SCHEDA TECNICA

FireEye Endpoint Security

Blocca gli attacchi con conoscenze derivanti da risposte in prima linea

CARATTERISTICHE PRINCIPALI

- 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
- Protezioni e funzionalità attraverso moduli scaricabili
- 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 (*Advanced Persistent Threat*, APT). Al fine di mantenere la sicurezza degli endpoint, una soluzione deve riconoscere rapidamente la minaccia e rispondere con la tecnologia più efficace.

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. Basata su un modello di difesa approfondita, Endpoint Security utilizza un'architettura modulare con motori predefiniti e moduli scaricabili per proteggere, rilevare, rispondere e gestire gli agenti.

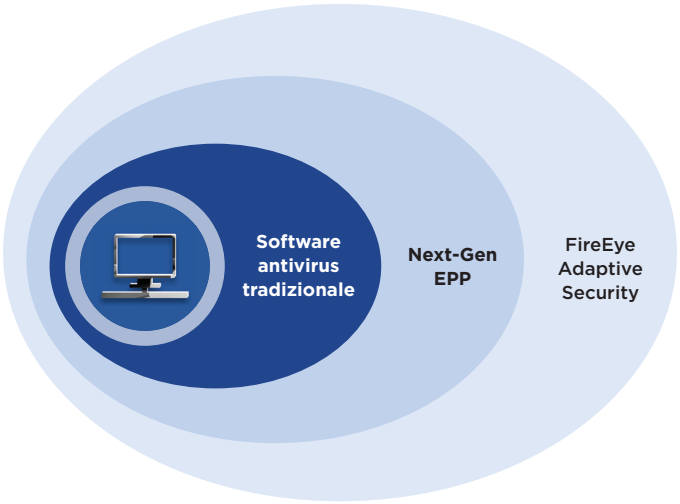
Per prevenire i classici malware, Endpoint Security utilizza un motore Piattaforma di protezione endpoint (*Endpoint Protection Platform*, EPP) basato su firma. Al fine di trovare minacce per cui non è ancora stata creata una firma, MalwareGuard utilizza tecnologie di apprendimento automatico con conoscenze derivanti in prima linea dagli attacchi informatici. Per gestire le minacce avanzate, gli endpoint (*Endpoint Detection and Response*, EDR) attivano delle funzionalità di rilevamento e risposta (EDR) tramite un motore di analisi basato sul comportamento. Un motore di indicatori di compromissione in tempo reale (*Indicators of Compromise*, IOC) basati sull'intelligenza attuale in prima linea aiutano a trovare minacce nascoste. Per aggiungere nuovi motori e caratteristiche, puoi scaricare i moduli da FireEye Market.

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 utilizza la difesa approfondita 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	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
Mac	OS X 10.9+
Linux	RedHat Enterprise Linux 6.8+, 7.2+, 8 CentOS 6.8+, 7.2+, 8 Ubuntu 14.04, 16.04, 18.04 SUSE 11.3, 11.4, 12.2, 12.3, 15 Open SUSE 15.1 Amazon AMI 2018.3, AMI2 Oracle Linux 6.10 & 7.6

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

SE Labs AA JAN-MAR 2020 ENTERPRISE ENDPOINT PROTECTION · AV comparatives APPROVED Business Security DEC 2019 · vb 100 VIRUS virusbtn.com · OPSWAT. Access Control Certification Anti-Malware GOLD

AV-TEST · MITRE · VirusTotal

Per ulteriori informazioni su FireEye, visita il sito Web **www.FireEye.com**

FireEye Italia Srl
Piazza IV Novembre, 7. 20124
Milano Italia
+39 0294750535
italy@FireEye.com

Informazioni su FireEye, Inc.

FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Operando come estensione intuitiva e scalabile dei processi operativi di sicurezza dei clienti, FireEye offre un'unica piattaforma in grado di coniugare tecnologie di sicurezza innovative, intelligence sulle minacce a livello nazionale e servizi di consulenza Mandiant® di fama mondiale. Grazie a questo approccio, FireEye elimina la complessità e l'onere della sicurezza informatica per le aziende che hanno difficoltà a prepararsi per futuri attacchi, prevenirli e rispondere ad essi.

FIREEYE™