McAfee Enterprise Security Manager

Priorizar. Investigar. Responder.

La seguridad más eficaz empieza por disponer de visibilidad de toda la actividad que se produce en los sistemas, redes, bases de datos y aplicaciones. Una solución de administración de información y eventos de seguridad (SIEM) es el pilar fundamental de una infraestructura de seguridad eficaz. McAfee® Enterprise Security Manager, núcleo central de la solución McAfee SIEM, ofrece el rendimiento, la inteligencia práctica y capacidad de integrar soluciones a la velocidad y escala que requieren las empresas de seguridad. Esta solución permite priorizar, investigar y responder rápidamente a las amenazas ocultas, así como cumplir los requisitos normativos.

Principales ventajas

- **Inteligente**: los análisis avanzados y el amplio contexto le ayudan a detectar y priorizar amenazas.
- **Práctica**: los datos que necesita se presentan en vistas dinámicas que incluyen la opción de tomar medidas para investigar, contener y corregir, así como adaptar lo necesario cuando se reciben alertas y patrones importantes.
- **Integrada**: supervisa y analiza datos desde una infraestructura de seguridad amplia y heterogénea, y ofrece integración bidireccional a través de interfaces abiertas. Asimismo, permite automatizar muchas respuestas iniciales.

McAfee Enterprise Security Manager suministra en tiempo real información del mundo exterior —de amenazas y reputación— y permite ver los sistemas, datos, riesgos y actividades de la empresa. El equipo de seguridad puede disponer de acceso completo y de manera correlacionada al contenido y al contexto necesarios para adoptar de forma rápida decisiones basadas en los riesgos, de manera que pueda invertir los recursos adecuados para reaccionar de la mejor forma frente a un panorama de amenazas dinámico y muy activo. Esto resulta fundamental para investigar ataques discretos y lentos, buscar identificadores de peligro o corregir los problemas detectados en auditorías. Para conseguir que la gestión de amenazas y el cumplimiento de normativas sea parte integral de las operaciones de seguridad, McAfee Enterprise Security Manager ofrece también herramientas integradas para la configuración y gestión de cambios, la gestión de incidencias y la administración centralizada de directivas —todo lo que necesita para mejorar el flujo de trabajo y la eficacia del equipo de operaciones de seguridad. Además, los paquetes de contenido disponibles para McAfee Enterprise Security Manager ofrecen configuraciones predefinidas para casos de uso de seguridad avanzados, que ayudan a simplificar las operaciones de seguridad.

Diseñada para grandes empresas

Los equipos de operaciones de seguridad necesitan aumentar su eficacia, ya que cada vez recopilan y examinan mayores volúmenes de datos sin procesar y analizados, procedentes de las arquitecturas empresariales dinámicas y distribuidas actuales. Para superar este desafío, McAfee Enterprise Security Manager utiliza un sistema de administración de datos (reconocido por analistas del sector y clientes como un punto fuerte de las soluciones SIEM de McAfee®) que fue creado específicamente para procesar grandes volúmenes de datos. Además, una arquitectura de datos muy escalable admite la ingestión, la administración y el análisis, para evitar poner en riesgo la recopilación, búsqueda y retención de datos. Estos riesgos pueden

Opciones de despliegue escalables

- Las opciones de distribución híbrida ofrecen la flexibilidad de seleccionar dispositivos físicos y virtuales con gran disponibilidad, así como proveedores de servicios de seguridad gestionados (del inglés, MSSP).
- Soluciones que crecen con usted; desde despliegues de un solo dispositivo para pequeñas empresas a soluciones distribuidas para grandes empresas.
- Los dispositivos muy escalables permiten recopilar muchos datos en una amplia gama de activos de seguridad y de infraestructura, y convertirlos en inteligencia práctica y priorizada.

afectar a las investigaciones cuando los datos fundamentales no están disponibles más tarde, si la respuesta a las consultas ralentiza el análisis o si únicamente puede realizarse una búsqueda parcial por causa del rendimiento.

Datos cruciales en minutos, no en horas

El acceso rápido a los datos de eventos que llevan mucho tiempo almacenados es fundamental para investigar incidentes, buscar pruebas de ataques avanzados o intentar corregir 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.

Nuestros dispositivos especializados pueden recopilar, procesar y correlacionar eventos incluidos en registros de varios años con otras fuentes de datos, como la inteligencia sobre amenazas basada en STIX, con la rapidez que requieren las empresas. McAfee Enterprise Security Manager es capaz de almacenar miles de millones de eventos y flujos, de manera que toda la información esté disponible de forma inmediata para consultas específicas, análisis forenses, validación de reglas y cumplimiento de normativas.

Conocimiento del contexto y del contenido

Cuando hay información de contexto disponible —como fuentes de datos de amenazas y reputación, sistemas de administración de identidades y acceso, soluciones de privacidad u otros sistemas admitidos— dicha información se añade para completar el contexto de los eventos. Esta información complementaria permite ampliar el conocimiento y conseguir una clasificación más precisa, gracias a la correlación entre los eventos de seguridad y de la red con los atributos de los activos y los procesos y directivas empresariales.

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

Interpretación de amenazas avanzadas

Independientemente de si se trata de tráfico de red, actividades de los usuarios o uso de las aplicaciones, cualquier variación de la actividad normal puede ser indicio de la existencia de una amenaza inminente, y de que sus datos o su infraestructura están en peligro. McAfee Enterprise Security Manager calcula la actividad típica para toda la información recopilada y emite alertas con prioridades, con el objetivo de descubrir las amenazas potenciales antes de que se produzcan. Al mismo tiempo, analiza la información en busca de patrones que puedan ser indicativos de una amenaza mayor. Además, McAfee Enterprise Security Manager aprovecha la información de contexto de cada evento para poder entender mejor el impacto que pueden tener los eventos de seguridad en los procesos empresariales reales.

Los paneles de Cyber Threat Manager de McAfee Enterprise Security Manager ofrecen una mejor supervisión y comprensión de las amenazas emergentes en tiempo real. La información sobre amenazas, ya estén bajo sospecha o confirmadas, que se haya comunicado a través de STIX/TAXII, McAfee Advanced Threat Defense y/o URL web de terceros se puede agregar y correlacionar casi en tiempo real o a posteriori (mediante la herramienta Backtrace) con datos de los eventos, con el fin de facilitar a los equipos de seguridad un conocimiento más profundo de la propagación de las amenazas en un entorno concreto. Esta inteligencia permite a las organizaciones suministrar los datos correctos a las personas adecuadas para emprender medidas casi en tiempo real y tomar decisiones más acertadas.

Operaciones de seguridad optimizadas

La experiencia del usuario centrada en el análisis de McAfee Enterprise Security Manager ofrece una mayor flexibilidad y facilidad de personalización, así como una respuesta más rápida a las investigaciones. Gracias a los flujos de trabajo simplificados, la administración de incidentes es más puntual y efectiva. Con un acceso rápido e inteligente a la información, para todos los analistas, ya sean principiantes o expertos, será más fácil priorizar, investigar y responder a las amenazas en evolución.

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. Ya se trate de fijar una referencia para determinar el uso típico de la red o simplemente para personalizar las alertas, el panel de McAfee Enterprise Security Manager facilita la visualización, investigación y generación de 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.

Además, McAfee Enterprise Security Manager incluye paquetes de contenido para simplificar las operaciones de seguridad con casos de uso prediseñados que ofrecen acceso rápido a funciones de administración de amenazas avanzadas o cumplimiento de normativas. Estos paquetes de contenido son configuraciones preconfiguradas para casos de uso de seguridad habituales que proporcionan grupos de reglas, alarmas, vistas, informes, variables y listas de vigilancia. Muchos paquetes de contenido proporcionan activadores preconfigurados para los comportamientos, que garantizan un escrutinio adicional o una solución automática.

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 de cumplimiento unificado (Unified Compliance Framework, UCF) permite aprovechar la información recopilada una vez para demostrar el cumplimiento de muchas normativas, con el fin de satisfacer los requisitos y mantener al mínimo los gastos y el trabajo de auditoría. La compatibilidad con UCF facilita el cumplimiento, ya que al estandarizar los detalles de cada normativa, se puede saber fácilmente a qué norma corresponde cada grupo concreto de eventos recopilados.

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

La integración en toda su infraestructura de seguridad proporciona un nivel sin precedentes de visibilidad en tiempo real del estado de seguridad de su empresa. McAfee Enterprise Security Manager puede recopilar datos de gran valor de cientos de dispositivos de proveedores de seguridad, así como de fuentes de inteligencia sobre amenazas. La integración con McAfee Global Threat Intelligence (McAfee GTI) aporta datos de McAfee Labs procedente 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. McAfee Enterprise Security Manager puede también ingerir información de amenazas, comunicada a través de STIX/TAXII y/o URL web de terceros, y tomar medidas basadas en análisis.

Asimismo McAfee Enterprise Security Manager ofrece integraciones activas con docenas de soluciones de administración y análisis de incidentes complementarias, como las soluciones de partners de McAfee e McAfee Security Innovation Alliance.

Por ejemplo, McAfee Threat Intelligence Exchange, que se basa en la supervisión de endpoints, agrega ataques de baja prevalencia para aprovechar inteligencia sobre amenazas mundial, de terceros y local. McAfee Threat Intelligence Exchange puede utilizar también otros productos integrados, como McAfee Advanced Threat Defense, para análisis adicionales y captura de archivos.

Los equipos de respuesta a incidentes y los administradores utilizan McAfee Active Response para buscar archivos maliciosos de tipo zero-day que estén inactivos en los sistemas, así como procesos activos en la memoria. Además, McAfee Active Response emplea recopiladores continuos para supervisar de forma constante sus endpoints y descubrir indicadores de peligro concretos, de manera que pueda alertarle si alguno aparece en su entorno. Esta combinación, a diferencia del enfoque de seguridad estándar, ofrece a las empresas un flujo de trabajo detallado y de bucle cerrado que va del descubrimiento a la contención y la solución.

McAfee proporciona un sistema de seguridad integrado que le permite prevenir y responder a las amenazas emergentes. Le ayudamos a resolver más amenazas, de forma más rápida y con menos recursos. Nuestra arquitectura conectada y nuestra administración centralizada reducen la complejidad y mejoran la eficacia operativa en su infraestructura de seguridad completa. McAfee se ha comprometido a ser su partner de seguridad número uno, proporcionándole un paquete completo de funciones de seguridad integradas.

Más información

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

Para obtener más información sobre las soluciones integradas, visite **www.mcafee.com/mx/solutions/intelligent-security-operations.aspx**.

McAfee Ireland LLC
2821 Mission College Blvd,
Santa Clara, CA – 95054
www.mcafee.com/mx