

# McAfee Vulnerability Manager

Supervisión de activos continua, en tiempo real y de alto rendimiento

## Principales diferenciadores

- Escalabilidad y flexibilidad de instalación sin igual
- Evaluación en tiempo real de nuevos dispositivos en cuanto se detectan en la red, inventario completo de software y hardware, correspondencia entre los usuarios y los activos, y topología de red automática
- Combinación del descubrimiento de la red activo y pasivo, y la supervisión para descubrir los dispositivos virtualizados, móviles y ocultos
- Exhaustivas auditorías de dispositivos que determinan los análisis y alimentan una base de datos de activos de gran fiabilidad
- El etiquetado dinámico de sistemas puede automatizar completamente la evaluación de vulnerabilidades
- Con la actualización de las últimas vulnerabilidades y amenazas obtenida a través de McAfee Global Threat Intelligence™
- Alta seguridad basada en credenciales con integración con Cyber-Ark
- Análisis de redes IPv4 e IPv6
- Generación de informes de máxima flexibilidad: los activos se analizan una vez y los informes se generan en cualquier momento
- Los flujos de gestión de riesgos automáticos pueden incluir las aplicaciones de McAfee, domésticas y de terceros

Proteja su empresa con la solución más flexible, acreditada y ampliable del sector: gestión integral de vulnerabilidades simplificada y en tiempo real. McAfee® Vulnerability Manager con la función McAfee Asset Manager proporciona una capacidad de ampliación y un rendimiento inigualables, que cubre de manera activa y pasiva todo en su red. Cualquier dispositivo o activo que tenga una dirección IP o utilice su red puede ser identificado y evaluado por McAfee Vulnerability Manager, de manera automática o en tiempo real. Esto permite conocer con exactitud el estado de cumplimiento de todos los activos de su red.

McAfee Vulnerability Manager marca la pauta en el mercado al trabajar con las realidades que definen su empresa y analizar todos los tipos de configuraciones de redes y activos. Puede realizar análisis de manera pasiva, ininterrumpida o activa cuando y donde sea necesario, lo que le permitirá detectar, evaluar y corregir sus activos, así como realizar los informes necesarios. Puede descubrir los dispositivos ocultos en su red, así como los smartphones, tablets y portátiles que se conectan y desconectan entre los distintos análisis planificados. Se sorprenderá de lo que no veía o analizaba, y que podía poner en peligro el cumplimiento de las normativas. Miles de empresas confían en McAfee Vulnerability Manager para detectar y priorizar rápidamente vulnerabilidades, con despliegues que incluyen desde unos pocos cientos de nodos hasta los que analizan continuamente más de cuatro millones de direcciones IP.

## Fácil implementación

McAfee facilita la implementación de análisis fiables. McAfee Vulnerability Manager se instala fácilmente en su hardware físico o virtual, aunque también puede utilizar nuestros dispositivos con seguridad reforzada. En cuestión de minutos, pondrá en marcha su primer análisis.

La carga y el mantenimiento de su inventario de activos también es simple. Con el módulo McAfee Asset Manager, la base de datos de activos se actualiza inmediatamente a medida que se conectan nuevos dispositivos, para que sepa en tiempo real qué dispositivos hay. Además, McAfee Vulnerability Manager se integra directamente con las herramientas de administración de activos de la empresa, incluidas LDAP, Microsoft Active Directory y la plataforma de administración McAfee® ePolicy Orchestrator® (McAfee ePO™), por lo que podrá mantener un repositorio central de datos de activos.

## Visibilidad de todos los activos

La opción McAfee Asset Manager incrementa la visibilidad gracias a la supervisión y el descubrimiento pasivo y siempre en funcionamiento. Este sistema, que se despliega rápidamente en un puerto SPAN, supervisa el tráfico con el fin de descubrir y asignar todo lo que haya en la red, como dispositivos no fiables, hosts VMware olvidados y dispositivos móviles. Mientras vigila, esta opción muestra los dispositivos, patrones y comunicaciones, detalles que le ayudarán a calibrar y mitigar los riesgos. Los datos de los dispositivos se envían automáticamente a McAfee Vulnerability Manager para su evaluación inmediata. Además, McAfee Asset Manager puede crear un inventario completo de software y hardware de cada activo que identifica.

## Análisis personalizados según sus necesidades

McAfee Vulnerability Manager ofrece varias opciones para medir y documentar el cumplimiento de las normativas del sector. Para una rápida definición de directivas, analice un sistema "patrón oro" para establecer un punto de referencia, utilice las plantillas de cumplimiento de normativas incluidas o cargue directivas aprovechando nuestra compatibilidad con el protocolo SCAP (Security Content Automation Protocol).

McAfee Vulnerability Manager analiza todos los activos conectados a la red, incluso los segmentos en entornos aislados y las infraestructuras críticas. Por ejemplo, si tiene redes sin una conexión externa, puede desplegar un analizador virtual o basado en un portátil para descubrir y analizar estos activos. A continuación, tiene la opción de mantener los resultados en el entorno restringido o, si es necesario, acumularlos en un sistema centralizado.

### Cobertura de análisis

- Análisis de más de 450 variedades de sistemas operativos, incluidos Microsoft Windows, UNIX, Cisco, Android, Linux, Apple Macintosh, Apple iOS y VMware
- Analiza en profundidad aplicaciones web (OWASP Top 10 y CWE Top 25)
- Busca vulnerabilidades y malware en Adobe, AOL, Apple, Microsoft (Office, IIS, Exchange), Blue Coat, CA, Cisco, Citrix, Facebook, Google, HP, IBM (Lotus Notes y WebSphere), Novell, Oracle, Real Networks, RIM (Blackberry Enterprise Server), SAP, Oracle Java, Symantec y VMware
- Analiza bases de datos líderes del sector, incluidas DB2, MySQL, Oracle, Microsoft SQL Server y Sybase

### Estándares y certificaciones

- Incluye plantillas para ASCII 33, BASEL II, BILL 198 (CSOX), BSI IT (GR), COBIT, FDCC, FISMA, GLBA, HIPAA, ISO 27002, JSOX, MIT5, PCI, SOX, NIST SP 800-68, SANS Top 20, SCAP, OVAL, y otras muchas
- Es compatible con numerosos estándares, como las auditorías con certificación CIS, COBIT, CPE, CVE, CVSS, DISA STIG, FDCC/SCAP, ISO17799/ISO 27002/FINRA, ITIL, NIST-SP800, NSA, OVAL y SANS Top 20
- Certificación Common Criteria
- Validación FIPS-140-2 para el cifrado

### Especificaciones técnicas

Visite [www.mcafee.com/es](http://www.mcafee.com/es) para consultar las especificaciones y requisitos actuales de hardware y software.

La mayoría de los sistemas operativos requieren credenciales de activos para revelar la información de configuración confidencial, sin embargo, algunos equipos de seguridad consiguen acceder a dichas credenciales. Gracias a la integración con la suite Privileged Identity Management de Cyber-Ark, se realiza el descubrimiento y el análisis basados en credenciales de manera rápida y segura con un excelente resultado.

### Determinación del riesgo en cuestión de minutos

Cuando McAfee Asset Manager identifica un nuevo sistema en la red, transmite información detallada sobre él a McAfee Vulnerability Manager para activar un análisis selectivo. En solo unos minutos, conocerá el estado de ese sistema y el riesgo que supone para su entorno.

### Etiquetado de activos para mejorar la eficacia

También puede utilizar directivas de etiquetado para colocar los nuevos dispositivos en grupos de análisis automáticamente, en función del perfil y el riesgo de cada dispositivo. Según las directivas, el análisis puede realizarse de manera inmediata o como parte del próximo análisis periódico.

### Detección de vulnerabilidades y malware

Mientras otros simplemente realizan un análisis superficial de puertos abiertos y configuraciones, McAfee Vulnerability Manager va mucho más allá. Realiza evaluaciones en el nivel de aplicaciones y sistemas, que incluyen banners de bases de datos, configuraciones de directivas, claves de registro, permisos de archivos y unidades, y servicios en ejecución. El producto prueba más de 450 versiones de sistemas operativos para detectar una amplia gama de vulnerabilidades. Nuestras inspecciones también detectan contenido malicioso, incluidos troyanos, virus y otro malware.

Puede complementar nuestras comprobaciones predefinidas y actualizaciones para amenazas de tipo zero-day con comprobaciones y secuencias de comandos personalizadas para probar programas propios y heredados. McAfee Vulnerability Manager también evalúa contenido de otros fabricantes que cumpla con XCCDF, OVAL y otros estándares SCAP.

### Especial atención a las aplicaciones web

McAfee Vulnerability Manager permite a los administradores gestionar aplicaciones web del mismo modo que gestionan activos basados en redes tradicionales. Los activos de aplicaciones web pueden agruparse y tienen su propia importancia, propietarios y personalidad. Con las funciones totalmente automatizadas, McAfee Vulnerability Manager realiza análisis de aplicaciones web en profundidad en todo el espectro de vulnerabilidades web.

### Siempre al día

Millones de sensores en todo el mundo informan a cientos de investigadores de los laboratorios McAfee Labs sobre los cambios más recientes en el panorama de amenazas. McAfee Global Threat Intelligence proporciona las evaluaciones de riesgos en tiempo real y las notificaciones de amenazas directamente a McAfee Vulnerability Manager para que la solución le proteja anticipándose a las nuevas amenazas.

### Administración, escalabilidad e integración según sus necesidades

McAfee ofrece flexibilidad para diseñar sus análisis, informes y tareas de gestión conforme a sus preferencias. Puede supervisar solamente los activos de un analizador concreto o bien observar el progreso de cientos de motores de análisis remotos desde una sola consola. Nuestra arquitectura de varias capas puede adaptarse para satisfacer las necesidades de empresas de cualquier tamaño.

A través de una interfaz de programación de aplicaciones (API) abierta, McAfee Vulnerability Manager puede integrar la mayoría de las aplicaciones.

### Respuesta en función del riesgo

Con una única vista de las vulnerabilidades se reducen los parches y los costes de las auditorías. Por ejemplo, los Martes de parches puede decidir rápidamente qué equipos podrían estar afectados por una nueva vulnerabilidad de Microsoft Windows o Adobe. En cuestión de minutos, sin necesidad de realizar un nuevo análisis de toda la red, McAfee Vulnerability Manager visualiza y clasifica el potencial de riesgo de nuevas amenazas basándose en calificaciones de riesgos y datos de configuración existentes.

Con esta información, puede seleccionar activos en función de su importancia y hacer clic con el botón derecho del ratón para ejecutar un análisis selectivo inmediato.

### Cumplimiento de normativas y confianza

Las pruebas concluyentes, como resultados de análisis previstos y reales, sistemas no analizados y errores de análisis, demuestran que los sistemas en cuestión "no son vulnerables", un requisito de autoría cada vez más común. Gracias a la combinación de supervisión activa y pasiva, las pruebas de penetración, los análisis autenticados y los análisis sin credenciales, McAfee Vulnerability Manager permite detectar las vulnerabilidades y las infracciones de directivas con el máximo nivel de precisión. La gestión integral de vulnerabilidades no ha sido nunca tan sencilla.

