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

Highlights

- Proporcionar visibilidad actualizada y control a partir de una única consola de gestión
- empleando un único agente versátil e inteligente que evalúa y remedia los problemas para ayudar a asegurar seguridad y conformidad continuas.
- Gestionar cientos de miles de puntos finales, físicos y virtuales, independientemente de la ubicación, tipo de conexión o estado
- Gestionar automáticamente parches para los sistemas y aplicaciones de los sistemas operativos múltiples

En un mundo donde el número de puntos finales, y las amenazas que pueden ponerlos en riesgo, están creciendo a un ritmo sin precedentes, IBM Tivoli® Endpoint Manager for Security and Compliance proporciona visibilidad y vigilancia unificadas y en tiempo real para proteger sus entornos distribuidos y altamente complejos.

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. Ofrece una solución de gestión fácil y de despliegue rápido que da soporte a la seguridad en un entorno con posibilidad de incluir una extensa diversidad y un gran número de puntos finales, desde servidores a PCs de escritorio, computadoras portátiles de 'servicios itinerantes' conectadas a Internet, y equipos especializados como dispositivos de puntos de ventas (POS), ATMs y kioscos de autoservicio.

Tivoli Endpoint Manager for Security and Compliance puede reducir los costos y la complejidad de gestión de TI conforme aumenta la agilidad empresarial, la velocidad de remediación 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 auditoríade puntos auditables en forma continua.

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 y distribuidos. Al proporcionar la gestión de puntos finales y seguridad en una única solución, ayuda a garantizar protección y conformidad continuas. Por ejemplo, puede reducir notablemente las brechas de vulnerabilidad de seguridad al aplicar parches de software en minutos. Y 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 de modo seguro las instrucciones para puntos finales como es demostrado a través de las certificaciones Nivel 2, NIAP CCEVS EAL3 y FIPS 104-2.
- 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 a través de informes avanzados.

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

- Descubrir puntos finales que las organizaciones podrían no saber que se encontraban en sus entornos, hasta en un 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, los problemas con virus y programas malignos son abordados con posibilidades rápidas de gestión de parches.

Ofreciendo un amplio rango de funciones de seguridad de gran alcance

Tivoli Endpoint Manager for Security and Compliance incluye las siguientes funciones clave y le brinda la capacidad de agregar fácilmente otras funciones dirigidas según se necesite, sin adicionar costos de infraestructura o implementación.

Gestión de parches

La gestión de parches incluye las posibilidades completas para ofrecer parches para Sistemas Operativos Microsoft® Windows®, UNIX®, Linux® y Mac, y para los proveedores de aplicaciones, tales como Adobe®, Mozilla, Apple y Java™ para puntos finales

distribuidos, independientemente 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 de 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.

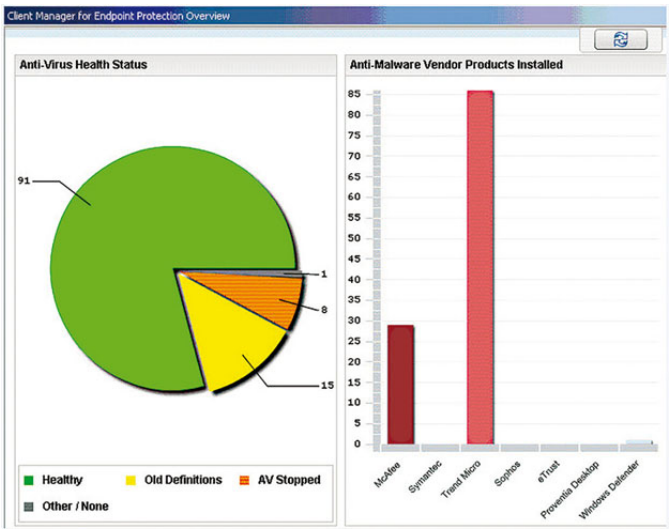
Gestión de configuración de seguridad

Validados 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 lograr la conformidad de seguridad por medio de la detección y vigilancia de las configuraciones de seguridad. Las bibliotecas de políticas dan soporte al monitoreo y control constante de las líneas 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 remediación 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 contra las definiciones e informes de vulnerabilidad del lenguaje de seguridad del código abierto estandarizado (OVAL) de políticas de no conformidad en tiempo real. El resultado es



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.

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 a lo largo de 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 extender la gestión de seguridad hacia los clientes móviles conectados o desconectados de la red, configurando alarmas para identificar rápidamente los activos de invasores y tomando las medidas con el fin de localizarlos para su solución o eliminación.

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 capacidad de explorar la red por completo brinda, frecuentemente, la visibilidad y el control dominantes para ayudar a asegurar que las organizaciones identifiquen rápidamente todos los dispositivos de IP a los que se les puedan asignar direcciones, incluso dispositivos de red y periféricos como impresoras, escáneres, enrutadores y conmutadores, además de los puntos finales de la computadora, con impacto mínimo en 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 contra las configuraciones de conformidad necesarias, y si el punto final se encuentra fuera de conformidad, la solución puede configurar el punto final de tal manera que este sea colocado en cuarentena en la red hasta que se obtenga la conformidad. El servidor de Tivoli Endpoint Manager tiene acceso de gestión al punto final, pero el resto de los accesos se encuentran desactivados.

Servicio de reputación de la Web y anti-malware (suplemento opcional)

La integración profunda con Core Protection Module(CPM) de Trend Micro proporciona dispositivos para proteger los puntos finales contra virus, caballos de Troya, worms, spyware, rootkits, y nuevas variantes de programas y sitios Web malignos, al efectuar consultas en tiempo real en los datos de inteligencia de amenazas de la nube, para prácticamente eliminar la necesidad de archivos de firma en los puntos finales. La tecnología de reputación de la Web previene que el usuario acceda a sitios Web maliciosos, ya sea mediante sus propias acciones o mediante acciones ocultas, acciones automatizadas ejecutadas por programas malignos.

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 Power Management** – Esta opción permite hacer cumplir las políticas de conservación de energía a lo largo de toda la organización, con la granularidad necesaria para permitir la aplicación de políticas en una única computadora.
- **Tivoli Endpoint Manager for Lifecycle Management** – Este enfoque completo y altamente eficaz atiende a las convergencias de hoy en funciones de TI, al proporcionar visibilidad en tiempo real hacia el estado de los puntos finales del sistema y al brindar a los administradores funcionalidades avanzadas para gestionar esos puntos finales.

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:

- **Un agente inteligente** – Tivoli Endpoint Manager utiliza un abordaje líder en la industria que coloca un agente inteligente en cada punto final. Este agente único realiza múltiples funciones incluyendo auto-evaluación continua y cumplimiento de políticas – sin embargo tiene un impacto mínimo en 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 es 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 conoce el estado de conformidad y de cambio de los puntos finales, permitiendo reportes de conformidad rápidos y actualizados.
- **Informes** – la consola única y unificada incorporada en Tivoli Endpoint Manager orquesta un alto nivel de visibilidad que incluye reportes y análisis continuos y en tiempo real provenientes de agentes inteligentes ubicados en los puntos finales de la organización.
- **Capacidades de Relay** – la arquitectura escalable y ligera de Tivoli Endpoint Manager permite a cualquier agente ser 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®** – El Fixlet Relevance Language es un lenguaje de comandos publicado que permite a los clientes, asociados de negocios y desarrolladores crear políticas y servicios personalizados para 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 un vistazo

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

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 gestión de servicio TI flexible y responsiva, 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.

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

Producido en los Estados Unidos de América
Febrero de 2011

Tivoli software

TID14075-COES-00