# McAfee Enterprise Security Manager

**Descubrir. Responder. Cumplir.**

La seguridad más eficaz empieza por la visibilidad en tiempo real de la actividad de todos los sistemas, redes, bases de datos y aplicaciones. McAfee® Enterprise Security Manager, base de la familia de soluciones de administración de información y eventos de seguridad (SIEM) de McAfee, ofrece rendimiento, información útil y conocimiento de la situación en tiempo real con la rapidez y el alcance que necesitan las organizaciones de seguridad para identificar, comprender y responder a las amenazas ocultas, y además incorpora un marco de cumplimiento que simplifica el cumplimiento de normativas.

**Principales ventajas**

- Visibilidad histórica y en tiempo real para facilitar una detección y una corrección exhaustivas de las amenazas.
- Información útil prioritaria en cuestión de minutos para agilizar la reacción ante las amenazas.
- Análisis avanzados y enriquecimiento de datos para convertir los datos en información de seguridad.
- Marco de cumplimiento de normativas con más de 240 normas de todo el mundo.

McAfee Enterprise Security Manager suministra en tiempo real información del mundo exterior —datos de amenazas, información de reputación y estado de vulnerabilidad— y permite ver los sistemas, datos, riesgos y actividades de la empresa. El departamento de TI puede por fin disponer de acceso completo y correlacionado al contenido y el contexto necesarios para adoptar con rapidez decisiones basadas en los riesgos, empleando los recursos para reaccionar de la mejor manera frente a un panorama de amenazas dinámico. Esto es fundamental para investigar ataques discretos y lentos, buscar indicadores de ataque y corregir controles de cumplimiento de normativas. Para optimizar las operaciones de seguridad, McAfee Enterprise Security Manager proporciona además herramientas integradas para la configuración y administración de cambios, la administración de casos y la administración centralizada de directivas: todo lo que se necesita para mejorar el flujo de trabajo y la eficacia del equipo de operaciones de seguridad.

## Información sobre amenazas avanzadas

Independientemente de si se trata del tráfico de la red, las actividades de los usuarios o el uso de aplicaciones, cualquier variación de la actividad normal puede ser indicio de una amenaza inminente, y de que sus datos o su infraestructura están en peligro. Con toda la información recopilada, McAfee Enterprise Security Manager calcula la actividad básica en tiempo real y emite alertas prioritarias con el fin de descubrir las amenazas potenciales antes de que actúen. Al mismo tiempo, analiza esos datos en busca de patrones que puedan ser indicativos de una amenaza mayor. Además, McAfee Enterprise Security Manager aprovecha la información contextual (como los análisis de vulnerabilidades y los sistemas de administración de identidades y autenticación) para completar los eventos de seguridad y comprender mejor cómo pueden afectar a los procesos reales de la empresa. Esta información permite a las organizaciones suministrar la información correcta a las personas adecuadas para emprender medidas en tiempo real y tomar decisiones más acertadas.

**Opciones de despliegue escalables**

- Las posibilidades de distribución híbrida incluyen dispositivos físicos y virtuales con opciones de alta disponibilidad.
- Despliegue en un solo dispositivo para empresas pequeñas o soluciones distribuidas para grandes compañías.
- Los dispositivos altamente escalables permiten recopilar enormes cantidades de datos de una amplia variedad de recursos e infraestructuras de seguridad.

## Datos cruciales en minutos, no en horas

Nuestro dispositivo de base de datos especializado puede recopilar, procesar y correlacionar miles de millones de eventos de registro de varios años con otros flujos de datos a la velocidad que necesitan las empresas. McAfee Enterprise Security Manager es capaz de almacenar miles de millones de eventos y flujos, haciendo que toda la información esté disponible de forma inmediata para consultas específicas, análisis forenses, validación de reglas y cumplimiento de normativas.

El acceso rápido a los datos de eventos almacenados durante largo tiempo es fundamental para investigar los ataques discretos y lentos, buscar indicios de amenazas persistentes avanzadas (APT) o intentar resolver una auditoría de cumplimiento de normativas no superada. Todo ello requiere visibilidad de los datos históricos y acceso total a los detalles de cada evento específico.

## Diseñado para Big Data

La seguridad basada en los grandes volúmenes de datos, lo que se conoce como Big Data, puede ser extremadamente valiosa, aunque el aumento permanente del volumen de eventos y de información de recursos, amenazas, usuarios y otros datos de interés supone un reto gigantesco para los equipos de seguridad. Para superarlo, McAfee Enterprise Security Manager empezó por un sistema de administración de datos (reconocido por Gartner como una de las principales ventajas de las soluciones SIEM de McAfee) pensado expresamente para el tipo de operaciones que requiere SIEM.

McAfee Enterprise Security Manager se diseñó para almacenar enormes cantidades de datos contextuales (cientos de millones) y completar los eventos en tiempo real. Toda esta información se somete a un exhaustivo proceso de indexación, normalización y correlación para detectar una gama más amplia de riesgos y amenazas. A fin de responder rápidamente a consultas sencillas y complejas, McAfee Enterprise Security Manager posee un sistema de indexación eficaz que también permite efectuar operaciones simultáneas, en tiempo real e históricas para optimizar las investigaciones y los análisis forenses de amenazas. Un requisito fundamental de SIEM es extraer Big Data para hallar información crucial de seguridad. McAfee Enterprise Security Manager aprovecha estos grandes volúmenes de datos de seguridad y va mucho más allá de la comparación con patrones para proporcionar indicadores de ataque a largo plazo e información práctica sobre amenazas.

## Conocimiento del contexto y del contenido

Cuando se dispone de información sobre el contexto —obtenida mediante analizadores de vulnerabilidades, sistemas de administración de identidades y autenticación, soluciones de privacidad u otros sistemas compatibles—, cada evento se completa con esa información y es posible comprender mejor la correlación entre los eventos de red y de seguridad, y los procesos y directivas reales.

La escalabilidad y el rendimiento de McAfee Enterprise Security Manager permiten recopilar más información procedente de un número mayor de fuentes, incluido el contenido de las aplicaciones, como documentos, transacciones y comunicaciones, que puede utilizarse para llevar a cabo análisis forenses más completos. Toda esta información se somete a un exhaustivo proceso de indexación, normalización y correlación para detectar una gama más amplia de riesgos y amenazas.

## Operaciones de seguridad optimizadas

McAfee Enterprise Security Manager simplifica las operaciones de seguridad proporcionando una vista centralizada del nivel de seguridad de la organización, el estado de cumplimiento normativo y los problemas de seguridad prioritarios que requieren investigación.

McAfee Enterprise Security Manager demuestra su utilidad desde el primer día, con cientos de informes, vistas, reglas y alertas que pueden emplearse de inmediato y personalizarse con facilidad. Tanto si va a establecer los criterios básicos para comprender el uso habitual de la red o simplemente a personalizar alertas, el panel de McAfee Enterprise Security Manager permite ver, investigar y generar informes sobre la información de seguridad más relevante. Ahora las organizaciones pueden disponer de acceso completo y correlacionado a los datos y el contexto necesarios para tomar decisiones rápidas y acertadas.

## Simplifique el cumplimiento de normativas

Al centralizar y automatizar la supervisión y la generación de informes de cumplimiento de normativas, McAfee Enterprise Security Manager elimina los largos procesos manuales. Además, la integración con el marco unificado de cumplimiento (Unified Compliance Framework, UCF) permite aprovechar la información recopilada una vez para demostrar el cumplimiento de muchas normativas, con el fin de satisfacer sus requisitos y mantener al mínimo los gastos y el trabajo de auditoría. La compatibilidad con UCF mejora la eficacia del cumplimento porque normaliza las particularidades de cada normativa, lo que permite asociar fácilmente cada conjunto de eventos recopilados a la normativa que corresponda.

McAfee Enterprise Security Manager facilita y agiliza la administración del cumplimiento normativo gracias a cientos de paneles preconfigurados, pistas de auditoría exhaustivas e informes para más de 240 normas y marcos de control mundiales, como PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX y SOX. Aparte de la amplia compatibilidad instantánea, todos los paneles, reglas e informes de cumplimiento de McAfee Enterprise Security Manager son totalmente personalizables.

## Conexión de su infraestructura de TI

Integradas, las soluciones de seguridad y de cumplimiento ofrecen juntas más que ninguna otra solución independiente, por sí sola, y brindan un nivel sin precedentes de visibilidad en tiempo real sobre el nivel de seguridad de una organización. Aunque las soluciones SIEM de McAfee recopilan información valiosa de cientos de tipos de dispositivos de seguridad de una infraestructura, McAfee Enterprise Security Manager también ofrece integración activa con la plataforma McAfee® ePolicy Orchestrator® (McAfee ePO™) para la administración de endpoints según las directivas, con McAfee Network Security Manager para la prevención de intrusiones y con McAfee Vulnerability Manager para el análisis y la corrección de vulnerabilidades.

McAfee Enterprise Security Manager viene integrado con McAfee Threat Intelligence Exchange. A diferencia de los métodos de seguridad estándar, esta combinación proporciona a las organizaciones un flujo de trabajo detallado en bucle cerrado que va desde la detección a la contención. A partir de la supervisión de los endpoints, McAfee Threat Intelligence Exchange identifica los ataques de baja frecuencia nutriéndose de la información mundial, local y de terceros sobre amenazas. Además, McAfee Threat Intelligence Exchange puede utilizar cualquier producto integrado de Security Connected, como McAfee Advanced Threat Defense, para analizar los archivos con más detalle y determinar cuáles son maliciosos. Esta técnica proporciona a las organizaciones información contextual y situacional del efecto que tienen los eventos de seguridad en sus procesos y directivas reales para decidir cómo enfocar mejor las estrategias de seguridad.

Esta profunda integración con las soluciones de seguridad de McAfee eleva la información de seguridad a un nivel superior, ya que permite implementar medidas inteligentes desde la consola de McAfee Enterprise Security Manager. McAfee Enterprise Security Manager aprovecha esta integración para modificar las directivas en los endpoints, poner en cuarentena los sistemas sospechosos de la red y reunir información determinante a través del análisis de vulnerabilidades, siempre desde la consola de McAfee Enterprise Security Manager. La integración de McAfee Global Threat Intelligence (McAfee GTI) con McAfee Enterprise Security Manager incluye datos de McAfee Labs procedentes de más de 100 millones de sensores de amenazas de todo el mundo, lo que constituye una fuente constante y actualizada de direcciones IP maliciosas conocidas. Gracias a este nivel de integración, McAfee Enterprise Security Manager puede automatizar numerosas medidas de respuesta inicial, lo que ayuda a las organizaciones a reaccionar ante los ataques con más rapidez y eficacia.

La plataforma Security Connected de McAfee ofrece un marco unificado para cientos de productos, servicios y partners que colaboran entre sí. Con las soluciones de Security Connected, como McAfee Enterprise Security Manager, los equipos de seguridad pueden ver la información específica del contexto en tiempo real, lo que les brinda una visibilidad inmediata del nivel de seguridad de toda la infraestructura de la organización para optimizar el tiempo de respuesta entre la detección y la corrección.

## Más información

Para obtener más información sobre McAfee Enterprise Security Manager, visite **www.mcafee.com/es/products/siem/index.aspx**.

**McAfee. Part of Intel Security.**
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com