FIREEYE™

FICHA TÉCNICA

FireEye Endpoint Security

Detenha os ataques com conhecimento adquirido na linha de frente

DESTAQUES

- Impedir a maioria dos ataques cibernéticos contra os endpoints de um ambiente
- Detectar e bloquear violações que ocorrem para reduzir o impacto de uma violação
- Descobrir ameaças em vez de ir atrás de alertas para melhorar a produtividade e a eficiência
- Usar um único agente de pequeno rastro para impacto mínimo sobre o usuário final
- Proteções e funcionalidades por meio de módulos para download
- Cumprir os regulamentos, por exemplo, PCI-DSS e HIPAA
- Distribuir no local ou na nuvem

A segurança tradicional dos endpoints não é eficaz contra as ameaças modernas; ela nunca foi criada para lidar com ataques de ameaças persistentes (*Advanced Persistent Threat,* APT) avançados ou sofisticados. Para manter os endpoints seguros, uma solução deve detectar rapidamente a ameaça e reagir com a tecnologia mais eficaz.

O FireEye Endpoint Security combina o melhor dos produtos de segurança legados, aprimorados com tecnologia, conhecimento e inteligência FireEye para defender contra os ataques cibernéticos de hoje. Com base em um modelo de defesa aprofundado, o Endpoint Security emprega uma arquitetura modular com mecanismos padrão e módulos para download com o objetivo de proteger, detectar, responder e gerenciar agentes.

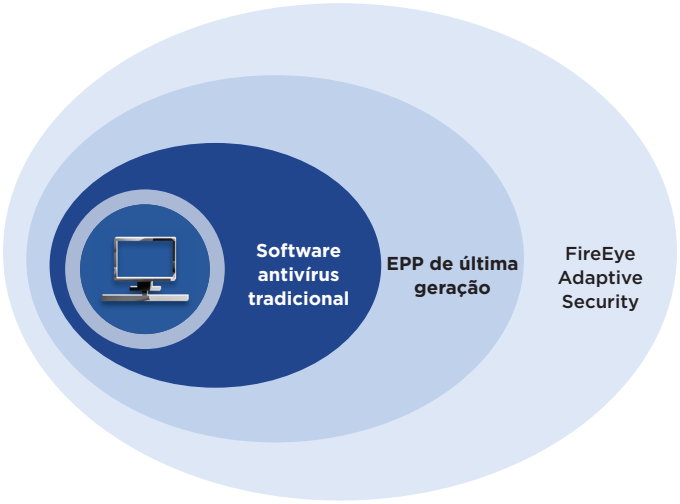
Para proteger contra ameaças de malware comuns, o Endpoint Security usa um mecanismo de plataforma de proteção de endpoint (*Endpoint Protection Platform,* EPP) em um modelo por assinatura. Para localizar ameaças para as quais ainda não exista uma assinatura, o MalwareGuard usa o aprendizado de máquina semeado, com o conhecimento das linhas de frente dos ataques cibernéticos. Para lidar com ameaças avançadas, as capacidades de resposta e detecção do endpoint (*Endpoint Detection and Response,* EDR) são habilitadas por meio de um mecanismo de análise baseada no comportamento. Um mecanismo de indicadores de comprometimento (*Indicators of Compromise,* IOC) em tempo real conta com informações atuais da linha de frente para ajudar a encontrar ameaças ocultas. Para adicionar novos mecanismos e recursos, você pode baixar os módulos no FireEye Market.

Mesmo com a melhor proteção, as violações são inevitáveis. Para assegurar uma resposta substancial que minimiza a interrupção do negócio, o Endpoint Security fornece ferramentas para:

- Procurar e investigar ameaças conhecidas e desconhecidas em dezenas de milhares de endpoints em questão de minutos;
- Identificar e detalhar vetores que um ataque usou para infiltrar um endpoint;
- Determinar se ocorreu um ataque (e se ele persiste) em um endpoint específico e onde ele se espalhou;
- Estabelecer cronograma e duração de comprometimentos de endpoints e acompanhar o incidente;
- Identificar claramente quais endpoints e sistemas precisam de contenção para evitar novos comprometimentos.

O TI é um facilitador estratégico que promove nossa capacidade de instruir efetivamente nossos estudantes. Utilizar o FireEye Endpoint Security garante que nossos ativos de TI fiquem disponíveis e sejam altamente funcionais e seguros, o que é fundamental para a realização da nossa missão.

— James D. Perry II
Diretor de segurança da informação, Universidade da Carolina do Sul



Muitas vezes, a gerência acha que qualquer vírus é quase o fim do mundo. Com o FireEye, posso apresentar indícios reais sobre a natureza do problema e que fomos capazes de administrá-lo e contê-lo. Tornar rapidamente conhecidos todos esses desconhecidos ajuda a reduzir a pressão sobre todos na organização.

— Michael Hennessy, diretor de serviços de tecnologia
Alpha Grainer Manufacturing, Inc

Recursos principais

- Agente único que usa defesa aprofundada para minimizar a necessidade de configuração e maximizar as atividades de detecção e bloqueio
- Fluxo de trabalho único integrado para analisar e responder a ameaças dentro do Endpoint Security
- Proteção totalmente integrada contra malware com defesas antivírus (AV), aprendizado de máquina, análise de comportamento, indicadores de comprometimento (IOCs) e visibilidade de endpoints
- Visualizador de auditoria e resumo de triagem para realizar inspeção e análise exaustivas de ameaças

Recursos adicionais

- Pesquisa de segurança corporativa para encontrar e lançar luz rapidamente sobre atividade suspeita e ameaças
- Aquisição de dados para realizar análise e inspeção aprofundadas e detalhadas do endpoint em um período específico
- Visibilidade abrangente que permite que as equipes de segurança busquem, identifiquem e avaliem rapidamente o nível das ameaças
- Capacidades de detecção e resposta para detectar, investigar e conter rapidamente endpoints para agilizar a resposta
- Interface fácil de entender para rápida interpretação e resposta a qualquer atividade suspeita no endpoint

Ambientes e sistemas operacionais compatíveis	
Windows	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
Mac	OS X 10.9+
Linux	RedHat Enterprise Linux versões 6.8+, 7.2+, 8 CentOS 6.8+, 7.2+, 8 Ubuntu 14.04, 16.04, 18.04 SUSE 11.3, 11.4, 12.2, 12.3, 15 Open SUSE 15.1 Amazon AMI 2018.3, AMI2 Oracle Linux 6.10 e 7.6

Opções de distribuição: appliance físico no local, appliance virtual no local, serviço na nuvem FireEye

SE Labs AA JAN–MAR 2020 ENTERPRISE ENDPOINT PROTECTION · AV comparatives APPROVED Business Security DEC 2019 · vb100 VIRUS virusbtn.com · OPSWAT. Access Control Certification Anti-Malware GOLD

AV-TEST · MITRE · VirusTotal

Para saber mais sobre a FireEye, visite: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Sobre a FireEye, Inc.

A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência de ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e reagir a ataques cibernéticos.

FIREEYE™