Endpoint Security

Difesa endpoint remota o in loco
dalle minacce ed exploit sconosciuti

PANORAMICA

Gli aggressori esperti di oggi aggirano le difese endpoint tradizionali (firewall, software antivirus) su cui la maggior parte dei team di sicurezza fa affidamento da anni. Anche quando una difesa tradizionale ferma una minaccia nota, non è in grado di determinare ciò che tale minaccia stava cercando di fare. FireEye Endpoint Security (serie HX) può essere implementato in loco per gli endpoint all'interno e all'esterno della rete aziendale. Aiutate il vostro team di sicurezza a rilevare, contenere e comprendere la natura e lo scopo di minacce note e sconosciute utilizzando funzioni quali:

- Triage Viewer e Audit Viewer per ispezionare e analizzare gli indicatori di minaccia
- Enterprise Security Search per cercare rapidamente, trovare e contenere le minacce
- Data Acquisition per un'ispezione e analisi approfondita degli endpoint
- Exploit Guard per rilevare e inviare avvisi sui processi di exploit degli endpoint

Con FireEye Endpoint Security le aziende possono controllare, analizzare e contenere proattivamente le minacce note e sconosciute su qualsiasi endpoint.

Estendete le informazioni sulle minacce a ogni endpoint

Per essere efficaci, le informazioni sulle minacce devono essere presenti nel punto di attacco. HX Endpoint Detection and Response (EDR) estende senza interruzioni le capacità di informazioni sulle minacce degli altri prodotti FireEye all'endpoint. Se un prodotto FireEye rileva un attacco in qualsiasi punto della rete, gli endpoint vengono aggiornati automaticamente e possono essere ispezionati in cerca di IOC.

Migliora la visibilità degli endpoint

La visibilità è fondamentale per identificare la causa principale di un avviso e condurre analisi approfondite di una minaccia. La cache lookback in Endpoint Security consente di controllare e analizzare avvisi presenti e passati nell'endpoint. Triage Viewer consente anche di creare automaticamente una cronologia degli eventi per l'analisi forense.

CARATTERISTICHE

- Distribuite Endpoint Security su appliance locali con il software agente endpoint per monitorare gli endpoint aziendali e remoti
- Estendete la protezione contro le minacce avanzate con FireEye Dynamic Threat Intelligence (DTI) dalla rete principale agli endpoint
- Eseguite un'indagine dettagliata degli endpoint e create linee temporali per identificare e contenere gli IOC
- Cercate, rilevate, identificate e contenete le minacce su decine di migliaia di endpoint (collegati o non) in pochi minuti
- Valutate facilmente tutte le attività degli endpoint da una singola interfaccia per identificare exploit da analizzare e prendere decisioni di contenimento o di risposta
- Rispettate entrambi gli standard governativi Common Criteria e FIPS
- Centralizzate i flussi di lavoro basati su host con una singola posizione per gli avvisi correnti, i dettagli del sistema e le acquisizioni
- Rispondete rapidamente alle minacce note e sconosciute con informazioni contestuali critiche
- Proteggete tutti gli endpoint sia locali che remoti, al di fuori della rete o dietro Network Address Translation (NAT)
- Contenete le minacce e i dispositivi compromessi con un solo clic, pur consentendo un'indagine a distanza
- Migliorate il flusso di lavoro con Audit Viewer per un'analisi completa delle minacce all'interno di Endpoint Security
- Personalizzate le funzionalità Endpoint Security per affrontare le caratteristiche uniche di un incidente
- Supportate più implementazioni DMZ

FireEye

Ottenere una copertura completa degli endpoint

Gli endpoint locali e remoti al di fuori della rete aziendale possono essere vulnerabili agli attacchi. Endpoint Security copre tutti gli endpoint, inviando loro informazioni indipendentemente dal tipo di collegamento Internet. Ciò permette di ricercare le cause e isolare gli endpoint in qualunque parte del mondo, senza la necessità di connessioni VPN aggiuntive.

Contenete gli endpoint compromessi e prevenite la diffusione laterale

Gli attacchi che partono da un endpoint possono diffondersi rapidamente attraverso la rete. Dopo aver identificato un attacco, Endpoint Security vi consente di isolare immediatamente i dispositivi compromessi per fermare l'attacco e prevenire la diffusione laterale, il tutto con un solo clic. Potete quindi condurre un'indagine forense completa dell'incidente senza il rischio di ulteriori infezioni.

Rileva i processi nascosti di exploit degli endpoint

Quando si tratta di rilevamento degli exploit, le capacità di protezione tradizionale degli endpoint (EPP) sono limitate rispetto alle firme in un database. FireEye Endpoint Security fornisce flessibilità, informazioni sugli exploit guidate dai dati attraverso una funzione chiamata Exploit Guard. Questa funzione dispone di funzioni di rilevamento e risposta degli endpoint (EDR) e raccoglie informazioni dettagliate sulle aree che le soluzioni endpoint tradizionali saltano. Utilizza informazioni dettagliate esclusive di FireEye per correlare molteplici attività discrete e scoprire exploit.

Come funziona Endpoint Security

Endpoint Security può cercare e indagare le minacce note e sconosciute su decine di migliaia di endpoint in pochi minuti. Utilizza Dynamic Threat Intelligence per correlare gli avvisi generati dai prodotti per la sicurezza di rete e dagli endpoint di FireEye e la gestione dei log.

Dopo la convalida di una minaccia, è possibile determinare:

- Quali vettori ha usato un attacco per infiltrarsi in un endpoint
- Se un attacco è avvenuto (e persiste) su un endpoint specifico
- Se si è verificata una diffusione laterale e a quali endpoint
- Per quanto tempo uno o più endpoint sono stati compromessi
- Se un IP è stato esfiltrato
- Quali endpoint e sistemi contenere per prevenire ulteriori compromissioni

REQUISITI DI ENDPOINT SECURITY

SISTEMA OPERATIVO	MEMORIA MINIMA DI SISTEMA (RAM)
Windows XP SP3	512 MB
Windows 2003 SP2	512 MB
Windows Vista SP1 o più recente	1 GB (32-bit), 2 GB (64-bit)
Windows 2008 (compreso R2)	2 GB (64-bit)
Windows 7	1 GB (32-bit), 2 GB (64-bit)
Windows 2012 (compreso R2)	2 GB (64-bit)
Windows 8	1 GB (32-bit), 2 GB (64-bit)
Windows 8.1	1 GB (32-bit), 2 GB (64-bit)
Windows 10	1 GB (32-bit), 2 GB (64-bit)
Windows Server dal 2008 al 2016	2 GB
Red Hat Enterprise Linux (RHEL) versioni 6.8, 7.2, 7.3	2 GB

Nota: Endpoint Security richiede un processore compatibile Pentium da 1 GHz o superiore e almeno 300 MB di spazio libero su disco. Funziona con i seguenti sistemi operativi

SPECIFICHE DELLE APPLIANCE HARDWARE

SPECIFICHE	HX 4402	HX 4400D
Capacità archiviazione	4 x 1,8 TB, RAID 10, 2,5 pollici	4x 600 GB, SAS, 2,5 pollici, FRU
Involucro	1RU, Rack 19 pollici	
Dimensioni chassis (LxPxA)	43,7 x 70,6 x 4,3 cm	
Alimentatore CA	Ridondante (1+1) 750 watt, 100 - 240 VAC	
Consumo massimo (watt)	313 watt	
MTBF (h)	35.200 ore	
Solo appliance	32 lb. (15 kg)	

Nota: Endpoint Security può essere implementato attraverso cloud oppure come appliance hardware virtuale o in loco. Un'unica appliance supporta fino a 100.000 endpoint.

Collegare avvisi a livello di rete alle minacce per gli endpoint

Leggete come funziona FireEye Endpoint Security con altre implementazioni FireEye per consentire ai team di sicurezza di prendere decisioni più accurate sui potenziali problemi di sicurezza.

Per maggiori informazioni su FireEye, visitate il sito:
www.FireEye.com

A proposito di FireEye, Inc.

FireEye® è leader nella sicurezza come servizio basato sulle informazioni. 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 cybersicurezza per le aziende che hanno difficoltà a prepararsi, prevenire e rispondere agli attacchi informatici. FireEye ha oltre 5.000 clienti in 67 Paesi, tra cui più di 940 dei Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye