FIREEYE™

FICHA TÉCNICA

FireEye Endpoint Security

Detenga los ataques con conocimiento a partir de las respuestas de primera línea

ASPECTOS DESTACADOS

- Prevenir la mayoría de los ataques cibernéticos contra los endpoints de un entorno
- Detectar y bloquear las vulneraciones para reducir su impacto
- Mejorar la productividad y la eficiencia al descubrir amenazas en lugar de perseguir alertas
- Utilizar un solo agente de tamaño pequeño para un impacto mínimo en el usuario final
- Obtener protección y funcionalidad adicionales a través de módulos descargables
- Cumplir con las regulaciones, como HIPAA y PCI-DSS
- Implementar en el sitio o en la nube

Cada día trae consigo un nuevo ataque cibernético, una nueva vulnerabilidad o un nuevo ataque de ransomware. Los equipos de seguridad ven que es cada vez más difícil mantenerse al tanto con las amenazas a sus usuarios, los datos de la empresa y la propiedad intelectual, y no siempre brindan ayuda adicional. Los responsables de responder a incidentes están cargados con demasiadas herramientas que no funcionan juntas y crean más ruido que señales útiles. Los sistemas implementados no siempre brindan una detección y respuesta adecuadas a estas amenazas avanzadas.

FireEye Endpoint Security defiende contra los ataques cibernéticos actuales mejorando las mejores partes de la tecnología, la experiencia y la inteligencia heredadas de FireEye. Utilizando un modelo de defensa en profundidad, la arquitectura modular de Endpoint Security une motores predeterminados y módulos descargables para proteger, detectar y responder, y gestionar la seguridad del endpoint.

Para evitar el malware común, Endpoint Security utiliza un motor de plataforma de protección del endpoint (EPP) basado en firmas. Para encontrar amenazas para las cuales todavía no existe una firma, MalwareGuard utiliza el aprendizaje automático sembrado con conocimiento desde la primera línea de los ciberataques. Para ataques a exploits en software y navegadores comunes, ExploitGuard utiliza un motor de análisis de comportamiento que determina si se está utilizando un exploit y evita que se ejecute. Además, FireEye crea continuamente módulos para detectar técnicas de ataque y acelerar las respuestas a las amenazas emergentes. Por ejemplo, Process Guard se desarrolló para detener la exfiltración de credenciales.

> TI es un factor estratégico que impulsa nuestra capacidad de educar eficazmente a nuestros estudiantes. El uso de FireEye Endpoint Security garantiza que nuestros activos de TI estén disponibles, sean altamente operativos y estén protegidos, lo cual es fundamental para lograr nuestra misión.
>
> **— James D. Perry II**
> Director de Seguridad de la Información, Universidad de Carolina del Sur

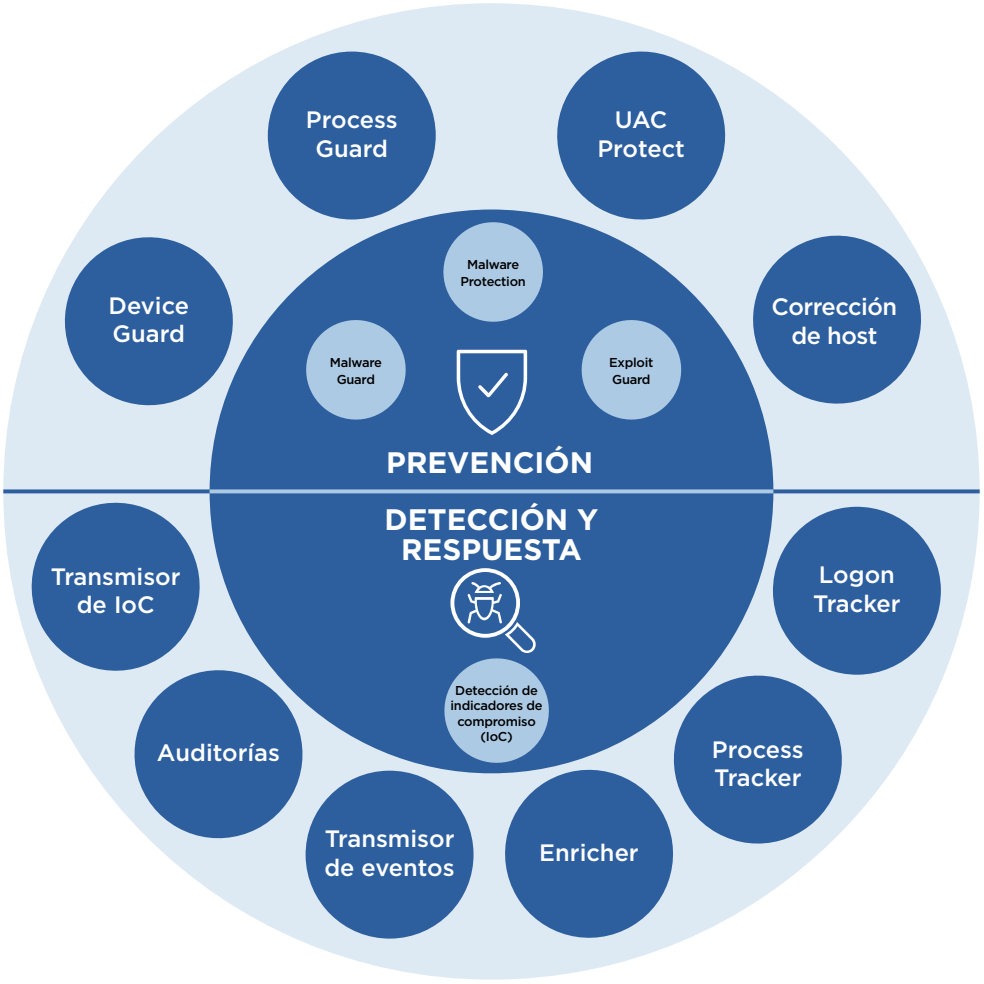
Incluso con la mejor protección, las brechas son inevitables. Para garantizar una respuesta sustancial que minimice la interrupción del negocio, Endpoint Security incluye capacidades de detección y respuesta del endpoint (EDR) que se basan en indicadores de compromiso (IOC) en tiempo real desarrollados con la ayuda de los responsables de respuesta de primera línea de Mandiant. Las herramientas de FireEye también hacen lo siguiente:

- Buscar e investigar amenazas conocidas y desconocidas en decenas de miles de endpoint en minutos
- Identificar y detallar los vectores que utilizó un ataque para infiltrar un endpoint
- Determinar si un ataque ocurrió (y continúa) en un endpoint específico y dónde se propagó
- Establecer la cronología y la duración de las vulnerabilidades del endpoint y hacer un seguimiento del incidente

Las amenazas modernas no se detienen en un solo endpoint, por lo que la reparación en un solo endpoint no resolverá la mayoría de las vulneraciones. La corrección completa se comunica de manera eficiente y apunta a todos los dispositivos donde una amenaza puede estar escondida y correlaciona esta información en tiempo real. Endpoint Security es un componente de FireEye Helix XDR, que conecta a la perfección todas las tecnologías y servicios de FireEye para detectar y responder a todas las amenazas más sofisticadas.

Figura 1.

Motores centrales de FireEye Endpoint Security (centro) y módulos disponibles (anillo exterior).



A menudo, los entes gerenciales piensan que cualquier virus es casi el fin del mundo. Con FireEye, podemos presentar pruebas reales para demostrar la naturaleza del problema y que hemos sido capaces de gestionarlo y contenerlo. Hacer que todas esas incógnitas se conozcan rápidamente ayuda a aliviar la presión de todos en la organización.

— Michael Hennessy, Director de Servicios Tecnológicos
Alpha Grainer Manufacturing, Inc

Características principales

- Agente único que utiliza defensa en profundidad para minimizar la configuración, la detección y el bloqueo
- Flujo de trabajo integrado para analizar y responder a amenazas dentro de Endpoint Security
- Protección contra malware con defensas antivirus (AV), aprendizaje automático, análisis de comportamiento, indicadores de riesgo (IOC) y visibilidad del endpoint
- Componente de FireEye Helix XDR para corregir completamente todas las amenazas en una organización

Características adicionales

- Enterprise Security Search para encontrar y resaltar rápidamente las actividades y amenazas sospechosas
- Data Acquisition para llevar a cabo inspección y análisis profundo del endpoint durante un período de tiempo específico
- Visibilidad integral que permite a los equipos de seguridad buscar, identificar y discernir rápidamente el nivel de las amenazas
- Capacidades de detección y respuesta para detectar, investigar y contener los endpoints rápidamente a fin de agilizar la respuesta
- Interfaz fácil de entender para una interpretación y respuesta rápidas ante cualquier actividad del endpoint sospechosa

Sistemas y entornos operativos compatibles	
Windows	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
Mac	10.9 – 10.15, 11
Linux	RHEL 6.8 – 6.10, 7.1 – 7.7, 8–8.2 CentOS 6.9 – 6.10, 7.1 – 7.7, 8 SUSE 11.3, 11.4,12.2 - 12.5 y 15 SUSE abierto 15.1, 15.2 Ubuntu 12.04, 14.04, 16.04, 18.04, 19.04, 20.04, 20.10 Amazon Linux AMI 2018.3, AM2 Oracle Linux 6.10, 7.6, 8 (1 and 2)

Opciones de implementación: dispositivo físico in situ, dispositivo virtual in situ, servicio FireEye Cloud Service

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

FireEye es una empresa de seguridad basada en inteligencia sobre amenazas. 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 la de un Estado 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.