FIREEYE™

FICHA TÉCNICA

FireEye Endpoint Security

Detenha os ataques com conhecimento adquirido na linha de frente

DESTAQUES

- Impedir a maioria dos ataques cibernéticos contra endpoints
- Detectar e bloquear violações para reduzir seu impacto
- Descobrir ameaças em vez de ir atrás de alertas para melhorar a produtividade e a eficiência
- Usar um único agente para impacto mínimo sobre o usuário final
- Obter proteções e funcionalidades adicionais por meio de módulos para download
- Cumprir os regulamentos, por exemplo, PCI-DSS e HIPAA
- Deploy local ou em nuvem

Cada dia traz um novo ataque cibernético, uma nova vulnerabilidade ou um novo alvo de ransomware. As equipes de segurança acham cada vez mais difícil acompanhar as ameaças para seus usuários, dados da empresa e propriedade intelectual e nem sempre contam com ajuda extra. Os responsáveis pela resposta ficam sobrecarregados com ferramentas demais que não funcionam juntas e criam mais ruídos do que informações úteis. Os sistemas existentes nem sempre proporcionam detecção e resposta adequadas a essas ameaças avançadas.

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 a segurança de endpoints.

Para proteger contra ameaças de malware comuns, o Endpoint Security usa um mecanismo de plataforma de proteção de endpoint (EPP) em um modelo por assinatura. Para localizar ameaças para as quais ainda não exista uma assinatura, o MalwareGuard usa o aprendizado de máquina, com o conhecimento das linhas de frente dos ataques cibernéticos. Para ataques com explorações em navegadores e softwares comuns, o ExploitGuard usa um mecanismo de análise de comportamento que determina se uma exploração está sendo usada e impede que ela seja executada. Além disso, a FireEye continuamente cria módulos para detectar técnicas de ataque e acelerar respostas às ameaças emergentes. Por exemplo, o Process Guard foi desenvolvido para impedir a exfiltração de credenciais.

A 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

Mesmo com a melhor proteção, as violações são inevitáveis. Para garantir uma resposta substancial que minimiza a interrupção das operações, o Endpoint Security inclui recursos de resposta e detecção de endpoint (EDR) que conta com indicadores de comprometimento (IOCs) em tempo real, desenvolvidos com a ajuda dos responsáveis pela resposta da linha de frente da Mandiant. Além disso, as ferramentas da FireEye também ajudam a:

- Procurar e investigar ameaças conhecidas e desconhecidas em dezenas de milhares de endpoints em questão de minutos;
- Identificar e detalhar os 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 um cronograma e duração de comprometimentos de endpoints e acompanhar o incidente.

As ameaças modernas não param em um endpoint; por isso, corrigir em um único endpoint não resolverá a maioria das violações. A correção total comunica e aponta eficientemente todos os dispositivos em que uma ameaça possa estar escondida e correlaciona essa informação em tempo real. O Endpoint Security é um componente do FireEye Helix XDR, que conecta de forma integrada todas as tecnologias e serviços FireEye para detectar e responder a todas as ameaças mais sofisticadas.

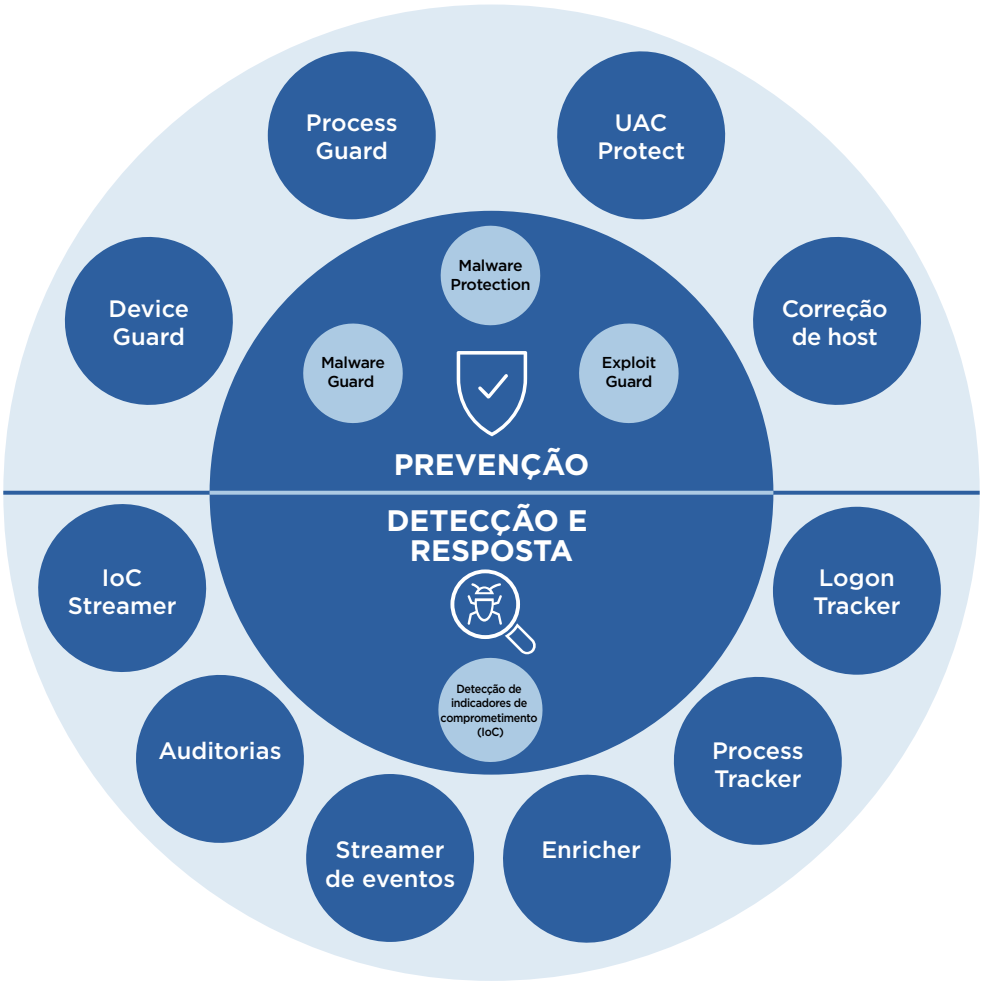

Figura 1.

Os mecanismos principais do FireEye Endpoint Security (centro) e módulos disponíveis (círculo externo).

Muitas vezes, a gerência acha que qualquer vírus é quase o fim do mundo. Com a 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 integrado para analisar e responder a ameaças dentro do Endpoint Security
- Proteção contra malware com defesas antivírus (AV), aprendizado de máquina, análise de comportamento, indicadores de comprometimento (IOCs) e visibilidade de endpoints
- Componente do FireEye Helix XDR para corrigir completamente todas as ameaças em uma organização

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	10.9 – 10.15, 11
Linux	RHEL 6.8 – 6.10, 7.1 – 7.7, 8–8.2 CentOS 6.9 – 6.10, 7.1 – 7.7, 8 SUSE 11.3, 11.4,12.2 - 12.5 e 15 Open SUSE 15.1, 15.2 Ubuntu 12.04, 14.04, 16.04, 18.04, 19.04, 20.04, 20.10 Amazon Linux AMI 2018.3, AM2 Oracle Linux 6.10, 7.6, 8 (1 e 2)

Opções de deploy: appliance físico ou virtual on-premise, como serviço na nuvem FireEye

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

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

Sobre a FireEye
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 cibersegurança para organizações empenhadas em se preparar, prevenir e reagir a ataques cibernéticos.