Ficha técnica

FireEye Email Security Server Edition

Defensa adaptable, inteligente y escalable contra amenazas en el correo electrónico

Aspectos destacados

- Ofrece seguridad integral para el correo electrónico contra archivos adjuntos maliciosos, URL de suplantación de identidad de credenciales, falsificación informática (spoofing) y ataques de etapas múltiples y de día cero
- Admite el análisis de las imágenes de los sistemas operativos Microsoft Windows y Apple Mac OS X
- Examina extensivamente el correo electrónico para detectar amenazas ocultas en archivos adjuntos protegidos por contraseña, archivos adjuntos cifrados y URL
- Obtiene información sobre amenazas en tiempo real de la nube FireEye DTI
- Prioriza y contiene amenazas al proporcionar información contextual para las alertas
- Se implementa en las instalaciones con el servicio MVX integrado o distribuido

Figura 1. Los dispositivos de seguridad integrada para el correo electrónico incluyen EX 3500, EX 5500 y EX 8500.

Descripción general

El correo electrónico es el factor más vulnerable para los ataques cibernéticos ya que es el punto de ingreso de datos de mayor volumen. Las organizaciones enfrentan un número en constante crecimiento de desafíos de seguridad de amenazas avanzadas basadas en el correo electrónico. Las amenazas más avanzadas utilizan el correo electrónico para entregar URL vinculadas a sitios de suplantación de identidad de credenciales y archivos adjuntos armados. Debido a su elevado nivel de segmentación y personalización, el correo electrónico es el medio principal para los delitos cibernéticos.

FireEye Email Security ayuda a las organizaciones a minimizar el riesgo de costosas brechas de seguridad provocadas por ataques de correos electrónicos avanzados. Implementado en el sitio, FireEye Email Security Server Edition lidera la industria en cuanto a la identificación, aislamiento y detención inmediata de los ataques basados en archivos adjuntos y URL, antes de que los mismos ingresen al entorno de la organización. Email Security combina complementos de detección y contexto basado en la información para revelar las URL maliciosas y benignas de suplantación de identidad en una plataforma escalable de grandes datos. El motor Multi-Vector Virtual Execution™ (MVX) sin firma analiza archivos adjuntos de correo electrónico y las URL vinculadas al contenido descargable en función de una matriz cruzada integral de los sistemas operativos, aplicaciones y navegadores web. Las amenazas se identifican con un ruido mínimo y los falsos positivos son prácticamente inexistentes.

FireEye recopila amplia inteligencia sobre amenazas relativas a adversarios a través de investigaciones directas de las brechas de seguridad y millones de sensores. Email Security utiliza evidencia concreta e inteligencia contextual sobre ataques y atacantes para priorizar alertas y bloquear amenazas en tiempo real.

Al integrarse con FireEye Network Security y Endpoint Security las organizaciones pueden obtener una mayor visibilidad con respecto a ataques combinados de vectores múltiples y coordinar protección en tiempo real.

Defensa contra amenazas en el correo electrónico
La enorme cantidad de información personal disponible en línea hace posible que un delincuente cibernético pueda utilizar técnicas de ingeniería social para convencer a casi cualquier usuario de hacer clic en una URL o abrir un archivo adjunto.

Email Security proporciona detección y prevención en tiempo real contra ataques de phishing selectivo, recopilación de credenciales y suplantación que por lo general eluden las defensas de seguridad del correo electrónico tradicional. Los correos electrónicos se analizan y ponen en cuarentena (bloquean) si se detectan amenazas desconocidas y avanzadas que estén ocultas en:

- Tipos de archivos adjuntos que incluyen, entre otros, los siguientes: archivos EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 y ZIP/RAR/TNEF
- Archivos adjuntos protegidos por contraseña y cifrados
- Archivos adjuntos protegidos con contraseña con contraseñas enviadas por medio de una imagen
- URL integradas en correos electrónicos, documentos de MS Office, PDF y archivos de almacenamiento (ZIP, ALZIP, JAR), y otros tipos de archivos (Uuencoded, HTML)
- Archivos descargados a través de URL, e incluso enlaces FTP
- URL confusas, falsificadas, acortadas y redirigidas dinámicamente
- URL de suplantación de identidad de credenciales y errores tipográficos
- Vulnerabilidades desconocidas de la aplicación, el explorador y las imágenes de los sistemas operativos Microsoft Windows y Apple Mac OS X
- Código malicioso integrado en correos electrónicos de suplantación de identidad selectiva

Si bien los ataques de ransomware comienzan con un correo electrónico, normalmente se requiere una devolución a un servidor de comando y control para cifrar los datos. Email Security identifica y detiene estas campañas de malware de etapas múltiples difíciles de detectar.

Detección de amenazas superior

Email Security ayuda a mitigar el riesgo de costosas brechas de seguridad al identificar y aislar los ataque avanzados, selectivos y otros tipos de ataques evasivos que se ocultan como tráfico normal. Una vez que se detectaron, estos ataques se interceptan, analizan y almacenan en la memoria para identificar más rápidamente las amenazas futuras.

La parte central de Email Security se encuentran Advanced URL Defense, el motor MVX y MalwareGuard. Estas tecnologías utilizan análisis y aprendizaje automático a fin de identificar los ataques que eluden las defensas tradicionales basadas en firmas y políticas.

Una parte integral de Advanced URL Defense, PhishVision es un motor de clasificación de imágenes que utiliza el aprendizaje profundo para recopilar y comparar capturas de pantalla de marcas confiables y comúnmente atacadas con respecto a las páginas web a las que se hace referencia en las URL. Trabajando en combinación con PhishVision, Kraken es un complemento de detección de suplantación de identidad que aplica análisis de dominio y de contenido de la página para aumentar el aprendizaje automático. Skyfeed, otro avance en cuanto a la detección de URL, es un sistema de recopilación de información sobre malware de diseño específico y totalmente automatizado. A fin de descubrir falsos negativos se recopilan cuentas de redes sociales, blogs, foros y envíos de información sobre amenazas. La naturaleza multifacética de Advanced URL Defense ofrece a las organizaciones que están protegidas por Email Security una defensa incomparable contra los ataques de phishing selectivo y recopilación de credenciales.

MalwareGuard es una herramienta de aprendizaje automático que capta archivos binarios y genera una calificación de nivel de sospecha. MalwareGuard analiza todos los archivos ejecutables portables (Portable Executable, PE) que se detectan en línea. Se tomó una decisión en función de la calificación y se asigna un nombre a las detecciones que MalwareGuard desencadena.

El motor MVX detecta ataques de día cero, flujo múltiple y otros ataques evasivos al usar un análisis dinámico sin firma en un ambiente seguro y virtual. Identifica vulnerabilidades y malware no vistos anteriormente y detiene la infección y riesgo.

Mitigación de evasiones

Email Security admite una función de modo real controlado para defenderse contra los ataques que eluden las solicitudes de objetos remotos. El motor MVX detecta el malware que solicita descargas múltiples y devuelve los objetos remotos que solicitó el binario de muestra. El modo real controlado disminuye los falsos negativos para las descargas de etapas múltiples, los ataques de phishing selectivo avanzados y las intrusiones de ransomware avanzadas.

Los atacantes también pueden intentar eludir la tecnología que se utiliza para detectar las URL sospechosas. Como parte de Advanced URL Defense, las mitigaciones de evasión para los sitios de suplantación de identidad cambian de manera continua. Como parte de Advanced URL Defense, las mitigaciones de evasión se mejoran de manera continua. Otra mitigación de evasión, Guest Images puede personalizarse a fin de imitar un endpoint "usado" cuando se ejecuta un objeto potencialmente malicioso. Muchas técnicas de evasión se previenen garantizando que Guest Image reproduzca un dominio de endpoint, un usuario de dominio, datos de Outlook y el historial del navegador.

Integración para mejorar las eficiencias en el manejo de alertas
Email Security analiza todos los adjuntos de correo electrónico y las URL para identificar con precisión los ataques avanzados actuales. Las actualizaciones en tiempo real de todo el ecosistema de seguridad de FireEye, combinadas con la atribución de alertas de perpetradores conocidos, proporcionan contexto para priorizar y actuar en caso de alertas críticas y bloquear los ataques por correo electrónico avanzados. Las amenazas conocidas, desconocidas y no basadas en malware se identifican con un ruido y falsos positivos mínimos, de forma tal que los recursos se enfoquen en ataques reales para reducir los gastos operativos. La categorización de software de riesgo separa los intentos de ataque genuinos de la actividad indeseable pero menos maliciosa (como adware y spyware) para priorizar la respuesta a las alertas.

Adaptación rápida al cambiante panorama de las amenazas
Email Security ayuda a su organización a adaptar continuamente su defensa proactiva contra amenazas en el correo electrónico a través de información sobre amenazas en tiempo real proveniente de la nube FireEye Dynamic Threat Intelligence (DTI). La inteligencia profunda sobre las amenazas y atacantes combina inteligencia de adversarios, máquinas y víctimas para:

- Brindar una visibilidad mayor y oportuna ante las amenazas
- Identificar capacidades y funciones específicas del malware y los archivos adjuntos maliciosos detectados
- Proporcionar información contextual para priorizar y acelerar la respuesta
- Determinar la probable identidad y los motivos de un atacante, y realizar un seguimiento de sus actividades dentro de su organización
- Reescribir todas las URL integradas un correo electrónico a fin de proteger a los usuarios contra los enlaces maliciosos
- Identificar retroactivamente ataques de suplantación de identidad selectiva y prevenir el acceso a sitios de suplantación de identidad al destacar URL maliciosas

Integración del flujo de trabajo de respuesta
Email Security funciona sin interrupciones con FireEye Helix y FireEye Central Management.

- Como componente de la plataforma de operaciones de seguridad, FireEye Helix, proporciona visibilidad en toda la infraestructura. FireEye Helix aumenta las alertas de correo electrónico y de terceros con inteligencia, correlación con el endpoint, automatización y consejos de investigación. Con estas capacidades, FireEye Helix pone de manifiesto las amenazas inadvertidas y potencia las decisiones de los expertos.
- La administración central correlaciona las alertas de Email Security y Network Security para obtener una vista más amplia de un ataque y establecer reglas de bloqueo a fin de evitar que el ataque se propague.
- La administración central admite el etiquetado basado en roles para saber a quién se dirige.
- Central Management admite la respuesta de alerta y las correcciones de acuerdo con criterios basados en roles.

Capacidades adicionales
Personalización mediante reglas basadas en YARA
Email Security permite que los analistas especifiquen y prueben reglas personalizadas a fin de analizar los adjuntos de correo electrónico con el objetivo de detectar amenazas que atentan contra su organización.

Protección contra su suplantación ejecutiva
Email Security Server Edition ofrece la capacidad de bloquear los compromisos de correos electrónicos empresariales (Business Email Compromises, BEC) a fin de proteger contra la falsificación a los empleados importantes. Se crea una política que compara los nombres para mostrar del correo electrónico entrante con respecto a una lista aprobada que coincide con los remitentes aprobados.

Administración de la cola de mensajes, alerta y cuarentena
Email Security – Server Edition ofrece un alto nivel de control sobre los mensajes de correo electrónico que analiza. En el caso de implementaciones activas en modo de protección, es posible administrar y realizar un seguimiento de los mensajes a medida que avanzan en la cola del MTA. Los atributos de correo electrónico pueden utilizarse para buscar y verificar que los mensajes se recibieron, analizaron y entregaron al siguiente salto. Además, se pueden supervisar las tendencias en el tiempo a través de un panel intuitivo. Las listas explícitas para permitir/bloquear ofrecen un control personalizado sobre el procesamiento del correo electrónico. Es posible buscar y seleccionar los atributos de alertas comunes. Y pueden realizarse operaciones masivas en las alertas y los mensajes en cuarentena.

Protección activa o modo de solo supervisión
Email Security puede analizar los correos electrónicos y poner en cuarentena amenazas para una protección activa. Para implementaciones solo de supervisión, las organizaciones configuran una regla BCC transparente para enviar copias de los correos electrónicos a Email Security para el análisis.

Opciones de implementación flexibles
Email Security – Server Edition ofrece distintas opciones de implementación para que se ajusten a las necesidades y el presupuesto de una organización:

- **Seguridad integrada para el correo electrónico:** aparato de hardware independiente y todo en uno con servicio MVX integrado para proteger un punto de ingreso de correo electrónico en un solo lugar. FireEye Email Security es una solución fácil de gestionar que se implementa en menos de 60 minutos. No requiere reglas, políticas o configuración.
- **Seguridad distribuida para el correo electrónico:** aparatos extensibles con servicio MVX compartido centralmente a fin de proteger los puntos de acceso del correo electrónico dentro de las organizaciones.
- **Nodo inteligente de correo electrónico:** los sensores virtuales analizan el tráfico de correo electrónico para detectar y bloquear el tráfico malicioso y enviar actividad sospechosa a través de una conexión cifrada al servicio MVX para el análisis definitivo del veredicto.
- **Cuadro inteligente de MVX:** servicio MVX elástico, ubicado centralmente y en el sitio que ofrece escalabilidad transparente, tolerancia a errores N+1 incorporada y equilibrio de carga automatizado.

  La ampliación desde un aparato de hardware integrado a un cuadro inteligente de MVX proporciona una capacidad adicional para detectar y analizar amenazas en el correo electrónico durante períodos pico de rendimiento de mensajes.
- **FireEye Cloud MVX:** Suscripción al servicio MVX que garantiza la privacidad analizando el tráfico en el Nodo inteligente de correo electrónico. Solamente los objetos sospechosos se envían por medio de una conexión cifrada al servicio MVX, donde los objetos benignos se descartan.

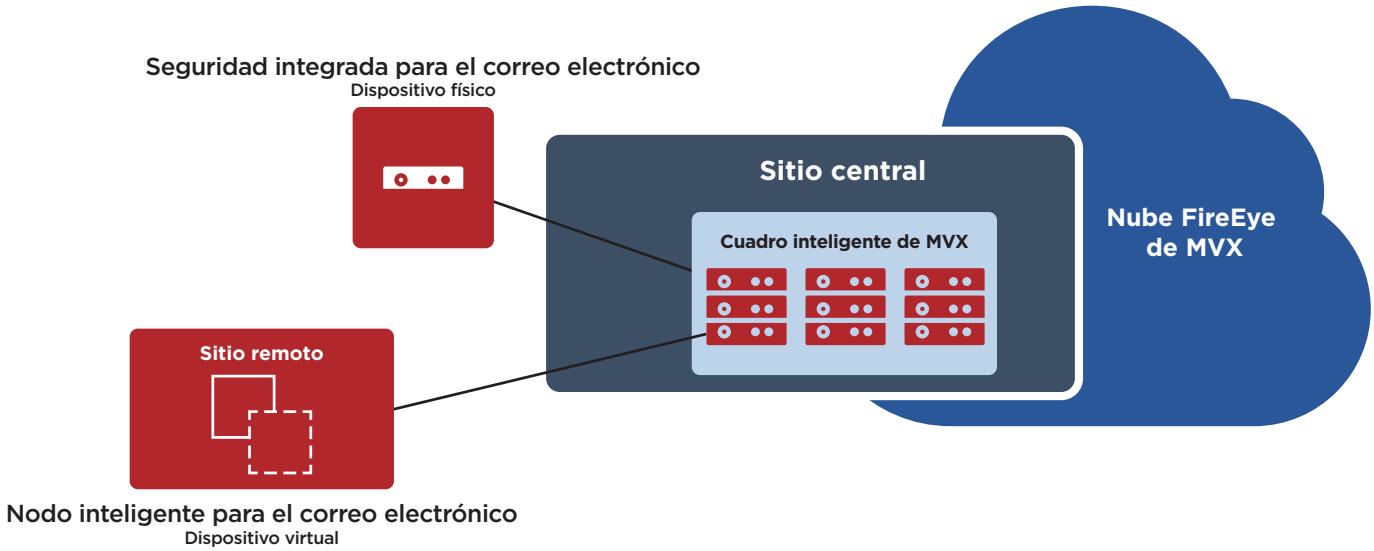

Figura 2. Modelos de implementación distribuidos y de ampliación de seguridad para el correo electrónico.

Tabla 1. Especificaciones técnicas.

	EX 3500	EX 5500	EX 8500
Rendimiento*	Hasta 700 archivos adjuntos únicos por hora	Hasta 1800 archivos adjuntos únicos por hora	Hasta 2650 archivos adjuntos únicos por hora
Puertos de interfaz de red	2 puertos 1 GigE BaseT	2 puertos 1 GigE BaseT	4 puertos SFP + (soporte de fibra 10GigE, cobre 10GigE, cobre 1GigE), 2 puertos 1GigE BaseT
Puertos de administración	2 puertos 1 GigE BaseT	2 puertos 1 GigE BaseT	2 puertos 1 GigE BaseT
Supervisión de IPMI	Incluidos	Incluidos	Incluidos
Puerto VGA (panel trasero)	Incluidos	Incluidos	Incluidos
Puertos USB (panel trasero)	4 puertos USB tipo A traseros	2 puertos USB tipo A frontales, 2 puertos USB tipo A traseros	2 puertos USB tipo A frontales, 2 puertos USB tipo A traseros
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 discos duros de 2 TB, RAID 10, 3,5 in, FRU	4 discos duros de 2 TB, RAID 10, 3,5 in, FRU	4 discos duros de 2 TB, RAID 10, 3,5 in, FRU
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)	Redundante (1+1) 750 W, 100 - 240 VCA, 9 - 4,5 A, conector IEC60320-C14 50 - 60 Hz, FRU	Redundante (1+1) 800 W, 100 - 240 VCA, 9 - 4,5 A, conector IEC60320-C14 50 - 60 Hz, FRU	Redundante (1+1) 800 W, 100 - 240 VCA, 9 - 4,5 A, conector IEC60320-C14 50 - 60 Hz, FRU
Alimentación eléctrica (CC)	No disponible	No disponible	No disponible
Potencia térmica máxima	245 vatios (836 BTU por hora)	456 vatios (1556 BTU por hora)	530 vatios (1808 BTU por hora)
Tiempo medio entre fallos (h)	54.200 horas	57.401 horas	53.742 horas
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)	20,2 kg (44,4 lb)/29,8 kg (65,6 lb)
Cumplimiento de las normas de seguridad	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Cumplimiento de la compatibilidad electromagnética	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015	FCC Parte 15 ICES-003 Clase A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 y V-3/2015
Certificaciones de seguridad	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
Cumplimiento ambiental	Directiva RoHS 2011/65/EU; REACH; Directiva WEEE 2012/19/UE	Directiva RoHS 2011/65/EU; REACH; Directiva WEEE 2012/19/UE	Directiva RoHS 2011/65/EU; REACH; Directiva WEEE 2012/19/UE
Temperatura de funcionamiento	0 ~ 35 °C (32 ~ 95 °F)	0 ~ 35 °C (32 ~ 95 °F)	0 ~ 35 °C (32 ~ 95 °F)
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	3000 m/9,842 pies	3000 m/9,842 pies	3000 m/9,842 pies

* Todos los valores de rendimiento varían en función de la configuración del sistema y del perfil del tráfico de correo electrónico procesado. Dimensione los dispositivos según los archivos adjuntos únicos por hora.

Tabla 2. Especificaciones del cuadro inteligente de FireEye MVX.

	VX 5500	VX 12500
SO compatibles	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
Rendimiento*	Hasta 480 archivos adjuntos únicos por hora	Hasta 3780 archivos adjuntos únicos por hora
Alta disponibilidad**	N+1	N+1
Puertos de administración (panel trasero)	1 puerto BASE-T de 10/100/1000 Mbit/s	1 puerto BASE-T de 10/100/1000 Mbit/s
Puertos de clúster (panel trasero)	3 puertos BASE-T de 10/100/1000 Mbit/s	1 puerto BASE-T 10/100/1000 Mbit/s, 2 puertos BASE-T de 10 Gbit/s
Puerto IPMI (panel trasero)	Incluidos	Incluidos
Monitor LCD delantero y teclado	No disponible	Incluidos
Puertos VGA	Incluidos	Incluidos
Puertos USB (panel trasero)	4 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
Capacidad del disco	2 unidades SAS HDD de 2 TB, 3,5 in, RAID 1, intercambiable sobre la marcha, FRU	4 unidades HDD de 4 TB, 3,5 in, SAS3, RAID 1, FRU
Caja	Montaje en bastidor 1RU, para un rack de 19 in	Montaje en bastidor 2RU, para un rack de 19 in
Dimensiones del chasis (Ancho x Profundidad x Alto)	17. 437 x 650 x 43,2 mm (2 x 25,6 x 1,7 in)	437 x 851 x 89 mm (17,2 x 33,5 x 3,5 in)
Alimentación eléctrica (CC)	No disponible	No disponible
Alimentación eléctrica (CA)	Redundante (1+1) 750 W, 100 - 240 VCA, 8 - 3,8 A, conector IEC60320-C14 de 50-60 Hz, intercambiable sobre la marcha, FRU	Redundante (1+1) 800 W: 100 - 127 V, 9,8 A - 7 A 1000 W: 220 - 240 V, 7 - 5 A, conector IEC60320-C14 FRU de 50 - 60 Hz, FRU
Consumo máximo de energía	285 W	760 W
Disipación térmica máxima	972 BTU por hora	2594 BTU por hora
Tiempo medio entre fallos	54.200 horas	38.836 horas
Peso neto/embalado	15 kg (33 lb)/21,8 kg (48 lb)	21 kg (46 lb)/40,2 kg (90 lb)
Certificación de seguridad	FIPS 140-2 Nivel 1, CC NDPP v1.1	FIPS 140-2 Nivel 1, CC NDPP v1.1
Cumplimiento de normativas de seguridad	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

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

** Con las configuraciones de hardware redundante adecuadas.

Tabla 3. Nodo inteligente FireEye Email Security, especificaciones del sensor virtual.

	EX 5500V
SO compatibles	Microsoft Windows, Apple macOS X
Rendimiento*	Hasta 1250 archivos adjuntos únicos por hora
Puertos de supervisión de red	2
Puertos de administración de red	2
Núcleos del CPU	8
Memoria	16 GB
Capacidad del disco	384 GB
Adaptadores de red	VMXNet 3, vNIC
Compatibilidad con hipervisores	VMWare ESXi 6.0 o posterior

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

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.