FIREEYE™

Ficha técnica

FireEye Email Security Cloud Edition

Proteção com base em nuvem que identifica, analisa e bloqueia ataques de e-mail

Destaques

- Oferece segurança abrangente para e-mails recebidos e enviados
- Consolida a pilha de segurança de e-mails com uma solução abrangente de fornecedor único
- Suporta regras personalizadas do YARA para melhorar a eficácia da detecção de ameaças
- Habilita o recurso automático do Office 365 para remover e-mails que se tornam maliciosos após a entrega
- Integra-se com qualquer provedor de e-mails de terceiros
- Fornece conhecimento profundo sobre ataques e invasores de investigações de linha de frente e observações de adversários
- Atende aos requisitos de segurança do FedRAMP

"O e-mail é fundamental para todos os ambientes de colaboração, portanto a implantação do FireEye Email Security nos permite reduzir os riscos de comprometimento desse canal altamente explorado usando uma única solução."

Nils Göldner
Parceiro de gerenciamento e consultor de nuvem
Blackboat GmbH

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 ameaças baseadas em e-mail, como spam, malware e ameaças avançadas. A maioria das ameaças avançadas chega por e-mail na forma de URLs vinculados a sites de phishing de credenciais, solicitações fraudulentas de transferências bancárias e anexos armamentizados. A natureza altamente direcionável e personalizável dos e-mails permite que criminosos cibernéticos a explorem com sucesso, fazendo dos e-mails a opção mais usada para crimes cibernéticos.

O FireEye Email Security pode reduzir custos e aumentar a produtividade dos funcionários por meio de uma única solução de segurança que minimiza o risco de violações dispendiosas causadas por ataques avançados de e-mail. Implementado na nuvem, o FireEye Email Security é um gateway de e-mail seguro com todos os recursos que lidera o mercado em identificação, isolamento e contenção imediata de ataques de personificação, com base em URLs e anexos antes que estes adentrem o ambiente de uma organização. Com a correção automática do Office 365 (O365), os e-mails que se tornam retroativamente maliciosos após a entrega na caixa de entrada de um usuário podem ser extraídos. O FireEye Email Security também verifica o tráfego de e-mails enviados em busca de ameaças avançadas, spam e vírus.

Usando uma confluência de plug-ins de contexto e detecção orientados por inteligência, as URLs maliciosas são detectadas por uma plataforma real escalonável e de big data. Os nomes de remetentes e endereços de e-mail são verificados quanto à autenticidade e o conteúdo é examinado visando identificar táticas de personificação para impedir fraudes com executivos e outros ataques sem malware. O mecanismo sem assinatura Multi-Vector Virtual Execution™ (MVX) analisa anexos de e-mail e URLs 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.

O 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 reais e inteligência contextual sobre ataques e maus agentes para priorizar alertas e interceptar ameaças em tempo real.

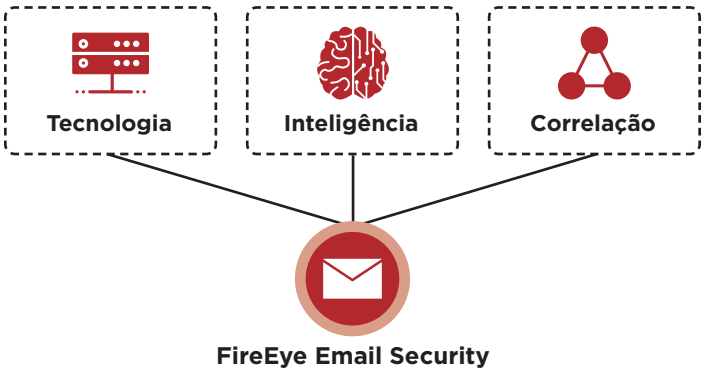

Figura 1. Um gateway de e-mail seguro.

Com a integração com o FireEye Network 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 as informações pessoais prontamente 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 proteção em tempo real contra ataques de obtenção de credenciais, personificação de remetentes e spear-phishing que geralmente contornam serviços 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:

- Todos os tipos de anexos, incluindo 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
- URLs incorporados em e-mails, PDFs e documentos do Microsoft Office
- URLs de phishing de credenciais e typosquatting
- Vulnerabilidades desconhecidas de SOs, 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 e o mecanismo MVX. Essas tecnologias usam aprendizado de máquina de última geração e análises para identificar ataques quem 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 páginas web e de login referenciadas por 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. Outro avanço na detecção de URLs é o Skyfeed, 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.

Um e-mail pode começar como benigno para passar pelas defesas de segurança. Somente após a entrega na caixa de entrada de um destinatário é que o e-mail se torna malicioso. O Email Security—Cloud Edition analisa e alerta retroativamente quando um e-mail se torna malicioso após a entrega. Por meio da API do O365, os e-mails que se tornam retroativamente maliciosos podem ser extraídos automaticamente da caixa de entrada criando uma política de correção automática do O365.

O mecanismo MVX detecta ataques de dia zero, de fluxos múltiplos e outros ataques evasivos com análise dinâmica e sem assinaturas em ambientes virtuais seguros. Ele interrompe as fases de infecção e comprometimento da cadeia de destruição do ataque cibernético identificando malware e exploits nunca antes vistos.

Proteção AVAS aprimorada

O Email Security—Cloud Edition está disponível com proteção antispam e antivírus (AVAS) para detectar ataques comuns que utilizam correspondência de assinatura convencional, assim como técnicas de personificação.

Ataques de personificação, como falsificação de executivos (geralmente chamadas de comprometimento de e-mails comerciais), continuam trazendo prejuízos às empresas. Isso se deve em parte à falta de indicadores de ameaças tradicionais, como anexos ou links maliciosos, já que os ataques são livres de malware e dependem de técnicas de engenharia social. Para combater esses ataques e proteger os clientes, a FireEye desenvolveu algoritmos, sistemas e ferramentas inovadores, especializadas na detecção e defesa contra personificação.

Um indicador comum de um ataque por e-mail é o domínio do remetente. Ao criarem uma campanha de personificação, criminosos cibernéticos enviam e-mails com ataques de um domínio similar ao da pessoa ou empresa sendo personificada, geralmente algumas horas após a criação do domínio.

O Email Security tem a capacidade de determinar a idade a maturidade de um domínio, usando as ferramentas próprias Newly Existing Domains (NED) e Newly Observed Domains (NOD). Os domínios identificados como novos são tratados com suspeita e inspecionados minuciosamente visando a identificar outros indicadores de ataques, como typosquatting e falsificação de nome do remetente ou nome de usuário.

Em vez de ter que passar pelo processo de comprar e registrar um domínio, os criminosos cibernéticos podem simplesmente alterar o nome de exibição ou nome de usuário do remetente, fazendo com que o e-mail aparente ter vindo de fonte conhecida. O Email Security proporciona proteção contra essa falsificação de remetentes ao determinar a autenticidade de nome de exibição e de usuário usando a identificação de nomes conhecidos.

Varredura de mensagens enviadas

O Email Security detecta ameaças avançadas desconhecidas, incluindo anexos maliciosos e URLs de phishing entregues por meio de mensagens de e-mail enviadas. O tráfego de e-mails enviados também é verificado em busca de malware e spam para proteger os domínios de uma organização da inclusão na lista negra.

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.

Adaptação rápida às evoluções do cenário de ameaças

O Email Security ajuda sua organização a adaptar continuamente a defesa proativa contra ameaças recebidas por e-mail. O Email Security gera sua própria inteligência contra ataques em vez de confiar em feeds de terceiros, geralmente atrasados. Inteligência própria, específica para ameaças em e-mails (ou Smart DNS), recursos de coleta de dados, especialistas em segurança de e-mails e analistas de ameaças formam a infraestrutura de base para tecnologias aprimoradas antispam e de detecção de personificação. Inteligência aprofundada 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
- Identificar ataques de spear-phising retroativamente e evitar o acesso a sites de phishing reescrevendo os URLs nocivos

As organizações podem acessar o portal do Email Security para visualizar alertas em tempo real, criar regras inteligentes personalizadas e gerar relatórios. Regras inteligentes personalizadas permitem que sua organização crie políticas e regras com base em várias condições granulares.

Integração de fluxos de trabalho de resposta

O Email Security trabalha em conjunto com outras soluções da FireEye para ajudar a automatizar os fluxos de trabalho de resposta a alertas:

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.

A plataforma FireEye Helix trabalha com o Email Security e foi desenvolvida especificamente para simplificar, integrar e automatizar operações de segurança.

Facilidade de distribuição e proteção entre empresas

O Email Security—Cloud Edition é baseado na nuvem, sem a necessidade de instalação de hardware ou software. Ele é ideal para organizações que estão migrando sua infraestrutura de e-mail para a nuvem. Essa migração acaba com a complexidade de aquisição, instalação e gerenciamento de uma infraestrutura física.

O Email Security—Cloud Edition se integra perfeitamente a sistemas de e-mail baseados na nuvem, como o Microsoft Office 365 com Exchange Online Protection e G Suite.

Para se protegerem de e-mails nocivos e fraudulentos, as organizações simplesmente encaminham as mensagens para o Email Security, que primeiro analisa os e-mails em busca de spam e malware e as táticas de personificação conhecidas. Em seguida, ele utiliza tecnologias de defesa de URLs e o mecanismo MVX, uma câmara de destruição sem assinaturas, para analisar todos os anexos e URLs com o intuito de detectar ameaças e impedir ataques em tempo real.

Recursos adicionais

Regras com base em YARA permitem personalização

O Email Security permite que os analistas usem regras personalizadas do YARA para gerenciar e aprimorar detecções, interromper as ameaças mais recentes e identificar campanhas em andamento.

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. As organizações só precisam atualizar seus registros MX para encaminhar mensagens à FireEye. Para distribuições destinadas apenas ao monitoramento, as organizações só precisam configurar uma regra de BCC transparente para enviar cópias de e-mails à FireEye para análise do MVX.

Autorizações e certificações

ISO 27001

O Email Security—Cloud Edition atende ao padrão ISO 27001 de segurança de informações, garantindo a administração segura de centros de dados.

FedRAMP

O Email Security—Cloud Edition com proteção AVAS atende às exigências de segurança FedRAMP para serviços de nuvem operados pelo governo e por entidades de educação pública.

SOC 2 tipo 2

O Email Security—Cloud Edition atende à certificação de segurança e confidencialidade para controles de organização de serviço (Service Organization Controls, SOC 2) tipo 2 do Instituto Americano de Contadores Públicos Certificados (American Institute of Certified Public Accountants, AICPA).

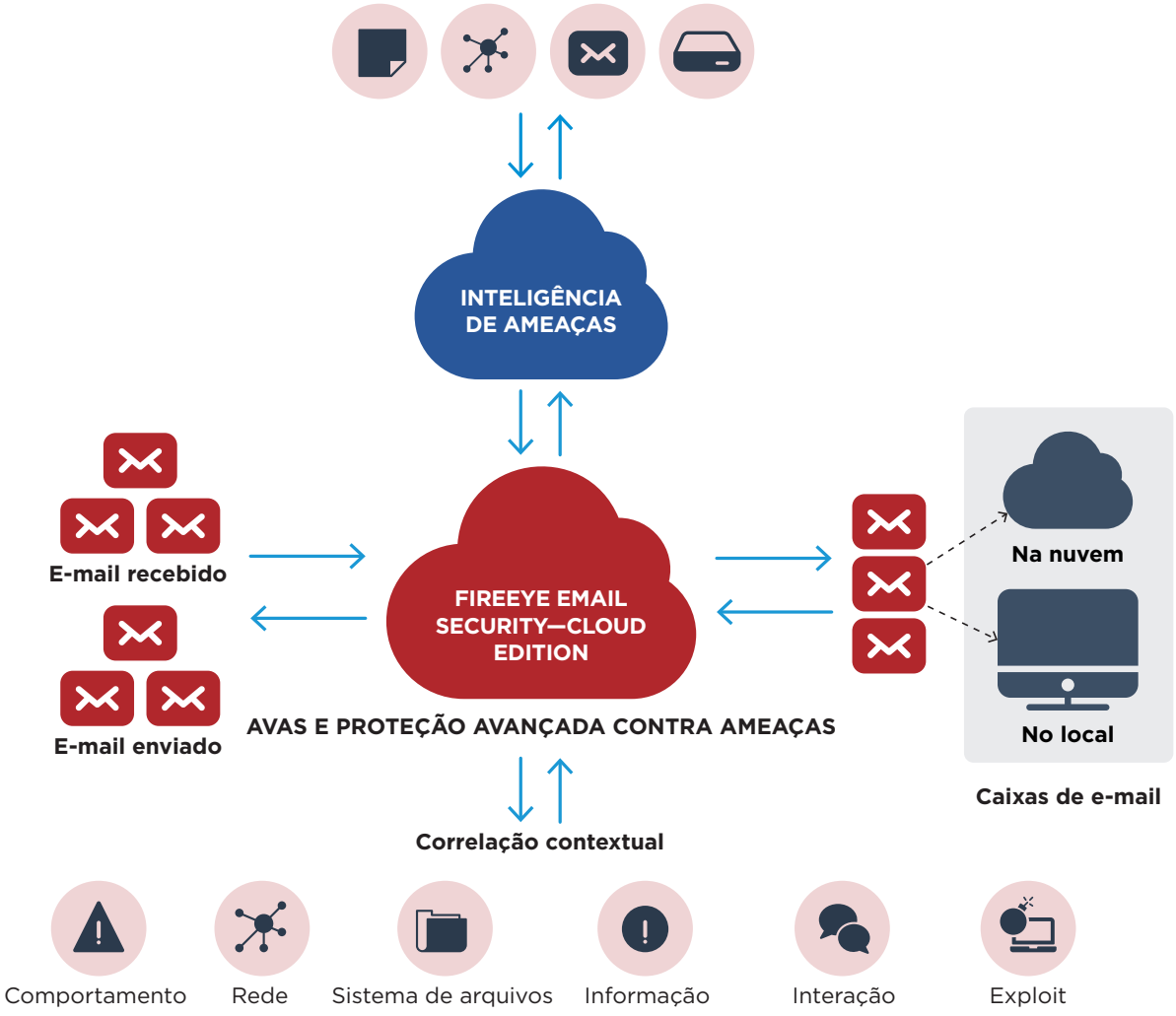

Figura 2. FireEye Email Security – Cloud Edition.

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

©2019 FireEye, Inc. Todos os direitos reservados. FireEye é uma marca registrada da FireEye, Inc. Todos os outros nomes de marcas, produtos e serviços são ou podem ser marcas comerciais ou marcas de serviços de seus respectivos proprietários. E-EXT-DS-US-EN-000087-06

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.