McAfee®

VirusScan® Plus

AntiVirus, Firewall & AntiSpyware

Kullanıcı Kılavuzu

İçindekiler

Giriş **3**

McAfee SecurityCenter....5
SecurityCenter özellikleri....6
SecurityCenter'ı kullanma....7
Koruma sorunlarını onarma veya yok sayma....17
Uyarılarla çalışma....21
Olayları görüntüleme....27
McAfee VirusScan....29
VirusScan özellikleri....30
Bilgisayarınızı tarama....31
Tarama sonuçlarıyla çalışma....35
Tarama türleri....38
Ek koruma kullanma....41
Virüsten korumayı ayarlama....45
McAfee Personal Firewall....61
Personal Firewall özellikleri....62
Firewall'u Başlatma....63
Uyarılarla çalışma....65
Bilgi uyarılarını yönetme....67
Firewall korumasını yapılandırma....69
Programları ve izinleri yönetme....79
Bilgisayar bağlantılarını yönetme....85
Sistem hizmetlerini yönetme....93
Günlüğe kaydetme, izleme ve analiz....99
Internet güvenliği hakkında bilgi alma....109
McAfee QuickClean....111
QuickClean özellikleri....112
Bilgisayarınızı temizleme....113
Bilgisayarınızı birleştirme....117
Görev zamanlama....119
McAfee Shredder....123
Shredder özellikleri....124
Dosyaları, klasörleri ve diskleri parçalama....124
McAfee Network Manager....127
Network Manager özellikleri....128
Network Manager simgeleri hakkında bilgi....129
Yönetilen bir ağ kurma....131
Ağı uzaktan yönetme....137
Ağlarınızı izleme....143
McAfee EasyNetwork....147
EasyNetwork özellikleri....148
EasyNetwork'ü ayarlama....149
Dosyaları paylaşma ve gönderme....153
Yazıcıları paylaşma....159

Başvuru 161

Sözlük **162**

McAfee Hakkında **175**

Lisans 175
Telif Hakkı 176
Müşteri Desteği ve Teknik Destek 177
McAfee Virtual Technician'ı kullanma 178

Dizin **188**

BÖLÜM 1

Giriş

Bilgisayarınızı McAfee'nin güvenlik duvarı, virüs tarama ve casus yazılımdan koruma teknolojilerinin savunmasıyla donatın. VirusScan Plus'ı kullanarak bilgisayarınızı virüslerden koruyabilir, Internet trafiğinde şüpheli etkinliği izleyebilir ve casus yazılımların kişisel bilgilerinizi tehlikeye atmasını engelleyebilirsiniz.

Bu bölümde

McAfee SecurityCenter 5
McAfee VirusScan 29
McAfee Personal Firewall 61
McAfee QuickClean 111
McAfee Shredder 123
McAfee Network Manager 127
McAfee EasyNetwork 147
Başvuru 161
McAfee Hakkında 175
Müşteri Desteği ve Teknik Destek 177

BÖLÜM 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 algılarsa, 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
Koruma sorunlarını onarma veya yok sayma 17
Uyarılarla çalışma 21
Olayları görüntüleme 27

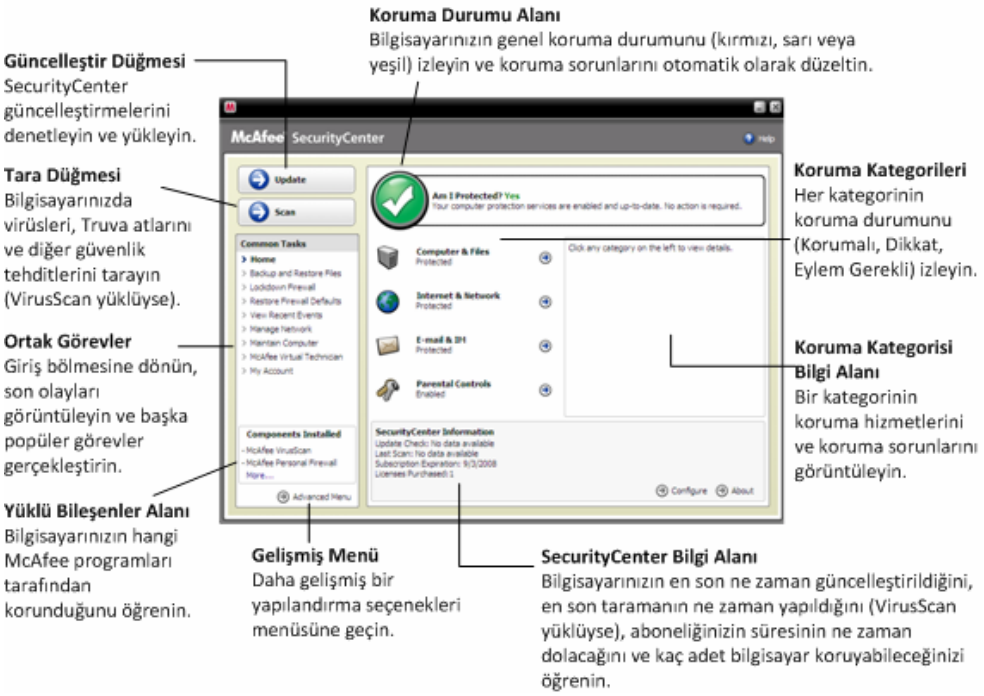
SecurityCenter özellikleri

Basitleştirilmiş koruma durumu	Kolayca bilgisayarınızın korunma durumunu inceleyin, güncelleştirmeleri denetleyin ve korunma sorunlarını düzeltin.
Otomatik güncelleştirmeler ve yükseltmeler	SecurityCenter, programlarınız için güncelleştirmeleri otomatik olarak yükleyip kurar. Bir McAfee programının yeni sürümü çıktığında, aboneliğiniz geçerli olduğu sürece otomatik olarak bilgisayarınıza aktarılır ve böylece her zaman en güncel korumaya sahip olduğunuzdan emin olursunuz.
Gerçek zamanlı uyarılar	Güvenlik uyarıları, acil virüs saldırılarını ve güvenlik tehditlerini size bildirir.

BÖLÜM 3

SecurityCenter'ı kullanma

SecurityCenter'ı 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
Aboneliklerinizi yönetme..... 11
SecurityCenter'ı güncelleştirme 13

Koruma durumu hakkında bilgi

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

Koruma hizmetlerini yapılandırmak için bir kategori adını tıklatın ve varsa bu hizmetlerle ilgili algılanan güvenlik sorunlarını görüntüleyin. Bilgisayarınızın koruma durumu kırmızı veya sarı ise, bir veya birkaç kategoride *Eylem Gerekli* veya *Dikkat* iletisi görüntülenir; bu, SecurityCenter'ın 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 ▪ Casus Yazılımdan Koruma ▪ Sistem Koruması ▪ Windows Koruması ▪ PC Sağlığı
Internet ve Ağ	Internet ve Ağ kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: ▪ Güvenlik Duvarı Koruması ▪ Phishing Koruması ▪ Kimlik Koruma
E-posta ve Anlık İleti	E-posta ve Anlık İleti kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: ▪ E-Posta Virüsünden Koruma ▪ IM Virüsten Koruma ▪ E-Posta Casus Yazılımdan Koruma ▪ IM Casus Yazılımdan Koruma ▪ Spam'den Korunma
Ebeveyn Denetimleri	Ebeveyn Denetimleri kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: ▪ İçerik Engelleme

Koruma hizmetleri hakkında bilgi

Koruma hizmetleri, bilgisayarınızı ve dosyalarınızı korumak için yapılandırdığınız çeşitli güvenlik bileşenleridir. Koruma hizmetleri, doğrudan McAfee programlarıyla ilişkilidir. Örneğin VirusScan yüklediğinizde, şu koruma hizmetlerini kullanabilirsiniz: Virus Protection, Spyware Protection, Sistem Koruması ve Komut Dosyası Tarama. Bu özel koruma hizmetleri hakkında ayrıntılı bilgi için VirusScan yardımına bakın.

Varsayılan olarak, bir programı yüklediğinizde bu programla ilişkili tüm koruma hizmetleri etkindir; ancak istediğiniz zaman koruma hizmetini devre dışı bırakabilirsiniz. Örneğin Ebeveyn Denetimleri 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.

Aboneliklerinizi yönetme

Satın aldığınız her McAfee koruma ürünü, ürünü belli bir süre boyunca belirli sayıda bilgisayarda kullanmanızı sağlayan bir abonelikle birlikte gelir. Aboneliğinizin süresi satın aldığınız ürüne göre değişir, ancak genellikle ürününüzü etkinleştirdiğinizde başlar. Etkinleştirme basit ve ücretsiz bir işlemdir (yalnızca Internet bağlantınızın olması yeterlidir), ancak size bilgisayarınızı en son tehditlerden koruyan düzenli ve otomatik ürün güncelleştirmeleri alma hakkı tanıdığı için son derece önemlidir.

Etkinleştirme, normalde ürün yüklendiği zaman gerçekleşir, ancak beklemeye karar verirseniz (örneğin Internet bağlantınız olmadığı için) etkinleştirme için 15 gün süreniz vardır. 15 gün içinde etkinleştirmezseniz, ürünleriniz artık kritik güncelleştirmeleri almaz veya taramalar gerçekleştirmez. Ayrıca aboneliğinizin süresi sona ermeye yaklaştığında size bunu düzenli aralıklarla (ekran iletileriyle) bildiririz. Bu yolla, aboneliğinizi erkenden yenileyerek veya Web sitemizde otomatik yenilemeyi ayarlayarak, korumanızda kesinti olmasını önleyebilirsiniz.

SecurityCenter'da etkinleştirmenizi isteyen bir bağlantı görürseniz, aboneliğiniz henüz etkinleştirilmemiş demektir. Aboneliğinizin süresinin ne zaman dolacağını görmek için Hesabım sayfanızı denetleyebilirsiniz.

McAfee hesabınıza erişme

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

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

Ürününüzü etkinleştirme

Etkinleştirme normalde ürününüzü yüklediğinizde gerçekleşir. Ancak gerçekleşmezse, SecurityCenter'da etkinleştirmenizi isteyen bir bağlantı görürsünüz. Ayrıca bunu size düzenli olarak bildiririz.

- SecurityCenter Giriş bölmesinde **SecurityCenter Bilgisi** altında **Lütfen aboneliğinizi etkinleştirin**'i tıklatın.

İpucu: Düzenli olarak görüntülenen uyarıdan da etkinleştirebilirsiniz.

Aboneliğinizi doğrulama

Süresinin sona ermediğinden emin olmak için aboneliğinizi doğrularsınız.

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

Aboneliğinizi yenileme

Aboneliğinizin süresi dolmadan kısa bir süre önce, SecurityCenter'da yenilemenizi isteyen bir bağlantı görürsünüz. Ayrıca yaklaşan süre sonunu size uyarılarla düzenli olarak bildiririz.

- SecurityCenter Giriş bölmesinde **SecurityCenter Bilgisi** altında **Yenile**'yi tıklatın.

İpucu: Ürününüzü düzenli olarak görüntülenen bildirim iletisinden de yenileyebilirsiniz. Ayrıca Hesabım sayfanıza giderek yenileyebilir veya otomatik yenilemeyi ayarlayabilirsiniz.

BÖLÜM 4

SecurityCenter'ı güncelleştirme

SecurityCenter, dört saatte bir çevrimiçi güncelleştirmeleri denetleyip yükleyerek, kayıtlı McAfee programlarınızın güncel olmasını sağlar. yüklediğiniz veya etkinleştirdiğiniz 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 önerilmese de, SecurityCenter'ın güncelleştirmeleri denetleme ve yükleme biçimini değiştirebilirsiniz. Örneğin, SecurityCenter'ı güncelleştirmeleri yükleyecek ancak kurmayacak ya da güncelleştirmeleri yüklemeden veya kurmadan önce size bildirecek şekilde yapılandırabilirsiniz. Ayrıca otomatik güncelleştirmeyi devre dışı bırakabilirsiniz.

Not: McAfee Ürününüzü CD'den yüklediyseniz, 15 gün içinde etkinleştirmeniz gerekir; aksi halde ürünleriniz kritik güncelleştirmeleri almaz veya taramalar gerçekleştirmez.

Bu bölümde

Güncelleştirmeleri denetleme 13
Otomatik güncelleştirmeleri yapılandırma 14
Otomatik güncelleştirmeleri devre dışı bırakma 15

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 bölmesinde **Güncelleştir**'i tıklatın.

İpucu: Görev çubuğunun sağ ucundaki bildirim alanında bulunan SecurityCenter simgesini sağ tıklatıp, ardından **Güncelleştirmeler**'i tıklatarak, 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 yüklemeden 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 bölmesini açın.

   Nasıl?

   1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
   2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.

2. SecurityCenter Yapılandırma bölmesinde, **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 yüklemeden 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 bölmesini açın.

   Nasıl?

   1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
   2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.

2. SecurityCenter Yapılandırma bölmesinde, **Otomatik güncelleştirmeler etkin** altında **Kapalı**'yı tıklatın.
3. Onay iletişim kutusunda **Evet**'i tıklatın.

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

BÖLÜM 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 dönüşür). 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 19

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 etkinleştirilmemiş ve tam koruma alamıyor.	Programı McAfee Web sitesinde etkinleştirin.
Aboneliğiniz sona erdi.	Hesap durumunuzu McAfee Web sitesinde denetleyin. Ayrıntılı bilgi için bkz. Aboneliklerinizi yönetme (sayfa 11).

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).

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

Koruma sorunlarını yok sayma

SecurityCenter kritik olmayan bir sorun algılarsa, bunu düzeltebilir veya yok sayabilirsiniz. Diğer kritik olmayan sorunlar (örneğin, Anti-Spam veya Ebeveyn Denetimleri yüklü değilse) otomatik olarak yok sayılır. Bilgisayarınızın koruma durumu yeşil olmadığı sürece, yok sayılan sorunlar SecurityCenter Giriş bölmesindeki 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 verirseniz, yok sayılan sorunu gösterebilirsiniz.

Koruma sorununu yok sayma

SecurityCenter kritik olmayan bir sorun algılarsa 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 bölmesinde, 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 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. SecurityCenter Yapılandırma bölmesinde **Yoksayılan Sorunlar**'ı tıklatın.
3. Yoksayılan Sorunlar bölmesinde 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 tıklatarak da sorunu yok sayabilirsiniz.

BÖLÜM 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 23

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 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 SecurityCenter Yapılandırma bölmesinde **Bilgi Uyarıları**'nı tıklatın.

3 Bilgi Uyarıları bölmesinde 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 bölmesinde 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 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, **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 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, **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 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 **Virüs veya güvenlik tehditi oluştuğunda beni uyar** onay kutusunun işaretini kaldırın.

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

Güvenlik iletilerini gizleme

Ev ağınızda daha fazla bilgisayarı koruma hakkındaki güvenlik bildirimlerini gizleyebilirsiniz. Bu iletiler aboneliğiniz, aboneliğinizle koruyabileceğiniz bilgisayarların sayısı ve kapsamını genişletme daha fazla bilgisayarı koruyacak şekilde aboneliğinizin hakkında bilgiler sağlar.

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 **Virüs önerilerini veya diğer güvenlik iletilerini göster** onay kutusunun işaretini kaldırın.

İpucu: Virüs önerilerini veya diğer güvenlik iletilerini göster onay kutusunu işaretleyerek, istediğiniz zaman bu güvenlik iletilerini gösterebilirsiniz.

BÖLÜM 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 bölmesinde **Günlüğü Görüntüle**'yi tıklatın.
3. Olay günlüğünün soldaki bölmesinde, görüntülemek istediğiniz olay türlerini tıklatın.

BÖLÜM 8

McAfee VirusScan

VirusScan'in 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
Bilgisayarınızı tarama 31
Tarama sonuçlarıyla çalışma 35
Tarama türleri 38
Ek koruma kullanma 41
Virüsten korumayı ayarlama 45

VirusScan özellikleri

Kapsamlı virüsten koruma	Kendinizi ve bilgisayarınızı virüsler, Truva atları, izleme tanımlama bilgileri, casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar gibi tehditlere karşı savunun. 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	İsterseniz tarama seçeneklerini özelleştirin ancak özelleştirme yapmasanız da bilgisayarınız korunur. Tarama hızı yavaşlarsa, minimum bilgisayar kaynağının kullanılması için seçeneği devre dışı bırakabilirsiniz; ancak virüs korumasına diğer görevlerden daha fazla öncelik tanınacağını unutmayın.
Otomatik düzeltmeler	VirusScan tarama çalıştırırken bir güvenlik tehdidi algılarsa, 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 etkinliklerin veya bilgisayar ekranınızın tamamını kaplayan herhangi bir etkinliğin keyfini çıkarırken, VirusScan el ile taramalar gibi çeşitli görevleri duraklatır.

BÖLÜM 9

Bilgisayarınızı tarama

SecurityCenter'ı ilk kez başlatmadan önce bile, 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. Tarama seçeneklerini ayarlama hakkında ayrıntılı bilgi için bkz. Virüsten korumayı ayarlama (sayfa 45).

VirusScan, düzenli aralıklarla daha kapsamlı taramalar çalıştırmanıza olanak vererek, virüsten korumaya yönelik daha ayrıntılı tarama seçenekleri sunar. SecurityCenter'dan tam, hızlı, özel veya zamanlanmış tarama çalıştırabilirsiniz. El ile taramaları, çalıştığınız sırada 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.

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

PC'nizi tarama 32
Tarama sonuçlarını görüntüleme..... 34

PC'nizi tarama

VirusScan, gerçek zamanlı tarama (PC'nizde sürekli tehdit etkinliğini izleyen), Windows Gezgini'nden el ile tarama ve SecurityCenter'dan tam, hızlı, özel veya zamanlanmış tarama gibi eksiksiz bir dizi tarama seçeneği sağlar.

Bunu yapmak için...	Bunu yapın...
Siz veya bilgisayarınız dosyalara erişince bunları tarayarak, bilgisayarınızda virüs etkinliğini sürekli izlemek için Gerçek zamanlı taramayı başlatmak	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 **Açık**'ı tıklatın. **Not:** Gerçek zamanlı tarama varsayılan olarak etkindir.
Bilgisayarınızda tehditleri hızla denetlemek için Hızlı Tarama başlatmak	1. Temel menüde **Tara**'yı tıklatın. 2. Tarama Seçenekleri bölmesinde Hızlı Tarama altında **Başlat**'ı tıklatın.
Bilgisayarınızda tehditleri kapsamlı olarak denetlemek için Tam Tarama başlatmak	1. Temel menüde **Tara**'yı tıklatın. 2. Tarama Seçenekleri bölmesinde Tam Tarama altında **Başlat**'ı tıklatın.
Ayarlarınızı temel alan bir Özel Tarama başlatmak	1. Temel menüde **Tara**'yı tıklatın. 2. Tarama Seçenekleri bölmesinde Ben Seçeceğim altında **Başlat**'ı tıklatın. 3. Şunları işaretleyerek veya işaretini kaldırarak taramayı özelleştirin: **Dosyalardaki Tüm Tehditler** **Bilinmeyen Virüsler** **Arşiv Dosyaları** **Casus Yazılımlar ve Olası Tehditler** **İzleme Tanımlama Bilgileri** **Görünmez Programlar** 4. **Başlat**'ı tıklatın.

Bunu yapmak için...	Bunu yapın...
Dosyalarda, klasörlerde veya sürücülerde tehditleri denetlemek için El İle Tarama başlatmak	1. Windows Gezgini'ni açın. 2. Dosyayı, klasörü veya sürücüyü sağ tıklatın ve sonra **Tara**'yı tıklatın.
Bilgisayarınızda tehditleri düzenli aralıklarla taramak için Zamanlanan Tarama başlatmak	1. Zamanlanan Tarama bölmesini açın. Nasıl? 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın. 2. SecurityCenter Giriş bölmesinde **Bilgisayar ve Dosyalar**'ı tıklatın. 3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklatın. 4. Bilgisayar ve Dosyalar Yapılandırma bölmesinde, virüsten korumanın etkin olduğundan emin olun ve **Gelişmiş**'i tıklatın. 5. Virüsten Koruma bölmesinde **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.

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.

Not: Tarama seçenekleri hakkında daha fazla bilgi almak için bkz. Tarama Türleri. (sayfa 38)

Tarama sonuçlarını görüntüleme

Tarama bitince, taramada neler bulunduğunu belirlemek ve bilgisayarınızın geçerli koruma durumunu analiz etmek için sonuçları görüntülersiniz. Tarama sonuçları size VirusScan'in 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** simgesine 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	1. Görev çubuğunuzdaki bildirim alanında **Tarama tamamlandı** simgesini çift tıklatın. 2. Tam Tarama, Hızlı Tarama, Özel Tarama veya El İle Tarama bölmesinde **Ayrıntılar**'ı tıklatın.
En son taramanızla ilgili ayrıntıları görüntülemek	Görev çubuğunuzdaki bildirim alanında **Tarama tamamlandı** simgesini çift tıklatın ve Tam Tarama, Hızlı Tarama, Özel Tarama veya El İle Tarama bölmesinde Taramanız altında en son taramanızın ayrıntılarını görüntüleyin.

BÖLÜM 10

Tarama sonuçlarıyla çalışma

VirusScan tarama çalıştırırken bir güvenlik tehdidi algılarsa, tehdit türüne göre tehdidi otomatik olarak ele almayı dener. Örneğin, VirusScan bilgisayarınızda bir virüs, Truva atı veya izleme tanımlama bilgisi algılarsa, virüslü dosyayı temizlemeyi dener. VirusScan bir dosyayı temizlemeyi denemeden önce her zaman onu karantinaya alır. Temiz değilse dosya 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 36
Olası istenmeyen programlarla çalışma 36
Karantinadaki dosyalarla çalışma 37
Karantinadaki programlar ve tanımlama bilgileriyle çalışma 37

Virüsler ve Truva atlarıyla çalışma

VirusScan bilgisayarınızdaki bir dosyada virüs veya Truva atı algılarsa, 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 İlerleyişi: El İle Tarama bölmesinde **Sonuçları Görüntüle**'yi tıklatın.

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

Not: VirusScan'in karantinaya aldığı dosyalarla çalışmak için bkz. Karantinadaki dosyalarla çalışma (sayfa 37).

Olası istenmeyen programlarla çalışma

VirusScan bilgisayarınızda olası istenmeyen bir program algılarsa, programı kaldırabilirsiniz veya programa güvenebilirsiniz. Programı tanımıyorsanız, bunu kaldırmayı düşünmenizi öneririz. Olası istenmeyen program kaldırıldığında, gerçekte sisteminizden silinmez. Kaldırma işlemi, programı karantinaya alarak bilgisayarınıza veya dosyalarınıza daha fazla zarar vermesini engeller.

1 Tarama Sonuçları bölmesini açın.

Nasıl?

1. Görev çubuğunuzun en sağındaki bildirim alanında **Tarama tamamlandı** simgesini çift tıklatın.
2. Tarama İlerleyişi: El İle Tarama bölmesinde **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 bölmesini 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 bölmesini 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.

Tarama türleri

VirusScan, gerçek zamanlı tarama (PC'nizde sürekli tehdit etkinliğini izleyen), Windows Gezgini'nden el ile tarama ve SecurityCenter'dan tam, hızlı, özel tarama çalıştırma veya zamanlanan taramaların gerçekleşeceği zamanı özelleştirme becerisi gibi virüsten korunmaya yönelik eksiksiz bir dizi tarama seçeneği sağlar. SecurityCenter'da tarama yapmak, tarama seçeneklerini anında değiştirme avantajı sağlar.

Gerçek Zamanlı Tarama:

Gerçek zamanlı virüsten koruma, siz veya bilgisayarınız dosyalara erişince bunları tarayarak, 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.

Bilinmeyen virüsleri tarama ve izleme tanımlama bilgilerinde ve ağ sürücülerinde tehditleri denetleme gibi gerçek zamanlı tarama için varsayılan seçenekleri ayarlayabilirsiniz. Ayrıca varsayılan olarak etkin olan arabellek taşması korumasından da yararlanabilirsiniz (Windows Vista 64 bit işletim sistemi kullanmıyorsanız). Daha fazla bilgi için bkz. Gerçek zamanlı tarama seçeneklerini ayarlama (sayfa 46).

Hızlı Tarama

Hızlı Tarama, bilgisayarınızdaki işlemlerde, kritik Windows dosyalarında ve diğer hassas alanlarda tehdit etkinliğini denetlemenize olanak verir.

Tam Tarama

Tam Tarama, tüm bilgisayarınızda PC'nizin herhangi bir yerinde bulunan virüsleri, casus yazılımları ve diğer güvenlik tehditlerini kapsamlı olarak denetlemenize olanak verir.

Özel Tarama

Özel Tarama, PC'nizde tehdit etkinliğini denetlemek için tarama ayarlarınızı seçmenize olanak verir. Özel tarama seçenekleri tüm dosyalarda, arşiv dosyalarında ve tanımlama bilgilerinde tehditleri denetlemenin yanı sıra bilinmeyen virüsleri, casus yazılımları ve görünmez dosyaları taramayı içerir.

Bilinmeyen virüsleri, arşiv dosyalarını, casus yazılımları ve olası tehditleri, izleme tanımlama bilgilerini ve görünmez dosyaları tarama gibi özel tarama için varsayılan seçenekleri ayarlayabilirsiniz. Ayrıca en az bilgisayar kaynağı kullanarak tarama yapabilirsiniz. Daha fazla bilgi için bkz. Özel tarama seçeneklerini ayarlama (sayfa 48).

El İle Tarama

El İle Tarama, anında dosyalar, klasörler ve sürücülerdeki tehditleri Windows Gezgini'nden hızla denetlemenize olanak verir.

Zamanlanan Tarama

Zamanlanan taramalar, haftanın herhangi bir gününde ve saatinde bilgisayarınızda virüsleri ve diğer tehditleri kapsamlı olarak denetler. Zamanlanan taramalar, her zaman varsayılan tarama seçeneklerinizi 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. Daha fazla bilgi için bkz. Tarama zamanlama (sayfa 50).

Not: Sizin için en iyi tarama seçeneğini başlatma hakkında bilgi için bkz. PC'nizi tarama (sayfa 32).

BÖLÜM 11

Ek koruma kullanma

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 veya web tarayıcınızda 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 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 42
Casus yazılım korumasını başlatma 42
E-posta korumasını başlatma 43
Anlık ileti korumasını başlatma 43

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 bölmesini açın.

Nasıl?

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

2 **Komut dosyası tarama koruması** altında **Açık**'ı tıklatın.

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 bölmesini açın.

Nasıl?

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

2 **Komut dosyası tarama koruması** altında **Açık**'ı tıklatın.

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 bölmesini açın.

Nasıl?

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

2 **E-posta koruması** altında **Açık**'ı tıklatın.

Not: İstediğiniz 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 bölmesini açın.

Nasıl?

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

2 **Anlık İleti koruması** altında **Açık**'ı tıklatın.

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

BÖLÜM 12

Virüsten korumayı ayarlama

Zamanlanan, özel ve gerçek zamanlı tarama 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.

Ayrıca VirusScan'in, Sistem Koruması veya Güvenilenler Listeleri kullanarak, PC'nizde olası yetkisiz veya istenmeyen değişiklikleri nasıl izlemesini ve yönetmesini istediğinize karar verebilirsiniz. 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. Güvenilenler Listelerini kullanarak, dosya veya kayıt defteri değişikliklerini (Sistem Koruması), programları veya arabellek taşmalarını algılayan kurallara güvenmek mi yoksa kaldırmak mı istediğinize karar verebilirsiniz. Öğeye 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.

Bu bölümde

Gerçek zamanlı tarama seçeneklerini ayarlama 46
Özel tarama seçeneklerini ayarlama 48
Tarama zamanlama 50
Sistem Koruması seçeneklerini kullanma 51
Güvenilenler listelerini kullanma 57

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'in neleri denetleyeceğini, tarayacağı konumları ve dosya türlerini belirlemeniz gerekir. Örneğin, VirusScan'in 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 taşması 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'in neleri arayacağını, tarayacağı konumları ve dosya türlerini özelleştirmek için gerçek zamanlı tarama seçeneklerini ayarlarsınız. Seçenekler, bilinmeyen virüsleri ve tanımlama bilgilerini taramanın yanı sıra, arabellek taşma 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 bölmesinde **Bilgisayar ve Dosyalar**'ı tıklatın.
3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklatın.
4. Bilgisayar ve Dosyalar Yapılandırma bölmesinde, 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	**Bilinmeyen virüsleri tara**'yı seçin.
Tanımlama bilgilerini algılamak	**İzleme tanımlama bilgilerini tara ve temizle**'yi seçin.
Ağınıza bağlı sürücülerde virüsleri ve diğer olası tehditleri algılamak	**Ağ sürücülerini tara**'yı seçin.
Bilgisayarınızı arabellek taşmalarından korumak	**Arabellek taşması korumasını etkinleştir**'i seçin.
Hangi dosya türlerinin taranacağını belirtmek	**Tüm dosyalar (önerilir)** veya **Yalnızca program dosyaları ve belgeler**'i tıklatın.

Gerçek zamanlı virüsten korumayı durdurma

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 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.

Özel tarama seçeneklerini ayarlama

Özel virüsten koruma, istediğinizde dosyaları sizin taramanıza olanak verir. Özel taramayı başlattığınızda, VirusScan daha kapsamlı birtakım tarama seçenekleri kullanarak bilgisayarınızda virüsleri ve diğer olası zararlı öğeleri denetler. Özel tarama seçeneklerini değiştirmek için VirusScan'in tarama sırasında neleri denetleyeceğini belirlemeniz gerekir. Örneğin, VirusScan'in virüsleri, casus yazılım veya reklam yazılım gibi olası istenmeyen programları, görünmez programları ve köke inme programlarını (bilgisayarınıza yetkisiz erişim verebilen) ve Web sitelerinin davranışınızı izlemek için kullanabileceği tanımlama bilgilerini arayıp aramayacağını belirleyebilirsiniz. Denetlenen dosya türlerini de belirlemeniz gerekir. Örneğin, VirusScan'in 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 özel tarama çalıştırdığında, bilgisayarınızdaki ve tüm ağ sürücülerindeki tüm sürücüleri ve klasörleri denetler; ancak varsayılan konumları, gereksinimlerinize uygun olarak değiştirebilirsiniz. Örneğin, yalnızca kritik PC dosyalarını, masaüstünüzdeki öğeleri veya Program Files klasöründeki öğeleri tarayabilirsiniz. Her özel 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 etkinliklerin veya bilgisayar ekranınızın tamamını kaplayan herhangi bir etkinliğin keyfini çıkarırken, VirusScan otomatik güncelleştirmeler ve özel taramalar gibi çeşitli görevleri duraklatır.

Özel tarama seçeneklerini ayarlama

Özel tarama sırasında VirusScan'in neleri arayacağını, tarayacağı konumları ve dosya türlerini özelleştirmek için özel tarama seçeneklerini ayarlarsınız. Seçenekler; bilinmeyen virüsleri, dosya arşivlerini, casus yazılımları ve olası istenmeyen programları, izleme tanımlama bilgilerini, köke inme programlarını ve hayalet programları içerir. Özel tarama sırasında VirusScan'in virüsleri ve diğer zararlı öğeleri nerede arayacağını belirlemek için özel tarama konumunu da ayarlayabilirsiniz. Bilgisayarınızdaki tüm dosyalar, klasörler ve sürücüleri tarayabilir veya tarama işlemini belirli klasörler ve sürücülerle sınırlandırabilirsiniz.

1 Özel Tarama bölmesini açın.

Nasıl?

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

2 Özel tarama seçeneklerinizi belirtin ve sonra **Tamam**'ı tıklatın.

Bunu yapmak için...	Bunu yapın...
Bilinmeyen virüsleri ve bilinen virüslerin yeni türevlerini algılamak	**Bilinmeyen virüsleri tara**'yı seçin.
.Zip ve diğer arşiv dosyalarındaki virüsleri algılamak ve kaldırmak	**Arşiv dosyalarını tara**'yı seçin.
Casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programları algılamak	**Casus yazılımları ve olası tehditleri tara**'yı seçin.
Tanımlama bilgilerini algılamak	**İzleme tanımlama bilgilerini tara ve temizle**'yi seçin.
Varolan Windows sistem dosyalarını değiştirebilen ve kullanabilen köke inme programlarını ve hayalet programları algılamak	**Görünmez programları tara**'yı seçin.
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**'yı seçin.

Bunu yapmak için...	Bunu yapın...
Hangi dosya türlerinin taranacağını belirtmek	**Tüm dosyalar (önerilir)** veya **Yalnızca program dosyaları ve belgeler**'i tıklatın.

3 **Taranacak Varsayılan Konum**'u tıklatın, ardından taramak veya atlamak istediğiniz konumları seçin veya işaretini kaldırın ve sonra **Tamam**'ı tıklatın:

Bunu yapmak için...	Bunu yapın...
Bilgisayarınızdaki tüm dosya ve klasörleri taramak	**Bilgisayarım**'ı seçin.
Bilgisayarınızdaki belirli dosyalar, klasörler ve sürücüleri 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.

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.

Varsayılan tarama seçeneklerinizi kullanarak tüm bilgisayarınızda virüsleri ve diğer tehditleri kapsamlı olarak denetleyen taramalar zamanlayın. Varsayılan olarak, VirusScan haftada bir kez zamanlanan tarama gerçekleştirir.

1 Zamanlanan Tarama bölmesini açın.

Nasıl?

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

5. Virüsten Koruma bölmesinde **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 (Internet'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, appInit DLL dosyaları ve Windows hosts dosyasını içerir. Windows Sistem Koruması teknolojisi, bunları izleyerek 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.

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 bölmesini açın.

Nasıl?

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

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

Not: **Kapalı**'yı tıklatarak 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 bölmesini 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 bölmesinde **Bilgisayar ve Dosyalar**'ı tıklatın.
3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklatın.
4. Bilgisayar ve Dosyalar Yapılandırma bölmesinde, Siste Koruması'nın etkin olduğundan emin olun ve **Gelişmiş**'i tıklatın.

2 Listeden 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 54).

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 (Internet'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.

Sistem Koruması	Şunları algılar...
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.

Sistem Koruması	Şunları algılar...
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 algılarsa, buna güvenmenizi veya bunu kaldırmanızı ister. Öğeye 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 verirseniz bunu yapabilirsiniz. Engellendiğinde, öğenin çalışması veya her girişimde bulunduğunda 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'in yeniden algılaması için güvenilenler listesinden de kaldırabilirsiniz.

1 Güvenilenler Listeleri bölmesini açın.

Nasıl?

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

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 tıklatın.
- 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 58).

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.

Seçenek	Açıklama
Windows Sistem Koruması	Güvenilenler Listeleri bölmesindeki Windows Sistem Koruması, VirusScan tarafından önceden algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölmesinden izin vermeyi seçtiğiniz, yetkisiz kayıt defteri ve dosya değişikliklerini yansıtır. Windows Sistem Koruması; içerik menüsü işleyicileri, appInit 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 bölmesindeki Tarayıcı Sistem Koruması, VirusScan tarafından önceden algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölmesinden 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 davranışı 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 bölmesinden izin vermeyi seçtiğiniz olası istenmeyen programlardır.
Güvenilen Arabellek Taşmaları	Güvenilen arabellek taşmaları, VirusScan tarafından algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölmesinden 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.

BÖLÜM 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 62
Firewall'u Başlatma 63
Uyarılarla çalışma 65
Bilgi uyarılarını yönetme 67
Firewall korumasını yapılandırma 69
Programları ve izinleri yönetme 79
Bilgisayar bağlantılarını yönetme 85
Sistem hizmetlerini yönetme 93
Günlüğe kaydetme, izleme ve analiz 99
Internet güvenliği hakkında bilgi alma 109

Personal Firewall özellikleri

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 gerekmediğine karar vermenize 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 bilgisayarınızı izinsiz giriş denemelerinden, istenmeyen programlardan ve ağ trafiğinden koruyun.
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.
Güvenlik duvarını 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. Sezgisel işlevler kullanarak, saldırı belirtileri veya korsanlık girişimi özellikleri sergileyen öğeleri engelleyip üçüncü bir koruma katmanı sağlıyoruz.
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.

BÖLÜM 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 Otomatik güvenlik düzeyi (programların yalnızca giden Internet erişimine izin verme seçeneği belirlenmiş) otomatik olarak etkinleştirilir.

Internet ve Ağ Yapılandırması bölmesinden 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 bölmesini açın.

Bu bölümde

Güvenlik duvarı korumasını başlatma..... 63
Güvenlik duvarı korumasını durdurma 64

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 bölmesinde **Internet ve Ağ**'ı ve sonra **Yapılandır**'ı tıklatın.
2. Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruması devre dışı** altında **Açık**'ı tıklatın.

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 tıklatın.
2. Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Kapalı**'yı tıklatın.

BÖLÜM 15

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..... 66

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, 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 Bağlantısı** uyarısı görüntülenir. Bu ağa atamak istediğiniz güven düzeyini belirtebilirsiniz ve sonra Ağlar listenizde bu ağ görüntülenir. Akıllı Öneriler etkinse, bilinen programlar otomatik olarak Program İzinleri bölmesine 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.

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.

BÖLÜM 16

Bilgi uyarılarını yönetme

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

Bu bölümde

Oyun sırasında uyarıları görüntüleme 67
Bilgi uyarılarını gizleme 67

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.

BÖLÜM 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 Otomatik 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 70
Akıllı Önerileri uyarılar için yapılandırma 72
Firewall güvenliğini iyileştirme 74
Firewall'u kilitleme ve geri yükleme 77

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 Otomatik seçeneğine ayarlıdır.

Otomatik güvenlik düzeyi ayarlıysa ve Akıllı Öneriler etkinse, sarı uyarılar gelen erişimi gerektiren bilinmeyen programlara erişim izni vermek veya erişimi engellemek için seçenek sunar. Yeşil uyarılar varsayılan olarak devre dışı olsa bile, bilinen programlar algılandığında bunlar görüntülenir ve otomatik olarak erişim izni verilir. Erişim izni verilmesi, programın giden bağlantılar oluşturmasına ve istenmeyen gelen bağlantıları dinlemesine olanak verir.

Genel olarak, güvenlik düzeyi ne kadar kısıtlayıcıysa (Görünmez ve Standart), 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 üç güvenlik düzeyi açıklanmaktadır:

Düzey	Açıklama
Görünmez	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 bölmesinde görüntülenir.
Standart	Gelen ve giden bağlantıları izler ve yeni programlar Internet'e erişmeye çalıştığında sizi uyarır. Engellenen ve eklenen programlar, Program İzinleri bölmesinde görüntülenir.
Otomatik	Programların gelen ve giden (tam) veya yalnızca giden Internet erişimine izin verir. Varsayılan güvenlik düzeyi, programların yalnızca giden erişimine izin verme seçeneği belirlenmiş durumda Otomatik olarak ayarlıdır. Bir programa tam erişim izni verilirse, Firewall programa otomatik olarak güvenir ve bunu Program İzinleri bölmesinde 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 güvenilmez.

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

Güvenlik düzeyini Görünmez seçeneğine ayarlama

Açık portlar dışında tüm gelen ağ bağlantılarını engellemek ve bilgisayarınızın Internet'teki varlığını gizlemek için Firewall'un güvenlik düzeyini Görünmez 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, **Görünmez** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
4. **Tamam**'ı tıklatın.

Not: Görünmez modunda, yeni programlar giden Internet bağlantısı istediğinde veya gelen bağlantı istekleri aldığında Firewall sizi uyarır.

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 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, **Standart** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
4. **Tamam**'ı tıklatın.

Güvenlik düzeyini Otomatik seçeneğine ayarlama

Tam erişim veya yalnızca giden ağ erişimi izni vermek için Firewall'un güvenlik düzeyini Otomatik 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, **Otomatik** 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.

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 uygulandığında (ve güvenlik düzeyi yalnızca giden erişimi etkin olarak Otomatik seçeneğine ayarlandığında), Firewall otomatik olarak bilinen programlara izin verir ve olası tehlikeli programları engeller.

Akıllı Öneriler uygulanmadığında, Firewall Internet erişimine izin vermez veya engellemez ve uyarının içinde öneri sağlamaz.

Akıllı Öneriler Göster seçeneğine ayarlandığında, uyarıyla erişime izin vermeniz veya engellemeniz istenir ve Firewall uyarının içinde öneri sağlar.

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 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, **Akıllı Öneriler**'in altında **Akıllı Önerileri Uygula**'yı 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 algılarsa, programın Internet'e erişmesini otomatik olarak engeller.

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, **Akıllı Öneriler**'in altında **Akıllı Önerileri Uygulama**'yı seçin.
4. **Tamam**'ı tıklatın.

Akıllı Önerileri görüntüleme

Uyarıların yalnızca uyarı içinde öneri görüntülemesi ve böylece tanınmayan ve tehlikeli olma olasılığı bulunan programlara izin verme veya engelleme kararını verebilmeniz için Akıllı Öneriler'i görüntüleyebilirsiniz.

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, **Akıllı Öneriler**'in altında **Akıllı Önerileri Göster**'i seçin.
4. **Tamam**'ı tıklatın.

Firewall güvenliğini iyileştirme

Bilgisayarınızın güvenliği çeşitli şekillerde tehlikeye girebilir. Örneğin, bazı programlar Windows® başlarken Internet'e bağlanmaya çalışabilir. Ayrıca deneyimli bilgisayar kullanıcıları, bilgisayarınızın ağa bağlı olup olmadığını belirlemek için onu izleyebilirler (ping işlemi yapabilirler). Bunun yanı sıra ileti birimleri (datagramlar) biçiminde UDP protokolünü kullanarak bilgisayarınıza bilgi gönderebilirler. Firewall, Windows başlarken programların Internet'e erişmelerini engelleyerek bu tür saldırılara karşı bilgisayarınızı korur; böylece başka kullanıcıların ağ üzerinde bilgisayarınızı algılamalarına yardımcı olan ping isteklerini engellemenize ve başka kullanıcıların bilgisayarınıza ileti birimleri (datagramlar) biçiminde bilgi göndermelerini devre dışı bırakmanıza olanak verir.

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.

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** altında **Windows başlangıcında korumayı 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**'ı tıklatın.

UDP ayarlarını yapılandırma

Diğer ağ bilgisayarı kullanıcılarının, UDP protokolünü kullanarak bilgisayarınıza ileti birimleri (datagramlar) göndermelerine izin verebilirsiniz. Ancak yalnızca bu protokolü engellemek için kapalı sistem hizmeti portunuz varsa bunu yapabilirsiniz.

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:
   - Diğer bilgisayar kullanıcılarının bilgisayarınıza ileti birimleri (datagramlar) göndermelerine izin vermek için **UDP izlemeyi etkinleştir**'i seçin.
   - Diğer bilgisayar kullanıcılarının bilgisayarınıza ileti birimleri (datagramlar) göndermelerini engellemek için **UDP izlemeyi etkinleştir**'in işaretini kaldırın.
4. **Tamam**'ı 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**'ı 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 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, Web sitelerine, e-postalara ve güvenlik güncelleştirmelerine erişim dahil olmak üzere tüm gelen ve giden ağ bağlantılarını anında engeller. Kilitleme, bilgisayarınızın ağ kablolarını çekmekle aynı etkiyi yapar. Bu ayarı kullanarak, Sistem Hizmetleri bölmesindeki açık portları engelleyebilir ve bilgisayarınızdaki bir sorunu izole edip sorun giderebilirsiniz.

Firewall'u anında kilitleme

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

1. McAfee SecurityCenter bölmesinde, **Ortak Görevler** altında **Güvenlik Duvarını Kilitle**'yi tıklatın.
2. Güvenlik Duvarını Kilitle bölmesinde **Güvenlik Duvarı Kilitlemesini Etkinleştir**'i tıklatın.
3. Onaylamak için **Evet**'i tıklatın.

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

Firewall'un kilidini anında açma

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

1. McAfee SecurityCenter bölmesinde, **Ortak Görevler** altında **Güvenlik Duvarını Kilitle**'yi tıklatın.
2. Kilit Etkin bölmesinde **Güvenlik Duvarı Kilitlemesini Devre Dışı Bırak**'ı tıklatın.
3. Onaylamak için **Evet**'i tıklatın.

Firewall ayarlarını geri yükleme

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

1. McAfee SecurityCenter bölmesinde **Güvenlik Duvarı Varsayılanlarını Geri Yükle**'yi tıklatın.
2. Güvenlik Duvarı Koruması Varsayılanlarını Geri Yükle bölmesinde **Varsayılanları Geri Yükle**'yi tıklatın.
3. Onaylamak için **Evet**'i tıklatın.
4. **Tamam**'ı tıklatın.

BÖLÜM 18

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 80
Programlara yalnızca giden erişim izni verme 81
Programların Internet erişimini engelleme 82
Programların erişim izinlerini kaldırma 83
Programlar hakkında bilgi alma 84

Programlara Internet erişim izni verme

Internet tarayıcıları gibi bazı programların düzgün çalışabilmesi için Internet'e erişmeleri 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 tıklatın.
2. **Raporlar ve Günlükler**'i tıklatın.
3. **Son Olaylar** altında, olay açıklamasını seçin ve ardından **Erişime İzin Ver**'i tıklatın.
4. Onaylamak için Program İzinleri iletişim kutusunda **Evet**'i tıklatın.

İlgili konular

- Giden olayları görüntüleme (sayfa 101)

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

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 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, **Engellenen** veya **Tam Erişim** seçeneğine ayarlı bir program seçin.
5. **Eylem** altında **Yalnızca Giden Erişimine İzin Ver**'i tıklatın.
6. **Tamam**'ı tıklatın.

Son Olaylar günlüğünden yalnızca giden erişim izni verme

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

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

Giden Olaylar günlüğünden yalnızca giden erişim izni verme

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

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

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 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, **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 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 **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 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 bir program seçin.
5. **Eylem** altında **Program İznini Kaldır**'ı tıklatın.
6. **Tamam**'ı tıklatın.

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 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 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 bölmesinde **Gelişmiş Menü**'yü tıklatın.
2. **Raporlar ve Günlükler**'i tıklatın.
3. Son Olaylar altında bir olay seçin ve sonra **Günlüğü 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.

BÖLÜM 19

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. Güvenilen bir bilgisayara solucan veya başka bir mekanizma bulaşmışsa, bilgisayarınız etkilere açık olabilir. Ayrıca, McAfee güvendiğiniz bilgisayarın güvenlik duvarının yanı sıra güncel bir antivirüs programıyla korunmasını önerir. Firewall, **Ağlar** listesinde bulunan güvenilen IP adreslerinin trafiğini günlüğe kaydetmez veya bunlardan olay uyarıları üretmez.

Bilinmeyen, şüpheli veya güvenilmeyen IP adresleriyle ilişkili bilgisayarların, bilgisayarınıza bağlanmasını yasaklayabilirsiniz.

Firewall tüm istenmeyen trafiği engellediği için, genellikle bir IP adresini yasaklamanız gerekmez. Bir IP adresini ancak Internet bağlantısının belirli bir tehdit olduğundan eminseniz yasaklamalısınız. DNS veya DHCP sunucunuz ya da diğer ISS ile ilişkili sunucular gibi önemli IP adreslerini engellemediğinizden emin olun.

Bu bölümde

Bilgisayar bağlantıları hakkında 86
Bilgisayar bağlantılarını yasaklama 89

Bilgisayar bağlantıları hakkında

Bilgisayar bağlantıları, herhangi bir ağ ile kendi ağınız üzerindeki bilgisayarlar arasında oluşturduğunuz bağlantılardır. **Ağlar** listesinde IP adresleri ekleyebilir, düzenleyebilir ve kaldırabilirsiniz. Bu IP adresleri, bilgisayarınıza bağlanırken bir güvenlik düzeyi atamak istediğiniz ağlarla ilişkilidir: Güvenilen, Standart ve Kamu.

Düzey	Açıklama
Güvenilen	Firewall, bir IP'den gelen trafiğin herhangi bir port aracılığıyla bilgisayarınıza erişmesine izin verir. Güvenilen bir IP adresiyle ilişkili bilgisayar ve sizin bilgisayarınız arasındaki etkinlik, Firewall tarafından filtrelenmez veya analiz edilmez. Varsayılan olarak, Firewall'un bulduğu ilk özel ağ, **Ağlar** listesinde Güvenilen olarak listelenir. Yerel veya ev ağınızdaki bilgisayar veya bilgisayarlar, Güvenilen ağa örnek olarak verilebilir.
Standart	Firewall, bilgisayarınıza bağlandığında IP'den (ancak bu ağdaki herhangi bir bilgisayardan değil) gelen trafiği denetler ve **Sistem Hizmetleri** listesindeki kurallara göre buna izin verir veya engeller. Firewall, trafiği günlüğe kaydeder ve Standart IP adreslerinden olay uyarıları üretir. Şirket ağınızdaki bilgisayar veya bilgisayarlar, Standart ağa örnek olarak verilebilir.
Kamu	Firewall, **Sistem Hizmetleri** listesindeki kurallara göre kamu ağından gelen trafiği denetler. Bir kafede, otelde veya havaalanında bulunan Internet ağı Kamu ağına örnek olarak verilebilir.

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

Bilgisayar bağlantısı ekleme

Güvenilen, standart veya kamu bilgisayar bağlantısı ve bununla ilişkili IP adresi ekleyebilirsiniz.

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 **Ağlar**'ı tıklatın.
4. Ağlar bölmesinde **Ekle**'yi tıklatın.
5. Bilgisayar bağlantısı IPv6 ağı üzerindeyse, **IPv6** onay kutusunu seçin.

6 **Kural Ekle** altında aşağıdakilerden birini gerçekleştirin:
   - **Tek**'i seçin ve sonra IP adresini **IP Adresi** kutusuna girin.
   - **Aralık**'ı seçin ve sonra **IP Adreslerinden** ve **IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin. Bilgisayar bağlantınız bir IPv6 ağı üzerindeyse, **IP Adreslerinden** ve **Önek Uzunluğu** kutularına başlangıç IP adresini ve önek uzunluğunu girin.

7 **Tür** altında aşağıdakilerden birini gerçekleştirin:
   - Bu bilgisayar bağlantısına güvenildiğini belirtmek için **Güvenilen**'i seçin (örneğin ev ağındaki bir bilgisayar).
   - Bu bilgisayar bağlantısına (ağdaki bilgisayarlara değil) güvenildiğini belirtmek için **Standart**'ı seçin (örneğin şirket ağındaki bir bilgisayar).
   - Bu bilgisayar bağlantısının kamu olduğunu belirtmek için **Kamu**'yu seçin (örneğin Internet kafedeki, oteldeki veya havaalanındaki bir bilgisayar).

8 Sistem hizmeti Internet Bağlantısı Paylaşımı (ICS) kullanıyorsa, şu IP adresi aralığını ekleyebilirsiniz: 192.168.0.1 - 192.168.0.255.

9 İsterseniz, **Kuralın geçerlilik süresi**'ni seçip, kuralın geçerli olacağı gün sayısını girebilirsiniz.

10 Ayrıca, kural için bir açıklama da yazabilirsiniz.

11 **Tamam**'ı tıklatın.

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

Gelen Olaylar günlüğünden bir bilgisayarı ekleme

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

1 McAfee SecurityCenter bölmesinde, Ortak Görevler bölmesinde **Gelişmiş Menü**'yü tıklatın.

2 **Raporlar ve Günlükler**'i tıklatın.

3 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklatın.

4 **Internet ve Ağ**'ı tıklatın ve sonra **Gelen Olaylar**'ı tıklatın.

5 Bir kaynak IP adresi seçin ve **Şunu yapmak istiyorum** altında aşağıdakilerden birini gerçekleştirin:
   - Bu bilgisayarı **Ağlar** listenize Güvenilen olarak eklemek için **Bu IP'yi Güvenilen olarak ekle**'yi tıklatın.
   - Bu bilgisayar bağlantısını **Ağlar** listenize Standart olarak eklemek için **Bu IP'yi Standart olarak ekle**'yi tıklatın.

6 Onaylamak için **Evet**'i tıklatın.

Bilgisayar bağlantısını düzenleme

Güvenilen, standart veya kamu bilgisayar bağlantısını ve bununla ilişkili IP adresini düzenleyebilirsiniz.

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 **Ağlar**'ı tıklatın.
4. Ağlar bölmesinde bir IP adresi seçin ve ardından **Düzenle**'yi tıklatın.
5. Bilgisayar bağlantısı IPv6 ağı üzerindeyse, **IPv6** onay kutusunu seçin.
6. **Kuralı Düzenle** altında aşağıdakilerden birini gerçekleştirin:
   - **Tek**'i seçin ve sonra IP adresini **IP Adresi** kutusuna girin.
   - **Aralık**'ı seçin ve sonra **IP Adreslerinden** ve **IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin. Bilgisayar bağlantınız bir IPv6 ağı üzerindeyse, **IP Adreslerinden** ve **Önek Uzunluğu** kutularına başlangıç IP adresini ve önek uzunluğunu girin.
7. **Tür** altında aşağıdakilerden birini gerçekleştirin:
   - Bu bilgisayar bağlantısına güvenildiğini belirtmek için **Güvenilen**'i seçin (örneğin ev ağındaki bir bilgisayar).
   - Bu bilgisayar bağlantısına (ağdaki bilgisayarlara değil) güvenildiğini belirtmek için **Standart**'ı seçin (örneğin şirket ağındaki bir bilgisayar).
   - Bu bilgisayar bağlantısının kamu olduğunu belirtmek için **Kamu**'yu seçin (örneğin Internet kafedeki, oteldeki veya havaalanındaki bir bilgisayar).
8. İsterseniz **Kuralın geçerlilik süresi**'ni işaretleyip, kuralın geçerli olacağı gün sayısını girebilirsiniz.
9. Ayrıca, kural için bir açıklama da yazabilirsiniz.
10. **Tamam**'ı tıklatın.

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

Bilgisayar bağlantısını kaldırma

Güvenilen, standart veya kamu bilgisayar bağlantısını ve bununla ilişkili IP adresini kaldırabilirsiniz.

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 **Ağlar**'ı tıklatın.
4. Ağlar bölmesinde bir IP adresi seçin ve ardından **Kaldır**'ı tıklatın.
5. Onaylamak için **Evet**'i tıklatın.

Bilgisayar bağlantılarını yasaklama

Yasaklı IP'ler bölmesinde, yasaklanan IP adresleri ekleyebilir, düzenleyebilir ve kaldırabilirsiniz.

Bilinmeyen, şüpheli veya güvenilmeyen IP adresleriyle ilişkili bilgisayarların, bilgisayarınıza bağlanmasını yasaklayabilirsiniz.

Firewall tüm istenmeyen trafiği engellediği için, genellikle bir IP adresini yasaklamanız gerekmez. Bir IP adresini ancak Internet bağlantısının belirli bir tehdit olduğundan eminseniz yasaklamalısınız. DNS veya DHCP sunucunuz ya da diğer ISS ile ilişkili sunucular gibi önemli IP adreslerini engellemediğinizden emin olun.

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 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, **Yasaklı IP'ler** seçeneğini tıklatın.
4. Yasaklı IP'ler bölmesinde, **Ekle**'yi tıklatın.
5. Bilgisayar bağlantısı IPv6 ağı üzerindeyse, **IPv6** onay kutusunu seçin.

6 **Kural Ekle** altında aşağıdakilerden birini gerçekleştirin:
   - **Tek**'i seçin ve sonra IP adresini **IP Adresi** kutusuna girin.
   - **Aralık**'ı seçin ve sonra **IP Adreslerinden** ve **IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin. Bilgisayar bağlantınız bir IPv6 ağı üzerindeyse, **IP Adreslerinden** ve **Önek Uzunluğu** kutularına başlangıç IP adresini ve önek uzunluğunu girin.

7 İsterseniz, **Kuralın geçerlilik süresi**'ni seçip, kuralın geçerli olacağı gün sayısını girebilirsiniz.

8 Ayrıca, kural için bir açıklama da yazabilirsiniz.

9 **Tamam**'ı tıklatın.

10 Onaylamak için **Evet**'i tıklatın.

Yasaklanan bilgisayar bağlantısını düzenleme

Yasaklanan bir bilgisayar bağlantısını ve bununla ilişkili IP adresini düzenleyebilirsiniz.

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, **Yasaklı IP'ler** seçeneğini tıklatın.

4 Yasaklı IP'ler bölmesinde, **Düzenle**'yi tıklatın.

5 Bilgisayar bağlantısı IPv6 ağı üzerindeyse, **IPv6** onay kutusunu seçin.

6 **Kuralı Düzenle** altında aşağıdakilerden birini gerçekleştirin:
   - **Tek**'i seçin ve sonra IP adresini **IP Adresi** kutusuna girin.
   - **Aralık**'ı seçin ve sonra **IP Adreslerinden** ve **IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin. Bilgisayar bağlantınız bir IPv6 ağı üzerindeyse, **IP Adreslerinden** ve **Önek Uzunluğu** kutularına başlangıç IP adresini ve önek uzunluğunu girin.

7 İsterseniz, **Kuralın geçerlilik süresi**'ni seçip, kuralın geçerli olacağı gün sayısını girebilirsiniz.

8 Ayrıca, kural için bir açıklama da yazabilirsiniz.

9 **Tamam**'ı tıklatın.

Yasaklanan bilgisayar bağlantısını kaldırma

Yasaklanan bir bilgisayar bağlantısını ve bununla ilişkili IP adresini kaldırabilirsiniz.

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, **Yasaklı IP'ler** seçeneğini tıklatın.
4. Yasaklı IP'ler bölmesinde bir IP adresi seçin ve sonra **Kaldır**'ı tıklatın.
5. Onaylamak için **Evet**'i tıklatın.

Gelen Olaylar günlüğünden bir bilgisayarı yasaklama

Gelen Olaylar günlüğünden bir bilgisayar bağlantısını ve onunla ilişkili IP adresini yasaklayabilirsiniz. Şüpheli veya istenmeyen Internet etkinliğinin kaynağı olduğundan şüphelendiğiniz bir IP adresini yasaklamak için tüm gelen Internet trafiğinin IP adreslerini listeleyen bu günlüğü kullanın.

Sistem Hizmetleri portlarınızın açık veya kapalı olmasına bakılmaksızın bir IP adresinden gelen tüm Internet trafiğini engellemek için **Yasaklı IP'ler** listenize bir IP adresi ekleyin.

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

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 bölmesinde, **Ortak Görevler** altında, **Gelişmiş Menü**'yü tıklatın.
2. **Raporlar ve Günlükler**'i tıklatın.
3. **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklatın.
4. **Internet ve Ağ**'ı tıklatın ve ardından **İzinsiz Giriş Tespiti Olayları**'nı tıklatın.
5. Kaynak IP adresini seçin ve **Şunu yapmak istiyorum** altında **Bu IP'yi Yasakla** seçeneğini tıklatın.
6. Onaylamak için **Evet**'i tıklatın.

BÖLÜM 20

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 yapılandırma 94

Sistem hizmeti portlarını yapılandırma

Sistem hizmeti portları, bilgisayarınızda bir hizmete uzak ağ erişimi izni verecek veya engelleyecek şekilde yapılandırılabilir. Bu sistem hizmeti portları, **Ağlar** listenizde Güvenilen, Standart veya Kamu olarak listelenen bilgisayarlar için açılabilir veya kapatılabilir.

Aşağıdaki listede, yaygın sistem hizmetleri ve ilişkili portları gösterilmektedir:

- Ortak İşletim Sistemi Portu 5357
- 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 Çağrıları (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 sistem hizmetine uzak ağ erişimi 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 tıklatın.
2. Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
3. Güvenlik Duvarı bölmesinde **Sistem Hizmetleri**'ni tıklatın.
4. **Sistem Hizmeti Portu Aç** altında portunu açmak için bir sistem hizmeti seçin.
5. **Düzenle**'yi tıklatın.
6. Aşağıdakilerden birini gerçekleştirin:
   - Portu güvenilen, standart veya kamu ağı üzerinde herhangi bir bilgisayara açmak için (örneğin ev ağında, şirket ağında veya Internet ağında) **Güvenilen, Standart ve Kamu**'yu seçin.
   - Portu standart ağ üzerinde herhangi bir bilgisayara açmak için (örneğin şirket ağında) **Standart (Güvenilen dahil)** seçeneğini belirleyin.
7. **Tamam**'ı tıklatın.

Mevcut sistem hizmeti portuna erişimi engelleme

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

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. **Sistem Hizmeti Portu Aç** altında, kapatmak istediğiniz sistem hizmeti portunun yanındaki onay kutusunun işaretini kaldırın.
5. **Tamam**'ı tıklatın.

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 tıklatın.
2. Internet ve Ağ Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
3. Güvenlik Duvarı bölmesinde **Sistem Hizmetleri**'ni tıklatın.
4. **Ekle**'yi tıklatın.
5. Sistem Hizmetleri bölmesinde, **Sistem Hizmeti Kuralı Ekle** altında şunları girin:
   - Sistem Hizmeti adı
   - Sistem Hizmeti kategorisi
   - Yerel TCP/IP portları
   - Yerel UDP portları
6. Aşağıdakilerden birini gerçekleştirin:
   - Portu güvenilen, standart veya kamu ağı üzerinde herhangi bir bilgisayara açmak için (örneğin ev ağında, şirket ağında veya Internet ağında) **Güvenilen, Standart ve Kamu**'yu seçin.
   - Portu standart ağ üzerinde herhangi bir bilgisayara açmak için (örneğin şirket ağında) **Standart (Güvenilen dahil)** seçeneğini belirleyin.
7. Bu portun etkinlik bilgilerini, Internet bağlantınızı paylaşan başka bir Windows ağ bilgisayarına göndermek isterseniz, **Bu portun ağ etkinliğini, Internet Bağlantısı Paylaşımı kullanan ağ bilgisayarlarına iletin** seçeneğini belirleyin.
8. İsterseniz, yeni yapılandırmaya açıklama ekleyebilirsiniz.
9. **Tamam**'ı tıklatın.

Not: Bilgisayarınızda web veya FTP sunucusu bağlantılarını kabul eden bir program 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, **Ağlar** listesine güvenilen bilgisayar bağlantısı da eklemeniz gerekebilir. Ayrıntılı bilgi için bkz. 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 hizmetinin yanındaki onay kutusunu tıklatın ve sonra **Düzenle**'yi tıklatın.
5. Sistem Hizmetleri bölmesinde, **Sistem Hizmeti Kuralı Ekle** altında şunları değiştirin:
   - Sistem hizmeti adı
   - Yerel TCP/IP portları
   - Yerel UDP portları
6. Aşağıdakilerden birini gerçekleştirin:
   - Portu güvenilen, standart veya kamu ağı üzerinde herhangi bir bilgisayara açmak için (örneğin ev ağında, şirket ağında veya Internet ağında) **Güvenilen, Standart ve Kamu**'yu seçin.
   - Portu standart ağ üzerinde herhangi bir bilgisayara açmak için (örneğin şirket ağında) **Standart (Güvenilen dahil)** seçeneğini belirleyin.
7. Bu portun etkinlik bilgilerini, Internet bağlantınızı paylaşan başka bir Windows ağ bilgisayarına göndermek isterseniz, **Bu portun ağ etkinliğini, Internet Bağlantısı Paylaşımı kullanan ağ bilgisayarlarına iletin** seçeneğini belirleyin.
8. İsterseniz, değiştirilen yapılandırmaya açıklama ekleyebilirsiniz.
9. **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 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 **Kaldır**'ı tıklatın.
5. Onaylamak için açılan sorgu penceresinde **Evet**'i tıklatın.

BÖLÜM 21

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..... 100
İstatistiklerle Çalışma..... 102
Internet trafiğini izleme..... 102
Internet trafiğini izleme..... 105

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 bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
2. Güvenlik Duvarı bölmesinde **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 bölmesinde, olayın tarihi ve açıklaması görüntülenir. Bu bölme, Internet erişimi açıkça engellenmiş olan programların etkinliğini görüntüler.

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

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 bölmesinde **Raporlar ve Günlükler**'i tıklatın.
2. **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklatın.
3. **Internet ve Ağ**'ı tıklatın ve sonra **Giden Olaylar**'ı tıklatın.

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 bölmesinde **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.

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 bölmesinde **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 bölmesinde **HackerWatch**'u tıklatın.
3. **En Son Port Etkinliği** altında en son olay portlarını görüntüleyin.

Internet trafiğini izleme

Firewall, Internet 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 bölmesinde **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 bölmesinde **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 bölmesinde **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 bölmesinde **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 bölmesinde, bir kaynak IP adresi seçin ve ardından **Bu IP'yi izle** seçeneğini tıklatın.
5. Görsel İzleyici bölmesinde, 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 bölmesinde **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 bölmesinde, bir kaynak IP adresi seçin ve sonra **Bu IP'yi izle** seçeneğini tıklatın.
4. Görsel İzleyici bölmesinde, 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 bölmesinde **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 izle** seçeneğini 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, ağ bağlantılarının büyük bir bölümünü kullanan programları ve bu programların eriştikleri IP adreslerini görüntüler.

Trafik Analizi bölmesinde, 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 bölmesi, 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, ağ bağlantılarının büyük bir bölümünü kullanan programları ve bu programların eriştikleri IP adreslerini görüntüler.

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

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

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 tıklatın.
2. Araçlar bölmesinde **Trafik Monitörü**'nü tıklatın.
3. **Trafik Monitörü** altında **Trafik Kullanımı**'nı tıklatın.

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

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 tıklatın.
2. Araçlar bölmesinde **Trafik Monitörü**'nü tıklatın.
3. **Trafik Monitörü** altında **Etkin Programlar**'ı tıklatın.
4. Aşağıdaki bilgileri görüntüleyebilirsiniz:
   - Program Etkinliği grafiği: Etkinlik grafiğini görüntüleyeceğiniz programı seçin.
   - Dinleme bağlantısı: Program adı altında bir Dinleme öğesi 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 tıklatın.

BÖLÜM 22

Internet güvenliği hakkında bilgi alma

Firewall, size programlar ve genel Internet etkinliği 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..... 110

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 tıklatın.
2. Araçlar bölmesinde **HackerWatch**'u tıklatın.
3. **HackerWatch Kaynakları** altında **Dersi Görüntüle**'yi tıklatın.

BÖLÜM 23

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 parçalanan dosya ve klasörleri daha sonra hızla çağrılabilecek 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 112
Bilgisayarınızı temizleme..... 113
Bilgisayarınızı birleştirme..... 117
Görev zamanlama..... 119

QuickClean özellikleri

Dosya Temizleyici	Çeşitli temizleyiciler kullanarak gereksiz dosyaları güvenli ve etkili bir biçimde silin. Bu dosyaları sildiğinizde, bilgisayarınızın sabit diskinde alan kazanır ve performansını geliştirirsiniz.

BÖLÜM 24

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 geçmişi 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.

Ad	İşlev
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 kaydolan veya siteyi ziyaret eden kullanıcıları tanımlamak için kullanılır; ancak bunlar, korsanlar için bilgi kaynağı da olabilir.
Tarayıcı Geçmişi Temizleyicisi	Web tarayıcısı geçmişinizi siler.
Outlook Express ve Outlook E-posta Temizleyicisi (gönderilmiş ve silinmiş öğeler)	Outlook® ve Outlook Express'ten gönderilmiş ve silinmiş e-postaları 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.

Bu bölümde

Bilgisayarınızı temizleme..... 115

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 bölmesinde, **Ortak Görevler** altında, **Bilgisayar Bakımı**'nı 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 işlemini onaylamak için **İleri**'yi tıklatın.
6. Aşağıdakilerden birini gerçekleştirin:
   - Varsayılan **Hayır, dosyalarımı standart Windows silme işlemini 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 öğe 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.

BÖLÜM 25

Bilgisayarınızı birleştirme

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

Bilgisayarınızı birleştirme

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

1. McAfee SecurityCenter bölmesinde, **Ortak Görevler** altında, **Bilgisayar Bakımı**'nı tıklatın.
2. **Disk Birleştirici** altında **Analiz**'i tıklatın.
3. Ekran yönergelerini izleyin.

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

BÖLÜM 26

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**'nı 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 işlemini 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 işlemini 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**'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.

4 **Sil**'i ve sonra silme işlemini 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**'nı 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 işlemini onaylamak için **Evet**'i tıklatın.

5 **Son**'u tıklatın.

BÖLÜM 27

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. Parçalanan 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 124
Dosyaları, klasörleri ve diskleri parçalama 124

Shredder özellikleri

Dosya ve klasörleri kalıcı olarak silme

Bilgisayarınızın sabit diskindeki öğeleri, ilişkili bilgilerin kurtarılamayacağı şekilde kaldırın. 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 bölmesinde, **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.
   - **Gözat**'ı tıklatın, parçalamak istediğiniz dosyaya gidip seçin ve sonra **Aç**'ı tıklatın.

6 **İleri**'yi tıklatın.

7 **Başlat**'ı 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 bölmesinde, **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.

BÖLÜM 28

McAfee Network Manager

Network Manager, ev ağınızı oluşturan bilgisayarların ve diğer aygıtların grafiksel görünümünü sunar. Network Manager'ı kullanarak, ağınızda yönetilen tüm bilgisayarların koruma durumunu uzaktan yönetebilir ve bu bilgisayarlarla ilgili raporlanan güvenlik açıklarını uzaktan düzeltebilirsiniz. McAfee Total Protection yüklediyseniz, Network Manager ağınızda bağlanmaya çalışan Saldırganları (tanımadığınız veya güvenmediğiniz bilgisayarlar veya aygıtlar) da izleyebilir.

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 algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Network Manager özellikleri 128
Network Manager simgeleri hakkında bilgi 129
Yönetilen bir ağ kurma 131
Ağı uzaktan yönetme 137
Ağlarınızı izleme 143

Network Manager özellikleri

Grafiksel ağ haritası

Ev ağınızı oluşturan bilgisayarların ve aygıtların koruma durumuna ilişkin grafiksel görünümü görüntüleyin. 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 aygıtla ilgili ayrıntıları da görüntüleyebilirsiniz.

Uzaktan yönetme

Ev ağınızı oluşturan bilgisayarların koruma durumunu yönetin. Yönetilen ağa katılması için bir bilgisayarı davet edebilir, yönetilen bilgisayarın koruma durumunu izleyebilir ve ağdaki uzak bir bilgisayarın bilinen güvenlik açıklarını düzeltebilirsiniz.

Ağ izleme

Kullanılıyorsa, Ağ Yöneticisi'nin ağlarınızı izlemesine ve Arkadaşlar veya Saldırganlar bağlandığında size bildirmesine izin verin. Ağ izleme, yalnızca McAfee Total Protection satın aldıysanız kullanılabilir.

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
	Internet'in bağlı olduğunu gösterir
	Internet bağlantısının kesildiğini gösterir

BÖLÜM 29

Yönetilen bir ağ kurma

Yönetilen bir ağ kurmak için ağa güvenin (henüz güvenmediyseniz) ve ağa üyeler (bilgisayarlar) ekleyin. Bir bilgisayarın uzaktan yönetilebilmesi veya ağdaki diğer bilgisayarları uzaktan yönetme izni alabilmesi için ağın güvenilen bir üyesi olması gerekir. 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 öğeyle ilgili ayrıntıları görüntüleyebilirsiniz.

Bu bölümde

Ağ haritasıyla çalışma 132
Yönetilen ağa katılma 133

Ağ haritasıyla çalışma

Ağa bilgisayar bağladığınızda, Network Manager yönetilen veya yönetilmeyen herhangi bir üye olup olmadığını, yönlendirici özniteliklerini 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 ağa bağlanan ilk bilgisayarın 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 öğelerini gösterebilir veya gizleyebilirsiniz. Ayrıca, ağ haritasında gösterilen herhangi bir öğeyle ilgili ayrıntıları da görüntüleyebilirsiniz.

Ağ haritasına erişme

Ağ haritası, ev ağınızı oluşturan bilgisayarları ve aygıtları grafiksel olarak gösterir.

- Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.

Not: Ağa henüz güvenmediyseniz (McAfee Personal Firewall kullanarak), ağ haritasına ilk eriştiğinizde sizden bunu yapmanız istenir.

Ağ haritasını yenileme

Ağ haritasını istediğiniz zaman, örneğin yönetilen ağa başka bir bilgisayar katıldıktan sonra yenileyebilirsiniz.

1. Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.
2. **Şunu yapmak istiyorum** altında **Ağ haritasını yenile**'yi tıklatın.

Not: **Ağ haritasını yenile** bağlantısı, yalnızca ağ haritasında hiç seçili öğe yoksa kullanılabilir. Bir öğenin seçimini kaldırmak için seçili öğeyi tıklatın veya ağ haritası üzerinde beyaz bir alanı tıklatın.

Ağın adını değiştirme

Varsayılan olarak, ağ adı SecurityCenter yüklü olan ve ağa bağlanan ilk bilgisayarın adını içerir. Farklı bir ad kullanmayı tercih ederseniz bunu değiştirebilirsiniz.

1. Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.
2. **Şunu yapmak istiyorum** altında **Ağın adını değiştir**'i tıklatın.
3. **Ağ Adı** kutusuna ağın adını yazın.
4. **Tamam**'ı tıklatın.

Not: **Ağın adını değiştir** bağlantısı, yalnızca ağ haritasında hiç seçili öğe yoksa kullanılabilir. Bir öğenin seçimini kaldırmak için seçili öğeyi tıklatın veya ağ haritası üzerinde beyaz bir alanı tıklatın.

Ağ haritasında öğeyi gösterme veya gizleme

Varsayılan olarak, ev ağınızdaki tüm bilgisayarlar ve aygıtlar 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 tıklatın ve ardından bunu yapın...
Ağ haritasında bir öğeyi gizlemek	Ağ haritasında bir öğeyi tıklatın ve ardından **Şunu yapmak istiyorum** bölümünde **Bu öğeyi gizle**'yi tıklatın. Onay iletişim kutusunda **Evet**'i tıklatın.
Ağ haritasında öğeleri göstermek	**Şunu yapmak istiyorum** bölümünde **Gizli öğeleri göster**'i tıklatın.

Öğenin ayrıntılarını görüntüleme

Ağ haritasında seçerek, ağınızdaki herhangi bir öğeyle ilgili ayrıntılı bilgi görüntüleyebilirsiniz. Bu bilgiler öğe adını, koruma durumunu ve öğeyi yönetmek için gerekli diğer bilgileri içerir.

1. Ağ haritasında öğenin simgesini tıklatın.
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 edebilir veya reddedebilirsiniz. Ayrıca ağ üzerindeki diğer bilgisayarların bu bilgisayarın güvenlik ayarlarını yönetmesini isteyip istemediğinizi belirleyebilirsiniz.

1. Yönetilen Ağ iletişim kutusunda, **Bu ağdaki her bilgisayarın güvenlik ayarlarını yönetmesine 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 görüntülemezse, 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 yönet**'i 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**'ı 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 görüntülemezse, yönetilen ağ üzerinde bir güvenlik ihlali olmuştur. Bilgisayarın ağa katılmasına izin verirseniz 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.

BÖLÜM 30

Ağı uzaktan yönetme

Yönetilen ağınızı kurduktan sonra, ağınızı oluşturan bilgisayarları ve aygıtları uzaktan yönetebilirsiniz. Bilgisayarların ve aygıtların durumunu ve izin düzeylerini yönetebilir; güvenlik açıklarının çoğunu uzaktan düzeltebilirsiniz.

Bu bölümde

Durum ve izinleri yönetme..... 138
Güvenlik açıklarını düzeltme 140

Durum ve izinleri yönetme

Yönetilen bir ağın yönetilen ve yönetilmeyen üyeleri vardır. Yönetilen üyeler, McAfee koruma durumlarının ağdaki diğer bilgisayarlar tarafından yönetilmesine izin verirler; yönetilmeyen üyeler buna izin vermezler. Yönetilmeyen üyeler, genellikle başka ağ özelliklerine erişmek (örneğin, dosya göndermek veya yazıcıları paylaşmak) isteyen konuk bilgisayarlardır. Yönetilmeyen bir bilgisayar, herhangi bir zamanda ağ üzerinde yönetici izinlerine sahip başka bir yönetilen bilgisayar tarafından yönetilen üye olmak üzere davet edilebilir. Benzer şekilde, yönetici izinlerine sahip yönetilen bir bilgisayar, başka bir yönetilen bilgisayarı herhangi bir zamanda yönetilmeyen bilgisayar yapabilir.

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 istediğiniz zaman 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 yönetme

Bir bilgisayarın koruma durumu ağ üzerinde yönetilmiyorsa (bilgisayar ağın üyesi değilse veya ağın yönetilmeyen bir üyesiyse), onu yönetmek için istekte bulunabilirsiniz.

1. Ağ haritasında yönetilmeyen bilgisayarın simgesini tıklatın.
2. **Şunu yapmak istiyorum** altında **Bu bilgisayarı yönet**'i tıklatın.

Bir bilgisayarın koruma durumunu yönetmeyi durdurma

Ağınızda yönetilen bir bilgisayarın koruma durumunu yönetmeyi durdurabilirsiniz; ancak bu durumda bilgisayar yönetilmeyen üye olur ve koruma durumunu uzaktan yönetemezsiniz.

1. Ağ haritasında yönetilen bilgisayarın simgesini tıklatın.
2. **Şunu yapmak istiyorum** altında **Bu bilgisayarı yönetmeyi 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 yönetebilen 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 yönetip yönetmeyeceklerini belirlemek için onay kutusunu seçin veya işaretini kaldırın.
4. **Tamam**'ı tıklatın.

Bir aygıtı yönetme

Ağ haritasından 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 McAfee 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 yönetebilir ve raporlanan güvenlik açıklarını uzaktan düzeltebilir. Örneğin, yönetilen bir bilgisayarın McAfee koruma durumu VirusScan'in devre dışı olduğunu gösteriyorsa, yönetici izinlerine sahip başka bir yönetilen bilgisayar VirusScan'i 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 öğenin simgesini tıklatın.
2. **Ayrıntılar** bölümünde, öğenin 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 sürümlerinden birini kullanmıyorsa, bunların koruma durumu uzaktan yönetilemez. Bu bilgisayarları uzaktan yönetmek istiyorsanız, her bilgisayara tek tek SecurityCenter'ın en son sürümlerinden birini yüklemeniz gerekir.

1. Uzaktan yönetmek istediğiniz bilgisayarda bu yönergeleri uyguladığınızdan emin olun.
2. McAfee oturum açma bilgilerinizi hazır bulundurun: Bu, McAfee yazılımı ilk etkinleştirilirken kullanılan e-posta adresi ve paroladır.
3. Tarayıcıda, McAfee Web sitesine gidin, oturum açın ve **Hesabım**'ı tıklatın.
4. Yüklemek istediğiniz ürünü bulun, **Yükle** düğmesini tıklatın ve sonra ekran yönergelerini uygulayın.

İpucu: Ayrıca ağ haritasını açıp **Şunu yapmak istiyorum** altında **PC'lerimi koru**'yu tıklatarak uzak bilgisayarlara McAfee güvenlik yazılımını nasıl yükleyeceğinizi öğrenebilirsiniz.

BÖLÜM 31

Ağlarınızı izleme

McAfee Total Protection yüklediyseniz, Network Manager da ağlarınızda saldırganları izler. Bilinmeyen bir bilgisayar veya aygıt ağınıza her bağlandığında bu size bildirilir; böylece bu bilgisayarın veya aygıtın Arkadaş mı yoksa Saldırgan mı olduğuna karar verebilirsiniz. Arkadaş tanıdığınız ve güvendiğiniz bir bilgisayar veya aygıt, Saldırgan ise tanımadığınız veya güvenmediğiniz bir bilgisayar veya aygıttır. Bir bilgisayarı veya aygıtı Arkadaş olarak işaretlerseniz, bu Arkadaş ağa her bağlandığında size bildirilmesini isteyip istemediğinize karar verebilirsiniz. Bir bilgisayarı veya aygıtı Saldırgan olarak işaretlerseniz, ağınıza her bağlandığında bunu size otomatik olarak bildiririz.

Bu Total Protection sürümünü yükledikten veya bu sürüme yükseltme yaptıktan sonra ağa ilk bağlandığınızda, her bilgisayarı veya aygıtı Arkadaş olarak otomatik işaretleriz ve ileride ağa bağlandıkları zaman bunu size bildirmeyiz. Üç gün sonra, bilinmeyen her bilgisayarı veya aygıtı size bildirmeye başlarız; böylece bunları kendiniz işaretleyebilirsiniz.

Not: Ağ izleme, Network Manager'ın yalnızca McAfee Total Protection ile kullanılabilen bir özelliğidir. Total Protection hakkında daha fazla bilgi için Web sitemizi ziyaret edin.

Bu bölümde

Ağları izlemeyi durdurma 143
Ağ izleme bildirimlerini yeniden etkinleştirme 144
Saldırgan olarak işaretleme 144
Arkadaş olarak işaretleme 145
Yeni Arkadaşlar algılamayı durdurma 145

Ağları izlemeyi durdurma

Ağ izlemeyi devre dışı bırakırsanız, ev ağınıza veya bağlandığınız başka herhangi bir ağa saldırganların bağlandığını artık size bildiremeyiz.

1. Internet ve Ağ Yapılandırma bölmesini açın.

   Nasıl?

   1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
   2. SecurityCenter Giriş bölmesinde **Internet ve Ağ**'ı tıklatın.
   3. Internet ve Ağ bilgi bölümünde **Yapılandır**'ı tıklatın.
2. **Ağ izleme** altında **Kapalı**'yı tıklatın.

Ağ izleme bildirimlerini yeniden etkinleştirme

Ağ izleme bildirimlerini devre dışı bırakabilirsiniz, ancak bunu önermiyoruz. Bunu yaparsanız, ağınıza bağlanan bilinmeyen bilgisayarları veya Saldırganları artık size bildiremeyebiliriz. Bu bildirimleri yanlışlıkla devre dışı bırakırsanız (örneğin bir uyarıda **Bu uyarıyı bir daha gösterme** onay kutusunu seçerseniz), bunları istediğiniz zaman yeniden etkinleştirebilirsiniz.

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 SecurityCenter Yapılandırma bölmesinde **Bilgi Uyarıları**'nı tıklatın.

3 Bilgi Uyarıları bölmesinde şu onay kutularının işaretlenmediğinden emin olun:

- **Yeni bilgisayarlar veya aygıtlar ağa bağlanınca uyarı gösterme**
- **Saldırganlar ağa bağlanınca uyarı gösterme**
- **Genellikle bana bildirilmesini istediğim Arkadaşlar için uyarı gösterme**
- **Bilinmeyen bilgisayarlar veya aygıtlar algılanınca bana anımsatma**
- **McAfee yeni Arkadaşlar algılamayı bitirdiğinde bana haber verme**

4 **Tamam**'ı tıklatın.

Saldırgan olarak işaretleme

Ağınızda bir bilgisayarı veya aygıtı, onu tanımıyorsanız ve güvenmiyorsanız Saldırgan olarak işaretleyin. Ağınıza her bağlandığında bunu size otomatik olarak bildiririz.

1 Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.

2 Ağ haritasında bir öğeyi tıklatın.

3 **Şunu yapmak istiyorum** altında **Arkadaş veya Saldırgan Olarak İşaretle**'yi tıklatın.

4 İletişim kutusunda **Saldırgan**'ı tıklatın.

Arkadaş olarak işaretleme

Ağınızda bir bilgisayarı veya aygıtı, yalnızca onu tanıyorsanız ve güveniyorsanız Arkadaş olarak işaretleyin. Bir bilgisayarı veya aygıtı Arkadaş olarak işaretlediğinizde, ağa her bağlandığında size bildirilmesini isteyip istemediğinize de karar verebilirsiniz.

1. Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.
2. Ağ haritasında bir öğeyi tıklatın.
3. **Şunu yapmak istiyorum** altında **Arkadaş veya Saldırgan Olarak İşaretle**'yi tıklatın.
4. İletişim kutusunda **Arkadaş**'ı tıklatın.
5. Bu Arkadaş ağa her bağlandığında size bildirilmesi için **Bu bilgisayar veya aygıt ağa bağlandığında bana bildir** onay kutusunu seçin.

Yeni Arkadaşlar algılamayı durdurma

Bu Total Protection sürümünü yükleyip ağa ilk kez bağlandıktan üç gün sonra, hakkında bildirim almak istemediğiniz her bilgisayarı veya aygıtı Arkadaş olarak otomatik işaretleriz. Bu üç gün içinde otomatik işaretlemeyi istediğiniz zaman durdurabilirsiniz, ancak sonra yeniden başlatamazsınız.

1. Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.
2. **Şunu yapmak istiyorum** altında **Yeni Arkadaşlar algılamayı durdur**'u tıklatın.

BÖLÜM 32

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 148
EasyNetwork'ü ayarlama 149
Dosyaları paylaşma ve gönderme 153
Yazıcıları paylaşma 159

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.

BÖLÜM 33

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 verirseniz, bunu istediğiniz zaman yapabilirsiniz.

Bu bölümde

EasyNetwork'ü açma 149
Yönetilen bir ağa katılma 150
Yönetilen ağı terk etme 152

EasyNetwork'ü açma

EasyNetwork'ü Windows Başlat menüsünden veya masaüstü simgesini tıklatarak açabilirsiniz.

- **Başlat** menüsünde **Programlar**'a gelin, **McAfee**'ye gelin ve ardından **McAfee EasyNetwork**'ü tıklatın.

İpucu: EasyNetwork'ü masaüstünüzdeki McAfee EasyNetwork simgesini çift tıklatarak da 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 görüntülemezse, 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 tıklatın.
4. Bilgisayarın, güvenlik onayı iletişim kutusunda gösterilen oyun kartlarını görüntülediğini doğrulayın ve sonra **Erişim İzni Ver**'i tıklatın.

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 verirseniz bilgisayarınız risk altına girebilir; bu nedenle, güvenlik onayı iletişim kutusunda **Erişimi Reddet**'i tıklatın.

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.
2. Yapılandır iletişim kutusunda, **Ağ Adı** kutusuna ağın adını yazın.
3. **Tamam**'ı tıklatın.

Yönetilen ağı terk etme

Yönetilen bir ağa katıldıktan sonra ağın üyesi olmak istemediğinize karar verirseniz, ağı terk edebilirsiniz. Yönetilen ağı terk ettikten sonra, her zaman yeniden katılabilirsiniz; ancak size yeniden izin verilmesi gerekir. Ağa katılma hakkında ayrıntılı bilgi için bkz. Yönetilen bir ağa katılma (sayfa 150).

Yönetilen ağı terk etme

Daha önceden katılmış olduğunuz yönetilen ağı terk edebilirsiniz.

1. Bilgisayarınızın ağ ile bağlantısını kesin.
2. EasyNetwork'te **Araçlar** menüsünde **Ağı Terket**'i tıklatın.
3. Ağı Terket iletişim kutusunda, terk etmek istediğiniz ağın adını seçin.
4. **Ağı Terket**'i tıklatın.

BÖLÜM 34

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 154
Dosyaları diğer bilgisayarlara gönderme 156

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. İstediğiniz 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 tıklatırsanız 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 ağınızdaki 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 155) tıklatın.
3. **Dosya veya Yol Adı** listesine, dosya adının veya yolun bir bölümünü ya da tamamını yazın.
4. **Tür** listesinde uygun dosya türünü (sayfa 155) 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 sonek 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 157).

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 tıklatır, dosyaları seçer ve sonra **Gönder**'i tıklatırsanız 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 iletisi görüntülenir. EasyNetwork'ü açıp dosyaya erişmek için bu bildirim iletisini 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 tıklatırsanız da başka bir bilgisayardan dosya alabilirsiniz. Klasöre kabul et iletişim 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.

BÖLÜM 35

Yazıcıları paylaşma

Yönetilen bir ağa katıldığınızda, EasyNetwork bilgisayarınıza bağlı yerel yazıcıları paylaştırır 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 paylaştırır. Ayrıca, istediğiniz zaman yazıcı paylaşımını durdurabilirsiniz.

Bu bölümde

Paylaşılan yazıcılarla çalışma 160

Paylaşılan yazıcılarla çalışma

EasyNetwork, ağdaki bilgisayarlar tarafından paylaşılan yazıcıları algılar. EasyNetwork bilgisayarınıza bağlı olmayan bir uzak yazıcı algılarsa, 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 ağ üzerinde veri iletmek için standartlar grubu. 802.11 genellikle Wi-Fi olarak bilinir.

802.11a

5 GHz 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 bir standart. 802.1x genellikle 802.11 kablosuz ağ ile kullanılır. Ayrıca bkz. kimlik doğrulama (sayfa 166).

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 ekranınızda diğer pencerelerin üzerinde beliren küçük pencereler. Açılan pencereler, reklamlar görüntülemek üzere web tarayıcılarında sıklıkla kullanılır.

ağ

Mantıksal bir birim olarak bir araya getirilen IP tabanlı sistemler (yönlendiriciler, anahtarlar, sunucular ve güvenlik duvarları) grubu. Örneğin, “Finans Ağı” finans departmanına hizmet veren tüm sunucuları, yönlendiricileri ve sistemleri içerebilir. Ayrıca bkz. ev ağı (sayfa 164).

ağ haritası

Ev ağınızı oluşturan bilgisayarların ve bileşenlerin grafiksel anlatımı.

ağ sürücüsü

Çok sayıda kullanıcı tarafından paylaşılan ağ üzerinde bir sunucuya bağlı disk veya teyp sürücü. Ağ sürücüleri bazen “uzak sürücüler” olarak adlandırılır.

akıllı sürücü

Bkz. USB sürücüsü (sayfa 172).

anahtar

İki aygıt tarafından aralarındaki iletişimin kimliğini doğrulamak için kullanılan harfler ve sayılar dizisi. Her iki aygıtın da anahtarı olmalıdır. Ayrıca bkz. WEP (sayfa 172), WPA (sayfa 173), WPA2 (sayfa 173), WPA2-PSK (sayfa 173), WPA-PSK (sayfa 173).

arabellek taşması

Şüpheli programlar veya işlemler, arabelleğe (geçici depolama alanı) saklayabileceğinden daha fazla veri depolamaya çalıştığında işletim sisteminde veya uygulamada ortaya çıkan durum. Arabellek taşması, belleği bozar veya komşu arabelleklerdeki verilerin üzerine yazar.

arşivleme

CD, DVD, USB sürücüsü, harici sabit disk veya ağ sürücüsü üzerinde önemli dosyaların yerel kopyasını oluşturmak. Karşılaştırın: yedekleme (sayfa 173).

B

bant genişliği

Belirli bir süre içinde iletilebilen veri miktarı.

beyaz liste

Güvenli olduğu düşünülen web sitelerinin veya e-posta adreslerinin listesi. Beyaz listedeki web siteleri, kullanıcılar tarafından erişim izni verilen sitelerdir. Beyaz listedeki e-posta adresleri, gönderdikleri iletileri almak istediğiniz güvenilen kaynakların adresleridir. Karşılaştırın: kara liste (sayfa 166).

D

DAT

Virüsler, Truva atları, casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programları (PUP) saptayan, algılayan ve onaran tanımlar içeren, aynı zamanda imza dosyaları olarak da bilinen algılama tanım dosyaları.

DNS

Etki Alanı Sistemi. 11.2.3.44 gibi bir IP adresini www.mcafee.com gibi bir etki alanı adına dönüştüren veritabanı sistemi.

dolaşım

Hizmette kesinti veya bağlantı kaybı olmaksızın, bir erişim noktası (AP) kapsama alanından diğerine hareket etme.

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 (sayfa 170).

E

e-posta

Elektronik posta. Bilgisayar ağında elektronik olarak gönderilen ve alınan iletiler. Ayrıca bkz. web postası (sayfa 172).

e-posta istemcisi

Bilgisayarınızda e-posta gönderip almak için çalıştırdığınız program (örneğin Microsoft Outlook).

eklenti

Büyük bir yazılıma özellikler ekleyen veya bunu geliştiren küçük bir 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 (AP)

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.

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 ağdır. Internet üzerinde etki alanı, her web adresinin bir parçasını oluşturur. Örneğin www.mcafee.com adresinde mcafee 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 (sayfa 167).

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 tarama işlemi.

Geri Dönüşüm Kutusu

Windows'ta silinen dosyalar ve klasörler için sanal bir çöp kutusu.

güvenilenler listesi

Güvendiğiniz ve algılanmayan öğelerin listesi. Bir öğeye (örneğin olası istenmeyen programa veya kayıt defteri değişikliğine) yanlışlıkla güvenirseniz 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. İntranete 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.

hizmet reddi (DOS) saldırısı

Bilgisayara, sunucuya veya ağa karşı düzenlenen ve ağ üzerinde trafiği yavaşlatan veya durduran bir saldırı türü. Ağ düzenli trafiği yavaşlatacak veya tamamen kesecek kadar çok istekle dolduğunda gerçekleşir. Hizmet reddi saldırısı, hedefini sahte bağlantı isteklerine boğar ve böylece hedef yasal istekleri yok sayar.

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.

intranet

Genellikle bir kuruluşun içinde bulunan ve yalnızca yetkili kullanıcılar tarafından erişilebilen özel bilgisayar ağı.

IP adresi

Internet Protokolü adresi. TCP/IP ağı üzerinde bir bilgisayarı veya aygıtı tanımlamak için kullanılan adres. 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

Tehdit, açık veya başka olası istenmeyen kod bulmak için seçili dosyalara, uygulamalara veya ağ aygıtlarına uygulanan zamanlanmış inceleme. Anında, daha sonra zamanlanan bir saatte veya zamanlanmış düzenli aralıklarla gerçekleşebilir. Erişim üzerine tarama ile karşılaştırın. Ayrıca bkz. açık.

istemci

Bilgisayar veya iş istasyonu üzerinde çalışan ve bazı işlemleri gerçekleştirmek için sunucuya gerek duyan bir program. Örneğin e-posta istemcisi, e-posta gönderip almanıza olanak veren bir uygulamadır.

izleme konumları

Backup and Restore'un bilgisayarınızda izlediği klasörler.

izlenen dosya türleri

Backup and Restore'un izleme konumlarında arşivlediği veya yedeklediği dosya türleri (örn., .doc, .xls).

K

kaba kuvvet saldırısı

Şifreyi kırana kadar olası tüm karakter birleşimlerini deneyerek parolaları veya şifre anahtarlarını bulmak için kullanılan bir korsanlık yöntemi.

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

Anti-Spam'de, iletilerin spam olduğunu düşündüğünüz için gönderdiği iletileri almak istemediğiniz e-posta adreslerinin listesi. Phishing korumasında, hileli oldukları düşünülen web sitelerinin listesi. Karşılaştırın: beyaz liste (sayfa 163).

karantina

Virüs, spam, şüpheli içerik veya olası istenmeyen programlar (PUP) içerdiğinden şüphelenilen bir dosyaya veya klasöre, dosyanın veya klasörün açılmasını veya yürütülmesini engelleyecek şekilde uygulanan yalıtım.

kayıt defteri

Windows tarafından her bilgisayar kullanıcısı, sistem donanımı, yüklenen programlar ve özellik ayarları hakkında yapılandırma bilgilerini depolamak için kullanılan veritabanı. Bu veritabanı anahtarlara ayrılır ve bunlar için değerler ayarlanır. İstenmeyen programlar, zararlı kodu yürütmek için kayıt defteri anahtarlarının değerini değiştirebilir veya yenilerini oluşturabilir.

kimlik doğrulama

Bir elektronik belgeyi gönderen kişinin dijital kimliğini doğrulama işlemi.

kısayol

Bilgisayarınızda başka bir dosyanın yalnızca konumunu içeren bir dosya.

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 aygıta (NIC, ağ arabirim kartı) atanan benzersiz bir seri numarası.

MAPI

İleti Uygulaması Programlama Arabirimi. Farklı ileti ve çalışma grubu programlarının (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 aygıta takılan ve aygıtı yerel ağa bağlayan kart.

numara çeviriciler

Bir içerik sağlayıcı, satıcı veya başka herhangi bir üçüncü tarafın ek bağlantı ücretleri alması için Internet bağlantılarını kullanıcının varsayılan ISS'sinden (Internet servis sağlayıcısı) başka bir tarafa yönlendiren yazılım.

O

olası istenmeyen program (PUP)

Kullanıcılar karşıdan yüklenmesine izin vermiş olsalar bile, istenmeyebilecek bir yazılım programı. Yüklendiği bilgisayarda güvenlik veya gizlilik ayarlarını değiştirebilir. PUP'ler, her zaman olmasa da casus yazılımlar, reklam yazılımlar ve numara çeviriciler içerebilir ve kullanıcının istediği bir programla birlikte karşıdan yüklenebilir.

olay

Bilgisayar sisteminde veya programında, önceden tanımlı ölçütlere göre güvenlik yazılımı tarafından algılanabilen durum. Olay, genellikle bildirim göndermek veya olay günlüğüne giriş eklemek gibi bir eylemi tetikler.

ortadaki adam saldırısı

İletişim bağlantısının ihlal edildiğini bilmeyen iki taraf arasındaki iletileri ele geçirmek ve büyük olasılıkla değiştirmek için bir yöntem.

Ö

önbellek

Bilgisayarınızda sık sık veya yakın zamanda erişilen veriler için geçici bir depolama alanı. Örneğin, web'de gezinme hızını ve etkinliğini artırmak için tarayıcınız, daha önce görüntülediğiniz bir web sayfasını uzak sunucu yerine önbellekten çağırabilir.

P

parola

Bilgisayarınıza, bir programa veya web sitesine erişim sağlamak için kullandığınız kod (genellikle harfler ve sayılardan oluşur).

parola kasası

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). RADIUS iletilerinin hassas bölümlerini korumak için kullanılır. Ayrıca bkz. RADIUS (sayfa 169).

paylaştırma

E-posta alıcılarının sınırlı bir süre için seçili yedeklenen dosyalara erişmelerine izin verme. Bir dosyayı paylaştırdığınızda, dosyanın yedeklenen kopyasını belirlediğiniz e-posta alıcılarına gönderirsiniz. Alıcılar Backup and Restore'dan dosyaların kendileriyle paylaşıldığını gösteren bir e-posta iletisi alırlar. E-posta, paylaşılan dosyalara bağlantı da içerir.

PCI kablosuz bağdaştırıcı kartı

Çevre Birim Bileşeni Bağlantısı. Bilgisayarın içindeki PCI genişletme yuvasına takılan kablosuz bağdaştırıcı kartı.

phishing

Bankalar veya yasal şirketler gibi güvenilir kaynaklardan geliyormuş gibi görünen hileli e-postalar göndererek, hileli yollardan parolalar, sosyal sigorta numaraları, kredi kartı bilgileri vb. kişisel bilgileri elde etme yöntemi. Phishing e-postalarda, genellikle alıcılardan iletişim bilgilerini veya kredi kartı bilgilerini doğrulamak veya günceleştirmek için e-postanın içindeki bağlantıyı tıklatmaları istenir.

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

Bilgisayara veri gönderip almak için kullanılan bir donanım konumu. Kişisel bilgisayarlarda; disk sürücülerini, monitörleri ve tüm klavyeleri bağlamak için dahili portların yanı sıra modemler, yazıcılar, fareler ve diğer çevre birimleri bağlamak için harici portları da içeren çok çeşitli port türleri vardır.

PPPoE

Ethernet Üzerinden Noktalar Arası Protokol. Aktarım olarak Ethernet'le Noktalar Arası Protokol (PPP) çevirmeli protokolünü kullanma yöntemi.

protokol

Bilgisayarlar veya aygıtlar arasında veri alışverişi sağlayan bir kurallar kümesi. Katmanlı ağ mimarisinde (Açık Sistemler Bağlantı modeli), her katmanın o düzeyde iletişimin nasıl gerçekleştiğini belirten kendi protokolleri vardır. Diğer bilgisayarlarla iletişim kurmak için bilgisayarınız veya aygıtınız doğru protokolü desteklemelidir. Ayrıca bkz. Açık Sistem Bağlantısı (OSI).

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 (sayfa 169).

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 bir protokol. İlk başlarda çevirmeli uzaktan erişim sunucularıyla kullanılmak üzere tanımlanan bu protokol, artık kablosuz yerel ağ kullanıcısının paylaşılan şifresinin 802.1x kimlik doğrulaması dahil, çok çeşitli kimlik doğrulama ortamlarında kullanılmaktadır. Ayrıca bkz. paylaşılan şifre.

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 çözme. Çevrimiçi yedekleme havuzundaki dosya sürümü diğer bilgisayarlardaki dosya sürümünden daha yeniyse dosyaları senkronize edersiniz.

sıkıştırma

Dosyaları, onları depolamak veya iletmek için gereken alanı en aza indirecek şekilde sıkıştıran bir işlem.

sistem geri yükleme noktası

Bilgisayar belleğinin veya bir veritabanının içeriklerinin anlık görüntüsü. Windows, düzenli olarak ve örneğin bir programın veya sürücünün yüklenmesi gibi önemli sistem olayları gerçekleştiğinde geri yükleme noktaları oluşturur. İstediğiniz 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 protokolüdür. Bu protokol, Internet üzerinde e-posta yönlendirmek için kullanılır.

solucan

Diğer sürücülerde, sistemlerde veya ağlarda kendi kopyalarını oluşturarak yayılan bir virüs. Toplu postayla gelen solucan, yayılmak için kullanıcının müdahalesine (örneğin bir eki açmak veya karşıdan yüklenen bir dosyayı yürütmek) gereksinim duyar. Bugün e-posta virüslerinin çoğu solucandır. Kendi kendine yayılan solucan, yayılmak için kullanıcının müdahalesine gereksinim duymaz. Blaster ve Sasser, kendi kendine yayılan solucanlara örnek olarak verilebilir.

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'te 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 (sayfa 169).

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

Yetkisiz kişilerin erişimini engellemek için bir bilgi kodlama yöntemi. Veriler kodlanınca, işlem bir "anahtar" ve matematik algoritmaları kullanır. Şifrelenen bilgilerin şifresi doğru anahtar olmadan çözülemez. Bazen virüsler algılanmamak için şifreleme kullanır.

şifreli metin

Şifrelenmiş metin. Şifreli metin, düz metne dönüştürülene (şifresi çözülene) kadar okunamaz. Ayrıca bkz. şifreleme (sayfa 170).

T

tanımlama bilgisi

Pek çok web sitesi tarafından ziyaret edilen sayfalarla ilgili bilgileri depolamak için kullanılan ve web'de gezinen kişinin bilgisayarında depolanan küçük bir metin dosyası. Oturum açma veya kayıt bilgilerini, alışveriş sepeti bilgilerini veya kullanıcı tercihlerini içerebilir. Tanımlama bilgileri, web siteleri tarafından genellikle web sitesine önceden kaydolan veya web sitesini ziyaret eden kullanıcıları tanımlamak için kullanılır; ancak bunlar, korsanlar için bilgi kaynağı da olabilir.

tarayıcı

Internet'te web sayfalarını görüntülemek için kullanılan program. Popüler web tarayıcıları arasında Microsoft Internet Explorer ve Mozilla Firefox sayılabilir.

TKIP

Geçici Anahtar Bütünlüğü Protokolü. Kablosuz yerel ağlar için 802.11i şifreleme standardının bir parçası. TKIP, 802.11 kablosuz yerel ağları korumak için kullanılan yeni nesil WEP'tir. TKIP, bir ileti bütünlüğü denetimi ve yeniden anahtarlama mekanizması olan pakette anahtar karıştırma özelliği sağlar ve böylece WEP kusurlarını giderir.

Truva, Truva atı

Çoğalmayan ancak bilgisayara zarar veren veya güvenliğini tehlikeye atan bir program. Genellikle birisi size Truva atı içeren e-posta gönderir; kendi kendisini e-posta ile göndermez. Truva atını, bir web sitesinden veya eşler arası ağ kurma programıyla da farkında olmadan karşıdan yükleyebilirsiniz.

tümleşik ağ geçidi

Erişim noktası (AP), yönlendirici ve güvenlik duvarı işlevlerini birleştiren bir aygıt. Bazı aygıtlar, güvenlik geliştirmeleri ve köprü kurma özellikleri de içerir.

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 yüklemeden veya depolamadan bir Windows bilgisayarda çalıştırmalarına olanak verir.

URL

Birörnek Kaynak Konumlayıcı. Internet adresleri için standart biçim.

USB

Evrensel Seri Veri Yolu. Modern bilgisayarlarda klavyeler ve farelerden web kameralarına, tarayıcılara ve yazıcılara kadar çok çeşitli aygıtları bağlayan sektör standardında bir bağdaştırıcı.

USB kablosuz bağdaştırıcı kartı

Bilgisayardaki USB portuna 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

Kendisini kopyalayabilen ve kullanıcının izni veya bilgisi olmadan bilgisayara bulaşabilen bir bilgisayar programı.

VPN

Sanal Özel Ağ. Internet gibi bir ana bilgisayar sunucusuyla yapılandırılan özel iletişim ağı. VPN bağlantısıyla gönderilip alınan veriler şifrelenir ve güçlü güvenlik özelliklerine sahiptir.

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

Web tabanlı posta. Genellikle Microsoft Outlook gibi bilgisayar tabanlı bir e-posta istemcisiyle web tarayıcısı üzerinden erişilen elektronik posta hizmeti. Ayrıca bkz. e-posta (sayfa 163).

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 laboratuarı ve takas odası görevi görür.

Wi-Fi Certified

Wi-Fi Alliance tarafından test edilmiş ve onaylanmış olmak. Wi-Fi onaylı ürünlerin, farklı üreticilere ait olsalar bile birbirleriyle çalışabilirliği onaylanmıştır. Wi-Fi onaylı 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 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, 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 erişmeleri 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 (sayfa 173), TKIP (sayfa 171).

WPA2

WPA güvenlik standardının 802.11i 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 açma işlemi. Yayımlanan dosyalara, Backup and Restore kitaplığında arama yaparak erişebilirsiniz.

yedekleme

Genellikle güvenli bir çevrimiçi sunucuda önemli dosyaların kopyasını oluşturmak. Karşılaştırın: arşivleme (sayfa 163).

yönlendirici

Bir ağdan diğerine veri paketleri ileten ağ aygıtı. Yönlendiriciler, gelen her paketi okur; kaynak ve hedef adreslere ve geçerli trafik koşullarına göre bunun nasıl iletileceğine karar verir. Yönlendirici bazen erişim noktası (AP) olarak da adlandırılır.

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.

Lisans

Telif Hakkı

BÖLÜM 36

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 dönüşür). 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 tıklatın. Virtual Technician Mozilla® Firefox ile çalışmaz.

Bu bölümde

McAfee Virtual Technician'ı kullanma 178

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.
2. Virtual Technician'ı yüklemek ve çalıştırmak için ekran yönergelerini izleyin.

Kullanıcı Kılavuzlarını içeren ülkenize veya bölgeniz özel McAfee Destek ve Yükleme siteleri için aşağıdaki tablolara başvurun.

Destek ve Yüklemeler

Ülke/Bölge	McAfee Destek	McAfee Yüklemeler
Almanya	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Avustralya	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Birleşik Devletler	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp
Brezilya	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Çek Cumhuriyeti	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Çin (Basitleştirilmiş Çince)	www.mcafeehelp.com	cn.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
İngiltere	www.mcafeehelp.com	uk.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
İtalya	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japonya	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Kanada (Fransızca)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48
Kanada (İngilizce)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kore	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Macaristan	www.mcafeehelp.com	hu.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
Rusya	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Slovakya	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
Tayvan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Türkiye	www.mcafeehelpturkey.com	tr.mcafee.com/root/downloads.asp
Yunanistan	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp

McAfee Total Protection Kullanıcı Kılavuzları

Ülke/Bölge	McAfee Kullanıcı Kılavuzları
Almanya	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Avustralya	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Çin (Basitleştirilmiş Çince)	download.mcafee.com/products/manuals/zh-cn/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
Hollanda	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
İngiltere	download.mcafee.com/products/manuals/en-uk/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
İtalya	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Macaristan	http://download.mcafee.com/products/manuals/hu/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
Rusya	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Slovakya	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Tayvan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Yunanistan	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf

McAfee Internet Security Kullanıcı Kılavuzları

Ülke/Bölge	McAfee Kullanıcı Kılavuzları
Almanya	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Avustralya	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Çin (Basitleştirilmiş Çince)	download.mcafee.com/products/manuals/zh-cn/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
Hollanda	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
İngiltere	download.mcafee.com/products/manuals/en-uk/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

İtalya	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Macaristan	download.mcafee.com/products/manuals/hu/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
Rusya	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Slovakya	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
Tayvan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Yunanistan	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf

McAfee VirusScan Plus Kullanıcı Kılavuzları

Ülke/Bölge	McAfee Kullanıcı Kılavuzları
Almanya	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Avustralya	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Çin (Basitleştirilmiş Çince)	download.mcafee.com/products/manuals/zh-cn/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
Hollanda	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
İngiltere	download.mcafee.com/products/manuals/en-uk/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
İtalya	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Macaristan	download.mcafee.com/products/manuals/hu/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
Rusya	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
Slovakya	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
Tayvan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Yunanistan	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf

McAfee VirusScan Kullanıcı Kılavuzları

Ülke/Bölge	McAfee Kullanıcı Kılavuzları
Almanya	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Avustralya	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Çin (Basitleştirilmiş Çince)	download.mcafee.com/products/manuals/zh-cn/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
Hollanda	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
İngiltere	download.mcafee.com/products/manuals/en-uk/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
İtalya	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Macaristan	download.mcafee.com/products/manuals/hu/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
Rusya	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Slovakya	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
Tayvan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Yunanistan	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf

Ülkenize veya bölgenize özel McAfee Threat Center ve Virüs Bilgisi siteleri için aşağıdaki tabloya başvurun.

Ülke/Bölge	Güvenlik Merkezi	Virüs Bilgisi
Almanya	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Avustralya	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Birleşik Devletler	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo
Brezilya	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Çek Cumhuriyeti	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Çin (Basitleştirilmiş Çince)	www.mcafee.com/us/threat_center	cn.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
Hollanda	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
İngiltere	www.mcafee.com/us/threat_center	uk.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
İtalya	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japonya	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Kanada (Fransızca)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo

Kanada (İngilizce)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kore	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Macaristan	www.mcafee.com/us/threat_center	hu.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
Rusya	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Slovakya	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
Tayvan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Türkiye	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Yunanistan	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo

Ülkenize veya bölgenize özel HackerWatch ve Virüs Bilgisi siteleri için aşağıdaki tabloya başvurun.

Ülke/Bölge	HackerWatch
Almanya	www.hackerwatch.org/?lang=de
Avustralya	www.hackerwatch.org
Birleşik Devletler	www.hackerwatch.org
Brezilya	www.hackerwatch.org/?lang=pt-br
Çek Cumhuriyeti	www.hackerwatch.org/?lang=cs
Çin (Basitleştirilmiş Çince)	www.hackerwatch.org/?lang=zh-cn
Danimarka	www.hackerwatch.org/?lang=da
Finlandiya	www.hackerwatch.org/?lang=fi
Fransa	www.hackerwatch.org/?lang=fr
Hollanda	www.hackerwatch.org/?lang=nl
İngiltere	www.hackerwatch.org
İspanya	www.hackerwatch.org/?lang=es
İsveç	www.hackerwatch.org/?lang=sv
İtalya	www.hackerwatch.org/?lang=it
Japonya	www.hackerwatch.org/?lang=jp
Kanada (Fransızca)	www.hackerwatch.org/?lang=fr-ca
Kanada (İngilizce)	www.hackerwatch.org
Kore	www.hackerwatch.org/?lang=ko

Macaristan	www.hackerwatch.org/?lang=hu
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
Rusya	www.hackerwatch.org/?lang=ru
Slovakya	www.hackerwatch.org/?lang=sk
Tayvan	www.hackerwatch.org/?lang=zh-tw
Türkiye	www.hackerwatch.org/?lang=tr
Yunanistan	www.hackerwatch.org/?lang=el

Dizin

8

802.11 162
802.11a 162
802.11b 162
802.1x 162

A

Aboneliğinizi doğrulama 12
Aboneliğinizi yenileme 12
Aboneliklerinizi yönetme 11, 18
ActiveX denetimi 162
açılan pencereler 162
ağ 162
ağ haritası 162
Ağ haritasına erişme 132
Ağ haritasında öğeyi gösterme veya gizleme 133
Ağ haritasını yenileme 132
Ağ haritasıyla çalışma 132
Ağ izleme bildirimlerini yeniden etkinleştirme 144
ağ sürücüsü 162
Ağa erişim izni verme 151
Ağa katılma 150
Ağdaki bilgisayarlara güvenmeyi durdurma 135
Ağı uzaktan yönetme 137
Ağın adını değiştirme 132, 152
Ağları izlemeyi durdurma 143
Ağlarınızı izleme 143
Akıllı Önerileri devre dışı bırakma 73
Akıllı Önerileri etkinleştirme 73
Akıllı Önerileri görüntüleme 73
Akıllı Önerileri uyarılar için yapılandırma 72
akıllı sürücü 162
anahtar 163
Anlık ileti korumasını başlatma 43
arabellek taşması 163
Arama ölçütleri 155
Arkadaş olarak işaretleme 145
arşivleme 163, 173

B

bant genişliği 163
Başka bir bilgisayara dosya gönderme 156
Başka bir bilgisayardan dosya kabul etme . 156, 157
Başlangıçta giriş ekranını gizleme 24
Başlatma sırasında bilgisayarınızı koruma ... 74
Başvuru 161
beyaz liste 163, 166
Bilgi uyarılarını gizleme 67
Bilgi uyarılarını gösterme ve gizleme 22
Bilgi uyarılarını gösterme veya gizleme 22
Bilgi uyarılarını yönetme 67
Bilgisayar ağ bilgilerini elde etme 103
Bilgisayar bağlantıları hakkında 86
Bilgisayar bağlantılarını yasaklama 89
Bilgisayar bağlantılarını yönetme 85
Bilgisayar bağlantısı ekleme 86
Bilgisayar bağlantısını düzenleme 88
Bilgisayar bağlantısını kaldırma 89
Bilgisayar kayıt bilgilerini elde etme 103
Bilgisayarınızı birleştirme 117
Bilgisayarınızı tarama 31
Bilgisayarınızı temizleme 113, 115
Bir ağ bilgisayarının coğrafi konumunu izleme 103
Bir aygıtı yönetme 139
Bir aygıtın görüntü özelliklerini değiştirme 139
Bir bilgisayarı yönetilen ağa katılmaya davet etme 134
Bir bilgisayarın koruma durumunu yönetme 138
Bir bilgisayarın koruma durumunu yönetmeyi durdurma 138
Bir programa tam erişim izni verme 80
Bir programa yalnızca giden erişim izni verme 81
Bir programın erişimini engelleme 82

C

Casus yazılım korumasını başlatma 42

D

DAT 163
Disk Birleştirici görevi zamanlama 121
Disk Birleştirici görevini değiştirme 122
Disk Birleştirici görevini silme 122
DNS 163
dolaşım 163
Dosya gönderildiğinde bildirim alma 157
dosya parçaları 163
Dosya paylaşma 154

Dosya paylaşmayı durdurma 154
Dosya ve klasörleri parçalama 124
Dosyaları diğer bilgisayarlara gönderme.....156
Dosyaları paylaşma 154
Dosyaları paylaşma ve gönderme.....153
Dosyaları, klasörleri ve diskleri parçalama .124
Durum ve izinleri yönetme.....138
düğüm.....163
düz metin 163

E

EasyNetwork özellikleri 148
EasyNetwork'ü açma 149
EasyNetwork'ü ayarlama.....149
Ek koruma kullanma 41
eklenti 164
e-posta 164, 172
e-posta istemcisi 164
E-posta korumasını başlatma.....43
erişim noktası (AP).....164
ESS 164
etki alanı 164
etkin nokta 164
ev ağı 162, 164

F

Firewall ayarlarını geri yükleme 78
Firewall güvenliğini iyileştirme 74
Firewall güvenlik düzeylerini yönetme.....70
Firewall Koruma Durumu ayarlarını yapılandırma 76
Firewall korumasını yapılandırma.....69
Firewall'u anında kilitleme 77
Firewall'u Başlatma 63
Firewall'u kilitleme ve geri yükleme 77
Firewall'un kilidini anında açma 77

G

geçici dosya 164
Gelen Olaylar günlüğünden bir bilgisayarı ekleme.....87
Gelen Olaylar günlüğünden bir bilgisayarı izleme.....104
Gelen Olaylar günlüğünden bir bilgisayarı yasaklama 91
Gelen olayları görüntüleme 101
Gelen ve giden trafiği analiz etme.....106
Genel güvenlik olayı istatistiklerini görüntüleme 102
Genel Internet port etkinliğini görüntüleme 102
gerçek zamanlı tarama.....164
Gerçek zamanlı tarama seçeneklerini ayarlama 38, 46
Gerçek zamanlı virüsten korumayı durdurma 47
Geri Dönüşüm Kutusu 165
Giden Olaylar günlüğünden program bilgilerini alma 84
Giden Olaylar günlüğünden tam erişim izni verme..... 81
Giden Olaylar günlüğünden yalnızca giden erişim izni verme..... 82
Giden olayları görüntüleme 81, 101
Giriş 3
Görev zamanlama 119
Güncelleştirmeleri denetleme 13, 15
Günlüğe kaydetme, izleme ve analiz 99
Güvenilenler listelerini kullanma 57
Güvenilenler listelerini yönetme..... 57
güvenilenler listesi 165
Güvenilenler listesi türleri hakkında..... 58
Güvenlik açıklarını düzeltme..... 140
güvenlik duvarı 165
Güvenlik duvarı korumasını başlatma 63
Güvenlik duvarı korumasını durdurma..... 64
Güvenlik düzeyini Görünmez seçeneğine ayarlama 71
Güvenlik düzeyini Otomatik seçeneğine ayarlama 72
Güvenlik düzeyini Standart seçeneğine ayarlama 71
Güvenlik iletilerini gizleme 25

H

HackerWatch dersini başlatma 110
harici sabit disk..... 165
hileli erişim noktası 165
hizmet reddi (DOS) saldırısı..... 165

I

Internet güvenliği hakkında bilgi alma..... 109
Internet trafiğini izleme 102, 105
IP adresi 165
IP hilesi 166

İ

içerik derecelendirme grubu 165
ileti kimlik doğrulama kodu (MAC)..... 165
intranet..... 165
İstatistiklerle Çalışma 102
isteğe bağlı tarama 166
istemci..... 166
İzinsiz Giriş Tespiti Olayları günlüğünden bir bilgisayarı izleme 104
İzinsiz Giriş Tespiti Olayları günlüğünden bir bilgisayarı yasaklama..... 92

İzinsiz giriş tespiti olaylarını görüntüleme ..101
İzinsiz giriş tespitini yapılandırma 76
izleme konumları.....166
İzlenen bir IP adresini izleme.....105
izlenen dosya türleri 166

K

kaba kuvvet saldırısı.....166
kablosuz bağdaştırıcı 166
kara liste 163, 166
karantina.....166
Karantinadaki dosyalarla çalışma.....36, 37
Karantinadaki programlar ve tanımlama bilgileriyle çalışma.....37
kayıt defteri 166
kısayol 167
kimlik doğrulama 162, 167
komut dosyası.....167
Komut dosyası tarama korumasını başlatma .42
Koruma durumu hakkında bilgi 7, 8, 9
Koruma hizmetleri hakkında bilgi.....10
Koruma kategorileri hakkında bilgi 7, 9, 27
Koruma sorunlarını el ile onarma.....18
Koruma sorunlarını onarma.....8, 18
Koruma sorunlarını onarma veya yok sayma .8, 17
Koruma sorunlarını otomatik olarak onarma 18
Koruma sorunlarını yok sayma 19
Koruma sorununu yok sayma.....19
köke inme 167
Kullanılabilir ağ yazıcısı yükleme.....160

L

LAN.....164, 167
launchpad 167
Lisans 175

M

MAC adresi 167
MAPI.....167
McAfee EasyNetwork 147
McAfee Hakkında 175
McAfee hesabınıza erişme 11
McAfee Network Manager.....127
McAfee Personal Firewall.....61
McAfee QuickClean.....111
McAfee SecurityCenter.....5
McAfee Shredder 123
McAfee Virtual Technician'ı kullanma 178
McAfee VirusScan 29
Mevcut sistem hizmeti portuna erişim izni verme 95
Mevcut sistem hizmeti portuna erişimi engelleme 95
MSN 167
Müşteri Desteği ve Teknik Destek 177

N

Network Manager özellikleri..... 128
Network Manager simgeleri hakkında bilgi 129
NIC 167
numara çeviriciler..... 167

O

olası istenmeyen program (PUP)..... 168
Olası istenmeyen programlarla çalışma..... 36
olay 168
Olay günlüğü ayarlarını yapılandırma..... 100
Olay Günlüğü Kaydetme..... 100
Olayları görüntüleme..... 18, 27
ortadaki adam saldırısı..... 168
Otomatik güncelleştirmeleri devre dışı bırakma 15
Otomatik güncelleştirmeleri yapılandırma ... 14
Oyun oynarken bilgi uyarılarını gösterme veya gizleme..... 23
Oyun sırasında uyarıları görüntüleme 67

Ö

Öğenin ayrıntılarını görüntüleme 133
önbellek 168
Özel tarama seçeneklerini ayarlama . 39, 48, 49

P

parola 168
parola kasası 168
Paylaşılan bir dosyayı arama 155
Paylaşılan dosyayı kopyalama..... 155
paylaşılan şifre..... 168
Paylaşılan yazıcılarla çalışma..... 160
paylaştırma..... 168
PCI kablosuz bağdaştırıcı kartı..... 168
PC'nizi tarama..... 32, 39
Personal Firewall özellikleri..... 62
phishing 169
Ping isteği ayarlarını yapılandırma..... 75
POP3..... 169, 170
port..... 169
PPPoE..... 169
Program bant genişliğini izleme 107
Program bilgilerini alma..... 84
Program etkinliğini izleme 107
Program iznini kaldırma 83
Programlar hakkında bilgi alma..... 84
Programlara Internet erişim izni verme 80

Programlara yalnızca giden erişim izni verme 81
Programları ve izinleri yönetme 79
Programların erişim izinlerini kaldırma 83
Programların Internet erişimini engelleme 82
protokol 169
proxy 169
proxy sunucusu 169

Q

QuickClean görevi zamanlama 119
QuickClean görevini değiştirme 120
QuickClean görevini silme 121
QuickClean özellikleri 112

R

RADIUS 168, 169

S

Saldırgan olarak işaretleme 144
savaş sürücüsü 169
SecurityCenter özellikleri 6
SecurityCenter'ı güncelleştirme 13
SecurityCenter'ı kullanma 7
senkronize etme 170
Shredder özellikleri 124
sıkıştırma 170
sistem geri yükleme noktası 170
Sistem hizmeti portlarını yapılandırma 94
Sistem hizmeti portunu değiştirme 97
Sistem hizmeti portunu kaldırma 98
Sistem hizmetlerini yönetme 93
Sistem Koruması 170
Sistem Koruması seçeneklerini kullanma 51
Sistem Koruması seçeneklerini yapılandırma 53
Sistem Koruması türleri hakkında 53, 54
Sistem Koruması'nı etkinleştirme 52
SMTP 170
solucan 170
Son Olaylar günlüğünden erişimi engelleme 83
Son Olaylar günlüğünden tam erişim izni verme 81
Son Olaylar günlüğünden yalnızca giden erişim izni verme 82
Son olayları görüntüleme 27, 100
sözlük saldırısı 170
SSID 170
SSL 170
standart e-posta hesabı 170
sunucu 170

Ş

şifreleme 163, 171
şifreli metin 171

T

tanımlama bilgisi 171
Tarama sonuçlarını görüntüleme 34
Tarama sonuçlarıyla çalışma 35
Tarama türleri 33, 38
Tarama zamanlama 39, 50
tarayıcı 171
Telif Hakkı 176
TKIP 171, 173
Trafik Analizi grafiği hakkında 106
Truva, Truva atı 171
Tüm diski parçalama 125
Tüm olayları görüntüleme 27
tümleşik ağ geçidi 171

U

U3 171
UDP ayarlarını yapılandırma 75
URL 171
USB 172
USB kablosuz bağdaştırıcı kartı 172
USB sürücüsü 162, 172
Uyarı seçeneklerini yapılandırma 23
Uyarılar hakkında 66
Uyarılarla birlikte sesi açma 23
Uyarılarla çalışma 14, 21, 65
Uzak bilgisayarlara McAfee güvenlik yazılımı yükleme 141

Ü

Ürününüzü etkinleştirme 11

V

Virtual Technician'ı başlatma 178
VirusScan özellikleri 30
virüs 172
Virüs saldırısı uyarılarını gizleme 24
Virüsler ve Truva atlarıyla çalışma 36
Virüsten korumayı ayarlama 31, 45
VPN 172

W

web bug'ları 172
web postası 164, 172
WEP 163, 172
Wi-Fi 172
Wi-Fi Alliance 172
Wi-Fi Certified 173
WLAN 173
WPA 163, 173
WPA2 ....163, 173

WPA2-PSK 163, 173
WPA-PSK 163, 173

Y

Yasaklanan bilgisayar bağlantısı ekleme 89
Yasaklanan bilgisayar bağlantısını düzenleme 90
Yasaklanan bilgisayar bağlantısını kaldırma.91
yayımlama 173
Yazıcı paylaşmayı durdurma.....160
Yazıcıları paylaşma 159
yedekleme.....163, 173
Yeni Arkadaşlar algılamayı durdurma 145
Yeni bir programa tam erişim izni verme.....80
Yeni bir programın erişimini engelleme 83
Yeni bir sistem hizmeti portunu yapılandırma 96
Yok sayılan sorunları gösterme veya gizleme 19
Yönetilen ağa katılma.....133
Yönetilen ağı terk etme 152
Yönetilen bir ağ kurma.....131
Yönetilen bir ağa katılma 134, 150, 152
Yönetilen bir bilgisayarın izinlerini değiştirme 139
yönlendirici.....173