

# IBM Tivoli Endpoint Manager for Security and Compliance

*Una única solución para gestionar la seguridad de los puntos finales a lo largo de la organización*



---

## Características principales

- Proporcionar la visibilidad y el control actualizados a partir de una única consola de gestión
  - Emplear un agente único, versátil e inteligente, que evalúe y solucione problemas con el fin de ayudar a garantizar la seguridad y la conformidad continuadas
  - Gestionar cientos de miles de puntos finales, físicos y virtuales, sea cual fuere la ubicación, tipo de conexión o estado
  - Identificar, gestionar y presentar informes sobre las excepciones de políticas y variaciones con analíticas de seguridad y conformidad
  - Gestionar parches automáticamente para sistemas y aplicaciones de sistemas operativos
- 

Como el número de puntos finales y las amenazas que pueden comprometerlo continua creciendo a un ritmo sin precedentes, IBM® Tivoli® Endpoint Manager for Security and Compliance proporciona la visibilidad unificada, en tiempo real y el cumplimiento para proteger su entorno distribuido y altamente complejo.

Diseñado para garantizar la seguridad de puntos finales a lo largo de toda la organización, Tivoli Endpoint Manager for Security and Compliance puede ayudar a su organización tanto a proteger los puntos finales como a asegurar a los reguladores que usted cumple con las normas de conformidad de seguridad. Es una solución fácil de gestionar, rápida de implementar que soporta seguridad en un entorno susceptible de incluir una amplia variedad y un gran número de puntos finales – a partir de servidores a PC de escritorio, laptops de ‘servicio itinerario’ conectados a Internet, teléfonos inteligentes y otros dispositivos móviles, además de equipos especializados como dispositivos de puntos de ventas (POS), ATMs y quioscos de autoservicio.

Tivoli Endpoint Manager for Security and Compliance puede reducir los costos y la complejidad de la gestión de TI como aumentar la agilidad, velocidad para la solución y la precisión. Su bajo impacto sobre las operaciones de los puntos finales puede intensificar la productividad y mejorar la experiencia del usuario. Al hacer cumplir la conformidad de la política por dondequiera que los puntos finales transiten, Tivoli Endpoint Manager for Security and Compliance ayuda a reducir el riesgo y a aumentar la visibilidad auditoría. La velocidad y la eficiencia del agente inteligente proporcionan conformidad continua con ciclos de auditoría automatizados en minutos en vez de semanas.



## Abordando las necesidades de seguridad a lo largo de la organización

Tivoli Endpoint Manager for Security and Compliance atiende los desafíos de seguridad relacionados con entornos de escritorio, móviles y distribuidos. Al proporcionar la gestión de puntos finales y seguridad en una única solución, ayuda a garantizar protección y conformidad de forma continua. Por ejemplo, puede reducir notablemente las brechas de vulnerabilidad de seguridad al aplicar parches de software en minutos. Puede ayudar a reducir las diferencias entre funciones como aquellas que establecen y ejecutan estrategias y políticas, aquellas que gestionan dispositivos en tiempo real, y aquellas que generan informes sobre problemas de seguridad y conformidad.

Entre las posibilidades de Tivoli Endpoint Manager for Security and Compliance se encuentra su capacidad para:

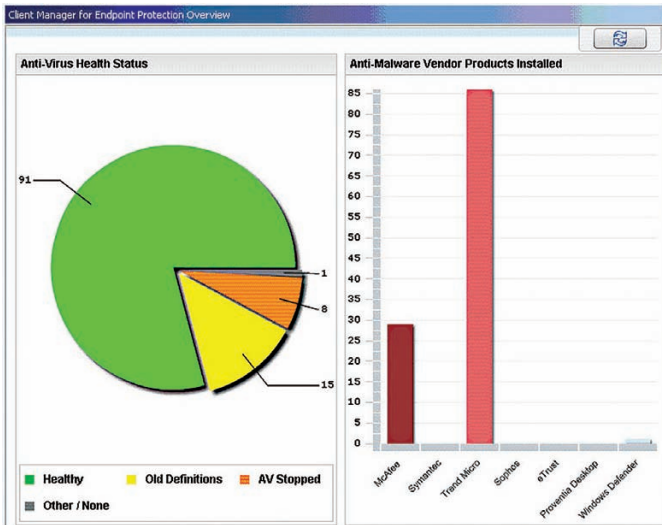
- Proporcionar visibilidad exacta, precisa y actualizada, y ejecución continua, de configuraciones y parches de seguridad.
- Centralizar la gestión de protección de anti-malware de terceros y firewall.
- Proporcionar buenas prácticas listas para usar, que cumplen con la reglamentación del Federal Desktop Configuration Control (FDCC) de los Estados Unidos y con las Guías de Implementación Técnica de la Agencia de Sistemas de Información de la Defensa (DISA STIGs).
- Dar soporte al Security Content Automation Protocol (SCAP); Tivoli Endpoint Manager es el primer producto certificado por el National Institute of Standards and Technology (NIST), tanto para evaluación como para resolución.
- Transmitir las instrucciones a los puntos finales con seguridad, como demostrado mediante las certificaciones Nivel 2, NIAP CCEVS EAL3 y FIPS 140-2.
- Dar soporte al estándar Open Vulnerability and Assessment Language (OVAL) para promover el contenido de seguridad abierto y públicamente disponible.
- Recibir y actuar con base en las alertas de riesgo de seguridad y vulnerabilidad publicadas por el Instituto SANS.

- Mostrar la tendencia y análisis de cambios de configuración de seguridad mediante la presentación de informes sobre analíticas de conformidad.
- Utilizar las analíticas para atender a las necesidades con el fin de obtener conocimiento y presentación de informes para cumplir las normas de conformidad y los objetivos de seguridad de TI, incluso: determinar el desarrollo y las tendencias históricas hacia la política de configuración de seguridad constante.

Capacidades adicionales proporcionadas para todos los productos de la familia Tivoli Endpoint Manager, basados en la tecnología Bigfix®, incluyen la capacidad de:

- Descubrir los puntos finales que las organizaciones pueden no darse cuenta que existen a su entorno – hasta 30 por ciento más en algunos casos.
- Proporcionar una única consola para las funciones de gestión, configuración y seguridad, simplificando las operaciones.
- Destinar acciones específicas a un tipo exacto de configuración de puntos finales o tipo de usuario, utilizando virtualmente cualquier propiedad de software o hardware para hacerlo.
- Emplear una infraestructura de gestión unificada de coordinación entre operaciones de TI, seguridad, escritorio y servidor.
- Llegar a los puntos finales independientemente de la localización, tipo de conexión o estado, con la gestión completa de todos los principales sistemas operativos, aplicaciones de terceros y parches basados en políticas.

Tivoli Endpoint Manager for Security and Compliance permite los procesos automatizados, altamente enfocados que proporcionan control, visibilidad y velocidad para efectuar un cambio e informar sobre la conformidad. Los ciclos de resolución son cortos y rápidos – con los problemas de programas malignos y virus atendidos con rápidas capacidades de gestión de parches.



Tivoli Endpoint Manager for Security and Compliance proporciona informes que ayudan a las organizaciones a visualizar los problemas que afectan la efectividad de los esfuerzos de seguridad y conformidad.

## Ofreciendo un amplio rango de funciones de seguridad de gran alcance

Tivoli Endpoint Manager for Security and Compliance incluye las funciones clave a continuación – y le brinda la posibilidad de adicionar fácilmente otras funciones dirigidas según se necesite, sin añadir costos de infraestructura o implementación.

### Gestión de parches

La gestión de parches incluye las capacidades completas para ofrecer parches a Microsoft Windows, UNIX, Linux y Mac OS y para los proveedores de aplicaciones, como Adobe, Mozilla, Apple y Java a los puntos finales distribuidos – independiente de su ubicación, tipo de conexión o estado. Un único servidor de gestión puede dar soporte a hasta 250.000 puntos finales, acortando los tiempos de los parches sin pérdida en funcionalidad de punto final, incluso a través de ancho de banda bajo o redes distribuidas globalmente. Los reportes en tiempo real proporcionan información de qué parches fueron desplegados, cuándo fueron desplegados, y quién los desplegó, así como la confirmación automática de que los parches fueron aplicados para obtener una solución completa de circuito cerrado para el proceso de parches.

### Gestión de configuración de seguridad

Homologado por el Instituto Nacional de Estándares y Tecnología, los dispositivos de configuración de seguridad de la solución proporcionan una biblioteca completa de controles técnicos que pueden ayudarlo a obtener la conformidad de seguridad mediante la detección y la aplicación de las configuraciones de seguridad. Las bibliotecas de políticas soportan el cumplimiento continuo de las líneas de base de la configuración; informan, resuelven y confirman en tiempo real la resolución de los puntos finales que no están en conformidad; y aseguran una visión verificada en tiempo real de todos los puntos finales.

Este dispositivo ofrece información significativa sobre el estado y la seguridad de los puntos finales independientemente de ubicación, sistema operativo, conexión (incluyendo computadoras con conexión física o computadoras portátiles móviles con conexión intermitente), o aplicaciones instaladas. Ayuda a consolidar y unificar el ciclo de vida de conformidad, reduciendo el tiempo de configuración y resolución de los puntos finales.

### Gestión de vulnerabilidad

La gestión de vulnerabilidad le permite descubrir, evaluar y remediar las vulnerabilidades antes de que los puntos finales sean afectados. El dispositivo evalúa los sistemas en comparación con las definiciones e informes de vulnerabilidad del lenguaje de seguridad del código abierto estandarizado (OVAL) de incumplimiento de políticas en tiempo real. El resultado es una visibilidad mejorada y una integración completa de cada paso en el flujo de trabajo completo para descubrir, evaluar, remediar e informar.

El personal de TI puede identificar y eliminar – usando las acciones manuales y automatizadas – las vulnerabilidades por todos los puntos finales. Al utilizar una única herramienta tanto para descubrir como para remediar las vulnerabilidades, los administradores pueden incrementar la velocidad y la precisión, disminuyendo los ciclos de resolución para el despliegue de parches, las actualizaciones de software y las soluciones de vulnerabilidades. Los administradores pueden configurar las alarmas para identificar más rápidamente los activos invasores y tomar medidas para ubicarlos con el fin de resolución o eliminación. Ellos pueden extender la gestión de seguridad para clientes móviles conectados o desconectados de la red.

### Descubrimiento de activos

Con Tivoli Endpoint Manager for Security and Compliance, el descubrimiento de activos deja de ser un ejercicio de trabajo minucioso. Crea conciencia de la situación dinámica acerca de las condiciones cambiantes en la infraestructura. La posibilidad de explorar la red por completo brinda, a menudo, la visibilidad y el control para ayudar a garantizar que las organizaciones identifiquen rápidamente los dispositivos localizables de IP – incluso máquinas virtuales, dispositivos y periféricos de red como impresoras, escáneres, enrutadores y conmutadores además de puntos finales de computadora – con el mínimo impacto de la red. Esta función ayuda a mantener la visibilidad de todos los puntos finales de la empresa, incluyendo computadoras móviles laptop y notebook, que tienen servicio itinerante que va más allá de la red de la empresa.

### Gestión de protección de puntos finales de multiprovedores

Este dispositivo brinda a los administradores un único punto de control para gestionar clientes de seguridad de puntos finales de terceros, a partir de proveedores, como por ejemplo Computer Associates, McAfee, Sophos, Symantec y Trend Micro. Con esta posibilidad de gestión centralizada, las organizaciones pueden mejorar la escalabilidad, la velocidad y la confiabilidad de soluciones de protección. El dispositivo supervisa el estado del sistema para asegurar que los clientes de seguridad de puntos finales estén siempre funcionando y que las firmas de virus se encuentren siempre actualizadas. Además de proporcionar una visión unificada de tecnologías dispares, facilita la migración de puntos finales a partir de una solución hacia otra, con la remoción y reinstalación del software ‘mediante un click’. La verificación de circuitos cerrados asegura que las actualizaciones y otros cambios sean concluidos, incluso la verificación habilitada mediante Internet para los puntos finales desconectados de la red.

### Cuarentena automática de red

Tivoli Endpoint Manager for Security and Compliance evalúa automáticamente los puntos finales en comparación con las configuraciones de conformidad necesarias – y si el punto final encontrado está fuera de la conformidad, la solución puede configurar el punto final para que éste sea colocado en cuarentena en la red hasta que se obtenga la conformidad. Tivoli Endpoint Manager tiene el acceso de gestión al punto final, pero el resto de los accesos se encuentra desactivados.

### La familia Tivoli Endpoint Manager

Además, usted puede consolidar herramientas, reducir el número de agentes de puntos finales y reducir sus costos de gestión al ampliar su inversión en Tivoli Endpoint Manager for Security and Compliance para incluir otros componentes de la familia Tivoli Endpoint Management. Debido a que todas las funciones operan desde la misma consola, el mismo servidor de gestión y el mismo agente de punto final, añadir más servicios es tan sencillo como un cambio de clave de licencia.

- **Tivoli Endpoint Manager for Core Protection** – Aplica las capacidades del firewall integradas contra programas maliciosos y personales a los puntos finales físicos y virtuales al efectuar consultas de la inteligencia en tiempo real en las amenazas de la nube con el fin de eliminar prácticamente la necesidad de ficheros de identificaciones documentales en los puntos finales.
- **Tivoli Endpoint Manager for Power Management** – Proporciona el cumplimiento de las políticas de conservación de energía por toda la organización, con la granularidad necesaria para habilitar la aplicación de políticas para una única computadora.
- **Tivoli Endpoint Manager for Lifecycle Management** – Atiende la convergencia de las funciones de TI de hoy al proporcionar la visibilidad en tiempo real hacia el estado de los puntos finales y al brindar a los administradores la funcionalidad avanzada para gestionar esos puntos finales.
- **Tivoli Endpoint Manager for Software Use Analysis** – Ofrece la posibilidad de descubrir y analizar las aplicaciones instaladas en escritorios, laptops y servidores. Detallar más la información sobre publicadores de software títulos y aplicaciones – hasta nivel de versión – también incluye estadísticas agregadas e información de uso.

## Tivoli Endpoint Manager: Construido sobre tecnología BigFix

El poder que está detrás de todas las funciones de Tivoli Endpoint Manager es único, un enfoque de infraestructura única que distribuye la toma de decisiones hacia los puntos finales, proporcionando beneficios extraordinarios a lo largo de toda la familia de soluciones, con funciones que incluyen:

- **An intelligent agent** – Tivoli Endpoint Manager utiliza un enfoque líder de la industria que coloca un agente inteligente en cada punto final. Este agente único desempeña múltiples funciones, incluso auto evaluación continua y cumplimiento de políticas – sin embargo tiene un impacto mínimo sobre el rendimiento del sistema. Al contrario de las arquitecturas tradicionales de cliente-servidor que esperan para recibir instrucciones desde un punto de control central, este agente inicia las acciones de una manera inteligente, enviando mensajes hacia arriba, hacia el servidor de gestión central y tomando parches, configuraciones u otra información hacia el punto final cuando sea necesario, para estar en conformidad con una política relevante. Como resultado de la inteligencia y de la velocidad del agente, el servidor de gestión central siempre sabe el estado de conformidad y de cambio de los puntos finales, permitiendo reportes de conformidad rápidos y actualizados.
- **Informes** – La consola única y unificada construida en Tivoli Endpoint Manager monta un alto nivel de visibilidad que incluye presentación de informes y análisis continuos a partir de los agentes inteligentes en los puntos finales de la organización.
- **Capacidades de Relay** – La arquitectura escalable y ligera de Tivoli Endpoint Manager permite que cualquier agente sea configurado como un relay entre otros agentes y la consola. Esta función de relay permite el uso de servidores o estaciones de trabajo existentes para transferir paquetes a lo largo de la red, reduciendo la necesidad de servidores.
- **Mensajes IBM Fixlet®** – Fixlet Relevance Language es un comando publicado que permite a los clientes, asociados de negocios y desarrolladores crear políticas y servicios personalizados para los puntos finales gestionados por las soluciones de Tivoli Endpoint Manager.

## Extendiendo el compromiso de Tivoli hacia la seguridad

Tivoli Endpoint Manager for Security and Compliance forma parte del portafolio completo de seguridad de IBM, que ayuda a atender los desafíos de seguridad a lo largo de la organización. Dando soporte a las operaciones de TI instrumentadas, interconectadas e inteligentes de un planeta más inteligente, las soluciones de seguridad de IBM ayudan a asegurar la visibilidad en tiempo real, el control centralizado y mejor seguridad para la infraestructura de TI completa, incluyendo sus puntos finales distribuidos globalmente.

---

### La familia Tivoli Endpoint Manager en resumen

---

#### Requerimientos de servidor:

- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

#### Requerimientos de consola:

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

#### Plataformas con soporte del agente:

- Microsoft Windows, incluyendo XP, 2000, 2003, Vista, 2008, 2008 R2, 7, CE, Mobile, XP Embedded y Embedded Point-of-Sale
  - Mac OS X
  - Solaris
  - IBM AIX®
  - Linux en IBM System z®
  - HP-UX
  - VMware ESX Server
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise
  - Oracle Enterprise Linux
  - CentOS Linux
  - Debian Linux
  - Ubuntu Linux
-

## Para obtener más información

Para saber más acerca de IBM Tivoli Endpoint Manager for Security and Compliance, póngase en contacto con su representante de ventas de IBM o Asociado de Negocios IBM, o visite [ibm.com/tivoli/endpoint](http://ibm.com/tivoli/endpoint)

## Acerca del software Tivoli de IBM

El software Tivoli de IBM ayuda a las organizaciones a gestionar de manera eficiente y efectiva sus recursos, tareas y procesos de TI, para cumplir con los siempre cambiantes requerimientos de negocios y entregar flexibilidad a la gestión de servicio de TI, mientras al mismo tiempo que ayuda a reducir costos. El portafolio Tivoli abarca software para seguridad, conformidad, almacenamiento, rendimiento, disponibilidad, configuraciones, operaciones y gestión de ciclo de vida de TI, y cuenta con el respaldo de servicios, soporte e investigación de IBM de clase mundial.

particular o no violación. Los productos de IBM están garantizados de acuerdo a los términos y condiciones de los contratos (ej. Contrato con el Cliente de IBM, Declaración de Garantía Limitada, Contrato de Licencia de Programa Internacional, etc.) bajo los cuales se proporcionan.

El cliente es responsable por asegurar la conformidad con los requerimientos legales. Es responsabilidad exclusiva del cliente el obtener asesoría o consejo legal competente en cuanto a la identificación e interpretación de las leyes relevantes y requerimientos regulatorios que puedan afectar a los negocios del cliente y cualquier acción que el cliente necesite emprender para cumplir con dichas leyes. IBM no proporciona asesoría legal ni declara o garantiza que sus servicios o productos aseguren que el cliente esté en conformidad con cualquier ley o regulación.



© Copyright IBM Corporation 2011

IBM Corporation  
Software Group  
Route 100  
Somers, NY 10589  
EE.UU.

Producido en los Estados Unidos de América  
Noviembre de 2011

IBM, el logotipo IBM, [ibm.com](http://ibm.com) y Tivoli son marcas o marcas registradas de International Business Machines Corporation en los Estados Unidos, otros países o ambos. Si estos y otros términos de marca registrada de IBM son comercializados durante la primera ocurrencia en esta información con un símbolo de marca registrada (® o ™), estos símbolos indican marcas o marcas registradas de derecho consuetudinario en los EE.UU. propiedad de IBM en el momento en que esta información sea publicada. Dichas marcas registradas también pueden ser marcas registradas o marcas registradas de derecho consuetudinario en otros países. Existe una lista actualizada de marcas registradas de IBM en la Web en 'Información de copyright y marcas registradas' en [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

BigFix y Fixlet son marcas registradas de BigFix, Inc., una compañía de IBM.

Adobe es una marca registrada de Adobe Systems Incorporated en los Estados Unidos, y/o en otros países.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos, otros países o ambos.

Microsoft y Windows son marcas registradas de Microsoft Corporation en los Estados Unidos, otros países o ambos.

UNIX es una marca registrada de Open Group en los Estados Unidos y otros países.

Java y todas las marcas y logotipos basados en Java son marcas registradas de Oracle y/o sus filiales.

Otros nombres de compañías, productos y servicios pueden ser marcas registradas o marcas de servicios de terceros.

Las referencias en esta publicación sobre los productos y servicios de IBM no significa que IBM tenga la intención de ponerlos a disposición en todos los países en los cuales IBM opera.

Ninguna parte de este documento puede ser reproducida ni transmitida bajo ninguna modalidad sin permiso por escrito de IBM Corporation.

Los datos del producto han sido revisados para obtener precisión a partir de la fecha de la publicación inicial. Los datos del producto están sujetos a cambios sin previo anuncio. Cualquier declaración en relación a la dirección futura e intenciones de IBM está sujeta a cambio o retiro sin notificación previa, y exclusivamente representa metas y objetivos.

La información proporcionada en este documento es distribuida 'como está' sin ninguna garantía, ya sea expresa o implícita. IBM expresamente se exime de cualquier garantía de comercialización, adecuación para un propósito en



Reciclar por favor