IBM Tivoli Endpoint Manager for Security and Compliance

Una sola solución para administrar la seguridad del equipo terminalde clientes finales a través de la organización

Destacados

- Brinda visibilidad y control actualizados desde una sola consola de administración.
- Emplea un solo agente inteligente, multipropósito que evalúa y remedia temas para ayudar a asegurar cumplimiento y seguridad continuos.
- Administra cientos de miles de clientes finales, físicos y virtuales, sin importar su ubicación, tipo de conexión o estado.
- Administra automáticamente parches para aplicaciones y sistemas operativos múltiples

En un mundo donde una cantidad de clientes finales y las amenazas que pueden comprometerlos están creciendo a un índice sin precedente, el Tivoli Endpoint Manager for Security and Compliance de IBM brinda una visibilidad y una aplicabilidad unificadas en tiempo real para proteger su entorno complejo y altamente distribuido.

Diseñado para asegurar la seguridad de los clientes finales a través de toda su organización, Tivoli Endpoint Manager for Security and Compliance puede ayudar a su organización a proteger los clientes finales y a asegurar los reguladores de que está en cumplimiento con los estándares de seguridad. Brinda una solución fácil de manejar y rápida para desplegar que soporta la seguridad en un entorno que puede incluir una gran variedad y una gran cantidad de clientes finales, desde servidores hasta equipos de escritorio, computadoras portátiles móviles conectadas a internet y equipos especializados como los mecanismos de punto de venta (POS), ATM y kioscos de autoservicio.

Tivoli Endpoint Manager for Security and Compliance puede reducir los costos y la complejidad de la administración de la tecnología informática ya que aumenta la agilidad, la velocidad de solución y la exactitud del negocio. Su bajo impacto sobre las operaciones de los clientes finales puede mejorar la productividad y mejorar la experiencia del usuario. Al aplicar en forma constante la política de cumplimiento donde sea que el cliente final se encuentre, Tivoli Endpoint Manager for Security and Compliance ayuda a reducir el riesgo y aumenta la visibilidad de la auditoría para un cumplimiento continuo.

Apuntando a las necesidades de seguridad a través de la organización

Tivoli Endpoint Manager for Security and Compliance apunta a los desafíos de seguridad relacionados con entornos distribuidos y de escritorio. Al brindar administración y seguridad para los clientes finales en una sola solución, ayuda a asegurar protección y cumplimiento continuos. Por ejemplo, puede reducir dramáticamente la brecha en las exposiciones de seguridad al aplicar parches de software en minutos. Y también puede ayudar a unir la brecha entre funciones tales como aquellas que establecen y ejecutan la estrategia y la política, aquellas que administran mecanismos en tiempo real y aquellas que generan informes sobre temas de cumplimiento y seguridad.

Entre las capacidades del Tivoli Endpoint Manager for Security and Compliance se encuentra su habilidad para:

- Brindar una visibilidad exacta, precisa y actualizada al último minuto y una aplicación continua de las configuraciones y los parches de seguridad.
- Centraliza la administración de la protección firewall y malware de terceros.
- Brinda de fábrica las mejores prácticas que cumplen las reglamentaciones de la Federal
- Implementation Guides (DISA STIG).
- Soporta el Security Content Automation Protocol (SCAP). Tivoli Endpoint Manager es el primer producto certificado por el National Institute of Standards and Technology (NIST) para la evaluación y la solución.
- Transmisión segura de las instrucciones de los clientes finales como se demuestra por medio de NIAP CCEVS EAL3 y FIPS 104-2, certificaciones de Nivel 2.
- Soporta el lenguaje estándar OVAL (Open Vulnerability and Assessment Language) para promover el contenido de seguridad abierto y disponible en forma pública.
- Recibe y actúa sobre las alertas de vulnerabilidad y riesgo de seguridad publicadas por el SANS Institute.
- Muestra la tendencia y el análisis de los cambios de configuración de seguridad por medio de informes avanzados.

Las capacidades adicionales que brindan todos los productos de la familia Tivoli Endpoint Manager, construidos con la tecnología BigFix, incluyen la habilidad para:

- Descubrir los clientes finales que las organizaciones pueden ignorar que están dentro de su entorno, hasta un 30 por ciento más en algunos casos.
- Brindar una sola consola de administración, configuración, funciones de seguridad y hallazgo, con una simplificación de las operaciones.
- Apuntar a acciones específicas hasta un tipo exacto de configuración de cliente final o de tipo de usuario y usar virtualmente cualquier propiedad de hardware o software para hacerlo.
- Emplear una infraestructura de administración unificada para coordinar la tecnología informática, la seguridad y las operaciones de escritorio y del servidor.
- Alcanzar los clientes finales sin importar su ubicación, tipo de conexión o estado con una administración integral para todos los sistemas operativos principales, aplicaciones de terceros y parches basados en la política.

Tivoli Endpoint Manager for Security and Compliance permite procesos automatizados de alto alcance que brindan control, visibilidad y velocidad para el efecto del cambio y el informe sobre el cumplimiento. Los ciclos de solución son cortos y rápidos, con temas de virus y malware abordados con capacidades de administración de parches rápidas.

Brindando una amplia gama de funciones de seguridad poderosas

Tivoli Endpoint Manager for Security and Compliance incluye las siguientes funciones clave y le otorga la habilidad de agregar fácilmente otras funciones deseadas según se necesiten, sin agregar infraestructura o costos de implementación.

Administración de parches

La administración de parches incluye capacidades integrales para la entrega de parches para Microsoft® Windows®, UNIX®, Linux® y Mac OS y para aplicaciones de otros proveedores como Adobe®, Mozilla, Apple y Java™ a los clientes finales distribuidos, sin importar su ubicación, tipo de conexión y estado. Un solo servidor de administración puede soportar hasta 250.000 clientes finales, acortando el tiempo para los parches sin pérdida para la funcionalidad del cliente final, aún sobre redes de trabajo distribuidas en forma global o de bajo ancho de banda. Los informes en tiempo real brindan información sobre qué fueron desplegados los parches, cuándo fueron desplegados y quiénes los desplegaron, como así también la confirmación automática de que los parches fueron aplicados para una solución de ciclo cerrado (closed-loop) completa para el proceso de parche.

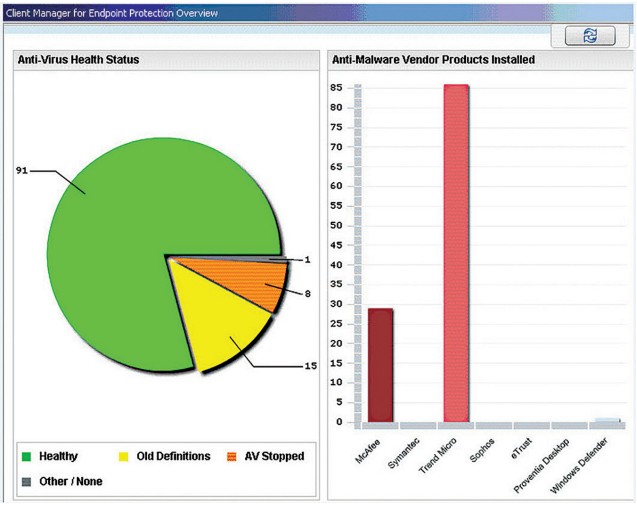
Administración de configuración de seguridad

Validados por el National Institute of Standards and Technology, las características de configuración de seguridad de la solución brindan una biblioteca integral de controles técnicos que pueden ayudarle a lograr el cumplimiento de seguridad al detectar y aplicar las configuraciones de seguridad. Las bibliotecas de políticas soportan la aplicación continua de configuraciónes base; reportan, solucionan y confirman la solución de clientes finales en no-cumplimiento en tiempo real y aseguran una visión verificada en tiempo real de todos los clientes finales.

Esta característica brinda una información significativa sobre la salud y la seguridad de los clientes finales sin importar la ubicación, el sistema operativo, la conexión (incluyendo las computadoras fijas o los equipos portátiles conectados en forma intermitente) o las aplicaciones instaladas. Ayuda a consolidar y unificar el cumplimiento del ciclo de vida, al reducir la configuración del cliente final y los tiempos de solución.

Administración de la vulnerabilidad

La administración de la vulnerabilidad le permite descubrir, evaluar y solucionar las vulnerabilidades antes de que los clientes finales se vean afectados. Esta característica evalúa los sistemas contra las definiciones de vulnerabilidad estandarizadas del lenguaje de seguridad de fuente abierta (OVAL, por su sigla en inglés) y los informes sobre las políticas de no cumplimiento en tiempo real. El resultado es una visibilidad mejorada y una plena integración en cada paso en el flujo de trabajo completo – descubrimiento-evaluación-solución-informe.



Tivoli Endpoint Manager for Security and Compliance brinda informes que ayudan a las organizaciones a visualizar los temas que impactan la efectividad de los esfuerzos de seguridad y cumplimiento.

El personal de tecnología informática puede identificar y eliminar, por medio de acciones automáticas o manuales, las conocidas vulnerabilidades a través de los clientes finales. Por medio del uso de una sola herramienta que descubre y soluciona vulnerabilidades, los administradores pueden aumentar la velocidad y la exactitud, acortando los ciclos de solución para el despliegue de los parches, las actualizaciones de software y las reparaciones de vulnerabilidad. Los administradores pueden extender la administración de la seguridad a los clientes móviles dentro o fuera de la red de trabajo, por medio de la configuración de alarmas para identificar rápidamente intrusos y dar paso a ubicarlos para su solución o eliminación.

Descubrimiento de activos

Con Tivoli Endpoint Manager for Security and Compliance, el descubrimiento de activos no es más un ejercicio puntual de "contar frijoles". Crea una conciencia de la situación dinámica acerca de las condiciones de cambio de la infraestructura. La habilidad de verificar la red de trabajo completa en forma frecuente para brindar una visibilidad y control dominantes que ayudan a asegurar que las organizaciones identifiquen rápidamente todos los dispositivos que pueden tener dirección IP, incluyendo máquinas virtuales, dispositivos de red y periféricos como impresoras, escáneres, routers e interruptores además de los clientes finales, con un impacto mínimo a la red de trabajo. Esta función ayuda a mantener la visibilidad dentro de todos los clientes finales de la empresa, incluyendo las computadoras portátiles que se conectan en forma itinerante más allá de la red de trabajo de la empresa.

Administración de protección de cliente final multiproveedores

Esta característica les otorga a los administradores un solo punto de control para administrar aplicaciones de seguridad para clientes finales de proveedores de terceros como Computer Associates, McAfee, Sophos, Symantec y Trend Micro. Con esta capacidad de administración centralizada, las organizaciones pueden mejorar la escalabilidad, la velocidad y la confiabilidad de sus soluciones de protección. Esta característica controla la salud del sistema para asegurar los terminales de seguridad de los clientes siempre se están ejecutando y que las firmas para control de virus están actualizadas. Además de brindar una visión unificada de tecnologías diferentes, facilita la migración de los clientes finales de una solución a otra con una eliminación y reinstalación de software con "un solo clic". La verificación de circuito cerrado asegura que las actualizaciones y otros cambios se han completado, incluyendo la verificación de internet habilitada para los clientes finales que están desconectados de la red de trabajo.

Auto cuarentena de la red de trabajo

El Tivoli Endpoint Manager for Security and Compliance evalúa en forma automática los clientes finales en contraste con las configuraciones de cumplimiento requeridas; y si el cliente final resulta estar en no cumplimiento, la solución puede configurar el cliente final para que quede en cuarentena en la red de trabajo hasta que se logre el cumplimiento. El servidor del Tivoli Endpoint Manager tiene acceso administrativo al cliente final pero todos los otros accesos se encuentran deshabilitados.

Servicio de reputación web y anti-malware (add-on opcional)

Una integración profunda con el Core Protection Module (CPM) de Trend Micro provee características que cuidan a los clientes finales de virus, troyanos, gusanos, espías, rootkits, nuevas variantes de malware y sitios web maliciosos por consulta en tiempo real, en la inteligencia de amenaza en la nube para prácticamente eliminar la necesidad de archivos de firma en los clientes finales. La tecnología de reputación web evita que los usuarios accedan a sitios web maliciosos, ya sea por medio de sus propias acciones o por medio de acciones automáticas, ocultas realizadas por el malware.

La familia del Tivoli Endpoint Manager

Usted puede consolidar aún más sus herramientas, reducir la cantidad de agentes terminales y disminuir sus costos administrativos extendiendo su inversión más allá del Tivoli Endpoint Manager for Security and Compliance al incluir otros componentes de la familia Tivoli Endpoint Management. Debido a que todas las funciones operan de una misma consola, de un mismo servidor de administración y un mismo agente terminal, agregar más servicios es tan solo un simple asunto de cambiar la clave de la licencia.

- **Tivoli Endpoint Manager for Power Management** — Esta opción permite la aplicación de políticas de conservación de energía a través de toda la organización, con la granulación necesaria para permitir la aplicación de políticas a una sola computadora.
- **Tivoli Endpoint Manager for Lifecycle Managemen** — Este enfoque integral y de gran alcance direcciona las convergencias actuales de las funciones de TI al proveer una visibilidad en tiempo real dentro del estado de los clientes finales del sistema y dar a los administradores una funcionalidad avanzada para administrar esos clientes finales.

Tivoli Endpoint Manager: Desarrollado con tecnología BigFix

El poder detrás de todas las funciones del Tivoli Endpoint Manager es un enfoque único de infraestructura simple que distribuye la toma de decisiones fuera de los clientes finales, y brinda beneficios extraordinarios a través de las familia entera de soluciones con características que incluyen:

- **Un agente inteligente** — El Tivoli Endpoint Manager utiliza un enfoque lider de la industria que ubica un agente inteligente en cada cliente final. Este agente único realiza funciones múltiples, incluyendo la autoevaluación continua y una política de aplicación, además con un impacto mínimo en el rendimiento del sistema. En contraste a las arquitecturas tradicionales cliente-servidor que esperan las instrucciones desde un punto de control central, este agente inicia las acciones de una manera inteligente, enviando mensajes continuos al servidor de administración central y enviando parches, configuraciones u otra información al cliente final cuando sea necesario cumplir una política importante. Como un resultado de la inteligencia y la velocidad del agente, el servidor de administración central siempre conoce el cumplimiento y el cambio de estado de los clientes finales, lo que permite informes de cumplimiento rápidos y actualizados.
- **Informes** — La consola de Tivoli Endpoint Manager orquestra un alto nivel de visibilidad que incluye informes y análisis continuos en tiempo real desde los agentes inteligentes en los clientes finales de la organización.
- **Capacidades de relevo** — La arquitectura liviana y escalable de Tivoli Endpoint Manager permite que cualquier agente sea configurado como un relevo entre otros agentes y la consola. Esta función de relevo permite el uso de servidores existentes o estaciones de trabajo para transferir paquetes a través de la red, reduciendo la necesidad de servidores.
- **Mensajes Fixlet de IBM** — El Fixlet Relevance Language es un lenguaje de comandos publicado que permite a los clientes, socios de negocios y desarrolladores crear políticas y servicios personalizados para los clientes finales administrados por las soluciones del Tivoli Endpoint Manager.

Extender el compromiso de Tivoli a la seguridad

El Tivoli Endpoint Manager for Security and Compliance es parte del portafolio integral de seguridad de IBM, para ayudar a focalizar los desafíos de seguridad a través de la organización. Al brindar soporte a las operaciones de tecnología informática inteligente, interconectada e instrumentada de un planeta más inteligente, las soluciones de seguridad IBM ayudan a asegurar la visibilidad en tiempo real, control centralizado y seguridad mejorada para toda la infraestructura de tecnología informática, incluyendo sus clientes finales distribuidos en forma global.

Una mirada a la familia Tivoli Endpoint Manager

Requerimientos del servidor:
- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

Requerimientos de la consola:
- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

Plataformas de soporte para el agente:
- Microsoft Windows, incluye X P, 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 más información

Para saber más acerca del Tivoli Endpoint Manager for Security and Compliance de IBM, contáctese con su representante de ventas de IBM o su Socio de negocios de IBM o visite: **ibm.com**/tivoli/endpoint

Acerca del software Tivoli de IBM

El software Tivoli de IBM ayuda a las organizaciones en forma eficiente y administra los recursos, tareas y procesos de tecnología informática en forma efectiva, de manera que cumplan los requerimientos de negocios cambiantes y brinda una administración del servicio tecnológico informático flexible y receptivo, mientras que ayuda a reducir los costos. El portafolio de Tivoli se extiende al software para seguridad, cumplimiento, almacenamiento, rendimiento, disponibilidad, configuración, operaciones y administración del ciclo de vida de la tecnología informática y está respaldado por la investigación, el soporte y los servicios de clase mundial de IBM.

IBM Latin America HQ
One Alhambra Plaza
Coral Gables, FL 33134
USA

Febrero de 2011

Tivoli software

TID14075-LAES-00