SCHEDA TECNICA

FireEye

FireEye Endpoint Security

Coinvolgi più motori di difesa con un singolo agente

VANTAGGI

- Prevenire la maggior parte degli attacchi informatici contro gli endpoint di un ambiente
- Rilevare e bloccare le violazioni che si verificano per ridurre l'impatto di una violazione
- Migliorare la produttività e l'efficienza scoprendo le minacce piuttosto che inseguendo gli avvisi
- Utilizzare un unico agente di dimensioni ridotte per un impatto minimo sull'utente finale
- Rispettare le normative, come PCI-DSS e HIPAA
- Distribuzione in loco o nel cloud

La sicurezza tradizionale degli endpoint non è efficace contro le minacce moderne; non è mai stata progettata per gestire attacchi di minacce persistenti avanzate o sofisticate (APT). Per mantenere sicuri gli endpoint, la soluzione sarebbe analizzare velocemente e rispondere a tali minacce.

FireEye Endpoint Security combina il meglio dei prodotti di sicurezza legacy con i progressi della tecnologia, della competenza e dell'intelligenza FireEye, per difendersi dagli attacchi informatici di oggi. FireEye utilizza quattro motori in Endpoint Security per prevenire, rilevare e rispondere a una minaccia.

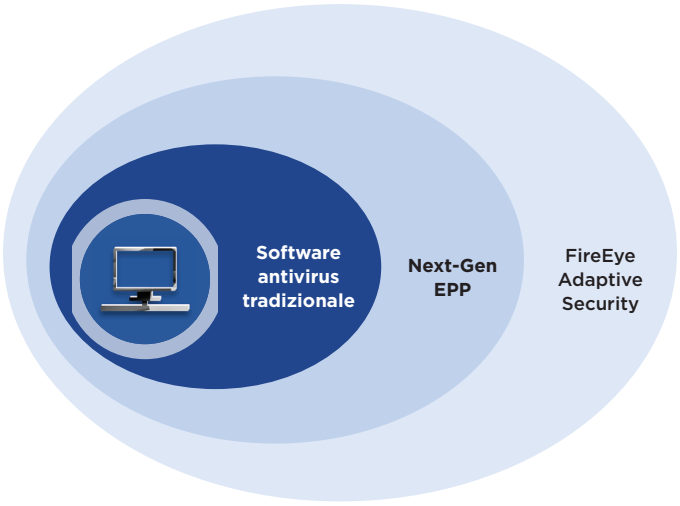
Per prevenire i classici malware, Endpoint Security utilizza un motore EPP (Endpoint Protection Platform) basato su firma. Al fine di trovare minacce per cui non è ancora stata creata una firma, MalwareGuard utilizza tecnologie di apprendimento automatico con conoscenze derivanti in prima linea dagli attacchi informatici. Per gestire le minacce avanzate, gli endpoint (EDR) attivano delle funzionalità di rilevamento e risposta (EDR) tramite un motore di analisi basato sul comportamento. Infine, la presenza di indicatori di compromissione in tempo reale (IOC) basati sull'intelligenza attuale in prima linea aiutano a trovare minacce nascoste. Questa strategia di difesa approfondita aiuta a proteggere informazioni essenziali contenute negli endpoint dei clienti.

Anche con la migliore protezione, le violazioni sono inevitabili. Per garantire una risposta sostanziale che minimizzi le interruzioni dell'attività, Endpoint Security fornisce strumenti per:

- Cercare e indagare minacce note e sconosciute su decine di migliaia di endpoint in pochi minuti
- Identificare e descrivere i vettori utilizzati da un attacco per infiltrarsi in un endpoint
- Determinare se un attacco è avvenuto (e persiste) su un endpoint specifico e dove si è diffuso
- Stabilire la tempistica e la durata degli endpoint compromessi e seguire l'incidente
- Identificare chiaramente quali endpoint e sistemi necessitano di contenimento per prevenire ulteriori compromissioni

L'IT è un abilitatore strategico che guida la nostra capacità di educare in modo efficace i nostri studenti. L'utilizzo di FireEye Endpoint Security garantisce che le risorse IT siano disponibili, altamente funzionanti e sicure, il che è fondamentale per raggiungere la nostra missione.

— James D. Perry II
Responsabile della sicurezza informatica presso la University of South Carolina



Nelle imprese, spesso, si pensa che un virus sia quasi la fine del mondo. Grazie a FireEye, posso dimostrare con prove concrete la natura del problema e il modo in cui è stato gestito e risolto. Condividere queste informazioni aiuta a ridurre la pressione per qualsiasi membro all'interno di un'organizzazione.

— Michael Hennessy, Direttore dei servizi tecnologici
Alpha Grainer Manufacturing, Inc

Caratteristiche principali

- Un singolo agente con tre motori di rilevamento per ridurre al minimo la configurazione e massimizzare il rilevamento e il blocco
- Un unico flusso di lavoro integrato per analizzare e rispondere alle minacce all'interno di Endpoint Security
- Protezione anti-malware completamente integrata con difese antivirus (AV), machine learning, analisi del comportamento, indicatori di compromissione (IOC) e visibilità degli endpoint
- Triage Summary e Audit Viewer per ispezionare e analizzare completamente le minacce

Funzionalità aggiuntive

- Enterprise Security Search per cercare rapidamente e segnalare attività sospette o minacce
- Data Acquisition per condurre ispezioni e analisi dettagliate e approfondite degli endpoint in determinati periodi di tempo
- Visibilità end-to-end che consente ai team di sicurezza di cercare, individuare e discernere rapidamente il livello delle minacce
- Funzionalità di rilevamento e risposta per rilevare, analizzare e isolare rapidamente gli endpoint per accelerare la risposta
- Interfaccia di facile comprensione per un'interpretazione e una risposta rapida a qualsiasi attività sospetta dell'endpoint

Sistemi operativi e ambienti supportati	
Windows	XP SP3, 2003 SP2, Vista SP1 and up, 2008, Win7, 2012, 8, 8.1, 10, Server 2016
Mac	OS X 10.9+
Linux	Red Hat Enterprise Linux 6.8+, 7.2 + CentOS 6.9+, 7.4+

Opzioni di distribuzione: appliance fisica in loco, appliance virtuale in loco, FireEye Cloud Service

ICSA labs CERTIFIED ANTI-VIRUS

vb 100 VIRUS virusbtn.com

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 operazioni di sicurezza del cliente, FireEye offre un'unica piattaforma che fonde tecnologie di sicurezza innovative, informazioni sulle minacce a livello nazionale e i 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