FireEye

Ficha técnica

Serie HX

Plataforma de prevención de amenazas contra endpoints que detecta, analiza y resuelve incidentes de seguridad en el endpoint

Aspectos destacados

- **Seguridad integrada para la red y los endpoints:** valide y analice las alertas de la red localizando la actividad correspondiente en los endpoints.
- **Llegue a los endpoints dondequiera que se encuentren:** la innovadora tecnología Agent Anywhere llega a endpoints remotos ubicados fuera de la red corporativa y detrás de NAT.
- **Detecte las amenazas con un robusto sistema de información:** aplique la información sobre amenazas que ofrece FireEye para localizar las amenazas avanzadas en su entorno de TI.
- **Contenga los dispositivos amenazados con un solo clic:** aísle los dispositivos que están en riesgo con solo hacer clic, para que los atacantes no puedan acceder a los sistemas y, al mismo tiempo, se permita la investigación a distancia.
- **Investigue rápidamente todos los endpoints:** compruebe decenas o cientos de miles de endpoints en cuestión de minutos.

Las empresas gastan millones de dólares en personal de seguridad de primera y en construir redes seguras para prevenir las amenazas y mantener a los agresores alejados de sus entornos de TI. A pesar de estas inversiones, los atacantes con más determinación consiguen poner en peligro a las empresas y robar su propiedad intelectual y sus activos financieros. La plataforma Endpoint Threat Prevention ofrece a los técnicos de seguridad los medios para detectar, analizar y resolver con confianza los incidentes en menos tiempo que cuando se aplican planteamientos convencionales.

Búsqueda de APT y atacantes avanzados

Los indicadores de riesgo con detección basada en host identifican amenazas que los antivirus pasan por alto, incluidos los ataques avanzados y las amenazas persistentes avanzadas (APT). Los usuarios reciben inmediatamente una notificación cuando uno de esos indicadores identifica que un dispositivo está en riesgo.

Extienda la detección de FireEye a los endpoints

Extienda la visibilidad de otras plataformas de prevención de amenazas de FireEye®, como la plataforma FireEye Network Threat Prevention (serie NX), hasta los endpoints. Los agentes de endpoints se actualizan automáticamente con los indicadores de riesgo para ofrecer una "defensa a fondo" e integrada para las amenazas más importantes: las que se están produciendo en estos momentos.

Valide las alertas de la red

Confirme si los ataques detectados en la red han llegado a afectar a un endpoint. Cada vez que reciba una alerta de otro producto de FireEye, identifique todos los endpoints afectados. Para profundizar en lo que causó una alerta de la red (incluso las de un sistema SIEM) los analistas pueden ver una cronología recogida automáticamente de los eventos producidos en el agente afectado.

Cobertura completa con Agent Anywhere

Gracias a la tecnología Agent Anywhere, la cobertura puede extenderse a endpoints remotos fuera de la red corporativa, sin importar el tipo de conexión a Internet que tengan. A los endpoints remotos que no están en redes protegidas por productos de FireEye se les envían indicadores de los ataques actuales. Así, los analistas pueden investigar y contener endpoints en cualquier lugar del mundo, sin necesidad de conexiones VPN adicionales.

FireEye

Ficha técnica

Contención de endpoints

Actúe de inmediato para aislar los dispositivos atacados e impedir que los agresores accedan a los sistemas, sin dificultar la investigación a distancia.

Cómo funciona

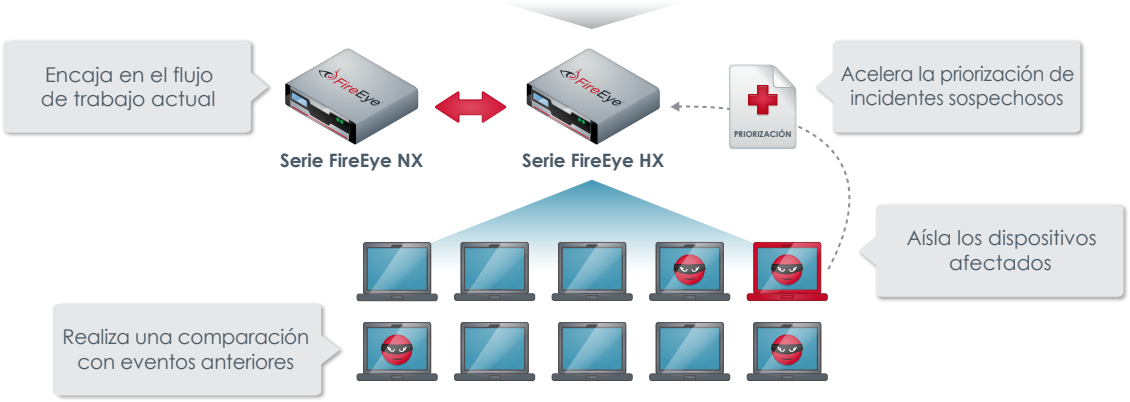
La plataforma Endpoint Threat Prevention permite que el personal de seguridad correlacione la actividad de la red y los endpoints. Las empresas pueden investigar automáticamente las alertas generadas por las plataformas de prevención de amenazas de FireEye y los productos de administración de registros y seguridad de redes, aplicar la información exclusiva de FireEye o buscar indicadores de riesgo a fin de identificar los dispositivos afectados y evaluar los riesgos. Además, las empresas pueden priorizar rápidamente el incidente para comprender los detalles de la afectación y contener los endpoints expuestos con un solo clic.

Investigación automática de las alertas de los dispositivos: cree indicadores de riesgo de forma automática a partir de las alertas generadas en los dispositivos de la red. Confirme las alertas de amenaza en todos los endpoints para identificar los problemas críticos.

Consulta rápida a todos los endpoints: investigue decenas o cientos de miles de endpoints en cuestión de minutos.

Agent Anywhere: investigue cualquier endpoint aunque no esté en su red.

Interfaz fácil de entender: convierta a sus analistas de primera línea en investigadores facilitando y simplificando la interpretación rápida de los datos y el seguimiento pertinente.



Especificaciones técnicas

	HX 4000 / HX 4000D
CPU	De 6 núcleos, a 2,5 GHz
Memoria	16 GB
Disco	4 de 2 TB (RAID 10)
Número de endpoints	Hasta 100 000 endpoints
Conexiones de red	4 puertos BASE-T 10/100/1000 (2 activos)
Dimensiones (ancho x fondo x alto)	43,7 x 69,9 x 4.3 cm (17,2" x 27,5" x 1,7")
Fuente de alimentación/RAID	Doble, intercambiable en caliente
Potencia máxima	700 W

Nota: todas las cifras de rendimiento varían en función de la configuración del sistema y del perfil del tráfico procesado.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | LATAM@FireEye.com | www.FireEye.com