FIREEYE™

Ficha técnica

Network Forensics

Minimice el impacto de los ataques a la red con captura de paquetes de alto rendimiento y análisis de investigación

Las organizaciones necesitan una detección temprana y una investigación rápida de los incidentes para determinar el alcance y el impacto, contener eficazmente las amenazas y volver a proteger la red.

La solución FireEye Network Forensics combina la solución de recuperación y captura de datos de red sin pérdida más rápida de la industria con análisis y visualización centralizados. Acelera el proceso forense de la red con una sola área de trabajo que simplifica las investigaciones y reduce los riesgos.

FireEye Network Forensics le permite identificar y resolver incidentes de seguridad más rápido al capturar e indexar paquetes completos a velocidades extremadamente rápidas. Con Network Forensics, puede detectar una amplia gama de incidentes de seguridad, mejorar la calidad de su respuesta y cuantificar con precisión el impacto de cada incidente.

Como parte de la solución FireEye Network Forensics, los dispositivos de análisis de investigación revelan amenazas ocultas y aceleran la respuesta ante incidentes al agregar un área de trabajo centralizada con una interfaz analítica fácil de usar.

Los analistas pueden revisar paquetes y sesiones de red específicos antes, durante y después de un ataque. Ser capaz de reconstruir y visualizar los eventos que desencadenan la descarga de malware o la devolución de llamada que permite a su equipo de seguridad responder de manera efectiva y rápida para evitar que vuelva a ocurrir. Pueden ampliar la visibilidad de la actividad del atacante decodificando los protocolos que normalmente se utilizan para propagar lateralmente los ataques en una red.

Esta combinación única de captura de paquetes de alto rendimiento y análisis profundo ayuda a reconocer y monitorear rápidamente cada elemento de un ataque.

Figura 1. Dispositivos de FireEye Network Forensics para la captura y el análisis de paquetes.

Aspectos destacados de la captura de paquetes

- **Alto rendimiento:** Captura continua de paquetes sin pérdida con registro de tiempo a velocidades de hasta 20 Gbit/s
- **Alta fidelidad:** Indexación en tiempo real de todos los paquetes capturados con registro de tiempo y atributos de conexión. Exportación de indexaciones de flujo y metadatos de conexión en formato JSON. Las indexaciones de flujos se pueden convertir a formatos de datos NetFlow V9, IPFIX y herramientas Silk
- **Resultados rápidos:** Búsqueda ultrarrápida y recuperación de conexiones y paquetes de destino utilizando una arquitectura de indexación patentada
- **Contexto enriquecido:** Interfaz de usuario basada en la Web para la búsqueda e inspección de paquetes, conexiones y sesiones
- **Visibilidad extensa:** Compatibilidad con un decodificador de sesiones para consultar y buscar información detallada sobre conexiones web, de correo electrónico, FTP, DNS, de chat y SSL, así como sobre los archivos adjuntos
- **Captura inteligente:** Filtrado selectivo del tráfico capturado para eliminar la transmisión de video, grandes transferencias de archivos, cargas útiles cifradas, etc.
- **Eficiencias mejoradas:** Procesos automatizados para identificar el robo de datos, utilizando algoritmos patentados para diagnosticar comportamientos de red potencialmente anómalos

Tabla 1. Dispositivos de captura de paquetes disponibles.

Modelo	Configuración de puertos de captura	Puertos de administración	Máxima velocidad de grabación	Almacenamiento total en placa	Dimensiones	Fuente de alimentación/ carga típica en funcionamiento
PX 1004S-6	1 x 2 GigE	1 x 1 GbE	500 Mbit/s	6 TB	1U 437 mm (17,2 in) x 500 mm (19,7 in) x 44 mm (1,7 in) 8,2 kg (18 lb)	CA, CA fija de 100 ~ 240 V @ 50 ~ 60 Hz, conector IEC60320-C14
PX 2060ESS-96	4 x 10 GE SFP+	2 x 1 GbE	2 Gbit/s	96 TB, almacenamiento SAS ampliable	2U 438 mm (17,24 in) x 620 mm (24,41 in) x 88,4 mm (3,48 in) 26,0 kg (57,3 lb)	Redundante (1+1) 800 W, 100 - 240 V CA, 10,5 - 4,0 A, conector IEC60320-C14 de 50-60 Hz, FRU
PX 2060ESS-120	4 x 10 GE SFP+	2 x 1 GbE	7,5 Gbit/s	120 TB, almacenamiento SAS ampliable	2U 438 mm (17,24 in) x 620 mm (24,41 in) x 88,4 mm (3,48 in) 26,0 kg (57,3 lb)	Redundante (1+1) 800 W, 100 - 240 V CA, 10,5 - 4,0 A, conector IEC60320-C14 de 50-60 Hz, FRU
PX 1004EXT-4G	4 x 1 Gbit/s, 10/100/1000 BaseT, SFP	2 x BASE-T 10/100/1000 2 x BASE-T 10/100/1000/10G	4 Gbit/s	Sin almacenamiento en placa. Adaptador de host de canal de fibra a almacenamiento SAN externo	Montaje en bastidor 1U 4,3 cm (1,7 in) x 43,7 cm (17,2 in) x 65,0 cm (25,6 in) 20,9 kg (46 lb)	Fuente de corriente alterna redundante (1+1), alto rendimiento, 650 W, 100 a 240 V CA, selección automática de rango, 60-50 Hz, 230 a 280 W estándar
PX 1040EXT-20G	4 x 1 Gbit/s	2 x BASE-T 10/100/1000 2 x BASE-T 10/100/1000/10G	20 Gbit/s	Sin almacenamiento en placa. Adaptador de host de canal de fibra a almacenamiento SAN externo	Montaje en bastidor 1U 4,3 cm (1,7 in) x 43,7 cm (17,2 in) x 65,0 cm (25,6 in) 20,9 kg (46 lb)	Fuente de corriente alterna redundante (1+1), alto rendimiento, 650 W, 100 a 240 V CA, selección automática de rango, 60-50 Hz, 230 a 280 W estándar
PX 4000SX440	n/d	n/d	n/d	Unidad de almacenamiento sin procesar 440 TB	437 mm (17,2 in) x 698 mm (27,5 in) x 178 mm (7 in) 34 kg (76 lb)	Fuente de corriente alterna redundante (1+1), alto rendimiento, 1280 W, 100 a 240 V CA, selección automática de rango, 60 a 50 Hz

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

Los dispositivos de FireEye Investigation Analysis permiten varias configuraciones adaptadas a arquitecturas distribuidas y de un solo nodo a fin de optimizar el ancho de banda y el rendimiento de la acumulación de metadatos, las consultas y los análisis.

Aspectos destacados de Investigation Analysis

- **Visualización:** Ver y compartir metadatos y actividad de la red a través de paneles fáciles de personalizar
- **Respuestas rápidas:** Llevar a cabo consultas centralizadas de palabra clave, expresiones regulares y genéricas a nivel de aplicación en todas las alertas, flujo capturado y metadatos
- **Interfaz ágil:** Pase inmediato y descarga de datos PCAP individuales o masivos para sesiones de interés
- **Búsqueda potente:** Acelere la búsqueda con metadatos indexados de una gran cantidad de protocolos como HTTP, SMTP, POP3, IMAP, SSL, TLS, DNS y FTP
- **Consolidación de los indicadores de riesgo (IOC):** Consolide las alertas de productos FireEye Network Security, Email Security y Endpoint Security junto con todos los metadatos de la red en una sola área de trabajo con un acceso inmediato de "un clic" a los datos de la sesión desde las alertas
- **Cacería de amenazas retroactiva:** Análisis de amenazas de los IOC "antiguos" a través de la integración de los envíos de información de FireEye Threat Intelligence, STIX y OpenIOC con la función de búsqueda IA automatizada. Se le alertará automáticamente de los IOC presentes en la red con días o semanas de anticipación
- **Reconstrucción de archivos con un clic:** Reconstruya archivos, páginas web y correos electrónicos sospechosos de forma rápida y segura para un análisis posterior

Tabla 2. Dispositivos de análisis de investigación disponibles.

Modelo	Almacenamiento total en placa	Dimensiones	Fuente de alimentación/carga típica en funcionamiento
IA 1000 DIR	6 TB	437 mm (17,2 in) x 500 mm (19,7 in) x 44 mm (1,7 in)	CA, CA fija de 100 ~ 240 V @ 50 ~ 60 Hz, conector IEC60320-C14
IA 2100-48	48 TB	437 mm (17,2 in) x 500 mm (19,7 in) x 44 mm (1,7 in)	Redundante (1+1) 800 W, 100 - 240 V CA, 10,5 - 4,0 A, conector IEC60320-C14 de 50-60 Hz, FRU

Para obtener más información sobre FireEye, visite: **www.FireEye.com**

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

Acerca de FireEye, Inc.
FireEye es una empresa de seguridad basada en inteligencia. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a los de una Nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.