güvenli bir saklama alanı da sağlar.

Privacy Service'i kullanmaya başlamadan önce, en popüler özelliklerden bazıları hakkında bilgi edinebilirsiniz. Bu özelliklerin yapılandırılması ve kullanımıyla ilgili ayrıntılar, Privacy Service yardımında sunulmaktadır.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Privacy Service özellikleri	150
Ebeveyn Denetimleri'ni ayarlama	151
Web'de bilgileri koruma	167
Parolaları koruma	169

Privacy Service özellikleri

Privacy Service aşağıdaki özellikleri sunar:

- Ebeveyn Denetimleri
- Kişisel Bilgilerin Korunması
- Parola Mahzeni

Ebeveyn Denetimleri

Ebeveyn Denetimleri, olası uygunsuz görüntüleri filtrelemenize, içerik derecelendirme gruplarını (kullanıcının görüntüleyebileceği Web sitelerini ve içeriği kısıtlamak için kullanılan yaş grupları) yapılandırmanıza ve Web'de gezinme saat sınırlamalarını (kullanıcının Web'e erişebileceği zaman aralığı ve süre) ayarlamanıza olanak verir. Ebeveyn Denetimleri, belirli Web sitelerine erişimi genel olarak kısıtlamanızı ve ilişkili anahtar sözcüklere göre erişime izin vermenizi veya engellemenizi de sağlar.

Kişisel Bilgilerin Korunması

Kişisel Bilgilerin Korunması, hassas veya gizli bilgilerin (örneğin kredi kartı numaraları, banka hesap numaraları, adresler gibi) Web üzerinden iletilmesini engellemenizi sağlar.

Parola Mahzeni

Parola Mahzeni, kişisel parolalarınız için güvenli bir saklama alanıdır. Parolalarınızı başka hiçbir kullanıcının (hatta Yöneticinin) erişemeyeceği şekilde güvenli olarak saklamanıza olanak verir.

B Ö L Ü M 3 1

Ebeveyn Denetimleri'ni ayarlama

Çocuğunuz bilgisayarınızı kullanıyorsa, onun için Ebeveyn Denetimleri'ni yapılandırabilirsiniz. Çocuklarınızın Web'de gezinirken görebilecekleri ve yapabilecekleri şeyleri düzenlemenize yardımcı olması için Ebeveyn Denetimleri'ni kullanırsınız. Ebeveyn Denetimleri'ni ayarlamak için görüntü filtrelemeyi etkinleştirebilir veya devre dışı bırakabilir, içerik derecelendirme grubu seçebilir ve Web'de gezinme saat sınırlamalarını ayarlayabilirsiniz. Görüntü filtreleme, çocuğunuz Web'de gezinirken olası uygunsuz görüntülerin gösterilmesini engeller; içerik derecelendirme grubu, çocuğunuzun yaş grubuna göre erişebileceği içerik türünü ve Web sitelerini belirler; Web'de gezinme saat sınırlamaları, çocuğunuzun Web'e erişebileceği günleri ve saatleri tanımlar. Ebeveyn Denetimleri, tüm çocuklar için belirli Web sitelerini filtrelemenizi (engellemenizi veya izin vermenizi) de sağlar.

Not: Ebeveyn Denetimleri'ni ayarlamak için Yönetici olmanız gerekir.

Bu bölümde

Kullanıcıları yapılandırma	152
Olası uygunsuz Web resimlerini filtreleme.....	157
içerik derecelendirme grubunu ayarlama.....	158
Web'de gezinme saat sınırlarını ayarlama	160
Filtrelenen Web siteleri	161
Anahtar sözcükler kullanarak Web sitelerini filtreleme	164

Kullanıcıları yapılandırma

Ebeveyn Denetimleri'ni yapılandırmak için SecurityCenter kullanıcılarına izinler atarsınız. Varsayılan olarak, SecurityCenter kullanıcıları, bilgisayarınızda ayarladığınız Windows kullanıcılarına karşılık gelir. Ancak McAfee kullanıcılarını kullanan önceki bir SecurityCenter sürümünden yükseltme yaptıysanız, McAfee kullanıcılarınız ve izinleri geçerlidir.

Not: Kullanıcıları yapılandırmak için SecurityCenter'da yönetici oturumu aşmanız gerekir.

Windows kullanıcılarıyla çalışma

Ebeveyn Denetimleri'ni yapılandırmak için her bir kullanıcının Internet'te neler görebileceğini ve yapabileceğini belirleyen kullanıcı izinleri atamanız gerekir. Varsayılan olarak, SecurityCenter kullanıcıları, bilgisayarınızda ayarladığınız Windows kullanıcılarına karşılık gelir. Windows'da Bilgisayar Yönetimi altında kullanıcı ekleyebilir, bir kullanıcının hesap bilgilerini düzenleyebilir ve kullanıcı kaldırabilirsiniz. Daha sonra SecurityCenter'da bu kullanıcılar için Ebeveyn Denetimleri ayarlarsınız.

Ancak McAfee kullanıcılarını kullanan önceki bir SecurityCenter sürümünden yükseltme yaptıysanız bkz. McAfee kullanıcılarıyla çalışma (sayfa 154).

McAfee kullanıcılarıyla çalışma

McAfee kullanıcılarını kullanan önceki bir SecurityCenter sürümünden yükseltme yaptıysanız, McAfee kullanıcılarınız ve izinleri otomatik olarak geçerlidir. McAfee kullanıcılarını yapılandırmaya ve yönetmeye devam edebilirsiniz; ancak işlemi kolaylaştırmak için McAfee, Windows kullanıcılarına geçmenizi önerir. Windows kullanıcılarına geçtikten sonra, hiçbir zaman yeniden McAfee kullanıcılarına dönemezsiniz.

McAfee kullanıcılarını kullanmaya devam ederseniz, kullanıcı ekleyebilir, düzenleyebilir veya kaldırabilir ve McAfee yönetici parolasını değiştirebilir veya alabilirsiniz.

Windows kullanıcılarına geçme

İşlem kolaylığı için McAfee Windows kullanıcılarına geçmenizi önerir. Windows kullanıcılarına geçtikten sonra, hiçbir zaman yeniden McAfee kullanıcılarına dönemezsiniz.

1 Kullanıcı Ayarları bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklayın.
2. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklayın.
3. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklayın.
4. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklayın.

2 Kullanıcı Ayarları bölümünde **Değiştir**'i tıklayın.

3 İşlemi onaylayın.

McAfee kullanıcısı ekleme

McAfee kullanıcısı oluşturduktan sonra, bu kullanıcı için Ebeveyn Denetimleri'ni yapılandırabilirsiniz. Ayrıntılı bilgi için Privacy Service yardımına bakın.

1 SecurityCenter'da Yönetici olarak oturum açın.

2 Kullanıcı Ayarları bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
3. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
4. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
- 3 Kullanıcı Ayarları bölümünde **Ekle**'yi tıklatın.
- 4 Kullanıcı adı, parola, hesap türü ve ebeveyn denetimlerini ayarlamak için ekran yönergelerini izleyin.
- 5 **Oluştur**'u tıklatın.

[Bir McAfee kullanıcısının hesap bilgilerini düzenleme](#)

Bir McAfee kullanıcısının parolasını, hesap türünü veya otomatik oturum açma özelliğini değiştirebilirsiniz.

- 1 SecurityCenter'da Yönetici olarak oturum açın.
- 2 Kullanıcı Ayarları bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
3. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
4. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
- 3 Kullanıcı Ayarları bölümünde bir kullanıcı adını tıklatın ve sonra **Düzenle**'yi tıklatın.
- 4 Kullanıcının parolasını, hesap türünü veya ebeveyn denetimlerini düzenlemek için ekran yönergelerini izleyin.
- 5 **Tamam**'ı tıklatın.

[Bir McAfee kullanıcısını kaldırma](#)

İstediğiniz zaman bir McAfee kullanıcısını kaldırabilirsiniz.

McAfee kullanıcısını kaldırmak için:

- 1 SecurityCenter'da Yönetici olarak oturum açın.
- 2 Kullanıcı Ayarları bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
 3. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
 4. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
- 3 Kullanıcı Ayarları bölümünde, **McAfee Kullanıcı Hesapları** altında bir kullanıcı adı seçin ve sonra **Kaldır**'ı tıklatın.

[McAfee yönetici parolasını değiştirme](#)

McAfee yönetici parolasını anımsamakta zorlanıyor veya parolanın ele geçirildiğinden şüpheleniyorsanız, onu değiştirebilirsiniz.

- 1 SecurityCenter'da Yönetici olarak oturum açın.
- 2 Kullanıcı Ayarları bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
 3. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
 4. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
- 3 Kullanıcı Ayarları bölümünde, **McAfee Kullanıcı Hesapları** altında **Yönetici**'yi seçin ve sonra **Düzenle**'yi tıklatın.
- 4 Kullanıcı Hesabını Düzenle iletişim kutusunda, **Yeni Parola** kutusuna yeni parolanızı yazın ve sonra **Parolayı Yeniden Girin** kutusuna parolanızı yeniden yazın.
- 5 **Tamam**'i tıklatın.

[McAfee yönetici parolasını alma](#)

Yönetici parolasını unutursanız, bunu alabilirsiniz.

- 1 SecurityCenter simgesini  sağ tıklatın ve sonra **Kullanıcı Değiştir**'i tıklatın.
- 2 **Kullanıcı Adı** listesinde **Yönetici**'yi seçin ve sonra **Parolayı mı Unuttunuz?**'u tıklatın.
- 3 **Yanıt** kutusuna gizli sorunuzun yanıtını yazın.
- 4 **Gönder**'i tıklatın.

Olası uygunsuz Web resimlerini filtreleme

Kullanıcının yaşına ve olgunluk düzeyine göre, kullanıcı Web'de gezinirken olası uygunsuz resimleri filtreleyebilirsiniz (engelleyebilir veya izin verebilirsiniz). Örneğin, küçük çocuğunuz Web'de gezinirken olası uygunsuz resimlerin görüntülenmesini engelleyebilir, ancak bunların evinizdeki gençler ve yetişkinler için görüntülenmesine izin verebilirsiniz. Varsayılan olarak, resim filtreleme özelliği Yetişkin grubunun tüm üyeleri için devre dışıdır; bu kullanıcılar Web'de gezinirken olası uygunsuz resimleri görebilirler. Kullanıcının yaş grubunu ayarlama hakkında ayrıntılı bilgi için bkz. İçerik derecelendirme grubunu ayarlama (sayfa 158).

Olası uygunsuz Web resimlerini filtreleme

Varsayılan olarak, yeni kullanıcılar Yetişkin grubuna eklenir ve görüntü filtreleme devre dışı bırakılır. Belirli bir kullanıcı Web'de gezinirken olası uygunsuz resimlerin görüntülenmesini engellemek isterseniz, görüntü filtrelemeyi etkinleştirebilirsiniz. Olası uygunsuz Web resimlerinin yerine otomatik olarak sabit bir McAfee görüntüsü gösterilir.

1 Kullanıcı Ayarları bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
4. Ebeveyn Denetimleri bölümünde **Kullanıcı Ayarları**'nı tıklatın.

2 Kullanıcı Ayarları bölümünde bir kullanıcı adını tıklatın ve sonra **Düzenle**'yi tıklatın.

3 Kullanıcı Hesabını Düzenle penceresinde, **Görüntü Filtreleme** altında **Açık**'i tıklatın.

4 **Tamam**'i tıklatın.

İçerik derecelendirme grubunu ayarlama

Kullanıcı aşağıdaki içerik derecelendirme gruplarından birine ait olabilir:

- Küçük çocuk
- Çocuk
- Büyük çocuk
- Genç
- Yetişkin

Privacy Service, kullanıcının ait olduğu gruba göre Web içeriğini derecelendirir (engeller veya izin verir). Bu, evinizdeki bazı kullanıcılar için belirli Web sitelerini engellemeyi veya izin vermenizi sağlar. Örneğin, bir Web sitesini Küçük çocuk grubundan kullanıcılar için engelleyebilir, ancak Genç grubundan kullanıcılar için bu siteye izin verebilirsiniz. Bir kullanıcı için içeriği daha kısıtlı şekilde derecelendirmek isterseniz, kullanıcının yalnızca **Filtrelenen Web Siteleri** listesinde izin verilen Web sitelerini görüntülemesine izin verebilirsiniz. Ayrıntılı bilgi için bkz. Web sitelerini filtreleme (sayfa 161).

Varsayılan olarak, yeni bir kullanıcı Yetişkin grubuna eklenir ve bu kullanıcının tüm Web içeriğine erişmesine izin verilir.

Kullanıcının içerik derecelendirme grubunu ayarlama

Varsayılan olarak, yeni bir kullanıcı Yetişkin grubuna eklenir ve bu kullanıcının tüm Web içeriğine erişmesine izin verilir. Daha sonra yaşına ve olgunluk düzeyine göre kullanıcının içerik derecelendirme grubunu ayarlayabilirsiniz.

1 Kullanıcı Ayarları bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklayın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklayın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklayın.
4. Ebeveyn Denetimleri bölümünde **Kullanıcı Ayarları**'ni tıklayın.

2 Kullanıcı Ayarları bölümünde bir kullanıcı adını tıklayın ve sonra **Düzenle**'yi tıklayın.

3 Kullanıcı Hesabını Düzenle penceresinde, **İçerik Derecelendirmesi** altında kullanıcıya atamak istediğiniz yaş grubunu tıklayın.

Kullanıcının **Filtrelenen Verilen Web Siteleri** listesinde engellenen Web sitelerine girmesini önlemek için **Bu kullanıcı**

yalnızca Filtrelenen Web Siteleri listesindeki sitelere erişebilir onay kutusunu işaretleyin.

4 **Tamam'ı** tıklatın.

Web'de gezinme saat sınırlarını ayarlama

Sorumsuz veya aşırı Internet kullanımı hakkında endişeleriniz varsa, çocuğunuzun Web'de gezinmesi için uygun saat sınırlamaları ayarlayabilirsiniz. Çocuğunuzun Web'de gezinmesini belirli saatlerle kısıtladığınızda, siz evde olmasanız bile SecurityCenter'ın bu kısıtlamaları uygulayacağından emin olabilirsiniz.

Varsayılan olarak, çocukların haftada yedi gün, gece ve gündüz her saat Web'de gezinmelerine izin verilir; ancak Web'de gezinmeyi belirli saatlerle veya günlerle sınırlayabilir ya da Web'de gezinmeyi tamamen yasaklayabilirsiniz. Bir çocuk yasaklanan zamanda Web'de gezinmeye çalışırsa, McAfee çocuğa bunu yapamayacağını bildirir. Web'de gezinmeyi tamamen yasaklarsanız, çocuk oturum açıp bilgisayar ve e-posta, anlık ileti programları, ftp, oyunlar gibi diğer Internet programlarını kullanabilir ancak Web'de gezinemez.

Web'de gezinme saat sınırlarını ayarlama

Çocuğunuzun Web'de gezinmesini belirli günler ve saatlerle kısıtlamak için Web'de gezinme saat sınırlamaları kılavuzunu kullanabilirsiniz.

1 Kullanıcı Ayarları bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklayın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklayın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklayın.
4. Ebeveyn Denetimleri bölümünde **Kullanıcı Ayarları**'nı tıklayın.

2 Kullanıcı Ayarları bölümünde bir kullanıcı adını tıklayın ve sonra **Düzenle**'yi tıklayın.

3 Kullanıcı Hesabını Düzenle penceresinde, **Internet Zaman Sınırları** altında fareni sürükleyerek bu kullanıcının Web'de gezinemeyeceği günleri ve saatleri belirtin.

4 **Tamam**'ı tıklayın.

Filtrelenen Web siteleri

Yetişkin grubuna ait kullanıcılar dışında tüm kullanıcılar için Web sitelerini filtreleyebilirsiniz (engelleyebilir veya izin verebilirsiniz). Çocuğunuzun Web'de gezinirken bir Web sitesine erişmesini önlemek için bu siteyi engellersiniz. Çocuğunuz engellenen Web sitesine erişmeye çalışırsa, bir iletiyle McAfee tarafından engellendiği için siteye erişilemeyeceği bildirilir.

Varsayılan olarak McAfee tarafından engellenen bir Web sitesine çocuklarınızın erişmesini isterseniz siteye izin verirsiniz. McAfee tarafından varsayılan olarak engellenen Web siteleri hakkında ayrıntılı bilgi için bkz. Anahtar sözcükler kullanarak Web sitelerini filtreleme (sayfa 164). Ayrıca filtrelenen bir Web sitesini istediğiniz zaman güncelleştirebilir veya kaldırabilirsiniz.

Not: Yetişkin yaş grubuna ait kullanıcılar (Yöneticiler dahil), engellenenler dahil olmak üzere tüm Web sitelerine erişebilirler. Engellenen Web sitelerini test etmek için Yetişkin olmayan kullanıcı olarak oturum açmanız gerekir.

Bir Web sitesini engelleme

Çocuğunuzun Web'de gezinirken bir Web sitesine erişmesini önlemek için bu siteyi engellersiniz. Çocuğunuz engellenen Web sitesine erişmeye çalışırsa, McAfee tarafından engellendiği için siteye erişilemediğini bildiren bir ileti görüntülenir.

1 Ebeveyn Denetimleri bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklatın.

2 Ebeveyn Denetimleri bölümünde **Filtrelenen Web Siteleri**'ni tıklatın.

3 Filtrelenen Web Siteleri bölümünde **http://** kutusuna bir Web sitesinin adresini yazın ve sonra **Engelle**'yi tıklatın.

4 **Tamam**'ı tıklatın.

İpucu: Web sitesinin adresini **Filtrelenen Web Siteleri** listesinde tıklatıp ardından **Engelle**'yi tıklatarak, daha önceden izin verilen bir Web sitesini engelleyebilirsiniz.

Bir Web sitesine izin verme

Hiçbir kullanıcı erişiminin engellenmediğinden emin olmak için Web sitesine izin verirsiniz. Varsayılan olarak McAfee tarafından engellenen bir Web sitesine izin verirsiniz, varsayılan ayarı geçersiz kılırsınız.

1 Ebeveyn Denetimleri bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklayın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklayın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklayın.

2 Ebeveyn Denetimleri bölümünde **Filtrelenen Web Siteleri**'ni tıklayın.

3 Filtrelenen Web Siteleri bölümünde **http://** kutusuna bir Web sitesinin adresini yazın ve sonra **İzin Ver**'i tıklayın.

4 **Tamam**'ı tıklayın.

İpucu: Web sitesinin adresini **Filtrelenen Web Siteleri** listesinde tıklayıp ardından **İzin Ver**'i tıklayarak, daha önceden engellenen bir Web sitesine izin verebilirsiniz.

Filtrelenen bir Web sitesini güncelleştirme

Bir Web sitesinin adresi değişirse ya da onu engellerken veya izin verirken adresi yanlış girdiyse güncelleştirebilirsiniz.

1 Ebeveyn Denetimleri bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklayın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklayın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklayın.

2 Ebeveyn Denetimleri bölümünde **Filtrelenen Web Siteleri**'ni tıklayın.

3 Filtrelenen Web Siteleri bölümünde, **Filtrelenen Web Siteleri** listesinden bir girişi tıklayın, **http://** kutusunda Web sitesinin adresini değiştirin ve sonra **Güncelleştir**'i tıklayın.

4 **Tamam**'ı tıklayın.

Filtrelenen bir Web sitesini kaldırma

Artık engellemek veya izin vermek istemediğiniz filtrelenen Web sitesini kaldırabilirsiniz.

1 Ebeveyn Denetimleri bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklayın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklayın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklayın.

2 Ebeveyn Denetimleri bölümünde Filtrelenen Web Siteleri'ni tıklayın.

3 Filtrelenen Web Siteleri bölümünde, Filtrelenen Verilen Web Siteleri listesinden bir girişi tıklayın ve sonra **Kaldır**'ı tıklayın.

4 Tamam'ı tıklayın.

Anahtar sözcükler kullanarak Web sitelerini filtreleme

Anahtar sözcük filtreleme, Yetişkin olmayan kullanıcıların olası uygunsuz sözcükler içeren Web sitelerine girmelerini engellemeye olanak verir. Anahtar sözcük filtreleme özelliği etkinleştirildiğinde, içerik derecelendirme grubuna göre kullanıcıların görebilecekleri içeriği derecelendirmek için varsayılan anahtar sözcük listesi ve ilişkili kurallar kullanılır. Kullanıcılar, bazı anahtar sözcükleri içeren Web sitelerine erişmek için belirli bir yaş grubuna ait olmalıdır. Örneğin, *porno* sözcüğünü içeren Web sitelerine yalnızca Yetişkin grubunun üyeleri girebilirken, *ilaçlar* sözcüğünü içeren Web sitelerine yalnızca Çocuk grubunun (ve daha büyük grupların) üyeleri girebilir.

Bu varsayılan listeye kendi anahtar sözcüklerinizi de ekleyebilir ve bunları belirli içerik derecelendirme gruplarıyla ilişkilendirebilirsiniz. Eklediğiniz anahtar sözcük kuralları, varsayılan listede eşleşen bir anahtar sözcükle önceden ilişkilendirilmiş kuralı geçersiz kılar.

Anahtar sözcük filtrelemeyi devre dışı bırakma

Varsayılan olarak anahtar sözcük filtreleme özelliği etkindir; böylece, içerik derecelendirme grubuna göre kullanıcıların görebilecekleri içeriği derecelendirmek için varsayılan anahtar sözcük listesi ve ilişkili kurallar kullanılır. McAfee tarafından önerilmemesine karşın, istediğiniz zaman anahtar sözcük filtrelemeyi devre dışı bırakabilirsiniz.

1 Ebeveyn Denetimleri bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklatın.

2 Ebeveyn Denetimleri bölümünde **Anahtar Sözcükler**'i tıklatın.

3 Anahtar Sözcükler bölümünde **Kapalı**'yı tıklatın.

4 **Tamam**'ı tıklatın.

Web sitelerini anahtar sözcüklere göre engelleme

Web sitelerini uygunsuz bir içeriğe göre engellemek istiyor ancak site adreslerini tam olarak bilemiyorsanız, siteleri anahtar sözcüklerine göre engelleyebilirsiniz. Bunun için bir anahtar sözcük girip, daha sonra bu anahtar sözcüğü içeren Web sitelerinin hangi içerik derecelendirme grupları tarafından görüntülenebileceğini belirlemeniz yeterlidir.

1 Ebeveyn Denetimleri bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklayın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklayın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklayın.

2 Ebeveyn Denetimleri bölümünde **Anahtar Sözcükler**'i tıklayın ve anahtar sözcük filtrelemenin etkin olduğundan emin olun.

3 **Anahtar Sözcük Listesi** altında **Aranan** kutusuna bir anahtar sözcük yazın.

4 Minimum yaş grubunu belirtmek için **Minimum Yaş** kaydırma çubuğunu hareket ettirin.

Bu yaş grubunda ve daha büyük gruplardaki kullanıcılar, bu anahtar sözcüğü içeren Web sitelerine girebilirler.

5 **Tamam**'ı tıklayın.

B Ö L Ü M 3 2

Web'de bilgileri koruma

Bilgileri engelleyerek, Web'de gezinirken özel bilgilerinizi ve dosyalarınızı koruyabilirsiniz. Örneğin, engellenen bilgi alanına ekleyerek, kişisel bilgilerinizin (ad, adres, kredi kartı numaraları ve banka hesap numaraları gibi) Web üzerinden iletilmesini engelleyebilirsiniz.

Not: Privacy Service, kişisel bilgilerin iletilmesini, banka siteleri gibi güvenli Web siteleriyle (<https://> protokolünü kullanan Web siteleri) engellemez.

Bu bölümde

Kişisel bilgileri koruma 168

Kişisel bilgileri koruma

Engelleyerek, kişisel bilgilerinizin (ad, adres, kredi kartı numaraları ve banka hesap numaraları gibi) Web üzerinden iletilmesini engelleyin. McAfee Web üzerinden gönderilmek üzere olan bir şeyde (örneğin form alanı veya dosya) kişisel bilgiler algılsa şunlar gerçekleşir:

- Yöneticiyseniz, bilgi gönderme işlemini onaylamanız gerekir.
- Yönetici değilseniz, engellenen bölümün yerine yıldız işaretleri (*) yerleştirilir. Örneğin, kötü niyetli bir Web sitesi kredi kartı numaranızı başka bir bilgisayara göndermeye çalışırsa, numaranın yerine yıldız işaretleri yerleştirilir.

Kişisel bilgileri koruma

Şu türde kişisel bilgileri engelleyebilirsiniz: ad, adres, posta kodu, sosyal sigorta numarası, telefon numarası, kredi kartı numaraları, banka hesapları, komisyonculuk hesapları ve telefon kartları. Farklı türde kişisel bilgileri engellemek istiyorsanız, bilgi türünü **diğer** olarak ayarlayabilirsiniz.

1 Korunan Bilgiler bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklatın.
3. Internet ve Ağ bilgi bölümünde **Yapılandır**'ı tıklatın.
4. Internet ve Ağ Yapılandırması bölümünde, Kişisel bilgi korumanın etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklatın.

2 Korunan Bilgiler bölümünde **Ekle**'yi tıklatın.

3 Listedeki engellemek istediğiniz bilgi türünü seçin.

4 Kişisel bilgilerinizi girin ve ardından **Tamam**'ı tıklatın.

B Ö L Ü M 3 3

Parolaları koruma

Parola Mahzeni, kişisel parolalarınız için güvenli bir saklama alanıdır. Parolalarınızı başka hiçbir kullanıcının (hatta Yöneticinin) erişemeyeceği şekilde güvenle saklamanıza olanak verir.

Bu bölümde

Parola Mahzeni'ni ayarlama 170

Parola Mahzeni'ni ayarlama

Parola Mahzeni'ni kullanmaya başlamadan önce, Parola Mahzeni parolasını ayarlamanız gerekir. Yalnızca bu parolayı bilen kullanıcılar Parola Mahzeni'ne erişebilirler. Parola Mahzeni parolanızı unutursanız, onu sıfırlayabilirsiniz; ancak bu durumda Parola Mahzeni'nde daha önceden saklanan tüm parolalar silinir.

Parola Mahzeni parolasını ayarladıktan sonra, mahzeninizde parolalar ekleyebilir, silebilir veya kaldırabilirsiniz. İstediğiniz zaman Parola Mahzeni parolanızı da değiştirebilirsiniz.

Parola ekleme

Parolalarınızı anımsamakta zorlanıyorsanız, bunları Parola Mahzeni'ne ekleyebilirsiniz. Parola Mahzeni, yalnızca Parola Mahzeni parolasını bilen kullanıcılar tarafından erişilebilen güvenli bir konumdur.

- 1 Parola Mahzeni bölmesini açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklatın.
 3. Internet ve Ağ bilgi bölümünde **Yapılandır**'ı tıklatın.
 4. Internet ve Ağ Yapılandırması bölümünde, **Parola Mahzeni** altında **Gelişmiş**'i tıklatın.
- 2 Parola Mahzeni'nde **Parola** kutusuna parolanızı yazın ve sonra **Parolayı Yeniden Girin** kutusuna parolanızı yeniden yazın.
- 3 **Aç**'i tıklatın.
- 4 Parola Mahzenini Yönet bölümünde **Ekle**'yi tıklatın.
- 5 **Açıklama** kutusuna parola açıklamasını (örneğin parolanın neyle ilgili olduğu) yazın ve ardından **Parola** kutusuna parolayı yazın.
- 6 **Tamam**'i tıklatın.

Parolayı değiştirme

Parola Mahzeni'ndeki girişlerin her zaman doğru ve güvenilir olmasını sağlamak için, parolalar değiştiğinde bunları güncelleştirmeniz gerekir.

- 1 Parola Mahzeni bölmesini açın.
Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklatın.
3. Internet ve Ağ bilgi bölümünde **Yapılandır**'ı tıklatın.
4. Internet ve Ağ Yapılandırması bölümünde, **Parola Mahzeni** altında **Gelişmiş**'i tıklatın.
- 2 Parola Mahzeni parolanızı **Parola** kutusuna yazın.
- 3 **Aç**'ı tıklatın.
- 4 Parola Mahzenini Yönet bölümünde bir parola girişini tıklatın ve sonra **Düzenle**'yi tıklatın.
- 5 **Açıklama** kutusundaki parola açıklamasını (örneğin parolanın neyle ilgili olduğu) değiştirin ve ardından **Parola** kutusundaki parolayı değiştirin.
- 6 **Tamam**'i tıklatın.

Parolayı kaldırma

İstediğiniz zaman Parola Mahzeni'nden bir parolayı kaldırabilirsiniz. Mahzenden kaldırdığınız parolayı hiçbir şekilde kurtaramazsınız.

- 1 Parola Mahzeni bölümünü açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklatın.
 3. Internet ve Ağ bilgi bölümünde **Yapılandır**'ı tıklatın.
 4. Internet ve Ağ Yapılandırması bölümünde, **Parola Mahzeni** altında **Gelişmiş**'i tıklatın.
- 2 Parola Mahzeni parolanızı **Parola** kutusuna yazın.
- 3 **Aç**'ı tıklatın.
- 4 Parola Mahzenini Yönet bölümünde bir parola girişini tıklatın ve sonra **Kaldır**'ı tıklatın.
- 5 Kaldırma Onayı iletişim kutusunda **Evet**'i tıklatın.

Parola Mahzeni parolanızı değiştirme

İstediğiniz zaman Parola Mahzeni parolanızı değiştirebilirsiniz.

- 1 Parola Mahzeni bölümünü açın.
Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklatın.
3. Internet ve Ağ bilgi bölümünde **Yapılandır**'ı tıklatın.
4. Internet ve Ağ Yapılandırması bölümünde, **Parola Mahzeni** altında **Gelişmiş**'i tıklatın.
- 2 Parolayı Mahzeni bölümünde, **Parola** kutusuna geçerli parolanızı yazın ve sonra **Aç**'ı tıklatın.
- 3 Parola Mahzenini Yönet bölümünde **Parolayı Değiştir**'i tıklatın.
- 4 **Parola Seçin** kutusuna yeni bir parola yazın ve sonra **Parolayı Yeniden Girin** kutusuna parolanızı yeniden yazın.
- 5 **Tamam**'ı tıklatın.
- 6 Parola Mahzeni Parolası Değiştirildi iletişim kutusunda **Tamam**'ı tıklatın.

Parola Mahzeni parolanızı sıfırlama

Parola Mahzeni parolanızı unutursanız, onu sıfırlayabilirsiniz; ancak bu durumda daha önceden girmiş olduğunuz tüm parolalar silinir.

- 1 Parola Mahzeni bölümünü açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklatın.
 3. Internet ve Ağ bilgi bölümünde **Yapılandır**'ı tıklatın.
 4. Internet ve Ağ Yapılandırması bölümünde, **Parola Mahzeni** altında **Gelişmiş**'i tıklatın.
- 2 **Parola Mahzenini Sıfırla** altında, **Parola** kutusuna yeni bir parola yazın ve sonra **Parolayı Yeniden Girin** kutusuna parolanızı yeniden yazın.
- 3 **Sıfırla**'yı tıklatın.
- 4 Parola Onayını Sıfırla iletişim kutusunda **Evet**'i tıklatın.

B Ö L Ü M 3 4

McAfee Data Backup

Dosyalarınızı CD, DVD, USB sürücüye, harici sabit diske veya ağ sürücüsüne arşivleyerek verilerinizin yanlışlıkla kaybolmasını engellemek için Data Backup kullanın. Yerel arşivleme, kişisel verilerinizi CD, DVD, USB sürücüye, harici sabit diske veya ağ sürücüsüne arşivlemenize (yedeklemenize) olanak verir. Bu özellik, yanlışlıkla kaybettiğiniz kayıtlarınızın, belgelerinizin ve kişisel olarak ilgilendiğiniz diğer malzemelerin yerel kopyasını sağlar.

Data Backup'ı kullanmaya başlamadan önce, en popüler özelliklerden bazıları hakkında bilgi edinebilirsiniz. Bu özelliklerin yapılandırılması ve kullanımıyla ilgili ayrıntılar, Data Backup yardımında sunulmaktadır. Program özelliklerine göz attıktan sonra, yerel arşivler gerçekleştirmek için yeterli kullanılabilir arşiv ortamının bulunduğundan emin olmalısınız.

Bu bölümde

Özellikler	174
Dosyaları arşivleme	175
Arşivlenen dosyalarla çalışma	183

Özellikler

Data Backup, fotoğraflarınızı, müziğinizi ve diğer önemli dosyalarınızı kaydetmek ve geri yüklemek için aşağıdaki özellikleri sunar.

Yerel zamanlanan arşivleme

Dosyaları ve klasörleri CD, DVD, USB sürücüsüne, harici sabit diske veya ağ sürücüsüne arşivleyerek verilerinizi koruyun. Siz ilk arşivlemeyi başlattıktan sonra, artımlı arşivler otomatik olarak gerçekleşir.

Tek tıklatmayla geri yükleme

Dosyalar ve klasörler bilgisayarınızda yanlışlıkla silinir veya bozulursa, en son arşivlenen sürümleri kullanılan arşiv ortamından geri yükleyebilirsiniz.

Sıkıştırma ve şifreleme

Varsayılan olarak, arşivlenen dosyalarınız sıkıştırılır ve bu şekilde arşiv ortamınızda alan kazanılır. Ek güvenlik önlemi için, arşivleriniz varsayılan olarak şifrelenir.

B Ö L Ü M 3 5

Dosyaları arşivleme

McAfee Data Backup'ı kullanarak, bilgisayarınızdaki dosyaların kopyasını CD, DVD, USB sürücüye, harici sabit diske veya ağ aygıtına arşivleyebilirsiniz. Dosyalarınızı bu şekilde arşivlemek, yanlışlıkla kaybolan veya zarar gören verileri geri almanızı kolaylaştırır.

Dosyaları arşivlemeye başlamadan önce, varsayılan arşiv konumunuzu (CD, DVD, USB sürücü, harici sabit disk veya ağ sürücüsü) seçmeniz gerekir. McAfee, örneğin arşivlemek istediğiniz klasörler ve dosya türleri gibi bazı ayarları önceden yapmıştır, ancak bu ayarları değiştirebilirsiniz.

Yerel arşiv seçeneklerini ayarladıktan sonra, Data Backup'ın tam veya hızlı arşivlemeleri çalıştırma sıklığı ile ilgili varsayılan ayarları değiştirebilirsiniz. İstediğiniz zaman el ile arşivlemeleri çalıştırabilirsiniz.

Bu bölümde

Arşiv seçeneklerini ayarlama	176
Tam ve hızlı arşivlemeleri çalıştırma	180

Arşiv seçeneklerini ayarlama

Verilerinizi arşivlemeye başlamadan önce, bazı yerel arşiv seçeneklerini ayarlamalısınız. Örneğin, izleme konumlarını ve izlenen dosya türlerini ayarlamanız gereklidir. İzleme konumları, Data Backup'ın bilgisayarınızda yeni dosyaları veya dosya değişikliklerini izlediği klasörlerdir. İzlenen dosya türleri, Data Backup'ın izleme konumlarında arşivlediği dosya türleridir (örn., .doc, .xls gibi). Varsayılan olarak, Data Backup izleme konumlarınızda depolanan tüm dosya türlerini izler.

İki tür izleme konumu ayarlayabilirsiniz: ayrıntılı izleme konumları ve yüzeysel izleme konumları. Ayrıntılı izleme konumu ayarlarsanız, Data Backup bu klasörün ve alt klasörlerinin içindeki izlenen dosya türlerini arşivler. Yüzeysel izleme konumu ayarlarsanız, Data Backup yalnızca bu klasörün (alt klasörlerinin değil) içindeki izlenen dosya türlerini arşivler. Ayrıca, yerel arşivin dışında tutmak istediğiniz konumları da tanımlayabilirsiniz. Varsayılan olarak, Windows Masaüstü ve Belgelerim konumları ayrıntılı izleme konumları olarak ayarlıdır.

İzlenen dosya türlerini ve konumları ayarladıktan sonra, arşiv konumunu (arşivlenen verilerin depolanacağı CD, DVD, USB sürücü, harici sabit disk veya ağ sürücüsü) ayarlamanız gerekir. Arşiv konumunu istediğiniz zaman değiştirebilirsiniz.

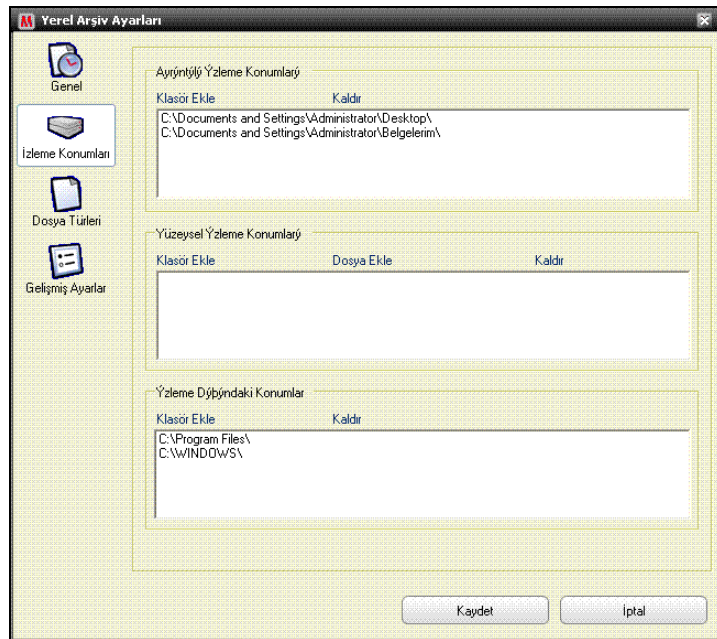
Güvenlik nedenleri veya boyut sorunlarından ötürü, arşivlenen dosyalarınızda varsayılan olarak şifreleme veya sıkıştırma etkindir. Bilgileri şifrenin nasıl çözüleceğini bilmeyen kişiler tarafından okunamayacak şekilde gizleyerek, şifrelenen dosyaların içeriği metinden şifreye dönüştürülür. Sıkıştırılan dosyalar, onları depolamak veya iletmek için gereken alanı en aza indirecek şekilde sıkıştırılır. McAfee tarafından önerilmemesine karşın, istediğiniz zaman şifreleme veya sıkıştırmayı devre dışı bırakabilirsiniz.

Arşivlemeye konum ekleme

Arşivleme için iki tür izleme konumu ayarlayabilirsiniz: ayrıntılı ve yüzeysel. Ayrıntılı izleme konumu ayarlarsanız, Data Backup klasörün ve alt klasörlerinin içeriklerindeki değişiklikleri izler. Yüzeysel izleme konumu ayarlarsanız, Data Backup yalnızca klasörün (alt klasörlerinin değil) içeriklerini izler.

Arşivlemeye konum eklemek için:

- 1 Yerel Arşiv sekmesini tıklatın.
- 2 Soldaki bölmede **Ayarlar**'ı tıklatın.
- 3 Yerel Arşiv Ayarları iletişim kutusunda **İzleme Konumları**'nı tıklatın.



- 4 Aşağıdakilerden birini gerçekleştirin:
 - Alt klasörlerinin içerikleri dahil, bir klasörün içeriklerini arşivlemek için **Ayrıntılı İzleme Konumları** bölümünde **Klasör Ekle**'yi tıklatın.
 - Alt klasörlerinin içerikleri hariç, bir klasörün içeriklerini arşivlemek için **Yüzeysel İzleme Konumları** bölümünde **Klasör Ekle**'yi tıklatın.
- 5 Klasöre Gözet iletişim kutusunda, izlemek istediğiniz klasöre gidin ve ardından **Tamam**'ı tıklatın.
- 6 **Kaydet**'i tıklatın.

İpucu: Data Backup'ın henüz oluşturmadığınız bir klasörü izlemesini istiyorsanız, bir klasör eklemek ve aynı zamanda bunu izleme konumu olarak ayarlamak için, Klasöre Gözet iletişim kutusunda **Yeni Klasör Oluştur**'u tıklatabilirsiniz.

Arşivleme dosyası türlerini ayarlama

Ayrıntılı veya yüzeysel izleme konumlarınızda hangi dosya türlerinin arşivleneceğini belirleyebilirsiniz. Bunları mevcut bir dosya türleri listesinden seçebilir veya listeye yeni bir tür ekleyebilirsiniz.

Arşivleme dosyası türlerini ayarlamak için:

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Soldaki bölmede **Ayarlar**'ı tıklatın.
- 3 Yerel Arşiv Ayarları iletişim kutusunda **Dosya Türleri**'ni tıklatın.
- 4 Dosya türleri listesini genişletin ve arşivlemek istediğiniz dosya türlerinin yanındaki onay kutularını seçin.
- 5 **Kaydet**'i tıklatın.

İpucu: **Seçili Dosya Türleri** listesine yeni bir dosya türü eklemek için, dosya uzantısını **Özel Dosya Türü**'nü **'Diğer'e Ekle** kutusuna yazın ve ardından **Ekle**'yi tıklatın. Yeni dosya türü, otomatik olarak izlenen dosya türü olur.

Bir konumu arşivlemenin dışında tutma

Bir konumun (klasör) ve içeriklerinin çevrimiçi olarak arşivlenmesini engellemek isterseniz, o konumu arşivlemenin dışında tutarsınız.

Bir konumu arşivlemenin dışında tutmak için:

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Soldaki bölmede **Ayarlar**'ı tıklatın.
- 3 Yerel Arşiv Ayarları iletişim kutusunda **İzlenen Klasörler**'i tıklatın.
- 4 **İzleme Dışındaki Konumlar** bölümünde **Klasör Ekle**'yi tıklatın.
- 5 Klasöre Gözetim iletişim kutusunda, dışarıda tutmak istediğiniz klasöre gidip seçin ve ardından **Tamam**'ı tıklatın.
- 6 **Kaydet**'i tıklatın.

İpucu: Data Backup'ın henüz oluşturmadığınız bir klasörü dışarıda tutmasını istiyorsanız, bir klasör eklemek ve aynı zamanda bunu dışarıda tutmak için, Klasöre Gözetim iletişim kutusunda **Yeni Klasör Oluştur**'u tıklatabilirsiniz.

Arşiv konumunu değiştirme

Arşiv konumunu değiştirdiğinizde, farklı bir konumda daha önceden arşivlenen dosyalar *Hiç Arşivlenmemiş* olarak listelenir.

Arşiv konumunu değiştirmek için:

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Soldaki bölmede **Ayarlar**'ı tıklatın.
- 3 **Arşiv Konumunu Değiştir**'i tıklatın.
- 4 Arşiv Konumu iletişim kutusunda, aşağıdakilerden birini gerçekleştirin:
 - **CD/DVD Yazıcı Seç**'i tıklatın, **Yazıcı** listesinde bilgisayarınızın CD veya DVD sürücüsünü tıklatın ve ardından **Kaydet**'i tıklatın.
 - **Sürücü Konumunu Seç**'i tıklatın; bir USB sürücüye, yerel sürücüye veya harici sabit diske gidip seçin ve ardından **Tamam**'ı tıklatın.
 - **Ağ Konumunu Seç**'i tıklatın, ağ klasörüne gidip seçin ve ardından **Tamam**'ı tıklatın.
- 5 **Seçili Arşiv Konumu** bölümünde yeni arşiv konumunu doğrulayın ve ardından **Tamam**'ı tıklatın.
- 6 Onay iletişim kutusunda **Tamam**'ı tıklatın.
- 7 **Kaydet**'i tıklatın.

Arşiv şifreleme ve sıkıştırmayı devre dışı bırakma

Arşivlenen dosyaları şifrelemek, dosyaların içeriklerinin okunmasını engelleyerek verilerinizin gizliliğini korur. Arşivlenen dosyaları sıkıştırmak, dosya boyutlarının en az indirilmesine yardımcı olur. Varsayılan olarak, şifreleme ve sıkıştırma etkindir; ancak bu seçenekleri istediğiniz zaman devre dışı bırakabilirsiniz.

Arşiv şifreleme ve sıkıştırmayı devre dışı bırakmak için:

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Soldaki bölmede **Ayarlar**'ı tıklatın.
- 3 Yerel Arşiv Ayarları iletişim kutusunda **Gelişmiş Ayarlar**'ı tıklatın.
- 4 **Güvenliği artırmak için şifrelemeyi etkinleştir** onay kutusunu temizleyin.
- 5 **Depolanma boyutunu azaltmak için sıkıştırmayı etkinleştir** onay kutusunu temizleyin.
- 6 **Kaydet**'i tıklatın.

Not: McAfee, dosyalarınızı arşivlerken şifreleme ve sıkıştırmayı devre dışı bırakmamanızı önerir.

Tam ve hızlı arşivlemeleri çalıştırma

İki tür arşivleme çalıştırabilirsiniz: tam veya hızlı. Tam arşivlemeyi çalıştırdığınızda, ayarladığınız izlenen dosya türleri ve konumlarını temel alan tam bir veri setini arşivlersiniz. Hızlı arşivlemeyi çalıştırdığınızda, yalnızca en son tam veya hızlı arşivleme işleminden sonra değiştirilmiş olan izlenen dosyaları arşivlersiniz.

Varsayılan olarak, Data Backup izleme konumlarınızda izlenen dosya türleri için her Pazartesi günü saat 9:00'da tam arşivlemeyi ve en son tam veya hızlı arşivlemeden sonra her 48 saatte bir hızlı arşivlemeyi çalıştırmaya zamanlanmıştır. Bu zamanlama, dosyalarınızın varolan arşivinin her zaman sürdürülmesini sağlar. Ancak 48 saatte bir arşivlemek istemiyorsanız, zamanlamayı gereksinimlerinize uygun şekilde ayarlayabilirsiniz.

İzleme konumlarınızın içeriklerini istek üzerine arşivlemek istiyorsanız, bunu istediğiniz zaman yapabilirsiniz. Örneğin, bir dosyada değişiklik yaptıysanız ve onu arşivlemek istiyorsanız ancak Data Backup tam veya hızlı arşivlemeyi birkaç saat sonra çalıştıracak şekilde zamanlanmışsa, dosyaları el ile arşivleyebilirsiniz. Dosyaları el ile arşivlediğinizde, otomatik arşivlemeler için ayarladığınız aralık sıfırlanır.

Ayrıca, uygun olmayan bir zamanda gerçekleşen otomatik veya el ile arşivlemeyi de kesebilirsiniz. Örneğin, kaynak ağırlıklı bir görev gerçekleştirdiğiniz sırada otomatik arşivleme başlarsa, onu durdurabilirsiniz. Otomatik arşivlemeyi durdurduğunuzda, otomatik arşivlemeler için ayarladığınız aralık sıfırlanır.

Otomatik arşivlemeleri zamanlama

Verilerinizin her zaman korunmasını sağlamak için, tam ve hızlı arşivlemelerin sıklığını ayarlayabilirsiniz.

Otomatik arşivlemeleri zamanlamak için:

- 1 Yerel Arşiv sekmesini tıklatın.
- 2 Soldaki bölmede **Ayarlar**'ı tıklatın.
- 3 Yerel Arşiv Ayarları iletişim kutusunda **Genel**'i tıklatın.
- 4 Tam arşivlemeyi her gün, her hafta veya her ay çalıştırmak için **Tam arşivleme sıklığı** bölümünde şu seçeneklerden birini tıklatın:
 - **Gün**
 - **Hafta**
 - **Ay**

- 5 Tam arşivlemeyi çalıştırmak istediğiniz günün yanındaki onay kutusunu seçin.
- 6 Tam arşivlemeyi çalıştırmak istediğiniz zamanı belirtmek için **Saat** listesinde bir değeri tıklayın.
- 7 Günlük veya saatlik olarak hızlı arşivlemeyi çalıştırmak için, **Hızlı Arşiv** bölümünde şu seçeneklerden birini tıklayın:
 - **Saat**
 - **Gün**
- 8 **Hızlı arşivleme sıklığı** kutusuna sıklığı temsil eden bir sayı yazın.
- 9 **Kaydet**'i tıklayın.

Otomatik arşivlemeyi kesme

Data Backup, izleme konumlarındaki dosyaları tanımladığınız zamanlamaya göre otomatik olarak arşivler. Ancak otomatik arşivlemeyi çalışırken kesmek isterseniz, bunu istediğiniz zaman yapabilirsiniz.

Otomatik arşivlemeyi kesmek için:

- 1 Soldaki bölmede **Arşivlemeyi Durdur**'u tıklayın.
- 2 Onay iletişim kutusunda **Evet**'i tıklayın.

Not: Arşivlemeyi Durdur bağlantısı, yalnızca arşivleme çalışırken görüntülenir.

Arşivlemeleri el ile çalıştırma

Otomatik arşivlemelerin önceden tanımlı zamanlamaya göre çalışmasına karşın, istediğiniz zaman el ile hızlı veya tam arşivlemeyi de çalıştırabilirsiniz. Hızlı arşivleme, yalnızca en son tam veya hızlı arşivlemeden sonra değiştirilen dosyaları arşivler. Tam arşivleme, tüm izleme konumlarındaki izlenen dosya türlerini arşivler.

Hızlı veya tam arşivlemeyi el ile çalıştırmak için:

- 1 **Yerel Arşiv** sekmesini tıklayın.
- 2 Hızlı arşivlemeyi çalıştırmak için, sol bölmede **Hızlı Arşiv**'i tıklayın.
- 3 Tam arşivlemeyi çalıştırmak için, sol bölmede **Tam Arşiv**'i tıklayın.
- 4 Arşivlemeyi başlatmaya hazır iletişim kutusunda, depolama alanınızı ve ayarlarınızı doğrulayın ve ardından **Devam Et**'i tıklayın.

B Ö L Ü M 3 6

Arşivlenen dosyalarla çalışma

Bazı dosyaları arşivledikten sonra, bunlarla çalışmak için Data Backup'ı kullanabilirsiniz. Arşivlenen dosyalarınız, onları kolayca bulmanıza olanak veren geleneksel gezgin görünümünde sunulur. Arşiviniz genişledikçe, dosyaları sıralamak veya aramak isteyebilirsiniz. Ayrıca, dosyaları almaya gerek kalmadan incelemek için, onları doğrudan gezgin görünümünde açabilirsiniz.

Dosyanızın yerel kopyası eskiyse, eksikse veya bozulmuşsa, dosyaları arşivden alırsınız. Data Backup, çevrimiçi arşivlerinizi ve depolama ortamınızı yönetmek için gerek duyduğunuz bilgileri de sağlar.

Bu bölümde

Yerel arşivleme gezginini kullanma	184
Arşivlenen dosyaları geri yükleme	186
Arşivleri yönetme	188

Yerel arşivleme gezginini kullanma

Yerel arşivleme gezgini, yerel olarak arşivlediğiniz dosyaları görüntülemenize ve yönetmenize olanak verir. Her dosyanın adını, konumunu, boyutunu, durumunu (arşivlenmiş, arşivlenmemiş veya arşivleniyor) ve her dosyanın en son arşivlendiği tarihi görüntüleyebilirsiniz. Ayrıca dosyaları bu ölçütlerden birine göre sıralayabilirsiniz.

Geniş bir arşiviniz varsa, arama yaparak bir dosyayı hızla bulabilirsiniz. Dosya adının veya yolunun tamamı veya bir kısmı ile arama yapabilir ve daha sonra yaklaşık dosya boyutunu ve en son arşivleme tarihini belirterek aramanızın kapsamını daraltabilirsiniz.

Dosyayı bulduktan sonra, onu doğrudan yerel arşivleme gezgininden açabilirsiniz. Data Backup, dosyayı kendi programında açarak, yerel arşivleme gezgininden çıkmadan değişiklikler yapmanıza olanak verir. Dosya, bilgisayarınızda özgün izleme konumuna kaydedilir ve tanımladığınız arşivleme zamanlamasına göre otomatik olarak arşivlenir.

Arşivlenen dosyaları sıralama

Arşivlenen dosyalarınızla klasörlerinizi şu ölçütlere göre sıralayabilirsiniz: ad, dosya türü, boyut, durum (arşivlenmiş, arşivlenmemiş veya arşivleniyor), dosyaların en son arşivlendiği tarih veya dosyaların bilgisayarınızdaki konumu (yolu).

Arşivlenen dosyaları sıralamak için:

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Sağ bölmede bir sütun adını tıklatın.

Arşivlenen bir dosyayı arama

Geniş bir arşivlenmiş dosya havuzunuz varsa, arama yaparak bir dosyayı hızla bulabilirsiniz. Dosya adının veya yolunun tamamı veya bir kısmı ile arama yapabilir ve daha sonra yaklaşık dosya boyutunu ve en son arşivleme tarihini belirterek aramanızın kapsamını daraltabilirsiniz.

Arşivlenen bir dosyayı aramak için:

- 1 Dosya adının tamamını veya bir kısmını ekranın üst bölümündeki **Ara** kutusuna yazın ve ardından ENTER tuşuna basın.
- 2 **Yolun tamamı veya bir kısmı** kutusuna yolun tamamını veya bir kısmını yazın.
- 3 Aşağıdakilerden birini yaparak, aradığınız dosyanın yaklaşık boyutunu belirtin:
 - **<100 KB, <1 MB veya >1 MB** seçeneğini tıklatın.
 - **Boyut (KB)**'u tıklatın ve ardından kutularda uygun boyut değerlerini belirtin.

- 4 Aşağıdakilerden birini gerçekleştirerek, dosyanın en son yaklaşık çevrimiçi yedekleme tarihini belirtin:
- **Bu Hafta, Bu Ay** veya **Bu Yıl**'ı tıklatın.
 - **Tarihleri Belirt**'i tıklatın, listede **Arşivlendi**'yi tıklatın ve ardından tarih listelerinde uygun tarih değerlerini tıklatın.
- 5 **Ara**'yı tıklatın.

Not: En son arşivlemenin yaklaşık boyutunu veya tarihini bilmiyorsanız, **Bilinmiyor**'u tıklatın.

Arşivlenen bir dosyayı açma

Arşivlenen bir dosyayı doğrudan yerel arşivleme gezgininde açarak içeriğini inceleyebilirsiniz.

Arşivlenen dosyaları açmak için:

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Sağ bölmede, bir dosya adını tıklatın ve ardından **Aç**'ı tıklatın.

İpucu: Ayrıca, dosya adını çift tıklatarak da arşivlenen bir dosyayı açabilirsiniz.

Arşivlenen dosyaları geri yükleme

İzlenen bir dosya bozulur, kaybolur veya yanlışlıkla silinirse, dosyanın kopyasını yerel arşivden geri yükleyebilirsiniz. Bu nedenle, dosyalarınızı düzenli olarak arşivlemeniz önemlidir. Ayrıca, yerel arşivden dosyaların eski sürümlerini de geri yükleyebilirsiniz. Örneğin, bir dosyayı düzenli olarak arşivlemenize karşın dosyanın daha önceki bir sürümüne dönmek isterseniz, dosyayı arşiv konumunda bularak bunu gerçekleştirebilirsiniz. Arşiv konumu bir yerel sürücü veya ağ sürücüsü ise, dosyaya göz atabilirsiniz. Arşiv konumu bir harici sabit disk veya USB sürücü ise, dosyaya göz atmak için sürücüyü bilgisayara bağlamanız gerekir. Arşiv konumu CD veya DVD ise, dosyaya göz atmak için CD veya DVD'yi bilgisayara takmanız gerekir.

Ayrıca, bir bilgisayardan başka bir bilgisayara arşivlediğiniz dosyaları da geri yükleyebilirsiniz. Örneğin, bir dosya grubunu A bilgisayarındaki bir harici sabit diske arşivlediyseniz, bu dosyaları B bilgisayarına geri yükleyebilirsiniz. Bunun için, B bilgisayarına McAfee Data Backup yüklemeniz ve harici sabit diski bağlamanız gerekir. Daha sonra, Data Backup'ta dosyalara göz attığınızda, dosyalar geri yükleme için **Eksik Dosyalar** listesine eklenir.

Dosyaları arşivleme hakkında ayrıntılı bilgi için, bkz. Dosyaları arşivleme. İzlenen bir dosyayı bilerek arşivinizden silerseniz, **Eksik Dosyalar** listesinden girişi de silebilirsiniz.

Eksik dosyaları yerel arşivden geri yükleme

Data Backup'ın yerel arşivi, yerel bilgisayarınızda izlenen bir klasördeki eksik verileri kurtarmanıza olanak verir. Örneğin, bir dosya izlenen klasörden taşınmış veya silinmişse ve önceden arşivlenmişse, onu yerel arşivden geri yükleyebilirsiniz.

Eksik bir dosyayı yerel arşivden almak için:

- 1 Yerel Arşiv** sekmesini tıklatın.
- Ekranın altında bulunan **Eksik Dosyalar** sekmesinde, geri yüklemek istediğiniz dosya adının yanındaki onay kutusunu seçin.
- 3 Geri Yükle**'yi tıklatın.

İpucu: Tümünü Geri Yükle'yi tıklatarak, **Eksik Dosyalar** listesindeki tüm dosyaları geri yükleyebilirsiniz.

Yerel arşivden bir dosyanın eski sürümünü geri yükleme

Arşivlenen bir dosyanın eski sürümünü geri yüklemek isterseniz, onu bulup **Eksik Dosyalar** listesine ekleyebilirsiniz. Daha sonra, bu dosyayı **Eksik Dosyalar** listesindeki herhangi bir dosya için yapacağınız gibi geri yükleyebilirsiniz.

Yerel arşivden bir dosyanın eski sürümünü geri yüklemek için:

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Ekranın altında bulunan **Eksik Dosyalar** sekmesinde, **Gözet**'i tıklatın ve ardından arşivin depolandığı konuma gidin.

Arşivlenen dosya adları şu biçimde olur: `cre ggaayy_ss-dd-ss_***`; burada `ggaayy` dosyaların arşivlendiği tarihtir, `ss-dd-ss` dosyaların arşivlendiği saattir ve `***` gerçekleştirilen arşivlemenin tam veya hızlı arşivleme olmasına göre **Tam** veya **Kapsam**'dir.
- 3 Konumu seçin ve ardından **Tamam**'i tıklatın.

Seçili konumda bulunan dosyalar **Eksik Dosyalar** listesinde görüntülenir ve geri yüklenmeye hazırdır. Ayrıntılı bilgi için, bkz. Eksik dosyaları yerel arşivden geri yükleme.

Dosyaları eksik dosyalar listesinden kaldırma

Arşivlenen bir dosya izlenen klasörden taşındığında veya silindiğinde, otomatik olarak **Eksik Dosyalar** listesinde görüntülenir. Bu, arşivlenen dosyalarla izlenen klasörlerde bulunan dosyalar arasında tutarsızlık olduğunu size bildirir. Dosya bilerek izlenen klasörden kaldırılmışsa veya silinmişse, dosyayı **Eksik Dosyalar** listesinden silebilirsiniz.

Eksik Dosyalar listesinden dosya kaldırmak için:

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Ekranın altında bulunan **Eksik Dosyalar** sekmesinde, kaldırmak istediğiniz dosya adının yanındaki onay kutusunu seçin.
- 3 **Sil**'i tıklatın.

İpucu: **Tümünü Sil**'i tıklatarak, **Eksik Dosyalar** listesindeki tüm dosyaları kaldırabilirsiniz.

Arşivleri yönetme

Tam ve hızlı arşivlemelerinizle ilgili bilgilerin özetini istediğiniz zaman görüntüleyebilirsiniz. Örneğin izlenen verilerin miktarı, arşivlenmiş verilerin miktarı ve izlenen ancak henüz arşivlenmemiş verilerin miktarı hakkında bilgiler görüntüleyebilirsiniz. Ayrıca, en son ve bir sonraki arşivlemelerin gerçekleşme tarihi gibi arşivleme zamanlamanızla ilgili bilgileri de görüntüleyebilirsiniz.

Arşivleme etkinliğinizin özetini görüntüleme

İstediğiniz zaman arşivleme etkinliğinizle ilgili bilgiler görüntüleyebilirsiniz. Örneğin, arşivlenmiş dosyaların yüzdesini, izlenen verilerin boyutunu, arşivlenmiş verilerin boyutunu ve izlenen ancak henüz arşivlenmemiş verilerin boyutunu görüntüleyebilirsiniz. Ayrıca, en son ve bir sonraki arşivlemelerin gerçekleşme tarihlerini de görüntüleyebilirsiniz.

Yedekleme etkinliğinizin özetini görüntülemek için:

- 1 Yerel Arşiv sekmesini tıklatın.
- 2 Ekranın üst bölümündeki **Hesap Özeti**'ni tıklatın.

B Ö L Ü M 3 7

McAfee QuickClean

QuickClean, bilgisayarınızda dağınıklığa neden olabilecek dosyaları silerek bilgisayarınızın performansını geliştirir. Geri Dönüşüm Kutusu'nu boşaltır ve geçici dosyaları, kısayolları, kayıp dosya parçalarını, kayıt defteri dosyalarını, önbellek dosyalarını, tanımlama bilgilerini, tarayıcı geçmişi dosyalarını, gönderilen ve silinen e-postaları, en son kullanılan dosyaları, Active-X dosyalarını ve sistem geri yükleme noktası dosyalarını siler. QuickClean, adınız ve adresiniz gibi hassas ve kişisel bilgiler içerebilen öğeleri güvenli ve kalıcı şekilde silmek için McAfee Shredder bileşenini kullanarak gizliliğinizi de korur. Dosyaları parçalama hakkında bilgi için bkz. McAfee Shredder.

Disk Birleştirici, bilgisayarınızdaki dosya ve klasörleri düzenleyerek, bilgisayarınızın sabit diskine kaydedildiklerinde bunların dağılmamalarını (parçalanmamalarını) sağlar. Sabit diskinizi düzenli olarak birleştirdiğinizde, bu parçalanmış dosya ve klasörleri daha sonra hızla çağrılacak şekilde bir araya getirirsiniz.

Bilgisayarınıza el ile bakım yapmak istemiyorsanız, hem QuickClean hem de Disk Birleştirici uygulamalarını, istediğiniz sıklıkta bağımsız görevler halinde otomatik olarak çalışacak şekilde zamanlayabilirsiniz.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

QuickClean özellikleri	190
Bilgisayarınızı temizleme	191
Bilgisayarınızı birleştirme	194
Görev zamanlama	195

QuickClean özellikleri

QuickClean, gereksiz dosyaları güvenli ve etkili olarak silen çeşitli temizleyiciler içerir. Bu dosyaları sildiğinizde, bilgisayarınızın sabit diskinde alan kazanır ve performansını geliştirirsiniz.

Bilgisayarınızı temizleme

QuickClean, bilgisayarınızda dağınıklığa neden olabilecek dosyaları siler. Geri Dönüşüm Kutusu'nu boşaltır ve geçici dosyaları, kısayolları, kayıp dosya parçalarını, kayıt defteri dosyalarını, önbellek dosyalarını, tanımlama bilgilerini, tarayıcı geçmiş dosyalarını, gönderilen ve silinen e-postaları, en son kullanılan dosyaları, Active-X dosyalarını ve sistem geri yükleme noktası dosyalarını siler. QuickClean, bu öğeleri diğer gerekli bilgileri etkilemeden siler.

Bilgisayarınızdan gereksiz dosyaları silmek için QuickClean'in temizleyicilerinden herhangi birini kullanabilirsiniz. Aşağıdaki tabloda QuickClean temizleyicileri açıklanmaktadır:

Ad	İşlev
Geri Dönüşüm Kutusu Temizleyicisi	Geri Dönüşüm Kutusu'ndaki dosyaları siler.
Geçici Dosya Temizleyicisi	Geçici klasörlerinizde saklanan dosyaları siler.
Kısayol Temizleyicisi	Bozuk kısayolları ve herhangi bir programla ilişkili olmayan kısayolları siler.
Kayıp Dosya Parçası Temizleyicisi	Bilgisayarınızda kaybolan dosya parçalarını siler.
Kayıt Defteri Temizleyicisi	Bilgisayarınızda artık bulunmayan programların Windows® kayıt defteri bilgilerini siler. Kayıt defteri, Windows'un yapılandırma bilgilerini depoladığı bir veritabanıdır. Kayıt defteri, tüm bilgisayar kullanıcılarının profillerini ve sistem donanımı, yüklenen programlar ve özellik ayarları hakkındaki bilgileri içerir. Windows çalışırken sürekli bu bilgilere başvurur.
Önbellek Temizleyicisi	Siz Web sayfalarında gezinirken biriken önbellek dosyalarını siler. Bu dosyalar, genellikle önbellek klasöründe geçici dosyalar halinde depolanır. Önbellek klasörü, bilgisayarınızda geçici bir depolama alanıdır. Web'de gezinme hızını ve etkinliğini artırmak için tarayıcınız, daha önce görüntülediğiniz bir Web sayfasını önbellekten (uzak sunucu yerine) çağırabilir.

Tanımlama Bilgisi Temizleyicisi	Tanımlama bilgilerini siler. Bu dosyalar, genellikle geçici dosyalar halinde depolanır. Tanımlama bilgisi, genellikle Web'de gezinen kişinin bilgisayarında depolanan ve kullanıcı adı ve geçerli tarih ve saat gibi bilgiler içeren küçük bir dosyadır. Tanımlama bilgileri, Web siteleri tarafından genellikle siteye önceden kaydolun veya siteyi ziyaret eden kullanıcıları tanımlamak için kullanılır; ancak bunlar, korsanlar için bilgi kaynağı da olabilir.
Tarayıcı Geçmiş Temizleyicisi	Web tarayıcısı geçmişinizi siler.
Outlook Express ve Outlook E-posta Temizleyicisi (gönderilmiş ve silinmiş öğeler)	Outlook® ve Outlook Express'ten gönderilmiş ve silinmiş öğeleri siler.
Son Kullanılanlar Temizleyicisi	Şu programlardan herhangi birinde oluşturulan son kullanılan dosyaları siler: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX Temizleyicisi	ActiveX denetimlerini siler. ActiveX, programla veya Web sayfasıyla bütünleşip onun doğal bir parçası gibi görünen, programlar veya Web sayfaları tarafından işlevsellik eklemek üzere kullanılan bir yazılım bileşenidir. Çoğu ActiveX denetimi zararsızdır; ancak bazıları bilgisayarınızdan bilgiler yakalayabilir.
Sistem Geri Yükleme Noktası Temizleyicisi	Eski sistem geri yükleme noktalarını (en sonuncusu dışında) bilgisayarınızdan siler. Sistem geri yükleme noktaları, herhangi bir sorun ortaya çıkarsa önceki duruma geri dönebilmeniz için bilgisayarınızda yapılan değişiklikleri işaretlemek üzere Windows tarafından oluşturulur.

Bilgisayarınızı temizleme

Bilgisayarınızdan gereksiz dosyaları silmek için QuickClean'in temizleyicilerinden herhangi birini kullanabilirsiniz. İşlemi tamamladığınızda, **QuickClean Özeti** altında, temizlik işleminden sonra kazanılan disk alanı miktarını, silinen dosyaların sayısını, bilgisayarınızda en son çalıştırılan QuickClean işleminin tarih ve saatini görüntüleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklatın.
- 2 **McAfee QuickClean** altında **Başlat**'ı tıklatın.
- 3 Aşağıdakilerden birini gerçekleştirin:
 - Listedeki varsayılan temizleyicileri kabul etmek için **İleri**'yi tıklatın.
 - Uygun temizleyicileri seçin veya işaretini kaldırın ve ardından **İleri**'yi tıklatın. Son Kullanılanlar Temizleyicisi'ni seçerseniz, listedeki programlarla en son oluşturulan dosyaları seçmek veya işaretini kaldırmak için **Özellikler** seçeneğini belirleyin ve sonra **Tamam**'ı tıklatın.
 - Varsayılan temizleyicileri geri yüklemek için **Varsayılanları Geri Yükle**'yi ve ardından **İleri**'yi tıklatın.
- 4 Analizi gerçekleştirdikten sonra **İleri**'yi tıklatın.
- 5 Dosya silme işlemi onaylamak için **İleri**'yi tıklatın.
- 6 Aşağıdakilerden birini gerçekleştirin:
 - Varsayılan **Hayır, dosyalarımı standart Windows silme işlemi kullanarak silmek istiyorum**'u kabul etmek için **İleri**'yi tıklatın.
 - **Evet, Shredder kullanarak dosyalarımı güvenli bir şekilde silmek istiyorum**'u tıklatın, geçiş sayısını (en çok 10) belirtin ve sonra **İleri**'yi tıklatın. Büyük miktarda silinecek bilgi varsa, dosya parçalama işlemi uzun sürebilir.
- 7 Temizleme işlemi sırasında herhangi bir dosya veya öge kilitlenirse, bilgisayarınızı yeniden başlatmanız istenebilir. Pencereyi kapatmak için **Tamam**'ı tıklatın.
- 8 **Son**'u tıklatın.

Not: Shredder ile silinen dosyalar kurtarılamaz. Dosyaları parçalama hakkında bilgi için bkz. McAfee Shredder.

Bilgisayarınızı birleştirme

Disk Birleştirici, bilgisayarınızdaki dosya ve klasörleri düzenleyerek, bilgisayarınızın sabit diskine kaydedildiklerinde bunların dağılmamalarını (parçalanmamalarını) sağlar. Sabit diskinizi düzenli olarak birleştirdiğinizde, bu parçalanmış dosya ve klasörleri daha sonra hızla çağırılacak şekilde bir araya getirirsiniz.

Bilgisayarınızı birleştirme

Dosya ve klasörlere daha kolay erişmek ve bunları çağırmak için bilgisayarınızı birleştirebilirsiniz.

- 1 McAfee SecurityCenter bölümünde, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklayın.
- 2 **Disk Birleştirici** altında **Analiz**'i tıklayın.
- 3 Ekran yönergelerini izleyin.

Not: Disk Birleştirici hakkında ayrıntılı bilgi için Windows Yardımı'na bakın.

Görev zamanlama

Görev Zamanlayıcı, QuickClean veya Disk Birleştirici uygulamasının bilgisayarınızdaki çalışma sıklığını otomatikleştirir. Örneğin, QuickClean'i her Pazar günü saat 21:00 'de Geri Dönüşüm Kutusu'nu boşaltması veya Disk Birleştirici'yi her ayın son gününde bilgisayarınızın sabit diskini birleştirmesi için zamanlayabilirsiniz. İstediğiniz zaman bir görev oluşturabilir, bunu değiştirebilir veya silebilirsiniz. Zamanlanan görevin çalışabilmesi için bilgisayarınızda oturum açmış olmanız gerekir. Görev herhangi bir nedenle çalışmazsa, bir sonraki oturum açışınızdan beş dakika sonrası için yeniden zamanlanır.

QuickClean görevi zamanlama

Bir veya birkaç temizleyici kullanarak bilgisayarınızı otomatik olarak temizlemek için QuickClean görevi zamanlayabilirsiniz. İşlem tamamlandığında, **QuickClean Özeti** altında, görevin bir daha çalışmak üzere zamanlandığı tarih ve saati görüntüleyebilirsiniz.

- 1 Görev Zamanlayıcı bölmesini açın.
Nasıl?
 1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklatın.
 2. **Görev Zamanlayıcı** altında **Başlat**'ı tıklatın.
- 2 **Zamanlanacak işlemi seçin** listesinde, **McAfee QuickClean**'i tıklatın.
- 3 Görev adını **Görev adı** kutusuna yazın ve sonra **Oluştur**'u tıklatın.
- 4 Aşağıdakilerden birini gerçekleştirin:
 - Listedeki temizleyicileri kabul etmek için **İleri**'yi tıklatın.
 - Uygun temizleyicileri seçin veya işaretini kaldırın ve sonra **İleri**'yi tıklatın. Son Kullanılanlar Temizleyicisi'ni seçerseniz, listedeki programlarla en son oluşturulan dosyaları seçmek veya işaretini kaldırmak için **Özellikler** seçeneğini belirleyin ve sonra **Tamam**'ı tıklatın.
 - Varsayılan temizleyicileri geri yüklemek için **Varsayılanları Geri Yükle**'yi ve sonra **İleri**'yi tıklatın.
- 5 Aşağıdakilerden birini gerçekleştirin:
 - Varsayılan **Hayır, dosyalarımı standart Windows silme işlemi kullanarak silmek istiyorum**'u kabul etmek için **Zamanlama**'yı tıklatın.
 - **Evet, Shredder kullanarak dosyalarımı güvenli bir şekilde silmek istiyorum**'u tıklatın, geçiş sayısını (en çok 10) belirtin ve sonra **Zamanlama**'yı tıklatın.

- 6 **Zamanlama** iletişim kutusunda, görevin çalışmasını istediğiniz sıklığı seçin ve sonra **Tamam**'ı tıklatın.
- 7 Son Kullanılanlar Temizleyicisi özelliklerinde değişiklik yaptıysanız, bilgisayarınızı yeniden başlatmanız istenebilir. Pencereyi kapatmak için **Tamam**'ı tıklatın.
- 8 **Son**'u tıklatın.

Not: Shredder ile silinen dosyalar kurtarılamaz. Dosyaları parçalama hakkında bilgi için bkz. McAfee Shredder.

QuickClean görevini değiştirme

Programın kullandığı temizleyicileri veya bilgisayarınızda otomatik olarak çalışma sıklığını değiştirmek için zamanlanan bir QuickClean görevinde değişiklik yapabilirsiniz. İşlem tamamlandığında, **QuickClean Özeti** altında, görevin bir daha çalışmak üzere zamanlandığı tarih ve saati görüntüleyebilirsiniz.

- 1 Görev Zamanlayıcı bölmesini açın.
Nasıl?
 1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı**'nı tıklatın.
 2. **Görev Zamanlayıcı** altında **Başlat**'ı tıklatın.
- 2 Zamanlanacak işlemi seçin listesinde, **McAfee QuickClean**'i tıklatın.
- 3 **Varolan bir görev seçin** listesinden görevi seçin ve sonra **Değiştir**'i tıklatın.
- 4 Aşağıdakilerden birini gerçekleştirin:
 - Görevle ilgili seçilen temizleyicileri kabul etmek için **İleri**'yi tıklatın.
 - Uygun temizleyicileri seçin veya işaretini kaldırın ve sonra **İleri**'yi tıklatın. Son Kullanılanlar Temizleyicisi'ni seçerseniz, listedeki programlarla en son oluşturulan dosyaları seçmek veya işaretini kaldırmak için **Özellikler** seçeneğini belirleyin ve sonra **Tamam**'ı tıklatın.
 - Varsayılan temizleyicileri geri yüklemek için **Varsayılanları Geri Yükle**'yi ve ardından **İleri**'yi tıklatın.
- 5 Aşağıdakilerden birini gerçekleştirin:
 - Varsayılan **Hayır, dosyalarımı standart Windows silme işlemi kullanarak silmek istiyorum**'u kabul etmek için **Zamanlama**'yı tıklatın.
 - **Evet, Shredder kullanarak dosyalarımı güvenli bir şekilde silmek istiyorum**'u tıklatın, geçiş sayısını (en çok 10) belirtin ve sonra **Zamanlama**'yı tıklatın.

- 6 **Zamanlama** iletişim kutusunda, görevin çalışmasını istediğiniz sıklığı seçin ve sonra **Tamam**'ı tıklatın.
- 7 Son Kullanılanlar Temizleyicisi özelliklerinde değişiklik yaptıysanız, bilgisayarınızı yeniden başlatmanız istenebilir. Pencereyi kapatmak için **Tamam**'ı tıklatın.
- 8 **Son**'u tıklatın.

Not: Shredder ile silinen dosyalar kurtarılamaz. Dosyaları parçalama hakkında bilgi için bkz. McAfee Shredder.

QuickClean görevini silme

Otomatik olarak çalışmasını istemediğiniz zamanlanan bir QuickClean görevini silebilirsiniz.

- 1 Görev Zamanlayıcı bölmesini açın.
Nasıl?
 1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklatın.
 2. **Görev Zamanlayıcı** altında **Başlat**'ı tıklatın.
- 2 **Zamanlanacak işlemi seçin** listesinde, **McAfee QuickClean**'i tıklatın.
- 3 **Varolan bir görev seçin** listesinden görevi seçin.
- 4 **Sil**'i ve sonra silme işlemi onaylamak için **Evet**'i tıklatın.
- 5 **Son**'u tıklatın.

Disk Birleştirici görevi zamanlama

Bilgisayarınızın sabit diskinin otomatik olarak birleştirilme sıklığını zamanlamak için bir Disk Birleştirici görevi zamanlayabilirsiniz. İşlem tamamlandığında, **Disk Birleştirici** altında, görevin bir daha çalışmak üzere zamanlandığı tarih ve saati görüntüleyebilirsiniz.

- 1 Görev Zamanlayıcı bölmesini açın.
Nasıl?
 1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklatın.
 2. **Görev Zamanlayıcı** altında **Başlat**'ı tıklatın.
- 2 **Zamanlanacak işlemi seçin** listesinde, **Disk Birleştirici**'yi tıklatın.
- 3 Görev adını **Görev adı** kutusuna yazın ve sonra **Oluştur**'u tıklatın.
- 4 Aşağıdakilerden birini gerçekleştirin:
 - Varsayılan **Boş alan az olsa da birleştirmeyi gerçekleştir** seçeneğini kabul etmek için **Zamanlama**'yı tıklatın.

- **Boş alan az olsa da birleştirmeyi gerçekleştir** seçeneğinin işaretini kaldırın ve sonra **Zamanlama**'yı tıklatın.
- 5 **Zamanlama** iletişim kutusunda, görevin çalışmasını istediğiniz sıklığı seçin ve sonra **Tamam**'ı tıklatın.
 - 6 **Son**'u tıklatın.

Disk Birleştirici görevini değiştirme

Programın bilgisayarınızda otomatik olarak çalışma sıklığını değiştirmek için zamanlanan bir Disk Birleştirici görevinde değişiklik yapabilirsiniz. İşlem tamamlandığında, **Disk Birleştirici** altında, görevin bir daha çalışmak üzere zamanlandığı tarih ve saati görüntüleyebilirsiniz.

- 1 Görev Zamanlayıcı bölmesini açın.
Nasıl?
 1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı**'nı tıklatın.
 2. **Görev Zamanlayıcı** altında **Başlat**'ı tıklatın.
- 2 **Zamanlanacak işlemi seçin** listesinde, **Disk Birleştirici**'yi tıklatın.
- 3 **Varolan bir görev seçin** listesinden görevi seçin ve sonra **Değiştir**'i tıklatın.
- 4 Aşağıdakilerden birini gerçekleştirin:
 - Varsayılan **Boş alan az olsa da birleştirmeyi gerçekleştir** seçeneğini kabul etmek için **Zamanlama**'yı tıklatın.
 - **Boş alan az olsa da birleştirmeyi gerçekleştir** seçeneğinin işaretini kaldırın ve sonra **Zamanlama**'yı tıklatın.
- 5 **Zamanlama** iletişim kutusunda, görevin çalışmasını istediğiniz sıklığı seçin ve sonra **Tamam**'ı tıklatın.
- 6 **Son**'u tıklatın.

Disk Birleştirici görevini silme

Otomatik olarak çalışmasını istemediğiniz zamanlanan bir Disk Birleştirici görevini silebilirsiniz.

- 1 Görev Zamanlayıcı bölmesini açın.
Nasıl?

1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı'nı** tıklatın.
2. **Görev Zamanlayıcı** altında **Başlat'**ı tıklatın.
- 2 **Zamanlanacak işlemi seçin** listesinde, **Disk Birleştirici'yi** tıklatın.
- 3 **Varolan bir görev seçin** listesinden görevi seçin.
- 4 **Sil'i** ve sonra silme işlemi onaylamak için **Evet'i** tıklatın.
- 5 **Son'u** tıklatın.

B Ö L Ü M 3 8

McAfee Shredder

McAfee Shredder, öğeleri bilgisayarınızın sabit diskinden kalıcı olarak siler (veya parçalar). Bu dosyaları ve klasörleri el ile sildiğinizde, Geri Dönüşüm Kutusu'nu boşalttığınızda veya Temporary Internet Files klasörünü sildiğinizde bile, bilgisayarın teknik araçlarını kullanarak bu bilgileri kurtarabilirsiniz. Bunun yanı sıra, bazı programlar dosyaların geçici, gizli kopyalarını çıkardığı için silinen bir dosya kurtarılabilir. Shredder, bu istenmeyen dosyaları güvenli ve kalıcı bir şekilde silerek gizliliğinizi korur. Parçalanmış dosyaların geri yüklenemediğini unutmayın.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Shredder özellikleri	202
Dosyaları, klasörleri ve diskleri parçalama	203

Shredder özellikleri

Shredder tarafından bilgisayarınızın sabit diskinden silinen öğelerle ilişkili bilgiler kurtarılamaz. Bu program, dosyaları ve klasörleri, Geri Dönüşüm Kutusu ve Temporary Internet Files klasöründeki öğeleri ve yeniden yazılabilir CD'ler, harici sabit diskler ve disketler gibi bilgisayar disklerinin tüm içeriklerini güvenli ve kalıcı şekilde silerek gizliliğinizi korur.

Dosyaları, klasörleri ve diskleri parçalama

Shredder, Geri Dönüşüm Kutusu ve Temporary Internet Files klasöründeki silinen dosya ve klasörlerde bulunan bilgilerin, özel araçlarla bile kurtarılamamasını güvence altına alır. Shredder ile bir öğenin kaç kez (en çok 10) parçalanmasını istediğinizi belirtebilirsiniz. Parçalama sayısı arttıkça, güvenli dosya silme düzeyi de artar.

Dosya ve klasörleri parçalama

Geri Dönüşüm Kutusu ve Temporary Internet Files klasöründe bulunan öğeler dahil olmak üzere, bilgisayarınızın sabit diskindeki dosya ve klasörleri parçalayabilirsiniz.

1 Shredder'ı açın.

Nasıl?

1. McAfee SecurityCenter bölmesinde, **Ortak Görevler** altında, **Gelişmiş Menü**'yü tıklatın.
2. Soldaki bölmede **Araçlar**'ı tıklatın.
3. **Shredder**'ı tıklatın.

2 Dosya ve klasörleri parçala bölümünde, **Şunu yapmak istiyorum** altında, **Dosya ve klasörleri silmek** seçeneğini tıklatın.

3 **Parçalama Düzeyi** altında, aşağıdaki parçalama düzeylerinden birini tıklatın:

- **Hızlı:** Seçilen öğeleri bir kez parçalar.
- **Kapsamlı:** Seçilen öğeleri 7 kez parçalar.
- **Özel:** Seçilen öğeleri en fazla 10 kez parçalar.

4 **İleri**'yi tıklatın.

5 Aşağıdakilerden birini gerçekleştirin:

- **Parçalanacak dosyaları seçin** listesinde, **Geri Dönüşüm Kutusu içeriği** veya **Geçici Internet dosyaları** seçeneğini tıklatın.
- **Gözet**'i tıklatın, parçalamak istediğiniz dosyaya gidip seçin ve sonra **Aç**'i tıklatın.

6 **İleri**'yi tıklatın.

7 **Başlat**'i tıklatın.

8 Shredder işlemi tamamlayınca **Bitti**'yi tıklatın.

Not: Shredder görevi tamamlayıncaya dek lütfen hiçbir dosyayla çalışmayın.

Tüm diski parçalama

Bir diskin tüm içeriğini aynı anda silebilirsiniz. Yalnızca harici sabit diskler, yazılabilir CD'ler ve disketler gibi çıkarılabilir sürücüler parçalanabilir.

1 Shredder'ı açın.

Nasıl?

1. McAfee SecurityCenter bölmesinde, **Ortak Görevler** altında, **Gelişmiş Menü'yü** tıklatın.
2. Soldaki bölmede **Araçlar'ı** tıklatın.
3. **Shredder'ı** tıklatın.

2 Dosya ve klasörleri parçala bölümünde, **Şunu yapmak istiyorum** altında, **Tüm diski silmek** seçeneğini tıklatın.

3 Parçalama Düzeyi altında, aşağıdaki parçalama düzeylerinden birini tıklatın:

- **Hızlı:** Seçilen sürücüyü bir kez parçalar.
- **Kapsamlı:** Seçilen sürücüyü 7 kez parçalar.
- **Özel:** Seçilen sürücüyü en fazla 10 kez parçalar.

4 İleri'yi tıklatın.

5 Diski seçin listesinde, parçalamak istediğiniz sürücüyü tıklatın.

6 İleri'yi ve sonra seçiminizi onaylamak için **Evet'i** tıklatın.

7 Başlat'ı tıklatın.

8 Shredder işlemi tamamlayınca **Bitti'yi** tıklatın.

Not: Shredder görevi tamamlayıncaya dek lütfen hiçbir dosyayla çalışmayın.

B Ö L Ü M 39

McAfee Network Manager

Network Manager, ev ađınızı oluřturan bilgisayarların ve bileřenlerin grafiksel görünümünü sunar. Network Manager'ı kullanarak, ađınızda yönetilen tüm bilgisayarların koruma durumunu uzaktan izleyebilir ve bu bilgisayarlarla ilgili raporlanan güvenlik açıklarını uzaktan düzeltebilirsiniz.

Network Manager'ı kullanmadan önce, bu özelliklerden bazıları hakkında bilgi edinebilirsiniz. Bu özelliklerin yapılandırılması ve kullanımıyla ilgili ayrıntılar, Network Manager yardımında sunulmaktadır.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladıđı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Network Manager özellikleri.....	206
Network Manager simgeleri hakkında bilgi	207
Yönetilen bir ađ kurma.....	209
Ađı uzaktan yönetme	215

Network Manager özellikleri

Network Manager, aşağıdaki özellikleri sunar.

Grafiksel ağ haritası

Network Manager'ın ağ haritası, ev ağını oluşturan bilgisayarlarla bileşenlerin korunma durumuna ilişkin grafiksel görünümü sunar. Ağınızda değişiklikler yaptığınızda (örneğin bilgisayar eklediğinizde), ağ haritası bu değişiklikleri tanır. Ağ haritasını yenileyebilir, ağın adını değiştirebilir ve görünümü özelleştirmek için ağ haritasının bileşenlerini gösterebilir veya gizleyebilirsiniz. Ayrıca, ağ haritasında gösterilen herhangi bir bileşenle ilgili ayrıntıları da görüntüleyebilirsiniz.

Uzaktan yönetme

Network Manager'ın ağ haritasını kullanarak, ev ağını oluşturan bilgisayarların korunma durumunu yönetin. Yönetilen ağa katılması için bir bilgisayarı davet edebilir, yönetilen bilgisayarın koruma durumunu izleyebilir ve ağdaki uzak bir bilgisayardan bilinen güvenlik açıklarını düzeltebilirsiniz.

Network Manager simgeleri hakkında bilgi

Aşağıdaki tabloda, Network Manager ağ haritasında yaygın olarak kullanılan simgeler açıklanmaktadır.

Simge	Açıklama
	Çevrimiçi ve yönetilen bir bilgisayarı temsil eder
	Çevrimdışı ve yönetilen bir bilgisayarı temsil eder
	SecurityCenter yüklenmiş yönetilmeyen bir bilgisayarı temsil eder
	Çevrimdışı ve yönetilmeyen bir bilgisayarı temsil eder
	SecurityCenter yüklenmemiş çevrimiçi bir bilgisayarı veya bilinmeyen bir ağ aygıtını temsil eder
	SecurityCenter yüklenmemiş çevrimdışı bir bilgisayarı veya bilinmeyen çevrimdışı bir ağ aygıtını temsil eder
	Karşılık gelen öğenin korunduğunu ve bağlı olduğunu gösterir
	Karşılık gelen öğeyle ilgilenmeniz gerekebileceğini gösterir
	Karşılık gelen öğeyle hemen ilgilenmeniz gerektiğini gösterir
	Kablosuz ev yönlendiricisini temsil eder
	Standart ev yönlendiricisini temsil eder
	İnternet'in bağlı olduğunu gösterir
	İnternet bağlantısının kesildiğini gösterir

B Ö L Ü M 4 0

Yönetilen bir ağ kurma

Yönetilen bir ağ kurmak için ağ haritanızdaki öğelerle çalışın ve bu ağa üyeler (bilgisayarlar) ekleyin. Bir bilgisayarın uzaktan yönetilebilmesi veya ağdaki diğer bilgisayarları uzaktan yönetme izni alabilmesi için bu bilgisayar ağın güvenilen bir üyesi olmalıdır. Ağ üyeliği, yeni bilgisayarlara yönetici izinlerine sahip mevcut ağ üyeleri (bilgisayarlar) tarafından sağlanır.

Ağınızda değişiklik yapsanız (örneğin bilgisayar ekleseniz) bile, ağ haritasında gösterilen herhangi bir bileşenle ilgili ayrıntıları görüntüleyebilirsiniz.

Bu bölümde

Ağ haritasıyla çalışma.....	210
Yönetilen ağa katılma	212

Ağ haritasıyla çalışma

Ağa bilgisayar bağladığınızda, Network Manager yönetilen veya yönetilmeyen herhangi bir üye olup olmadığını, yönlendirici özneliklerini ve Internet durumunu belirlemek için ağı analiz eder. Herhangi bir üye bulunamazsa, Network Manager bağlı olan bu bilgisayarın ağdaki ilk bilgisayar olduğunu varsayar ve bu bilgisayarı yönetici izinlerine sahip yönetilen bir üye yapar. Varsayılan olarak, ağ adı SecurityCenter yüklenmiş ağı bağlanan ilk bilgisayarın çalışma grubu veya etki alanı adını içerir; ancak istediğiniz zaman ağın adını değiştirebilirsiniz.

Ağınızda değişiklikler yaptığınızda (örneğin bilgisayar eklediğinizde), ağ haritasını özelleştirebilirsiniz. Örneğin, ağ haritasını yenileyebilir, ağın adını değiştirebilir ve görünümü özelleştirmek için ağ haritasının bileşenlerini gösterebilir veya gizleyebilirsiniz. Ayrıca, ağ haritasında gösterilen herhangi bir bileşenle ilgili ayrıntıları da görüntüleyebilirsiniz.

Ağ haritasına erişme

Ağ haritası, ev ağınıza oluşturan bilgisayarların ve bileşenlerin grafiksel anlatımını sunar.

- Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklayın.

Not: Ağ haritasına ilk eriştiğinizde, ağdaki diğer bilgisayarlara güvenmeniz istenir.

Ağ haritasını yenileme

Ağ haritasını istediğiniz zaman, örneğin yönetilen ağı başka bir bilgisayar katıldıktan sonra yenileyebilirsiniz.

- 1 Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklayın.
- 2 **Şunu yapmak istiyorum** bölümünde **Ağ haritasını yenile**'yi tıklayın.

Not: **Ağ haritasını yenile** bağlantısı, yalnızca ağ haritasında hiç seçili öğe yoksa kullanılabilir. Bir öğenin seçimini kaldırmak için seçili öğeyi tıklayın veya ağ haritası üzerinde beyaz bir alanı tıklayın.

Ağın adını değiştirme

Varsayılan olarak, ağ adı SecurityCenter yüklü olan ve ağa bağlanan ilk bilgisayarın çalışma grubu veya etki alanı adını içerir. Farklı bir ad kullanmayı tercih ederseniz bunu değiştirebilirsiniz.

- 1 Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklayın.
- 2 **Şunu yapmak istiyorum** bölümünde **Ağın adını değiştir**'i tıklayın.
- 3 **Ağ Adı** kutusuna ağın adını yazın.
- 4 **Tamam**'ı tıklayın.

Not: **Ağın adını değiştir** bağlantısı, yalnızca ağ haritasında hiç seçili öğe yoksa kullanılabilir. Bir öğenin seçimini kaldırmak için seçili öğeyi tıklayın veya ağ haritası üzerinde beyaz bir alanı tıklayın.

Ağ haritasında öğeyi gösterme veya gizleme

Varsayılan olarak, ev ağınızdaki tüm bilgisayarlar ve bileşenler ağ haritasında görüntülenir. Ancak öğeleri gizlediyseniz, bunları istediğiniz zaman yeniden gösterebilirsiniz. Yalnızca yönetilmeyen öğeler gizlenebilir; yönetilen bilgisayarlar gizlenemez.

Bunu yapmak için...	Temel veya Gelişmiş Menü'de Ağı Yönet 'i tıklayın ve ardından bunu yapın...
Ağ haritasında bir öğeyi gizlemek	Ağ haritasında bir öğeyi tıklayın ve ardından Şunu yapmak istiyorum bölümünde Bu öğeyi gizle 'yi tıklayın. Onay iletişim kutusunda Evet 'i tıklayın.
Ağ haritasında öğeleri göstermek	Şunu yapmak istiyorum bölümünde Gizli öğeleri göster 'i tıklayın.

Öğenin ayrıntılarını görüntüleme

Ağ haritasında seçerek, ağınızdaki herhangi bir bileşenle ilgili ayrıntılı bilgi görüntüleyebilirsiniz. Bu bilgiler bileşen adını, koruma durumunu ve bileşeni yönetmek için gerekli diğer bilgileri içerir.

- 1 Ağ haritasında öğenin simgesini tıklayın.
- 2 **Ayrıntılar** bölümünde, öğe hakkındaki bilgileri görüntüleyin.

Yönetilen ağa katılma

Bir bilgisayarın uzaktan yönetilebilmesi veya ağdaki diğer bilgisayarları uzaktan yönetme izni alabilmesi için bu bilgisayar ağın güvenilen bir üyesi olmalıdır. Ağ üyeliği, yeni bilgisayarlara yönetici izinlerine sahip mevcut ağ üyeleri (bilgisayarlar) tarafından sağlanır. Yalnızca güvenilen bilgisayarların ağa bağlanmasını sağlamak için, ağa katılan ve üyeliği veren bilgisayarlar birbirlerinin kimliğini doğrulamalıdır.

Bir bilgisayar ağa katıldığında, ondan McAfee koruma durumunu ağdaki diğer bilgisayarlara göstermesi istenir. Bilgisayar koruma durumunu göstermeyi kabul ederse, ağın yönetilen bir üyesi olur. Bilgisayar koruma durumunu göstermeyi kabul etmezse, ağın yönetilmeyen bir üyesi olur. Ağın yönetilmeyen üyeleri, genellikle başka ağ özelliklerine erişmek (örneğin, dosyalar göndermek veya yazıcıları paylaşmak) isteyen konuk bilgisayarlardır.

Not: Ağa katıldıktan sonra, başka McAfee ağ programları yüklenmişse (örneğin EasyNetwork), bilgisayarınız bu programlar tarafından da yönetilen bir bilgisayar olarak tanınır. Network Manager'da bir bilgisayara atanan izin düzeyi, tüm McAfee ağ programlarında geçerlidir. Diğer McAfee ağ programlarında konuk, tam veya yönetici izinlerinin anlamları hakkında ayrıntılı bilgi için o programlarla birlikte sağlanan belgelere bakın.

Yönetilen bir ağa katılma

Yönetilen bir ağa katılmak için davet aldığınızda, bunu kabul veya reddedebilirsiniz. Ayrıca bu bilgisayarın ve ağdaki diğer bilgisayarların birbirlerinin güvenlik ayarlarını (örneğin bir bilgisayarın virüsten korunma hizmetlerinin güncelleştirme düzeyini) izlemelerini isteyip istemediğinizi de belirleyebilirsiniz.

- 1 Yönetilen Ağ iletişim kutusunda, **Bu ağdaki her bilgisayarın güvenlik ayarlarını izlemesine izin ver** onay kutusunun işaretli olduğundan emin olun.
- 2 **Katıl**'ı tıklatın.
Daveti kabul ettiğinizde, iki oyun kartı görüntülenir.
- 3 Oyun kartlarının, sizi yönetilen ağa katılmak üzere davet eden bilgisayarda görüntülenen kartlarla aynı olduğunu doğrulayın.
- 4 **Tamam**'ı tıklatın.

Not: Sizi yönetilen ağa katılmak üzere davet eden bilgisayar, güvenlik onayı iletişim kutusunda görüntülenen oyun kartlarıyla aynı kartları görüntülemeyse, yönetilen ağ üzerinde bir güvenlik ihlali olmuştur. Ağa katılırsanız bilgisayarınız risk altına girebilir; bu nedenle, Yönetilen Ağ iletişim kutusunda **İptal**'i tıklatın.

Bir bilgisayarı yönetilen ağa katılmaya davet etme

Yönetilen ağa bir bilgisayar eklenirse veya ağ üzerinde başka bir yönetilmeyen bilgisayar varsa, bu bilgisayarı yönetilen ağa katılmak üzere davet edebilirsiniz. Yalnızca ağ üzerinde yönetici izinlerine sahip bilgisayarlar diğer bilgisayarları katılmaya davet edebilir. Daveti gönderdiğinizde, katılacak olan bilgisayara atamak istediğiniz izin düzeyini de belirtebilirsiniz.

- 1 Ağ haritasında yönetilmeyen bilgisayarın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Bu bilgisayarı izle**'yi tıklatın.
- 3 Bir bilgisayarı yönetilen ağa katılmaya davet et iletişim kutusunda, aşağıdakilerden birini yapın:
 - Bilgisayarın ağa erişmesine izin vermek için **Yönetilen ağ programlarına konuk erişim izni ver**'i tıklatın (bu seçeneği, evinizdeki geçici kullanıcılar için kullanabilirsiniz).
 - Bilgisayarın ağa erişmesine izin vermek için **Yönetilen ağ programlarına tam erişim izni ver**'i tıklatın.
 - Bilgisayarın ağa yönetici haklarıyla erişmesine izin vermek için **Yönetilen ağ programlarına yönetici erişim izni ver**'i tıklatın. Bu, bilgisayarın yönetilen ağa katılmak isteyen diğer bilgisayarlara erişim sağlamasına da olanak verir.
- 4 **Tamam**'i tıklatın.
Bilgisayara, yönetilen ağa katılması için davet gönderilir.
Bilgisayar daveti kabul ettiğinde, iki oyun kartı görüntülenir.
- 5 Oyun kartlarının, yönetilen ağa katılmak üzere davet ettiğiniz bilgisayarda görüntülenen kartlarla aynı olduğunu doğrulayın.
- 6 **Erişim İzni Ver**'i tıklatın.

Not: Yönetilen ağa katılmak üzere davet ettiğiniz bilgisayar, güvenlik onayı iletişim kutusunda görüntülenen oyun kartlarıyla aynı kartları görüntülemese, yönetilen ağ üzerinde bir güvenlik ihlali olmuştur. Bilgisayarın ağa katılmasına izin vererseniz diğer bilgisayarlar risk altına girebilir; bu nedenle, güvenlik onayı iletişim kutusunda **Erişimi Reddet**'i tıklatın.

Ağdaki bilgisayarlara güvenmeyi durdurma

Ağdaki diğer bilgisayarlara yanlışlıkla güvendiyseniz, bunlara güvenmeyi durdurabilirsiniz.

- **Şunu yapmak istiyorum** altında **Bu ağdaki bilgisayarlara güvenmeyi durdur'u** tıklatın.

Not: Yönetici izinleriniz varsa ve ağda başka yönetilen bilgisayarlar bulunuyorsa, **Bu ağdaki bilgisayarlara güvenmeyi durdur** bağlantısı kullanılamaz.

B Ö L Ü M 4 1

Ağı uzaktan yönetme

Yönetilen ağınıza kurduktan sonra, ağınıza oluşturan bilgisayarları ve bileşenleri uzaktan yönetebilirsiniz. Bilgisayarların ve bileşenlerin durumunu ve izin düzeylerini izleyebilir; güvenlik açıklarının çoğunu uzaktan düzeltebilirsiniz.

Bu bölümde

Durumu ve izinleri izleme.....	216
Güvenlik açıklarını düzeltme.....	218

Durumu ve izinleri izleme

Yönetilen bir ağın yönetilen ve yönetilmeyen üyeleri vardır. Yönetilen üyeler, McAfee koruma durumlarının ağdaki diğer bilgisayarlar tarafından izlenmesine izin verirler; yönetilmeyen üyeler buna izin vermezler. Yönetilmeyen üyeler, genellikle başka ağ özelliklerine erişmek (örneğin, dosyalar göndermek veya yazıcıları paylaşmak) isteyen konuk bilgisayarlardır. Yönetilmeyen bir bilgisayar, herhangi bir zamanda ağdaki yönetilen başka bir bilgisayar tarafından yönetilen bir üye olmak üzere davet edilebilir. Benzer şekilde, yönetilen bir bilgisayar da herhangi bir zamanda yönetilmeyen üye olabilir.

Yönetilen bilgisayarlar yönetici, tam veya konuk izinlerine sahiptir. Yönetici izinleri, yönetilen bilgisayarın ağdaki diğer tüm bilgisayarların koruma durumunu yönetmesine ve diğer bilgisayarlara ağ üzerinde üyelik sağlamasına olanak verir. Tam ve konuk izinleri, bilgisayarın yalnızca ağa erişmesine olanak verir. Bir bilgisayarın izin düzeyini herhangi bir zamanda değiştirebilirsiniz.

Yönetilen bir ağda aygıtlar da (örneğin yönlendiriciler) olabileceği için bunları yönetmek için Network Manager'ı kullanabilirsiniz. Ayrıca, bir aygıtın görüntü özelliklerini ağ haritasında yapılandırabilir veya değiştirebilirsiniz.

Bir bilgisayarın koruma durumunu izleme

Bir bilgisayarın koruma durumu ağ üzerinde izlenmiyorsa (bilgisayar ağın üyesi değilse veya ağın yönetilmeyen bir üyesiye), onu izlemek için istekte bulunabilirsiniz.

- 1 Ağ haritasında yönetilmeyen bilgisayarın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Bu bilgisayarı izle**'yi tıklatın.

Bir bilgisayarın koruma durumunu izlemeyi durdurma

Ağınızda yönetilen bir bilgisayarın koruma durumunu izlemeyi durdurabilirsiniz; ancak bu durumda bilgisayar yönetilmeyen üye olur ve koruma durumunu uzaktan izleyemezsiniz.

- 1 Ağ haritasında yönetilen bilgisayarın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Bu bilgisayarı izlemeyi durdur**'u tıklatın.
- 3 Onay iletişim kutusunda **Evet**'i tıklatın.

Yönetilen bir bilgisayarın izinlerini değiştirme

Yönetilen bir bilgisayarın izinlerini herhangi bir zamanda değiştirebilirsiniz. Bu, ağdaki diğer bilgisayarların koruma durumunu izleyebilen bilgisayarları değiştirmenize olanak verir.

- 1 Ağ haritasında yönetilen bilgisayarın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Bu bilgisayardaki izinleri değiştir**'i tıklatın.
- 3 İzinleri değiştirme iletişim kutusunda, bu bilgisayarla yönetilen ağdaki diğer bilgisayarların birbirlerinin koruma durumunu izleyip izleyemeyeceklerini belirlemek için, onay kutusunu seçin veya temizleyin.
- 4 **Tamam**'ı tıklatın.

Bir aygıtı yönetme

Network Manager'dan yönetici Web sayfasına erişerek, bir aygıtı yönetebilirsiniz.

- 1 Ağ haritasında aygıtın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Bu aygıtı yönet**'i tıklatın. Bir Web tarayıcısı açılır ve aygıtın yönetici Web sayfasını görüntüler.
- 3 Web tarayıcınızda oturum açma bilgilerini sağlayın ve aygıtın güvenlik ayarlarını yapılandırın.

Not: Aygıt Wireless Network Security tarafından korunan bir kablosuz yönlendirici veya erişim noktasıysa, aygıtın güvenlik ayarlarını yapılandırmak için Wireless Network Security kullanmanız gerekir.

Bir aygıtın görüntü özelliklerini değiştirme

Bir aygıtın görüntü özelliklerini değiştirdiğinizde, ağ haritasında aygıtın görüntü adını değiştirebilir ve aygıtın kablosuz yönlendirici olup olmadığını belirtebilirsiniz.

- 1 Ağ haritasında aygıtın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** bölümünde **Aygıt özelliklerini değiştir**'i tıklatın.
- 3 Aygıtın görüntü adını belirtmek için, **Ad** kutusuna bir ad yazın.
- 4 Aygıtın türünü belirtirken, aygıt kablosuz yönlendirici değilse **Standart Yönlendirici**'yi, kablosuzsa **Kablosuz Yönlendirici**'yi tıklatın.
- 5 **Tamam**'ı tıklatın.

Güvenlik açıklarını düzeltme

Yönetici izinlerine sahip yönetilen bilgisayarlar, ağdaki diğer yönetilen bilgisayarların McAfee koruma durumunu izleyebilir ve raporlanan güvenlik açıklarını uzaktan düzeltebilir. Örneğin, yönetilen bir bilgisayarın McAfee koruma durumu VirusScan'ın devre dışı olduğunu gösteriyorsa, yönetici izinlerine sahip başka bir yönetilen bilgisayar VirusScan'ı uzaktan etkinleştirebilir.

Güvenlik açıklarını uzaktan düzelttiğinizde, Network Manager en çok raporlanan sorunları onarır. Ancak bazı güvenlik açıkları, yerel bilgisayarda el ile müdahale gerektirebilir. Bu durumda, Network Manager uzaktan onarılabilen sorunları düzeltir ve daha sonra geri kalan sorunları, tehditlere açık bilgisayarda SecurityCenter oturumu açıp size sağlanan önerileri izleyerek düzeltmenizi ister. Bazen çözüm olarak, uzak bilgisayara veya ağınızdaki bilgisayarlara SecurityCenter'ın en son sürümünü yüklemeniz önerilebilir.

Güvenlik açıklarını düzeltme

Network Manager'ı kullanarak, yönetilen uzak bilgisayarlarda pek çok güvenlik açığını düzeltebilirsiniz. Örneğin, uzak bilgisayarda VirusScan devre dışıysa bunu etkinleştirebilirsiniz.

- 1 Ağ haritasında ögenin simgesini tıklatın.
- 2 **Ayrıntılar** bölümünde, ögenin koruma durumunu görüntüleyin.
- 3 **Şunu yapmak istiyorum** bölümünde **Güvenlik açıklarını düzelt**'i tıklatın.
- 4 Güvenlik açıkları düzeltilince, **Tamam**'ı tıklatın.

Not: Network Manager pek çok güvenlik açığını otomatik olarak düzeltir, ancak bazı onarımlarda tehditlere açık bilgisayarda SecurityCenter'ı açıp size sağlanan önerileri izlemeniz gerekebilir.

Uzak bilgisayarlara McAfee güvenlik yazılımı yükleme

Ağınızdaki bir veya daha fazla bilgisayar SecurityCenter'ın en son sürümünü kullanmıyorsa, bunların koruma durumu uzaktan izlenemez. Bu bilgisayarları uzaktan izlemek istiyorsanız, her bilgisayara tek tek SecurityCenter'ın en son sürümünü yüklemeniz gerekir.

- 1 Güvenlik yazılımınızı yüklemek istediğiniz bilgisayarda SecurityCenter'ı açın.
- 2 **Ortak Görevler** altında **Hesabım**'ı tıklatın.
- 3 İlk yüklediğinizde güvenlik yazılımınızı kaydettirmek için kullandığınız e-posta adresi ve parolayla oturum açın.
- 4 Uygun ürünü seçin, **Yükle/Kur** simgesini tıklatın ve sonra ekran yönergelerini izleyin.

B Ö L Ü M 4 2

McAfee EasyNetwork

EasyNetwork, dosyaları güvenli şekilde paylaşmanıza, dosya aktarımlarını basitleştirmenize ve ev ağınızdaki bilgisayarlar arasında yazıcıları paylaşmanıza olanak verir. Ancak program özelliklerine erişebilmeniz için ağınızdaki bilgisayarlarda EasyNetwork yüklü olmalıdır.

EasyNetwork'ü kullanmadan önce, bu özelliklerden bazıları hakkında bilgi edinebilirsiniz. Bu özelliklerin yapılandırılması ve kullanımıyla ilgili ayrıntılar, EasyNetwork yardımında sunulmaktadır.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

EasyNetwork özellikleri.....	220
EasyNetwork'ü ayarlama	221
Dosyaları paylaşma ve gönderme	227
Yazıcıları paylaşma	233

EasyNetwork özellikleri

EasyNetwork aşağıdaki özellikleri sunar.

Dosya paylaşımı

EasyNetwork, dosyaları ağınızdaki diğer bilgisayarlarla paylaşmanızı kolaylaştırır. Dosyaları paylaşırken, diğer bilgisayarlara bu dosyalar için salt okunur erişim izni verirsiniz. Yalnızca yönetilen ağınızda tam veya yönetici erişimine sahip bilgisayarlar (üyeler), diğer üyeler tarafından paylaşılan dosyaları paylaşabilir veya bunlara erişebilirler.

Dosya aktarımı

Yönetilen ağınızda tam veya yönetici erişimine sahip diğer bilgisayarlara (üyelere) dosyalar gönderebilirsiniz. Bir dosya aldığınızda, bu EasyNetwork gelen kutusunda görüntülenir. Gelen kutusu, ağdaki diğer bilgisayarların size gönderdiği tüm dosyalar için geçici bir depolama konumudur.

Otomatik yazıcı paylaşımı

Yönetilen bir ağa katıldığınızda, varsa bilgisayarınıza bağlı yerel yazıcıları, paylaşılan yazıcı adı için yazıcının geçerli adını kullanarak diğer üyelerle paylaşabilirsiniz. Ayrıca, ağınızdaki diğer bilgisayarlar tarafından paylaşılan yazıcıları algılar; bu yazıcıları yapılandırmanıza ve kullanmanıza olanak verir.

B Ö L Ü M 4 3

EasyNetwork'ü ayarlama

EasyNetwork'ü kullanabilmek için önce programı açıp yönetilen ağa katılmanız gerekir. Yönetilen ağa katıldıktan sonra, dosyaları ağdaki diğer bilgisayarlarla paylaşabilir, arayabilir ve bunlara gönderebilirsiniz. Yazıcıları da paylaşabilirsiniz. Ağı terk etmeye karar vererseniz, bunu istediğiniz zaman yapabilirsiniz.

Bu bölümde

EasyNetwork'ü açma	221
Yönetilen bir ağa katılma	222
Yönetilen ağı terk etme.....	226

EasyNetwork'ü açma

Varsayılan olarak, yüklemeyi bitirdikten sonra EasyNetwork'ü açmanız istenir; ancak EasyNetwork'ü daha sonra da açabilirsiniz.

- **Başlat** menüsünde **Programlar**'a gelin, **McAfee**'ye gelin ve ardından **McAfee EasyNetwork**'ü tıklayın.

İpucu: Yükleme sırasında masaüstü ve hızlı başlatma simgeleri oluşturduysanız, masaüstünüzde veya görev çubuğunuzun sağ ucundaki bildirim alanında bulunan McAfee EasyNetwork simgesini çift tıklayarak da EasyNetwork'ü açabilirsiniz.

Yönetilen bir ağa katılma

Bağlı olduğunuz ağdaki hiçbir bilgisayarda SecurityCenter yoksa, ağa üye olursunuz ve sizden bu ağın güvenilen bir ağ olup olmadığını tanımlamanız istenir. Ağa katılan ilk bilgisayar olduğu için bilgisayarınızın adı ağ adına eklenir; ancak istediğiniz zaman ağın adını değiştirebilirsiniz.

Ağa bir bilgisayar bağlandığında, ağ üzerindeki diğer tüm bilgisayarlara bir katılma isteği gönderir. Bu katılma isteğini, ağ üzerinde yönetim izinlerine sahip herhangi bir bilgisayar kabul edebilir. Katılma izni veren bilgisayar, ağa katılan bilgisayarın izin düzeyini de belirleyebilir: örneğin konuk (yalnızca dosya aktarımı) veya tam/yönetici (dosya aktarımı ve dosya paylaşımı). EasyNetwork'te yönetici erişimine sahip bilgisayarlar, diğer bilgisayarlara erişim izni verebilir ve izinleri yönetebilir (bilgisayarların izinlerini yükseltebilir veya düşürebilir); tam erişime sahip bilgisayarlar bu yönetici görevlerini gerçekleştiremez.

Not: Ağa katıldıktan sonra, başka McAfee ağ programları yüklenmişse (örneğin Network Manager), bilgisayarınız bu programlar tarafından da yönetilen bir bilgisayar olarak tanınır. EasyNetwork'te bilgisayara atanan izin düzeyi, tüm McAfee ağ programlarında geçerlidir. Diğer McAfee ağ programlarında konuk, tam veya yönetici izinlerinin anlamları hakkında ayrıntılı bilgi için o programlarla birlikte sağlanan belgelere bakın.

Ağa katılma

EasyNetwork yüklendikten sonra bilgisayar güvenilen ağa ilk kez bağlandığında, yönetilen ağa katılıp katılmayacağını soran bir ileti görüntülenir. Bilgisayar katılmayı kabul ederse, ağ üzerinde yönetici erişimine sahip diğer tüm bilgisayarlara bir istek gönderilir. Bilgisayarın yazıcıları veya dosyaları paylaşabilmesi ya da ağ üzerinde dosyalar gönderebilmesi ve kopyalayabilmesi için, bu isteğin kabul edilmesi gerekir. Ağ üzerindeki ilk bilgisayara, otomatik olarak yönetici izinleri verilir.

- 1 Paylaşılan Dosyalar penceresinde **Bu ağa katıl**'ı tıklatın. Ağdaki yönetici bilgisayar isteğinizi kabul ederse, bu bilgisayar ve ağ üzerindeki diğer bilgisayarlar tarafından güvenlik ayarlarının karşılıklı yönetilmesine izin verip vermediğinizi soran bir ileti görüntülenir.
- 2 Bu bilgisayar ve ağ üzerindeki diğer bilgisayarlar tarafından karşılıklı güvenlik ayarlarının yönetilmesine izin vermek için **Tamam**'ı, reddetmek içinse **İptal**'i tıklatın.
- 3 Ağa katılma izni veren bilgisayarda görüntülenen oyun kartlarıyla, güvenlik onayı iletişim kutusunda görüntülenen kartların aynı olduğunu doğrulayın ve sonra **Tamam**'ı tıklatın.

Not: Sizi yönetilen ağa katılmak üzere davet eden bilgisayar, güvenlik onayı iletişim kutusunda görüntülenen oyun kartlarıyla aynı kartları görüntüleyemezse, yönetilen ağ üzerinde bir güvenlik ihlali olmuştur. Ağa katılırsanız bilgisayarınız risk altına girebilir; bu nedenle, güvenlik onayı iletişim kutusunda **İptal**'i tıklatın.

Ağa erişim izni verme

Bir bilgisayar yönetilen ağa katılmak istediğinde, ağ üzerinde yönetici erişimine sahip diğer bilgisayarlara bir ileti gönderilir. İlk yanıt veren bilgisayar, katılma iznini veren bilgisayardır. Katılma iznini siz veriyorsanız, bilgisayara şu erişim izinlerinden hangisinin verileceğine karar verme sorumluluğu size aittir: konuk, tam veya yönetici.

- 1 Uyarıda, uygun erişim düzeyini tıklatın.
- 2 Bir bilgisayarı yönetilen ağa katılmaya davet et iletişim kutusunda, aşağıdakilerden birini yapın:
 - Bilgisayarın ağa erişmesine izin vermek için **Yönetilen ağ programlarına konuk erişim izni ver**'i tıklatın (bu seçeneği, evinizdeki geçici kullanıcılar için kullanabilirsiniz).
 - Bilgisayarın ağa erişmesine izin vermek için **Yönetilen ağ programlarına tam erişim izni ver**'i tıklatın.
 - Bilgisayarın ağa yönetici haklarıyla erişmesine izin vermek için **Yönetilen ağ programlarına yönetici erişim izni ver**'i tıklatın. Bu, bilgisayarın yönetilen ağa katılmak isteyen diğer bilgisayarlara erişim sağlamasına da olanak verir.

3 **Tamam'**ı tıkladın.

4 Bilgisayarın, güvenlik onayı iletişim kutusunda gösterilen oyun kartlarını görüntülediğini doğrulayın ve sonra **Erişim İzni Ver'i** tıkladın.

Not: Bilgisayarda görüntülenen oyun kartlarıyla güvenlik onayı iletişim kutusunda görüntülenen kartlar aynı değilse, yönetilen ağ üzerinde bir güvenlik ihlali olmuştur. Bu bilgisayara ağa erişim izni verirsiniz bilgisayarınız risk altına girebilir; bu nedenle, güvenlik onayı iletişim kutusunda **Erişimi Reddet'i** tıkladın.

Ağın adını değiştirme

Varsayılan olarak, ağın adı ilk katılan bilgisayarın adını içerir; ancak istediğiniz zaman ağın adını değiştirebilirsiniz. Ağın adını değiştirdiğinizde, EasyNetwork'te görüntülenen ağ açıklamasını da değiştirirsiniz.

- 1 Seçenekler** menüsünde **Yapılandır**'ı tıklatın.
- Yapılandır iletişim kutusunda, **Ağ Adı** kutusuna ağın adını yazın.
- 3 Tamam**'ı tıklatın.

Yönetilen ağı terk etme

Yönetilen bir ağı katıldıktan sonra ağın üyesi olmak istemediğinize karar vererseniz, ağı terk edebilirsiniz. Yönetilen ağı terk ettikten sonra, her zaman yeniden katılabilirsiniz; ancak size yeniden izin verilmesi gerekir. Ağı katılma hakkında ayrıntılı bilgi için bkz. Yönetilen bir ağı katılma (sayfa 222).

Yönetilen ağı terk etme

Daha önceden katılmış olduğunuz yönetilen ağı terk edebilirsiniz.

- 1 **Araçlar** menüsünde **Ağı Terket**'i tıklatın.
- 2 Ağı Terket iletişim kutusunda, terk etmek istediğiniz ağın adını seçin.
- 3 **Ağı Terket**'i tıklatın.

B Ö L Ü M 4 4

Dosyaları paylaşma ve gönderme

EasyNetwork, dosyaları ağdaki diğer bilgisayarlarla paylaşmanızı ve onlara göndermenizi kolaylaştırır. Dosyaları paylaşırken, diğer bilgisayarlara bunlar için salt okunur erişim izni verirsiniz. Yalnızca yönetilen ağın üyesi olan (tam veya yönetici erişimiyle) bilgisayarlar, dosyalar paylaşabilir veya diğer üye bilgisayarlar tarafından paylaşılan dosyalara erişebilir.

Not: Çok sayıda dosya paylaşıyorsanız, bilgisayarınızın kaynakları etkilenebilir.

Bu bölümde

Dosyaları paylaşma	228
Dosyaları diğer bilgisayarlara gönderme	231

Dosyaları paylaşma

Yalnızca yönetilen ağın üyesi olan (tam veya yönetici erişimiyle) bilgisayarlar, dosyalar paylaşabilir veya diğer üye bilgisayarlar tarafından paylaşılan dosyalara erişebilir. Bir klasörü paylaşıyorsanız, bu klasörde bulunan tüm dosyalar ve alt klasörler paylaşılır; ancak klasöre sonradan eklenen dosyalar otomatik olarak paylaşılmaz. Paylaşılan bir dosya veya klasör silinirse, Paylaşılan Dosyalar penceresinden kaldırılır. İstedığınız zaman dosya paylaşımını durdurabilirsiniz.

Paylaşılan bir dosyaya erişmek için dosyayı doğrudan EasyNetwork'ten açın veya bilgisayarınıza kopyalayıp daha sonra buradan açın. Paylaşılan dosyalar listeniz büyükse ve dosyanın nerede olduğunu görmek güçse, bunu arayabilirsiniz.

Not: EasyNetwork ile paylaşılan dosyalara, diğer bilgisayarlardan Windows Gezgini kullanılarak erişilemez, çünkü EasyNetwork dosya paylaşımı güvenli bağlantılar üzerinden gerçekleştirilmelidir.

Dosya paylaşma

Bir dosyayı paylaştığınızda, yönetilen ağ üzerinde tam veya yönetici erişimine sahip tüm üyeler dosyayı kullanabilir.

- 1 Windows Gezgini'nde, paylaşmak istediğiniz dosyayı bulun.
- 2 Dosyayı Windows Gezgini'ndeki konumundan, EasyNetwork'teki Paylaşılan Dosyalar penceresine sürükleyin.

İpucu: Ayrıca **Araçlar** menüsünde **Dosyaları Paylaş**'ı tıklarsanız da dosyayı paylaşabilirsiniz. Paylaş iletişim kutusunda, paylaşmak istediğiniz dosyanın depolandığı klasöre gidin, onu seçin ve sonra **Paylaş**'ı tıklatın.

Dosya paylaşmayı durdurma

Yönetilen ağ üzerinde bir dosyayı paylaşıyorsanız, istediğiniz zaman paylaşımı durdurabilirsiniz. Dosya paylaşımını durdurduğunuzda, yönetilen ağın diğer üyeleri bu dosyaya erişemez.

- 1 **Araçlar** menüsünde **Dosyaları Paylaştırmayı Durdur**'u tıklatın.
- 2 Dosyaları Paylaştırmayı Durdur iletişim kutusunda, artık paylaşmak istemediğiniz dosyayı seçin.
- 3 **Tamam**'ı tıklatın.

Paylaşılan dosyayı kopyalama

Paylaşılan dosyayı kopyaladığınızda, artık paylaşılmasa bile ona sahip olabilirsiniz. Yönetilen ağındaki herhangi bir bilgisayardan, paylaşılan bir dosyayı kopyalayabilirsiniz.

- EasyNetwork'te Paylaşılan Dosyalar penceresinden bir dosyayı, Windows Gezgini'ndeki bir konuma veya Windows masaüstüne sürükleyin.

İpucu: Ayrıca, EasyNetwork'te paylaşılan bir dosya seçip **Araçlar** menüsünde **Kopyala**'yı tıklatırsanız da dosyayı kopyalayabilirsiniz. Klasöre kopyala iletişim kutusunda, dosyayı kopyalamak istediğiniz klasöre gidip seçin ve ardından **Kaydet**'i tıklatın.

Paylaşılan bir dosyayı arama

Siz veya ağın başka bir üyesi tarafından paylaşılan bir dosyayı arayabilirsiniz. Arama ölçütlerinizi yazdığınızda, EasyNetwork ilişkili sonuçları Paylaşılan Dosyalar penceresinde görüntüler.

- 1 Paylaşılan Dosyalar penceresinde **Ara**'yı tıklatın.
- 2 **İçeriği** listesinde uygun seçeneği (sayfa 229) tıklatın.
- 3 **Dosya veya Yol Adı** listesine, dosya adının veya yolun bir bölümünü ya da tamamını yazın.
- 4 **Tür** listesinde uygun dosya türünü (sayfa 229) tıklatın.
- 5 **Başlangıç ve Bitiş** listelerinde, dosyanın oluşturulduğu tarih aralığını temsil eden tarihleri tıklatın.

Arama ölçütleri

Aşağıdaki tabloda, paylaşılan dosyaları ararken belirtebileceğiniz arama ölçütleri açıklanmaktadır.

Dosya adı veya yolu

İçeriği	Açıklama
Tüm sözcükleri içerir	Dosya veya Yol Adı listesinde, herhangi bir sırayla belirttiğiniz tüm sözcükleri içeren dosya veya yol adını arayın.
Herhangi bir sözcüğü içerir	Dosya veya Yol Adı listesinde, belirttiğiniz sözcüklerden herhangi birini içeren dosya veya yol adını arayın.
Tam dizeyi içerir	Dosya veya Yol Adı listesinde, belirttiğiniz tam tümceciği içeren dosya veya yol adını arayın.

Dosya türü

Tür	Açıklama
Herhangi	Tüm paylaşılan dosya türlerini arayın.
Belge	Tüm paylaşılan belgeleri arayın.
Resim	Tüm paylaşılan resim dosyalarını arayın.
Video	Tüm paylaşılan video dosyalarını arayın.
Ses	Tüm paylaşılan ses dosyalarını arayın.
Sıkıştırılmış	Tüm sıkıştırılmış dosyaları arayın (örneğin .zip dosyaları).

Dosyaları diğer bilgisayarlara gönderme

Yönetilen ağın üyesi olan diğer bilgisayarlara dosyalar gönderebilirsiniz. Bir dosya göndermeden önce, EasyNetwork dosyayı alan bilgisayarın yeterli kullanılabilir disk alanı olduğunu doğrular.

Bir dosya aldığınızda, bu EasyNetwork gelen kutusunda görüntülenir. Gelen kutusu, ağdaki diğer bilgisayarların size gönderdiği dosyalar için geçici bir depolama konumudur. Dosyayı aldığınızda EasyNetwork açıksa, dosya anında gelen kutunuzda görüntülenir; açık değilse, görev çubuğunuzun sağ ucundaki bildirim alanında bir ileti görüntülenir. Bildirim iletilerini almak istemiyorsanız (örneğin yaptığınız işe müdahale ettikleri için), bu özelliği kapatabilirsiniz. Gelen kutunuzda önceden aynı ada sahip bir dosya varsa, yeni dosya sayısal bir son eklenerek yeniden adlandırılır. Siz onları kabul edene (bilgisayarınıza kopyalayana) kadar, dosyalar gelen kutunuzda kalır.

Başka bir bilgisayara dosya gönderme

Bir dosyayı paylaşmadan, yönetilen ağdaki başka bir bilgisayara gönderebilirsiniz. Alıcı bilgisayardaki kullanıcının dosyayı görüntüleyebilmesi için dosyanın yerel bir konuma kaydedilmesi gerekir. Ayrıntılı bilgi için, bkz. Başka bir bilgisayardan dosya kabul etme (sayfa 231).

- 1 Windows Gezgini'nde, göndermek istediğiniz dosyayı bulun.
- 2 Dosyayı Windows Gezgini'ndeki konumundan, EasyNetwork'teki etkin bilgisayar simgesine sürükleyin.

İpucu: Bilgisayara birden fazla dosya göndermek için dosyaları seçerken CTRL tuşuna basın. Ayrıca, **Araçlar** menüsünde **Gönder**'i tıklar, dosyaları seçer ve sonra **Gönder**'i tıklattırsanız da dosyaları gönderebilirsiniz.

Başka bir bilgisayardan dosya kabul etme

Yönetilen ağdaki başka bir bilgisayar size dosya gönderirse, bunu bilgisayarınıza kaydederek kabul etmeniz gerekir. Bilgisayarınıza dosya gönderildiği sırada EasyNetwork çalışmıyorsa, görev çubuğunuzun sağ ucundaki bildirim alanında bir bildirim ileti görüntülenir. EasyNetwork'ü açıp dosyaya erişmek için bu bildirim iletilisini tıklatın.

- **Alınma tarihi**'ni tıklatın ve sonra dosyayı, EasyNetwork gelen kutunuzdan Windows Gezgini'nde bir klasöre sürükleyin.

İpucu: Ayrıca, EasyNetwork gelen kutunuzdan bir dosya seçer ve sonra **Araçlar** menüsünde **Kabul Et**'i tıklattırsanız da başka bir bilgisayardan dosya alabilirsiniz. Klasöre kabul et iletişimi kutusunda, aldığınız dosyaları kaydetmek istediğiniz klasöre gidip seçin ve ardından **Kaydet**'i tıklatın.

Dosya gönderildiğinde bildirim alma

Yönetilen ağdaki başka bir bilgisayar size dosya gönderdiğinde bildirim iletisi alabilirsiniz. EasyNetwork çalışmıyorsa, görev çubuğunuzun sağ ucundaki bildirim alanında bildirim iletisi görüntülenir.

- 1 **Seçenekler** menüsünde **Yapılandır**'ı tıklatın.
- 2 Yapılandır iletişim kutusunda, **Başka bilgisayar bana dosya gönderdiğinde bildir** onay kutusunu işaretleyin.
- 3 **Tamam**'ı tıklatın.

B Ö L Ü M 4 5

Yazıcıları paylaşma

Yönetilen bir ağa katıldığınızda, EasyNetwork bilgisayarınıza bağlı yerel yazıcıları paylaşır ve paylaşılan yazıcı adı için yazıcının adını kullanır. EasyNetwork, ağınızdaki diğer bilgisayarlar tarafından paylaşılan yazıcıları da algılar, bunları yapılandırmanıza ve kullanmanıza olanak verir.

Bir yazıcı sürücüsünü ağ yazıcı sunucusu (örneğin kablosuz USB yazdırma sunucusu) aracılığıyla yazdıracak şekilde yapılandırdıysanız, EasyNetwork bu yazıcıyı yerel yazıcı olarak görür ve ağ üzerinde paylaşır. Ayrıca, istediğiniz zaman yazıcı paylaşımını durdurabilirsiniz.

Bu bölümde

Paylaşılan yazıcılarla çalışma.....234

Paylaşılan yazıcılarla çalışma

EasyNetwork, ağdaki bilgisayarlar tarafından paylaşılan yazıcıları algılar. EasyNetwork bilgisayarınıza bağlı olmayan bir uzak yazıcı algılsa, EasyNetwork'ü ilk kez açtığınızda, Paylaşılan Dosyalar penceresinde **Kullanılabilir ağ yazıcıları** bağlantısı görüntülenir. Daha sonra, kullanılabilir yazıcıları yükleyebilir veya zaten bilgisayarınıza bağlı olan yazıcıları kaldırabilirsiniz. Ayrıca, görüntülediğiniz bilgilerin güncel olduğundan emin olmak için yazıcı listesini yenileyebilirsiniz.

Yönetilen ağa bağlı olmanıza karşın ağa katılmadıysanız, paylaşılan yazıcılara Windows yazıcı denetim masasından erişebilirsiniz.

Yazıcı paylaşmayı durdurma

Yazıcı paylaşımını durdurduğunuzda, üyeler bunu kullanamaz.

- 1 **Araçlar** menüsünde **Yazıcılar**'ı tıklatın.
- 2 Ağ Yazıcılarını Yönet iletişim kutusunda, artık paylaşmak istemediğiniz yazıcının adını tıklatın.
- 3 **Paylaştırma**'yı tıklatın.

Kullanılabilir ağ yazıcısı yükleme

Yönetilen ağın üyesiyseniz, paylaşılan yazıcılara erişebilirsiniz; ancak yazıcı tarafından kullanılan yazıcı sürücüsünü yüklemeniz gerekir. Yazıcının sahibi yazıcı paylaşımını durdurursa, bunu kullanamazsınız.

- 1 **Araçlar** menüsünde **Yazıcılar**'ı tıklatın.
- 2 Kullanılabilir Ağ Yazıcıları iletişim kutusunda, bir yazıcı adını tıklatın.
- 3 **Yükle**'yi tıklatın.

Başvuru

Bu Terimler Sözlüğü'nde, McAfee ürünlerinde bulunan ve en sık kullanılan güvenlik terminolojisi listelenmekte ve tanımlanmaktadır.

Sözlük

8

802.11

Kablosuz yerel ağda veri iletmek için IEEE standartları grubu. 802.11 genellikle Wi-Fi olarak bilinir.

802.11a

5GHz bantta 54 Mb/sn'ye kadar veri gönderen 802.11 uzantısı. İletim hızının 802.11b'den daha yüksek olmasına karşın, kapsanan uzaklık daha kısadır.

802.11b

2,4 GHz bantta 11 Mb/sn'ye kadar veri gönderen 802.11 uzantısı. İletim hızının 802.11a'dan daha düşük olmasına karşın, kapsanan uzaklık daha uzundur.

802.1x

Kablolu ve kablosuz ağlarda kimlik doğrulama için IEEE standardı. 802.1x genellikle 802.11 kablosuz ağı ile kullanılır.

A

ActiveX denetimi

Programlar veya Web sayfaları tarafından programın veya Web sayfasının doğal bir parçası gibi görünen işlevsellik eklemek üzere kullanılan bir yazılım bileşeni. Çoğu ActiveX denetimi zararsızdır; ancak bazıları bilgisayarınızdan bilgiler yakalayabilir.

açılan pencereler

Bilgisayar ekranlarında diğer pencerelerin üzerinde beliren küçük pencereler. Açılan pencereler, reklamlar görüntülemek üzere Web tarayıcılarında sıklıkla kullanılır.

ağ

Erişim Noktaları ve bunlara karşılık gelen kullanıcıların derlemesi; ESS ile aynıdır.

ağ haritası

Ev ağınıza oluşturan bilgisayarların ve bileşenlerin grafiksel anlatımı.

ağ sürücüsü

Çok sayıda kullanıcı tarafından paylaşılan ağ üzerinde bir sunucuya bağlı disk veya teyp sürücüsü. Ağ sürücülerini bazen uzak sürücüler olarak adlandırılır.

akıllı sürücü

Bkz. USB sürücüsü.

anahtar

İki aygıt tarafından aralarındaki iletişimin kimliğini doğrulamak için kullanılan harfler ve sayılar dizisi. Her iki aygıtın da anahtarı olmalıdır. Ayrıca bkz. WEP, WPA, WPA2, WPA-PSK ve WPA2-PSK.

anahtar sözcük

Aynı anahtar sözcüğün atandığı diğer dosyalarla ilişki veya bağlantı kurmak için yedeklenen bir dosyaya atayabileceğiniz sözcük. Dosyalara anahtar sözcükler atamak, İnternet'te yayımladığınız dosyaların aranmasını kolaylaştırır.

arabellek taşıması

Şüpheli programlar veya işlemler, bilgisayarınızdaki arabelleğe (geçici depolama alanı) saklayabileceğinden daha fazla veri depolamaya çalıştığında ortaya çıkan durum. Arabellek taşmaları, komşu arabelleklerdeki verileri bozar veya bunların üzerine yazar.

arşivleme

CD, DVD, USB sürücüsü, harici sabit disk veya ağ sürücüsü üzerinde önemli dosyaların yerel kopyasını oluşturmak.

ayrıntılı izleme konumu

Bilgisayarınızda Data Backup'ın değişikliklerini izlediği klasör. Ayrıntılı izleme konumu ayarlarsanız, Data Backup bu klasörün ve alt klasörlerinin içindeki izlenen dosya türlerini yedekler.

B**bant genişliği**

Belirli bir süre içinde iletebilen veri miktarı.

beyaz liste

Hileli olmadıkları düşünüldüğü için kullanıcıların erişimine izin verilen Web sitelerinin listesi.

Ç**çevrimiçi yedekleme havuzu**

Çevrimiçi sunucu üzerinde dosyalarınızın yedeklendikten sonra saklandığı konum.

D**DAT**

(Veri imza dosyaları) Bilgisayarınızdaki veya USB sürücünüzdeki virüsleri, Truva atlarını, casus yazılımları, reklam yazılımları ve diğer olası istenmeyen programları algılarken kullanılan tanımları içeren dosyalar.

DNS

(Etki Alanı Adı Sistemi) Ana bilgisayar adlarını veya etki alanı adlarını IP adreslerine dönüştüren bir sistem. Web'de DNS, Web sitesini çağırmak için kolay okunan Web adresini (örneğin www.anabilgisayarım.com) IP adreslerine (örneğin 111.2.3.44) dönüştürmede kullanılır. DNS olmadan IP adresini Web tarayıcınıza kendiniz yazmanız gerekir.

DNS sunucusu

(Etki Alanı Adı Sistemi sunucusu) Ana bilgisayarla veya etki alanı adıyla ilişkili IP adresini döndüren bilgisayar. Ayrıca bkz. DNS.

dolaşım

Hizmette kesinti veya bağlantı kaybı olmaksızın, bir Erişim Noktası (AP) kapsama alanından diğerine hareket etmek.

dosya parçaları

Bir dosyanın disk üzerine dağılmış kalıntıları. Dosya parçalanması, dosyalar eklenip silindikçe oluşur ve bilgisayarınızın performansını düşürebilir.

düğüm

Bir ağa bağlı olan tek bir bilgisayar.

düz metin

Şifreli olmayan metin. Ayrıca bkz. şifreleme.

E

e-posta

(elektronik posta) Bilgisayar ağında elektronik olarak gönderilen ve alınan iletiler. Ayrıca bkz. Web postası.

e-posta istemcisi

Bilgisayarınızda e-posta gönderip almak için çalıştırdığınız program (örneğin Microsoft Outlook).

Ebeveyn Denetimleri

Çocuklarınızın Web'de gezinirken görebilecekleri ve yapabilecekleri şeyleri düzenlemenize yardımcı olan ayarlar. Ebeveyn Denetimleri'ni ayarlamak için görüntü filtrelemeyi etkinleştirebilir veya devre dışı bırakabilir, içerik derecelendirme grubu seçebilir ve Web'de gezinme saat sınırlamalarını ayarlayabilirsiniz.

eklenti

Ek işlevsellik kazandırmak için daha büyük bir programla birlikte çalışan küçük yazılım programı. Örneğin eklentiler, HTML belgelerine gömülen ve tarayıcının normalde fark etmeyeceği biçimlerdeki (animasyon, video ve ses dosyaları gibi) dosyalara, Web tarayıcısının erişmesine ve bunları yürütmesine izin verir.

Erişim Noktası

Kablosuz kullanıcının fiziksel hizmet kapsamını genişletmek için Ethernet merkezine veya anahtarına takılan ağ aygıtı (genellikle kablosuz yönlendirici olarak adlandırılır). Kablosuz kullanıcılar mobil cihazlarıyla dolaşıma girdiklerinde, bağlantıyı korumak için iletim bir Erişim Noktasından (AP) başka bir erişim noktasına geçer.

ESS

(Uzatılmış Hizmet Seti) Tek bir alt ağ oluşturan iki veya daha fazla ağ seti.

etki alanı

Internet üzerindeki siteler için bir yerel alt ağ veya tanımlayıcı.

Etki alanı, yerel ağ (LAN) üzerinde tek güvenlik veritabanı tarafından kontrol edilen istemci ve sunucu bilgisayarlardan oluşan bir alt ağıdır. Bu bağlamda, etki alanları performansı geliştirebilir. Etki alanı, Internet üzerinde her Web adresinin bir parçasıdır (örneğin www.abc.com'da abc etki alanıdır).

etkin nokta

Wi-Fi (802.11) erişim noktası (AP) kapsamındaki coğrafi sınır. Etkin nokta yayın yapıyorsa (varlığını duyuruyorsa) ve kimlik doğrulaması gerekmiyorsa, kablosuz dizüstü bilgisayarla etkin noktaya giren kullanıcılar Internet'e bağlanabilirler. Etkin noktalar genellikle havaalanları gibi kalabalık yerlerde bulunur.

ev ağı

Evde dosya ve Internet erişimini paylaşmak üzere birbirine bağlanan iki veya daha çok bilgisayar. Ayrıca bkz. LAN.

G

geçici dosya

İşletim sistemi veya başka bir program tarafından, bir oturum sırasında kullanılıp daha sonra silinmek üzere bellekte veya diskte oluşturulan dosya.

gerçek zamanlı tarama

Siz veya bilgisayarınız tarafından erişilen dosya ve klasörlerde virüsleri ve diğer etkinliği taramak.

Geri Dönüşüm Kutusu

Windows'da silinen dosyalar ve klasörler için sanal bir çöp kutusu.

geri yükleme

Çevrimiçi yedekleme havuzundan veya arşivden bir dosyanın kopyasını almak.

görüntü filtreleme

Oalsı uygunsuz Web görüntülerinin gösterilmesini engelleyen Ebeveyn Denetimleri seçeneği.

güvenilenler listesi

Güvendiğiniz ve algılanmayan öğeleri içerir. Bir öğeye (örneğin olası istenmeyen programa veya kayıt defteri değişikliğine) yanlışlıkla güvenirsiniz veya öğenin yeniden algılanmasını isterseniz, onu bu listeden kaldırmanız gerekir.

güvenlik duvarı

Özel bir ağa veya ağdan yetkisiz erişimi engellemek için tasarlanan sistem (donanım, yazılım veya her ikisi birden). Güvenlik duvarları, yetkisiz Internet kullanıcılarının Internet'e ve özellikle bir intranete bağlanan özel ağlara erişmelerini engellemek için sıklıkla kullanılır. İtranete giren veya çıkan tüm iletiler güvenlik duvarından geçer; güvenlik duvarı, tüm iletileri inceler ve belirtilen güvenlik ölçütlerini karşılamayanları engeller.

H

harici sabit disk

Bilgisayar kasasının dışında saklanan harici sürücü.

hileli erişim noktası

Yetkisiz Erişim Noktası. Hileli erişim noktaları, yetkisiz taraflara ağ erişimi sağlamak için güvenli şirket ağına yüklenebilir. Bunlar, saldırganın ortadaki adam saldırısı gerçekleştirmesini sağlamak için de oluşturulabilir.

hızlı arşivleme

Yalnızca en son tam veya hızlı arşivlemeden sonra değiştirilmiş olan dosyaları arşivlemek. Ayrıca bkz. tam arşivleme.

hizmet reddi

Ağda trafiği yavaşlatan veya durduran bir saldırı türü. Hizmet reddi saldırısı (DoS saldırısı), ağ düzenli trafiği yavaşlatacak veya tamamen kesecek kadar çok istekle dolduğunda gerçekleşir. Genellikle bilgi hırsızlığıyla veya diğer güvenlik açıklarıyla sonuçlanmaz.

I

içerik derecelendirme grubu

Ebeveyn Denetimleri'nde, bir kullanıcının ait olduğu yaş grubu. İçerik, kullanıcının ait olduğu içerik derecelendirme grubuna göre kullanıma açılır. İçerik derecelendirme grupları şunları kapsar: Küçük Çocuk, Çocuk, Büyük Çocuk, Genç ve Yetişkin.

ileti kimlik doğrulama kodu (MAC)

Bilgisayarlar arasında gönderilen iletileri şifrelemek için kullanılan güvenlik kodu. Bilgisayar şifresi çözülen kodun geçerli olduğunu anlarsa ileti kabul edilir.

Internet

Internet, verilerin bulunması ve aktarımı için TCP/IP protokolleri kullanan birbirine bağlı çok sayıda ağdan oluşur. Internet, ABD Savunma Bakanlığı tarafından finanse edilen ve ARPANET adı verilen, birbirine bağlı üniversite ve fakülte bilgisayarlarından (1960'ların sonunda ve 1970'lerin başında) geliştirilmiştir. Günümüzde Internet neredeyse 100.000 bağımsız ağdan oluşan genel bir ağıdır.

intranet

Genellikle bir kuruluşun içinde bulunan ve yalnızca yetkili kullanıcılar tarafından erişilebilen özel bilgisayar ağı.

IP adresi

TCP/IP ağı üzerinde bir bilgisayarın veya aygıtın tanımlayıcısı. TCP/IP protokolünü kullanan ağlar, hedef IP adresine göre iletileri yönlendirirler. IP adresi, noktalarla birbirinden ayrılan dört sayı şeklinde yazılan 32 bitlik sayısal bir adrestir. Her sayı 0 ile 255 arasında olabilir (örneğin, 192.168.1.100).

IP hilesi

Bir IP paketi içindeki IP adreslerinin sahtelerini yapmak. Bu, oturum soymak dahil, çok çeşitli saldırı türlerinde kullanılır. Genellikle tam olarak izlenememeleri için SPAM e-posta başlıklarının sahtelerini yapmada kullanılır.

isteğe bağlı tarama

İstek üzerine (işlemi açtığınızda) başlatılan tarama. Gerçek zamanlı taramanın aksine, isteğe bağlı arama otomatik olarak başlamaz.

istemci

Bilgisayar veya iş istasyonu üzerinde çalışan ve bazı işlemleri gerçekleştirmek için sunucuya gerek duyan bir uygulama. Örneğin e-posta istemcisi, e-posta gönderip almanıza olanak veren bir uygulamadır.

izleme konumları

Data Backup'ın bilgisayarınızda izlediği klasörler.

izlenen dosya türleri

Data Backup'ın izleme konumlarında yedeklediği veya arşivlediği dosya türleri (örn., .doc, .xls gibi).

K

kaba kuvvet saldırısı

Zeka stratejisi yerine yoğun çabayla (kaba kuvvet kullanarak), parolalar gibi şifreli verilerin şifresini çözme yöntemi. Çok fazla zaman almasına karşın, kaba kuvvet yönteminin hatasız olduğu düşünülmektedir. Kaba kuvvet saldırısı, kaba kuvvet darbesi olarak da bilinir.

kablosuz bağdaştırıcı

Bilgisayara veya PDA'ya kablosuz özelliği ekleyen aygıt. USB port, PC kartı (CardBus) yuvası, bellek kartı yuvası üzerinden veya dahili olarak PCI veri yoluna takılır.

kara liste

Phishing korumasında, hileli oldukları düşünülen Web sitelerinin listesi.

karantina

İzole etmek. Örneğin VirusScan'de, şüpheli dosyalar algılanır, bilgisayarınıza ve dosyalarınıza zarar vermemeleri için karantinaya alınır.

kayıt defteri

Windows'un yapılandırma bilgilerini depoladığı bir veritabanı. Kayıt defteri, tüm bilgisayar kullanıcılarının profillerini ve sistem donanımı, yüklenen programlar ve özellik ayarları hakkındaki bilgileri içerir. Windows çalışırken sürekli bu bilgilere başvurur.

kimlik doğrulama

Genellikle benzersiz bir ada ve parolaya göre bir kişinin kimliğini belirleme işlemi.

kısayol

Bilgisayarınızda başka bir dosyanın yalnızca konumunu içeren bir dosya.

kitaplık

Yedeklediğiniz ve yayımladığınız dosyalar için çevrimiçi depolama alanı. Data Backup Kitaplığı, Internet erişimi olan herkesin erişebildiği Internet üzerindeki bir Web sitesidir.

komut dosyası

Otomatik olarak yürütülebilen (kullanıcı etkileşimi olmadan) komut listesi. Programların aksine komut dosyaları, genellikle düz metin biçiminde depolanır ve çalıştırıldıkları her seferde derlenir. Makrolar ve toplu iş dosyaları da komut dosyaları olarak adlandırılır.

köke inme

Bir bilgisayarda veya bilgisayar ağında kullanıcıya yönetici düzeyinde erişim sağlayan araçlar grubu (programlar). Köke inme programları, bilgisayarınızdaki veriler veya kişisel bilgileriniz için ek güvenlik veya gizlilik riskleri oluşturabilen casus yazılımları ve diğer olası istenmeyen programları içerebilir.

L

LAN

(Yerel Ağ) Göreceli olarak küçük bir alanı (örneğin bir tek bina) kapsayan bilgisayar ağı. Yerel ağ üzerindeki bilgisayarlar, birbirleriyle iletişim kurabilir, yazıcı ve dosya gibi kaynakları paylaşabilir.

launchpad

U3 USB programlarını başlatmak ve yönetmek için başlangıç noktası görevi gören bir U3 arabirim bileşeni.

M

MAC adresi

(Ortam Erişim Denetimi adresi) Ağa erişen fiziksel ağıta atanan benzersiz bir seri numarası.

MAPI

(İleti Uygulaması Programlama Arabirimi) Farklı ileti ve çalışma grubu uygulamalarının (e-posta, sesli posta ve faks dahil) Exchange istemcisi gibi tek bir istemci aracılığıyla çalışmasına izin veren Microsoft arabirimi belirtimi.

MSN

(Microsoft Ağı) Microsoft Corporation tarafından sunulan arama motoru, e-posta, anlık ileti ve portal gibi Web tabanlı hizmetler grubu.

N

NIC

(Ağ Arabirim Kartı) Dizüstü bilgisayara veya başka bir ağıta takılan ve ağıtı yerel ağa bağlayan kart.

numara çevirici

Internet bağlantısı kurmanıza yardımcı olan yazılım. Kötü niyetle kullanıldığında, numara çeviriciler Internet bağlantılarınızı varsayılan Internet Servis Sağlayıcınız (ISS) yerine, ek maliyeti size bildirmeden başka birisine yeniden yönlendirebilir.

O

olası istenmeyen program (PUP)

İzinsiz olarak kişisel bilgileri toplayan ve ileten program (örneğin casus yazılımlar ve reklam yazılımlar).

olay

Kullanıcı, bir aygıt veya bilgisayarın kendisi tarafından başlatılan ve yanıtı tetikleyen bir eylem. McAfee, olayları olay günlüğüne kaydeder.

ortadaki adam saldırısı

İletişim bağlantısının ihlal edildiğini bilmeyen iki taraf arasındaki iletileri ele geçirmek ve büyük olasılıkla değiştirmek için bir yöntem.

Ö

önbellek

Bilgisayarınızdaki geçici bir depolama alanı. Örneğin, Web'de gezinme hızını ve etkinliğini artırmak için tarayıcınız, daha önce görüntülediğiniz bir Web sayfasını önbellekten (uzak sunucu yerine) çağırabilir.

P

parola

Bilgisayarınıza, bir programa veya Web sitesine erişim sağlamak için kullandığınız kod (genellikle harfler ve sayılardan oluşur).

Parola Mahzeni

Kişisel parolalarınız için güvenli bir saklama alanı. Parolalarınızı başka hiçbir kullanıcının (hatta yöneticinin) erişemeyeceği şekilde güvenle saklamanıza olanak verir.

paylaşılan şifre

İletişim başlamadan önce iletişim kuran iki taraf arasında paylaşılan bir dize veya anahtar (genellikle parola). Paylaşılan şifre, RADIUS iletilerinin hassas bölümlerini korumak için kullanılır.

paylaştırma

E-posta alıcılarının sınırlı bir süre için seçili yedeklenen dosyalara erişmelerine izin vermek. Bir dosyayı paylaştırdığınızda, dosyanın yedeklenen kopyasını belirlediğiniz e-posta alıcılarına gönderirsiniz. Alıcılar Data Backup'tan dosyaların kendileriyle paylaşıldığını gösteren bir e-posta iletisi alırlar. E-posta, paylaşılan dosyalara bağlantı da içerir.

PCI kablosuz bağdaştırıcı kartları

(Çevre Birim Bileşeni Bağlantısı) Bilgisayarın içindeki PCI genişletme yuvasına takılan kablosuz bağdaştırıcı kartı.

phishing

Hileli kullanım amacıyla haberleri olmadan insanlardan değerli bilgiler (kredi kartı ve sosyal sigorta numaraları, kullanıcı kimlikleri ve parolalar gibi) almak için tasarlanan bir Internet aldatmacası.

POP3

(Posta Ofis Protokolü 3) E-posta istemci programı ve e-posta sunucusu arasındaki arabirim. Ev kullanıcılarının çoğu, standart e-posta hesabı olarak da bilinen bu hesap türüne sahiptir.

port

Bilgilerin bilgisayara girip çıktığı yer. Örneğin geleneksel analog modem seri porta bağlanır.

PPPoE

(Ethernet Üzerinden Noktalar Arası Protokol) Aktarma olarak Ethernet'le Noktalar Arası Protokol (PPP) çevirmeli protokolünü kullanma yöntemi.

protokol

İki aygıt arasında veri iletmek için bir biçim (donanım veya yazılım). Diğer bilgisayarlarla iletişim kurmak istiyorsanız, bilgisayarınız veya aygıtınız doğru protokolü desteklemelidir.

proxy

Harici sitelere yalnızca tek bir ağ adresi vererek, ağ ile Internet arasında engel görevi gören bilgisayar (veya bilgisayarda çalışan yazılım). Proxy, tüm dahili bilgisayarları temsil ederek, bir yandan Internet'e erişim sağlarken diğer yandan da ağ kimliklerini korur. Ayrıca bkz. proxy sunucusu.

proxy sunucusu

Yerel ağa (LAN) girip çıkan Internet trafiğini yöneten bir güvenlik duvarı bileşeni. Proxy sunucusu, popüler bir Web sayfası gibi sık sık istenen verileri sağlayarak performansı geliştirebilir ve özel dosyalara yetkisiz erişim gibi kullanıcının uygun görmediği istekleri filtreleyip silebilir.

R

RADIUS

(Uzaktan Erişim Çevirme Kullanıcı Hizmeti) Genellikle uzaktan erişimde, kullanıcı kimlik doğrulamasına olanak veren protokol. İlk başlarda çevirmeli uzaktan erişim sunucularıyla kullanılmak üzere tanımlanan RADIUS protokolü, artık kablosuz yerel ağ kullanıcısının paylaşılan şifresinin 802.1x kimlik doğrulaması dahil, çok çeşitli kimlik doğrulama ortamlarında kullanılmaktadır.

S

savaş sürücüsü

Wi-Fi bilgisayar ve birtakım özel donanımlar veya yazılımlarla şehirde dolaşarak Wi-Fi (802.11) ağları arayan kişi.

senkronize etme

Yedeklenen dosyalarla yerel bilgisayarınızda saklanan dosyalar arasındaki tutarsızlıkları çözmek. Çevrimiçi yedekleme havuzundaki dosya sürümünü diğer bilgisayarlardaki dosya sürümünden daha yeniyse dosyaları senkronize edersiniz.

sıkıştırma

Dosyaları sıkıştırarak, bunları saklamak veya iletmek için gereken alanı en aza indiren işlem.

sistem geri yükleme noktası

Bilgisayar belleğinin veya bir veritabanının içeriklerinin anlık görüntüsü. Windows, düzenli olarak ve önemli sistem olayları gerçekleştiğinde (örneğin bir program veya sürücü yüklendiğinde) geri yükleme noktaları oluşturur. İstedığınız zaman kendi geri yükleme noktalarınızı da oluşturup adlandırabilirsiniz.

Sistem Koruması

Bilgisayarınızdaki yetkisiz değişiklikleri algılayan ve bunlar oluştuğunda size bildiren McAfee uyarıları.

SMTP

(Basit Dosya Paylaşım Protokolü) Bir ağ üzerinde bir bilgisayardan diğerine iletiler göndermeyi sağlayan TCP/IP protokolü. Bu protokol, Internet üzerinde e-posta yönlendirmek için kullanılır.

solucan

Kendi kendine çoğalan, etkin belleğe yerleşen ve e-posta ile kendi kopyalarını gönderebilen bir virüs. Solucanlar, çoğalarak sistem kaynaklarını tüketir ve performansı yavaşlatır veya görevleri durdururlar.

sözlük saldırısı

Parolayı bulmak için yaygın sözcükleri kullanan bir tür kaba kuvvet saldırısı.

SSID

(Hizmet Seti Tanımlayıcısı) Wi-Fi (802.11) ağını tanımlayan belirteç (gizli anahtar). SSID, ağ yöneticisi tarafından ayarlanır ve ağa katılmak isteyen kullanıcılar tarafından sağlanmalıdır.

SSL

(Güvenli Yuva Katmanı) Netscape tarafından Internet üzerinde özel belgeleri iletmek üzere geliştirilen bir protokol. SSL, SSL bağlantısı üzerinden aktarılan verileri şifrelemek için ortak bir anahtar kullanarak çalışır. SSL bağlantısı gerektiren URL'ler http. yerine https ile başlar.

standart e-posta hesabı

Bkz. POP3.

sunucu

Diğer bilgisayarlardan veya programlardan bağlantılar kabul eden ve uygun yanıtları veren bir bilgisayar veya program. Örneğin, her e-posta iletisi gönderip aldığınızda, e-posta programınız bir e-posta sunucusuna bağlanır.

Ş

şifreleme

Bilgileri şifrenin nasıl çözüleceğini bilmeyen kişilerin okuyamayacakları şekilde gizleyerek, verilerin metinden şifreye dönüştürüldüğü bir işlem. Şifrelenen veriler şifreli metin olarak da adlandırılır.

şifreli metin

Şifrelenmiş metin. Şifreli metin, düz metne dönüştürülene (şifresi çözülene) kadar okunamaz.

T

tam arşivleme

Kurmuş olduğunuz dosya türleri ve konumlarını temel alan tam bir veri setini arşivlemek. Ayrıca bkz. hızlı arşivleme.

tanımlama bilgisi

Genellikle Web'de gezinen kişinin bilgisayarında depolanan ve kullanıcı adı ve geçerli tarih ve saat gibi bilgiler içeren küçük bir dosya. Tanımlama bilgileri, Web siteleri tarafından genellikle siteye önceden kaydolun veya siteyi ziyaret eden kullanıcıları tanımlamak için kullanılır; ancak bunlar, korsanlar için bilgi kaynağı da olabilir.

tarayıcı

İnternet'te Web sayfalarını görüntülemek için kullanılan program. Popüler Web tarayıcıları arasında Microsoft Internet Explorer ve Mozilla Firefox sayılabilir.

TKIP

(Geçici Anahtar Bütünlüğü Protokolü) WEP güvenliğindeki açıkları ve özellikle şifreleme anahtarlarının yeniden kullanımını ele alan protokol. TKIP, her 10.000 pakette bir geçici anahtarları değiştirerek, ağın güvenliğini büyük ölçüde geliştiren dinamik bir dağıtım yöntemi sağlar. TKIP (güvenlik) işlemi, istemcilerle erişim noktaları (AP'ler) arasında paylaşılan 128 bit geçici anahtarla başlar. TKIP bu geçici anahtarı (istemcinin) MAC adresiyle birleştirir ve daha sonra verileri şifreleyen anahtarı üretmek için, göreceli olarak büyük bir 16 sekizlik başlangıç vektörü ekler. Bu prosedür, her istasyonun verileri şifrelemek için farklı anahtar akışları kullanmasını sağlar. TKIP, şifreleme işlemini gerçekleştirmek için RC4 kullanır.

Truva Atı

Yasal programlar gibi görünen ancak değerli dosyalara zarar verebilen, performansı düşürebilen ve bilgisayarınızda yetkisiz erişime izin verebilen program.

tümleşik ağ geçidi

Erişim noktası (AP), yönlendirici ve güvenlik duvarı işlevlerini birleştiren bir aygıt. Bazı aygıtlar, güvenlik geliştirmeleri ve köprü kurma özellikleri de içerebilir.

U

U3

(Siz: Basitleştirilmiş, Daha Akıllı, Mobil) Windows 2000 veya Windows XP programlarını doğrudan USB sürücüsünden çalıştırmak için bir platform. U3 girişimi, 2004 yılında M-Systems ve SanDisk tarafından gerçekleştirilmiştir ve kullanıcıların U3 programlarını bilgisayara veriler veya ayarlar yüklemekten veya depolamadan bir Windows bilgisayarda çalıştırmalarına olanak verir.

URL

(Birörnek Kaynak Konumlayıcı) İnternet adresleri için standart biçim.

USB

(Evrensel Seri Veri Yolu) Bilgisayarınıza klavyeler, oyun çubukları ve yazıcılar gibi çevrebirim aygıtları eklemenize olanak veren standartlaştırılmış bir seri bilgisayar arabirimi.

USB kablosuz bağdaştırıcı kartı

Bilgisayardaki USB yuvasına takılan kablosuz bağdaştırıcı kartı.

USB sürücüsü

Bilgisayarın USB portuna takılan küçük bellek sürücüsü. USB sürücüsü, küçük bir sabit disk gibi hareket ederek, bir bilgisayardan diğerine dosyalar aktarmayı kolaylaştırır.

V

virüs

Dosyalarınızı veya verilerinizi değiştirebilen, kendini çoğaltan programlar. Bunlar çoğunlukla güvenilen bir göndericiden geliyormuş gibi veya zararsız içerikliymiş gibi görünür.

VPN

(Sanal Özel Ağ) Bir ortak ağ içinde ortak ağın yönetim olanaklarından yararlanmak için yapılandırılan özel ağ. VPN'ler, kuruluşlar tarafından büyük coğrafi alanları kapsayan geniş alan ağları (WAN) oluşturmak, şubelere sahalar arası bağlantılar sağlamak veya mobil kullanıcıların şirketlerinin yerel alan ağlarını çevirmelerine olanak vermek için kullanılır.

W

Web bug'ları

Kendilerini HTML sayfalarına gömebilen ve yetkisiz bir kaynağın bilgisayarınızda tanımlama bilgileri ayarlamasına izin veren küçük grafik dosyaları. Bu tanımlama bilgileri, daha sonra yetkisiz kaynağa bilgi iletebilir. Web bug'ları, Web işaretleri, piksel etiketleri, net GIF'ler veya görünmez GIF'ler olarak da adlandırılır.

Web postası

Internet'te elektronik olarak gönderilen ve alınan iletiler. Ayrıca bkz. e-posta.

WEP

(Kablolu Eşdeğeri Gizlilik) Wi-Fi (802.11) standardının bir parçası olarak tanımlanan şifreleme ve kimlik doğrulama protokolü. Başlangıç sürümleri, RC4 şifrelerini temel alır ve önemli açıkları vardır. WEP, bir uçtan diğerine iletilirken korunması için, telsiz dalgaları üzerinden verileri şifreleyerek güvenliği sağlamaya çalışır. Ancak WEP'in eskiden zannedildiği kadar güvenli olmadığı görülmüştür.

Wi-Fi

(Kablosuz Sadakat) Wi-Fi Alliance tarafından 802.11 türünde ağlardan söz ederken kullanılan terim.

Wi-Fi Alliance

Lider kablosuz donanım ve yazılım sağlayıcılardan oluşan bir kuruluş. Wi-Fi Alliance, tüm 802.11 tabanlı ürünlerin birlikte çalışabilirliğini doğrulamayı ve Wi-Fi teriminin tüm pazarlarda bütün 802.11 tabanlı kablosuz yerel ağ ürünleri için genel marka adı olmasını teşvik etmeyi amaçlar. Bu kuruluş, sektör büyümesini teşvik etmek isteyen satıcılar için bir konsorsiyum, test laboratuvarı ve takas odası görevi görür.

Wi-Fi Certified

Wi-Fi Alliance tarafından test edilmiş ve onaylanmış olmak. Wi-Fi Certified ürünlerin, farklı üreticilere ait olsalar bile birbirleriyle çalışabilirliği onaylanmıştır. Wi-Fi Certified ürünü bulunan bir kullanıcı, herhangi bir markaya ait Erişim Noktasını (AP), başka herhangi bir markaya ait onaylı istemci donanımlarıyla birlikte kullanabilir.

WLAN

(Kablosuz Yerel Ağ) Kablosuz bağlantı kullanan kullanan yerel ağ (LAN). Kablosuz yerel ağ, bilgisayarların birbirleriyle iletişim kurmasına olanak vermek için kablolar yerine yüksek frekanslı telsiz dalgaları kullanır.

WPA

(Wi-Fi Korumalı Erişim) Mevcut ve gelecekteki kablosuz yerel ağ sistemleri için veri korumasının ve erişim denetiminin düzeyini önemli ölçüde artıran bir belirtim standardı. Yazılım yükseltmesi olarak mevcut donanımın üzerinde çalışmak için tasarlanan WPA, IEEE 802.11i standardından türetilmiştir ve bununla uyumludur. Doğru şekilde yüklendiğinde, kablosuz yerel ağ kullanıcılarına verilerinin korunmaya devam edeceği ve yalnızca yetkili kullanıcıların ağa erişebilecekleri yönünde üst düzey güvence sağlar.

WPA-PSK

Güçlü şirket sınıfı güvenliğe ihtiyaç duymayan ve kimlik doğrulama sunucularına erişimleri gerekmeyen ev kullanıcıları için tasarlanan özel WPA modu. Bu modda, ev kullanıcısı Önceden Paylaşılan Anahtar modunda Wi-Fi Korumalı Erişim'i etkinleştirmek için, başlangıç parolasını el ile girer ve her kablosuz bilgisayardaki geçiş sözcüğünü ve Erişim Noktasını düzenli olarak değiştirmesi gerekir. Ayrıca bkz. WPA2-PSK ve TKIP.

WPA2

WPA güvenlik standardının 802.11i IEEE standardını temel alan güncelleştirmesi.

WPA2-PSK

WPA-PSK'ye benzeyen ve WPA2 standardını temel alan özel WPA modu. Daha eski aygıtlar genelde her seferinde yalnızca tek bir şifreleme modunu desteklerken (tüm istemcilerin aynı şifreleme modunu kullanmaları gerekiyordu), WPA2-PSK'nin genel özelliği aygıtların çoğunlukla eşzamanlı olarak çoklu şifreleme modlarını (örneğin AES, TKIP) desteklemesidir.

Y

yayımlama

Yedeklenen bir dosyayı Internet üzerinde kullanıma açmak. Yayımlanan dosyalara, Data Backup kitaplığında arama yaparak erişebilirsiniz.

yedekleme

Güvenli, çevrimiçi bir sunucuda önemli dosyaların kopyasını oluşturmak.

yönetilen ağ

İki tür üyesi bulunan ev ağı: yönetilen üyeler ve yönetilmeyen üyeler. Yönetilen üyeler, koruma durumlarının ağdaki diğer bilgisayarlar tarafından izlenmesine izin verirler; yönetilmeyen üyeler buna izin vermezler.

yönlendirici

Bir ağdan diğerine veri paketleri ileten ağ aygıtı. Dahili yönlendirme tablolarını temel alan yönlendiriciler, tüm gelen paketleri okuyarak, kaynak ve hedef adres birleşimlerinin yanı sıra geçerli trafik koşullarına (örneğin yük, hat maliyetleri, kötü hatlar) da dayanarak bunların nasıl iletileceğine karar verir. Yönlendirici bazen Erişim Noktası (AP) olarak da adlandırılır.

yüzeysel izleme konumları

Bilgisayarınızda Data Backup'ın değişikliklerini izlediği klasör. Yüzeysel izleme konumu ayarlarsanız, Data Backup izlenen dosya türlerini bu klasörün içine yedekler, ancak alt klasörleri içermez.

McAfee Hakkında

Merkezi Santa Clara, California'da bulunan ve İzinsiz Girişleri Engelleme ve Güvenlik Risk Yönetimi alanında dünya lideri olan McAfee, Inc., tüm dünyada sistemleri ve ağları güvence altına alan etkin ve kanıtlanmış çözümler ve hizmetler sunar. McAfee, güvenlik alanında sahip olduğu eşsiz uzmanlığı ve yeniliğe olan bağlılığıyla, ev kullanıcılarını, şirketleri, devlet sektörünü ve hizmet sağlayıcıları, saldırıları engelleme, aksaklıkları önleme, güvenliği sürekli izleme ve geliştirme olanağıyla güçlendirir.

Telif Hakkı

Telif Hakkı © 2007-2008 McAfee, Inc. Tüm Hakları Saklıdır. McAfee, Inc.'nin yazılı izni olmaksızın, bu yayımın hiçbir bölümü çoğaltılamaz, aktarılamaz, uyarlanamaz, bir çağırma sisteminde saklanamaz veya hiçbir şekilde ya da hiçbir yolla herhangi bir dile çevirisi yapılamaz. McAfee ve burada belirtilen diğer ticari markalar, ABD ve/veya diğer ülkelerde McAfee, Inc. ve/veya bağlı kuruluşlarına ait tescilli ticari markalar veya ticari markalardır. Güvenlikle bağlantılı olarak McAfee Red, McAfee markalı ürünlerden farklıdır. Burada yer alan diğer tüm tescilli veya tescilsiz ticari markalar ve telif hakkı korumalı materyal, yalnızca ilgili sahiplerinin mülkiyetindedir.

TİCARİ MARKA ÖZELLİKLERİ

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, MCAFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN.

Lisans

TÜM KULLANICILAR İÇİN BİLDİRİM: LİSANSLI YAZILIMIN KULLANIMINA YÖNELİK GENEL KOŞULLAR VE HÜKÜMLERİ ORTAYA KOYAN, SATIN ALDIĞINIZ LİSANSLA İLİŞKİLİ UYGUN YASAL ANLAŞMAYI DİKKATLE OKUYUN. LİSANSINIZIN TÜRÜNÜ BİLMİYORSANIZ, LÜTFEN YAZILIM PAKETİYLE BİRLİKTE SAĞLANAN VEYA SATIN ALMA SİRASINDA AYRICA ALDIĞINIZ SATIŞ VEYA DİĞER İLGİLİ LİSANS BELGELERİNE YA DA SİPARİŞ BELGELERİNE (KİTAPÇIK, ÜRÜN CD'SİNDEKİ DOSYA VEYA YAZILIM PAKETİNİ YÜKLEDİĞİNİZ WEB SİTESİNDEKİ DOSYA) BAŞVURUN. ANLAŞMADA YER ALAN BÜTÜN KOŞULLARI KABUL ETMİYORSANIZ, YAZILIMI YÜKLEMİYİN: UYGUNSA, ÜRÜNÜ MCAFEE, INC.'YE VEYA SATIN ALDIĞINIZ YERE İADE EDEREK PARANIZIN TAMAMINI GERİ ALABİLİRSİNİZ.

B Ö L Ü M 4 6

Müşteri Desteği ve Teknik Destek

SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Kritik sorunlarla hemen ilgilenilmesi gerekir ve bunlar koruma durumunuzu tehlikeye atar (rengi kırmızıya döner). Kritik olmayan sorunlarla hemen ilgilenilmesi gerekmez ve bunlar koruma durumunuzu tehlikeye atabilir veya atmayabilir (sorunun türüne göre). Yeşil koruma durumuna ulaşmak için tüm kritik sorunları düzeltmeniz ve tüm kritik olmayan sorunları düzeltmeniz veya yok saymanız gerekir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz. McAfee Virtual Technician hakkında ayrıntılı bilgi için McAfee Virtual Technician yardımına bakın.

Güvenlik yazılımınızı McAfee dışındaki bir ortaktan veya sağlayıcıdan satın aldıysanız, bir Web tarayıcı açın ve www.mcafeehelp.com adresine gidin. Sonra Ortak Bağlantıları altında, McAfee Virtual Technician'a erişmek için ortağınızı veya sağlayıcınızı seçin.

Not: McAfee Virtual Technician'ı yükleyip çalıştırmak için bilgisayarınızda Windows Yöneticisi olarak oturum açmanız gerekir. Aksi halde, MVT sorunlarınızı çözemeyebilir. Windows Yöneticisi olarak oturum açma hakkında ayrıntılı bilgi için Windows Yardımı'na bakın. Windows Vista™'da MVT'yi çalıştırdığınızda bir sorgu penceresi açılır. Bu durumda **Kabul Et**'i tıklayın. Virtual Technician Mozilla® Firefox ile çalışmaz.

Bu bölümde

McAfee Virtual Technician'ı kullanma	254
Destek ve Yüklemler	255

McAfee Virtual Technician'ı kullanma

Virtual Technician, kişisel teknik destek temsilciniz gibi çalışarak, SecurityCenter programlarınız hakkında bilgi toplar ve bilgisayarınızın korunma sorunlarını çözmenize yardımcı olur. Virtual Technician'ı çalıştırdığınızda, SecurityCenter programlarınızın doğru şekilde çalıştığından emin olmak için denetim yapar. Sorunlar bulursa, Virtual Technician bunları sizin için düzeltmeyi önerir veya size bunlarla ilgili ayrıntılı bilgi verir. İşlem tamamlanınca, Virtual Technician analizinin sonuçlarını görüntüler ve gerekirse McAfee'den ek teknik destek istemenize olanak verir.

Virtual Technician, bilgisayarınızın ve dosyalarınızın güvenliğini ve bütünlüğünü korumak için kişisel ve tanımlayıcı bilgiler toplamaz.

Not: Virtual Technician hakkında ayrıntılı bilgi için Virtual Technician'da **Yardım** simgesini tıklatın.

Virtual Technician'ı başlatma

Virtual Technician, SecurityCenter programlarınız hakkında bilgi toplar ve bilgisayarınızın korunma sorunlarını çözmenize yardımcı olur. Gizliliğinizi korumak için bu bilgilere kişisel ve tanımlayıcı bilgiler eklenmez.

- 1 Ortak Görevler** altında **McAfee Virtual Technician'ı** tıklatın.
- Virtual Technician'ı yüklemek ve çalıştırmak için ekran yönergelerini izleyin.

Destek ve Yüklemler

Kullanıcı Kılavuzlarını içeren ülkenize özel McAfee Destek ve Yükleme siteleri için aşağıdaki tablolara başvurun.

Destek ve Yüklemler

Ülke	McAfee Destek	McAfee Yüklemler
Avustralya	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brezilya	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Kanada (İngilizce)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kanada (Fransızca)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Çin (chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Çin (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Çek Cumhuriyeti	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Danimarka	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finlandiya	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Fransa	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Almanya	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Büyük Britanya	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
İtalya	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japonya	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Kore	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Meksika	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norveç	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polonya	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

Portekiz	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
İspanya	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
İsveç	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Türkiye	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Birleşik Devletler	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection Kullanıcı Kılavuzları

Ülke	McAfee Kullanıcı Kılavuzları
Avustralya	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Çin (chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Çin (tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Danimarka	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finlandiya	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Fransa	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Almanya	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Büyük Britanya	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Hollanda	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
İtalya	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

Kore	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Meksika	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norveç	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polonya	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portekiz	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
İspanya	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
İsveç	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security Kullanıcı Kılavuzları

Ülke	McAfee Kullanıcı Kılavuzları
Avustralya	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Çin (chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Çin (tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Danimarka	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finlandiya	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Fransa	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Almanya	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

Büyük Britanya	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Hollanda	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
İtalya	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Meksika	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norveç	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polonya	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portekiz	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
İspanya	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
İsveç	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus Kullanıcı Kılavuzları

Ülke	McAfee Kullanıcı Kılavuzları
Avustralya	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Çin (chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Çin (tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Danimarka	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finlandiya	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Fransa	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Almanya	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Büyük Britanya	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Hollanda	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
İtalya	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Meksika	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norveç	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polonya	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portekiz	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
İspanya	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
İsveç	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan Kullanıcı Kılavuzları

Ülke	McAfee Kullanıcı Kılavuzları
Avustralya	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Çin (chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Çin (tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Danimarka	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finlandiya	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Fransa	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Almanya	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Büyük Britanya	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Hollanda	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
İtalya	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Meksika	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norveç	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polonya	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portekiz	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
İspanya	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
İsveç	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Ülkenize özel McAfee Threat Center ve Virüs Bilgisi siteleri için aşağıdaki tabloya başvurun.

Ülke	Güvenlik Merkezi	Virüs Bilgisi
Avustralya	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brezilya	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Kanada (İngilizce)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kanada (Fransızca)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Çin (chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Çin (tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Çek Cumhuriyeti	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Danimarka	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finlandiya	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Fransa	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Almanya	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Büyük Britanya	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Hollanda	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
İtalya	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japonya	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Kore	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Meksika	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norveç	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polonya	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portekiz	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
İspanya	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
İsveç	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Türkiye	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Birleşik Devletler	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Ülkenize özel HackerWatch ve Virüs Bilgisi siteleri için aşağıdaki tabloya başvurun.

Ülke	HackerWatch
Avustralya	www.hackerwatch.org
Brezilya	www.hackerwatch.org/?lang=pt-br
Kanada (İngilizce)	www.hackerwatch.org
Kanada (Fransızca)	www.hackerwatch.org/?lang=fr-ca
Çin (chn)	www.hackerwatch.org/?lang=zh-cn
Çin (tw)	www.hackerwatch.org/?lang=zh-tw
Çek Cumhuriyeti	www.hackerwatch.org/?lang=cs
Danimarka	www.hackerwatch.org/?lang=da
Finlandiya	www.hackerwatch.org/?lang=fi
Fransa	www.hackerwatch.org/?lang=fr
Almanya	www.hackerwatch.org/?lang=de
Büyük Britanya	www.hackerwatch.org
Hollanda	www.hackerwatch.org/?lang=nl
İtalya	www.hackerwatch.org/?lang=it
Japonya	www.hackerwatch.org/?lang=jp
Kore	www.hackerwatch.org/?lang=ko
Meksika	www.hackerwatch.org/?lang=es-mx
Norveç	www.hackerwatch.org/?lang=no
Polonya	www.hackerwatch.org/?lang=pl
Portekiz	www.hackerwatch.org/?lang=pt-pt
İspanya	www.hackerwatch.org/?lang=es
İsveç	www.hackerwatch.org/?lang=sv
Türkiye	www.hackerwatch.org/?lang=tr
Birleşik Devletler	www.hackerwatch.org

Dizin

8

802.11	236
802.11a	236
802.11b	236
802.1x.....	236

A

Aboneliğinizi doğrulama	11
ActiveX denetimi.....	236
açılan pencereler.....	236
Adres defteri ekleme	128
Adres defterini düzenleme.....	128
Adres defterini kaldırma	129
ağ	236
ağ haritası.....	236
Ağ haritasına erişme	210
Ağ haritasında öğeyi gösterme veya gizleme.....	211
Ağ haritasını yenileme.....	210
Ağ haritasıyla çalışma	210
ağ sürücüsü.....	236
Ağa erişim izni verme	223
Ağa katılma	223
Ağdaki bilgisayarlara güvenmeyi durdurma	214
Ağı uzaktan yönetme.....	215
Ağın adını değiştirme	211, 225
Akıllı Önerileri devre dışı bırakma	78
Akıllı Önerileri etkinleştirme.....	78
Akıllı Önerileri uyarılar için yapılandırma.....	78
Akıllı Önerileri yalnızca görüntüleme.....	79
akıllı sürücü	236
anahtar	237
anahtar sözcük.....	237
Anahtar sözcük filtrelemeyi devre dışı bırakma	164
Anahtar sözcükler kullanarak Web sitelerini filtreleme	161, 164
Anlık ileti korumasını başlatma.....	35
Anti-Spam araç çubuğundan arkadaş ekleme.....	130
Anti-Spam araç çubuğundan bir iletiyi işaretleme.....	141
Anti-Spam araç çubuğunu devre dışı bırakma	142
Anti-Spam özellikleri.....	121

arabellek taşması	237
Arama ölçütleri	229
Arkadaşınızı düzenleme.....	131
Arkadaşınızı el ile ekleme	130
Arkadaşınızı kaldırma.....	132
Arkadaşları ayarlama	127
Arkadaşları el ile ayarlama	130
Arkadaşları otomatik olarak ayarlama ..	128
Arşiv konumunu değiştirme	179
Arşiv seçeneklerini ayarlama.....	176
Arşiv şifreleme ve sıkıştırmayı devre dışı bırakma	179
arşivleme	237
Arşivleme dosyası türlerini ayarlama....	178
Arşivleme etkinliğinizin özetini görüntüleme	188
Arşivlemeleri el ile çalıştırma.....	181
Arşivlemeye konum ekleme	177
Arşivlenen bir dosyayı açma	185
Arşivlenen bir dosyayı arama	184
Arşivlenen dosyaları geri yükleme.....	186
Arşivlenen dosyaları sıralama	184
Arşivlenen dosyalarla çalışma	183
Arşivleri yönetme	188
ayrıntılı izleme konumu	237

B

bant genişliği	237
Başka bir bilgisayara dosya gönderme ..	231
Başka bir bilgisayardan dosya kabul etme	231
Başlangıçta giriş ekranını gizleme.....	24
Başlatma sırasında bilgisayarınızı koruma	80
Başvuru	235
beyaz liste	237
Beyaz listeden Web sitesini kaldırma...	148
Beyaz listenizdeki siteleri düzenleme...	148
Beyaz listeye Web sitesi ekleme	147
Bilgi uyarılarını gizleme	71
Bilgi uyarılarını gösterme ve gizleme	22
Bilgi uyarılarını gösterme veya gizleme..	22
Bilgi uyarılarını yönetme.....	71
Bilgisayar ağ bilgilerini elde etme	111
Bilgisayar bağlantılarına güvenme	100
Bilgisayar bağlantılarını yasaklama	103
Bilgisayar bağlantılarını yönetme	99

Bilgisayar kayıt bilgilerini elde etme	111
Bilgisayarınızı birleştirme	194
Bilgisayarınızı tarama	31, 55, 56
Bilgisayarınızı temizleme	191, 193
Bir ağ bilgisayarının coğrafi konumunu izleme	111
Bir aygıtı yönetme	217
Bir aygıtın görüntü özelliklerini değiştirme	217
Bir bilgisayarı yönetilen ağa katılmaya davet etme	213
Bir bilgisayarın koruma durumunu izleme	216
Bir bilgisayarın koruma durumunu izlemeyi durdurma	216
Bir konumu arşivlemenin dışında tutma	178
Bir McAfee kullanıcısını kaldırma	155
Bir McAfee kullanıcısının hesap bilgilerini düzenleme	155
Bir programa tam erişim izni verme	86
Bir programa yalnızca giden erişim izni verme	88
Bir programın erişimini engelleme	89
Bir tarama zamanlama	43
Bir Web sitesine izin verme	162
Bir Web sitesini engelleme	161

C

Casus yazılım korumasını başlatma	34
---	----

Ç

çevrimiçi yedekleme havuzu	237
----------------------------------	-----

D

DAT	237
Destek ve Yüklemler	255
Disk Birleştirici görevi zamanlama	197
Disk Birleştirici görevini değiştirme	198
Disk Birleştirici görevini silme	198
DNS	237
DNS sunucusu	238
dolaşım	238
Dosya gönderildiğinde bildirim alma	232
dosya parçaları	238
Dosya paylaşma	228
Dosya paylaşmayı durdurma	228
Dosya ve klasörleri parçalama	203
Dosyaları arşivleme	175
Dosyaları diğer bilgisayarlara gönderme	231
Dosyaları eksik dosyalar listesinden kaldırma	187
Dosyaları paylaşma	228
Dosyaları paylaşma ve gönderme	227

Dosyaları, klasörleri ve diskleri parçalama	203
Durumu ve izinleri izleme	216
düğüm	238
düz metin	238

E

EasyNetwork özellikleri	220
EasyNetwork'ü açma	221
EasyNetwork'ü ayarlama	221
Ebeveyn Denetimleri	238
Ebeveyn Denetimleri'ni ayarlama	151
Ek korumayı başlatma	33
eklenti	238
Eksik dosyaları yerel arşivden geri yükleme	186
El ile tarama konumunu ayarlama	42
El ile tarama seçeneklerini ayarlama	40
e-posta	238
E-posta filtreleme	141
e-posta istemcisi	238
E-posta korumasını başlatma	34
Erişim Noktası	238
ESS	238
etki alanı	239
Etki alanı ekleme	131
Etki alanını düzenleme	132
etkin nokta	239
ev ağı	239

F

Filtreleme düzeyini değiştirme	134
Filtreleme seçeneklerini ayarlama	134
Filtrelenen bir Web sitesini güncelleştirme	162
Filtrelenen bir Web sitesini kaldırma	163
Filtrelenen e-posta ile çalışma	145
Filtrelenen Web posta iletilisini kopyalama veya silme	146
Filtrelenen Web postasında olay görüntüleme	146
Filtrelenen Web siteleri	158, 161
Firewall ayarlarını geri yükleme	84
Firewall güvenliğini iyileştirme	80
Firewall güvenlik düzeylerini yönetme	74
Firewall Koruma Durumu ayarlarını yapılandırma	82
Firewall korumasını yapılandırma	73
Firewall'u anında kilitleme	83
Firewall'u başlatma	67
Firewall'u kilitleme ve geri yükleme	83
Firewall'un kilidini anında açma	83

G

geçici dosya.....	239
Gelen Olaylar günlüğünden bir bilgisayarı izleme.....	112
Gelen Olaylar günlüğünden bir bilgisayarı yasaklama.....	105
Gelen Olaylar günlüğünden güvenilen bir bilgisayar ekleme.....	101
Gelen olayları görüntüleme.....	109
Gelen ve giden trafiği analiz etme.....	115
Genel güvenlik olayı istatistiklerini görüntüleme.....	110
Genel Internet port etkinliğini görüntüleme.....	110
gerçek zamanlı tarama.....	239
Gerçek zamanlı tarama seçeneklerini ayarlama.....	38
Gerçek zamanlı virüsten korumayı başlatma.....	31
Gerçek zamanlı virüsten korumayı durdurma.....	31
Geri Dönüşüm Kutusu.....	239
geri yükleme.....	239
Giden Olaylar günlüğünden program bilgilerini alma.....	92
Giden Olaylar günlüğünden tam erişim izni verme.....	87
Giden Olaylar günlüğünden yalnızca giden erişim izni verme.....	88
Giden olayları görüntüleme.....	87, 109
Görev zamanlama.....	195
görüntü filtreleme.....	239
Güncelleştirmeleri denetleme.....	13, 14
Günlüğe kaydetme, izleme ve analiz....	107
Güvenilen bilgisayar bağlantısı ekleme	100
Güvenilen bilgisayar bağlantısını düzenleme.....	101
Güvenilen bilgisayar bağlantısını kaldırma.....	102
Güvenilenler listelerini kullanma.....	51
Güvenilenler listelerini yönetme.....	51
güvenilenler listesi.....	239
Güvenilenler listesi türleri hakkında.....	52
Güvenlik açıklarını düzeltme.....	218
güvenlik duvarı.....	239
Güvenlik duvarı korumasını başlatma....	67
Güvenlik duvarı korumasını durdurma...	68
Güvenlik düzeyini Açık seçeneğine ayarlama.....	77
Güvenlik düzeyini Gizli seçeneğine ayarlama.....	75
Güvenlik düzeyini Güvenilen seçeneğine ayarlama.....	76

Güvenlik düzeyini Kilitle seçeneğine ayarlama.....	75
Güvenlik düzeyini Sıkı seçeneğine ayarlama.....	76
Güvenlik düzeyini Standart seçeneğine ayarlama.....	76

H

HackerWatch dersini başlatma.....	118
harici sabit disk.....	240
hızlı arşivleme.....	240
hileli erişim noktası.....	240
hizmet reddi.....	240

I

Internet.....	240
Internet güvenliği hakkında bilgi alma ..	117
Internet trafiğini izleme.....	111, 114
IP adresi.....	240
IP hilesi.....	241

i

içerik derecelendirme grubu.....	240
içerik derecelendirme grubunu ayarlama.....	157, 158
ileti kimlik doğrulama kodu (MAC).....	240
İletin işleme ve işaretlenme biçimini değiştirme.....	137, 142
intranet.....	240
İstatistiklerle Çalışma.....	110
isteğe bağlı tarama.....	241
istemci.....	241
İzinsiz Giriş Tespiti Olayları günlüğünden bir bilgisayarı izleme.....	112
İzinsiz Giriş Tespiti Olayları günlüğünden bir bilgisayarı yasaklama.....	105
İzinsiz giriş tespiti olaylarını görüntüleme.....	109
İzinsiz giriş tespitini yapılandırma.....	81
izleme konumları.....	241
İzlenen bir IP adresini izleme.....	113
izlenen dosya türleri.....	241

K

kaba kuvvet saldırısı.....	241
kablosuz bağdaştırıcı.....	241
kara liste.....	241
Karakter kümesi filtrelerini uygulama ...	136
karantina.....	241
Karantinadaki dosyalarla çalışma.....	60
Karantinadaki programlar ve tanımlama bilgileriyle çalışma.....	61
kayıt defteri.....	241
kısayol.....	241

kimlik doğrulama	241
Kişisel bilgileri koruma	168
Kişisel filtre ekleme	137
Kişisel filtreleri kullanma	137
Kişisel filtreyi belirtme	137, 138
Kişisel filtreyi düzenleme	138
Kişisel filtreyi kaldırma	138
kitaplık	242
komut dosyası	242
Komut dosyası tarama korumasını başlatma	34
Koruma durumu hakkında bilgi	7, 8, 9
Koruma hizmetleri hakkında bilgi	10
Koruma kategorileri hakkında bilgi	7, 9, 27
Koruma sorunlarını el ile onarma	19
Koruma sorunlarını onarma	8, 18
Koruma sorunlarını onarma veya yok sayma	8, 17
Koruma sorunlarını otomatik olarak onarma	18
Koruma sorunlarını yok sayma	20
Koruma sorununu yok sayma	20
köke inme	242
Kullanıcıları yapılandırma	152
Kullanıcının içerik derecelendirme grubunu ayarlar	158
Kullanılabilir ağ yazıcısı yükleme	234

L

LAN	242
launchpad	242
Lisans	252

M

MAC adresi	242
MAPI	242
McAfee Anti-Spam	119
McAfee Data Backup	173
McAfee EasyNetwork	219
McAfee Hakkında	251
McAfee hesabınızı yönetme	11
McAfee Internet Security	3
McAfee kullanıcılarıyla çalışma	153, 154
McAfee kullanıcısı ekleme	154
McAfee Network Manager	205
McAfee Personal Firewall	63
McAfee Privacy Service	149
McAfee QuickClean	189
McAfee SecurityCenter	5
McAfee Shredder	201
McAfee Virtual Technician'ı kullanma...	254
McAfee VirusScan	29
McAfee yönetici parolasını alma	156
McAfee yönetici parolasını değiştirme..	156

McAfee'ye spam raporlama	145
Mevcut sistem hizmeti portuna erişim izni verme	95
Mevcut sistem hizmeti portuna erişimi engelleme	95
MSN	242
Müşteri Desteği ve Teknik Destek	253

N

Network Manager özellikleri	206
Network Manager simgeleri hakkında bilgi	207
NIC	242
numara çevirici	242

O

olası istenmeyen program (PUP)	243
Olası istenmeyen programlarla çalışma .	60
Olası uygunsuz Web resimlerini filtreleme	157
olay	243
Olay günlüğü ayarlarını yapılandırma ..	108
Olay Günlüğü Kaydetme	108
Olayları görüntüleme	18, 27
ortadaki adam saldırısı	243
Otomatik arşivlemeleri zamanlama	180
Otomatik arşivlemeyi kesme	181
Otomatik güncelleştirmeleri devre dışı bırakma	14
Otomatik güncelleştirmeleri yapılandırma	14
Oyun oynarken bilgi uyarılarını gösterme veya gizleme	23
Oyun sırasında uyarıları görüntüleme	71

Ö

Öğenin ayrıntılarını görüntüleme	211
ön bellek	243
Özel filtreyi devre dışı bırakma	135
Özellikler	174

P

parola	243
Parola ekleme	170
Parola Mahzeni	243
Parola Mahzeni parolanızı değiştirme ..	171
Parola Mahzeni parolanızı sıfırlama	172
Parola Mahzeni'ni ayarlama	170
Parolaları koruma	169
Parolayı değiştirme	170
Parolayı kaldırma	171
Paylaşılan bir dosyayı arama	229
Paylaşılan dosyayı kopyalama	229
paylaşılan şifre	243

Paylaşılan yazıcılarla çalışma	234
paylaştırma.....	243
PCI kablosuz bağdaştırıcı kartları	243
Personal Firewall özellikleri	64
phishing	243
Phishing korumasını devre dışı bırakma	148
Phishing korumasını yapılandırma	147
Ping isteği ayarlarını yapılandırma	81
POP3	244
port	244
PPPoE	244
Privacy Service özellikleri	150
Program bant genişliğini izleme	115
Program bilgilerini alma	92
Program etkinliğini izleme	115
Program iznini kaldırma.....	91
Programlar hakkında bilgi alma.....	92
Programlara Internet erişim izni verme ..	86
Programlara yalnızca giden erişim izni verme	88
Programları ve izinleri yönetme	85
Programların erişim izinlerini kaldırma ...	91
Programların Internet erişimini engelleme	89
protokol.....	244
proxy.....	244
proxy sunucusu	244

Q

QuickClean görevi zamanlama	195
QuickClean görevini değiştirme.....	196
QuickClean görevini silme.....	197
QuickClean özellikleri	190

R

RADIUS	244
--------------	-----

S

savaş sürücüsü	244
SecurityCenter özellikleri	6
SecurityCenter'ı güncelleştirme.....	13
SecurityCenter'ı kullanma.....	7
senkronize etme	244
Shredder özellikleri.....	202
sıkıştırma	244
sistem geri yükleme noktası	245
Sistem hizmeti portlarını yapılandırma ...	94
Sistem hizmeti portunu değiştirme	96
Sistem hizmeti portunu kaldırma	97
Sistem hizmetlerini yönetme	93
Sistem Koruması	245
Sistem Koruması seçeneklerini kullanma	44

Sistem Koruması seçeneklerini yapılandırma	45
Sistem Koruması türleri hakkında	46, 47
Sistem Koruması'nı etkinleştirme	45
SMTP	245
solucan.....	245
Son Olaylar günlüğünden erişimi engelleme.....	90
Son Olaylar günlüğünden tam erişim izni verme	87
Son Olaylar günlüğünden yalnızca giden erişim izni verme	88
Son olayları görüntüleme	27, 108
sözlük saldırısı.....	245
Spam algılamayı yapılandırma.....	133
Spam korumasını devre dışı bırakma ..	133
SSID	245
SSL.....	245
standart e-posta hesabı.....	245
sunucu.....	245

Ş

şifreleme.....	245
şifreli metin	245

T

tam arşivleme	246
Tam ve hızlı arşivlemeleri çalıştırma	180
tanımlama bilgisi.....	246
Tarama sonuçlarını görüntüleme	56
Tarama sonuçlarıyla çalışma	59
tarayıcı.....	246
Telif Hakkı	251
TKIP	246
Trafik Analizi grafiği hakkında	114
Truva Atı.....	246
Tüm diski parçalama	204
Tüm olayları görüntüleme.....	27
tümleşik ağ geçidi.....	246

U

U3.....	246
URL	246
USB	246
USB kablosuz bağdaştırıcı kartı	247
USB sürücüsü	247
Uyarı seçeneklerini yapılandırma	24
Uyarılar hakkında	70
Uyarılarla birlikte sesi açma	24
Uyarılarla çalışma.....	14, 21, 69
Uzak bilgisayarlara McAfee güvenlik yazılımı yükleme	218

V

Virtual Technician'ı başlatma	254
VirusScan özellikleri	30
virüs	247
Virüs saldırısı uyarılarını gizleme	24
Virüsler ve Truva atlarıyla çalışma	59
Virüsten korumayı ayarlama	37, 55
VPN	247

W

Web bug'ları	247
Web posta hesabı bilgilerini anlama....	124, 125
Web posta hesabı ekleme	123
Web posta hesabını düzenleme	124
Web posta hesabını kaldırma	125
Web posta hesaplarınızı ayarlama	123
Web postası	247
Web sitelerini anahtar sözcüklere göre engelleme	165
Web'de bilgileri koruma	167
Web'de gezinme saat sınırlarını ayarlama	160
WEP	247
Wi-Fi	247
Wi-Fi Alliance	247
Wi-Fi Certified	248
Windows kullanıcılarına geçme	154
Windows kullanıcılarıyla çalışma	153
WLAN	248
WPA	248
WPA2	248
WPA2-PSK	248
WPA-PSK	248

Y

Yasaklanan bilgisayar bağlantısı ekleme	103
Yasaklanan bilgisayar bağlantısını düzenleme	104
Yasaklanan bilgisayar bağlantısını kaldırma	104
yayımlama	248
Yazıcı paylaşmayı durdurma	234
Yazıcıları paylaşma	233
yedekleme	248
Yeni bir programa tam erişim izni verme	86
Yeni bir programın erişimini engelleme	89
Yeni bir sistem hizmeti portunu yapılandırma	95
Yerel arşivden bir dosyanın eski sürümünü geri yükleme	187
Yerel arşivleme gezginini kullanma	184

Yok sayılan sorunları gösterme veya

gizleme	20
yönetilen ağ	248
Yönetilen ağa katılma	212
Yönetilen ağı terk etme	226
Yönetilen bir ağ kurma	209
Yönetilen bir ağa katılma	212, 222, 226
Yönetilen bir bilgisayarın izinlerini değiştirme	217
yönlendirici	249
yüzeysel izleme konumları	249