Ajuda do Symantec™ Endpoint Protection para cliente Mac - Portuguese - Brazil

December 2020

Como o Symantec Endpoint Protection protege seu Mac

O Symantec Endpoint Protection combina várias camadas de proteção para proteger seu computador contra ataques de vírus e spyware, assim como tentativas de intrusão.

Os Tipos de proteção descrevem cada camada de proteção.

Table 1: Tipos de proteção

Proteção	Descrição
Proteção contra vírus e spyware	O Symantec Endpoint Protection inclui verificações de vírus agendadas, verificações sob demanda e o Auto-Protect, que são executados em segundo plano, fazendo a monitoração em busca de vírus. Quando um vírus for encontrado, o Symantec Endpoint Protection o eliminará. Como a Proteção contra vírus e spyware protege seu Mac
Proteção contra ameaças à rede	O Symantec Endpoint Protection intercepta os dados na camada da rede. Ele usa assinaturas para verificar pacotes ou fluxos de pacotes. Ele verifica cada pacote individualmente procurando padrões que correspondam a ataques à rede ou ao navegador. A Proteção contra ameaças à rede inclui o seguinte: • Prevenção contra intrusões, que detecta ataques a componentes do sistema operacional e à camada do aplicativo. Quando o Symantec Endpoint Protection detectar uma ameaça à rede, ele bloqueará essa ameaça. • Firewall, que permite ou bloqueia o tráfego da rede com base em políticas e regras de firewall. (A partir da versão 14.2.) Como a Proteção contra ameaças à rede protege seu Mac
Controle de dispositivo	Os administradores do Symantec Endpoint Protection Manager configuram uma política de controle do dispositivo. Os dispositivos podem ser bloqueados ou desbloqueados com essa política pelo nome de dispositivo, pelo fornecedor do dispositivo, pelo modelo do dispositivo ou pelo número de série. Em um cliente gerenciado, você pode ver as configurações do Controle de dispositivos na guia **Avançado**. O controle de dispositivo não está disponível para clientes não gerenciados. Sobre o controle de dispositivo no cliente Mac do Symantec Endpoint Protection
Detecção e resposta do endpoint	Os administradores do Symantec Endpoint Protection Manager configuram uma política do Activity Recorder que fornece os meios para detectar e expor atividades suspeitas na rede.

O cliente faz o download automaticamente de definições de vírus, definições do IPS e atualizações do produto para o computador.

Como atualizar as definições de vírus, definições da prevenção contra intrusões e o software cliente

Como a Proteção contra vírus e spyware protege seu Mac

O Symantec Endpoint Protection usa definições de vírus para detectar vírus conhecidos durante verificações agendadas e verificações manuais. O Auto-Protect usa definições de vírus para verificar constantemente sua atividade do computador.

O Symantec Endpoint Protection avisará quando um vírus ou outro risco à segurança for detectado. Um vírus ou outro risco de segurança é detectado quando ocorre uma das seguintes situações:

- O Auto-Protect encontrou um vírus enquanto monitorava o computador.
- O Auto-Protect encontrou um vírus em uma verificação manual ou agendada.

Com as configurações padrão, o Symantec Endpoint Protection tentará reparar automaticamente qualquer vírus encontrado. Se não for possível reparar o arquivo, o cliente manterá o arquivo em quarentena com segurança, de modo que ele não possa danificar o computador. Normalmente, o cliente executa esses reparos sem que você precise executar qualquer ação. Quando seu computador encontrar um vírus, você poderá optar por enviá-lo à Symantec.

Em alguns casos, o cliente solicitará que você escolha entre reparar, excluir ou restaurar um arquivo infectado que ele encontrou. Suas respostas determinam o que o cliente deverá fazer com o arquivo infectado.

Como responder a mensagens sobre detecções de infecções e riscos

Como ativar ou desativar o envio de informações de segurança à Symantec

Como a Proteção contra ameaças à rede protege seu Mac

Proteção contra ameaças à rede inclui as seguintes tecnologias de proteção:

- Prevenção contra intrusões
- Firewall

Prevenção contra intrusões

A prevenção contra intrusões automaticamente detecta e bloqueia ataques à rede. A Prevenção contra intrusões é uma camada interna de defesa para proteger computadores cliente. A prevenção contra intrusões é às vezes chamada de sistema de prevenção contra intrusões (IPS, Intrusion Prevention System).

A prevenção contra intrusões intercepta dados na camada da rede. Ele usa assinaturas para verificar pacotes ou fluxos de pacotes. Ele verifica cada pacote individualmente procurando padrões que correspondam a ataques à rede ou ao navegador. A prevenção contra intrusões detecta ataques a componentes do sistema operacional e à camada do aplicativo.

A prevenção contra intrusões usa assinaturas para identificar ataques em computadores-cliente. Para ataques conhecidos, a prevenção contra intrusões descartará automaticamente os pacotes que corresponderem às assinaturas.

Firewall

O firewall monitora o tráfego na rede e bloqueia o tráfego potencialmente prejudicial para proteger seu Mac. O firewall do Symantec Endpoint Protection não está disponível no cliente não gerenciado.

O firewall do Symantec Endpoint Protection monitora o tráfego na camada de transporte e Internet. O firewall integrado do Mac monitora o tráfego na camada do aplicativo mais alta, depois que o firewall do Symantec Endpoint Protection monitorá-la. Portanto, você pode ativar ambos os firewalls ao mesmo tempo para serem executados em paralelo.

O firewall usa os seguintes tipos de regra para permitir ou bloquear o tráfego da rede:

- Regras padrão
- Regras personalizadas
- Regras integradas
- Regras de proteção

Essas regras incluem detecção de verificação de porta, detecção de negação de serviço, antispoofing de MAC, DHCP inteligente e DNS inteligente. As configurações de firewall são totalmente controladas pelo administrador do Symantec Endpoint Protection Manager. Você poderá ativar ou desativar o firewall somente se o administrador permitir o controle de cliente do usuário no Mac.

A proteção de firewall foi adicionada à versão 14.2.

Como gerenciar a prevenção contra intrusões

Como gerenciar a proteção de firewall para o cliente Mac

Compatibilidade do sistema operacional com o Symantec Endpoint Protection para Mac

O Symantec Endpoint Protection para Mac oferece suporte às seguintes versões do sistema operacional:

- macOS 12
- macOS 11 (processador Intel e chip M1)
- macOS 10.15 a 10.15.7

Para obter informações adicionais sobre o suporte a versões anteriores do sistema operacional Mac, consulte Mac compatibility with the Endpoint Protection client (em inglês).

Sobre a autorização de extensões do sistema para o Symantec Endpoint Protection para macOS 10.15 ou posterior

Notas de versão, novas correções e requisitos do sistema para todas as versões do Endpoint Protection

Para instalar o cliente do Symantec Endpoint Protection para Mac

É possível instalar um cliente do Symantec Endpoint Protection diretamente em um computador Mac caso você não possa ou não queira usar a instalação remota por envio. As etapas são similares para clientes gerenciados e não gerenciados.

A única maneira de instalar um cliente gerenciado por meio de um pacote criado pelo Symantec Endpoint Protection Manager. Você pode converter um cliente não gerenciado em cliente gerenciado a qualquer momento importando as configurações de comunicação do servidor-cliente no cliente Mac.

NOTE

A fim de preparar o cliente do Symantec Endpoint Protection para Mac para uso com software de implementação remota de terceiros, consulte:

Como exportar e implementar um cliente do Symantec Endpoint Protection pelo Casper ou pela área de trabalho remota da Apple.

Table 2: Métodos para instalar o cliente para o Mac

Se você tiver feito download do arquivo de instalação.	1. Extraia o conteúdo em uma pasta de um computador Mac e, em seguida, abra-a. 2. Abra `SEP_MAC`. 3. Copie `Symantec Endpoint Protection.dmg` na área de trabalho do computador Mac. 4. Clique duas vezes em `Symantec Endpoint Protection.dmg` para montar o arquivo como um disco virtual. Em seguida, instale o cliente do Symantec Endpoint Protection para Mac
Se você tiver um pacote .zip de instalação de cliente do Portal de suporte da Broadcom. Para obter mais informações, consulte: Portal de suporte da Broadcom	1. Copie o arquivo na área de trabalho do computador Mac. O arquivo pode ser denominado `Symantec Endpoint Protection.zip` ou `Symantec_Endpoint_Protection_versão_Mac_Client.zip`, em que versão é a versão do produto. 2. Clique com o botão direito do mouse em **Abrir com > Utilitário de arquivamento** para extrair o conteúdo do arquivo. 3. Abra a pasta resultante. Depois, instale o cliente do Symantec Endpoint Protection para Mac.

A imagem do disco virtual ou a pasta resultante contem o instalador do aplicativo e uma pasta chamada Recursos adicionais. Ambos os itens devem estar presentes no mesmo local para uma instalação com êxito. Se você copiar o instalador a outro local, deverá também copiar os Recursos adicionais.

Para instalar o cliente do Symantec Endpoint Protection para Mac:

1. Clique duas vezes em `Instalar Symantec Endpoint Protection`.
2. Para começar a instalação, clique em **Instalar**.
3. Para instalar uma ferramenta auxiliar necessária para a instalação do cliente do Symantec Endpoint Protection, digite o nome de usuário e a senha do administrador do Mac e clique em **Instalar Auxiliar**.
4. Após a instalação, clique em **Continuar** para concluir a configuração do cliente do Symantec Endpoint Protection.
5. Para configurar o cliente do Symantec Endpoint Protection, execute as seguintes etapas:

Autorize a extensão do sistema do Symantec Endpoint Protection.	Na caixa de diálogo **Segurança e Privacidade**, guia **Geral**, em **O software de sistema do aplicativo "Symantec Endpoint Protection" não pôde ser carregado**, clique em **Permitir**. Se necessário, clique no ícone de bloqueio para fazer as alterações. É necessário autorizar a extensão do sistema para que o Symantec Endpoint Protection funcione corretamente. Consulte: Sobre a autorização de extensões do sistema para o Symantec Endpoint Protection para macOS 10.15 ou posterior
Permita o acesso completo ao disco.	Na caixa de diálogo **Segurança e Privacidade**, na guia **Privacidade**, verifique se a **Symantec System Extension** tem permissão para acessar os dados e as configurações administrativas para todos os usuários do dispositivo Mac. Se necessário, clique no ícone de bloqueio para fazer as alterações.
Permita alterações no perfil de rede.	Quando a mensagem **Symantec Endpoint Protection Deseja Filtrar Conteúdo da Rede** for exibida, clique em **Permitir**.

6. Clique em **Concluído**.

Sobre a autorização de extensões do sistema para o Symantec Endpoint Protection para macOS 10.15 ou posterior

A solicitação de autorização de extensões do sistema é um recurso de segurança do macOS 10.15.É necessário autorizar a extensão do sistema para que o Symantec Endpoint Protection funcione corretamente.

Para autorizar a extensão do sistema para o Symantec Endpoint Protection, durante a configuração do seu cliente do Symantec Endpoint Protection, na caixa de diálogo **Segurança e Privacidade**, guia **Geral**, em **O software de sistema do aplicativo "Symantec Endpoint Protection" não pôde ser carregado**, clique em **Permitir**.

Para obter mais informações, consulte:

Como instalar o cliente do Symantec Endpoint Protection para Mac

Solicitação de upgrade para o cliente Mac do Symantec Endpoint Protection

Os administradores do Symantec Endpoint Protection Manager podem atribuir um pacote de instalação do cliente para fazer upgrade automaticamente dos computadores cliente gerenciados, com configurações para a instalação do cliente.

Se estiver conectado no Mac, você poderá ver uma solicitação de reiniciar para concluir a instalação. Você talvez possa atrasar a reinicialização com base nas configurações de instalação do cliente.

Se você não estiver conectado no Mac, a instalação reinicia automaticamente o Mac.

Guia de introdução ao cliente do Symantec Endpoint Protection

Quando o cliente do Symantec Endpoint Protection é aberto, a mensagem **You are Protected** é exibida na parte superior da página, a menos que haja um problema que precise ser resolvido. Clique em **Corrigir** para solucionar qualquer problema.

O cliente do Symantec Endpoint Protection exibe as tarefas principais que você pode executar.

Table 3: Páginas do cliente do Symantec Endpoint Protection

Opção	Descrição
Segurança	Mostra o status da proteção do seu computador.
Verificações	Permite verificar o computador. Você pode optar por executar uma verificação rápida ou completa. Também é possível arrastar e soltar um arquivo ou uma pasta para verificação. Como executar uma verificação manual
LiveUpdate	Executa o LiveUpdate para atualizar as definições e arquivos do produto do Symantec Endpoint Protection. Como atualizar o conteúdo no Symantec Endpoint Protection imediatamente
Avançado	Oferece opções mais detalhadas para a Proteção contra vírus e spyware, a Proteção contra ameaças à rede e o LiveUpdate.

Para gerenciar a proteção do Mac com o Symantec Endpoint Protection

As configurações padrão do Symantec Endpoint Protection protegem seu Mac contra muitos tipos de malware. O cliente controla automaticamente o malware ou permite a você escolher como controlar o malware.

Dependendo das configurações que seu administrador definir, você deverá executar as seguintes tarefas para ajudar a manter sua proteção.

NOTE
Seu administrador pode não ter lhe dado controle sobre essas tarefas.

Table 4: Para proteger seu computador

Etapas	Descrição
Etapa 1: verifique se a Proteção contra vírus e spyware e a Proteção contra ameaças à rede estão ativadas.	A página **Segurança** será exibida e mostrará uma marca de seleção verde e a mensagem **You are Protected** se as proteções estiverem ativadas. Para ativar e desativar a Proteção contra vírus e spyware Como ativar ou desativar a Proteção contra ameaças à rede
Etapa 2: certifique-se de que o software e as definições estejam atualizados.	A página **Segurança** exibe a hora da última atualização das definições da Proteção contra vírus e spyware e da Proteção contra ameaças à rede. Em **LiveUpdate**, a hora da última atualização do produto é exibida. Para ver o número da versão do software, clique em **Ajuda > Sobre**.
Etapa 3: atualize o software ou as definições, se necessário.	No cliente do Symantec Endpoint Protection, clique em **LiveUpdate** para atualizar o software e as definições imediatamente. Como atualizar as definições de vírus, definições da prevenção contra intrusões e o software cliente
Etapa 4: execute uma verificação.	Você pode agendar a execução da verificação em intervalos regulares, ou executar uma verificação imediatamente. Como configurar verificações agendadas Como executar uma verificação manual

Como gerenciar as configurações da Proteção contra vírus e spyware

Renovando sua licença de produto

No ícone do cliente Symantec Endpoint Protection, na barra de menus, você poderá ver uma mensagem de que essa licença para o Symantec Endpoint Protection expirou. O cliente do Symantec Endpoint Protection usa uma licença para atualizar o seguinte:

- O software do cliente
- Os arquivos com as definições de proteção para verificações de vírus e spyware e prevenção contra intrusões

O cliente pode usar uma licença de teste ou uma licença paga. Se uma dessas licenças estiver expirada, o cliente não atualizará as definições nem o software-cliente.

Para ambos os tipos de licença, é necessário entrar em contato com seu administrador para atualizar ou renovar a licença.

Como responder a mensagens sobre detecções de infecções e riscos

Ativando ou desativando o controle de dispositivos no cliente do Symantec Endpoint Protection para Mac

Os administradores do Symantec Endpoint Protection Manager podem configurar clientes gerenciados com uma política de controle do dispositivo. Os dispositivos podem ser bloqueados ou desbloqueados com essa política pelo nome de dispositivo, pelo fornecedor do dispositivo, pelo modelo do dispositivo ou pelo número de série.

Você pode exibir as atividades de controle de dispositivos na página **Avançado** clicando em **Atividade > Security History**.

As configurações no cliente do Symantec Endpoint Protection para o **Controle de dispositivos** permitem ativar ou desativar essa opção. Se o controle de dispositivo estiver ativado, você poderá opcionalmente ativar ou desativar notificações quando os dispositivos forem bloqueados ou desbloqueados.

Para mudar as configurações, você deve fazer a autenticação com credenciais de administrador do Mac. Se essas configurações estiverem esmaecidas, significa que o administrador as bloqueou para impedir que você ative ou desative esse recurso.

Você não pode adicionar ou editar os dispositivos para serem bloqueados ou desbloqueados através da interface do cliente Symantec Endpoint Protection.

NOTE
A política de controle do dispositivo do Symantec Endpoint Protection Manager controla as configurações do controle de dispositivo. Na pulsação seguinte, todas as mudanças que você fizer a essas configurações reverterão ao que a política dita.

O controle de dispositivo não está disponível para clientes não gerenciados.

Sobre o Proteção de acesso a web e nuvem para cliente Mac

O Proteção de acesso a web e nuvem automatiza o redirecionamento de tráfego da web para o Symantec Web Security Service e protege o tráfego em cada computador que usa o Symantec Endpoint Protection.

O administrador controla as configurações usadas pelo Proteção de acesso a web e nuvem, que inclui o URL de configuração de proxy e o certificado raiz opcional do Symantec Web Security Service. Apenas o administrador do Symantec Endpoint Protection Manager pode definir essas configurações, que não aparecem na interface do cliente Symantec Endpoint Protection. Você pode exibir o URL do arquivo de configuração de proxy no Mac em **Preferências do Sistema > Rede**, em **Proxies**. O certificado de serviços na nuvem aparece em **Chaves**.

Os navegadores Safari, Chrome e Firefox versão 65 e posteriores suportam o Proteção de acesso a web e nuvem. As versões do Symantec Endpoint Protection anteriores à 14.2 RU1 só dão suporte ao Safari e ao Chrome.

NOTE
O método de encapsulamento não é executado em clientes Mac.

Para desinstalar o cliente do Symantec Endpoint Protection para Mac

Desinstale o cliente do Symantec Endpoint Protection para Mac por meio do ícone do cliente na barra de menus. A desinstalação do cliente do Symantec Endpoint Protection para Mac exige credenciais de usuário administrativas.

NOTE
Após desinstalar o cliente do Symantec Endpoint Protection, você será solicitado a reiniciar o computador cliente para concluir a desinstalação. Certifique-se de salvar todo o trabalho inacabado ou fechar todos os aplicativos abertos antes de começar.

Como desinstalar o cliente do Symantec Endpoint Protection para Mac

1. No computador cliente Mac, abra o cliente do Symantec Endpoint Protection e clique em **Symantec Endpoint Protection > Desinstalar Symantec Endpoint Protection**.
2. Clique em **Desinstalar** novamente para começar a desinstalação.
3. Para instalar uma ferramenta auxiliar necessária à desinstalação do cliente do Symantec Endpoint Protection, digite o nome de usuário e a senha do administrador do Mac e clique em **Instalar Auxiliar**.
4. Na caixa de diálogo **Symantec Endpoint Protection está tentando modificar uma Extensão do Sistema**, digite o nome de usuário e a senha de administrador do Mac e, em seguida, clique em **OK**.

   Você também pode ser solicitado a digitar uma senha para desinstalar o cliente. Essa senha pode ser diferente da senha administrativa do Mac.
5. Uma vez que a desinstalação tenha sido concluída, clique em **Reiniciar Agora**.

Se a desinstalação falhar, talvez seja necessário usar um método alternativo para desinstalá-lo. Consulte:

Desinstalar o Symantec Endpoint Protection

Como atualizar as definições de vírus, definições da prevenção contra intrusões e o software cliente

Os produtos da Symantec dependem das informações atualizadas para proteger o computador contra ameaças recém-descobertas. A Symantec disponibiliza essas informações para o Symantec Endpoint Protection através do LiveUpdate. O LiveUpdate usa a conexão à Internet para obter atualizações do produto e das definições para o computador.

As atualizações de definição são os arquivos que mantêm seus produtos da Symantec atualizados com as tecnologias mais recentes de proteção contra ameaças. O LiveUpdate recupera as novas assinaturas de prevenção contra intrusões ou os arquivos de definição de vírus por um site da Symantec na internet e depois substitui os arquivos antigos.

As atualizações do produto são melhorias no cliente instalado. As atualizações do produto são criadas geralmente para estender a compatibilidade do sistema operacional ou do hardware, para ajustar problemas de desempenho ou para corrigir erros do produto. As atualizações do produto são lançadas de acordo com as necessidades. O cliente recebe atualizações do produto diretamente de um servidor do LiveUpdate. As atualizações de produto e de definições juntas são chamadas de atualizações de conteúdo.

Table 5: Maneiras de atualizar o conteúdo em seu computador

Tarefa	Descrição
Atualizar o conteúdo imediatamente	Você pode executar o LiveUpdate imediatamente. Como atualizar o conteúdo no Symantec Endpoint Protection imediatamente
Atualizar o conteúdo em um agendamento	Por padrão, o LiveUpdate é executado automaticamente em intervalos agendados. Para atualizar o conteúdo no Symantec Endpoint Protection em um agendamento

Como gerenciar a proteção do Mac com o Symantec Endpoint Protection

Como atualizar o conteúdo no Symantec Endpoint Protection imediatamente

Você pode atualizar imediatamente as definições e os arquivos do produto através do LiveUpdate. Você deve executar o LiveUpdate manualmente pelas seguintes razões:

- O software-cliente foi instalado recentemente.
- A última verificação foi executada há muito tempo.
- Você suspeita de que tenha um vírus ou outro problema de malware.

Para atualizar o conteúdo no Symantec Endpoint Protection imediatamente:

Inicie o LiveUpdate de uma das seguintes maneiras:

- Clique com o botão direito do mouse no ícone do Symantec Endpoint Protection na barra de menus e, em seguida, clique em **LiveUpdate**.
- Abra o cliente do Symantec Endpoint Protection e, em seguida, clique em **LiveUpdate**.

O LiveUpdate conecta-se ao servidor configurado do LiveUpdate, procura as atualizações disponíveis e, em seguida, faz o download e instala as atualizações automaticamente. Uma barra de status indica o andamento do download.

Para atualizar o conteúdo no Symantec Endpoint Protection em um agendamento

Como atualizar as definições de vírus, definições da prevenção contra intrusões e o software cliente

Para atualizar o conteúdo no Symantec Endpoint Protection em um agendamento

Agendamentos em clientes Mac gerenciados

Por padrão, os clientes Mac gerenciados recebem um agendamento do Symantec Endpoint Protection Manager que executa o LiveUpdate a cada quatro horas. O administrador do Symantec Endpoint Protection Manager controla o agendamento. Os clientes gerenciados não podem remover, modificar nem exibir o agendamento criado pelo administrador nem criar um agendamento.

Agendamentos em clientes Mac não gerenciados

É possível criar um agendamento para que o LiveUpdate seja executado automaticamente em intervalos agendados. Convém agendar a execução do LiveUpdate durante um período em que você não usa seu computador.

Para atualizar o conteúdo do Symantec Endpoint Protection em um agendamento:

1. No cliente do Symantec Endpoint Protection, na página **Avançado**, clique em **Configurações do produto** e, em seguida, clique no ícone para configurar o **LiveUpdate programado**.

   Seu agendamento atual aparecerá.

2. Selecione um intervalo no menu suspenso Agendamento do LiveUpdate.

   A configuração inicial está definida para ser executada a cada **4** horas. Você também pode optar pela execução **diária** ou **semanal**, selecionando uma hora ou uma data e hora, respectivamente.

3. Clique em **Apply Changes**.

Como atualizar o conteúdo no Symantec Endpoint Protection imediatamente

Como atualizar as definições de vírus, definições da prevenção contra intrusões e o software cliente

Sobre a conexão com o servidor de gerenciamento por meio de um servidor proxy

Pode ser solicitado que você permita que o Symantec Endpoint Protection use suas credenciais para se conectar ao servidor de gerenciamento através de um proxy. Você recebe uma mensagem perguntando se deseja permitir o acesso às suas credenciais para o processo `symdaemon`.

Na mensagem, clique em **Permitir sempre**. Caso contrário, você continuará recebendo a mesma mensagem sempre que o cliente se comunicar com o servidor do LiveUpdate. Se você clicar em **Negar**, seu cliente não poderá receber atualizações de software ou definições.

Como atualizar as definições de vírus, definições da prevenção contra intrusões e o software cliente

Como gerenciar as configurações da Proteção contra vírus e spyware

Por padrão, o Symantec Endpoint Protection protege contra vírus e riscos à segurança, inclusive contra ameaças à rede, assim que seu computador é iniciado. A Proteção contra vírus e spyware inclui o Auto-Protect, que verifica se há vírus nos programas enquanto eles são executados. Ele também monitora seu computador durante atividades que podem indicar a presença de vírus ou de riscos à segurança. A interceptação do Auto-Protect impede que os vírus infectem seu computador, e você deve manter o Auto-Protect ativado.

Para clientes gerenciados, a quantidade de controle que você tem sobre estas configurações depende de como o administrador configurou o cliente. Além disso, todas as mudanças que você fizer a estas configurações podem ser revertidas ao que a política ditar na pulsação seguinte.

A Gerenciamento da proteção contra vírus e spyware descreve as tarefas que você pode realizar para gerenciar a Proteção contra vírus e spyware em seu Mac.

Table 6: Como gerenciar a proteção contra vírus e spyware

Etapas	Descrição
Etapa 1: ative ou desative a Proteção contra vírus e spyware	Você pode ativar e desativar a Proteção contra vírus e spyware com facilidade. A Symantec recomenda que você a deixe ativada. Para ativar e desativar a Proteção contra vírus e spyware
Etapa 2: personalize as configurações do Auto-Protect	O Auto-Protect é uma parte importante da Proteção contra vírus e spyware. Você pode configurar essas opções na página **Avançado**. Como configurar as definições do Auto-Protect e da Zona de Verificação
Etapa 3: verifique se há vírus no computador	Você pode configurar as verificações de vírus para que sejam executadas conforme um agendamento ou imediatamente. Como configurar verificações agendadas Para pausar, pausar intermitentemente, e interromper verificações Como executar uma verificação manual
Etapa 4: responda quando o Symantec Endpoint Protection detectar um vírus	Quando o Symantec Endpoint Protection verifica o computador, ele pode: • Notificar sobre as ações que você pode executar. • Informar sobre as ações de proteção executadas para você. Como responder a mensagens sobre detecções de infecções e riscos

Para ativar e desativar a Proteção contra vírus e spyware

Por padrão, a Proteção contra vírus e spyware está ativada juntamente com o Auto-Protect.

Você pode exercer um controle mais preciso sobre o Auto-Protect definindo opções específicas.

Se a Proteção contra vírus e spyware for desativada, um "x" vermelho aparecerá na página **Status** com a mensagem **Proteção contra vírus e spyware desativada**. Se a proteção estiver desativada, você deverá ativá-la assim que possível.

> **NOTE**
> As verificações agendadas continuam, independentemente da ativação ou desativação da Proteção contra vírus e spyware. Seu administrador pode restringir o acesso a algumas configurações do Symantec Endpoint Protection. Você pode não ter permissão para desativar essas configurações, agendar verificações ou

personalizar opções de proteção.A sua senha de administrador do Mac pode ser solicitada para alterar quaisquer dessas configurações.

Para ativar e desativar a Proteção contra vírus e spyware:

1. Para ativar a Proteção contra vírus e spyware, no cliente do Symantec Endpoint Protection, na página **Avançado**, clique em **Protect My Mac** e, em seguida, ative a opção **Automatic Scans**.
2. Para desativar a Proteção contra vírus e spyware, no cliente do Symantec Endpoint Protection, na página **Avançado**, clique em **Protect My Mac** e, em seguida, desative a opção **Automatic Scans**.

Como configurar as definições do Auto-Protect e da Zona de Verificação

Como gerenciar as configurações da Proteção contra vírus e spyware

Como responder a mensagens sobre detecções de infecções e riscos

Para configurar as definições do Auto-Protect e da Zona de Verificação

Em clientes gerenciados, se seu administrador permitir, você poderá personalizar o modo pelo qual o Auto-Protect monitora vírus e repara arquivos infectados.

As configurações de proteção automática são exibidas como opções em **Protect My Mac**. Você deve ativar as **Automatic Scans** para ativar o Auto-Protect.

As **Configurações de zonas de verificação** permitem especificar os arquivos que devem ser incluídos ou excluídos de uma verificação.

Para configurar as definições do Auto-Protect:

1. No cliente do Symantec Endpoint Protection, na página **Avançado**, clique em **Protect My Mac** e, em seguida, clique no ícone para configurar as **Automatic Scans**.
2. Faça modificações em quaisquer das seguintes opções:

Quarentena automática	Você pode optar por enviar todos os arquivos que não puderem ser reparados para a quarentena.
Reparo automático	Você pode optar por fazer com que o Auto-Protect repare automaticamente todos os arquivos infectados que encontrar.
Verificar	Você pode escolher **Discos de dados** e **Todos os outros discos**.
Verificar arquivos compactados	Você pode optar por incluir arquivos compactados em uma verificação do Auto-Protect. A verificação inclui o arquivo compactado e os arquivos dentro do arquivo compactado.

WARNING
Se não selecionar **Reparo automático**, nenhum arquivo infectado será movido para a Quarentena, mesmo se você escolher **Colocar em quarentena automaticamente**.O software pergunta se você deseja reparar um arquivo infectado. Se você não reparar o arquivo, ele será deixado no computador. Se você selecionar **Reparo automático** e não selecionar **Quarentena automática**, qualquer arquivo infectado será excluído.

3. Clique em **Concluído**.

Para configurar as Configurações de zonas de verificação:

1. No cliente do Symantec Endpoint Protection, na página **Avançado**, clique em **Protect My Mac** e, em seguida, clique no ícone das **Configurações de zonas de verificação**.
2. Faça modificações em quaisquer das seguintes opções:

Verificar tudo	Todos os arquivos e processos em seu computador serão verificados quando você os acessar.
Verificar apenas	Apenas os arquivos ou pastas que você especificar serão incluídos na verificação.
Não verificar	Todos os arquivos serão verificados, com exceção dos arquivos ou pastas que você especificar para excluir da verificação.
Usar padrões	Essa opção verifica tudo.

3. Clique em **OK**.

Como a Proteção contra vírus e spyware protege seu Mac

Para ativar e desativar a Proteção contra vírus e spyware

Como gerenciar arquivos em quarentena

Para configurar verificações agendadas

O Symantec Endpoint Protection executa uma verificação padrão automaticamente se você tiver um cliente gerenciado. Se o administrador permitir, você poderá configurar verificações agendadas adicionais.

Em um cliente não gerenciado, você deve executar suas próprias verificações.A Symantec recomenda executar uma verificação manual completa o quanto antes e depois configurar uma verificação agendada regular. É possível pausar ou adiar qualquer verificação, tanto a verificação agendada quanto a manual.

Em um cliente gerenciado, as verificações padrão são executadas diariamente às 8:00 da manhã com o Reparo automático ativado.

> **NOTE**
> A Symantec não recomenda executar uma verificação agendada mais de uma vez por dia. Aumentar a frequência das verificações ou configurar várias verificações agendadas pode causar problemas de desempenho.

Como executar uma verificação manual

Para configurar verificações agendadas:

1. No cliente do Symantec Endpoint Protection, na página **Avançado**, clique em **Protect My Mac** e, em seguida, clique no ícone para configurar as **Verificações agendadas**.
2. Na caixa de diálogo, clique em **Adicionar verificações agendadas** ou clique em uma verificação agendada atual e depois clique em **Editar** para ajustar as configurações para ele.
3. Na guia **Itens de verificação**, você pode definir as seguintes opções:

Unidades	Você pode escolher se **Discos rígidos** e **Unidades removíveis** devem ser verificados.
Pastas	Você pode optar por verificar sua **Pasta pessoal (Usuário ativo)**, seus **Aplicativos** e arquivos de **Bibliotecas**. Se nenhum usuário estiver conectado no momento da verificação agendada de uma pasta Início, a verificação não será executada.

Opções de verificação	Selecione dentre as seguintes opções: • **Verificar compactado** • **Reparo automático** • **Quarentena automática** • **Ativar a verificação durante tempo ocioso**

4. Na guia **Agendamento da verificação**, você pode definir as seguintes opções:

Agendamento de verificação	Você pode configurar a execução de uma verificação em um intervalo específico em horas, diariamente, semanalmente ou mensalmente. **Executar em um intervalo específico** está selecionado por padrão durante o agendamento de uma nova verificação.
Executar a cada	Disponível quando a opção **Executar em intervalo específico** estiver selecionada para **Agendamento da verificação**.
Hora de início	Disponível quando você selecionar **Diariamente**, **Semanalmente** ou **Mensalmente** para o agendamento de verificação. É possível escolher a hora do dia para executar a verificação. Você deve escolher uma hora na qual você não esteja normalmente no trabalho, porque as verificações podem reduzir o desempenho do computador.
Ativado	Disponível quando você selecionar **Semanalmente** ou **Mensalmente** para o agendamento de verificação. Você pode escolher o dia da semana ou o mês para executar a verificação. Recomendamos que você escolha uma hora na qual você não esteja normalmente no trabalho, porque as verificações podem reduzir o desempenho do computador.

5. Na guia **Ajuste**, é possível ajustar a maneira como o desempenho da verificação é otimizado.
6. Clique em **OK**.
7. Clique em **Concluído**.

Para pausar, pausar intermitentemente, e interromper verificações

Como gerenciar a proteção do Mac com o Symantec Endpoint Protection

Como responder a mensagens sobre detecções de infecções e riscos

Como ativar ou desativar o envio de informações de segurança à Symantec

Para executar uma verificação manual

Poderá ser necessário verificar alguns arquivos manualmente. Por exemplo, poderá ser necessário verificar os arquivos que foram salvos em seu computador antes da instalação do Symantec Endpoint Protection. Você poderá também decidir que alguns arquivos que foram excluídos em uma verificação agendada devem ser verificados.

NOTE
É possível pausar ou adiar qualquer verificação, tanto a verificação agendada quanto a manual.

Para executar uma verificação manual:

No cliente do Symantec Endpoint Protection, na página **Verificações**, proceda de uma das seguintes maneiras:

- Para iniciar uma verificação rápida, clique em **Quick Scan** e, em seguida, clique em **Start a Quick Scan**.
- Para iniciar uma verificação completa, clique em **Verificação completa** e, em seguida, clique em **Start a Full Scan**.
- Para verificar um arquivo ou uma pasta, clique em **File Scan** e, em seguida, clique em **Selecionar arquivo**.O Finder será aberto e você poderá escolher se deseja **Mostrar arquivos ocultos** e **Verificar arquivos compactados**. Você também pode optar por ativar o **Reparo automático** e a **Quarentena automática**.

Para pausar, pausar intermitentemente, e interromper verificações

Como configurar verificações agendadas

Como ativar ou desativar o envio de informações de segurança à Symantec

Para pausar, pausar intermitentemente, e interromper verificações

O recurso de pausa permite interromper uma verificação e retomá-la em outro momento de sua preferência. Você também pode interromper e cancelar uma verificação a qualquer momento. Não são necessários privilégios de administrador para usar esses recursos.

Quando uma verificação é retomada, ela inicia do ponto onde foi interrompida.

> **NOTE**
> Se você interromper uma verificação enquanto um computador cliente estiver verificando um arquivo compactado, ele poderá levar alguns minutos para responder ao pedido de pausa.

Se a pausa intermitente estiver ativada, você também poderá pausar uma verificação intermitentemente, mas somente antes do início da verificação. Você não poderá pausar intermitentemente uma verificação em andamento.

Para pausar ou parar uma verificação agendada em execução:

1. Na caixa de diálogo de andamento da verificação, clique em **Pausar**.
2. Na caixa de diálogo de andamento da verificação, clique em **Retomar** para continuar a verificação, ou em **Parar** para interromper a verificação. Você também pode clicar em **Concluído** para fechar a janela.

Para pausar ou interromper uma verificação manual:

1. Na caixa de diálogo de andamento da verificação, clique em **Pausar** para pausar a verificação.
2. Clique em **Cancelar** para parar uma verificação manual em andamento, ou em **Retomar** para continuar a verificação.

Para pausar intermitentemente uma verificação prestes a ser iniciada:

1. Na janela que aparecer, clique no menu suspenso para selecionar um valor da pausa intermitente. Você pode pausar intermitentemente por no mínimo 15 minutos ou no máximo um dia.
2. Clique em **OK** para pausar intermitentemente a verificação.

   Você não precisa executar outras ações se você quiser que a verificação seja executar conforme agendada.

Como configurar verificações agendadas

Como executar uma verificação manual

Para responder a mensagens sobre detecções de infecções e riscos

Você poderá verificar se seu computador está infectado e executar algumas tarefas adicionais se quiser maior segurança ou melhor desempenho.

O administrador pode gerenciar o cliente ou você pode executar um cliente não gerenciado. As tarefas de proteção que você poderá executar dependem do nível de controle que seu administrador mantém sobre o cliente.

Se o Symantec Endpoint Protection encontrar um vírus ou um risco à segurança, você poderá ser solicitado a tomar uma ação quanto ao risco. De acordo com as configurações que seu administrador escolher, você poderá ser informado sobre a ação realizada pelo cliente automaticamente.

Table 7: Para responder a mensagens sobre infecções

Conteúdo da mensagem	Ação necessária
Arquivo infectado foi reparado	Nenhuma
Solicita sua aprovação para reparar o arquivo infectado	Aprove a reparação. Essa opção depende das preferências de seu Auto-Protect. Como gerenciar as configurações da Proteção contra vírus e spyware Se a opção de reparar os arquivos infectados automaticamente estiver desmarcada, será necessário reparar o arquivo manualmente. Para reparar arquivos infectados
Não foi possível reparar o arquivo infectado	Gerencie a infecção na Quarentena. Como gerenciar arquivos em quarentena

Como a Proteção contra vírus e spyware protege seu Mac

Para reparar arquivos infectados

Se um arquivo infectado não for automaticamente reparado ou colocado em Quarentena, você poderá reparar o arquivo através da lista de resultados da verificação. Você pode reparar arquivos manualmente no disco rígido do computador ou em mídia removível.

Para reparar arquivos infectados:

1. Na lista de resultados de verificação, selecione o arquivo a ser reparado e então clique em **Reparar**.

   Você também pode clicar com o botão direito do mouse em qualquer arquivo no menu **Finder** ou **Pesquisar** do Mac.
2. Repita conforme necessário.
3. Execute outra verificação para identificar outros arquivos infectados.
4. Verifique os arquivos reparados para ter certeza de que eles funcionam corretamente.

Como gerenciar as configurações da Proteção contra vírus e spyware

Como gerenciar arquivos em quarentena

Como gerenciar arquivos em quarentena

Por padrão, se o cliente detectar um vírus em um arquivo, ele tentará removê-lo. Se o vírus não puder ser removido, o arquivo será colocado na Quarentena do computador. Se o Symantec Endpoint Protection detectar um risco à segurança em um arquivo, primeiro ele colocará o arquivo em Quarentena. Em seguida, ele vai reparar qualquer efeito colateral do risco.

Quando você atualizar suas definições de vírus, o cliente verificará automaticamente a Quarentena. Você pode repetir a verificação dos itens na Quarentena. As definições mais recentes podem ser capazes de limpar ou reparar os arquivos em quarentena.

Para gerenciar arquivos em quarentena:

1. No cliente do Symantec Endpoint Protection, na página **Avançado**, clique em **Atividade > Security History > Quarentena**.
2. Selecione o arquivo a ser gerenciado e então escolha a opção apropriada:

Reparar	Escolha essa opção para tentar reparar um arquivo em quarentena. Certifique-se de que suas definições de vírus são mais recentes que a data do arquivo em quarentena.
Excluir	Escolha essa opção para excluir quaisquer arquivos da Quarentena que não são mais necessários.
Restaurar	Se tiver certeza de que o arquivo não contém um vírus, você poderá restaurá-lo para o local original no computador. Essa opção não verifica o arquivo nem tenta repará-lo.

Como responder a mensagens sobre detecções de infecções e riscos

Para ativar ou desativar o envio de informações de segurança à Symantec

O Symantec Endpoint Protection pode enviar à Symantec informações pseudoanonimizadas sobre as ameaças detectadas. A Symantec usa essas informações para proteger seus computadores cliente contra ameaças novas, direcionadas e polimórficas. Todos os dados que você enviar melhorarão a capacidade da Symantec de responder a ameaças e personalizar a proteção para seu computador.

Os dados que a telemetria da Symantec coleta podem incluir elementos pseudoanônimos que não são diretamente identificáveis. A Symantec não precisa nem busca usar dados de telemetria para identificar usuários individualmente.

Por padrão, seu computador cliente envia as informações sobre detecções para a Symantec. Você pode desativar o envio, mas a Symantec recomenda deixar essa configuração ativada.

Esta opção apenas envia informações sobre detecções de vírus.

NOTE
A Symantec recomenda que você deixe a opção ativada.

Para ativar ou desativar o envio de informações de segurança pseudoanônimas à Symantec:

No cliente do Symantec Endpoint Protection, na página **Avançado**, clique em **Product Settings** e, em seguida, ative ou desative a opção **Security Info Submission**.

Como configurar verificações agendadas

Como executar uma verificação manual

Para gerenciar a prevenção contra intrusões

As configurações padrão da prevenção contra intrusões protegem seu cliente Mac. Porém, se preferir gerenciar sua própria proteção, você poderá gerenciar a prevenção contra intrusões como parte da Proteção contra ameaças à rede.

Table 8: Para gerenciar a prevenção contra intrusões

Etapas	Descrição
Etapa 1: saiba mais sobre a prevenção contra intrusões.	Aprenda como a prevenção contra intrusões detecta e bloqueia ataques à rede. Como a Proteção contra ameaças à rede protege seu Mac
Etapa 2: faça download das assinaturas IPS mais recentes.	Por padrão, o download das assinaturas mais recentes é feito no cliente. No entanto, convém fazer download das assinaturas imediatamente. Como atualizar o conteúdo no Symantec Endpoint Protection imediatamente
Etapa 3: ative ou desative a prevenção contra intrusões.	Convém desativar a prevenção contra intrusões para fins de solução de problemas ou se os computadores-cliente detectarem um número excessivo de falsos positivos. Normalmente, você não deve desativar a prevenção contra intrusões. Como ativar ou desativar a Proteção contra ameaças à rede
Etapa 4: ative as notificações da prevenção contra intrusões.	É possível configurar as notificações para serem exibidas quando o Symantec Endpoint Protection detectar um ataque. Para ativar ou desativar as notificações da Proteção contra ameaças à rede

Como gerenciar a proteção de firewall para o cliente Mac

O firewall do Symantec Endpoint Protection para Mac fornece uma proteção de firewall que se integra totalmente ao Symantec Endpoint Protection, incluindo eventos, políticas e comandos. O firewall do Symantec Endpoint Protection somente está disponível em clientes gerenciados.

> **NOTE**
> O firewall do Symantec Endpoint Protection para Mac não se integra ao firewall integrado do sistema operacional. Em vez disso, ele é executado em paralelo. O firewall do sistema operacional inspeciona a camada do aplicativo, enquanto o firewall do Symantec Endpoint Protection inspeciona os níveis mais baixos (IP e transporte).O firewall do Symantec Endpoint Protection para Mac não oferece regras de bloqueio de ponto a ponto, embora você possa criá-las em parte por meio de regras de firewall personalizadas.

Table 9: Como gerenciar a proteção de firewall

Etapas	Descrição
Etapa 1: saiba mais sobre a proteção de firewall.	Saiba como a proteção de firewall monitora o tráfego e protege contra vetores de ataque comuns. Como a Proteção contra ameaças à rede protege seu Mac
Etapa 2: ative ou desative o firewall.	Talvez seja preciso desativar o firewall para solução de problemas, como quando o tráfego for bloqueado e você esperar que seja permitido. Tipicamente, você não deve desativar o firewall. Como ativar ou desativar a Proteção contra ameaças à rede

Para ativar ou desativar a Proteção contra ameaças à rede

Normalmente, quando você desativa os componentes da Proteção contra ameaças à rede em seu computador, o computador fica menos seguro. No entanto, é recomendável desativar a prevenção contra intrusões para evitar falsos

positivos ou desativar o firewall para solucionar problemas de tráfego bloqueado. A prevenção contra intrusões e o firewall fazem parte da Proteção contra ameaças à rede.

Para clientes gerenciados, a quantidade de controle que você tem sobre estas configurações depende de como o administrador configurou o cliente. Além disso, todas as mudanças que você fizer a estas configurações podem ser revertidas ao que a política ditar na pulsação seguinte.

Para clientes não gerenciados, o firewall não está disponível.

Para ativar ou desativar a Proteção contra ameaças à rede:

1. No cliente do Symantec Endpoint Protection, na página **Avançado**, clique em **Proteção contra ameaças à rede**.
2. Para ativar ou desativar a prevenção contra intrusões, clique em **Prevenção contra intrusões**.
3. Para ativar ou desativar o firewall, clique em **Firewall**.
4. Para ativar ou desativar as notificações da prevenção contra intrusões e do firewall, clique no ícone para configurar a **Proteção contra vulnerabilidades** e, em seguida, na caixa de diálogo, marque ou desmarque a opção **Display Vulnerability Protection Notifications**.
5. Clique em **Concluído**.

Se desativar esses componentes, você deverá ativá-los novamente assim que possível para certificar-se de que seu computador tenha a melhor proteção.

Como gerenciar a prevenção contra intrusões

Como gerenciar a proteção de firewall para o cliente Mac


Symantec
A Division of Broadcom