FIREEYE™

FICHA TÉCNICA

FireEye Email Security Server Edition

Defesa adaptável, inteligente e expansível contra ameaças recebidas por e-mail

DESTAQUES

- Segurança abrangente para e-mails contra anexos maliciosos, URLs de phishing de informações pessoais, e-mails falsos, dia zero e ataques em várias etapas
- Suporte à análise de imagens dos sistemas operacionais Microsoft Windows e Apple macOS X
- Examina minuciosamente e-mails para encontrar ameaças escondidas em arquivos protegidos por senhas, anexos criptografados e URLs
- Obtém informações sobre ameaças em tempo real da nuvem FireEye DTI
- Prioriza e impede ameaças fornecendo insights sobre o contexto dos alertas
- Implementação local com serviço MVX integrado ou distribuído

Figura 1. Appliances de segurança de e-mail integrados incluindo EX 3500, EX 5500 e EX 8500.

Visão geral

O e-mail é o vetor mais vulnerável a ataques cibernéticos, pois é o ponto com maior volume de entrada de dados. As organizações enfrentam um número cada vez maior de desafios de segurança em e-mails com ameaças avançadas. A maioria das ameaças avançadas usam e-mails para entregar URLs vinculados a sites de phishing e anexos de arquivos transformados em armas. Sendo altamente direcionável e personalizável, o e-mail é o principal meio dos crimes cibernéticos.

O FireEye Email Security ajuda as organizações a reduzir o risco de violações causadas por ataques avançados em e-mails que podem custar caro. Implementado localmente, o FireEye Email Security – Server Edition é líder de mercado na identificação, isolamento e contenção imediata de ataques com base em URLs e anexos antes que estes adentrem o ambiente de uma organização. O Email Security usa plug-ins de contexto e detecção orientados por inteligência para detectar URLs maliciosas e benignas de phishing em uma plataforma real escalonável e de big data. O mecanismo sem assinatura Multi-Vector Virtual Execution™ (MVX) analisa anexos de e-mail e URLs vinculados a conteúdo baixável diante de uma ampla matriz mista de sistemas operacionais, aplicativos e navegadores de internet. As ameaças são identificadas com níveis mínimos de ruído e os falsos positivos são praticamente inexistentes.

A FireEye coleta uma série de informações de ameaças sobre adversários, investigações diretas de violações e por meio de milhões de sensores. O Email Security utiliza essas evidências concretas e inteligência contextual sobre ataques e agressores para priorizar alertas e interceptar ameaças em tempo real.

Com a integração com o FireEye Network Security e Endpoint Security, as organizações podem ampliar a visibilidade de ataques mistos de vários vetores e coordenar a proteção em tempo real.

Defesa contra ameaças recebidas por e-mail
Com todas as informações pessoais disponíveis on-line, um criminoso cibernético pode usar engenharia social para fazer com que praticamente qualquer usuário execute uma ação, clique em um URL ou abra um anexo.

O Email Security oferece detecção e prevenção de ameaças em tempo real contra ataques de obtenção de credenciais, personificação de remetentes e spear-phishing que geralmente contornam sistemas de defesa tradicionais de e-mails. Os e-mails são analisados e colocados em quarentena (bloqueados) se forem encontradas ameaças desconhecidas e avançadas escondidas em:

- Tipos de anexos, incluindo, entre outros: arquivos EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 e ZIP/RAR/TNEF
- Anexos protegidos por senha e criptografados
- Anexos protegidos por senha enviada em imagem
- URLs incorporados em e-mails, documentos do MS Office, arquivos PDF e comprimidos (ZIP, ALZIP, JAR) e outros tipos de arquivos (Uuencoded, HTML)
- Arquivos baixados por URLs e até por links de FTP
- URLs ofuscados, falsificados, encurtados e dinamicamente redirecionados
- URLs de phishing de credenciais e typosquatting
- Imagens desconhecidas dos sistemas operacionais Microsoft Windows e Apple macOS X, e vulnerabilidades de navegadores e aplicativos
- Código nocivo incorporado em e-mails de spear-phishing

Embora os ataques de ransomware comecem com um e-mail, é necessária uma conexão com um servidor de comando e controle para criptografar os dados. O Email Security identifica e bloqueia essas campanhas de malware de estágios múltiplos e de detecção difícil.

Detecção superior de ameaças

O Email Security ajuda a diminuir os riscos de falhas de segurança que custam caro ao identificar e isolar ataques avançados e direcionados, além de outros ataques evasivos camuflados como tráfego normal. Após serem detectados, os ataques são imediatamente contidos, analisados e classificados, para identificação mais rápida de ameaças futuras.

Integrantes essenciais do Email Security são a Advanced URL Defense, o mecanismo MVX e o MalwareGuard. Essas tecnologias usam aprendizado de máquina e análises para identificar ataques que escapam de sistemas de defesa tradicionais, com base em assinaturas e políticas.

Integrado à Advanced URL Defense, o PhishVision é um mecanismo de classificação de imagens que usa aprendizado profundo para compilar e comparar telas de marcas confiáveis e geralmente utilizadas como alvo em relação a telas vinculadas a URLs em um e-mail. Trabalhando simultaneamente com o PhishVision, o Kraken é um plug-in de detecção de phishing que aplica análises de conteúdo de domínios e páginas para aprimorar o aprendizado de máquina. O Skyfeed, um outro avanço na detecção de URLs, é um sistema totalmente automatizado, projetado especificamente para obtenção de informações sobre malware. Contas de redes sociais, blogs, fóruns e feeds com ameaças são coletados visando a descoberta de falsos negativos. A natureza polivalente do Advanced URL Defense oferece às organizações protegidas pelo Email Security defesa incomparável contra obtenção de credenciais e ataques de spear-phishing.

O MalwareGuard é um utilitário de aprendizado de máquina que analisa arquivos binários para gerar uma pontuação de suspeição. Todo arquivo portátil executável detectado é analisado pelo MalwareGuard. Uma decisão é tomada com base na pontuação, e as detecções acionadas pelo MalwareGuard recebem um nome.

O mecanismo 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 identifica ataques e malware nunca vistos anteriormente para impedir a infecção e o comprometimento.

Redução de fugas

O Email Security possui um recurso de controle em tempo real para defesa contra ataques que fogem de solicitações de vários objetos. O mecanismo MVX detecta malware que exige vários downloads e fornece os objetos remotos solicitados pelo código amostrado. O controle em tempo real reduz falsos negativos em downloads em várias etapas, ataques avançados de spear-phishing e invasões avançadas de ransomware.

Os invasores também tentam se desvencilhar da tecnologia usada para detecção de URLs falsos. Parte integrante da Advanced URL Defense, os mecanismos de redução de fugas em sites de phishing estão em constante evolução. As reduções de fugas estão sendo sempre aprimoradas no Advanced URL Defense. Outro mecanismo de redução de fugas, as imagens de visitantes podem ser personalizadas para personificar um endpoint “usado” quando um objeto potencialmente malicioso é executado. Muitas técnicas de fuga são bloqueadas quando a imagem de visitante reproduz um domínio de endpoint, domínio de usuário, dados de Outlook e histórico de navegação.

Integração para aprimoramento da eficiência no manuseio de alertas
O Email Security analisa todos os anexos e URLs em e-mails para identificar os ataques avançados de hoje em dia com precisão. Atualizações em tempo real de todo o ecossistema de segurança da FireEye, combinadas com a atribuição de alertas a autores de ameaças conhecidos, fornecem contexto para priorização e ação contra alertas críticos e bloqueio de ameaças avançadas em e-mails. As ameaças conhecidas, desconhecidas e não baseadas em malware são identificadas com níveis mínimos de ruído e falsos positivos para que os recursos sejam concentrados em ataques reais, reduzindo as despesas operacionais. A categorização do riskware distingue entre tentativas autênticas de violação e atividades indesejáveis, mas menos nocivas (como adware e spyware) para priorizar a resposta aos alertas.

Adaptação rápida às evoluções do cenário de ameaças
O Email Security ajuda a sua organização a adaptar a defesa proativa contra ameaças trazidas por e-mail usando inteligência em tempo real da nuvem FireEye Dynamic Threat Intelligence (DTI). Inteligência profunda sobre ameaças e invasores, que combina informações sobre adversários, sistemas e vítimas para:

- Fornecer visibilidade ampla e oportuna das ameaças
- Identificar capacidades e recursos específicos do malware e dos anexos nocivos detectados
- Fornecer insights contextuais para priorizar e acelerar a resposta
- Determinar a identidade e as motivações prováveis de um agressor e rastrear as atividades dele em sua organização
- Reescrever todos os URLs incorporados a um e-mail para proteger usuários de links maliciosos
- Identificar ataques de spear-phising retroativamente e evitar o acesso a sites de phishing com a exibição destacada de URLs nocivos

Integração de fluxos de trabalho de resposta
O Email Security funciona perfeitamente com o FireEye Helix e o FireEye Central Management.

- Como um componente da plataforma de operações de segurança — a FireEye Helix —, ele oferece visibilidade em toda a infraestrutura. O FireEye Helix aumenta os alertas de terceiros e e-mail com inteligência, faz correlação com terminal, automação e dicas investigativas. Com esses recursos, o FireEye Helix enfrenta ameaças invisíveis e viabiliza decisões de especialistas.
- O Central Management correlaciona alertas do Email Security e do Network Security, para oferecer uma visão mais ampla do ataque e definir regras de bloqueio que impeçam a propagação do ataque.
- O Central Management é compatível com rotulagem com base em funções para saber quem está sendo alvo.
- O Central Management é compatível com resposta a alertas e correção com base em critérios baseados em função.

Recursos adicionais

Regras com base em YARA permitem personalização
O Email Security permite que analistas de segurança especifiquem e testem as regras personalizadas para analisar anexos de e-mail que possam conter ameaças direcionadas à organização.

Proteção contra a personificação de executivos
O Email Security – Server Edition oferece a capacidade de bloquear ameaças à segurança e e-mails comerciais (BEC - business email compromises) para impedir que funcionários de alto nível sejam personificados. É criada uma política que compara os nomes exibidos em e-mails recebidos com uma lista com remetentes aprovados.

Gerenciamento de filas, alertas de mensagens e quarentena
O Email Security – Server Edition proporciona um alto grau de controle sobre as mensagens de e-mail examinadas. Para as distribuições em modo de proteção, as mensagens podem ser rastreadas e gerenciadas conforme elas passam pela fila MTA. Os atributos de e-mail podem ser utilizados para pesquisa e confirmação de que as mensagens foram recebidas, analisadas e entregues ao próximo estágio, e as tendências ao longo do tempo podem ser monitoradas por meio de um painel intuitivo. Listas explícitas de permissão e bloqueio proporcionam controle personalizado sobre o processamento de e-mail. É possível procurar e selecionar atributos de alerta comuns. E as operações em massa podem ser executadas em mensagens de alertas e quarentena.

Modo de proteção ativa ou apenas de monitoramento
O Email Security pode analisar e-mails e pôr as ameaças em quarentena para oferecer proteção ativa. Para distribuições destinadas apenas ao monitoramento, as organizações apenas configuraram uma regra transparente de cópia oculta para enviar as cópias de e-mails ao Email Security para a análise.

Opções de distribuição versáteis

O Email Security – Server Edition oferece várias opções de distribuição, conforme as necessidades e o orçamento da organização:

- **Segurança de e-mail integrada:** appliance de hardware completo e autônomo, com um serviço MVX integrado para proteger uma entrada de e-mail em um único local. O FireEye Email Security é uma solução fácil de gerenciar e que pode ser distribuída em menos de 60 minutos. Ele não requer regras, políticas ou ajustes.
- **Segurança de e-mail distribuída:** appliances expansíveis com um serviço MVX compartilhado centralmente, para proteger as entradas de e-mail dentro das organizações.
- **Nó de e-mail inteligente:** appliances virtuais que analisam o tráfego de e-mail para detectar e bloquear tráfego nocivo e enviar as atividades suspeitas, através de uma conexão criptografada, ao serviço MVX para um veredito de análise definitivo.
- **MVX Smart Grid:** serviço MVX situado no local, centralizado e elástico, que oferece expansibilidade transparente, tolerância a falhas N+1 e balanceamento de carga automático.

  A passagem de um dispositivo de hardware integrado para o MVX Smart Grid fornece capacidade para detectar e analisar as ameaças recebidas em e-mail durante os horários de pico de transferência de mensagens.
- **FireEye Cloud MVX:** Assinatura do serviço MVX, que assegura privacidade ao analisar o tráfego no nó de e-mail inteligente. Somente objetos suspeitos são enviados por uma conexão criptografada para o serviço MVX, onde os objetos considerados benignos são descartados.

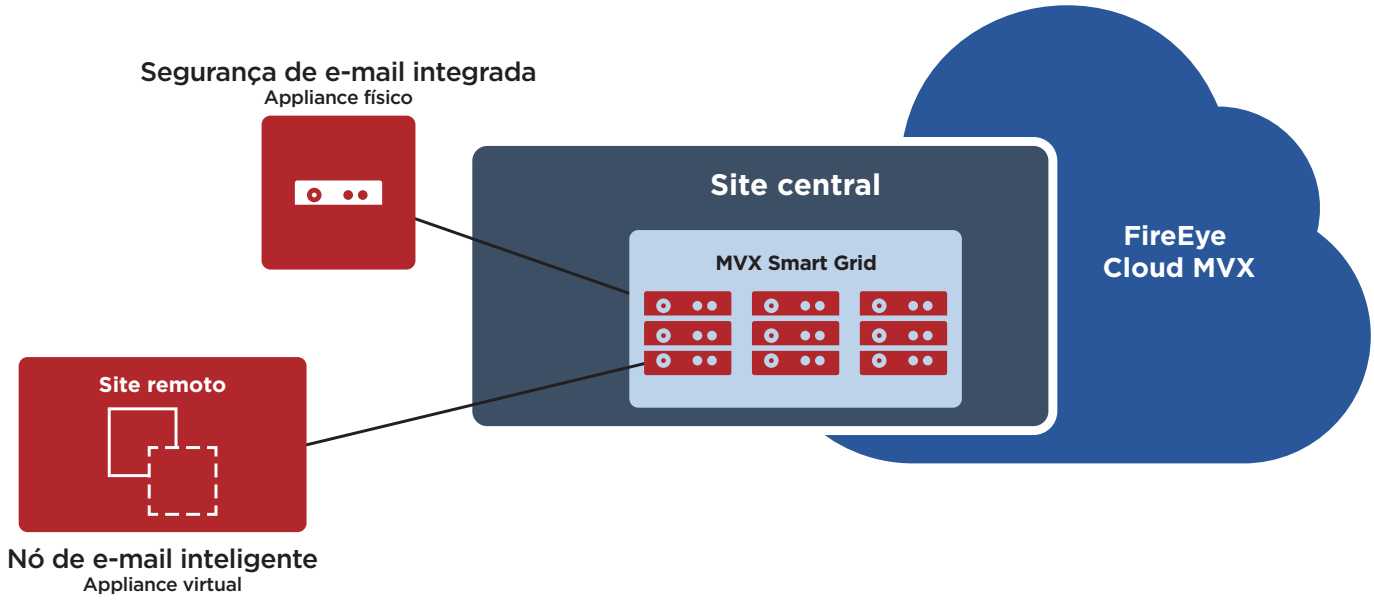

Figura 2. Modelos de implantação distribuídos e ampliados para segurança de e-mail.

Tabela 1. Especificações técnicas.

	EX 3500	**EX 5500**	**EX 8500**
Desempenho*	Até 700 anexos diferentes por hora	Até 1.800 anexos diferentes por hora	Até 2.650 anexos diferentes por hora
Portas de interface de rede	2 unidades de 1GigE BaseT	2 unidades de 1GigE BaseT	4 unidades SFP+ (compatíveis com 10GigE Fiber, 10GigE Copper, 1GigE Copper), 2 unidades 1GigE BaseT
Portas de gerenciamento	2 unidades de 1GigE BaseT	2 unidades de 1GigE BaseT	2 unidades de 1GigE BaseT
Monitoramento de IPMI	Incluídas	Incluídas	Incluídas
Porta VGA (painel traseiro)	Incluídas	Incluídas	Incluídas
Portas USB (painel traseiro)	4 portas USB tipo A traseiras	2 portas USB tipo A frontais, 2 portas USB tipo A traseiras	2 portas USB tipo A frontais, 2 portas USB tipo A traseiras
Porta serial (painel traseiro)	115.200 bps, sem paridade, 8 bits, 1 stop bit	115.200 bps, sem paridade, 8 bits, 1 stop bit	115.200 bps, sem paridade, 8 bits, 1 stop bit
Capacidade de armazenamento	4 unidades de disco rígido de 2 TB, RAID 10 e 3,5”, FRU	4 unidades de disco rígido de 2 TB, RAID 10 e 3,5”, FRU	4 unidades de disco rígido de 2 TB, RAID 10 e 3,5”, FRU
Gabinete	1 RU, para rack de 19”	2 RU, para rack de 19”	2 RU, para rack de 19”
Dimensões do chassi (L x P x A)	437 x 650 x 43,2 mm	438 x 620 x 88,4 mm	438 x 620 x 88,4 mm
Fonte de alimentação CA	Redundante (1+1) de 750 W, 100–240 VCA, 9–4,5 A, 50–60 Hz, entrada IEC 60320-C14, FRU	Redundante (1+1) de 800 W, 100–240 VCA, 9–4,5 A, 50–60 Hz, entrada IEC 60320-C14, FRU	Redundante (1+1) de 800 W, 100–240 VCA, 9–4,5 A, 50–60 Hz, entrada IEC 60320-C14, FRU
Fonte de alimentação CC	Não disponível	Não disponível	Não disponível
Potência térmica máxima	245 watts (836 BTU por hora)	456 watts (1.556 BTU por hora)	530 watts (1.808 BTU por hora)
MTBF (h)	54.200 horas	57.401 horas	53.742 horas
Peso líquido/total (kg)	13,6 kg/18,6 kg	20,0 kg/29,6 kg	20,2 kg/29,8 kg
Segurança do dispositivo	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Conformidade EMC	FCC Parte 15 ICES-003 Classe A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 e V-3/2015	FCC Parte 15 ICES-003 Classe A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 e V-3/2015	FCC Parte 15 ICES-003 Classe A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 e V-3/2015
Certificações de segurança	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
Conformidade ambiental	Diretiva RoHS 2011/65/EU; REACH; Diretiva WEEE 2012/19/EU	Diretiva RoHS 2011/65/EU; REACH; Diretiva WEEE 2012/19/EU	Diretiva RoHS 2011/65/EU; REACH; Diretiva WEEE 2012/19/EU
Temperatura de funcionamento	0 ~ 35 °C	0 ~ 35 °C	0 ~ 35 °C
Umidade relativa de funcionamento	10 ~ 95% a 40 °C, sem condensação	10 ~ 95% a 40 °C, sem condensação	10 ~ 95% a 40 °C, sem condensação
Altitude de funcionamento	3.000 m	3.000 m	3.000 m

* Todos os valores de desempenho variam dependendo da configuração do sistema e do perfil de tráfego de e-mail sendo processado. Tamanho dos appliances com base em anexos exclusivos por hora.

Tabela 2. Especificações do FireEye MVX Smart Grid.

	VX 5500	**VX 12500**
Sistemas operacionais compatíveis	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
Desempenho*	Até 480 anexos diferentes por hora	Até 3.780 anexos diferentes por hora
Alta disponibilidade**	N+1	N+1
Portas de gerenciamento (painel traseiro)	1 porta 10/100/1000 Mbps BASE-T	1 porta 10/100/1000 Mbps BASE-T
Portas de cluster (painel traseiro)	3 portas 10/100/1000 Mbps BASE-T	1 porta 10/100/1000 Mbps BASE-T, 2 portas BASE-T de 10 Gbps
Porta IPMI (painel traseiro)	Incluídas	Incluídas
Teclado numérico e LCD frontal	Não disponível	Incluídas
Portas VGA	Incluídas	Incluídas
Portas USB (painel traseiro)	4 portas USB tipo A	2 portas USB tipo A
Porta serial (painel traseiro)	115.200 bps, sem paridade, 8 bits, 1 stop bit	115.200 bps, sem paridade, 8 bits, 1 stop bit
Capacidade das unidades	2 unidades de disco rígido SAS de 2TB, 3,5", RAID 1, troca a quente, FRU	4 unidades de disco rígido de 4 TB, 3,5", SAS3 HDD, RAID1, FRU
Gabinete	1 RU, para rack de 19"	2 RU, para rack de 19"
Dimensões do chassi (L x P x A)	17. 437 x 650 x 43,2 mm	437 x 851 x 89 mm
Fonte de alimentação CC	Não disponível	Não disponível
Fonte de alimentação CA	Redundante (1+1), 750 W, 100–240 VCA, 8–3,8 A, 50–60 Hz, entrada IEC60320-C14, troca a quente, FRU	Redundante (1+1), 800 W: 100–127 V, 9,8 A–7 A, 1.000 W: 220–240 V, 7–5 A, 50–60 Hz, FRU, entrada IEC60320-C14, FRU
Consumo de energia máximo	285 W	760 W
Dissipação térmica máxima	972 BTU por hora	2594 BTU por hora
Tempo médio entre falhas (MTBF)	54.200 horas	38.836 horas
Peso líquido / enviado	15 kg/21,8 kg	21 kg/40,2 kg
Certificação de segurança	FIPS 140-2 Nível 1, CC NDPP v1.1	FIPS 140-2 Nível 1, CC NDPP v1.1
Conformidade regulatória de segurança	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

* Todos os valores de desempenho variam dependendo da configuração do sistema e do perfil de tráfego sendo processado.

** Com configurações apropriadas de hardware redundante.

Tabela 3. Nó inteligente FireEye Email Security, especificações dos sensores virtuais.

	EX 5500V
Sistemas operacionais compatíveis	Microsoft Windows, Apple macOS X
Desempenho*	Até 1.250 anexos diferentes por hora
Portas de monitoramento de rede	2
Portas de gerenciamento de rede	2
Núcleos de CPU	8
Memória	16 GB
Capacidade das unidades	384 GB
Adaptadores de rede	VMXNet 3, vNIC
Suporte para hipervisor	VMWare ESXi 6.0 ou posterior

* Todos os valores de desempenho variam dependendo da configuração do sistema e do perfil de tráfego sendo processado.

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 responder a ataques cibernéticos.