FIREEYE™

FICHA TÉCNICA

FireEye Network Security

Proteção eficaz contra violações cibernéticas para organizações de médio a grande porte

Visão Geral

O FireEye Network Security é uma solução eficaz de proteção contra ameaças cibernéticas que ajuda as organizações a minimizar os riscos de violações onerosas, detectando com precisão e interrompendo imediatamente ataques avançados, direcionados e outros ataques evasivos escondidos no tráfego de internet. Ele possibilita resolver de maneira eficiente e em questão de minutos os incidentes de segurança detectados, com evidências concretas, inteligência decisiva e integração de fluxos de trabalho de resposta. Com o FireEye Network Security, as organizações são efetivamente protegidas contra as ameaças atuais, as quais exploram vulnerabilidades em aplicativos ou em sistemas operacionais Microsoft Windows ou Apple OS X, são direcionadas contra sedes corporativas ou filiais, ou se ocultam em um grande volume de tráfego de entrada de internet que precisa ser inspecionado em tempo real.

No núcleo do FireEye Network Security estão as tecnologias Multi-Vector Virtual Execution™ (MVX) e tecnologias de aprendizado de máquina dinâmico e inteligência artificial (IA).

MVX é um mecanismo de análise dinâmica e sem assinaturas que inspeciona tráfego de rede suspeito para identificar ataques que contornam defesas tradicionais com base em assinaturas e políticas. Múltiplos mecanismos de correlação, IA e aprendizado de máquina representam uma coletânea de mecanismos de regras dinâmicas contextuais, que detecta e bloqueia atividades nocivas, tanto em tempo real quanto retroativamente, com base na inteligência mais recente obtida de máquinas, atacantes e vítimas. O FireEye Network Security também inclui tecnologia de sistema de prevenção de intrusão (IPS) para detectar ataques comuns usando correspondência de assinatura convencional.

O FireEye Network Security está disponível em uma variedade de opções de formato, instalação e desempenho. Ele costuma ser posicionado no caminho do tráfego de internet, atrás de appliances tradicionais de segurança de rede, como firewalls de última geração, IPS e gateways seguros da web (SWG). O FireEye Network Security complementa essas soluções ao detectar rapidamente ataques conhecidos e desconhecidos com alta precisão e poucos falsos positivos, ao mesmo tempo em que viabiliza uma resposta eficiente para cada alerta.

Figura 1. Configuração típica — Soluções de Segurança de rede.

Capacidades	Vantagens
Detecção	
Detecção precisa de ataques avançados, direcionados e outros ataques cibernéticos evasivos	Minimiza o risco de violações cibernéticas onerosas
Arquitetura de segurança modular e dimensionável	Fornece proteção ao investimento e dá suporte ao crescimento dos negócios
Nível de proteção consistente para ambientes com múltiplos sistemas operacionais e todos os pontos de acesso à internet	Cria uma defesa forte por toda a organização, para todos os tipos de dispositivos
Opções de implantação integrada, múltipla, física, virtual, on-premise e na nuvem	Oferece flexibilidade, conforme as preferências e recursos da organização
Correlação multivetorial com a Segurança de E-mail e de Conteúdo	Proporciona visibilidade por uma superfície de ataque mais ampla
Prevenção	
Bloqueio imediato de ataques a velocidades de 250 Mbps a 10 Gbps	Oferece proteção em tempo real contra ataques evasivos
Visibilidade sobre o tráfego criptografado	Compatibilidade com descriptografia TLS 1.3 integrada disponível em appliances sem taxa de licença adicional
Resposta	
Baixa taxa de falsos alertas, categorização de Riskware e mapeamento para o framework MITRE ATT&CK	Reduz o custo operacional da triagem de alertas não confiáveis
Mudança para investigação e validação de alertas, contenção de endpoints e resposta a incidentes	Automatiza e simplifica os fluxos de trabalho de segurança
Evidência de execução e inteligência decisiva sobre ameaças	Acelera a priorização e a resolução dos incidentes de segurança detectados

Vantagens Técnicas

Insights e Detecção de Ameaças Acionáveis e Precisos

O FireEye Network Security utiliza múltiplas técnicas de análise para detectar ataques com alta precisão e uma baixa taxa de alertas falsos:

- O **mecanismo Multi-Vector Virtual Execution™ (MVX)** detecta ataques de dia-zero, de fluxos múltiplos e outros ataques evasivos com análise dinâmica e sem assinaturas em um ambiente virtual seguro. Ele interrompe as fases de infecção e comprometimento da cadeia de destruição do ataque cibernético, identificando malware e exploits nunca antes vistos.
- **Múltiplos mecanismos dinâmicos de correlação, IA e aprendizado de máquina** detectam e bloqueiam ataques ofuscados, direcionados e outros ataques personalizados com análise contextual baseada em regras de insights em tempo real colhidos nas linhas de frente de milhares de horas de experiência em resposta a incidentes. Ele bloqueia as fases de infecção, comprometimento e intrusão da cadeia de destruição do ataque cibernético identificando exploits maliciosos, malware, ataques de phishing e callbacks de comando e controle (CnC). Ele também extrai e envia o tráfego de rede suspeito ao mecanismo MVX para uma análise de veredito definitiva.
  Além da proteção do lado do cliente, os mecanismos dão suporte a detecções no lado do servidor, detecção de movimento lateral e detecção no tráfego pós-exploração.
- Os alertas gerados pelo FireEye Network Security incluem evidências concretas em tempo real para responder, priorizar e conter ataques direcionados e descobertos recentemente. As ameaças detectadas também podem ser mapeadas para o framework MITRE ATT&CK para evidências contextuais.

Proteção Imediata e Resiliente

O FireEye Network Security oferece modos de implantação versáteis, incluindo:

- Monitoramento out-of-band por meio de um TAP/SPAN, monitoramento em linha ou bloqueio ativo em linha. O modo de bloqueio em linha interrompe automaticamente o malware e exploits de entrada e callbacks de múltiplos protocolos de saída. No modo de monitoramento em linha, são gerados alertas e as organizações decidem como responder a eles. No modo de prevenção out-of-band, o FireEye Network Security envia pacotes TCP reset para o bloqueio out-of-band de conexões TCP ou HTTP.
- Modelos selecionados oferecem uma opção de alta disponibilidade (HA) ativa para fornecer resiliência em caso de falhas de rede ou dispositivo.

Cobertura de uma Ampla Superfície de Ataque

O FireEye Network Security oferece um nível de proteção consistente para os atuais ambientes de rede diversificados:

- Compatibilidade com os sistemas operacionais Microsoft Windows e Apple Mac OS X mais comuns.
- Análise de mais de 160 tipos de arquivos diferentes, incluindo executáveis portáteis (PE), conteúdo ativo da web, arquivos compactados, imagens, Java, aplicativos Microsoft e Adobe e arquivos multimídia.
- Execução de tráfego de rede suspeito contra milhares de combinações de sistemas operacionais, service packs, tipos de aplicativos da Internet das Coisas (IoT) e versões de aplicativos.
- Proteção contra ataques avançados e tipos de malware que são difíceis de detectar por meio de assinaturas: atualizações de web shell, web shell existente, ransomware, cryptominers.

Alertas Validados e Priorizados

Além de detectar ataques genuínos, a tecnologia FireEye MVX também é utilizada para validar alertas detectados por métodos convencionais de correspondência de assinaturas e para identificar e priorizar ameaças críticas:

- O sistema de prevenção de intrusões (IPS), com validação pelo mecanismo MVX, reduz o tempo necessário para a triagem da detecção com base em assinaturas, tradicionalmente propensa a falsos alertas.
- A categorização do Riskware distingue entre tentativas autênticas de violação e atividades indesejadas, mas menos maliciosas (como adware e spyware) para priorizar a resposta aos alertas.

Integração de Fluxos de Trabalho de Resposta

O FireEye Network Security pode ser complementado de diversas formas para automatizar os fluxos de trabalho de resposta a alertas:

- O **FireEye Central Management** correlaciona alertas do FireEye Network Security e do FireEye Email Security para uma visão mais ampla do ataque e para definir regras de bloqueio que impeçam o ataque de se espalhar ainda mais.
- O **FireEye Network Forensics** integra-se com o FireEye Network Security para proporcionar capturas detalhadas de pacotes associados a um alerta, possibilitando investigações aprofundadas.
- O **FireEye Endpoint Security** identifica, valida e contém comprometimentos detectados pelo FireEye Network Security para simplificar a contenção e a correção dos endpoints afetados.

Opções de Instalação Versáteis

O FireEye Network Security oferece várias opções de instalação, conforme as necessidades e o orçamento da organização:

- **Segurança de Rede Integrada:** appliance de hardware completo e autônomo, com um serviço MVX integrado para proteger um ponto de acesso à internet em um único local. O FireEye Network Security é uma plataforma sem agente, fácil de gerenciar, que implementa rapidamente sem exigir regras, políticas ou ajustes.
- **Segurança de Rede Distribuída:** appliances expansíveis com um serviço MVX compartilhado centralmente, para proteger pontos de acesso à internet dentro das organizações.
  - **Nó de Rede Inteligente:**appliances físicos ou virtuais, que analisam o tráfego de internet para detectar e bloquear tráfego nocivo e enviar atividades suspeitas através de uma conexão criptografada ao serviço MVX, para um veredito de análise definitivo.
  - **MVX Smart Grid:** serviço MVX on-premise, centralizado e dinâmico, que oferece escalabilidade transparente, tolerância a falhas N+1 e balanceamento de carga automático.
  - **FireEye Cloud MVX:** Assinatura do serviço MVX hospedado pela FireEye, que assegura privacidade ao analisar o tráfego no nó de rede inteligente. Somente objetos suspeitos são enviados por uma conexão criptografada para o serviço MVX, onde os objetos considerados benignos são descartados.
  - **Proteção on-premise ou na nuvem:** Além dos appliances autônomos e virtuais, a FireEye oferece Network Security na Nuvem Pública com disponibilidade na Amazon e Azure.

Figura 2. Os exemplos de Segurança de Rede Integrada incluem NX 2550, NX 3500, NX 5500 e NX 10550.

Figura 3.

Modelos de instalação distribuída do Network Security.

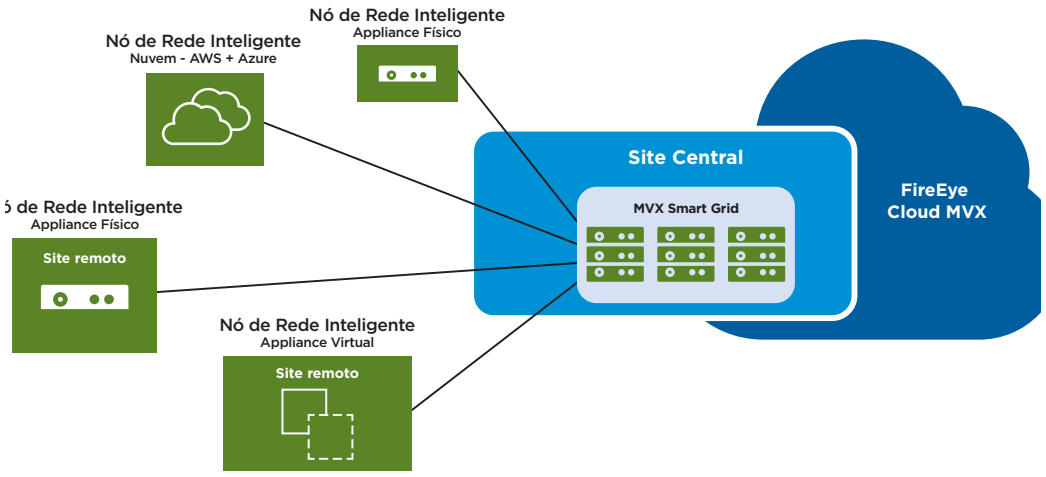

Figura 4.

Componentes modulares do FireEye Network Security.

Alto Desempenho e Escalabilidade

O FireEye Network Security protege os pontos de acesso à internet na velocidade da conexão, com opções de desempenho para escritórios centrais e filiais de diversos portes:

A arquitetura expansível do MVX Smart Grid e do FireEye Cloud MVX permite que o serviço MVX acomode desde um até milhares de nós de rede inteligentes, expandindo-se perfeitamente conforme a necessidade.

Formato Físico	Desempenho
Segurança de Rede Integrada	50 Mbps a 5 Gbps
Nó de Rede Física Inteligente	50 Mbps a 10 Gbps
Nó Inteligente de Rede de Nuvem Pública e Virtual	50 Mbps a 8 Gbps

Vantagens Corporativas

Desenvolvido para satisfazer as necessidades de organizações situadas em um único local ou distribuídas por vários locais, o FireEye Network Security oferece várias vantagens:

Minimiza o Risco de Violações Cibernéticas

O FireEye Network Security é uma solução de defesa cibernética altamente eficaz que:

- Impede que intrusos invadam uma organização para roubar ativos valiosos ou perturbar seus negócios, ao interromper ataques avançados, direcionados e outros ataques evasivos;
- Detém ataques e contêm intrusões mais rapidamente com evidências concretas, inteligência decisiva, bloqueio em linha e automação dos fluxos de resposta;
- Elimina os pontos fracos das defesas cibernéticas da organização com proteção consistente para vários sistemas operacionais, tipos de aplicativos e localizações centrais ou em filiais.

Retorno Rápido do Investimento

Segundo um estudo da Forrester Consulting[1], os clientes do FireEye Network Security podem esperar uma economia de 152% no retorno do investimento ao longo de três anos e o retorno do investimento inicial em apenas 9,7 meses. O FireEye Network Security:

- Concentra os recursos da equipe de segurança em ataques reais para reduzir as despesas operacionais;
- Otimiza o gasto de capital com um serviço MVX compartilhado e uma grande variedade de pontos de desempenho para implementar o tamanho certo para atender aos requisitos;
- Prepara o investimento em segurança para o futuro ao se expandir harmoniosamente quando o número de filiais ou o volume de tráfego de internet aumenta;
- Protege os investimentos existentes ao permitir uma migração sem custos de uma distribuição integrada para uma distribuição múltipla;
- Reduz gastos futuros de capital, com sua arquitetura modular e expansível.

1 Forrester (Maio de 2016). The Total Economic Impact of FireEye.

Prêmios e Certificações

O portfólio de produtos FireEye Network Security ganhou vários prêmios e certificações setoriais e governamentais:

- Em 2020, a FireEye conquistou o primeiro lugar no Naval Information Warfare Systems Command (NAVWAR) Artificial Intelligence Cybersecurity Challenge[2].
- Em 2020, a KuppingerCole concedeu à FireEye a premiação Leadership Compass for Network Detection and Response[3].
- Em 2020, a Forrester reconheceu a FireEye como um grande fornecedor de Visibilidade e Análise de Rede[4].
- Em 2018, a Frost & Sullivan reconheceu a FireEye como líder indiscutível de mercado, com 46% de participação, mais que os dez concorrentes seguintes juntos[5].
- O FireEye Network Security conquistou certificações, entre elas, Common Criteria, FIPS 140-2 e SOC 2.
- O FireEye Network Security tem sido agraciado com vários prêmios do SANS Institute, SC Magazine, CRN e outros.
- O FireEye Network Security foi a primeira solução de segurança do mercado a receber a certificação SAFETY Act do Departamento de Segurança Interna dos EUA.

2 FireEye (6 de Janeiro de 2021). Naval Information Warfare Systems Command (NAVWAR) concede à FireEye o primeiro lugar no Network Threat Detection Challenge.
3 KuppingerCole (10 de Junho de 2020). Prêmio Leadership Compass em resposta e detecção de rede.
4 Forrester (23 de Junho de 2020) Now Tech: Network Analysis and Visibility, segundo trimestre de 2020.
5 Frost & Sullivan (5 de Julho de 2018) Advanced Malware Sandbox (AMS) Solutions Market, Global, Forecast to 2022.

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.

FIREEYE™