

McAfee Complete Endpoint Threat Protection

Proteção contra ameaças avançadas para ataques sofisticados

Os tipos de ameaças que a sua organização enfrenta exigem alta visibilidade e ferramentas que permitam a você agir e assumir o controle de todo o ciclo de vida da defesa contra ameaças. Isso significa armar seus especialistas em segurança com capacidades de mais precisão e que ofereçam insights mais fortes sobre as ameaças avançadas. O McAfee® Complete Endpoint Threat Protection oferece defesas avançadas que investigam, contêm e executam ações contra ameaças de dia zero e ataques sofisticados. Sua proteção essencial de endpoint trabalha com autoaprendizagem e contenção dinâmica integradas para detectar ameaças de dia zero quase em tempo real, classificando-as e interrompendo-as antes que possam infectar os seus sistemas. Dados e relatórios forenses decisivos mantêm você informado e ajudam a passar da resposta a epidemias à investigação e reforço das suas defesas. Como a solução se baseia em uma estrutura expansível, é possível adicionar outras defesas contra ameaças avançadas facilmente, tanto hoje quanto no futuro, conforme suas necessidades e o cenário de ameaças evoluírem.

Defesas contra ameaças avançadas e automatizadas

É preciso deter as ameaças avançadas antes que elas comecem. É por isso que o McAfee Complete Endpoint Threat Protection inclui as tecnologias de contenção dinâmica de aplicativos (DAC) e Real Protect¹. A DAC bloqueia automaticamente greyware e ameaças de dia zero suspeitas quando comportamentos maliciosos são detectados, impedindo-os de infectar

os seus sistemas ou de afetar os seus usuários. Utilizando autoaprendizagem, o Real Protect consegue investigar e classificar as ameaças, salvando os insights obtidos para providências futuras que podem ser tomadas automaticamente.

Feito para reduzir a complexidade

A complexidade é inimiga da eficiência. Agora você não precisa perder tempo tentando gerenciar várias soluções separadas com interfaces e consoles de gerenciamento

Principais vantagens

- Ajuda você a se manter à frente de ameaças de dia zero, ransomware e greyware com autoaprendizagem e contenção dinâmica de aplicativos
- Acelera a remediação e protege a sua produtividade com análises e ações automatizadas
- Simplifica o seu ambiente, a sua distribuição e o gerenciamento contínuo com gerenciamento centralizado

DATA SHEET

diferentes. O McAfee Complete Endpoint Threat Protection é gerenciado por meio de um único console: o software McAfee® ePolicy Orchestrator® (McAfee ePO™). Com esse painel unificado, você pode se qualificar mais rapidamente, acelerar a distribuição e reduzir a sobrecarga do gerenciamento contínuo. Clientes com múltiplos sistemas operacionais em seus ambientes poderão aumentar sua produtividade utilizando políticas multiplataforma para sistemas Microsoft Windows, Apple Macintosh e Linux.

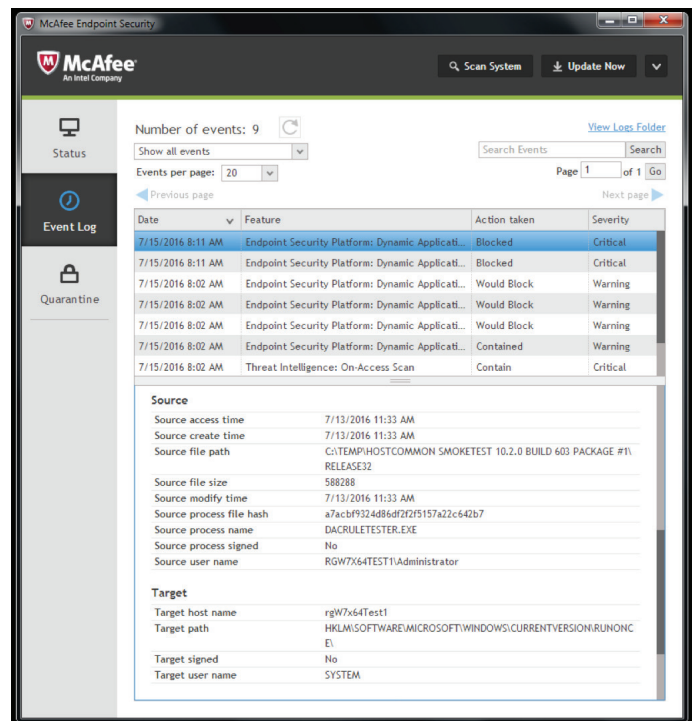


Figura 1. A contenção dinâmica de aplicativos bloqueia e contém as ameaças conforme sua gravidade.

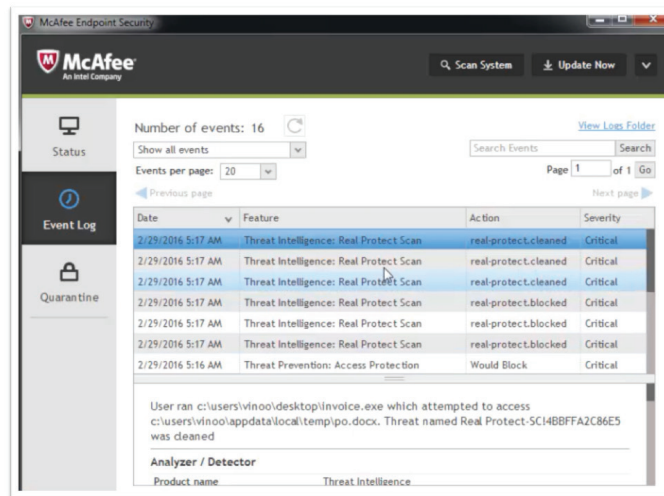


Figura 2. O Real Protect utiliza autoaprendizagem para detectar, quase em tempo real, o malware de dia zero que as varreduras com base em assinaturas costumam deixar passar.

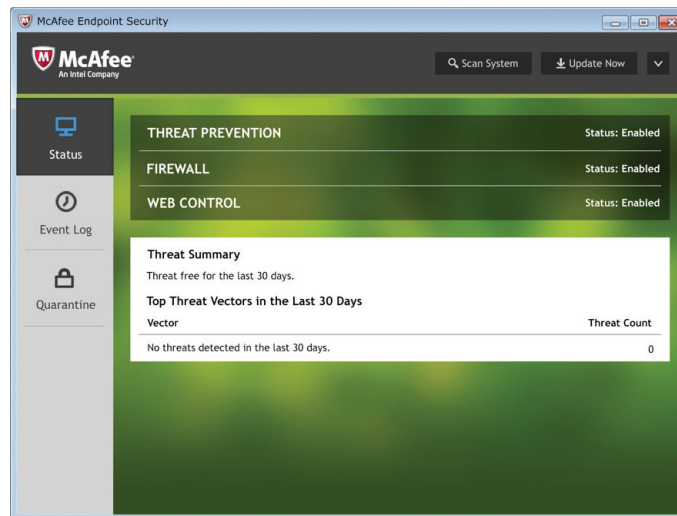


Figura 3. A interface de usuário intuitiva mantém as coisas simples para administradores e usuários.

Uma estrutura de trabalho flexível para hoje e amanhã

O McAfee Complete Endpoint Threat Protection oferece uma estrutura de trabalho colaborativa e conectada e proteção quase em tempo real com várias tecnologias de proteção. Isso não só possibilita análises mais fortes das ameaças, como também permite que os dados forenses sobre ameaças coletados sejam compartilhados com outras defesas para torná-las mais inteligentes. Utilizando uma camada de comunicação comum, defesas essenciais de proteção de endpoint podem informar e consultar defesas contra ameaças avançadas para obter condenações e insights mais sólidos a partir do momento em que as ameaças forem encontradas pela primeira vez.

Graças a essa abordagem, a distribuição também é mais flexível, portanto, você pode instalar tudo o que está incluído na sua compra hoje. Você pode decidir agora quais capacidades serão configuradas e ativadas e, então, ativar facilmente as que decidir usar no futuro, por meio de uma alteração de política.

Enfim, nossa estrutura permite expandir a sua proteção conforme suas necessidades mudarem, graças a uma arquitetura desenvolvida para incluir tecnologias adicionais.

Plataformas compatíveis

- Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary
- Mac OSX 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

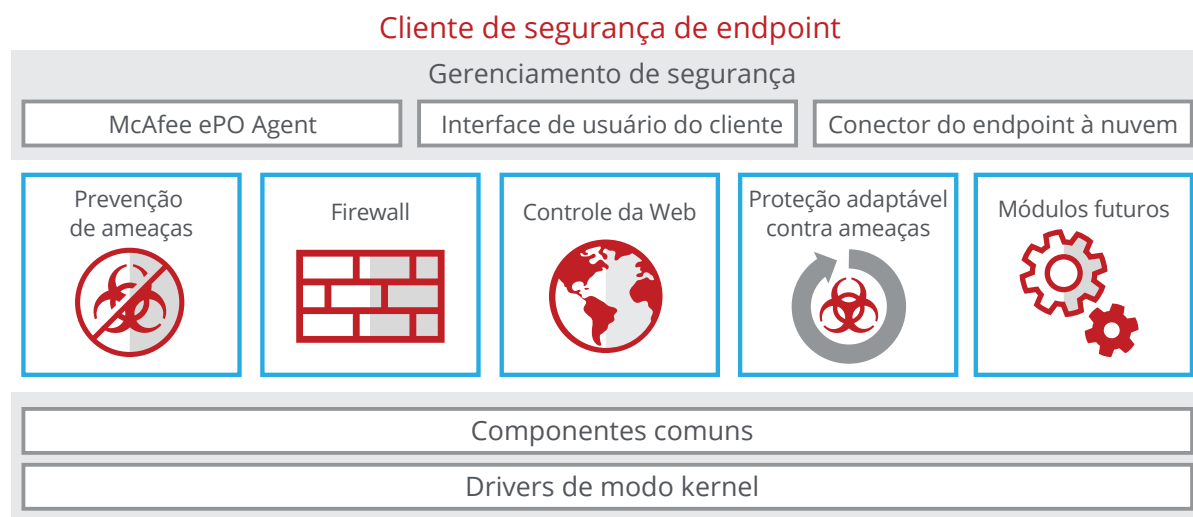


Figura 4. A estrutura de cliente de segurança de endpoint da McAfee.

DATA SHEET

Componente	Vantagem	Benefícios para o cliente	Diferenciação
Contenção dinâmica de aplicativos	Protege o paciente zero evitando que o greyware faça alterações maliciosas em endpoints	<ul style="list-style-type: none"> ▪ Aumenta a proteção sem afetar os usuários finais ou os aplicativos confiáveis ▪ Reduz o tempo decorrido da descoberta à contenção, com o mínimo de intervenção manual ▪ Protege o paciente zero e isola a rede da infecção 	<ul style="list-style-type: none"> ▪ Trabalha com ou sem uma conexão com a Internet e não requer interação ou análise externa ▪ Transparente para o usuário ▪ Modo de observação, que proporciona visibilidade instantânea sobre as ameaças ao expor possíveis comportamentos de exploração dentro do ambiente
Real Protect	Aplica classificação de comportamento por autoaprendizagem para bloquear ameaças de dia zero antes que estas sejam executadas e impede a execução imediata de ameaças que tenham escapado de detecções anteriores	<ul style="list-style-type: none"> ▪ Derrota facilmente mais malware de dia zero, incluindo objetos de difícil detecção, como ransomware ▪ Desmascara, analisa e neutraliza ameaças automaticamente, sem a necessidade de intervenção manual ▪ Adapta as defesas utilizando classificação automatizada e uma infraestrutura de segurança conectada 	<ul style="list-style-type: none"> ▪ Detecta malware que só pode ser encontrado por meio de análise comportamental dinâmica. Uma integração avançada compartilha atualizações de reputação em tempo real e aumenta a eficácia da segurança para todos os componentes de segurança
Prevenção de ameaças	Proteção abrangente que localiza, congela e corrige malware rapidamente, com múltiplas camadas de proteção	<ul style="list-style-type: none"> ▪ Detém malware conhecido e desconhecido utilizando técnicas heurísticas, comportamentais e de varredura ao acessar ▪ Simplifica políticas e distribuições com proteção para desktops e servidores em máquinas Windows, Mac e Linux ▪ Incrementa o desempenho evitando varreduras em processos confiáveis e priorizando processos aparentemente suspeitos 	Antimalware multicamada que colabora com as defesas de firewall e de Web para prevenção de ameaças e análises mais fortes
Firewall integrado	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"> ▪ Protege os usuários e a produtividade ao impor as suas políticas ▪ Regula a largura de banda bloqueando conexões de entrada indesejáveis e controlando requisições de saída ▪ Capacita os usuários ao informá-los sobre redes e executáveis confiáveis e arquivos ou conexões arriscadas 	Políticas de aplicativos e localizações protegem laptops e desktops, especialmente quando estes não se encontram na rede corporativa

DATA SHEET

Componente	Vantagem	Benefícios para o cliente	Diferenciação
Controle da Web	Garante uma navegação segura na Web, com proteção de Web e filtragem para endpoints	<ul style="list-style-type: none">▪ Reduz o risco e assegura conformidade alertando os usuários antes que estes visitem sites maliciosos▪ Previne ameaças e protege a produtividade autorizando ou bloqueando o acesso aos sites▪ Interrompe downloads perigosos com segurança, bloqueando-os antes que o download seja concluído	Proteção para Windows, Mac, Linux e vários navegadores
Data Exchange Layer	Conecta a segurança para integrar e simplificar a comunicação com produtos da McAfee e de terceiros	<ul style="list-style-type: none">▪ Risco e tempo de resposta reduzidos através de integração▪ Menos sobrecarga e menores custos com a equipe operacional▪ Processos otimizados e recomendações práticas	Compartilha as informações mais importantes sobre ameaças entre as defesas de segurança
Gerenciamento pelo McAfee ePO	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">▪ Unifica e simplifica os fluxos de trabalho de segurança para obter eficiências comprovadas▪ Mais visibilidade e flexibilidade para tomar decisões com confiança▪ Distribui e gerencia rapidamente um agente único com imposição de políticas personalizáveis▪ Reduz o tempo do insight à resposta com relatórios e dashboards intuitivos	<ul style="list-style-type: none">▪ Mais controle, menores custos e um gerenciamento de segurança operacional mais rápido com um console único▪ Uma interface comprovada que vem sendo amplamente reconhecida no setor por sua superioridade▪ Arraste e solte dashboards em um amplo ecossistema de segurança▪ Plataforma aberta que viabiliza a adoção rápida de inovações em segurança

Saiba mais

Para obter mais informações sobre as vantagens do McAfee Complete Endpoint Threat Protection, visite: www.mcafee.com/br/products/complete-endpoint-threat-protection.aspx.

1. A solução inclui data centers hospedados nos EUA que são utilizados para verificar reputações de arquivos e armazenar dados relevantes para a detecção de arquivos suspeitos. Embora não seja obrigatório, a tecnologia DAC funciona melhor com uma conexão com a nuvem. O pleno aproveitamento das capacidades DAC e Real Protect do produto exige acesso à nuvem e suporte ativo, além de estar sujeito aos termos e condições do serviço de nuvem.



Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br

McAfee e o logotipo da McAfee, ePolicy Orchestrator e McAfee ePO são marcas comerciais ou marcas registradas da McAfee, LLC ou de suas afiliadas nos EUA e em outros países. Outros nomes e marcas podem ser propriedade de terceiros. Copyright © 2017 McAfee, LLC. 1771_1016
OUTUBRO DE 2016