FIREEYE™

FICHA TÉCNICA

File Protect

Detecta y elimina malware en archivos compartidos y dispositivos de almacenamiento de contenido

ASPECTOS DESTACADOS

- Encuentra malware latente que no detectan los motores antivirus tradicionales.
- Se implementa en cuarentena activa (modo de protección) o en análisis solamente (modo de supervisión).
- Ofrece análisis a pedido, programados y recurrentes de recursos compartidos de archivos compatibles con protocolos CIFS y NFS.
- Ofrece protección proactiva para OneDrive y Sharepoint de Microsoft
- Incluye el análisis de una amplia gama de tipos de archivo como PDF, documentos de Microsoft Office y archivos multimedia.
- Se integra con FireEye Endpoint Security para optimizar el establecimiento de prioridades de la respuesta ante incidentes y los convenios de nomenclatura.
- Comparte los datos de las amenazas a través de FireEye Central Management y la nube FireEye DTI

Descripción general

FireEye File Protect protege los activos de datos en una amplia gama de tipos de archivo contra los ataques que se originan desde el correo web, las herramientas de transferencia de archivos en línea, la nube y los dispositivos de almacenamiento de archivos portátiles. Estos ataques pueden propagarse a archivos compartidos y dispositivos de almacenamiento. File Protect analiza los recursos compartidos de archivos de la red y los dispositivos de almacenamiento para detectar y poner en cuarentena el malware que elude el firewall, sistema de detección de intrusiones (Intrusion Prevention System, IPS), el antivirus y las vías de acceso.

Desafíos del malware en archivos compartidos

Los ataques cibernéticos avanzados de la actualidad usan tácticas sofisticadas de malware y amenazas persistentes avanzadas (APT) para penetrar en las defensas y propagarse lateralmente a través de archivos compartidos y dispositivos de almacenamiento de contenido. Esto permite que el malware establezca una presencia a largo plazo en la red y que infecte varios sistemas, incluso aquellos que no están conectados a Internet. Muchos centros de datos corporativos quedan especialmente vulnerables ante el malware avanzado basado en contenido porque las defensas tradicionales no son eficaces ante estos ataques, que a menudo ingresan a la red por medios legítimos. Los ciberdelincuentes aprovechan estas vulnerabilidades para propagar el malware en archivos compartidos de la red e integrar código malicioso en enormes almacenes de datos, lo que resulta en una amenaza persistente incluso después de la corrección.

Importancia de la protección del contenido del archivo

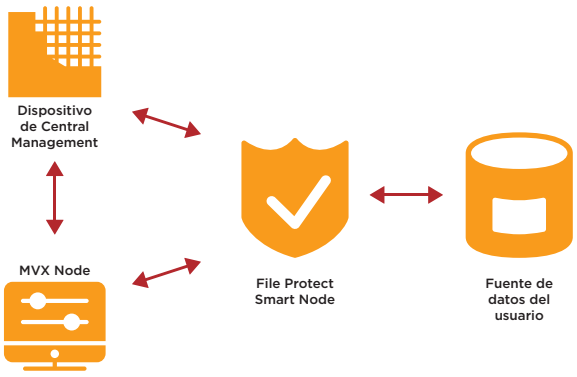
Sin tener una manera de detectar el malware latente en el contenido, las amenazas persistentes avanzadas (APT) pueden aprovechar los activos de la red para extraer información del propietario y causar importantes daños. File Protect analiza recursos compartidos de archivos y dispositivos de almacenamiento usando el motor FireEye Multi-Vector Virtual Execution™ (MVX) patentado que detecta códigos maliciosos desconocidos integrados en tipos de archivo (PDF, MS Office, vCards, ZIP/RAR/TNEF, etc.) y contenido multimedia (QuickTime, MP3, Real Player, JPG, PNG, etc.) comunes. File Protect realiza análisis a pedido, programados y recurrentes de archivos compartidos de la red y almacenes de contenido accesibles para identificar y poner en cuarentena el malware residente. Esto detiene una etapa clave del ciclo de vida del ataque avanzado.

Revelaciónes desconocidas; amenazas día-cero

FireEye FX usa el motor FireEye MVX para inspeccionar cada archivo y confirmar si existen exploits o código malicioso desconocidos. El motor FireEye MVX detecta día-cero, flujo múltiple y otros ataques evasivos mediante un análisis dinámico, sin firma. en un ambiente seguro y virtual. Detiene las fases de infección y vulneración de la cadena letal de ataque cibernético al identificar exploits y malware no vistos anteriormente.

El poder del MVX Smart Grid

FireEye MVX Smart Grid mejora FireEye Seguridad en red con una arquitectura de implementación adaptable y flexible a través de una nube híbrida o privada. MVX Smart Grid utiliza un enfoque innovador para proteger de forma más eficaz los campus, sucursales y usuarios remotos separando el motor MVX del hardware y Smart Nodes™ virtuales. Smart Nodes análisis de trafico de Internet para detectar y bloquear amenazas utilizando una variedad de técnicas como el análisis estático, el análisis, IPS, la inteligencia aplicada y más, mientras que el motor MVX realiza un análisis dinámico básico.



Protección para OneDrive y Sharepoint de Microsoft

File Protect analiza continuamente el contenido para alertar sobre el malware que se descubre en repositorios OneDrive y Sharepoint y ponerlo en cuarenta de forma permanente. La plataforma aprovecha el protocolo WebDAV para integrar de manera segura los servicios de SharePoint a fin de proteger los flujos de trabajo comerciales de las empresas que usan repositorios de SharePoint.

Personalización mediante reglas basadas en YARA

File Protect admite reglas YARA personalizadas para analizar grandes cantidades de amenazas de archivos específicas de la organización.

Jerarquización de incidentes optimizada

Con FireEye Endpoint Security, cada objeto malicioso puede analizarse en profundidad con el fin de determinar si los proveedores de antivirus pudieron detectar el malware interceptado por File Protect. Esto les permite a las organizaciones priorizar de manera más eficaz los seguimientos de la respuesta ante incidentes y usar convenios de nomenclatura comunes para el malware conocido.

Inteligencia sobre malware compartida

La información sobre amenazas que ha sido generada de manera dinámica en tiempo real puede facilitar a que todos los productos de FireEye protejan la red local a través de la integración con Central Management. Esta información se puede compartir de forma global a través de la nube FireEye Dynamic Threat Intelligence (DTI) para avisar a todos los suscriptores de la existencia de nuevas amenazas.

Sin necesidad de ajustar reglas y prácticamente sin falsos positivos

A diferencia de los sistemas IPS, File Protect no requiere absolutamente ninguna configuración. Los modos de implementación flexibles incluyen análisis solamente, supervisión y puesta en cuarentena activa. Esto les permite a las empresas saber cuánto malware hay residente en los archivos compartidos y detener activamente la propagación lateral del malware.

Content Smart Notes para protección en donde se necesita

Con el FireEye Content Smart Nodes los gestores de seguridad y contenido obtienen una solución virtual y flexible para proteger el contenido crucial en toda la empresa. Cuando se utiliza junto con el MVX Smart Grid, la protección de contenido se escala e implementa sin interrupciones en donde se la necesita.

Factores de forma flexibles

Ideales para cualquier entorno de red, los clientes pueden elegir entre FireEye Content Smart Nodes o dispositivos de hardware en el sitio tradicionales.

Tabla 1. Smart Node de contenido FireEye.

	FX 2500V
Asistencia OS	Microsoft Windows, MacOS X
Rendimiento	40 000 archivos/día
Puertos de interfaz de red	Ether 1, Ether 2
Núcleos del CPU	2
Memoria	8 GB
Capacidad del disco	512 GB
Compatibilidad con hipervisores	VMWare ESXi 6.0 o posterior

Tabla 2. Especificaciones técnicas de FireEye.

	FX 6500
Rendimiento*	Hasta 70 000 archivos por día
Puertos de interfaz de red	4 puertos 1 GigE BaseT
Puerto IPMI (panel trasero)	Incluidos
Puertos USB (panel trasero)	2 puertos USB tipo A frontales, 2 puertos USB tipo A traseros
Puerto serie (panel trasero)	115 200 bits/s, sin paridad, 8 bits, 1 bit de parada
Capacidad de almacenamiento	4 discos duros de 2TB, RAID 10, 3,5in, FRU
Empaque	Montaje en bastidor 2RU, para un rack de 19in
Dimensiones del chasis (Ancho x Profundidad x Alto)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
Alimentación eléctrica (CA)	Redundante (1+1) 800 W, 100 - 240 VCA, 9 - 4,5 A, conector IEC60320-C14 50 - 60Hz, FRU
Consumo máximo de energía	530 W
Disipación térmica máxima	1808 BTU/h
Tiempo medio entre fallos	53.742 h
Peso neto/embalado kg (lb)	20,2kg (44,4lb)/29,8kg (65,6lb)
Certificaciones de seguridad	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Certificaciones CEM/IEM	FCC Parte 15 ICES-003 Clase 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 y V-3/2015
Cumplimiento de normativas	Directiva RoHS 2011/65/EU; REACH; Directiva WEEE 2012/19/UE
Temperatura de funcionamiento	0 a 40 °C (32 a 104 °F)
Humedad relativa de funcionamiento	10 a 95 % a 40 °C, sin condensación
Altitud de funcionamiento	3000 m/9,842 pies

Para obtener más información sobre FireEye, visite: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Acerca de FireEye, Inc.

FireEye es una empresa de seguridad basada en inteligencia. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a los de una Nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.

FIREEYE™