FIREEYE™

Conheça o desafio das ameaças à rede em evolução

Esteja preparado para ataques que outros deixam passar

Os atuais desafios da segurança
Ataques avançados, direcionados e outros ataques evasivos tornam extremamente difícil para as organizações prevenir efetivamente as violações cibernéticas:

- Os criminosos cibernéticos utilizam ataques avançados para evitar firewalls de última geração, soluções IPS e antivírus, e ficam ocultos nas organizações durante meses (320 dias, em média, em 2015, até receberem notificações de fora)[1]
- Mais de 68% do malware é específico para cada organização e 80% desse malware é utilizado apenas uma vez[2], o que torna as defesas com base em assinaturas ineficazes contra ataques direcionados
- Mais de 80% dos alertas gerados por segurança com base em assinaturas e políticas não são confiáveis[3] e ocupam recursos que poderiam se concentrar em alertas críticos

A atual transformação da TI orientada por negócios está agravando esse desafio ao expandir a superfície de ataque da organização:

- Até 2020, os aplicativos de nuvem pública representarão mais de dois terços dos gastos corporativos.[4] As operações baseadas em nuvem aumentam o tráfego de entrada e saída da internet de uma organização, e as ameaças em potencial, em 40%.[5] Todo esse tráfego precisa ser inspecionado
- Os dispositivos não Windows, adotados por 96% das organizações atualmente[6], não têm sido bem protegidos
- A adoção de links diretos com a internet por 40% das filiais[5] aumenta sua exposição a ataques fora da fortemente protegida sede central

Quatro requisitos para proteção contra violações cibernéticas
Para minimizar o risco de uma violação cibernética onerosa, organizações de todos os portes precisam de uma solução que efetivamente as proteja contra ataques. Essa solução precisa:

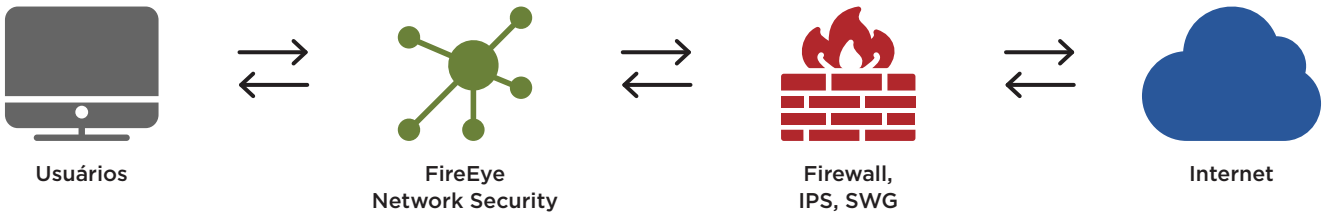
1. Detectar e interromper as ameaças que os produtos de segurança tradicionais deixam passar
2. Responder rapidamente aos incidentes e limitar seu impacto
3. Adaptar-se continuamente ao cenário de ameaças em evolução
4. Expandir-se e continuar flexível conforme o crescimento da organização ou as mudanças no modo de entrega dos serviços de TI

FireEye Network Security
O FireEye Network Security ajuda organizações de todos os portes 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. No coração do FireEye Network Security estão as tecnologias Multi-Vector Virtual Execution™ (MVX) e Intelligence-Driven Analysis (IDA). MVX é um mecanismo de análise dinâmica e sem assinaturas que inspeciona objetos suspeitos para identificar ameaças direcionadas, evasivas e desconhecidas. Os mecanismos IDA detectam e bloqueiam objetos maliciosos com base em inteligência obtida de máquinas, atacantes e vítimas.

O FireEye Network Security está disponível em uma variedade de opções de formato físico e modelos de distribuição. Ele costuma ser posicionado no caminho do tráfego de internet, atrás de recursos tradicionais de segurança de rede, como firewalls de última geração, IPS e gateways seguros da web (secure web gateways, SWG).

1 FireEye (fevereiro de 2016). M-Trends 2016.
2 Joshua Goldfarb (19 de setembro de 2016). “Detection Innovations” (Inovações em detecção).
3 Ponemon Institute LLC (janeiro de 2015). “The Cost of Malware Containment” (O custo da contenção de malware).
4 Forrester (setembro de 2016). “The Public Cloud Services Market Will Grow Rapidly to $236 Billion in 2020” (O mercado de serviços públicos na nuvem crescerá rapidamente até US$ 236 bilhões em 2020).
5 IDC (fevereiro de 2016). “Communication Service Provider Adoption of SD-WAN Technology and Its Impact to MPLS VPN Services” (Adoção da tecnologia SD-WAN por provedores de serviços de comunicação e seu impacto sobre serviços de VPN MPLS).
6 JAMF Software (2015). Pesquisa de 2015: Managing Apple Devices in the Enterprise (Gerenciamento de dispositivos Apple na empresa)

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



Para proteger eficazmente organizações de todos os portes contra violações cibernéticas, o FireEye Network Security oferece:

- **Detecção precisa:** tecnologias MVX e IDA detectam ataques com alta precisão, além de gerar uma baixa taxa de alertas falsos. Essas tecnologias também correlacionam eventos entre múltiplos fluxos e vetores de ameaças para proteção contra ataques de vários estágios que outras soluções não conseguem detectar ou deter.
- **Proteção imediata e resistente:** os ataques são interrompidos imediatamente pelo bloqueio em linha de malware e exploits de entrada e callbacks de múltiplos protocolos de saída. Uma opção de alta disponibilidade proporciona resistência e proteção adicionais quando um dispositivo ou link de rede falha.
- **Insights decisivos:** os alertas incluem evidências concretas e inteligência contextual para responder a, priorizar e conter uma ameaça rapidamente.
- **Assimilação de indicadores:** o formato Structured Threat Intelligence eXpression (STIX) permite a assimilação de inteligência personalizada nos mecanismos IDA.
- NOVO **Arquitetura expansível:** o projeto de software e de sistema possibilita o fornecimento de múltiplas tecnologias de proteção contra ameaças na forma de módulos de software.

- **Proteção abrangente:** diversos ambientes são suportados, incluindo os sistemas operacionais Microsoft Windows e Apple OS X mais comuns, mais de 140 tipos de arquivos diferentes e milhares de combinações de sistema operacional, Service Pack e aplicativo, abrangendo uma ampla superfície de ataque
- **Integração de fluxos de trabalho de resposta:** validação de alertas, categorização de riskware e mudança para captura de pacotes para investigações aprofundadas automatizam e aceleram os fluxos de trabalho de resposta aos alertas

Perfeito para sua organização

O FireEye Network Security oferece opções de distribuição flexíveis e expansíveis de até 8 Gbps para as necessidades e orçamentos de organizações de médio e grande porte.

- **Segurança de rede integrada:** um appliance de hardware completo e autônomo que utiliza o serviço MVX para proteger um único ponto de acesso à internet
- NOVO **Segurança de rede distribuída:** os nós de rede inteligentes e o serviço MVX compartilhado estendem a proteção por toda a organização
  - **Nó de rede inteligente:** appliances físicos ou virtuais distribuídos em pontos de acesso à internet para identificação e proteção contra atividades suspeitas
  - **MVX Smart Grid ou FireEye Cloud MVX:** serviço MVX no local ou com base na nuvem que realiza análises adicionais para detectar ataques avançados e tornar as equipes de segurança mais eficientes

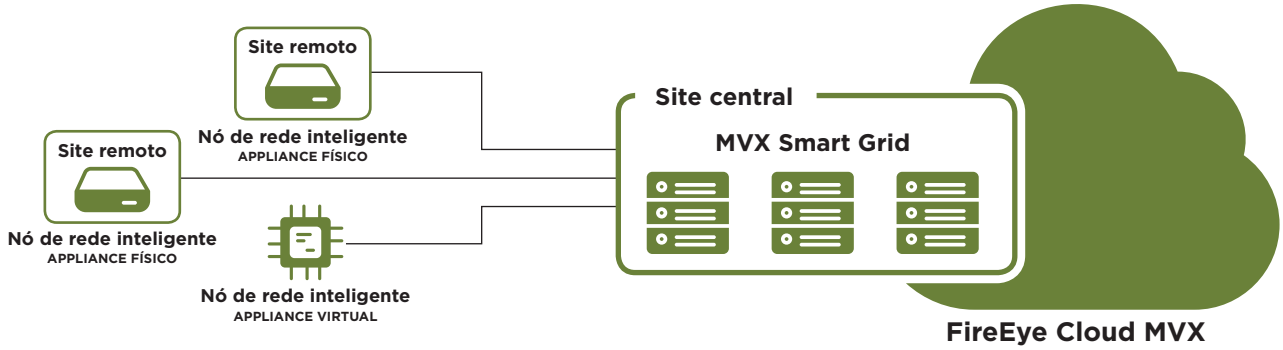


Figura 2. Segurança de rede distribuída:

O FireEye Network Security Essentials oferece opções de distribuição econômicas, integradas e múltiplas, de 10 Mbps a 2 Gbps, para organizações pequenas e médias.

Tabela 1. Opções de distribuição do FireEye Network Security.

	Appliance integrado	Nó de rede inteligente	MVX Smart Grid Requer nós de rede inteligentes	FireEye Cloud MVX Requer nós de rede inteligentes
FireEye Network Security para organizações de médio e grande porte	No local	Físico ou virtual	No local e distribuído	Baseado em nuvem e distribuído
FireEye Network Security Essentials para organizações de médio e grande porte	No local	Físico ou virtual	Não disponível	Baseado em nuvem e distribuído

Retorno rápido do investimento

Desenvolvido para satisfazer as necessidades de organizações situadas em um único local ou distribuídas por vários locais, o FireEye Network Security minimiza o risco de violações cibernéticas e reduz o tempo de retorno do investimento.

Segundo um estudo recente da Forrester Consulting[7], os clientes do FireEye Network Security podem esperar um ROI de 152% com redução de custos ao longo de três anos e o retorno do investimento inicial em apenas 9,7 meses. Reduções de custos atuais e futuras podem ser conseguidas por:

- Concentrar recursos da equipe de segurança em ataques reais para reduzir as despesas operacionais
- Otimizar o capital gasto com opções para compartilhar a capacidade do MVX e uma grande variedade de pontos de desempenho para dimensionar corretamente a distribuição
- Preparar o investimento em segurança para o futuro por meio de expansão incremental da capacidade quando o número de filiais ou o volume de tráfego de internet crescer
- Proteger investimentos existentes permitindo uma migração sem custos de uma distribuição integrada para uma distribuição múltipla
- Reduzir gastos futuros de capital, com arquitetura modular e expansível

Por que escolher o FireEye Network Security?

O mecanismo FireEye MVX é a solução original e mais bem-sucedida[8] de proteção contra ameaças no mercado:

- Desde 2013, a FireEye descobriu mais ataques de dia zero à solta, em ativa exploração, do que todas as outras soluções combinadas.
- Em 2016, a Frost & Sullivan reconheceu a FireEye como líder indiscutível de mercado, com 56% de participação, mais que os dez concorrentes seguintes juntos[9].
- 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.

7 Forrester (maio de 2016). "The Total Economic Impact Of FireEye" (O impacto econômico total da FireEye).

8 IDC (2015). Worldwide Specialized Threat Analysis and Protection Market Shares (Participações no mercado de proteção e análise global e especializada de ameaças).

9 Frost & Sullivan (setembro de 2016). "Network Security Sandbox Market Analysis" (Análise de mercado de sandbox de segurança de rede).

Tabela 2. Benefícios do FireEye Network Security.

CAPACIDADE	VANTAGEM
Detectar e interromper as ameaças que os produtos de segurança tradicionais deixam passar	
Detecção de ameaças sem assinaturas (MVX)	Detecta ataques de múltiplos fluxos, de vários estágios, zero-day, polimórficos, de ransomware e outros ataques evasivos
Detecção em tempo real e retroativa	Detecta ameaças conhecidas e desconhecidas em tempo real, além de viabilizar a detecção retroativa de ameaças
Correlação de múltiplos vetores	Automatiza a validação e o bloqueio de ataques nos vetores de e-mail, endpoint e arquivo
Suporte para múltiplos sistemas operacionais, arquivos e aplicativos	Compatível com ambientes de endpoint heterogêneos para uma ampla variedade de aplicativos
Hipervisor reforçado	Previne a evasão
Responder rapidamente aos incidentes e limitar seu impacto	
Bloqueio em linha em tempo real	Interrompe os ataques imediatamente
Fluxos de trabalho de segurança integrados	Mudança de detecção para investigação e resposta
Alta disponibilidade (HA)	Defesa resistente
Detecção por IPS com base em assinaturas e com redução de ruído	Automatiza e acelera a triagem de alertas tradicionalmente ruidosos para eliminar a sobrecarga manual
Detecção e categorização de riskware	Categoriza malware crítico e não crítico para priorizar os recursos de resposta
Inteligência decisiva contextual	Acelera a contenção de ameaças avançadas com informações detalhadas sobre o ataque e o atacante
Adaptar-se continuamente ao cenário de ameaças em evolução	
Compartilhamento em tempo real de inteligência sobre ameaças	Evidências reais compartilhadas globalmente para bloquear imediatamente ataques desconhecidos e acelerar a resposta
NOVO **Inteligência sobre ameaças compartilhada e de terceiros (STIX)**	Assimilação de indicadores da FireEye e de terceiros nos mecanismos IDA compatíveis com STIX
Inteligência estratégica sobre ameaças	Permite uma avaliação proativa das mudanças no cenário de ameaças e viabiliza uma postura de segurança com vistas ao futuro
Expandir-se e continuar flexível conforme o crescimento da organização ou as mudanças no modo de entrega dos serviços de TI	
Larguras de banda suportadas	10 Mbps a 8 Gbps
Escala suportada	De um único local a milhares de locais para distribuições múltiplas
Formatos suportados	Físico, virtual e na nuvem
Modelos de distribuição	Segurança de rede integrada e segurança de rede distribuída com nós de rede inteligentes e arquitetura de serviço MVX

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 sobre ameaças em nível de país 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 responder a ataques cibernéticos. A FireEye tem mais de 6.600 clientes em 67 países, incluindo mais de 45 por cento das empresas da Forbes Global 2000.

FIREEYE™