FireEye

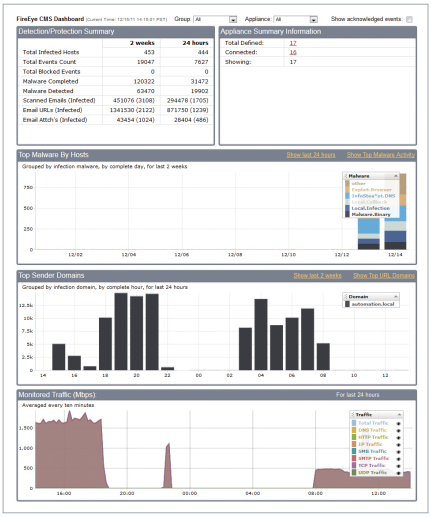
Ficha técnica

Central Management System

Intercambio local de datos sobre amenazas en tiempo real y administración unificada de despliegues empresariales

Aspectos destacados

- Dispositivo específico que puede desplegarse en aproximadamente 30 minutos
- Ideal para organizaciones que tienen que administrar cinco o más dispositivos de FireEye, o para aquellas que utilicen de forma conjunta Web MPS, Email MPS, File MPS y/o MAS de FireEye
- Dos modelos disponibles para adaptarse a despliegues de FireEye crecientes
- Administración centralizada y simplificada de varios dispositivos de FireEye que reduce el tiempo necesario para configuraciones, actualizaciones de amenazas y actualizaciones de software
- Panel de seguridad que permite consultar, de un vistazo, el estado de protección frente a ataques selectivos avanzados
- Almacén de eventos de seguridad consolidado que agiliza la generación de informes y las auditorías



El panel ofrece una vista en tiempo real del estado de seguridad de la red y de la carga de trabajo de los dispositivos

El sistema FireEye Central Management System (CMS) consolida las tareas de administración, generación de informes y uso compartido de datos de FireEye Malware Protection Systems (MPS) en un dispositivo fácil de desplegar y basado en la red.

El sistema CMS permite compartir en tiempo real información sobre malware generada automáticamente dentro de su despliegue de FireEye, con el fin de neutralizar los ataques avanzados contra la empresa. Además, centraliza la configuración, administración y generación de informes de los dispositivos de seguridad de FireEye.

Compartir en tiempo real información sobre malware local

Los dispositivos de FireEye generan protecciones contra el malware avanzado en tiempo real gracias al motor Virtual Execution (VX). CMS es un centro de distribución que garantiza que todo el despliegue de FireEye disfrute de protecciones dinámicas contra los ataques selectivos avanzados en curso. Además, los suscriptores a Malware Protection Cloud (MPC) pueden utilizarlo para centralizar el envío y recepción de información sobre malware.

Panel de seguridad con información resumida y detallada

El sistema CMS consolida las actividades y mejora el conocimiento de la situación gracias a un panel de seguridad unificado. Este panel ofrece a los administradores una visión en tiempo real del número de sistemas infectados, así como la posibilidad de acceder directamente a los detalles de la infección para determinar los pasos a seguir.

Análisis unificado de los ataques selectivos avanzados

El despliegue de Web MPS, Email MPS, File MPS y Malware Analysis System (MAS) de FireEye con FireEye CMS permite analizar de manera detallada las amenazas combinadas, por ejemplo, facilita la identificación de los mensajes de correo electrónico de phishing selectivo (o *spearphishing*) que se utilizan para distribuir URL maliciosas. Los analistas de seguridad pueden ahora encajar las piezas de un ataque combinado, lo que les permite tomar las medidas necesarias, de manera informada, para proteger a las empresas contra los ataques selectivos avanzados.

"Nuestro centro se toma muy en serio la seguridad de los usuarios, de ahí que apliquemos parches y antivirus a los sistemas de escritorio y utilicemos sistemas firewall e IPS en la puerta de enlace. Sin embargo, debido a que hay usuarios que sufren infecciones fuera de nuestra puerta de enlace, además de la realidad de los ataques de *spearphishing*, desconocidos (*zero-day*) y selectivos, sabemos que una solución basada en firmas no ofrece una protección completa contra los exploits web y las redes de bots actuales".

— Jefe de sistemas y servidores de una institución de estudios superiores de Artes Liberales

Consola y generación de alertas de categoría empresarial

La consola web de CMS permite buscar y filtrar los eventos, así como ver las notificaciones de alerta en tiempo real o enviarlas a través de SMTP, SNMP, syslog o HTTP POST. Los administradores pueden filtrar por evento, fecha o intervalo de IP, y en los resultados solo se muestran los datos que el administrador está autorizado a examinar según su función de TI. Las notificaciones también pueden enviarse a herramientas de administración de eventos y seguridad de la información (SIEM, Security Information and Event Management) de terceros, como ArcSight, Nitro Security, Splunk y RSA.

Desde la consola de CMS, los administradores pueden hacer clic en el vínculo de un evento y conectarse fácilmente a dispositivos de FireEye específicos para ver el sistema de administración local y comprobar el segmento de red que se está protegiendo.

Configuración y actualización de dispositivos centralizadas

Para llevar a cabo despliegues empresariales eficaces, FireEye CMS ofrece configuraciones dinámicas. La configuración puede determinarse de manera centralizada y, a continuación, distribuirse como corresponda. Los administradores pueden establecer y ver de forma remota la configuración de uno o varios dispositivos. Además, las actualizaciones pueden desplegarse en todos los dispositivos gestionados, lo que garantiza que todos ellos disfruten de las funciones de seguridad más actualizadas. Las actualizaciones del motor VX (como nuevas imágenes de invitado para obtener los últimos Service Packs) pueden desplegarse pulsando un botón.

Almacén consolidado y generación de informes detallados

Las organizaciones más grandes y reguladas pueden aprovechar las ventajas del almacén de datos de seguridad central de CMS para generar informes de manera eficaz y consolidada. El sistema CMS proporciona una forma de recopilar y almacenar los eventos de seguridad relevantes para las auditorías con el fin de satisfacer los requisitos de conservación de datos a largo plazo.

El sistema FireEye CMS ofrece métodos eficaces para buscar e informar sobre tipos concretos de amenazas, por nombre o por tipo. Los clientes también pueden ver resúmenes, como los principales hosts infectados y los principales eventos de malware y devolución de llamadas, así como detalles de geolocalización. Las vistas de tendencias pueden ayudar a demostrar cómo progresa la reducción del número de sistemas comprometidos.

Especificaciones técnicas

	CMS 4310	CMS 7300
Formato	Montaje en bastidor (1 unidad)	Montaje en bastidor (1 unidad)
Peso	13,6 kg	13,6 kg
Dimensiones (ancho x fondo x alto)	43,7 cm x 65 cm x 4,3 cm	43,7 cm x 65 cm x 4,3 cm
Alojamiento	Cabe en bastidor de 19 pulgadas	Cabe en bastidor de 19 pulgadas
Puertos de administración	(2) Puertos BASE-T 10/100/1000	(2) Puertos BASE-T 10/100/1000
Puertos de supervisión	N/D	N/D
Voltaje de entrada (CA)	Conmutación automática, 100 - 240 V de CA, de onda completa	Conmutación automática, 100 - 240 V de CA, de onda completa
Corriente de entrada (CA)	8,5 - 6,0 A	8,5 - 6,0 A
Fuente de alimentación/RAID	Dual 700 W/3 discos (HDD) SAS en hardware RAID5	Dual 700 W/3 discos (HDD) SAS en hardware RAID5
Frecuencia	50 - 60 Hz	50 - 60 Hz
Temp. de funcionamiento	10 °C a 35 °C	10 °C a 35 °C

Nota: todos los valores de rendimiento varían en función de la configuración del sistema y del perfil del tráfico procesado.