



# McAfee Endpoint Threat Protection

**Proteção essencial e eficaz que cresce com os seus negócios**

**Principais vantagens**

- Reforce sua postura de segurança com camadas de tecnologias de proteção colaborativa
- Obtenha a flexibilidade de expandir rapidamente a sua proteção conforme suas necessidades mudarem
- Aumente a produtividade com gerenciamento centralizado, varreduras de usuário com impacto zero e consumo mínimo dos recursos do sistema

Não há dúvida de que o cenário de ameaças continuará a evoluir. Você já sabe que a construção de uma defesa forte começa no endpoint. No entanto, pode ser difícil obter a proteção de que você precisa hoje sem a capacidade de acrescentar, com o tempo, tecnologias novas. Sem isso, o resultado são operações de segurança complexas e isoladas. O McAfee® Endpoint Threat Protection oferece a proteção essencial de que você necessita hoje e o deixa preparado para os requisitos de defesa contra ameaças avançadas de amanhã. Ele integra prevenção de ameaças, firewall, defesas de Web e e-mail e controle de dispositivos que funcionam juntos em tempo real, analisando e colaborando contra as ameaças, bloqueando-as e corrigindo-as rapidamente, antes que elas afetem seus sistemas ou usuários.

**Uma estrutura de endpoints colaborativa**

Levando em consideração a integração, as defesas do McAfee Endpoint Threat Protection colaboram e compartilham o que veem em tempo real para coordenar a identificação e bloquear a execução de programas potencialmente indesejados, sites e arquivos suspeitos para um nível mais alto de proteção.

**Caso de uso**

**Download de um arquivo malicioso da Web**

Um hash de arquivo é enviado do **Controle da Web para a Prevenção contra ameaças**, desencadeando uma varredura solicitada.

Os arquivos maliciosos são detectados e **bloqueados** antes que tenham acesso total ao sistema.

**Dados forenses são capturados** (URL de origem, hash do arquivo e outras informações).

Os dados do evento são **compartilhados** com outros módulos e com o software McAfee® ePolicy Orchestrator® (McAfee ePO™), ficando visíveis na interface de usuário do cliente.

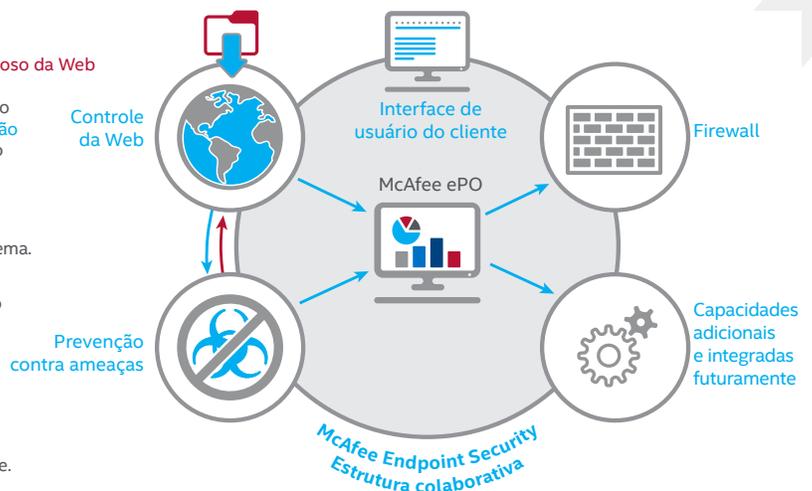


Figura 1. Como as defesas do McAfee Endpoint Threat Protection funcionam conjuntamente.

### Uma solução integrada para o presente e o futuro

Com o McAfee Endpoint Threat Protection, você pode substituir distribuições desconectadas de produtos isolados por uma estrutura conectada e colaborativa, com proteção quase em tempo real através de múltiplas tecnologias de proteção. Isso não apenas viabiliza análises mais fortes das ameaças, como também permite que os dados forenses coletados sobre as ameaças sejam compartilhados com outras defesas para torná-las mais inteligentes e ajudá-las a identificar e a bloquear ameaças mais rapidamente em outros endpoints ou ao encontrá-las em um ponto de entrada diferente.

A distribuição também é flexível, graças a essa abordagem. Você pode instalar tudo o que está incluído na sua compra hoje, decidir quais funcionalidades serão configuradas e ativá-las já. Com uma simples alteração de política, você pode ativar facilmente as capacidades que resolver utilizar posteriormente.

Enfim, nossa estrutura permite expandir rapidamente a sua proteção conforme suas necessidades mudarem, graças a uma arquitetura desenvolvida para incluir tecnologias adicionais. Isso assegura que você esteja sempre pronto para introduzir outras capacidades avançadas de proteção para defesa contra ameaças mais sofisticadas.

### Econômico sem prejudicar o desempenho

O McAfee Endpoint Threat Protection oferece uma estrutura expansível, com tecnologias essenciais de proteção, sem introduzir complexidade ou sacrificar o desempenho, proporcionando mais produtividade para você e para seus usuários. Por exemplo, suas operações funcionarão com mais eficiência devido ao gerenciamento centralizado com o software McAfee ePolicy Orchestrator, que oferece um painel único para distribuição, monitoramento e gerenciamento de políticas de segurança no seu ambiente. Clientes com vários sistemas operacionais em seus ambientes poderão aumentar sua produtividade utilizando políticas multiplataforma para sistemas Microsoft Windows, Apple Macintosh e Linux. Além disso, como uma linguagem comum (McAfee Data Exchange Layer) é utilizada pelos componentes do McAfee Endpoint Threat Protection, você pode otimizar processos entre tecnologias e acelerar as respostas às ameaças, reduzindo os riscos ao estreitar a janela de exposição.

Seus usuários também obterão aumentos de produtividade com varreduras de usuário de impacto zero e gerenciamento de uso da memória e da CPU, otimizados para minimizar o impacto sobre os sistemas. Uma interface de usuário intuitiva é fornecida por padrão, tornando fácil para você e para seus usuários obter insights rápidos sobre quais ações foram executadas e suas razões.

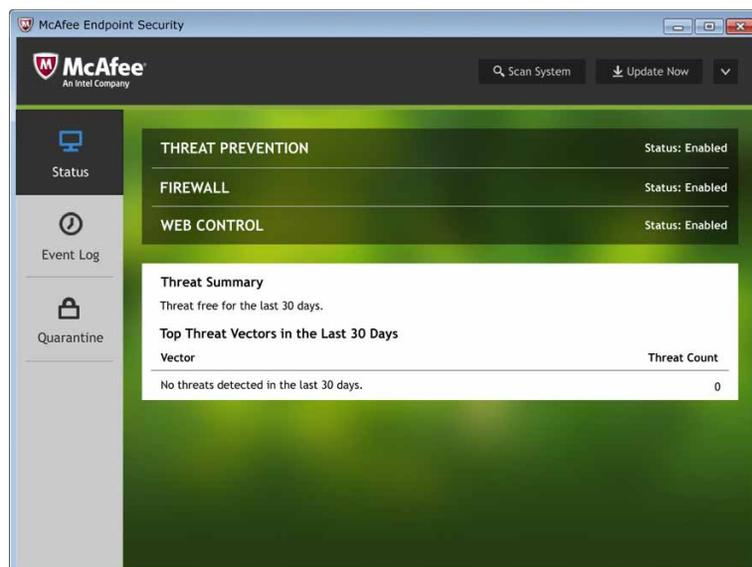


Figura 2. A interface de usuário intuitiva mantém as coisas simples para administradores e usuários.

### Plataformas compatíveis

- Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary
- Mac OS X versão 10.5 ou posterior
- Plataformas Linux de 32 e 64 bits: RHEL, SUSE, CentOS, OEL, Amazon Linux, e Ubuntu nas versões mais recentes

### Servidores:

- Windows Server (2003 SP2 ou posterior, 2008 SP2 ou posterior, 2012), Windows Server 2016
- Windows Embedded (Standard 2009, Point of Service 1.1 SP3 ou posterior)
- Citrix Xen Guest
- Citrix XenApp 5.0 ou posterior

Componente	Vantagem	Benefícios para o cliente	Diferenciação
<b>Prevenção de ameaças</b>	Proteção abrangente que localiza, congela e corrige malware rapidamente, com múltiplas camadas de proteção.	<ul style="list-style-type: none"> <li>• Detém malware conhecido e desconhecido utilizando técnicas heurísticas e de varredura ao acessar.</li> <li>• Simplifica políticas e distribuições com proteção em plataformas Windows, Mac e Linux.</li> <li>• Incrementa o desempenho evitando varreduras em processos confiáveis e priorizando processos aparentemente suspeitos.</li> </ul>	Antimalware multicamada que colabora com as defesas de firewall e de Web e que as mantém informadas para análises mais fortes e para aplicar de forma mais inteligente regras de bloqueio de ameaças potenciais.
<b>Firewall integrado</b>	Protege endpoints contra redes de bots, ataques de negação de serviços distribuída (DDoS), executáveis não confiáveis, ameaças persistentes avançadas e conexões arriscadas na Web.	<ul style="list-style-type: none"> <li>• Protege os usuários e a produtividade ao impor as suas políticas.</li> <li>• Regula a largura de banda bloqueando conexões de entrada indesejáveis e controlando requisições de saída.</li> <li>• Equipa os usuários ao informá-los sobre redes e executáveis confiáveis e arquivos ou conexões arriscadas.</li> </ul>	Políticas de aplicativos e localizações protegem laptops e desktops, especialmente quando estes não se encontram na rede corporativa.
<b>Controle da Web</b>	Garante uma navegação segura na Web, com proteção de Web e filtragem para endpoints.	<ul style="list-style-type: none"> <li>• Reduz o risco e assegura conformidade alertando os usuários antes que estes visitem sites maliciosos.</li> <li>• Previne ameaças e protege a produtividade autorizando ou bloqueando sites inadequados ou perigosos.</li> <li>• Interrompe downloads perigosos com segurança, bloqueando-os antes que o download seja concluído.</li> </ul>	Proteção para Windows, Mac, Linux e vários navegadores, com informações do McAfee Global Threat Intelligence.
<b>McAfee Data Exchange Layer</b>	Conecta a segurança para integrar e simplificar a comunicação com produtos da Intel Security e de terceiros.	<ul style="list-style-type: none"> <li>• A integração reduz o risco e o tempo de resposta.</li> <li>• Menos sobrecarga e menores custos com a equipe operacional.</li> <li>• Processos otimizados e recomendações práticas.</li> </ul>	<ul style="list-style-type: none"> <li>• Compartilha as informações mais importantes sobre ameaças entre os produtos de segurança.</li> <li>• Compartilha instantaneamente insights sobre ameaças do tipo "paciente zero" com todos os outros endpoints para prevenir infecções e atualizar a proteção.</li> </ul>
<b>Gerenciamento pelo McAfee ePO</b>	Um painel unificado para um gerenciamento altamente expansível, flexível e automatizado das políticas de segurança para identificar e responder a questões de segurança.	<ul style="list-style-type: none"> <li>• Unifique e simplifique os fluxos de trabalho de segurança para obter eficiências comprovadas.</li> <li>• Mais visibilidade e flexibilidade para tomar decisões com confiança.</li> <li>• Distribua e gerencie rapidamente um agente único com imposição de políticas personalizáveis.</li> <li>• Reduza o tempo do insight à resposta com consultas, dashboards e respostas dinâmicas e automatizadas.</li> </ul>	<ul style="list-style-type: none"> <li>• Mais controle, menos custos e um gerenciamento de segurança operacional mais rápido com um console único.</li> <li>• Uma interface comprovada que vem sendo amplamente reconhecida no setor por sua superioridade.</li> <li>• Arraste e solte dashboards em um amplo ecossistema de segurança.</li> <li>• Plataforma aberta que viabiliza a adoção rápida de inovações em segurança.</li> </ul>

Saiba mais sobre as vantagens do McAfee Endpoint Threat Protection em [www.mcafee.com/br/products/endpoint-threat-protection.aspx](http://www.mcafee.com/br/products/endpoint-threat-protection.aspx).



**McAfee. Part of Intel Security.**

Av. das Nações Unidas, 8.501 - 16º andar  
CEP 05425-070 - São Paulo - SP - Brasil  
Telefone: +55 (11) 3711-8200  
Fax: +55 (11) 3711-8286  
[www.intelsecurity.com](http://www.intelsecurity.com)

Intel, os logotipos da Intel e da McAfee, ePolicy Orchestrator e McAfee ePO são marcas comerciais da Intel Corporation ou da McAfee, Inc. nos EUA e/ou em outros países. Outros nomes e marcas podem ser propriedade de terceiros. Copyright © 2016 Intel Corporation. 1770\_1016 OUTUBRO DE 2016