FIREEYE™

FICHA TÉCNICA

File Protect

Detecte e elimine malware residente em compartilhamentos de arquivos e armazenamentos de conteúdo

DESTAQUES

- Encontra malware latente que não é detectado pelos mecanismos de antivírus tradicionais
- Pode ser distribuído em quarentena ativa (modo de proteção) ou somente análise (modo de monitoramento)
- Oferece varreduras recursivas, programadas e sob solicitação de compartilhamentos de arquivos compatíveis com CIFS e NFS
- Oferece proteção proativa para o Microsoft OneDrive e o SharePoint
- Inclui a análise de uma ampla gama de tipos de arquivos, como PDFs, documentos do Microsoft Office e arquivos de multimídia
- Integra-se com o pacote antivírus FireEye Endpoint Security para simplificar a priorização de respostas a incidentes e as convenções de nomenclatura
- Compartilha dados de ameaças através da FireEye Central Management e da nuvem DTI da FireEye

Visão geral

O FireEye File Protect protege ativos de dados em uma ampla gama de tipos de arquivos contra ataques originados de e-mails, ferramentas de transferências de arquivos online, da nuvem e de dispositivos portáteis de armazenamentos de arquivos. Tais ataques podem se espalhar para compartilhamentos de arquivos e repositórios de conteúdos. O File Protect analisa compartilhamentos de arquivos em rede e armazenamentos de gerenciamento de conteúdo para detectar e colocar em quarentena um malware capaz de contornar firewalls de próxima geração, sistemas de prevenção de intrusões, antivírus e gateways.

Desafios de malwares no compartilhamento de arquivos

Os ataques cibernéticos avançados de hoje usam malware sofisticado e táticas de ameaças persistentes avançadas (Advanced Persistent Threat, APT) para atravessar as defesas e se espalhar lateralmente pelos compartilhamentos de arquivos e repositórios de conteúdo. Isso permite que o malware estabeleça uma presença a longo prazo na rede e infecte múltiplos sistemas, até aqueles que estão off-line. Muitos data centers corporativos continuam especialmente vulneráveis ao malware avançado baseado em conteúdo, porque as defesas tradicionais não são eficientes contra esses ataques, que com frequência entram na rede por meios legítimos. Os criminosos cibernéticos aproveitam essas vulnerabilidades para espalhar malware nos compartilhamentos de arquivos da rede e incorporam código nocivo a vastos repositórios de dados, resultando em uma ameaça persistente mesmo após a correção.

A importância da proteção do conteúdo de arquivo

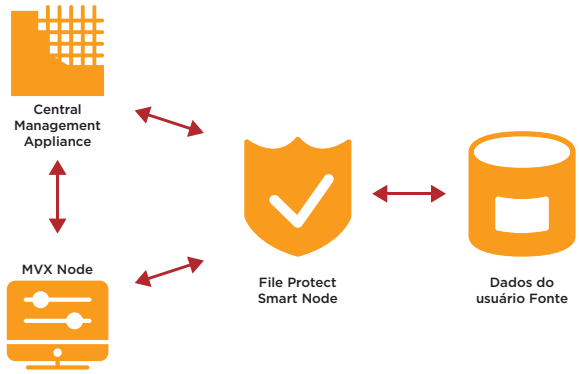
Sem uma forma de detectar malware no conteúdo, as APTs podem explorar os ativos da rede para extrair informações proprietárias e causar muitos danos. O File Protect analisa compartilhamentos de arquivos e repositórios de conteúdo corporativo usando o mecanismo patenteado FireEye Multi-Vector Virtual Execution™ (MVX), que detecta código nocivo de dia zero incorporado a tipos comuns de arquivos (PDF, MS Office, vCards, ZIP/RAR/TNEF etc.) e conteúdo de multimídia (QuickTime, MP3, Real Player, JPG, PNG etc.). O File Protect executa varreduras recursivas, programadas e sob solicitação em armazenamentos de conteúdo e compartilhamentos de arquivos de rede acessíveis para identificar e colocar em quarentena o malware residente. Isso suspende um estágio fundamental do ciclo de vida dos ataques avançados.

Revelando ameaças desconhecidas no dia zero

O FireEye FX usa o mecanismo FireEye MVX para inspecionar cada arquivo e confirmar a existência de ataques de dia zero ou de código malicioso. O mecanismo FireEye 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.

O poder do MVX Smart Grid

O FireEye MVX Smart Grid aprimora o FireEye Network Security com uma arquitetura de implementação flexível e escalável através de uma nuvem híbrida ou privada. O MVX Smart Grid usa uma abordagem inovadora para proteger de maneira mais eficaz campi, filiais de escritórios e usuários remotos separando o mecanismo MVX de Smart Nodes™ virtuais e de hardware. O Smart Nodes analisa o tráfego de internet para detectar e bloquear ameaças usando uma variedade de técnicas, tais como análise estática, analítica, IPS, inteligência aplicada e muito mais, enquanto o mecanismo MVX realiza análises da dinâmica central.



Proteção para o Microsoft OneDrive e o SharePoint

O File Protect faz varredura de conteúdo de maneira contínua para alertar e colocar permanentemente em quarentena qualquer malware descoberto em repositórios do OneDrive e do SharePoint. A plataforma aproveita o protocolo WebDAV para se integrar com segurança a serviços do SharePoint e proteger fluxos de trabalho corporativos que utilizam repositórios do SharePoint.

Regras com base em YARA permitem personalização

O File Protect suporta regras YARA personalizadas para analisar grandes quantidades de arquivos em busca de ameaças específicas à organização.

Priorização de incidentes simplificada

Com o FireEye Endpoint Security, todos os objetos maliciosos podem ser analisados mais minuciosamente para determinar se os fornecedores de antivírus conseguiram detectar o malware detido pelo File Protect. Isso permite que as empresas priorizem a resposta a incidentes de forma eficiente e utilizem convenções de nomenclatura comuns para o malware conhecido.

Compartilhamento de inteligência sobre malware

A inteligência resultante sobre ameaças, gerada dinamicamente e em tempo real, pode ajudar todos os produtos da FireEye a proteger a rede local por meio da integração com a Central Management. Essa inteligência pode ser compartilhada globalmente pela nuvem do FireEye Dynamic Threat Intelligence (DTI) para notificar todos os assinantes sobre ameaças emergentes.

Nenhum ajuste fino de regras e quase nenhum falso positivo

Diferentemente dos sistemas IPS, o File Protect não requer ajuste. Modos flexíveis de distribuição incluem quarentena ativa e monitoramento apenas para análise. Isso permite que as empresas saibam quanto malware reside em compartilhamentos de arquivos e possam deter ativamente a disseminação lateral do malware.

Content Smart Nodes para proteção, sempre que necessário

Com o FireEye Content Smart Nodes, gerentes de conteúdo e segurança têm uma solução virtual flexível para proteger conteúdo essencial em toda a empresa. Combinada com a FireEye MVX Smart Grid, a proteção de conteúdo pode ser dimensionada e distribuída com flexibilidade, onde você precisar.

Fatores de formulário flexíveis

Ideais para qualquer ambiente de rede, os clientes podem escolher entre o FireEye Content Smart Nodes ou equipamentos de hardware tradicionais no local.

Tabela 1. FireEye Content Smart Node.

	FX 2500V
Sistemas operacionais compatíveis	Microsoft Windows, MacOS X
Desempenho	40.000 arquivos/dia
Portas de interface de rede	Ether 1, Ether 2
Núcleos de CPU	2
Memória	8 GB
Capacidade das unidades	512 GB
Suporte para hipervisor	VMWare ESXi 6.0 ou posterior

Tabela 2. Especificações técnicas da FireEye.

	FX 6500
Desempenho*	Até 70.000 arquivos por dia
Portas de interface de rede	2 x 1GigE BaseT
Porta IPMI (painel traseiro)	Incluídas
Portas USB (painel traseiro)	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
Capacidade de armazenamento	4 unidades de disco rígido de 2 TB, RAID 10 e 3,5", FRU
Gabinete	2 RU, para rack de 19"
Dimensões do chassi (L x P x A)	438 x 620 x 88,4 mm
Fonte de alimentação CA	Redundante (1+1) de 800 W, 100–240 VCA, 9–4,5 A, 50–60 Hz, entrada IEC 60320-C14, FRU
Consumo de energia máximo	530 watts
Dissipação térmica máxima	1.808 BTU/h
Tempo médio entre falhas (MTBF)	53.742 h
Peso líquido/total (kg)	20,2 kg/29,8 kg
Certificações de segurança	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Certificações EMC/EMI	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
Conformidade regulatória	Diretiva RoHS 2011/65/EU; REACH; Diretiva WEEE 2012/19/EU
Temperatura de funcionamento	0 ~ 35 °C
Umidade relativa de funcionamento	10 ~ 95% a 40 °C, sem condensação
Altitude de funcionamento	3.000 m

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.