



Virus and Spyware Protection

Manual do Utilizador

Índice

McAfee VirusScan	3
McAfee SecurityCenter	5
Funcionalidades do SecurityCenter.....	6
Utilizar o SecurityCenter	7
Actualizar o SecurityCenter	13
Corrigir ou ignorar problemas de protecção.....	17
Utilizar alertas	23
Ver eventos	29
McAfee VirusScan	31
Funcionalidades do VirusScan	33
Iniciar a protecção antivírus em tempo real	34
Iniciar protecção adicional.....	37
Configurar a protecção antivírus	41
Analisar o computador	59
Utilizar os resultados da análise.....	63
McAfee QuickClean	67
Funcionalidades do QuickClean	68
Limpar o computador.....	69
Desfragmentar o computador.....	73
Programar uma tarefa.....	74
McAfee Shredder.....	79
Funcionalidades do Shredder	80
Destruir ficheiros, pastas e discos.....	81
McAfee Network Manager.....	83
Funcionalidades do Network Manager	84
Noções básicas sobre os ícones do Network Manager	85
Configurar uma rede gerida	87
Gerir a rede de forma remota	95
Referência.....	101
Glossário	102
Acerca da McAfee	117
Copyright	117
Licença	118
Suporte a Clientes e Suporte Técnico.....	119
Utilizar o Técnico Virtual da McAfee	120
Suporte e Transferências	121
Índice remissivo	130

CAPÍTULO 1

McAfee VirusScan

O VirusScan com SiteAdvisor proporciona serviços de protecção e detecção avançados para otimizar a protecção do computador contra as mais recentes ameaças de segurança, incluindo vírus, cavalos de Tróia, cookies de controlo, spyware, adware e outros programas potencialmente indesejados. Com o VirusScan, a protecção não se limita aos ficheiros e pastas do computador de secretária ou do portátil, abrangendo também diferentes pontos de entrada de ameaças, entre os quais o correio electrónico, as mensagens instantâneas e a Web. As classificações de segurança da Web do McAfee SiteAdvisor ajudam a evitar Web sites inseguros.

Neste capítulo

McAfee SecurityCenter	5
McAfee VirusScan	31
McAfee QuickClean.....	67
McAfee Shredder	79
McAfee Network Manager	83
Referência	101
Acerca da McAfee	117
Suporte a Clientes e Suporte Técnico	119

CAPÍTULO 2

McAfee SecurityCenter

O McAfee SecurityCenter permite monitorizar o estado de segurança do computador, saber instantaneamente se os serviços de protecção antivírus, anti-spyware, de correio electrónico e de firewall estão actualizados e adoptar medidas sobre potenciais vulnerabilidades de segurança. Fornece os controlos e as ferramentas de navegação necessários para coordenar e gerir todas as áreas da protecção do computador.

Antes de começar a configurar e gerir a protecção do computador, analise a interface do SecurityCenter e certifique-se de que compreende a diferença entre estado de protecção, categorias de protecção e serviços de protecção. Em seguida, actualize o SecurityCenter para assegurar que possui a mais recente protecção disponível da McAfee.

Depois de concluir as tarefas de configuração iniciais, utilize o SecurityCenter para monitorizar o estado de protecção do computador. Se o SecurityCenter detectar um problema de protecção, apresenta um alerta para que possa corrigi-lo ou ignorá-lo (dependendo da gravidade). Também pode analisar eventos do SecurityCenter, tais como alterações à configuração da análise de vírus, num registo de eventos.

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades do SecurityCenter	6
Utilizar o SecurityCenter	7
Actualizar o SecurityCenter	13
Corrigir ou ignorar problemas de protecção.....	17
Utilizar alertas	23
Ver eventos	29

Funcionalidades do SecurityCenter

O SecurityCenter oferece as seguintes funcionalidades:

Estado de protecção simplificado

Analisa facilmente o estado de protecção do computador, procura actualizações e corrige potenciais problemas de protecção.

Actualizações automáticas

Transfere e instala automaticamente actualizações para os seus programas registados. Quando está disponível uma nova versão de um programa registado da McAfee, a mesma pode ser obtida gratuitamente durante a validade da subscrição, garantindo sempre uma protecção actualizada.

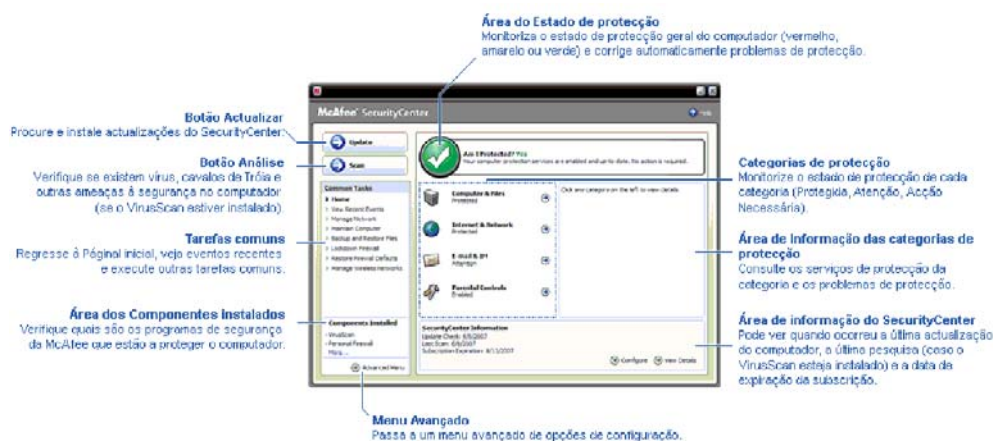
Alerta em tempo real

Os alertas de segurança informam-no sobre surtos de vírus e ameaças de segurança e fornecem opções para remover, neutralizar ou obter mais informações sobre a ameaça.

CAPÍTULO 3

Utilizar o SecurityCenter

Antes de começar a utilizar o SecurityCenter, analise os componentes e as áreas de configuração que utilizará para gerir o estado de protecção do computador. Para obter mais informações acerca da terminologia utilizada nesta imagem, consulte as secções **Noções sobre o estado de protecção** (página 8) e **Noções sobre categorias de protecção** (página 9). Em seguida, pode analisar a informação da sua conta McAfee e verificar a validade da subscrição.



Neste capítulo

Noções sobre o estado de protecção	8
Noções sobre categorias de protecção	9
Noções sobre serviços de protecção	10
Gerir a conta McAfee.....	11

Noções sobre o estado de protecção

O estado de protecção do computador é apresentado na área do estado de protecção no painel Página Inicial do SecurityCenter. O estado indica se o computador está totalmente protegido contra as mais recentes ameaças de segurança e pode ser influenciado por factores como ataques de segurança externos, outros programas de segurança e programas que acedem à Internet.

O estado de protecção do computador pode apresentar as cores vermelha, amarela ou verde.

Estado de protecção	Descrição
Vermelho	O computador não está protegido. A cor vermelha da área do estado de protecção no painel Página Inicial do SecurityCenter indica que não está protegido. O SecurityCenter comunica, pelo menos, um problema de segurança crítico. Para obter protecção total, deve corrigir todos os problemas de segurança críticos em cada categoria de protecção (o estado da categoria do problema é definido para Acção Necessária, também a vermelho). Para obter informações sobre como corrigir problemas de protecção, consulte a secção Corrigir problemas de protecção (página 18).
Amarelo	O computador está parcialmente protegido. A cor amarela da área do estado de protecção no painel Página Inicial do SecurityCenter indica que não está protegido. O SecurityCenter comunica, pelo menos, um problema de segurança não crítico. Para obter protecção total, deve corrigir ou ignorar os problemas de segurança não críticos associados a cada categoria de protecção. Para obter informações sobre como corrigir ou ignorar problemas de protecção, consulte a secção Corrigir ou ignorar problemas de protecção (página 17).
Verde	O computador está totalmente protegido. A cor verde da área do estado de protecção no painel Página Inicial do SecurityCenter indica que está protegido. O SecurityCenter não comunica quaisquer problemas de segurança críticos ou não críticos. Cada categoria de protecção lista os serviços que estão a proteger o computador.

Noções sobre categorias de protecção

Os serviços de protecção do SecurityCenter estão divididos em quatro categorias: Computador & Ficheiros, Internet & Rede, Correio electrónico & IM e Limitações de Acesso. Estas categorias ajudam-no a procurar e a configurar os serviços de segurança que protegem o computador.

Clique num nome de categoria para configurar os respectivos serviços de protecção e ver os problemas de segurança detectados para esses serviços. Se o estado de protecção do computador apresentar as cores vermelha ou amarela, uma ou mais categorias apresentam as mensagens *Ação Necessária* ou *Atenção* para indicar que o SecurityCenter detectou um problema na categoria. Para obter mais informações sobre o estado de protecção, consulte a secção **Noções sobre o estado de protecção** (página 8).

Categoria de Protecção	Descrição
Computador & Ficheiros	A categoria Computador & Ficheiros permite configurar os seguintes serviços de protecção: - Protecção Antivírus - Protecção contra PUP - Monitores do Sistema - Protecção do Windows
Internet & Rede	A categoria Internet & Rede permite configurar os seguintes serviços de protecção: - Protecção por Firewall - Protecção de Identidade
Correio electrónico & IM	A categoria Correio electrónico & IM permite configurar os seguintes serviços de protecção: - Protecção do Correio electrónico - Protecção contra Correio Publicitário Não Solicitado
Limitações de Acesso	A categoria Limitações de Acesso permite configurar os seguintes serviços de protecção: Bloqueio de Conteúdos

Noções sobre serviços de protecção

Os serviços de protecção são os componentes principais do SecurityCenter que deve configurar para proteger o computador. Os serviços de protecção correspondem directamente a programas da McAfee. Por exemplo, com a instalação do VirusScan, ficam disponíveis os seguintes serviços de protecção: Protecção Antivírus, Protecção contra PUP, Monitores do Sistema e Protecção do Windows. Para obter informações detalhadas sobre estes serviços de protecção específicos, consulte a ajuda do VirusScan.

Por predefinição, todos os serviços de protecção associados a um programa são activados quando o programa é instalado; no entanto, é possível desactivar um serviço de protecção em qualquer altura. Por exemplo, se instalar o Privacy Service, o Bloqueio de Conteúdos e a Protecção de Identidade são activados. Se não pretender utilizar o serviço de protecção Bloqueio de Conteúdos, pode desactivá-lo totalmente. Também pode desactivar temporariamente um serviço de protecção enquanto executa tarefas de configuração ou de manutenção.

Gerir a conta McAfee

Efectue a gestão da sua conta McAfee a partir do SecurityCenter, que permite aceder e analisar facilmente a informação da conta e verificar o estado actual da subscrição.

Nota: Se tiver instalado os programas da McAfee a partir de um CD, deve registá-los no Web site da McAfee para configurar ou actualizar a sua conta McAfee. Só então terá direito a actualizações regulares e automáticas dos programas.

Gerir a conta McAfee

Pode aceder facilmente à informação da sua conta McAfee (A Minha Conta) a partir do SecurityCenter.

- 1 Em **Tarefas Comuns**, clique em **A Minha Conta**.
- 2 Inicie sessão na sua conta McAfee.

Verifique a subscrição

Deve verificar a sua subscrição para assegurar-se de que ainda não expirou.

- Clique com o botão direito do rato no ícone do SecurityCenter  na área de notificação, na parte mais à direita da barra de tarefas e, em seguida, clique em **Verificar Subscrição**.

CAPÍTULO 4

Actualizar o SecurityCenter

O SecurityCenter assegura que os seus programas registados da McAfee estão actualizados ao procurar e instalar actualizações online de quatro em quatro horas. Dependendo dos programas que tiver instalado e registado, as actualizações online podem incluir as mais recentes definições de vírus e actualizações de protecção de privacidade ou contra hackers, correio publicitário não solicitado e spyware. Se pretender verificar a existência de actualizações durante o período predefinido de quatro horas, pode fazê-lo em qualquer altura. Enquanto o SecurityCenter verifica a existência de actualizações, pode continuar a executar outras tarefas.

Embora não seja recomendado, pode alterar a forma como o SecurityCenter verifica e instala as actualizações. Por exemplo, pode configurar o SecurityCenter para transferir e não instalar as actualizações ou para o notificar antes de transferir ou instalar as actualizações. Também pode desactivar a actualização automática.

Nota: Se tiver instalado programas da McAfee a partir de um CD, deverá registá-los no Web site da McAfee para poder receber actualizações regulares e automáticas para esses programas.

Neste capítulo

Verificar a existência de actualizações	13
Configurar actualizações automáticas	14
Desactivar as actualizações automáticas	14

Verificar a existência de actualizações

Por predefinição, o SecurityCenter verifica automaticamente a existência de actualizações de quatro em quatro horas quando o computador está ligado à Internet; no entanto, se pretender verificar a existência de actualizações dentro do período de quatro horas, pode fazê-lo. Se tiver desactivado as actualizações automáticas, deve verificar regularmente se existem actualizações.

- No painel Página Inicial do SecurityCenter, clique em **Actualizar**.

Sugestão: Para verificar a existência de actualizações sem iniciar o SecurityCenter, clique com o botão direito do rato no ícone do SecurityCenter  na área de notificação, na parte mais à direita da barra de tarefas e, em seguida, clique em **Actualizações**.

Configurar actualizações automáticas

Por predefinição, o SecurityCenter procura e instala automaticamente actualizações de quatro em quatro horas quando o computador está ligado à Internet. Se pretender alterar este comportamento predefinido, pode configurar o SecurityCenter para transferir automaticamente as actualizações e, em seguida, notificá-lo de que estas estão prontas para serem instaladas, ou notificá-lo antes de transferir as actualizações.

Nota: O SecurityCenter utiliza alertas para o notificar da existência de actualizações prontas para transferir ou instalar. A partir dos alertas, pode transferir ou instalar as actualizações ou adiar as actualizações. Ao actualizar os programas a partir de um alerta, poderá ser-lhe solicitado que verifique a sua subscrição antes de transferir e instalar. Para obter mais informações, consulte a secção **Utilizar alertas** (página 23).

- 1 Abra o painel de configuração do SecurityCenter.
Como?
 1. Em **Tarefas Comuns**, clique em **Página Inicial**.
 2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
- 2 No painel de configuração do SecurityCenter, em **As actualizações automáticas estão desactivadas**, clique em **Activar** e, em seguida, em **Avançadas**.
- 3 Clique num dos seguintes botões:
 - **Instalar as actualizações automaticamente e notificar-me quando os serviços forem actualizados (recomendado)**
 - **Transferir as actualizações automaticamente e notificar quando estiverem prontas para serem instaladas**
 - **Notificar antes de transferir quaisquer actualizações**
- 4 Clique em **OK**.

Desactivar as actualizações automáticas

Se desactivar as actualizações automáticas, deve verificar regularmente a existência de actualizações, caso contrário, o computador não terá a mais recente protecção de segurança. Para obter informações sobre a verificação manual de actualizações, consulte a secção **Verificar a existência de actualizações** (página 13).

- 1 Abra o painel de configuração do SecurityCenter.
Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
 2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
- 2** No painel de configuração do SecurityCenter, em **As actualizações automáticas estão activadas**, clique em **Desactivar**.

Sugestão: Para activar as actualizações automáticas clique no botão **Activar** ou desmarque a opção **Desactivar as actualizações automáticas e deixar-me verificar manualmente se existem actualizações** no painel Opções de Actualização.

CAPÍTULO 5

Corrigir ou ignorar problemas de protecção

O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Os problemas críticos requerem uma acção imediata e comprometem o estado de protecção (a cor muda para vermelho). Os problemas de protecção não críticos não requerem uma acção imediata e podem ou não comprometer o estado de protecção (dependendo do tipo de problema). Para obter o estado de protecção verde, deve corrigir todos os problemas críticos e corrigir ou ignorar todos os problemas não críticos. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee. Para obter mais informações sobre o Técnico Virtual da McAfee, consulte a ajuda do Técnico Virtual da McAfee.

Neste capítulo

Resolução de problemas relacionados com protecção	18
Ignorar problemas de protecção.....	20

Resolução de problemas relacionados com protecção

A maioria dos problemas de segurança pode ser corrigida automaticamente; no entanto, alguns problemas poderão requerer a sua acção. Por exemplo, se a Protecção de Firewall estiver desactivada, o SecurityCenter pode activá-la; no entanto, se não estiver instalada, deverá instalá-la. A tabela seguinte descreve algumas acções que deverá executar ao corrigir problemas de protecção manualmente:

Problema	Acção
Não foi executada uma análise completa do computador nos últimos 30 dias.	Analise o computador manualmente. Para obter mais informações, consulte a ajuda do VirusScan.
Os seus ficheiros de assinatura de detecção (DAT) estão desactualizados.	Actualize a protecção manualmente. Para obter mais informações, consulte a ajuda do VirusScan.
Um programa não está instalado.	Instale o programa a partir do Web site da McAfee ou de um CD.
Faltam componentes num programa.	Reinstale o programa a partir do Web site da McAfee ou de um CD.
Um programa não está registado e não pode receber protecção total.	Registe o programa no Web site da McAfee.
Um programa expirou.	Verifique o estado da sua conta no Web site da McAfee.

Nota: Muitas vezes, um único problema de protecção afecta mais do que uma categoria de protecção. Neste caso, a correcção do problema numa categoria apaga-o em todas as outras categorias.

Resolução automática de problemas de protecção

O SecurityCenter pode corrigir a maioria dos problemas de protecção automaticamente. As alterações de configuração efectuadas pelo SecurityCenter ao corrigir automaticamente problemas de protecção não são guardadas no registo de eventos. Para mais informações sobre eventos, consulte **Ver Eventos** (página 29).

- 1 Em **Tarefas Comuns**, clique em **Página Inicial**.
- 2 No painel **Página Inicial** do SecurityCenter, na área do estado de protecção, clique em **Corrigir**.

Resolução manual de problemas de protecção

Se um ou mais problemas de protecção persistirem depois de tentar corrigi-los automaticamente, pode tentar corrigi-los manualmente.

- 1** Em **Tarefas Comuns**, clique em **Página Inicial**.
- 2** No painel Página Inicial do SecurityCenter, clique na categoria de protecção em que o SecurityCenter comunica o problema.
- 3** Clique na ligação apresentada a seguir à descrição do problema.

Ignorar problemas de protecção

Se o SecurityCenter detectar um problema não crítico, pode optar por corrigi-lo ou ignorá-lo. Outros problemas não críticos (por exemplo, se o Anti-spam ou o Privacy Service não estiverem instalados) são ignorados automaticamente. Os problemas ignorados não são apresentados na área de informação da categoria da protecção no painel Página Principal do SecurityCenter, a menos que o estado de protecção do computador esteja verde. Se ignorar um problema e posteriormente decidir que pretende que o mesmo seja apresentado na área de informação da categoria de protecção mesmo que o estado de protecção do computador não esteja verde, pode mostrar esse problema ignorado.

Ignorar um problema de protecção

É possível ignorar um problema não crítico detectado pelo SecurityCenter se não pretender corrigi-lo. Se ignorar o problema, este será removido da área de informação da categoria de protecção no SecurityCenter.

- 1 Em **Tarefas Comuns**, clique em **Página Inicial**.
- 2 No painel Página Inicial do SecurityCenter, clique na categoria de protecção em que o problema é comunicado.
- 3 Clique na ligação **Ignorar** junto ao problema de protecção.

Mostrar ou ocultar problemas ignorados

Dependendo da gravidade, é possível mostrar ou ocultar um problema de protecção ignorado.

- 1 Abra o painel Opções de Alerta.
Como?
 1. Em **Tarefas Comuns**, clique em **Página Inicial**.
 2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
 3. Em **Alertas**, clique em **Avançado**.
- 2 No painel Configuração do SecurityCenter, clique em **Problemas Ignorados**.
- 3 No painel Problemas Ignorados, proceda de um dos seguintes modos:
 - Para ignorar um problema, seleccione a caixa de verificação respectiva.
 - Para comunicar um problema na área de informação da categoria de protecção, desmarque a respectiva caixa de verificação.

4 Clique em **OK**.

Sugestão: Também pode clicar na ligação **Ignorar** junto ao problema comunicado na área de informação da categoria de protecção para o ignorar.

CAPÍTULO 6

Utilizar alertas

Os alertas são pequenas caixas de diálogo de pop-up que são apresentadas no canto inferior direito do ecrã quando ocorrem determinados eventos do SecurityCenter. Um alerta fornece informações detalhadas acerca de um evento, bem como recomendações e opções para a resolução de problemas que podem estar associados ao evento. Alguns alertas podem também conter ligações para informações adicionais acerca do evento. Essas ligações permitem aceder ao Web site global da McAfee ou enviar informações à McAfee para resolução de problemas.

Existem três tipos de alertas: vermelho, amarelo e verde.

Tipo de Alerta	Descrição
Vermelho	Um alerta vermelho é uma notificação crítica que requer uma resposta por parte do utilizador. Os alertas vermelhos ocorrem quando o SecurityCenter não consegue determinar a forma de corrigir automaticamente um problema de protecção.
Amarelo	Um alerta amarelo é uma notificação não crítica que, normalmente, requer uma resposta por parte do utilizador.
Verde	Um alerta verde é uma notificação não crítica que não requer uma resposta por parte do utilizador. Os alertas verdes fornecem informações básicas acerca de um evento.

Uma vez que os alertas desempenham um papel extremamente importante na monitorização e gestão do estado de protecção, não é possível desactivá-los. No entanto, é possível controlar se determinados tipos de alertas informativos são apresentados e configurar algumas opções de alerta (tais como se o SecurityCenter reproduz um som com o alerta ou se apresenta o ecrã inicial da McAfee no arranque).

Neste capítulo

Mostrar e ocultar alertas informativos	24
Configurar opções de alerta	26

Mostrar e ocultar alertas informativos

Os alertas informativos notificam-no quando ocorrem eventos que não constituem ameaças para a segurança do computador. Por exemplo, se tiver configurado a Protecção de Firewall, é apresentado um alerta informativo por predefinição sempre que um programa do computador for autorizado a aceder à Internet. Se não pretender que um determinado tipo de alerta informativo seja apresentado, pode ocultá-lo. Se não pretender visualizar quaisquer alertas informativos, pode ocultá-los todos. Também pode ocultar todos os alertas informativos quando está a jogar em modo de ecrã completo no computador. Quando terminar o jogo e sair do modo de ecrã completo, o SecurityCenter volta a apresentar os alertas informativos.

Se ocultar um alerta informativo acidentalmente, pode mostrá-lo novamente em qualquer altura. Por predefinição, o SecurityCenter mostra todos os alertas informativos.

Mostrar ou ocultar alertas informativos

É possível configurar o SecurityCenter para mostrar alguns alertas informativos e ocultar outros, bem como para ocultar todos os alertas informativos.

- 1 Abra o painel Opções de Alerta.
Como?
 1. Em **Tarefas Comuns**, clique em **Página Inicial**.
 2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
 3. Em **Alertas**, clique em **Avançado**.
- 2 No painel Configuração do SecurityCenter, clique em **Alertas Informativos**.
- 3 No painel Alertas Informativos, proceda de um dos seguintes modos:
 - Para mostrar um alerta informativo, desmarque a respectiva caixa de verificação.
 - Para ocultar um alerta informativo, seleccione a respectiva caixa de verificação.
 - Para ocultar todos os alertas informativos, seleccione a caixa de verificação **Não mostrar alertas informativos**.
- 4 Clique em **OK**.

Sugestão: Também pode ocultar um alerta informativo seleccionando a caixa de verificação **Não mostrar este alerta novamente** no próprio alerta. Se o fizer, pode mostrar o alerta informativo novamente desmarcando a caixa de verificação adequada no painel Alertas Informativos.

Mostrar ou ocultar alertas informativos durante jogos

É possível ocultar todos os alertas informativos quando está a jogar em modo de ecrã completo no computador. Quando terminar o jogo e sair do modo de ecrã completo, o SecurityCenter volta a apresentar os alertas informativos.

- 1** Abra o painel Opções de Alerta.
Como?
 1. Em **Tarefas Comuns**, clique em **Página Inicial**.
 2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
 3. Em **Alertas**, clique em **Avançado**.
- 2** No painel Opções de Alerta, seleccione ou desmarque a caixa de verificação **Mostrar alertas informativos quando o modo de jogo for detectado**.
- 3** Clique em **OK**.

Configurar opções de alerta

O aspecto e a frequência dos alertas são configurados pelo SecurityCenter; no entanto, é possível ajustar opções básicas de alerta. Por exemplo, é possível reproduzir um som com os alertas ou ocultar a apresentação do alerta do ecrã inicial quando o Windows for iniciado. Também é possível ocultar alertas que notificam sobre surtos de vírus e outras ameaças de segurança na comunidade online.

Reproduzir um som com os alertas

Se pretender receber uma indicação audível de que ocorreu um alerta, pode configurar o SecurityCenter para reproduzir um som com cada alerta.

- 1 Abra o painel Opções de Alerta.
Como?
 1. Em **Tarefas Comuns**, clique em **Página Inicial**.
 2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
 3. Em **Alertas**, clique em **Avançado**.
- 2 No painel Opções de Alertas, em **Som**, seleccione a caixa de verificação **Reproduzir um som quando ocorre um alerta**.

Ocultar o ecrã inicial no arranque

Por predefinição, o ecrã inicial da McAfee é apresentado brevemente quando o Windows é iniciado, para informar que o SecurityCenter está a proteger o computador. No entanto, é possível ocultar o ecrã inicial se não quiser que seja apresentado.

- 1 Abra o painel Opções de Alerta.
Como?
 1. Em **Tarefas Comuns**, clique em **Página Inicial**.
 2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
 3. Em **Alertas**, clique em **Avançado**.
- 2 No painel Opções de Alerta, em **Ecrã Inicial**, desmarque a caixa de verificação **Mostrar o ecrã inicial da McAfee quando o Windows é iniciado**.

Sugestão: Para mostrar o ecrã inicial novamente em qualquer altura, seleccione a caixa de verificação **Mostrar o ecrã inicial da McAfee quando o Windows é iniciado**.

Ocultar alertas de surtos de vírus

É possível ocultar alertas que notificam sobre surtos de vírus e outras ameaças de segurança na comunidade online.

1 Abra o painel Opções de Alerta.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel direito, em **Informações sobre o SecurityCenter**, clique em **Configurar**.
3. Em **Alertas**, clique em **Avançado**.

2 No painel Opções de Alerta, desmarque a caixa de verificação **Alertar-me quando ocorrer uma infecção por vírus ou uma ameaça de segurança**.

Sugestão: Para apresentar alertas de surtos de vírus em qualquer altura, seleccione a caixa de verificação **Alertar-me quando ocorrer uma infecção por vírus ou uma ameaça de segurança**.

CAPÍTULO 7

Ver eventos

Um evento é uma acção ou uma alteração de configuração que ocorre numa categoria de protecção e nos serviços de protecção relacionados. Serviços de protecção diferentes registam tipos de eventos diferentes. Por exemplo, o SecurityCenter regista um evento se um serviço de protecção for activado ou desactivado; a Protecção de Vírus regista um evento sempre que é detectado e removido um vírus; a Protecção de Firewall regista um evento sempre que é bloqueada uma tentativa de ligação à Internet. Para obter mais informações sobre categorias de protecção, consulte a secção **Noções sobre categorias de protecção** (página 9).

É possível visualizar eventos durante a resolução de problemas de configuração ou durante a análise de operações efectuadas por outros utilizadores. Muitos pais utilizam o registo de eventos para controlar o comportamento dos filhos na Internet. Para examinar apenas os últimos 30 eventos ocorridos, visualize eventos recentes. Para examinar uma lista completa de todos os eventos ocorridos, visualize todos os eventos. Quando um utilizador visualiza todos os eventos, o SecurityCenter inicia o registo de eventos, o qual ordena os eventos de acordo com a categoria de protecção em que ocorreram.

Neste capítulo

Ver eventos recentes	29
Ver todos os eventos	30

Ver eventos recentes

Para examinar apenas os últimos 30 eventos ocorridos, visualize eventos recentes.

- Em **Tarefas Comuns**, clique em **Ver Eventos Recentes**.

Ver todos os eventos

Para examinar uma lista completa de todos os eventos ocorridos, visualize todos os eventos.

- 1** Em **Tarefas Comuns**, clique em **Ver Eventos Recentes**.
- 2** No painel Eventos Recentes, clique em **Ver Registo**.
- 3** No painel esquerdo do registo de eventos, clique no tipo de eventos que pretende visualizar.

CAPÍTULO 8

McAfee VirusScan

Os serviços de protecção e detecção avançados do VirusScan protegem o utilizador e o computador contra as mais recentes ameaças de segurança, incluindo vírus, cavalos de Tróia, cookies de controlo, spyware, adware e outros programas potencialmente indesejados. A protecção não se limita aos ficheiros e pastas do computador de secretária, abrangendo também diferentes pontos de entrada de ameaças, entre os quais o correio electrónico, as mensagens instantâneas e a Web.

Com o VirusScan, a protecção do computador é imediata e contínua (sem necessidade de tarefas de administração fastidiosas). Enquanto trabalha, navega na Web ou verifica o correio electrónico, o VirusScan monitoriza, analisa e detecta perigos potenciais em tempo real, trabalhando em segundo plano. As análises completas são executadas de acordo com a agenda, utilizando um conjunto de opções mais sofisticado para verificar periodicamente o computador. O VirusScan proporciona-lhe flexibilidade para personalizar este comportamento, mas o computador continua protegido se não o fizer.

Durante a utilização normal do computador, podem infiltrar-se vírus, worms e outras ameaças potenciais. Se isso ocorrer, o VirusScan notifica-o sobre a ameaça mas trata-a automaticamente e limpa ou coloca em quarentena os itens infectados antes que ocorram danos. Por vezes, podem ser necessárias acções adicionais. Nesses casos, o VirusScan permite ao utilizador decidir o que fazer (voltar a analisar na próxima vez que iniciar o computador, manter o item detectado ou removê-lo).

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades do VirusScan.....	33
Iniciar a protecção antivírus em tempo real	34
Iniciar protecção adicional.....	37
Configurar a protecção antivírus	41
Analisar o computador	59
Utilizar os resultados da análise	63

Funcionalidades do VirusScan

O VirusScan oferece as seguintes funcionalidades.

Protecção antivírus completa

Os serviços de protecção e detecção avançados do VirusScan protegem o utilizador e o computador contra as mais recentes ameaças de segurança, incluindo vírus, cavalos de Tróia, cookies de controlo, spyware, adware e outros programas potencialmente indesejados. A protecção não se limita aos ficheiros e pastas do computador de secretária, abrangendo também diferentes pontos de entrada de ameaças, entre os quais o correio electrónico, as mensagens instantâneas e a Web. Sem necessidade de tarefas de administração fastidiosas.

Opções de análise em função dos recursos

Se tiver velocidades de análise lentas, pode desactivar a opção para utilizar recursos mínimos do computador, mas tenha em atenção que será dada uma prioridade mais elevada à protecção antivírus do que a outras tarefas. O VirusScan proporciona-lhe flexibilidade para personalizar as opções de análise manual e em tempo real, mas o computador continua protegido se não o fizer.

Reparações automáticas

Se o VirusScan detectar uma ameaça de segurança durante a execução de uma análise manual ou em tempo real, tentará processá-la automaticamente de acordo com o tipo de ameaça. Deste modo, a maioria das ameaças pode ser detectada e neutralizada sem interacção do utilizador. Por vezes, o VirusScan poderá não conseguir neutralizar uma ameaça sozinho. Nesses casos, o VirusScan permite ao utilizador decidir o que fazer (voltar a analisar na próxima vez que iniciar o computador, manter o item detectado ou removê-lo).

Interromper tarefas em modo de ecrã completo

Quando está a ver filmes, a jogar no computador ou a realizar qualquer outra actividade que ocupe a totalidade do ecrã, o VirusScan interrompe diversas tarefas, incluindo actualizações automáticas e análises manuais.

Iniciar a protecção antivírus em tempo real

O VirusScan proporciona dois tipos de protecção antivírus: em tempo real e manual. A protecção antivírus em tempo real monitoriza continuamente a existência de actividades de vírus no computador, analisando os ficheiros sempre que são acedidos pelo utilizador ou pelo computador. A protecção antivírus manual permite analisar ficheiros a pedido. Para ter a certeza de que o computador está protegido contra as mais recentes ameaças de segurança, active a protecção antivírus em tempo real e agende análises manuais mais completas e regulares. Por predefinição, o VirusScan executa uma análise agendada uma vez por semana. Para obter mais informações sobre análise em tempo real e análise manual, consulte a secção **Analisar o computador** (página 59).

Por vezes, poderá querer interromper temporariamente as análises em tempo real (por exemplo, para alterar opções de análise ou resolver um problema de desempenho). Quando a protecção antivírus em tempo real está desactivada, o computador não está protegido e o estado de protecção do SecurityCenter fica vermelho. Para obter mais informações sobre o estado de protecção, consulte a secção "Noções sobre o estado de protecção" na ajuda do SecurityCenter.

Iniciar a protecção antivírus em tempo real

Por predefinição, a protecção antivírus em tempo real está activada e a proteger o computador contra vírus, cavalos de Tróia e outras ameaças de segurança. Se desactivar a protecção antivírus em tempo real, deve activá-la novamente para se manter protegido.

- 1** Abra o painel de configuração Computador & Ficheiros.
Como?
 1. No painel esquerdo, clique em **Menu Avançado**.
 2. Clique em **Configurar**.
 3. No painel Configurar, clique em **Computador & Ficheiros**.
- 2** Em **Protecção Antivírus**, clique em **Ligado**.

Interromper a protecção antivírus em tempo real

É possível desactivar temporariamente a protecção antivírus em tempo real e especificar quando deve ser retomada. É possível retomar automaticamente a protecção após 15, 30, 45 ou 60 minutos, quando o computador é reiniciado ou nunca.

- 1** Abra o painel de configuração Computador & Ficheiros.
Como?
 1. No painel esquerdo, clique em **Menu Avançado**.
 2. Clique em **Configurar**.
 3. No painel Configurar, clique em **Computador & Ficheiros**.
- 2** Em **Protecção Antivírus**, clique em **Desligado**.
- 3** Na caixa de diálogo, seleccione quando deve ser retomada a análise em tempo real.
- 4** Clique em **OK**.

CAPÍTULO 9

Iniciar protecção adicional

Além da protecção antivírus em tempo real, o VirusScan fornece protecção avançada contra scripts, spyware e anexos de correio electrónico e mensagens instantâneas potencialmente prejudiciais. Por predefinição, as protecções de análise de scripts, anti-spyware, de correio electrónico e de mensagens instantâneas estão activadas e a proteger o computador.

Protecção de análise de scripts

A protecção de análise de scripts detecta scripts potencialmente prejudiciais e impede que sejam executados no computador. A protecção monitoriza a existência de actividades de scripts suspeitas no computador, tais como um script que cria, copia ou elimina ficheiros, ou abre o registo do Windows, e alerta-o antes que ocorram danos.

Protecção anti-spyware

A protecção anti-spyware detecta spyware, adware e outros programas potencialmente indesejados. Spyware é software que pode ser instalado secretamente no computador para monitorizar o seu comportamento, recolher informações pessoais e mesmo interferir no controlo do computador através da instalação de software adicional ou do redireccionamento da actividade do browser.

Protecção do correio electrónico

A protecção do correio electrónico detecta actividades suspeitas nas mensagens e anexos de correio electrónico enviados e recebidos.

Protecção de mensagens instantâneas

A protecção de mensagens instantâneas detecta potenciais ameaças de segurança em anexos de mensagens instantâneas recebidas. De igual modo, impede que os programas de mensagens instantâneas partilhem informações pessoais.

Neste capítulo

Iniciar a protecção de análise de scripts.....	38
Iniciar a protecção anti-spyware	38
Iniciar a protecção do correio electrónico	39
Iniciar a protecção de mensagens instantâneas	39

Iniciar a protecção de análise de scripts

Active a protecção de análise de scripts para detectar scripts potencialmente prejudiciais e impedir que sejam executados no computador. A protecção de análise de scripts alerta o utilizador quando um script tenta criar, copiar ou eliminar ficheiros no computador ou alterar o registo do Windows.

- 1 Abra o painel de configuração Computador & Ficheiros.

Como?

1. No painel esquerdo, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Computador & Ficheiros**.

- 2 Em **Protecção de análise de scripts**, clique em **Ligado**.

Nota: Embora seja possível desactivar a protecção de análise de scripts em qualquer altura, o computador ficará vulnerável a scripts prejudiciais.

Iniciar a protecção anti-spyware

Active a protecção anti-spyware para detectar e remover spyware, adware e outros programas potencialmente indesejados que recolhem e transmitem os seus dados privados sem o seu conhecimento ou permissão.

- 1 Abra o painel de configuração Computador & Ficheiros.

Como?

1. No painel esquerdo, clique em **Menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Computador & Ficheiros**.

- 2 Em **Protecção de análise de scripts**, clique em **Ligado**.

Nota: Embora seja possível desactivar a protecção anti-spyware em qualquer altura, o computador ficará vulnerável a programas potencialmente indesejados.

Iniciar a protecção do correio electrónico

Active a protecção do correio electrónico para detectar worms e potenciais ameaças nas mensagens e anexos de correio electrónico a enviar (SMTP) e receber (POP3).

- 1** Abra o painel de configuração Correio Electrónico e Mensagens Instantâneas
Como?
 1. No painel esquerdo, clique em **Menu Avançado**.
 2. Clique em **Configurar**.
 3. No painel Configurar, clique em **Correio electrónico & IM**.
- 2** Em **Protecção do correio electrónico**, clique em **Ligado**.

Nota: Embora seja possível desactivar a protecção de correio electrónico em qualquer altura, o computador ficará vulnerável a ameaças de correio electrónico.

Iniciar a protecção de mensagens instantâneas

Active a protecção de mensagens instantâneas para detectar ameaças de segurança que podem estar incluídas em anexos de mensagens instantâneas a receber.

- 1** Abra o painel de configuração Correio Electrónico e Mensagens Instantâneas
Como?
 1. No painel esquerdo, clique em **Menu Avançado**.
 2. Clique em **Configurar**.
 3. No painel Configurar, clique em **Correio electrónico & IM**.
- 2** Em **Protecção de mensagens instantâneas**, clique em **Ligado**.

Nota: Embora seja possível desactivar a protecção de mensagens instantâneas em qualquer altura, o computador ficará vulnerável a anexos de mensagens instantâneas prejudiciais.

CAPÍTULO 10

Configurar a protecção antivírus

O VirusScan proporciona dois tipos de protecção antivírus: em tempo real e manual. A protecção antivírus em tempo real analisa os ficheiros sempre que o utilizador ou o computador acedem aos mesmos. A protecção antivírus manual permite analisar ficheiros a pedido. É possível configurar opções diferentes para cada tipo de protecção. Por exemplo, uma vez que a protecção em tempo real monitoriza continuamente o computador, pode seleccionar um conjunto específico de opções de análise básicas para esta protecção e reservar um conjunto mais abrangente de opções de análise para a protecção manual e a pedido.

Neste capítulo

Configurar opções de análise em tempo real.....	42
Definir opções de análise manual.....	44
Utilizar opções das Protecções do Sistema	48
Utilizar listas de confiança	55

Configurar opções de análise em tempo real

Quando a protecção antivírus em tempo real é iniciada, o VirusScan utiliza um conjunto de opções predefinido para analisar ficheiros; no entanto, é possível alterar as predefinições, se necessário.

Para alterar as opções de análise em tempo real, é necessário decidir o que o VirusScan deve inspeccionar durante uma análise, bem como as localizações e os tipos de ficheiros a analisar. Por exemplo, é possível especificar se o VirusScan analisa a existência de vírus desconhecidos ou cookies que podem ser utilizados por Web sites para registar o seu comportamento, ou se analisa unidades de rede mapeadas para o computador ou apenas unidades locais. Também é possível especificar os tipos de ficheiros a analisar (todos os ficheiros ou apenas ficheiros de programa e documentos, uma vez que a maioria dos vírus é detectada nestes tipos de ficheiros).

Ao alterar as opções de análise em tempo real, deve igualmente especificar se é importante que o computador possua protecção de sobrecarga da memória intermédia. Memória intermédia é uma parte da memória que é utilizada temporariamente para conter informações do computador. As sobrecargas da memória intermédia podem ocorrer quando a quantidade de informações que os programas ou processos suspeitos armazenam numa memória intermédia excede a capacidade da mesma. Quando esta situação ocorre, o computador fica mais vulnerável a ataques de segurança.

Configurar opções de análise em tempo real

A configuração de opções de análise em tempo real permite personalizar o que o VirusScan deve procurar durante uma análise em tempo real, bem como as localizações e os tipos de ficheiros a analisar. As opções incluem a análise de vírus desconhecidos e cookies de controlo, bem como a protecção contra sobrecarga da memória intermédia. Também é possível configurar a análise em tempo real para inspeccionar unidades de rede mapeadas para o computador.

1 Abra o painel Análise em Tempo Real.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
 2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
 3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
 4. No painel de configuração Computador & Ficheiros, certifique-se de que a protecção antivírus está activada e, em seguida, clique em **Avançada**.
- 2 Especifique as opções de análise em tempo real e, em seguida, clique em **OK**.

Para...	Efectue o seguinte...
Detectar vírus desconhecidos e novas variantes de vírus conhecidos	Selecione a caixa de verificação Analisar vírus desconhecidos utilizando heurística .
Detectar cookies	Selecione a caixa de verificação Analisar e remover cookies de controlo .
Detectar vírus e outras ameaças potenciais em unidades ligadas à rede	Selecione a caixa de verificação Analisar unidades de rede .
Proteger o computador contra sobrecargas da memória intermédia	Selecione a caixa de verificação Activar protecção contra sobrecarga da memória intermédia .
Especificar os tipos de ficheiros a analisar	Clique em Todos os ficheiros (recomendado) ou Apenas programas e documentos .

Definir opções de análise manual

A protecção antivírus manual permite analisar ficheiros a pedido. Quando é iniciada uma análise manual, o VirusScan verifica a existência de vírus e outros itens potencialmente prejudiciais no computador através de um conjunto mais abrangente de opções de análise. Para alterar as opções de análise manual, é necessário decidir o que o VirusScan deve inspeccionar durante uma análise. Por exemplo, é possível especificar se o VirusScan procura vírus desconhecidos, programas potencialmente indesejados, tais como spyware ou adware, programas furtivos, tais como rootkits que podem conceder acesso não autorizado ao computador, e cookies que podem ser utilizados por Web sites para registar o seu comportamento. É igualmente necessário decidir quais os tipos de ficheiros a analisar. Por exemplo, é possível especificar se o VirusScan verifica todos os ficheiros ou apenas ficheiros de programa e documentos (uma vez que é nestes tipos de ficheiros que é detectada a maioria dos vírus). Também é possível especificar se os ficheiros de arquivo (por exemplo, ficheiros .zip) são incluídos na análise.

Por predefinição, o VirusScan examina todas as unidades e pastas do computador sempre que é executada uma análise manual; no entanto, é possível alterar as localizações predefinidas, se necessário. Por exemplo, é possível analisar apenas ficheiros de sistema críticos, itens do ambiente de trabalho ou itens na pasta Ficheiros de Programa. A menos que pretenda executar manualmente todas as análises, pode configurar análises agendadas regulares. As análises agendadas verificam sempre a totalidade do computador, utilizando as opções de análise predefinidas. Por predefinição, o VirusScan executa uma análise agendada uma vez por semana.

Se concluir que as velocidades de análise são lentas, pode desactivar a opção para utilizar recursos mínimos do computador, mas tenha em atenção que será dada uma prioridade mais elevada à protecção antivírus do que a outras tarefas.

Nota: Quando está a ver filmes, a jogar no computador ou a realizar qualquer outra actividade que ocupe a totalidade do ecrã, o VirusScan interrompe diversas tarefas, incluindo actualizações automáticas e análises manuais.

Definir opções de análise manual

A configuração de opções de análise manual permite personalizar o que o VirusScan deve procurar durante uma análise manual, bem como as localizações e os tipos de ficheiros a analisar. As opções incluem a análise de vírus desconhecidos, ficheiros de arquivo, spyware e programas potencialmente indesejados, cookies de controlo, rootkits e programas furtivos.

1 Abra o painel Análise Manual.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
4. No painel de configuração Computador & Ficheiros, certifique-se de que a protecção antivírus está activada e, em seguida, clique em **Avançada**.
5. Clique em **Análise Manual** no painel Protecção Antivírus.

2 Especifique as opções de análise manual e, em seguida, clique em **OK**.

Para...	Efectue o seguinte...
Detectar vírus desconhecidos e novas variantes de vírus conhecidos	Selecione a caixa de verificação Analisar vírus desconhecidos utilizando heurística .
Detectar e remover vírus existentes em ficheiros .zip e noutros ficheiros de arquivo	Selecione a caixa de verificação Analisar ficheiros .zip e outros ficheiros de arquivo .
Detectar spyware, adware e outros programas potencialmente indesejados	Selecione a caixa de verificação Analisar spyware e programas potencialmente indesejados .
Detectar cookies	Selecione a caixa de verificação Analisar e remover cookies de controlo .
Detectar rootkits e programas furtivos que podem alterar e explorar os ficheiros de sistema do Windows existentes	Selecione a caixa de verificação Analisar rootkits e outros programas furtivos .

Utilizar menos capacidade do processador para as análises e dar uma prioridade mais elevada a outras tarefas (tais como navegar na Web ou abrir documentos).	Selecione a caixa de verificação Analisar utilizando recursos mínimos do computador.
Especificar os tipos de ficheiros a analisar	Clique em Todos os ficheiros (recomendado) ou Apenas programas e documentos.

Definir localização de análise manual

A configuração da localização de análise manual permite determinar as localizações onde o VirusScan deve procurar vírus e outros itens prejudiciais durante uma análise manual. É possível analisar todos os ficheiros, pastas e unidades do computador ou restringir a análise a pastas e unidades específicas.

1 Abra o painel Análise Manual.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
4. No painel de configuração Computador & Ficheiros, certifique-se de que a protecção antivírus está activada e, em seguida, clique em **Avançada**.
5. Clique em **Análise Manual** no painel Protecção Antivírus.

2 Clique em **Localização Predefinida a Analisar**.

3 Especifique a localização para a análise manual e, em seguida, clique em **OK**.

Para...	Efectue o seguinte...
Analisar todos os ficheiros e pastas do computador	Selecione a caixa de verificação (O Meu) Computador .
Analisar ficheiros, pastas e unidades específicas no computador	Desmarque a caixa de verificação (O Meu) Computador e selecione uma ou mais pastas ou unidades.

Analisar ficheiros de sistema críticos	Desmarque a caixa de verificação (O Meu) Computador e seleccione a caixa de verificação Ficheiros de Sistema Críticos .
--	---

Agendar uma análise

As análises agendadas permitem analisar cuidadosamente o computador para detectar vírus e outras ameaças em qualquer dia e hora da semana. As análises agendadas verificam sempre a totalidade do computador, utilizando as opções de análise predefinidas. Por predefinição, o VirusScan executa uma análise agendada uma vez por semana. Se concluir que as velocidades de análise são lentas, pode desactivar a opção para utilizar recursos mínimos do computador, mas tenha em atenção que será dada uma prioridade mais elevada à protecção antivírus do que a outras tarefas.

1 Abra o painel Análise Agendada.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
4. No painel de configuração Computador & Ficheiros, certifique-se de que a protecção antivírus está activada e, em seguida, clique em **Avançada**.
5. Clique em **Análise Agendada** no painel Protecção Antivírus.

2 Seleccione **Activar análise agendada**.

3 Para reduzir a capacidade do processador utilizada normalmente para as análises, seleccione **Analisar utilizando recursos mínimos do computador**.

4 Seleccione um ou mais dias.

5 Especifique uma hora de início.

6 Clique em **OK**.

Sugestão: Para restaurar a agenda predefinida, clique em **Repor**.

Utilizar opções das Protecções do Sistema

As Protecções do Sistema monitorizam, registam, comunicam e gerem eventuais alterações não autorizadas efectuadas no registo do Windows ou em ficheiros de sistema críticos no computador. As alterações não autorizadas do registo e de ficheiros podem danificar o computador, comprometer a respectiva segurança e danificar ficheiros de sistema valiosos.

As alterações do registo e de ficheiros são frequentes e ocorrem com regularidade no computador. Uma vez que muitas dessas alterações são inofensivas, as predefinições das Protecções do Sistema são configuradas de modo a fornecer uma protecção fiável, inteligente e em tempo real contra alterações não autorizadas que podem representar danos potenciais significativos. Por exemplo, quando as Protecções do Sistema detectam alterações invulgares e que constituem uma ameaça significativa potencial, a actividade é imediatamente comunicada e registada. As alterações mais comuns que ainda representam alguns danos potenciais são apenas registadas. No entanto, a monitorização de alterações normais e de baixo risco está desactivada por predefinição. A tecnologia das Protecções do Sistema pode ser configurada para alargar o âmbito da protecção a qualquer ambiente.

Existem três tipos de Protecções do Sistema: Programa de Protecções do Sistema, Protecções do Sistema do Windows e Protecções do Sistema do Browser.

Programa de Protecções do Sistema

O Programa de Protecções do Sistema detecta eventuais alterações não autorizadas no registo do computador e noutros ficheiros críticos essenciais do Windows. Estes itens do registo e ficheiros importantes incluem instalações ActiveX, itens de arranque, hooks de execução da shell do Windows e dos carregamentos com atraso do objecto do serviço da shell. Através da monitorização destes itens, o Programa de Protecções do Sistema detém programas ActiveX suspeitos (transferidos da Internet), bem como spyware e programas potencialmente indesejados que podem ser iniciados automaticamente no arranque do Windows.

Protecções do Sistema do Windows

As Protecções do Sistema do Windows também detectam eventuais alterações não autorizadas no registo do computador e noutros ficheiros críticos essenciais do Windows. Estes itens do registo e ficheiros importantes incluem processadores de menus de contexto, appInit DLLs e o ficheiro hosts do Windows. Através da monitorização destes itens, a tecnologia das Protecções do Sistema do Windows ajuda a impedir que o computador envie ou receba informações pessoais ou não autorizadas através da Internet. De igual modo, ajuda a deter programas suspeitos que podem efectuar alterações indesejadas no aspecto e no comportamento de programas importantes para si e para a sua família.

Protecções do Sistema do Browser

À semelhança do Programa de Protecções do Sistema e das Protecções do Sistema do Windows, as Protecções do Sistema do Browser detectam eventuais alterações não autorizadas no registo do computador e noutros ficheiros críticos essenciais do Windows. No entanto, as Protecções do Sistema do Browser monitorizam as alterações de ficheiros e itens importantes do registo, tais como suplementos, URLs e zonas de segurança do Internet Explorer. Através da monitorização destes itens, a tecnologia das Protecções do Sistema do Browser ajuda a impedir actividades não autorizadas do browser, tais como o redireccionamento para Web sites suspeitos, alterações de definições e opções do browser sem o seu conhecimento e confiança não desejada em Web sites suspeitos.

Activar Protecções do Sistema

Active as Protecções do Sistema para detectar e alertar sobre eventuais alterações não autorizadas do registo do Windows e ficheiros no computador. As alterações não autorizadas do registo e de ficheiros podem danificar o computador, comprometer a respectiva segurança e danificar ficheiros de sistema valiosos.

- 1** Abra o painel de configuração Computador & Ficheiros.
Como?
 1. No painel esquerdo, clique em **Menu Avançado**.
 2. Clique em **Configurar**.
 3. No painel Configurar, clique em **Computador & Ficheiros**.
- 2** Em **Protecção do Sistema**, clique em **Ligado**.

Nota: Para desactivar a Protecção do Sistema, clique em **Desligado**.

Configurar opções das Protecções do Sistema

Utilize o painel das Protecções do Sistema para configurar as opções de protecção, início de sessão e alerta contra alterações não autorizadas do registo e de ficheiros associadas a ficheiros do Windows, programas e ao Internet Explorer. As alterações não autorizadas do registo e de ficheiros podem danificar o computador, comprometer a respectiva segurança e danificar ficheiros de sistema valiosos.

1 Abra o painel das Protecções do Sistema.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
4. No painel de configuração Computador & Ficheiros, certifique-se de que a Protecção do Sistema está activada e, em seguida, clique em **Avançada**.

2 Seleccione um tipo de Protecção do Sistema na lista.

- **Programa de Protecções do Sistema**
- **Protecções do Sistema do Windows**
- **Protecções do Sistema do Browser**

3 Em **Quero**, proceda de um dos seguintes modos:

- Para detectar, registar e comunicar alterações não autorizadas do registo e de ficheiros associadas ao Programa de Protecções do Sistema e às Protecções do Sistema do Windows e dos Browsers, clique em **Mostrar alertas**.
- Para detectar e registar alterações não autorizadas do registo e de ficheiros associadas ao Programa de Protecções do Sistema e às Protecções do Sistema do Windows e dos Browsers, clique em **Registar apenas alterações**.
- Para desactivar a detecção de alterações não autorizadas do registo e de ficheiros associadas ao Programa de Protecções do Sistema e às Protecções do Sistema do Windows e dos Browsers, clique em **Desactivar a Protecção do Sistema**.

Nota: Para obter mais informações sobre os tipos de Protecções do Sistema, consulte a secção **Acerca dos tipos de Protecções do Sistema** (página 51).

Acerca dos tipos de Protecções do Sistema

As Protecções do Sistema detectam eventuais alterações não autorizadas no registo do computador e noutros ficheiros críticos essenciais do Windows. Existem três tipos de Protecções do Sistema: Programa de Protecções do Sistema, Protecções do Sistema do Windows e Protecções do Sistema do Browser

Programa de Protecções do Sistema

A tecnologia do Programa de Protecções do Sistema detém programas ActiveX suspeitos (transferidos da Internet), bem como spyware e programas potencialmente indesejados que podem ser iniciados automaticamente no arranque do Windows.

Protecção do Sistema	Detecta...
Instalações ActiveX	Alterações não autorizadas ao registo de instalações ActiveX que podem danificar o computador, comprometer a respectiva segurança e danificar ficheiros de sistema valiosos.
Itens de Arranque	Spyware, adware e outros programas potencialmente indesejados que podem instalar alterações a ficheiros dos itens de arranque, permitindo a execução de programas suspeitos quando o computador é iniciado.
Hooks de Execução da Shell do Windows	Spyware, adware e outros programas potencialmente indesejados que podem instalar hooks de execução da shell do Windows para evitar que os programas de segurança sejam executados correctamente.
Carregamento com Atraso do Objecto do Serviço da Shell	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo do carregamento com atraso do objecto do serviço da shell, permitindo a execução de ficheiros prejudiciais quando o computador é iniciado.

Protecções do Sistema do Windows

A tecnologia das Protecções do Sistema do Windows ajuda a impedir que o computador envie ou receba informações pessoais ou não autorizadas através da Internet. De igual modo, ajuda a deter programas suspeitos que podem efectuar alterações indesejadas no aspecto e no comportamento de programas importantes para si e para a sua família.

Protecção do Sistema	Detecta...
Processadores de Menus de Contexto	Alterações não autorizadas ao registo das rotinas de tratamento de menus de contexto do Windows que podem afectar o aspecto e o comportamento dos menus do Windows. Os menus de contexto permitem executar acções no computador, tais como clicar com o botão direito do rato em ficheiros.
AppInit DLLs	Alterações não autorizadas ao registo dos AppInit DLLs do Windows que podem permitir a execução de ficheiros potencialmente prejudiciais quando o computador é iniciado.
Ficheiro Hosts do Windows	Spyware, adware e programas potencialmente indesejados que podem efectuar alterações não autorizadas ao ficheiro hosts do Windows, permitindo o redireccionamento do browser para Web sites suspeitos e o bloqueio de actualizações de software.
Shell do Início de Sessão	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo da shell de Início de Sessão do Windows, permitindo a substituição do Explorador do Windows por outros programas.
Início de Sessão UserInit	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo da aplicação user init de Início de Sessão do Windows, permitindo a execução de programas suspeitos quando o utilizador inicia sessão no Windows.
Protocolos do Windows	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo dos protocolos do Windows, afectando a forma como o computador envia e recebe informação através da Internet.
Fornecedores de Serviços em Camadas do Winsock	Spyware, adware e outros programas potencialmente indesejados que podem instalar alterações ao registo dos Fornecedores de Serviços em Camadas (LSPs) do Winsock para interceptar e alterar informações enviadas e recebidas através da Internet.

Comandos Open da Shell do Windows	Alterações não autorizadas aos Open Commands da shell do Windows que podem permitir a execução de worms e de outros programas prejudiciais no computador.
Agendador de Tarefas Partilhado	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações a ficheiros e ao registo do agendador de tarefas partilhado, permitindo a execução de ficheiros potencialmente prejudiciais quando o computador é iniciado.
Windows Messenger Service	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo do serviço Windows Messenger, permitindo a existência de publicidade não solicitada e programas executados remotamente no computador.
Ficheiro Win.ini do Windows	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao ficheiro Win.ini, permitindo a execução de programas suspeitos quando o computador é iniciado.

Protecções do Sistema do Browser

A tecnologia das Protecções do Sistema do Browser ajuda a impedir actividades não autorizadas do browser, tais como o redireccionamento para Web sites suspeitos, alterações de definições e opções do browser sem o seu conhecimento e confiança não desejada em Web sites suspeitos.

Protecção do Sistema	Detecta...
Objectos de Auxiliares do Browser	Spyware, adware e outros programas potencialmente indesejados que podem utilizar os objectos auxiliares do browser para rastrear a navegação na Web e mostrar publicidade não solicitada.
Barras do Internet Explorer	Alterações não autorizadas ao registo dos programas da Barra do Internet Explorer, tais como Procurar ou Favoritos, que podem afectar o aspecto e o comportamento do Internet Explorer.
Suplementos do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem instalar suplementos do Internet Explorer para rastrear a navegação na Web e mostrar publicidade não solicitada.
Browser da Shell do Internet Explorer	Alterações não autorizadas ao registo do browser da shell do Internet Explorer que podem afectar o aspecto e o comportamento do Web browser.

Web Browser Internet Explorer	Alterações não autorizadas ao registo do Web browser Internet Explorer que podem afectar o aspecto e o comportamento do browser.
Hooks de Procura de URL do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo dos hooks de procura de URLs do Internet Explorer, permitindo o redireccionamento do browser para Web sites suspeitos ao efectuar procuras na Web.
URLs do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo dos URLs do Internet Explorer, afectando as definições do browser.
Restrições do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo das restrições do Internet Explorer, afectando as definições e as opções do browser.
Zonas de Segurança do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo das zonas de segurança do Internet Explorer, permitindo a execução de ficheiros potencialmente prejudiciais quando o computador é iniciado.
Sites Fidedignos do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo dos sites fidedignos do Internet Explorer, permitindo que o browser passe a confiar em Web sites suspeitos.
Política do Internet Explorer	Spyware, adware e outros programas potencialmente indesejados que podem efectuar alterações ao registo das políticas do Internet Explorer, afectando o aspecto e o comportamento do browser.

Utilizar listas de confiança

Se o VirusScan detectar uma alteração ao registo ou ficheiro (Protecção do Sistema), programa ou sobrecarga da memória intermédia, solicita-lhe que confie ou remova o item detectado. Se confiar no item e indicar que não pretende receber notificações futuras sobre a respectiva actividade, o item é adicionado a uma lista de confiança e o VirusScan deixa de o detectar ou de notificar sobre a respectiva actividade. É possível bloquear a actividade de um item que tenha sido adicionado a uma lista de confiança. O bloqueio impede que o item seja executado ou que efectue alterações ao computador sem o notificar de todas as tentativas. Também é possível remover um item de uma lista de confiança. A remoção permite ao VirusScan detectar a actividade do item novamente.

Gerir listas de confiança

Utilize o painel Listas de Confiança para confiar ou bloquear itens que tenham sido detectados e confiados anteriormente. Também pode remover um item de uma lista de confiança para que o VirusScan o detecte novamente.

1 Abra o painel Listas de Confiança.

Como?

1. Em **Tarefas Comuns**, clique em **Página Inicial**.
2. No painel Página Inicial do SecurityCenter, clique em **Computador & Ficheiros**.
3. Na área de informação Computador & Ficheiros, clique em **Configurar**.
4. No painel de configuração Computador & Ficheiros, certifique-se de que a protecção antivírus está activada e, em seguida, clique em **Avançada**.
5. Clique em **Listas de Confiança** no painel Protecção Antivírus.

2 Seccione um dos seguintes tipos de listas de confiança:

- **Programa de Protecções do Sistema**
- **Protecções do Sistema do Windows**
- **Protecções do Sistema do Browser**
- **Programas de Confiança**
- **Sobrecargas da Memória Intermédia de Confiança**

3 Em **Quero**, proceda de um dos seguintes modos:

- Para permitir que o item detectado efectue alterações ao registo do Windows ou a ficheiros do sistema críticos do computador sem o notificar, clique em **Confiar**.

- Para impedir que o item detectado efectue alterações ao registo do Windows ou a ficheiros do sistema críticos do computador sem o notificar, clique em **Bloquear**.
- Para remover o item detectado das listas de confiança, clique em **Remover**.

4 Clique em **OK**.

Nota: Para obter mais informações sobre os tipos de listas de confiança, consulte a secção **Acerca dos tipos de listas de confiança** (página 56).

Acerca dos tipos de listas de confiança

As Protecções do Sistema no painel Listas de Confiança representam alterações não autorizadas do registo e de ficheiros detectadas anteriormente pelo VirusScan, mas que o utilizador optou por permitir a partir de um alerta ou do painel Resultados da Análise. Existem cinco tipos de listas de confiança que podem ser geridos no painel Listas de Confiança: Programa de Protecções do Sistema, Protecções do Sistema do Windows, Protecções do Sistema do Browser, Programas de Confiança e Sobrecargas da Memória Intermédia de Confiança.

Opção	Descrição
Programa de Protecções do Sistema	O Programa de Protecções do Sistema no painel Listas de Confiança representa alterações não autorizadas do registo e de ficheiros detectadas anteriormente pelo VirusScan, mas que o utilizador optou por permitir a partir de um alerta ou do painel Resultados da Análise. O Programa de Protecções do Sistema detecta alterações não autorizadas do registo e de ficheiros associados a instalações ActiveX, itens de arranque, hooks de execução da shell do Windows e actividade de carregamento com atraso do objecto do serviço da shell. Estes tipos de alterações não autorizadas do registo e de ficheiros podem danificar o computador, comprometer a respectiva segurança e danificar ficheiros de sistema valiosos.

Protecções do Sistema do Windows	As Protecções do Sistema do Windows no painel Listas de Confiança representam alterações não autorizadas do registo e de ficheiros detectadas anteriormente pelo VirusScan, mas que o utilizador optou por permitir a partir de um alerta ou do painel Resultados da Análise. As Protecções do Sistema do Windows detectam alterações não autorizadas do registo e de ficheiros associadas a processadores de menus de contexto, appInit DLLs, o ficheiro hosts do Windows, a shell de início de sessão do Windows e Fornecedores de Serviços em Camadas (LSPs) do Winsock, entre outros. Estes tipos de alterações não autorizadas do registo e de ficheiros podem afectar a forma como o computador envia e recebe informação através da Internet, alterar o aspecto e o comportamento de programas e permitir a execução de programas suspeitos no computador.
Protecções do Sistema do Browser	As Protecções do Sistema do Browser no painel Listas de Confiança representam alterações não autorizadas do registo e de ficheiros detectadas anteriormente pelo VirusScan, mas que o utilizador optou por permitir a partir de um alerta ou do painel Resultados da Análise. As Protecções do Sistema do Browser detectam alterações não autorizadas do registo e outros comportamentos indesejados associados a objectos auxiliares do Browser, suplementos, URLs e zonas de segurança do Internet Explorer, entre outros. Estes tipos de alterações não autorizadas do registo podem resultar em actividades indesejadas do browser, tais como o redireccionamento para Web sites suspeitos, alterações de definições e opções do browser e confiança em Web sites suspeitos.
Programas de Confiança	Os programas de confiança são programas potencialmente indesejados detectados anteriormente pelo VirusScan, mas que o utilizador optou por confiar a partir de um alerta ou do painel Resultados da Análise.
Sobrecargas da Memória Intermédia de Confiança	As sobrecargas da memória intermédia de confiança representam actividades indesejadas detectadas anteriormente pelo VirusScan, mas que o utilizador optou por confiar a partir de um alerta ou do painel Resultados da Análise. As sobrecargas da memória intermédia podem danificar o computador e os respectivos ficheiros. As sobrecargas da memória intermédia ocorrem quando a quantidade de informações que os programas ou processos suspeitos armazenam numa memória intermédia excede a capacidade da mesma.

CAPÍTULO 11

Analisar o computador

Quando o SecurityCenter é iniciado pela primeira vez, a protecção antivírus em tempo real do VirusScan começa a proteger o computador contra vírus, cavalos de Tróia e outras ameaças de segurança potencialmente prejudiciais. A menos que a protecção antivírus em tempo real seja desactivada, o VirusScan utiliza as opções de análise em tempo real configuradas pelo utilizador para monitorizar continuamente a existência de actividades de vírus no computador, analisando os ficheiros sempre que são acedidos pelo utilizador ou pelo computador. Para ter a certeza de que o computador está protegido contra as mais recentes ameaças de segurança, active a protecção antivírus em tempo real e agende análises manuais mais completas e regulares. Para obter mais informações sobre a configuração de opções de análise manual e em tempo real, consulte a secção **Configurar a protecção antivírus** (página 41).

O VirusScan fornece um conjunto de opções de análise mais detalhado para protecção antivírus manual, permitindo a execução periódica de análises mais completas. A partir do SecurityCenter, é possível executar análises manuais sobre localizações específicas de acordo com uma agenda. No entanto, também pode executar análises manuais directamente no Explorador do Windows enquanto trabalha. A análise no SecurityCenter oferece a vantagem de alterar as opções de análise instantaneamente. No entanto, a análise a partir do Explorador do Windows oferece uma abordagem adequada à segurança do computador.

Independentemente de executar a análise manual a partir do SecurityCenter ou do Explorador do Windows, pode ver os resultados da análise depois de terminada. A visualização dos resultados de uma análise permite determinar se o VirusScan detectou, reparou ou colocou em quarentena vírus, cavalos de Tróia, spyware, adware, cookies e outros programas potencialmente indesejados. Os resultados de uma análise podem ser apresentados de diferentes formas. Por exemplo, é possível ver um resumo simples dos resultados da análise ou informações detalhadas, tais como o tipo e o estado da infecção. Também é possível ver estatísticas gerais de análise e detecção.

Neste capítulo

Analisar o computador	60
Ver resultados da análise	60

Analisar o computador

É possível executar uma análise manual a partir do menu Avançado ou do menu Básico no SecurityCenter. Se a análise for executada a partir do menu Avançado, é possível confirmar as opções da análise manual antes da execução. Se a análise for executada a partir do menu Básico, o VirusScan inicia imediatamente a análise utilizando as opções de análise existentes. Também é possível executar uma análise no Explorador do Windows utilizando as opções de análise existentes.

- Proceda de um dos seguintes modos:

Analisar no SecurityCenter

Para...	Efectue o seguinte...
Analisar utilizando as definições existentes	Clique em Analisar no menu Básico.
Analisar utilizando definições alteradas	Clique em Analisar no menu Avançado, seleccione as localizações a analisar, seleccione as opções de análise e, em seguida, clique em Analisar Agora .

Analisar no Explorador do Windows

1. Abra o Explorador do Windows.
2. Clique com o botão direito num ficheiro, pasta ou unidade e, em seguida, clique em **Analisar**.

Nota: Os resultados da análise são apresentados no alerta de Análise concluída. Os resultados incluem o número de itens analisados, detectados, reparados, colocados em quarentena e removidos. Clique em **Ver detalhes da análise** para saber mais acerca dos resultados da análise ou trabalhar com itens infectados.

Ver resultados da análise

Depois de uma análise manual terminar, visualize os resultados para determinar o que a análise encontrou e analisar o estado de protecção actual do computador. Os resultados da análise indicam se o VirusScan detectou, reparou ou colocou em quarentena vírus, cavalos de Tróia, spyware, adware, cookies e outros programas potencialmente indesejados.

- Nos menus Básico ou Avançado, clique em **Analisar** e, em seguida, proceda de um dos seguintes modos:

Para...	Efectue o seguinte...
Ver os resultados da análise no alerta	Veja os resultados da análise no alerta de Análise concluída.

Ver mais informações sobre os resultados da análise	Clique em Ver detalhes da análise no alerta de Análise concluída.
Ver um breve resumo dos resultados da análise	Aponte para o Ícone de análise concluída na área de notificação da barra de tarefas.
Ver estatísticas de análise e detecção	Faça duplo clique no ícone Análise concluída na área de notificação da barra de tarefas.
Ver detalhes sobre itens detectados e tipo e estado das infecções.	Faça duplo clique no ícone Análise concluída na área de notificação da barra de tarefas e, em seguida, clique em Ver Resultados no Progresso da Análise: painel Análise Manual.

CAPÍTULO 12

Utilizar os resultados da análise

Se o VirusScan detectar uma ameaça de segurança durante a execução de uma análise manual ou em tempo real, tentará processá-la automaticamente de acordo com o tipo de ameaça. Por exemplo, se o VirusScan detectar um vírus, um cavalo de Tróia ou um cookie de controlo no computador, tenta limpar o ficheiro infectado. Se não conseguir limpar o ficheiro, o VirusScan coloca-o em quarentena.

No que respeita a algumas ameaças de segurança, o VirusScan poderá não conseguir limpar ou colocar em quarentena um ficheiro com êxito. Nesse caso, o VirusScan solicita ao utilizador que processe a ameaça. É possível executar acções diferentes, dependendo do tipo de ameaça. Por exemplo, se for detectado um vírus num ficheiro e o VirusScan não conseguir limpar ou colocar em quarentena o ficheiro com êxito, nega o acesso posterior ao ficheiro. Se forem detectados cookies de controlo e o VirusScan não conseguir limpar ou colocar em quarentena os cookies com êxito, o utilizador pode decidir se confia ou remove os cookies. Se forem detectados programas potencialmente indesejados, o VirusScan não executa nenhuma acção automática, permitindo ao utilizador decidir se confia ou coloca em quarentena o programa.

Quando o VirusScan coloca itens em quarentena, encripta-os e isola-os numa pasta para impedir que os ficheiros, programas ou cookies possam danificar o computador. É possível restaurar ou remover os itens em quarentena. Na maioria dos casos, pode eliminar um cookie colocado em quarentena sem produzir qualquer impacto no sistema; no entanto, se o VirusScan tiver colocado em quarentena um programa que o utilizador reconhece e utiliza, pondere o seu restauro.

Neste capítulo

Tratar vírus e cavalos de Tróia	64
Tratar programas potencialmente indesejados.....	64
Tratar ficheiros em quarentena	65
Tratar programas e cookies em quarentena	65

Tratar vírus e cavalos de Tróia

Se o VirusScan detectar um vírus ou um cavalo de Tróia num ficheiro do computador durante uma análise manual ou em tempo real, tenta limpar o ficheiro. Se não conseguir limpar o ficheiro, o VirusScan tenta colocá-lo em quarentena. Se esta acção também falhar, o acesso ao ficheiro é negado (apenas em análises em tempo real).

1 Abra o painel Resultados da Análise.

Como?

1. Faça duplo clique no ícone **Análise concluída** na área de notificação, na parte mais à direita da barra de tarefas.
2. No painel Progresso da Análise: Análise Manual, clique em **Ver Resultados**.

2 Na lista de resultados da análise, clique em **Vírus e Cavalos de Tróia**.

Nota: Para tratar os ficheiros colocados em quarentena pelo VirusScan, consulte a secção **Tratar ficheiros em quarentena** (página 65).

Tratar programas potencialmente indesejados

Se o VirusScan detectar um programa potencialmente indesejado no computador durante uma análise manual ou em tempo real, o utilizador pode confiar ou remover o programa. A remoção do programa potencialmente indesejado não o elimina realmente do sistema. Em vez disso, coloca o programa em quarentena para evitar que danifique o computador ou ficheiros.

1 Abra o painel Resultados da Análise.

Como?

1. Faça duplo clique no ícone **Análise concluída** na área de notificação, na parte mais à direita da barra de tarefas.
2. No painel Progresso da Análise: Análise Manual, clique em **Ver Resultados**.

2 Na lista de resultados da análise, clique em **Programas Potencialmente Indesejados**.

3 Seccione um programa potencialmente indesejado.

4 Em **Quero**, clique em **Remover** ou em **Confiar**.

5 Confirme a opção seleccionada.

Tratar ficheiros em quarentena

Quando o VirusScan coloca ficheiros infectados em quarentena, encripta-os e move-os para uma pasta para impedir que danifiquem o computador. Depois, é possível restaurar ou remover os itens em quarentena.

- 1 Abra o painel Ficheiros em Quarentena.
Como?
 1. No painel esquerdo, clique em **Menu Avançado**.
 2. Clique em **Restaurar**.
 3. Clique em **Ficheiros**.
- 2 Seleccione um ficheiro em quarentena.
- 3 Proceda de um dos seguintes modos:
 - Para reparar um ficheiro infectado e devolvê-lo à sua localização original no computador, clique em **Restaurar**.
 - Para remover o ficheiro infectado do computador, clique em **Remover**.
- 4 Clique em **Sim** para confirmar a opção seleccionada.

Sugestão: É possível restaurar ou remover vários ficheiros ao mesmo tempo.

Tratar programas e cookies em quarentena

Quando o VirusScan coloca programas potencialmente indesejados ou cookies de controlo em quarentena, encripta-os e move-os para uma pasta protegida para impedir que danifiquem o computador. Depois, é possível restaurar ou remover os itens em quarentena. Na maioria dos casos, é possível eliminar um item em quarentena sem provocar impacto no sistema.

- 1 Abra o painel Programas e Cookies de Controlo em Quarentena.
Como?
 1. No painel esquerdo, clique em **Menu Avançado**.
 2. Clique em **Restaurar**.
 3. Clique em **Programas e Cookies**.
- 2 Seleccione um programa ou um cookie em quarentena.
- 3 Proceda de um dos seguintes modos:
 - Para reparar um ficheiro infectado e devolvê-lo à sua localização original no computador, clique em **Restaurar**.
 - Para remover o ficheiro infectado do computador, clique em **Remover**.

4 Clique em **Sim** para confirmar a operação.

Sugestão: É possível restaurar ou remover vários programas e cookies ao mesmo tempo.

CAPÍTULO 13

McAfee QuickClean

O QuickClean melhora o desempenho do computador através da eliminação de ficheiros desnecessários no computador. Esvazia a Reciclagem e elimina ficheiros temporários, atalhos, fragmentos perdidos de ficheiros, ficheiros de registo, ficheiros em cache, cookies, ficheiros do histórico do browser, correio electrónico enviado e recebido, ficheiros usados recentemente, ficheiros ActiveX e ficheiros de ponto de restauro do sistema. O QuickClean protege igualmente a sua privacidade através da utilização do componente McAfee Shredder para eliminar, de forma permanente e segura, itens que possam conter informações pessoais e confidenciais, tais como o seu nome e endereço. Para informações acerca da destruição de ficheiros, consulte o McAfee Shredder.

O Desfragmentador de Disco dispõe os ficheiros e as pastas no computador de modo a assegurar que não fiquem dispersos (ou seja, fragmentados) quando são guardados no disco rígido do computador. Através da desfragmentação periódica do disco rígido, é possível assegurar que esses ficheiros e pastas fragmentados são consolidados para rápida obtenção posterior.

Se não pretender efectuar manualmente a manutenção do computador, pode programar o QuickClean e o Desfragmentador de Disco para serem executados automaticamente, como tarefas independentes, com qualquer frequência.

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades do QuickClean.....	68
Limpar o computador.....	69
Desfragmentar o computador.....	73
Programar uma tarefa.....	74

Funcionalidades do QuickClean

O QuickClean fornece várias limpezas que eliminam ficheiros desnecessários de forma segura e eficaz. Através da eliminação desses ficheiros, é possível aumentar o espaço livre no disco rígido do computador e melhorar o seu desempenho.

Limpar o computador

O QuickClean elimina ficheiros desnecessários no computador. Esvazia a Reciclagem e elimina ficheiros temporários, atalhos, fragmentos perdidos de ficheiros, ficheiros de registo, ficheiros em cache, cookies, ficheiros do histórico do browser, correio electrónico enviado e recebido, ficheiros utilizados recentemente, ficheiros ActiveX e ficheiros de ponto de restauro do sistema. O QuickClean elimina estes itens sem afectar outras informações essenciais.

É possível utilizar qualquer uma das limpezas do QuickClean para eliminar ficheiros desnecessários do computador. A tabela seguinte descreve as limpezas do QuickClean:

Nome	Função
Limpeza da Reciclagem	Elimina ficheiros na Reciclagem.
Limpeza de Ficheiros Temporários	Elimina ficheiros armazenados em pastas temporárias.
Limpeza de Atalhos	Elimina atalhos quebrados e atalhos que não têm programas associados.
Limpeza de Fragmentos Perdidos de Ficheiros	Elimina fragmentos perdidos de ficheiros no computador.
Limpeza do Registo	Elimina informações de registo do Windows® relativas a programas que já não existem no computador. O registo é uma base de dados na qual o Windows armazena a sua informação de configuração. O registo contém os perfis de cada utilizador do computador e informações acerca do hardware do sistema, dos programas instalados e de definições de propriedade. O Windows consulta continuamente estas informações durante o seu funcionamento.
Limpeza da Cache	Elimina ficheiros de cache que se vão acumulando quando navega em páginas Web. Esses ficheiros são normalmente armazenados como ficheiros temporários numa pasta cache. Uma pasta cache é uma área de armazenamento temporário no computador. Para aumentar a velocidade e a eficiência da navegação na Web, o browser pode obter uma página Web da cache (em lugar de um servidor remoto) na próxima vez que a visualizar.

Limpeza de Cookies	Elimina cookies. Estes ficheiros são normalmente armazenados como ficheiros temporários. Um cookie é um pequeno ficheiro que contém informações, incluindo normalmente um nome de utilizador e a data e hora actuais, armazenadas no computador de uma pessoa que navega na Web. Os cookies são utilizados principalmente por Web sites para identificar utilizadores que tenham efectuado previamente um registo ou visitado o site; no entanto, também podem constituir uma fonte de informação para hackers.
Limpeza do Histórico do Browser	Elimina o histórico do browser.
Limpeza do Correio Electrónico do Outlook Express e do Outlook (itens enviados e eliminados)	Elimina o correio electrónico enviado e eliminado do Outlook® e do Outlook Express.
Limpeza de Ficheiros Utilizados Recentemente	Elimina ficheiros utilizados recentemente que tenham sido criados com qualquer um dos seguintes programas: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
Limpeza de ActiveX	Elimina controlos ActiveX. O ActiveX é um componente de software utilizado por programas ou páginas Web para adicionar funcionalidades que actuam dissimuladas e aparecem como uma parte normal do programa ou da página Web. A maioria dos controlos ActiveX são inofensivos; no entanto, alguns podem capturar informações do computador.

Limpeza de Pontos de Restauo do Sistema	Elimina pontos de restauro do sistema antigos (excepto o mais recente) do computador. Os pontos de restauro do sistema são criados pelo Windows para assinalar alterações efectuadas no computador a fim de que seja possível repor um estado anterior se ocorrerem problemas.
---	--

Limpar o computador

É possível utilizar qualquer uma das limpezas do QuickClean para eliminar ficheiros desnecessários do computador. Quando terminar, em **Resumo do QuickClean**, é possível ver a quantidade de espaço de disco recuperada após a limpeza, o número de ficheiros eliminados e a data e a hora em que foi executada a última operação do QuickClean no computador.

- 1 No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
- 2 Em **McAfee QuickClean**, clique em **Iniciar**.
- 3 Efectue um dos seguintes procedimentos:
 - Clique em **Seguinte** para aceitar as limpezas predefinidas na lista.
 - Seleccione ou desmarque as limpezas que considerar adequadas e, em seguida, clique em **Seguinte**. Se seleccionar a Limpeza de Ficheiros Utilizados Recentemente, pode clicar em **Propriedades** para seleccionar ou limpar os ficheiros que foram criados recentemente com os programas da lista e, em seguida, clicar em **OK**.
 - Clique em **Restaurar Predefinições** para repor as limpezas predefinidas e, em seguida, clique em **Seguinte**.
- 4 Depois de executada a análise, clique em **Seguinte**.
- 5 Clique em **Seguinte** para confirmar a eliminação dos ficheiros.
- 6 Efectue um dos seguintes procedimentos:
 - Clique em **Seguinte** para aceitar a opção predefinida **Não, quero eliminar os ficheiros utilizando o método padrão de eliminação do Windows**.
 - Clique em **Sim, pretendo apagar os ficheiros com segurança utilizando o Shredder**, especifique o número de passagens, até 10, e clique em **Seguinte**. A destruição de ficheiros pode tornar-se um processo demorado se existir uma grande quantidade de informação a apagar.

7 Se existirem ficheiros ou itens bloqueados durante a limpeza, poderá ser-lhe solicitado que reinicie o computador. Clique em **OK** para fechar o pedido.

8 Clique em **Concluir**.

Nota: Os ficheiros eliminados com o Shredder não podem ser recuperados. Para informações acerca da destruição de ficheiros, consulte o McAfee Shredder.

Desfragmentar o computador

O Desfragmentador de Disco dispõe os ficheiros e as pastas no computador de modo a que não fiquem dispersos (ou seja, fragmentados) quando são guardados no disco rígido do computador. Através da desfragmentação periódica do disco rígido, é possível assegurar que esses ficheiros e pastas fragmentados são consolidados para rápida obtenção posterior.

Desfragmentar o computador

É possível desfragmentar o computador para melhorar o acesso e a obtenção de ficheiros e pastas.

- 1 No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
- 2 Em **Desfragmentador de Disco**, clique em **Analisar**.
- 3 Siga as instruções indicadas no ecrã.

Nota: Para obter mais informações acerca do Desfragmentador de Disco, consulte a Ajuda do Windows.

Programar uma tarefa

O Programador de Tarefas automatiza a frequência com que o QuickClean ou o Desfragmentador de Disco são executados no computador. Por exemplo, é possível programar uma tarefa do QuickClean para esvaziar a Reciclagem todos os Domingos, às 21:00 ou uma tarefa do Desfragmentador de Disco para desfragmentar o disco rígido do computador no último dia de cada mês. É possível criar, modificar ou eliminar uma tarefa em qualquer altura. É necessário ter sessão iniciada no computador para que uma tarefa programada seja executada. Se uma tarefa não for executada por qualquer motivo, será reprogramada para cinco minutos depois de ter iniciado sessão novamente.

Programar uma tarefa do QuickClean

É possível programar uma tarefa do QuickClean para limpar automaticamente o computador utilizando uma ou mais limpezas. Quando terminar, em **Resumo do QuickClean**, é possível ver a data e a hora em que a tarefa será executada novamente.

- 1 Abra o painel Programador de Tarefas.
Como?
 1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
 2. Em **Programador de tarefas**, clique em **Iniciar**.
- 2 Na lista **Selecione a operação a programar**, clique em **McAfee QuickClean**.
- 3 Digite um nome para a tarefa na caixa **Nome da tarefa** e clique em **Criar**.
- 4 Efectue um dos seguintes procedimentos:
 - Clique em **Seguinte** para aceitar as limpezas da lista.
 - Selecione ou desmarque as limpezas que considerar adequadas e, em seguida, clique em **Seguinte**. Se seleccionar a Limpeza de Ficheiros Utilizados Recentemente, pode clicar em **Propriedades** para seleccionar ou limpar os ficheiros que foram criados recentemente com os programas da lista e, em seguida, clicar em **OK**.
 - Clique em **Restaurar Predefinições** para repor as limpezas predefinidas e, em seguida, clique em **Seguinte**.
- 5 Efectue um dos seguintes procedimentos:
 - Clique em **Programar** para aceitar a opção predefinida **Não, quero eliminar os ficheiros utilizando o método padrão de eliminação do Windows**.

- Clique em **Sim, pretendo apagar os ficheiros com segurança utilizando o Shredder**, especifique o número de passagens, até 10, e clique em **Programar**.
- 6 Na caixa de diálogo **Programar**, seleccione a frequência de execução da tarefa e clique em **OK**.
- 7 Se tiver alterado as propriedades da Limpeza de Ficheiros Utilizados Recentemente, poderá ser-lhe solicitado que reinicie o computador. Clique em **OK** para fechar o pedido.
- 8 Clique em **Concluir**.

Nota: Os ficheiros eliminados com o Shredder não podem ser recuperados. Para informações acerca da destruição de ficheiros, consulte o McAfee Shredder.

Modificar uma tarefa do QuickClean

É possível modificar uma tarefa programada do QuickClean para alterar as limpezas utilizadas ou a frequência com que a mesma é executada no computador. Quando terminar, em **Resumo do QuickClean**, é possível ver a data e a hora em que a tarefa será executada novamente.

- 1 Abra o painel Programador de Tarefas.
Como?
 1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
 2. Em **Programador de tarefas**, clique em **Iniciar**.
- 2 Na lista **Selecione a operação a programar**, clique em **McAfee QuickClean**.
- 3 Selecione a tarefa na lista **Selecione uma tarefa existente** e clique em **Modificar**.
- 4 Efectue um dos seguintes procedimentos:
 - Clique em **Seguinte** para aceitar as limpezas seleccionadas para a tarefa.
 - Selecione ou desmarque as limpezas que considerar adequadas e, em seguida, clique em **Seguinte**. Se seleccionar a Limpeza de Ficheiros Utilizados Recentemente, clique em **Propriedades** para seleccionar ou limpar os ficheiros que foram criados recentemente com os programas da lista e, em seguida, clique em **OK**.
 - Clique em **Restaurar Predefinições** para repor as limpezas predefinidas e, em seguida, clique em **Seguinte**.

- 5 Efectue um dos seguintes procedimentos:
 - Clique em **Programar** para aceitar a opção predefinida **Não, quero eliminar os ficheiros utilizando o método padrão de eliminação do Windows**.
 - Clique em **Sim, pretendo apagar os ficheiros com segurança utilizando o Shredder**, especifique o número de passagens, até 10, e clique em **Programar**.
- 6 Na caixa de diálogo **Programar**, seleccione a frequência de execução da tarefa e clique em **OK**.
- 7 Se tiver alterado as propriedades da Limpeza de Ficheiros Utilizados Recentemente, poderá ser-lhe solicitado que reinicie o computador. Clique em **OK** para fechar o pedido.
- 8 Clique em **Concluir**.

Nota: Os ficheiros eliminados com o Shredder não podem ser recuperados. Para informações acerca da destruição de ficheiros, consulte o McAfee Shredder.

Eliminar uma tarefa do QuickClean

É possível eliminar uma tarefa programada do QuickClean que já não pretende que seja executada automaticamente.

- 1 Abra o painel Programador de Tarefas.

Como?

 1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
 2. Em **Programador de tarefas**, clique em **Iniciar**.
- 2 Na lista **Selecione a operação a programar**, clique em **McAfee QuickClean**.
- 3 Selecione a tarefa na lista **Selecione uma tarefa existente**.
- 4 Clique em **Eliminar** e, em seguida, clique em **Sim** para confirmar a eliminação.
- 5 Clique em **Concluir**.

Programar uma tarefa do Desfragmentador de Disco

É possível programar uma tarefa do Desfragmentador de Disco para programar a frequência com que o disco rígido do computador é desfragmentado automaticamente. Quando terminar, em **Desfragmentador de Disco**, é possível ver a data e a hora em que a tarefa será executada novamente.

- 1 Abra o painel Programador de Tarefas.
Como?
 1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
 2. Em **Programador de tarefas**, clique em **Iniciar**.
- 2 Na lista **Selecione a operação a programar**, clique em **Desfragmentador de Disco**.
- 3 Digite um nome para a tarefa na caixa **Nome da tarefa** e clique em **Criar**.
- 4 Efectue um dos seguintes procedimentos:
 - Clique em **Programar** para aceitar a opção predefinida **Executar a defragmentação mesmo que exista pouco espaço livre em disco**.
 - Desmarque a opção **Executar a defragmentação mesmo que exista pouco espaço livre em disco** e clique em **Programar**.
- 5 Na caixa de diálogo **Programar**, selecione a frequência de execução da tarefa e clique em **OK**.
- 6 Clique em **Concluir**.

Modificar uma tarefa do Desfragmentador de Disco

É possível modificar uma tarefa programada do Desfragmentador de Disco para alterar a frequência com que é executada automaticamente no computador. Quando terminar, em **Desfragmentador de Disco**, é possível ver a data e a hora em que a tarefa será executada novamente.

- 1 Abra o painel Programador de Tarefas.
Como?

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.
- 2 Na lista **Selecione a operação a programar**, clique em **Desfragmentador de Disco**.
- 3 Selecione a tarefa na lista **Selecione uma tarefa existente** e clique em **Modificar**.
- 4 Efectue um dos seguintes procedimentos:
 - Clique em **Programar** para aceitar a opção predefinida **Executar a defragmentação mesmo que exista pouco espaço livre em disco**.
 - Desmarque a opção **Executar a defragmentação mesmo que exista pouco espaço livre em disco** e clique em **Programar**.
- 5 Na caixa de diálogo **Programar**, selecione a frequência de execução da tarefa e clique em **OK**.
- 6 Clique em **Concluir**.

Eliminar uma tarefa do Desfragmentador de Disco

É possível eliminar uma tarefa programada do Desfragmentador de Disco que já não pretende que seja executada automaticamente.

- 1 Abra o painel Programador de Tarefas.
Como?
 1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Fazer Manutenção do Computador**.
 2. Em **Programador de tarefas**, clique em **Iniciar**.
- 2 Na lista **Selecione a operação a programar**, clique em **Desfragmentador de Disco**.
- 3 Selecione a tarefa na lista **Selecione uma tarefa existente**.
- 4 Clique em **Eliminar** e, em seguida, clique em **Sim** para confirmar a eliminação.
- 5 Clique em **Concluir**.

CAPÍTULO 14

McAfee Shredder

O McAfee Shredder elimina (ou destrói) itens do disco rígido do computador de forma permanente. Mesmo quando apaga ficheiros e pastas manualmente, esvazia a Reciclagem ou elimina a pasta Temporary Internet Files, ainda é possível recuperar estas informações utilizando ferramentas informáticas forenses. De igual modo, um ficheiro eliminado pode ser recuperado porque alguns programas criam temporariamente cópias ocultas de ficheiros abertos. O Shredder protege a sua privacidade eliminando os ficheiros indesejados de forma segura e permanente. É importante ter em conta que os ficheiros destruídos não podem ser restaurados.

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades do Shredder	80
Destruir ficheiros, pastas e discos.....	81

Funcionalidades do Shredder

O Shredder elimina itens do disco rígido do computador de modo a que as respectivas informações associadas não possam ser recuperadas. Protege a sua privacidade eliminando, de forma permanente e segura, ficheiros e pastas, itens na Reciclagem e na pasta Temporary Internet Files e o conteúdo integral de discos de computador, tais como CDs regraváveis, unidades de disco externas e unidades de disquetes.

Destruir ficheiros, pastas e discos

O Shredder garante que as informações contidas nos ficheiros e pastas eliminados da Reciclagem e da pasta Temporary Internet Files não podem ser recuperadas, mesmo com ferramentas especiais. Com o Shredder, é possível especificar o número de vezes (até 10) que pretende que um item seja destruído. Um número maior de passagens de destruição aumenta o nível de eliminação segura dos ficheiros.

Destruir ficheiros e pastas

É possível destruir ficheiros e pastas do disco rígido do computador, incluindo itens da Reciclagem e da pasta Temporary Internet Files.

1 Abrir o **Shredder**.

Como?

1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Menu Avançado**.
2. No painel esquerdo, clique em **Ferramentas**.
3. Clique em **Shredder**.

2 No painel Destruir ficheiros e pastas, em **Quero**, clique em **Apagar ficheiros e pastas**.

3 Em **Nível de Destruição**, clique num dos níveis de destruição seguintes:

- **Rápido**: Destrói os itens seleccionados uma vez.
- **Abrangente**: Destrói os itens seleccionados 7 vezes.
- **Personalizado**: Destrói os itens seleccionados até 10 vezes.

4 Clique em **Seguinte**.

5 Efectue um dos seguintes procedimentos:

- Na lista **Selecione os ficheiros a destruir**, clique em **Conteúdo da Reciclagem** ou em **Ficheiros Temporários da Internet**.
- Clique em **Procurar**, procure o ficheiro que pretende destruir, selecione-o e, em seguida, clique em **Abrir**.

- 6 Clique em **Seguinte**.
- 7 Clique em **Iniciar**.
- 8 Quanto o Shredder terminar, clique em **Concluído**.

Nota: Não trabalhe com nenhum ficheiro até o Shredder concluir esta tarefa.

Destruir todo o disco

É possível apagar todo o conteúdo de um disco de uma vez. Apenas podem ser destruídas unidades amovíveis, tais como unidades de disco externas, CDs graváveis e unidades de disquete.

- 1 Abrir o **Shredder**.
Como?
 1. No painel do McAfee SecurityCenter, em **Tarefas Comuns**, clique em **Menu Avançado**.
 2. No painel esquerdo, clique em **Ferramentas**.
 3. Clique em **Shredder**.
- 2 No painel Destruir ficheiros e pastas, em **Quero**, clique em **Apagar um disco inteiro**.
- 3 Em **Nível de Destruição**, clique num dos níveis de destruição seguintes:
 - **Rápido:** Destrói a unidade seleccionada uma vez.
 - **Abrangente:** Destrói a unidade seleccionada 7 vezes.
 - **Personalizado:** Destrói a unidade seleccionada até 10 vezes.
- 4 Clique em **Seguinte**.
- 5 Na lista **Selecione o disco**, clique na unidade que pretende destruir.
- 6 Clique em **Seguinte** e, em seguida, clique em **Sim** para confirmar.
- 7 Clique em **Iniciar**.
- 8 Quanto o Shredder terminar, clique em **Concluído**.

Nota: Não trabalhe com nenhum ficheiro até que o McAfee Shredder tenha concluído esta tarefa.

CAPÍTULO 15

McAfee Network Manager

O Network Manager apresenta uma vista gráfica dos computadores e componentes que compõem a sua rede doméstica. Pode utilizar o Network Manager para monitorizar, de forma remota, o estado de protecção de cada computador gerido na sua rede e corrigir remotamente vulnerabilidades de segurança comunicadas nesses computadores.

Antes de utilizar o Network Manager, pode familiarizar-se com algumas das funcionalidades. A ajuda do Network Manager inclui detalhes sobre configuração e utilização dessas funcionalidades.

Nota: O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee.

Neste capítulo

Funcionalidades do Network Manager	84
Noções básicas sobre os ícones do Network Manager	85
Configurar uma rede gerida	87
Gerir a rede de forma remota	95

Funcionalidades do Network Manager

O Network Manager oferece as seguintes funcionalidades.

Mapeamento de rede gráfico

O mapeamento de rede do Network Manager proporciona uma visão gráfica global do estado de protecção dos computadores e componentes que compõem a sua rede doméstica. Quando altera a rede (por exemplo, adiciona um computador), o mapeamento de rede reconhece essas alterações. Pode actualizar o mapeamento de rede, mudar o nome da rede e mostrar ou ocultar componentes do mapeamento de rede, para personalizar a visualização. Pode também ver os detalhes de qualquer dos componentes apresentados no mapeamento de rede.

Gestão remota

Utilize o mapeamento de rede do Network Manager para gerir o estado de protecção dos computadores que fazem parte da sua rede doméstica. Pode convidar um computador a aderir à rede gerida, monitorizar o estado de protecção do computador gerido e resolver problemas de vulnerabilidade de segurança detectados a partir de um computador remoto da rede.

Noções básicas sobre os ícones do Network Manager

A tabela seguinte descreve os ícones normalmente utilizados no mapeamento de rede do Network Manager.

Ícone	Descrição
	Representa um computador gerido e online
	Representa um computador gerido e offline
	Representa um computador não gerido que tem o SecurityCenter instalado
	Representa um computador não gerido e offline
	Representa um computador online que não tem o SecurityCenter instalado ou um dispositivo de rede desconhecido
	Representa um computador offline que não tem o SecurityCenter instalado ou um dispositivo de rede desconhecido offline
	Significa que o item correspondente está protegido e ligado
	Significa que o item correspondente pode requerer a sua atenção
	Significa que o item correspondente requer a sua atenção imediata
	Representa um router de raiz sem fios
	Representa um router de raiz padrão
	Representa a Internet, quando está ligada
	Representa a Internet, quando está desligada

CAPÍTULO 16

Configurar uma rede gerida

Para configurar uma rede gerida, utilizar os itens do mapeamento de rede e adicionar membros (computadores) à rede. Antes de um computador poder ser gerido remotamente ou ser-lhe concedida permissão para gerir, de forma remota, outros computadores na rede, deve tornar-se um membro de confiança da rede. A confirmação de membro da rede é concedida a novos computadores através de membros de rede existentes (computadores) com permissões administrativas.

Pode ver os detalhes associados a qualquer dos componentes apresentados no mapeamento de rede, mesmo depois de efectuar alterações à rede (por exemplo, adicionar um computador).

Neste capítulo

Utilizar o mapeamento de rede	88
Aderir à rede gerida	90

Utilizar o mapeamento de rede

Quando um computador é ligado à rede, o Network Manager analisa a rede para determinar se existem membros geridos ou não geridos, quais são os atributos do router e o estado da Internet. Se não forem encontrados membros, o Network Manager presume que o computador actualmente ligado é o primeiro computador na rede e torna-o um membro gerido com permissões administrativas. Por predefinição, o nome da rede inclui o nome do grupo de trabalho ou do domínio do primeiro computador que é ligado à rede e que possui o SecurityCenter instalado; no entanto, é possível mudar o nome da rede a qualquer momento.

Se efectuar alterações na rede (por exemplo, adicionar um computador), pode personalizar o mapeamento de rede. Por exemplo, pode actualizar o mapeamento de rede, mudar o nome da rede, bem como mostrar ou ocultar componentes do mapeamento de rede para personalizar a sua vista. Pode também ver as informações associadas aos componentes apresentados no mapeamento de rede.

Aceder ao mapeamento de rede

O mapeamento de rede mostra uma representação gráfica dos computadores e componentes que compõem a sua rede doméstica.

- Nos Menus Básico ou Avançado, clique em **Gerir Rede**.

Nota: A primeira vez que acede ao mapeamento de rede, é-lhe solicitado que confie nos outros computadores da rede.

Actualizar o mapeamento de rede

Pode actualizar o mapeamento de rede em qualquer altura; por exemplo, depois de adicionar outro computador à rede gerida.

- 1 Nos Menus Básico ou Avançado, clique em **Gerir Rede**.
- 2 Clique em **Actualizar o mapeamento de rede** em **Quero**.

Nota: A ligação **Actualizar o mapeamento de rede** só está disponível se não estiverem seleccionados itens no mapeamento de rede. Para desmarcar um item, clique no item seleccionado ou numa área em branco no mapeamento de rede.

Mudar o nome da rede

Por predefinição, o nome da rede inclui o nome do grupo de trabalho ou do domínio do primeiro computador que é ligado à rede e possui o SecurityCenter instalado. Se preferir utilizar um nome diferente, pode alterá-lo.

- 1 Nos Menus Básico ou Avançado, clique em **Gerir Rede**.
- 2 Clique em **Mudar o nome da rede** em **Quero**.
- 3 Introduza o nome da rede na caixa **Nome da rede**.
- 4 Clique em **OK**.

Nota: A ligação **Mudar o nome da rede** só está disponível se não estiverem seleccionados itens no mapeamento de rede. Para desmarcar um item, clique no item seleccionado ou numa área em branco no mapeamento de rede.

Mostrar ou ocultar um item no mapeamento de rede

Por predefinição, todos os computadores e componentes na sua rede doméstica são apresentados no mapeamento de rede. No entanto, se tiver itens ocultos, pode mostrá-los novamente em qualquer altura. Só é possível ocultar os itens não geridos; os computadores geridos não podem ser ocultos.

Para...	No menu Básico ou Avançado, clique em Gerir Rede e efectue o seguinte...
Ocultar um item no mapeamento de rede	Clique num item no mapeamento de rede e, em seguida, clique em Ocultar este item em Quero . Na caixa de diálogo de confirmação, clique em Sim .
Mostrar itens ocultos no mapeamento de rede	Em Quero , clique em Mostrar itens ocultos .

Ver os detalhes de um item

Pode ver informações detalhadas sobre qualquer componente na sua rede se o seleccionar no mapeamento de rede. Estas informações incluem o nome do componente, o respectivo estado de protecção e outras informações necessárias para gerir o componente.

- 1 Clique no ícone de um item no mapeamento de rede.
- 2 Em **Detalhes**, visualize a informação sobre o item.

Aderir à rede gerida

Antes de um computador poder ser gerido remotamente ou ser-lhe concedida permissão para gerir, de forma remota, outros computadores na rede, deve tornar-se um membro de confiança da rede. A confirmação de membro da rede é concedida a novos computadores através de membros de rede existentes (computadores) com permissões administrativas. Para garantir que aderem apenas computadores de confiança à rede, os utilizadores dos computadores de concessão e adesão devem autenticar-se entre si.

Se um computador aderir à rede, ser-lhe-á solicitado para expor o respectivo estado de protecção McAfee a outros computadores na rede. Se um computador aceitar expor o respectivo estado de protecção, torna-se um membro gerido da rede. Se um computador recusar expor o respectivo estado de protecção, torna-se um membro não gerido da rede. Os membros não geridos da rede são normalmente computadores convidados que pretendem aceder a outras funções de rede (por exemplo, enviar ficheiros ou partilhar impressoras).

Nota: Depois de aderir, se tiver outros programas de rede da McAfee instalados (por exemplo, o EasyNetwork), o computador é igualmente reconhecido como um computador gerido nesses programas. O nível de permissão atribuído a um computador no Network Manager aplica-se a todos os programas de rede da McAfee. Para obter mais informações sobre o significado das permissões de convidado, de acesso total ou administrativo noutros programas de rede da McAfee, consulte a documentação fornecida com o respectivo programa.

Aderir a uma rede gerida

Se receber um convite para aderir a uma rede gerida, pode aceitá-lo ou recusá-lo. Pode também determinar se pretende que este computador e outros computadores na rede monitorizem as definições de segurança de cada um (por exemplo, se os serviços de protecção antivírus de um computador estão actualizados).

- 1 Na caixa de diálogo Rede Gerida, certifique-se de que a caixa de verificação **Permitir que todos os computadores desta rede monitorizem definições de segurança** está seleccionada.
- 2 Clique em **Aderir**.
Se aceitar o convite, são apresentadas duas cartas de jogar.
- 3 Confirme se essas cartas de jogar são iguais às apresentadas no computador que o convidou para aderir à rede gerida.
- 4 Clique em **OK**.

Nota: Se o computador que o convidou para aderir à rede gerida não apresentar as mesmas cartas de jogar apresentadas na caixa de diálogo de confirmação de segurança, isso significa que houve uma falha de segurança na rede gerida. A adesão à rede pode colocar o computador em risco; por conseguinte, clique em **Cancelar** na caixa de diálogo Rede Gerida.

Convidar um computador para aderir à rede gerida

Se um computador for adicionado à rede gerida ou existir outro computador não gerido na rede, pode convidar esse computador para aderir à rede gerida. Apenas os computadores com permissões administrativas na rede podem convidar outros computadores para aderir. Se enviar o convite, pode também especificar o nível de permissão que pretende atribuir ao computador aderente.

- 1 Clique no ícone de um computador não gerido no mapeamento de rede.
- 2 Clique em **Monitorizar este computador em Quero**.
- 3 Na caixa de diálogo Convidar um computador a aderir à rede gerida, clique numa das seguintes opções:
 - Clique em **Permitir acesso de convidado a programas da rede gerida** para permitir que o computador aceda à rede (pode utilizar esta opção para utilizadores temporários em casa).
 - Clique em **Permitir acesso total a programas da rede gerida** para permitir que o computador aceda à rede.

- Clique em **Permitir acesso administrativo a programas da rede gerida** para permitir que o computador acesse a rede com permissões administrativas. Permite também ao computador conceder acesso a outros computadores que pretendam aderir à rede gerida.
- 4 Clique em **OK**.
É enviado ao computador um convite para aderir à rede gerida. Se o computador aceitar o convite, são apresentadas duas cartas de jogar.
 - 5 Confirme se essas cartas de jogar são iguais às apresentadas no computador que convidou para aderir à rede gerida.
 - 6 Clique em **Conceder Acesso**.

Nota: Se o computador que convidou a aderir à rede gerida não apresentar as mesmas cartas de jogar apresentadas na caixa de diálogo de confirmação de segurança, isso significa que houve uma falha de segurança na rede gerida. Permitir a adesão de um computador à rede pode colocar outros computadores em risco; por conseguinte, clique em **Rejeitar Acesso** na caixa de diálogo de confirmação de segurança.

Parar de confiar nos computadores da rede

Se confiou noutros computadores na rede inadvertidamente, pode parar de confiar neles.

- Clique em **Parar de confiar em computadores nesta rede** em **Quero**.

Nota: A ligação **Parar de confiar em computadores nesta rede** não está disponível se possuir direitos administrativos e existirem outros computadores geridos na rede.

CAPÍTULO 17

Gerir a rede de forma remota

Depois de configurar a rede gerida, pode gerir remotamente os computadores e componentes que compõem a sua rede. Pode monitorizar o estado e os níveis de autorização dos computadores e componentes e corrigir a maioria das vulnerabilidades de segurança de forma remota.

Neste capítulo

Monitorizar o estado e as permissões	96
Corrigir vulnerabilidades de segurança.....	99

Monitorizar o estado e as permissões

Uma rede gerida possui membros geridos e membros não geridos. Os membros geridos permitem que outros computadores da rede monitorizem o respectivo estado de protecção McAfee; os membros não geridos não o permitem. Os membros não geridos são normalmente computadores convidados que pretendem aceder a outras funções de rede (por exemplo, enviar ficheiros ou partilhar impressoras). Um computador não gerido pode ser convidado a tornar-se um computador gerido em qualquer altura por outro computador gerido na rede. Do mesmo modo, um computador gerido pode tornar-se não gerido em qualquer altura.

Os computadores geridos têm permissões administrativas, totais ou de convidado. As permissões administrativas permitem ao computador gerido administrar o estado de protecção de todos os outros computadores geridos na rede e conceder aos computadores inscritos acesso à rede. As permissões de convidado e acesso total permitem que um computador aceda apenas à rede. Pode modificar o nível de permissão de um computador em qualquer altura.

Uma vez que a rede gerida também pode ter dispositivos (por exemplo, routers), pode utilizar o Network Manager para geri-los. Pode também configurar e modificar as propriedades de visualização de um dispositivo no mapeamento de rede.

Monitorizar o estado de protecção de um computador

Se o estado de protecção de um computador não estiver a ser monitorizado (o computador não é um membro ou é um membro não gerido), pode efectuar um pedido para monitorizá-lo.

- 1 Clique no ícone de um computador não gerido no mapeamento de rede.
- 2 Clique em **Monitorizar este computador** em **Quero**.

Parar de monitorizar o estado de protecção de um computador

Pode parar de monitorizar o estado de protecção de um computador gerido na rede; no entanto, o computador torna-se não gerido e não pode monitorizar o seu estado de protecção de forma remota.

- 1 Clique no ícone de um computador gerido no mapeamento de rede.
- 2 Clique em **Parar de monitorizar este computador** em **Quero**.
- 3 Na caixa de diálogo de confirmação, clique em **Sim**.

Modificar as permissões de um computador gerido

Pode alterar as permissões de um computador gerido em qualquer altura. Isto permite-lhe modificar os computadores que podem monitorizar o estado de protecção de outros computadores na rede.

- 1 Clique no ícone de um computador gerido no mapeamento de rede.
- 2 Clique em **Modificar as permissões deste computador** em **Quero**.
- 3 Na caixa de diálogo para modificar as permissões, seleccione ou desmarque a caixa de verificação para determinar se este e outros computadores na rede gerida podem monitorizar o estado de protecção de cada um.
- 4 Clique em **OK**.

Gerir um dispositivo

Pode gerir um dispositivo, acedendo à respectiva página Web de administração a partir do Network Manager.

- 1 Clique no ícone de um dispositivo no mapeamento de rede.
- 2 Clique em **Gerir este dispositivo** em **Quero**.
É aberto um Web browser e aparece a página Web de administração do dispositivo.
- 3 No Web browser, introduza as informações de início de sessão e configure as definições de segurança do dispositivo.

Nota: Se o dispositivo for um router ou um ponto de acesso sem fios protegido pelo Wireless Network Security, deve utilizar o Wireless Network Security para configurar as definições de segurança do dispositivo.

Modificar as propriedades de visualização de um dispositivo

Se modificar as propriedades de visualização de um dispositivo, pode também alterar o nome de visualização do dispositivo no mapeamento de rede e especificar se o dispositivo é um router sem fios.

- 1 Clique no ícone de um dispositivo no mapeamento de rede.
- 2 Clique em **Modificar as propriedades do dispositivo em Quero**.
- 3 Para especificar o nome de visualização do dispositivo, introduza um nome na caixa **Nome**.
- 4 Para especificar o tipo de dispositivo, clique em **Router Padrão** se não for um router sem fios, ou em **Router Sem Fios** se for o caso.
- 5 Clique em **OK**.

Corrigir vulnerabilidades de segurança

Os computadores geridos com autorizações administrativas podem monitorizar o estado de protecção McAfee de outros computadores geridos na rede e corrigir remotamente as vulnerabilidades de segurança comunicadas. Por exemplo, se o estado de protecção McAfee de um computador gerido indicar que o VirusScan está desactivado, outro computador gerido com autorizações administrativas pode activar o VirusScan remotamente.

Quando corrige vulnerabilidades de segurança remotamente, o Network Manager repara a maioria dos problemas comunicados. No entanto, algumas vulnerabilidades de segurança podem requerer intervenção manual no computador local. Neste caso, o Network Manager corrige os problemas que podem ser reparados remotamente e, em seguida, pede-lhe para corrigir os problemas restantes, iniciando sessão no SecurityCenter no computador vulnerável e seguindo as recomendações fornecidas. Nalguns casos, a resolução sugerida consiste em instalar a versão mais recente do SecurityCenter no(s) computador(es) remoto(s) da sua rede.

Corrigir vulnerabilidades de segurança

Pode utilizar o Network Manager para corrigir a maioria das vulnerabilidades de segurança de computadores remotos geridos. Por exemplo, se o VirusScan estiver desactivado num computador remoto, pode activá-lo.

- 1 Clique no ícone de um item no mapeamento de rede.
- 2 Veja o estado de protecção do item em **Detalhes**.
- 3 Clique em **Corrigir vulnerabilidades de segurança em Quero**.
- 4 Quando os problemas tiverem sido corrigidos, clique em **OK**.

Nota: Embora o Network Manager corrija automaticamente a maioria das vulnerabilidades de segurança, algumas correcções podem exigir que inicie o SecurityCenter no computador vulnerável e siga as recomendações fornecidas.

Instalar o software de segurança McAfee em computadores remotos

Se um ou mais computadores na sua rede não utilizarem a versão mais recente do SecurityCenter, o respectivo estado de protecção não pode ser monitorizado remotamente. Se pretender monitorizar esses computadores remotamente, deve aceder a cada computador e instalar a versão mais recente do SecurityCenter.

- 1** No computador em que pretende instalar o software de segurança, abra o SecurityCenter.
- 2** Em **Tarefas Comuns** clique em **A Minha Conta**.
- 3** Inicie sessão com o endereço de correio electrónico e a palavra-passe que utilizou para registar o software de segurança na primeira vez que o instalou.
- 4** Seleccione o produto adequado, clique no ícone **Transferir/Instalar** e siga as instruções apresentadas no ecrã.

Referência

O Glossário de Termos apresenta e define a terminologia de segurança mais utilizada que pode encontrar nos produtos da McAfee.

Glossário

8

802.11

Um conjunto de normas da IEEE para a transmissão de dados através de uma rede sem fios. A norma 802.11 é normalmente conhecida como Wi-Fi.

802.11a

Uma extensão da norma 802.11 que transmite dados até 54 Mbps na banda de frequências dos 5 GHz. Apesar da velocidade de transmissão ser superior à da norma 802.11b, a distância abrangida é muito menor.

802.11b

Uma extensão da norma 802.11 que transmite dados até 11 Mbps na banda de frequências dos 2,4 GHz. Apesar da velocidade de transmissão ser inferior à da norma 802.11a, a distância abrangida é maior.

802.1x

Uma norma da IEEE para autenticação em redes com e sem fios. A norma 802.1x é normalmente utilizada em redes sem fios 802.11.

A

adaptador sem fios

Um dispositivo que proporciona capacidades sem fios a um computador ou PDA. É ligado através de uma porta USB, ranhura PC Card (CardBus), ranhura de cartão de memória ou internamente ao barramento PCI.

Adaptador sem fios USB

Um adaptador sem fios que é ligado a uma ranhura USB do computador.

Adaptadores sem fios PCI

(Peripheral Component Interconnect) Um adaptador sem fios que é ligado a uma ranhura de expansão existente no interior do computador.

análise em tempo real

Para analisar a existência de vírus e outras actividades em ficheiros e pastas quando estes são acedidos pelo utilizador ou pelo computador.

arquivo

Para criar uma cópia dos seus ficheiros importantes em CD, DVD, unidade USB, unidade de disco externa ou unidade de rede.

arquivo integral

Para arquivar um conjunto completo de dados baseado nos tipos de ficheiros e localizações definidos. Consulte também arquivo rápido.

arquivo rápido

Para arquivar apenas os ficheiros que foram alterados desde o último arquivo completo ou rápido. Consulte também arquivo completo.

atalho

Um ficheiro que contém apenas a localização de outro ficheiro no computador.

ataque de dicionário

Um tipo de ataque de força bruta que utiliza palavras comuns para tentar descobrir uma palavra-passe.

ataque de força bruta

Um método de decodificação de dados encriptados, tais como palavras-passe, através do esforço exaustivo (força bruta) em vez da utilização de estratégias intelectuais. A força bruta é considerada um método infalível de ataque, se bem que demorado. O ataque de força bruta é também denominado descoberta por força bruta.

ataque de intermediário (man-in-the-middle)

Um método para interceptar e possivelmente modificar mensagens trocadas entre dois utilizadores sem que estes saibam que a ligação de comunicação foi violada.

autenticação

O processo de identificação de um indivíduo, normalmente através de um nome de utilizador e uma palavra-passe únicos.

B**biblioteca**

Uma área de armazenamento online para ficheiros copiados e publicados por utilizadores. A biblioteca do Data Backup é um Web site da Internet, que está acessível a todos os que tiverem acesso à Internet.

browser

Um programa utilizado para ver páginas Web na Internet. Os Web browsers mais conhecidos incluem o Microsoft Internet Explorer e o Mozilla Firefox.

C**cache**

Uma área de armazenamento de dados temporária no computador. Por exemplo, para aumentar a velocidade e a eficiência da navegação na Web, o browser pode obter uma página Web da cache (em lugar de um servidor remoto) na próxima vez que a visualizar.

Cavalo de Tróia

Um programa que aparenta ser legítimo mas que pode danificar ficheiros valiosos, interromper o desempenho e fornecer acesso não autorizado ao computador.

chave

Uma série de letras e números utilizada por dois dispositivos para autenticação da respectiva comunicação. Ambos os dispositivos têm de possuir a chave. Consulte também WEP, WPA, WPA2, WPA-PSK e WPA2-PSK.

cliente

Uma aplicação, em execução num computador pessoal ou estação de trabalho, que depende de um servidor para efectuar algumas operações. Por exemplo, um cliente de correio electrónico é uma aplicação que permite enviar e receber correio electrónico.

cliente de correio electrónico

Um programa que é executado no computador para enviar e receber correio electrónico (por exemplo, Microsoft Outlook).

Cofre de Palavras-passe

Área de armazenamento seguro para palavras-passe pessoais. Permite guardar palavras-passe com a certeza de que nenhum outro utilizador (nem mesmo um administrador) terá acesso às mesmas.

compressão

Processo pelo qual os ficheiros são comprimidos num formato que reduz o espaço necessário para os armazenar ou transmitir.

conta de correio electrónico padrão

Consulte POP3.

Controlo ActiveX

Um componente de software utilizado por programas ou páginas Web para adicionar funcionalidades que aparecem como uma parte normal do programa ou da página Web. A maioria dos controlos ActiveX são inofensivos; no entanto, alguns podem capturar informações do computador.

cookie

Um pequeno ficheiro que contém informações, incluindo normalmente um nome de utilizador e a data e hora actuais, armazenadas no computador de uma pessoa que navega na Web. Os cookies são utilizados principalmente por Web sites para identificar utilizadores que tenham efectuado previamente um registo ou visitado o site; no entanto, também podem constituir uma fonte de informação para hackers.

cópia de segurança

Para criar uma cópia dos ficheiros importantes num servidor online seguro.

D

DAT

(Ficheiros de assinatura de detecção) Ficheiros que contêm as definições utilizadas na detecção de vírus, cavalos de Tróia, spyware, adware e outros programas potencialmente indesejados num computador ou numa unidade USB.

DNS

(Sistema de Nomes de Domínio) Um sistema que converte nomes de anfitriões ou nomes de domínio em endereços IP. Na Web, o DNS é utilizado para converter endereços Web legíveis (por exemplo, www.omeuhost.com) em endereços IP (por exemplo, 111.2.3.44) para que o Web site possa ser obtido. Sem DNS, seria necessário introduzir o endereço IP no Web browser.

domínio

Uma sub-rede local ou um descritor de sites na Internet.

Numa rede de área local (LAN), um domínio é uma sub-rede constituída por computadores clientes e servidores controlados por uma base de dados de segurança. Neste contexto, os domínios podem melhorar o desempenho. Na Internet, o domínio faz parte de qualquer endereço Web (por exemplo, em www.abc.com, abc é o domínio).

E

criptação

Processo pelo qual os dados passam de texto a código, ocultando as informações para impedir que sejam lidas por pessoas que não sabem como as descriptar. Os dados encriptados também são conhecidos como texto cifrado.

endereço de correio electrónico

(correio electrónico) Mensagens enviadas e recebidas electronicamente através de uma rede de computadores. Consulte também Webmail.

endereço IP

Um identificador para um computador ou dispositivo localizado numa rede TCP/IP. As redes que utilizam o protocolo TCP/IP encaminham as mensagens com base no endereço IP do destino. O formato de um endereço IP é um endereço numérico de 32 bits escrito como quatro números separados por pontos. Cada número deve estar compreendido entre 0 e 255 (por exemplo, 192.168.1.100).

Endereço MAC

(Endereço de Controlo de Acesso a Suportes de Dados) Um número de série exclusivo atribuído a um dispositivo físico que acede à rede.

Erros de Web

Pequenos ficheiros gráficos que podem incorporar-se nas páginas HTML e permitir que uma fonte não autorizada instale cookies no computador. Estes cookies podem depois transmitir informações à fonte não autorizada. Erros de Web são também designados sinalizadores Web, pixel tags, GIFs limpos ou GIFs invisíveis.

ESS

(Extended Service Set) Um conjunto de duas ou mais redes que constituem uma única sub-rede.

evento

Uma acção iniciada pelo utilizador, um dispositivo ou o próprio computador que desencadeia uma resposta. A McAfee regista os eventos no seu registo de eventos.

F

Falsificação de IP

Falsificar os endereços IP existentes num pacote IP. Esta técnica é utilizada em vários tipos de ataques, incluindo a utilização indevida de sessões. Esta técnica é também frequentemente utilizada para falsificar os cabeçalhos de correio publicitário não solicitado, para impedir que estes sejam correctamente rastreados.

ficheiro temporário

Um ficheiro, criado na memória ou no disco pelo sistema operativo ou outro programa, para ser utilizado durante uma sessão e, em seguida, eliminado.

filtragem de imagens

Uma opção das Limitações de Acesso que bloqueia a apresentação de imagens da Web potencialmente inadequadas.

firewall

Um sistema (de hardware, software ou ambos) concebido para impedir o acesso não autorizado a uma rede privada. As firewalls são frequentemente utilizadas para impedir que utilizadores não autorizados acedam a redes privadas ligadas à Internet, especialmente a uma intranet. Todas as mensagens enviadas e recebidas pela intranet passam pela firewall, que examina e bloqueia as que não correspondem aos critérios de segurança especificados.

fragmentos de ficheiros

Vestígios de ficheiros dispersos no disco. A fragmentação de ficheiros ocorre à medida que os ficheiros são adicionados ou eliminados e pode diminuir o desempenho do computador.

G

gateway integrado

Um dispositivo que combina as funções de um ponto de acesso (AP), de um router e de um firewall. Alguns dispositivos também podem incluir melhoramentos de segurança e funcionalidades de bridging.

grupo de classificação de conteúdos

Nas Limitações de Acesso, um grupo etário a que um utilizador pertence. O conteúdo é disponibilizado ou bloqueado com base no grupo de classificação de conteúdos ao qual o utilizador pertence. Os grupos de classificação de conteúdos incluem: criança pequena, criança, adolescente mais novo, adolescente mais velho e adulto.

H

hotspot

Uma área geográfica abrangida por um ponto de acesso (AP) Wi-Fi (802.11). Os utilizadores que entram num hotspot através de um portátil sem fios podem ligar à Internet, desde que o hotspot esteja a sinalizar (ou seja, a divulgar a sua presença) e não seja exigida autenticação. Os hotspots encontram-se frequentemente localizados em áreas muito movimentadas, tais como aeroportos.

I

Internet

A Internet é composta por um grande número de redes interligadas que utilizam protocolos TCP/IP para localização e transferência de dados. A Internet surgiu a partir de uma rede criada para ligar computadores de universidades e faculdades (no fim da década de 60 e início de 70), fundada pelo Departamento de Defesa dos E.U.A. e era denominada ARPANET. Actualmente, a Internet é uma rede global de aproximadamente 100.000 redes independentes.

intranet

Uma rede de computadores privada, normalmente dentro de uma organização, que apenas pode ser acedida por utilizadores autorizados.

L

LAN

(Rede de Área Local) Uma rede de computadores que abrange uma área relativamente pequena (por exemplo, um edifício). Os computadores existentes numa LAN podem comunicar entre si e partilhar recursos, tais como impressoras e ficheiros.

largura de banda

A quantidade de dados que pode ser transmitida num período de tempo fixo.

launchpad

Um componente da interface U3 que actua como um ponto de arranque para o início e gestão de programas U3 USB.

Limitações de Acesso

Definições que ajudam a controlar o que as crianças podem ver e o que fazem enquanto navegam na Web. Para configurar Limitações de Acesso, é possível activar ou desactivar a filtragem de imagens, seleccionar um grupo de classificações de conteúdos e definir limites de tempo de navegação na Web.

lista de confiança

Contém itens em que o utilizador tem confiança e não são detectados. Se tiver confiado num item (por exemplo, um programa potencialmente indesejado ou uma alteração do registo) inadvertidamente ou pretender que o item seja detectado novamente, deve removê-lo desta lista.

lista de sites bloqueados

Em antiphishing, uma lista de Web sites considerados fraudulentos.

lista de sites seguros

Lista de Web sites a que os utilizadores podem aceder por não serem considerados fraudulentos.

localização com monitorização abrangente

Uma pasta do computador sujeita a monitorização para detecção de alterações efectuadas pelo Data Backup. Se tiver definido uma localização de monitorização abrangente, o Data Backup efectua a cópia de segurança dos tipos de ficheiros monitorizados dentro da pasta e respectivas subpastas.

localizações com monitorização superficial

Uma pasta do computador sujeita a monitorização para detecção de alterações efectuadas pelo Data Backup. Se tiver definido uma localização para monitorização superficial, o Data Backup efectua a cópia de segurança dos tipos de ficheiros monitorizados dentro da pasta, mas não inclui as respectivas subpastas.

localizações monitorizadas

Pastas do computador monitorizadas pelo Data Backup.

M

mapeamento de rede

Uma representação gráfica dos computadores e dos componentes que fazem parte de uma rede doméstica.

MAPI

(Messaging Application Programming Interface) Especificação de interface Microsoft que permite que diferentes aplicações de mensagens e de grupos de trabalho (incluindo correio electrónico, correio de voz e fax) funcionem através de um único cliente, como o cliente Exchange.

marcador

Software que ajuda a estabelecer uma ligação à Internet. Quando utilizados maliciosamente, os marcadores podem redireccionar as ligações à Internet para alguém que não seja o seu fornecedor de serviços Internet (ISP) predefinido, sem o informar dos custos adicionais.

message authentication code (MAC)

Um código de segurança utilizado para encriptar mensagens transmitidas entre computadores. A mensagem é aceite se o computador reconhecer o código decriptado como válido.

MSN

(Microsoft Network) Um grupo de serviços baseados na Web oferecido pela Microsoft Corporation, que inclui um motor de procura, correio electrónico, mensagens instantâneas e portal.

N

NIC

(Placa de Rede) Uma placa que é ligada a um computador portátil ou outro dispositivo, permitindo-lhe aceder à LAN.

nó

Um único computador ligado a uma rede.

P

palavra-chave

Palavra que pode atribuir a um ficheiro do qual foi efectuada uma cópia de segurança para estabelecer uma relação ou uma ligação com outros ficheiros aos quais foi atribuída a mesma palavra-chave. A atribuição de palavras-chave a ficheiros facilita a procura de ficheiros publicados na Internet.

palavra-passe

Um código (normalmente constituído por letras e números) utilizado para obter acesso a um computador, um programa ou um Web site.

partilha

Para permitir que os destinatários do correio electrónico tenham acesso a ficheiros com cópia de segurança durante um período de tempo limitado. Quando partilha um ficheiro, envia uma cópia de segurança do ficheiro para os destinatários do correio electrónico que especificar. Os destinatários recebem a mensagem de correio electrónico a partir do Data Backup, com a indicação de que os ficheiros foram partilhados com os mesmos. A mensagem de correio electrónico inclui ainda uma ligação para os ficheiros partilhados.

pesquisa a pedido

Uma análise que é iniciada a pedido (ou seja, quando a operação é iniciada). Ao contrário da análise em tempo real, a análise a pedido não é iniciada automaticamente.

phishing

Um esquema fraudulento da Internet concebido para obter informações valiosas (tais como números de cartões de crédito e de segurança social, IDs de utilizador e palavras-passe) de pessoas desconhecidas para utilização fraudulenta.

plug-in

Pequeno programa de software que funciona com um programa mais abrangente para proporcionar maior funcionalidade. Por exemplo, permite que um Web browser aceda a e execute ficheiros incorporados em documentos HTML em formatos que o browser normalmente não reconheceria (por exemplo, ficheiros de animação, vídeo e áudio).

Ponto de Acesso

Um dispositivo de rede (frequentemente designado por router sem fios) ligado a um concentrador ou comutador Ethernet para aumentar o alcance físico de assistência para os utilizadores sem fios. Quando os utilizadores sem fios vagueiam com os seus dispositivos móveis, a transmissão passa de um Ponto de Acesso (AP) para outro para manter a conectividade.

ponto de acesso não autorizado

Um Ponto de Acesso não autorizado. Os pontos de acesso não autorizados podem ser instalados numa rede empresarial protegida para conceder acesso à rede a pessoas não autorizadas. Também podem ser criados para permitir a um atacante executar um ataque de intermediário.

ponto de restauro do sistema

Uma descrição geral (imagem) do conteúdo da memória ou de uma base de dados do computador. O Windows cria pontos de restauro periodicamente quando ocorrem eventos de sistema significativos (como, por exemplo, quando é instalado um programa ou um controlador). Também pode criar e atribuir um nome aos seus pontos de restauro em qualquer altura.

pop-ups

Pequenas janelas que aparecem por cima de outras janelas no ecrã do computador. As janelas de pop-up são frequentemente utilizadas em Web browsers para apresentação de anúncios.

POP3

(Post Office Protocol 3) Uma interface entre um programa cliente de correio electrónico e o servidor de correio electrónico. A maioria dos utilizadores domésticos possui uma conta de correio electrónico POP3, também conhecida como conta padrão de correio electrónico.

porta

Local onde passam as informações para entrar e/ou sair de um computador. Por exemplo, um modem analógico convencional é ligado a uma porta série.

PPPoE

(Point-to-Point Protocol Over Ethernet) Um método de utilização do protocolo de acesso telefónico Point-to-Point Protocol (PPP) com a Ethernet como transporte.

programas potencialmente indesejados (PUPs)

Programas que recolhem e transmitem informações pessoais sem a sua permissão (por exemplo, spyware e adware).

Protecção do Sistema

Alertas da McAfee que detectam alterações não autorizadas ao computador e o notificam quando as mesmas ocorrem.

protocolo

Um formato (de hardware ou software) para a transmissão de dados entre dois dispositivos. O computador ou dispositivo deve suportar o protocolo correcto para comunicar com outros computadores.

proxy

Computador (ou software executado no mesmo) que funciona como barreira entre uma rede e a Internet, apresentando apenas um endereço de rede para sites externos. Ao agir como representante de todos os computadores internos, o proxy protege identidades de rede ao mesmo tempo que fornece acesso à Internet. Consulte também servidor proxy.

publicar

Disponibilizar publicamente na Internet um ficheiro do qual foi efectuada uma cópia de segurança. É possível aceder a ficheiros publicados, pesquisando a biblioteca do Data Backup.

Q

quarentena

Isolar. Por exemplo, no VirusScan, os ficheiros suspeitos são detectados e colocados em quarentena para que não possam danificar ficheiros ou o computador .

R

RADIUS

(Remote Access Dial-In User Service) Um protocolo que permite a autenticação de utilizadores, normalmente no contexto do acesso remoto. Originalmente definido para utilização com servidores de acesso telefónico remoto, o protocolo RADIUS é agora utilizado numa vasta gama de ambientes de autenticação, incluindo a autenticação 802.1x do segredo partilhado dos utilizadores de uma WLAN.

Reciclagem

Um recipiente de lixo simulado para os ficheiros e pastas eliminados no Windows.

recusa de serviço

Um tipo de ataque que torna lento ou interrompe o tráfego numa rede. Um ataque de recusa de serviço (ataque DoS) ocorre quando uma rede é inundada com um número demasiado elevado de pedidos adicionais que provocam a lentidão ou a paragem total do tráfego normal. Normalmente, não provoca furtos de informação ou outras vulnerabilidades na segurança.

rede

Um conjunto de Pontos de Acesso e dos utilizadores associados, equivalente a um ESS.

rede doméstica

Dois ou mais computadores ligados entre si numa casa particular para partilharem ficheiros e o acesso à Internet. Consulte também LAN.

rede gerida

Uma rede doméstica com dois tipos de membros: membros geridos e membros não geridos. Os membros geridos permitem que outros computadores da rede monitorizem o respectivo estado de protecção; os membros não geridos não o permitem.

registo

A base de dados na qual o Windows armazena as suas informações de configuração. O registo contém os perfis de cada utilizador do computador e informações acerca do hardware do sistema, dos programas instalados e de definições de propriedade. O Windows consulta continuamente estas informações durante o seu funcionamento.

repositório de cópia de segurança online

Localização do servidor online onde os ficheiros são guardados depois de ter sido efectuada a cópia de segurança.

restaurar

Para repor uma cópia de um ficheiro a partir de um arquivo ou do repositório de cópias de segurança online.

roaming

Para passar da área de cobertura de um Ponto de Acesso (AP) para outra sem interrupção do serviço ou perda de conectividade.

rootkit

Um conjunto de ferramentas (programas) que concede acesso de administrador a um computador ou rede de computadores. Os rootkits podem incluir spyware e outros programas potencialmente indesejados que podem criar riscos adicionais para a segurança ou privacidade dos dados do computador e das informações pessoais.

router

Um dispositivo de rede que encaminha pacotes de dados entre redes. Com base nas tabelas de encaminhamento internas, os routers lêem cada pacote recebido e decidem como o devem reencaminhar a partir de qualquer combinação de endereços de origem e destino, bem como pelas condições actuais de tráfego (por exemplo, a carga, os custos das linhas e a existência de linhas danificadas). Por vezes, um router é referido como Ponto de Acesso (AP).

S

script

Uma sequência de comandos que pode ser executada automaticamente (ou seja, sem interacção do utilizador). Ao contrário dos programas, os scripts são normalmente armazenados em formato de texto simples e compilados sempre que são executados. As macros e os ficheiros batch também são referidos como scripts.

segredo partilhado

Uma sequência ou chave (normalmente uma palavra-passe) que foi partilhada entre duas partes antes de iniciarem uma comunicação entre si. Os segredos partilhados são utilizados para proteger partes sensíveis de mensagens RADIUS.

servidor

Um computador ou programa que aceita ligações de outros computadores ou programas e devolve respostas adequadas. Por exemplo, o seu programa de correio electrónico liga a um servidor de correio electrónico sempre que envia ou recebe mensagens de correio electrónico.

Servidor DNS

(Servidor de Sistema de Nomes de Domínio) Um computador que devolve o endereço IP associado a um anfitrião ou a um nome de domínio. Consulte também DNS.

servidor proxy

Componente de firewall que gere o tráfego de Internet de e para uma rede local. Um servidor proxy pode melhorar o desempenho ao fornecer dados pedidos com frequência, como, por exemplo, uma página Web popular, e consegue filtrar e ignorar pedidos que o proprietário não considera adequados, como pedidos de acesso não autorizado a ficheiros de propriedade.

sincronizar

Permite resolver problemas de inconsistência entre ficheiros com cópia de segurança e ficheiros guardados no computador local. Sincroniza-se ficheiros quando a versão do ficheiro no repositório de cópias de segurança online é mais recente do que a versão do ficheiro existente nos outros computadores.

smart drive

Consulte unidade USB.

SMTP

(Simple Mail Transfer Protocol) Um protocolo TCP/IP para o envio de mensagens de um computador para outro numa rede. Este protocolo é utilizado na Internet para encaminhamento de correio electrónico.

sobrecarga da memória intermédia

Uma condição que ocorre quando programas ou processos suspeitos tentam armazenar numa memória intermédia (área de armazenamento de dados temporária) do computador mais informações do que o limite suportado. As sobrecargas da memória intermédia danificam ou substituem dados nas memórias intermédias adjacentes.

SSID

(Identificador do Conjunto de Serviços) Um token (chave secreta) que identifica uma rede Wi-Fi (802.11). O SSID é definido pelo administrador da rede e tem de ser fornecido a todos os utilizadores que pretendem ligar-se à rede.

SSL

(Secure Sockets Layer) Protocolo desenvolvido pela Netscape para a transmissão de documentos privados através da Internet. O SSL funciona através da utilização de uma chave pública para encriptar os dados que são transferidos através da ligação SSL. Os URLs que requerem uma ligação SSL começam por https em vez de http.

T

texto cifrado

Texto encriptado. O texto cifrado não é legível até ser convertido em texto simples (ou seja, desencriptado).

texto simples

Texto que não está encriptado. Consulte também encriptação.

tipos de ficheiros monitorizados

Tipos de ficheiros (por exemplo, .doc, .xls, etc.) que o Data Backup copia ou arquiva nas localizações de monitorização.

TKIP

(Temporal Key Integrity Protocol) Um protocolo que resolve os pontos fracos inerentes à segurança WEP, especialmente a reutilização de chaves de encriptação. O TKIP altera as chaves temporais a cada 10.000 pacotes, proporcionando um método de distribuição dinâmica que melhora significativamente a segurança da rede. O processo de segurança do TKIP começa com uma chave temporal de 128 bits que é partilhada entre os clientes e os pontos de acesso. O TKIP combina a chave temporal com o endereço MAC dos clientes e, em seguida, adiciona um vector de inicialização de 16 octetos, relativamente grande, para produzir a chave que encripta os dados. Este procedimento assegura que cada estação utiliza sequências de chaves diferentes para encriptar os dados. O TKIP utiliza o RC4 para a encriptação.

U

U3

(Você: Simplificado, Inteligente, Portátil) Uma plataforma para executar programas do Windows 2000 ou do Windows XP directamente a partir de um dispositivo USB. A iniciativa U3 foi fundada em 2004 pela M-Systems e pela SanDisk e permite aos utilizadores executarem programas U3 num computador Windows sem instalarem ou armazenarem dados ou definições no computador.

unidade de disco rígido externa

Uma unidade de disco rígido armazenada no exterior do computador.

unidade de rede

Uma unidade de disco ou uma unidade de banda que está ligada a um servidor de uma rede e que é partilhada por vários utilizadores. As unidades de rede são por vezes designadas unidades remotas.

Unidade USB

Uma pequena unidade de memória que é ligada a uma porta USB do computador. Uma unidade USB funciona como uma pequena unidade de disco, simplificando a transferência de ficheiros entre computadores.

URL

(Uniform Resource Locator) É o formato padrão para endereços da Internet.

USB

(Universal Serial Bus) Uma interface série de computador normalizada que permite ligar dispositivos periféricos, por exemplo, teclados, joysticks e impressoras, ao computador.

V

vírus

Programas de auto-replicação que podem alterar os seus ficheiros ou dados. Aparentam, com frequência, ter origem num remetente de confiança ou conter conteúdos benignos.

VPN

(Virtual Private Network) Uma rede privada configurada no interior de uma rede pública a fim de tirar partido das instalações de gestão de uma rede pública. AS VPN são utilizadas por empresas para criar redes alargadas (WANs) que abrangem áreas geográficas vastas, para proporcionar ligações site a site entre escritórios ou permitir que os utilizadores móveis acedam às LANs das respectivas empresas.

W

wardriver

Uma pessoa equipada com um computador Wi-Fi e algum hardware ou software especial e que percorre cidades para interceptar redes Wi-Fi (802.11).

Webmail

Mensagens enviadas e recebidas electronicamente através da Internet. Consulte também correio electrónico.

WEP

(Wired Equivalent Privacy) Um protocolo de encriptação e autenticação definido como parte da norma Wi-Fi (802.11). As versões iniciais são baseadas em cifras RC4 e têm vários pontos fracos. O WEP tenta proporcionar segurança, encriptando os dados transmitidos através das ondas de rádio, de modo a que estes estejam protegidos enquanto viajam entre dois pontos. No entanto, chegou-se à conclusão que o WEP não é tão seguro como se pensava inicialmente.

Wi-Fi

(Wireless Fidelity) Um termo utilizado genericamente pela Wi-Fi Alliance para referir qualquer tipo de rede 802.11.

Wi-Fi Alliance

Um organização composta pelos principais fabricantes de equipamentos de hardware e software sem fios. A Wi-Fi Alliance visa certificar a interoperacionalidade de todos os produtos baseados na norma 802.11 e promover o termo Wi-Fi como marca global em todos os mercados para todos os produtos sem fios baseados na norma 802.11. A organização age como um consórcio, laboratório de testes e ponto de encontro para todos os fabricantes que pretendam promover o crescimento da indústria.

Wi-Fi Certified

Produtos testados e aprovados pela Wi-Fi Alliance. Os produtos aprovados como Wi-Fi Certified têm a garantia de serem interoperacionais, mesmo que sejam provenientes de fabricantes diferentes. Um utilizador com um produto Wi-Fi Certified pode utilizar qualquer marca de Ponto de Acesso (AP) com qualquer outra marca de hardware cliente que também seja certificado.

WLAN

(Rede Local sem Fios) Uma rede local (LAN) que utiliza uma ligação sem fios. Uma WLAN utiliza ondas de rádio de alta frequência para a comunicação entre computadores, em vez de fios.

worm

Um vírus de replicação automática que reside na memória activa e que pode enviar cópias de si próprio através do correio electrónico. Os worms replicam-se e consomem recursos do sistema, diminuindo o desempenho ou parando tarefas.

WPA

(Wi-Fi Protected Access) Uma norma que aumenta significativamente o nível de protecção de dados e o controlo de acesso para os sistemas de LAN sem fios actuais e futuros. Concebido para funcionar no hardware existente, sob a forma de uma actualização de software, o WPA deriva e é compatível com a norma IEEE 802.11i. Quando instalado de modo correcto, fornece aos utilizadores da LAN sem fios um elevado grau de confiança em que os respectivos dados permanecem protegidos e que apenas os utilizadores autorizados da rede podem aceder a esta.

WPA-PSK

Um modo especial do WPA concebido para utilizadores domésticos que não requerem segurança de nível empresarial e que não dispõem de acesso a servidores de autenticação. Neste modo, o utilizador doméstico introduz manualmente a palavra-passe inicial para activar o Wi-Fi Protected Access no modo de Chave Pré-Partilhada, devendo alterar regularmente a frase-passe em cada computador e Ponto de Acesso sem fios. Consulte também WPA2-PSK e TKIP.

WPA2

Uma actualização da norma de segurança WPA e que se baseia na norma IEEE 802.11i.

WPA2-PSK

Um modo WPA especial idêntico ao modo WPA-PSK e que se baseia na norma WPA2. Uma funcionalidade comum do WPA2-PSK é o facto de os dispositivos suportarem normalmente vários modos de encriptação (por exemplo, AES, TKIP) em simultâneo, enquanto que os dispositivos mais antigos, geralmente, suportam apenas um único modo de encriptação de cada vez (ou seja, todos os clientes teriam de utilizar o mesmo modo de encriptação).

Acerca da McAfee

A McAfee, Inc., com sede em Santa Clara, Califórnia (EUA), é o líder global em Prevenção de Intrusões e Gestão de Riscos de Segurança, fornecendo soluções e serviços proactivos e comprovados destinados a proteger sistemas e redes em todo o mundo. Graças aos seus conhecimentos ímpares na área da segurança e ao compromisso de inovação, a McAfee permite que utilizadores domésticos, empresas, o sector público e fornecedores de serviços possam bloquear ataques, impedir interrupções e controlar e melhorar continuamente a respectiva segurança.

Copyright

Copyright © 2007-2008 McAfee, Inc. Todos os Direitos Reservados. Nenhuma parte desta publicação pode ser reproduzida, transmitida, transcrita, armazenada num sistema de recuperação ou traduzida para qualquer idioma em qualquer forma ou por qualquer meio sem a permissão, por escrito, da McAfee, Inc. McAfee e outras marcas comerciais aqui contidas são marcas registadas ou marcas comerciais da McAfee, Inc. e/ou respectivas filiais nos E.U.A e/ou noutros países. O símbolo McAfee vermelho em relação à segurança é característica dos produtos da marca McAfee. Todas as outras marcas registadas e não registadas, bem como material protegido por direitos de autor, aqui indicados, são propriedade exclusiva dos respectivos proprietários.

ATRIBUIÇÕES DE MARCAS COMERCIAIS

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, MCAFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN.

Licença

INFORMAÇÃO AOS UTILIZADORES: LEIA ATENTAMENTE O CONTRATO LEGAL CORRESPONDENTE À LICENÇA ADQUIRIDA, O QUAL ESTABELECE OS TERMOS E AS CONDIÇÕES GERAIS DE UTILIZAÇÃO DO SOFTWARE LICENCIADO. CASO DESCONHEÇA O TIPO DE LICENÇA QUE ADQUIRIU, CONSULTE A DOCUMENTAÇÃO DE COMPRA E VENDA OU OUTRA DOCUMENTAÇÃO RELACIONADA COM A CONCESSÃO DE LICENÇA OU ORDEM DE COMPRA INCLUÍDA NO PACOTE DO SOFTWARE OU FORNECIDA SEPARADAMENTE COMO PARTE DO PROCESSO DE COMPRA (COMO UM FOLHETO, UM FICHEIRO NO CD DO PRODUTO OU UM FICHEIRO DISPONÍVEL NO WEB SITE A PARTIR DO QUAL O PACOTE DE SOFTWARE FOI TRANSFERIDO). SE NÃO CONCORDAR COM TODOS OS TERMOS ESTABELECIDOS NO CONTRATO, NÃO INSTALE O SOFTWARE. SE FOR APLICÁVEL, PODERÁ DEVOLVER O PRODUTO À MCAFEE, INC. OU AO LOCAL DE AQUISIÇÃO PARA OBTER UM REEMBOLSO NA ÍNTEGRA.

CAPÍTULO 18

Suporte a Clientes e Suporte Técnico

O SecurityCenter comunica os problemas de protecção críticos e não críticos logo que são detectados. Os problemas críticos requerem uma acção imediata e comprometem o estado de protecção (a cor muda para vermelho). Os problemas de protecção não críticos não requerem uma acção imediata e podem ou não comprometer o estado de protecção (dependendo do tipo de problema). Para obter o estado de protecção verde, deve corrigir todos os problemas críticos e corrigir ou ignorar todos os problemas não críticos. Se necessitar de ajuda para diagnosticar os seus problemas de protecção, pode executar o Técnico Virtual da McAfee. Para obter mais informações sobre o Técnico Virtual da McAfee, consulte a ajuda do Técnico Virtual da McAfee.

Se tiver adquirido o software de segurança num parceiro ou fornecedor da McAfee, abra um Web browser e aceda a www.mcafeeajuda.com. Em seguida, em *Ligações de Parceiros*, seleccione o parceiro ou fornecedor para aceder ao Técnico Virtual da McAfee.

Nota: Para instalar e executar o Técnico Virtual da McAfee, é necessário iniciar sessão no computador como Administrador do Windows. Caso contrário, o MVT poderá não conseguir resolver os seus problemas. Para obter informações sobre o início de sessão como Administrador do Windows, consulte a Ajuda do Windows. No Windows Vista™, é-lhe solicitado quando executar o MVT. Clique em **Aceitar**. O Técnico Virtual não é compatível com o Mozilla® Firefox.

Neste capítulo

Utilizar o Técnico Virtual da McAfee	120
Suporte e Transferências	121

Utilizar o Técnico Virtual da McAfee

À semelhança de um representante físico do suporte técnico, o Técnico Virtual recolhe informações sobre os programas do SecurityCenter para resolver os problemas de protecção do computador. Quando é executado, o Técnico Virtual verifica se os programas do SecurityCenter estão a funcionar correctamente. Se encontrar problemas, o Técnico Virtual pode solucioná-los ou fornecer-lhe informações mais detalhadas sobre os mesmos. Quando termina, o Técnico Virtual apresenta os resultados da análise que efectuou e permite-lhe procurar suporte técnico adicional da McAfee, se necessário.

Para manter a segurança e a integridade do computador e dos ficheiros, o Técnico Virtual não recolhe informações de identificação pessoal.

Nota: Para obter mais informações sobre o Técnico Virtual, clique no ícone da **Ajuda** no Técnico Virtual.

Iniciar o Técnico Virtual

O Técnico Virtual recolhe informações sobre os programas do SecurityCenter para resolver os seus problemas de protecção. Para salvaguardar a sua privacidade, estas informações não incluem informações de identificação pessoal.

- 1** Em **Tarefas Comuns**, clique em **Técnico Virtual da McAfee**.
- 2** Siga as instruções apresentadas no ecrã para transferir e executar o Técnico Virtual.

Suporte e Transferências

Consulte as tabelas seguintes para conhecer os sites de Suporte e Transferência da McAfee no seu país, incluindo Manuais do Utilizador.

Suporte e Transferências

País	Suporte McAfee	Transferências McAfee
Austrália	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasil	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canadá (Inglês)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Canadá (Francês)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
China (chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
China (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
República Checa	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Dinamarca	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finlândia	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
França	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Alemanha	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Grã-Bretanha	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Itália	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japão	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Coreia	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
México	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Noruega	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polónia	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Espanha	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Suécia	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turquia	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Estados Unidos	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

Manuais do Utilizador do McAfee Total Protection

País	Manuais do Utilizador da McAfee
Austrália	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canadá (Inglês)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canadá (Francês)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Alemanha	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Grã-Bretanha	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

Coreia	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polónia	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

Manuais do Utilizador do McAfee Internet Security

País	Manuais do Utilizador da McAfee
Austrália	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canadá (Inglês)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canadá (Francês)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Alemanha	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

Grã-Bretanha	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Coreia	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polónia	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

Manuais do Utilizador do McAfee VirusScan Plus

País	Manuais do Utilizador da McAfee
Austrália	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canadá (Inglês)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canadá (Francês)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Dinamarca	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Alemanha	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Grã-Bretanha	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Coreia	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polónia	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

Manuais do Utilizador do McAfee VirusScan

País	Manuais do Utilizador da McAfee
Austrália	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canadá (Inglês)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

Canadá (Francês)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Alemanha	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Grã-Bretanha	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Coreia	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polónia	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Consulte a tabela seguinte para conhecer os sites do Centro de Ameaças e Informação de Vírus da McAfee no seu país.

País	Sede de Segurança	Informações de Vírus
Austrália	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasil	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canadá (Inglês)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canadá (Francês)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
China (chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
China (tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
República Checa	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Dinamarca	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finlândia	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
França	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Alemanha	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Grã-Bretanha	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Holanda	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Itália	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japão	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Coreia	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
México	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Noruega	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polónia	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo

Espanha	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Suécia	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turquia	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Estados Unidos	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Consulte a tabela seguinte para conhecer os sites da HackerWatch no seu país.

País	HackerWatch
Austrália	www.hackerwatch.org
Brasil	www.hackerwatch.org/?lang=pt-br
Canadá (Inglês)	www.hackerwatch.org
Canadá (Francês)	www.hackerwatch.org/?lang=fr-ca
China (chn)	www.hackerwatch.org/?lang=zh-cn
China (tw)	www.hackerwatch.org/?lang=zh-tw
República Checa	www.hackerwatch.org/?lang=cs
Dinamarca	www.hackerwatch.org/?lang=da
Finlândia	www.hackerwatch.org/?lang=fi
França	www.hackerwatch.org/?lang=fr
Alemanha	www.hackerwatch.org/?lang=de
Grã-Bretanha	www.hackerwatch.org
Holanda	www.hackerwatch.org/?lang=nl
Itália	www.hackerwatch.org/?lang=it
Japão	www.hackerwatch.org/?lang=jp
Coreia	www.hackerwatch.org/?lang=ko
México	www.hackerwatch.org/?lang=es-mx
Noruega	www.hackerwatch.org/?lang=no
Polónia	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Espanha	www.hackerwatch.org/?lang=es
Suécia	www.hackerwatch.org/?lang=sv
Turquia	www.hackerwatch.org/?lang=tr

Estados
Unidos

www.hackerwatch.org

Índice remissivo

8

802.11	102
802.11a	102
802.11b	102
802.1x	102

A

Aceder ao mapeamento de rede.....	88
Acerca da McAfee.....	117
Acerca dos tipos de listas de confiança	56
Acerca dos tipos de Protecções do Sistema..	50, 51
Activar Protecções do Sistema	49
Actualizar o mapeamento de rede	88
Actualizar o SecurityCenter	13
adaptador sem fios.....	102
Adaptador sem fios USB.....	102
Adaptadores sem fios PCI.....	102
Aderir à rede gerida.....	90
Aderir a uma rede gerida	91
Agendar uma análise	47
Analisar o computador	34, 59, 60
análise em tempo real.....	102
arquivo.....	102
arquivo integral	103
arquivo rápido	103
atalho	103
ataque de dicionário.....	103
ataque de força bruta	103
ataque de intermediário (man-in-the-middle)	103
autenticação	103

B

biblioteca	103
browser	103

C

cache.....	103
Cavalo de Tróia	103

Ch

chave.....	104
------------	-----

C

cliente	104
cliente de correio electrónico.....	104
Cofre de Palavras-passe.....	104
compressão	104
Configurar a protecção antivírus	41, 59
Configurar actualizações automáticas	14
Configurar opções das Protecções do Sistema	50
Configurar opções de alerta	26
Configurar opções de análise em tempo real	42
Configurar uma rede gerida.....	87
conta de correio electrónico padrão	104
Controlo ActiveX	104
Convidar um computador para aderir à rede gerida.....	91
cookie	104
cópia de segurança.....	104
Copyright	117
Corrigir ou ignorar problemas de protecção ..	8, 17
Corrigir vulnerabilidades de segurança	99

D

DAT	104
Definir localização de análise manual	46
Definir opções de análise manual	44, 45
Desactivar as actualizações automáticas.....	14
Desfragmentar o computador	73
Destruir ficheiros e pastas.....	81
Destruir ficheiros, pastas e discos.....	81
Destruir todo o disco.....	82
DNS	105
domínio.....	105

E

Eliminar uma tarefa do Desfragmentador de Disco	78
Eliminar uma tarefa do QuickClean	76
encriptação.....	105
endereço de correio electrónico.....	105
endereço IP	105
Endereço MAC	105
Erros de Web	105
ESS	105

evento 105

F

Falsificação de IP 106
 ficheiro temporário 106
 filtragem de imagens 106
 firewall 106
 fragmentos de ficheiros 106
 Funcionalidades do Network Manager 84
 Funcionalidades do QuickClean 68
 Funcionalidades do SecurityCenter 6
 Funcionalidades do Shredder 80
 Funcionalidades do VirusScan 33

G

gateway integrado 106
 Gerir a conta McAfee 11
 Gerir a rede de forma remota 95
 Gerir listas de confiança 55
 Gerir um dispositivo 97
 grupo de classificação de conteúdos 106

H

hotspot 106

I

Ignorar problemas de protecção 20
 Ignorar um problema de protecção 20
 Iniciar a protecção anti-spyware 38
 Iniciar a protecção antivírus em tempo real .. 34
 Iniciar a protecção de análise de scripts 38
 Iniciar a protecção de mensagens instantâneas 39
 Iniciar a protecção do correio electrónico 39
 Iniciar o Técnico Virtual 120
 Iniciar protecção adicional 37
 Instalar o software de segurança McAfee em computadores remotos 100
 Internet 107
 Interromper a protecção antivírus em tempo real 35
 intranet 107

L

LAN 107
 largura de banda 107
 launchpad 107
 Licença 118
 Limitações de Acesso 107
 Limpar o computador 69, 71
 lista de confiança 107
 lista de sites bloqueados 107
 lista de sites seguros 107
 localização com monitorização abrangente 108

localizações com monitorização superficial 108
 localizações monitorizadas 108

M

mapeamento de rede 108
 MAPI 108
 marcador 108
 McAfee Network Manager 83
 McAfee QuickClean 67
 McAfee SecurityCenter 5
 McAfee Shredder 79
 McAfee VirusScan 3, 31
 message authentication code (MAC) 108
 Modificar as permissões de um computador gerido 97
 Modificar as propriedades de visualização de um dispositivo 98
 Modificar uma tarefa do Desfragmentador de Disco 77
 Modificar uma tarefa do QuickClean 75
 Monitorizar o estado de protecção de um computador 96
 Monitorizar o estado e as permissões 96
 Mostrar e ocultar alertas informativos 24
 Mostrar ou ocultar alertas informativos 24
 Mostrar ou ocultar alertas informativos durante jogos 25
 Mostrar ou ocultar problemas ignorados 20
 Mostrar ou ocultar um item no mapeamento de rede 89
 MSN 108
 Mudar o nome da rede 89

N

NIC 108
 nó 109
 Noções básicas sobre os ícones do Network Manager 85
 Noções sobre categorias de protecção .. 7, 9, 29
 Noções sobre o estado de protecção 7, 8, 9
 Noções sobre serviços de protecção 10

O

Ocultar alertas de surtos de vírus 27
 Ocultar o ecrã inicial no arranque 26

P

palavra-chave 109
 palavra-passe 109
 Parar de confiar nos computadores da rede .. 93
 Parar de monitorizar o estado de protecção de um computador 96
 partilha 109
 pesquisa a pedido 109

phishing 109
 plug-in 109
 Ponto de Acesso 109
 ponto de acesso não autorizado 109
 ponto de restauro do sistema 110
 POP3..... 110
 pop-ups 110
 porta..... 110
 PPPoE..... 110
 Programar uma tarefa 74
 Programar uma tarefa do Desfragmentador de Disco 77
 Programar uma tarefa do QuickClean 74
 programas potencialmente indesejados (PUPs) 110
 Protecção do Sistema 110
 protocolo..... 110
 proxy..... 110
 publicar..... 110

Q

quarentena 111

R

RADIUS 111
 Reciclagem 111
 recusa de serviço 111
 rede 111
 rede doméstica 111
 rede gerida 111
 Referência 101
 registo 111
 repositório de cópia de segurança online..... 111
 Reproduzir um som com os alertas 26
 Resolução automática de problemas de protecção..... 18
 Resolução de problemas relacionados com protecção..... 8, 18
 Resolução manual de problemas de protecção 19
 restaurar 111
 roaming..... 112
 rootkit 112
 router 112

S

script 112
 segredo partilhado 112
 servidor 112
 Servidor DNS 112
 servidor proxy 112
 sincronizar 113
 smart drive..... 113
 SMTP 113

sobrecarga da memória intermédia 113
 SSID 113
 SSL 113
 Suporte a Clientes e Suporte Técnico 119
 Suporte e Transferências 121

T

texto cifrado 113
 texto simples 113
 tipos de ficheiros monitorizados 113
 TKIP 114
 Tratar ficheiros em quarentena 64, 65
 Tratar programas e cookies em quarentena .. 65
 Tratar programas potencialmente indesejados 64
 Tratar vírus e cavalos de Tróia 64

U

U3 114
 unidade de disco rígido externa 114
 unidade de rede 114
 Unidade USB..... 114
 URL 114
 USB 114
 Utilizar alertas..... 14, 23
 Utilizar listas de confiança..... 55
 Utilizar o mapeamento de rede 88
 Utilizar o SecurityCenter 7
 Utilizar o Técnico Virtual da McAfee 120
 Utilizar opções das Protecções do Sistema... 48
 Utilizar os resultados da análise 63

V

Ver eventos 18, 29
 Ver eventos recentes 29
 Ver os detalhes de um item..... 89
 Ver resultados da análise 60
 Ver todos os eventos 30
 Verificar a existência de actualizações ... 13, 14
 Verifique a subscrição 11
 vírus 114
 VPN 115

W

wardriver..... 115
 Webmail..... 115
 WEP 115
 Wi-Fi..... 115
 Wi-Fi Alliance 115
 Wi-Fi Certified 115
 WLAN 115
 worm 116
 WPA 116
 WPA2 116

WPA2-PSK	116
WPA-PSK	116