SCHEDA TECNICA

File Protect

Rilevare ed eliminare il malware nei file condivisi in rete e negli archivi di contenuti

CARATTERISTICHE PRINCIPALI

- Individua malware latente non rilevato dai motori antivirus tradizionali
- Implementazione in quarantena attiva (modalità protezione) o solo analisi (modalità monitoraggio)
- Offre analisi ricorrenti, pianificate e su richiesta di condivisioni di file compatibili con CIFS e NFS
- Fornisce protezione proattiva per Microsoft OneDrive e Sharepoint
- Include l'analisi di un'ampia gamma di tipologie di file come PDF, documenti Microsoft Office e file multimediali
- Integrazione con FireEye Endpoint Security per ottimizzare la prioritizzazione della risposta agli incidenti e convenzioni per la denominazione
- Condivisione dei dati delle minacce con FireEye Central Management e il cloud FireEye DTI

Panoramica
FireEye File Protect protegge le risorse dati per un'ampia gamma di tipi di file dagli attacchi provenienti dalla posta Web, dagli strumenti di trasferimento online dei file, dal cloud e dai dispositivi portatili per l'archiviazione dei file. Tali attacchi possono estendersi alle condivisioni di file e ai repository di contenuti. File Protect analizza i file condivisi in rete e archivi di gestione di contenuti per rilevare e mettere in quarantena i malware che aggirano i firewall di nuova generazione, i sistemi IPS, gli antivirus e i gateway.

Le sfide del malware nelle condivisioni di file
Le minacce informatiche avanzate del giorno d'oggi utilizzano malware sofisticato e tattiche APT (Advanced Persistent Threat o minacce persistenti avanzate) per penetrare le difese e diffondersi attraverso le cartelle condivise in rete e i repository di contenuti. Ciò permette al malware di creare un punto d'appoggio a lungo termine all'interno della rete e di infettare diversi sistemi, anche quelli offline. Molti centri dati aziendali rimangono particolarmente vulnerabili al malware avanzato basato sui contenuti poiché le difese tradizionali sono inefficaci contro tali attacchi, che spesso entrano nella rete tramite vettori legittimi. I criminali informatici sfruttano queste vulnerabilità per diffondere il malware all'interno delle cartelle condivise in rete e incorporano codice dannoso in archivi dati di grandi dimensioni, creando così una minaccia persistente anche a seguito di un'attività di remediation.

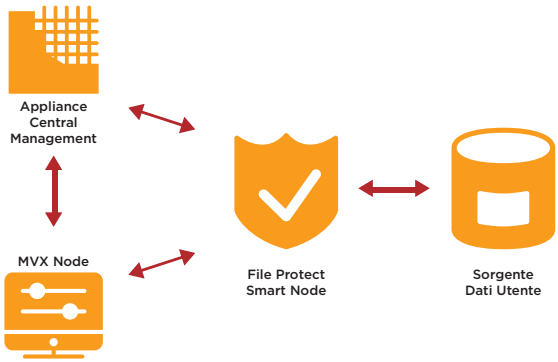
L'importanza della protezione del contenuto dei file
Senza un modo per rilevare il contenuto del malware dormiente, le minacce APT possono sfruttare le risorse di rete per estrarre informazioni di proprietà e provocare danni significativi. File Protect analizza le cartelle di file condivise in rete e i repository di contenuti aziendali utilizzando il motore brevettato FireEye Multi-Vector Virtual Execution™ (MVX) che rileva il codice zero-day pericoloso incorporato in tipologie di file comuni (PDF, MS Office, vCards, ZIP/RAR/TNEF, ecc.) e contenuti multimediali (QuickTime, MP3, Real Player, JPG, PNG, ecc.). File Protect esegue analisi ricorrenti, pianificate e su richiesta delle cartelle condivise in rete e archivi di contenuti accessibili per identificare e mettere in quarantena il malware residente. In questo modo si interrompe una fase fondamentale del ciclo di vita di una attacco avanzato.

Rilevamento di minacce zero-day sconosciute

FireEye FX utilizza il motore FireEye MVX per analizzare ogni file e confermare la presenza di exploit zero-day o codici pericolosi. Il motore FireEye MVX rileva attacchi zero-day, multi-flusso e altri attacchi evasivi con analisi dinamica, senza firma in un ambiente sicuro e virtuale. Ferma le fasi di infezione e compromissione della catena di attacchi informatici identificando exploit e malware mai visti prima.

La potenza di MVX Smart Grid

FireEye MVX Smart Grid migliora la sicurezza di FireEye Network Security con un'architettura di distribuzione flessibile e scalabile mediante cloud ibrido o privato. MVX Smart Grid utilizza un approccio innovativo per proteggere in maniera più efficace campus, filiali e utenti remoti attraverso la separazione del motore MVX dall'hardware e dagli Smart Nodes™ virtuali. Gli Smart Nodes analizzano il traffico Internet per rilevare e bloccare le minacce mediante una vasta gamma di tecniche come analisi statica, analisi, IPS, intelligenza applicata e molto altro, mentre il motore MVX esegue l'analisi dinamica del core.



Protezione per Microsoft OneDrive e SharePoint

File Protect analizza costantemente i contenuti per segnalare e mettere definitivamente in quarantena il malware individuato all'interno dei repository OneDrive e SharePoint. La piattaforma sfrutta il protocollo WebDAV per integrarsi in modo sicuro con i servizi SharePoint al fine di proteggere i flussi di lavoro aziendali che utilizzano i repository SharePoint.

Personalizzazione tramite regole YARA

File Protect supporta regole YARA personalizzate per l'analisi di grandi quantità di minacce specifiche per l'azienda.

Ottimizzazione della priorità degli incidenti

Con FireEye Endpoint Security, ogni oggetto dannoso può essere analizzato ulteriormente per stabilire se i fornitori di antivirus sono riusciti a identificare il malware bloccato da File Protect. In questo modo le aziende possono dare priorità in modo efficiente alle attività di follow-up alle risposte agli incidenti e utilizzare convenzioni di denominazione comuni per il malware noto.

Condivisione di informazioni sul malware

Le informazioni sulle minacce in tempo reale generate dinamicamente sono di supporto a tutti i prodotti FireEye per proteggere la rete locale grazie all'integrazione con Central Management. Queste informazioni possono essere condivise a livello globale attraverso il cloud FireEye Dynamic Threat Intelligence (DTI) per informare tutti gli abbonati delle minacce emergenti.

Nessuna attività di ottimizzazione delle regole e falsi positivi quasi inesistenti

A differenza dei sistemi IPS, File Protect non richiede alcuna ottimizzazione. Tra le modalità di implementazione flessibile vi sono il monitoraggio basato esclusivamente sull'analisi e la messa in quarantena attiva. Ciò permette alle aziende di sapere la quantità di malware residente sulle cartelle condivise in rete e per bloccare attivamente la diffusione collaterale di malware.

Content Smart Nodes per protezione laddove ce n'è bisogno

Con FireEye Content Smart Nodes, i responsabili di sicurezza e contenuti dispongono di una soluzione virtuale flessibile per proteggere i contenuti mission-critical in tutta l'azienda. Abbinata alla MVX Smart Grid, la protezione dei contenuti viene scalata e distribuita rapidamente dove ce n'è più bisogno.

Fattori di forma flessibili

Ideale per qualsiasi ambiente di rete: i clienti possono scegliere tra appliance FireEye Content Smart Nodes virtuali o tradizionali appliance hardware fisiche in loco.

Tabella 1. FireEye Content Smart Node.

	FX 2500V
Sistema operativo supportato	Microsoft Windows, MacOS X
Prestazioni	40.000 file/giorno
Porte interfacce di rete	Ether 1, Ether 2
CPU Cores	2
Memoria	8 GB
Capacità unità	512 GB
Supporto Hypervisor	VMWare ESXi 6.0 o successivo

Tabella 2. Caratteristiche tecniche FireEye.

	FX 6500
Prestazioni*	Fino a 70.000 file al giorno
Porte interfacce di rete	2x 1GigE BaseT
Porta IPMI (pannello posteriore)	Incluso
Porte USB (pannello posteriore)	2x USB Tipo A anteriore, 2x USB Tipo A posteriore
Porta seriale (pannello posteriore)	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop
Capacità di archiviazione	4x 2TB, RAID 10, HDD 3,5 pollici, FRU
Involucro	2RU, Rack 19 pollici
Dimensioni chassis (LxPxA)	17,24" x 24,41" x 3,48" (438 x 620 x 88,4 mm)
Alimentatore CA	Ridondante (1+1) 800 watt, 100 - 240 VCA, 9 – 4,5 A, 50-60 Hz, ingresso IEC60320-C14, FRU
Consumo energetico massimo	530 watt
Dissipazione termica massima	1.808 BTU/h
MTBF	53.742 h
Peso sola appliance/con confezione, kg (lb)	20,2 kg (44,4 lb)/29,8 kg (65,6 lb)
Certificazioni di sicurezza	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Certificazioni 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
Conformità normativa	Direttiva RoHS 2011/65/UE; REACH; Direttiva RAEE 2012/19/UE
Temperatura operativa	0 ~ 35 °C (32 ~ 95 °F)
Umidità operativa relativa	10 ~ 95% @ 40 °C, senza condensa
Altitudine operativa	3.000 m

Per ulteriori informazioni su FireEye, visitare il sito: **www.FireEye.com**

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

Informazioni su FireEye, Inc.
FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Fungendo da estensione semplice e scalabile delle attività di sicurezza del cliente, FireEye offre un'unica piattaforma che fonde tecnologie di sicurezza innovative, informazioni sulle minacce a livello nazionale e servizi di consulenza Mandiant®, rinomati in tutto il mondo. Con questo approccio, FireEye elimina la complessità e il peso della sicurezza informatica per le aziende che hanno difficoltà a prepararsi, prevenire e rispondere agli attacchi informatici.

FIREEYE™