## Ficha técnica

# FireEye Central Management

## Centralice la gestión de dispositivos e información para correlacionar los datos en todos los vectores de ataque

### Aspectos destacados

- Ofrece controles integrados para implementaciones en plataformas múltiples
- Permite la prevención de amenazas combinadas a través de la correlación de múltiples vectores
- Proporciona una plataforma específica que puede implementarse en menos de 60 minutos
- Muestra un tablero de seguridad con información rápida que proporciona un estado avanzado de la protección contra ataques individualizados
- Informes rápidos y auditorías a través de un depósito consolidado de eventos de seguridad
- Optimiza la gestión de múltiples soluciones de FireEye y reduce el tiempo dedicado a la gestión de configuraciones, actualizaciones de amenazas y actualizaciones de software

**Figura 1.** CM 4500 y CM 9500 (CM 7500 no ilustrado).

### Descripción general

FireEye® Central Management (serie CM) consolida la administración, informe y distribución de datos de los productos de FireEye en una solución basada en la red, fácil de implementar. Central Management permite la distribución en tiempo real de la información sobre amenazas generada automáticamente para identificar y bloquear ataques avanzados dirigidos a su organización. También permite la configuración, gestión e informes centralizados de las soluciones FireEye.

### Distribución en tiempo real de la inteligencia de amenazas locales

Las soluciones FireEye generan información sobre amenazas en tiempo real mediante el motor FireEye Multi-Vector Virtual Execution™ (MVX). Central Management distribuye esa información sobre amenazas a varias implementaciones de FireEye a nivel de todos los sistemas, lo que garantiza que cada solución tenga la misma protección dinámica contra los ataques avanzados. Los suscriptores de la nube FireEye Dynamic Threat Intelligence™ (DTI) pueden usar Central Management para centralizar el envío y recepción de la información sobre amenazas anónima en las soluciones de FireEye implementadas en los clientes, socios de tecnología y proveedores de servicios en todo el mundo.

### Tablero de seguridad con información general, más desgloses

Central Management consolida actividades y mejora el conocimiento de la situación con un tablero de seguridad unificado. El tablero proporciona a los administradores una visión en tiempo real de la cantidad de sistemas infectados y analizar directamente los detalles de la infección para determinar los próximos pasos.

### Análisis unificado de ataques individualizados avanzados

Es posible realizar un análisis de amenazas combinadas, tales como la detección de un correo electrónico de spear-phishing utilizado para distribuir URL maliciosas y la correlación de una alerta del perímetro en el endpoint. Los analistas de seguridad pueden relacionar las piezas de un ataque combinado, a fin de obtener la información viable que necesitan para proteger a la organización contra ataques individualizados avanzados.

### Consolas y alertas de clase empresarial

Central Management proporciona una consola GUI basada en la web donde se pueden observar, buscar y filtrar eventos y notificaciones de alerta en tiempo real que se pueden enviar a través de SMTP, SNMP, syslog o HTTP POST. Los administradores pueden filtrar por eventos, fechas o rangos de IP, y los resultados se exhiben para mostrar solo datos basados en el rol operativo TI del administrador. Las notificaciones también pueden enviarse a herramientas SIEM de terceros. Los administradores pueden hacer clic en el enlace de un evento y conectarse sin interrupciones con soluciones específicas de FireEye para ver el segmento de la red protegido.

### Configuración central y actualizaciones de plataformas

Para implementaciones empresariales eficientes, Central Management presenta configuraciones dinámicas. Los ajustes pueden determinarse centralmente y luego distribuirse apropiadamente en una organización. Los administradores pueden, de manera remota, configurar y ver los ajustes de una o más soluciones de seguridad de FireEye. Además, todas las actualizaciones pueden implementarse simultáneamente en todas las soluciones administradas, asegurando que todas ellas tengan las últimas capacidades de seguridad.

### Depósito consolidado e informes detallados

Las organizaciones reguladas de mayor tamaño pueden usar Central Management para un informe consolidado y eficiente de los datos de seguridad. Central Management le permite recopilar y almacenar eventos de seguridad relevantes para la auditoría que cumplan con los requisitos de retención de datos a largo plazo.

Central Management ofrece formas convenientes de buscar e informar las amenazas por nombre o tipo. Las organizaciones también pueden ver resúmenes, tales como los principales servidores infectados y eventos de malware y devolución de llamada, incluidos los detalles de ubicación geográfica. Las vistas de tendencia pueden ayudar a demostrar el progreso en la reducción de la cantidad de sistemas vulnerados.

**Tabla 1.** Especificaciones de los aparatos.

| | CM 4500 | CM 7500 | CM 9500 |
|---|---|---|---|
| **Puertos de interfaz de red** | 2 puertos 1 GigE BaseT | 2 puertos 1 GigE BaseT | 2 puertos 1 GigE BaseT |
| **Puertos de administración (panel trasero)** | 2 puertos 1 GigE BaseT | 2 puertos 1 GigE BaseT | 2 puertos 1 GigE BaseT |
| **Puerto IPMI (panel trasero)** | Incluido | Incluido | Incluido |
| **Panel LCD y teclado (panel frontal)** | Incluidos | Incluidos | Incluidos |
| **Puertos PS/2 para teclado y mouse, DB15 VGA (panel trasero)** | Incluidos | Incluidos | Incluidos |
| **Puertos USB (panel trasero)** | 2 puertos USB tipo A | 2 puertos USB tipo A | 2 puertos USB tipo A |
| **Puerto serie (panel trasero)** | 115 200 bits/s, sin paridad, 8 bits, 1 bit de parada | 115 200 bits/s, sin paridad, 8 bits, 1 bit de parada | 115 200 bits/s, sin paridad, 8 bits, 1 bit de parada |
| **Capacidad de almacenamiento** | 4 unidades de HDD de 4 TB, RAID 10 utilizable; 8 TB | 4 unidades de HDD de 4 TB, RAID 10 utilizable; 8 TB | 4 unidades de HDD de 4 TB, RAID 10 utilizable; 8 TB |
| **Caja** | Montaje en bastidor 1RU, para un rack de 19 in | Montaje en bastidor 2RU, para un rack de 19 in | Montaje en bastidor 2RU, para un rack de 19 in |
| **Dimensiones del chasis (Ancho x Profundidad x Alto)** | 437 x 650 x 43,2 mm (17,2 in x 25,6 in x 1,7 in) | 438 x 620 x 88,4 mm (17,24 in x 24,41 in x 3,48 in) | 438 x 620 x 88,4 mm (17,24 in x 24,41 in x 3,48 in) |
| **Alimentación eléctrica (CA)** | Fuentes de alimentación eléctrica (CA) redundantes (1+1) de 750 W | Fuentes de alimentación eléctrica (CA) redundantes (1+1) de 800 W | Fuentes de alimentación eléctrica (CA) redundantes (1+1) de 800 W |
| **Potencia máxima (vatios)** | 245 W | 456 W | 612 W |
| **Disipación térmica máxima (BTU/h)** | 836 BTU/h | 1556 BTU/h | 2088 BTU/h |
| **Tiempo medio entre fallos (h)** | 35 200 h | 60 700 h | 60 700 h |
| **Peso neto/embalado kg (lb)** | 13,6 kg (30,0 lb)/18,6 kg (41,0 lb) | 20,0 kg (44,1 lb)/29,6 kg (65,3 lb) | 22,9 kg (50,4 lb)/32,5 kg (71,6 lb) |

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

**Tabla 1.** Especificaciones de los aparatos.

| | CM 4500 | CM 7500 | CM 9500 |
|---|---|---|---|
| **Certificaciones de seguridad** | IEC 60950, EN 60950, CSA 60950-00, marcado CE | IEC 60950, EN 60950, CSA 60950-00, marcado CE | IEC 60950, EN 60950, CSA 60950-00, marcado CE |
| **Certificaciones CEM/IEM** | FCC Parte 15, Subparte B, Clase A; ICES-003 Clase A; EN 61000-3-2 Clase A; EN 61000-3-3; CISPR22 Clase A | FCC Parte 15, Subparte B, Clase A; ICES-003 Clase A; EN 61000-3-2 Clase A; EN 61000-3-3; CISPR22 Clase A | FCC Parte 15, Subparte B, Clase A; ICES-003 Clase A; EN 61000-3-2 Clase A; EN 61000-3-3; CISPR22 Clase A |
| **Cumplimiento de normativas** | RoHS, REACH, WEEE | RoHS, REACH, WEEE | RoHS, REACH, WEEE |
| **Temperatura de funcionamiento** | 0 - 35 °C | 0 - 35 °C | 0 - 35 °C |
| **Humedad relativa de funcionamiento** | 10 - 95 % a 40 °C, sin condensación | 10 - 95 % a 40 °C, sin condensación | 10 - 95 % a 40 °C, sin condensación |
| **Altitud de funcionamiento** | 1524 m | 1524 m | 1524 m |

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

**Tabla 2.** Especificaciones de los aparatos virtuales.

| Modelo | Núcleos del CPU | RAM | NICS virtuales | Espacio en el disco rígido |
|---|---|---|---|---|
| **CM2500V** | 4 | 32 GB | 4 (total):<br>1 (administración)<br>1-3 (para uso futuro) | 512 GB |
| **CM7500V** | 16 | 128 GB | 4 (total):<br>1 (administración)<br>1-3 (para uso futuro) | 1200 GB |

**Nota:** Cada dispositivo virtual debe cumplir las siguientes especificaciones.

## 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.