Kaspersky® Vulnerability & Patch Management

Reduzca la complejidad y refuerce la seguridad con herramientas de gestión de IT centralizadas

Las vulnerabilidades sin parches aplicados en las aplicaciones más populares plantean una amenaza importante para la seguridad de IT. Además, el problema no reside solo en las vulnerabilidades de día cero. La creciente complejidad de IT dificulta aún más la tarea de resolver a tiempo las brechas del software vulnerables: si no sabe exactamente qué tiene, ¿cómo puede protegerlo?

La gestión y la administración de actualizaciones de software y la supervisión constante de posibles vulnerabilidades es una de las tareas más importantes, pero también tediosas y laboriosas a las que se enfrentan los departamentos de IT. Mediante la centralización y la automatización de la seguridad esencial, las tareas de configuración y gestión, como la evaluación de vulnerabilidades, la distribución de parches y actualizaciones, la gestión del inventario y las implementaciones de aplicaciones, podrá ahorrar tiempo y optimizar la seguridad.

Visibilidad total

La visibilidad total de la red desde una única consola elimina las aproximaciones del administrador y proporciona control sobre cada aplicación y dispositivo (incluidos los invitados) que entran en la red. Este enfoque aumenta el control centralizado del acceso de los usuarios y los dispositivos a los datos y las aplicaciones de la empresa en función de las políticas y los requisitos de cumplimiento normativos de IT.

Mejore la seguridad

Aumente la eficacia de la seguridad de IT y reduzca las tareas rutinarias laboriosas mediante la aplicación de parches y actualizaciones automáticas. Kaspersky Vulnerability and Patch Management proporciona una visibilidad total, de forma que sepa exactamente las acciones que debe llevar a cabo para mantener la seguridad de su empresa. La automatización de todo el ciclo de evaluación de vulnerabilidades y gestión de parches, incluida la detección y priorización de vulnerabilidades, la descarga de parches y actualizaciones, la prueba y la distribución, la supervisión de resultados y la elaboración de informes, admite una mayor eficiencia y reduce significativamente la carga sobre los recursos.

Tareas de IT optimizadas

Kaspersky Vulnerability and Patch Management incluye un conjunto de herramientas de gestión de clientes que permite automatizar una amplia gama de funciones administrativas de IT. El aprovisionamiento automatizado de aplicaciones, el acceso remoto auditado y la solución de problemas ayudan a minimizar el tiempo y los recursos necesarios para configurar nuevas estaciones de trabajo e implementar nuevas aplicaciones.

Gestión central

Kaspersky Vulnerability and Patch Management es un componente gestionado de Kaspersky Security Center. El acceso a cada función y su gestión se realiza a través de esta consola central con el uso de interfaces y comandos coherentes e intuitivos para automatizar tareas rutinarias de IT.

Evaluación de las vulnerabilidades y gestión de parches

Supervisión de resultados y ejecución de informes

Kaspersky Vulnerability and Patch Management informa a los administradores de IT del estado de la instalación de los parches y les permite ejecutar informes sobre los análisis, buscar posibles puntos débiles, realizar un seguimiento de los cambios y obtener un mejor conocimiento de la seguridad de IT de la empresa, así como de cada dispositivo y sistema a lo largo de toda la red corporativa. También ofrece información sobre exploits existentes y amenazas conocidas, además de Common Vulnerabilities and Exposures (CVE).

Detección y priorización de vulnerabilidades

El análisis automático de vulnerabilidades permite la detección, priorización y corrección rápida de vulnerabilidades. El análisis de vulnerabilidades puede realizarse automáticamente o programarse según los requisitos del administrador. La gestión flexible de políticas facilita la distribución de software compatible y actualizado, así como la creación de excepciones.

Distribución ágil de software

Implemente o actualice el software de forma remota desde una única consola. Se pueden instalar de forma automática más de 150 aplicaciones populares, identificadas mediante Kaspersky Security Network, fuera del horario de trabajo si así lo desea. Reduzca el tráfico dirigido a oficinas remotas mediante la tecnología de multidifusión para la distribución de software local.

Descarga, prueba y distribución de parches y actualizaciones

Los parches y las actualizaciones pueden descargarse automáticamente a través de los servidores de Kaspersky Lab. Antes de su distribución, estos pueden probarse para garantizar que el rendimiento del sistema y la eficiencia de los empleados no se vean afectados. El administrador puede limitar la lista de parches aplicables en los endpoints para que solo incluya parches que hayan sido aprobados. La distribución de parches y aplicaciones se puede ejecutar de inmediato o posponerla a un momento más adecuado.

Cómo comprarlo

Kaspersky Vulnerability and Patch Management está disponible:

- Como parte de Kaspersky Total Security for Business
- Como parte de Kaspersky Endpoint Security for Business Advanced

También puede adquirirlo como complemento para Kaspersky Endpoint Security for Business Select o como solución específica independiente Kaspersky Vulnerability and Patch Management

Kaspersky Lab

Encuentre un partner próximo:
https://www.kasperskypartners.com/et.cfm?eid=global
Kaspersky for Business: **www.kaspersky.es/business**
True Cybersecurity: **www.kaspersky.es/true-cybersecurity**
Noticias de seguridad de IT: **www.business.kaspersky.com**
#truecybersecurity
#HuMachine

www.kaspersky.es

Herramientas de gestión de clientes

Analice su red para crear inventarios de hardware y software

La detección automática y el seguimiento del hardware y el software ofrecen a los administradores una visión detallada de todos los activos de la red corporativa. Los análisis automáticos de software permiten la rápida detección de aplicaciones obsoletas que pueden plantear un riesgo de seguridad si no se actualizan.

Aumento de la eficiencia con la solución remota de problemas

Para reducir los tiempos de respuesta, aumentar la eficiencia y optimizar la asistencia de los sitios remotos, Kaspersky Security Center utiliza el protocolo de escritorio remoto (RDP) y la tecnología de uso compartido de escritorios de Windows (utiliza en la asistencia remota de Windows). La conexión remota a los equipos cliente mediante el agente de red permite el acceso total del administrador a los datos y las aplicaciones instaladas en el cliente, incluso si los puertos TCP y UDP están cerrados.

Un mecanismo de autorización impide el acceso remoto no autorizado. En cuanto a la trazabilidad y la auditoría, todas las actividades realizadas durante una sesión de acceso remoto se registran.

Implementación cómoda de sistemas operativos

Kaspersky Vulnerability and Patch Management automatiza y centraliza la creación, el almacenamiento y la clonación de imágenes de sistemas protegidos, y permite la implementación del sistema operativo en nuevos equipos, así como las reinstalaciones. Todas las imágenes se guardan en un inventario especial, listas para su acceso durante la instalación.

La implementación de la imagen en la estación de trabajo cliente se puede realizar mediante servidores PXE (Preboot eXecution Environment; también en nuevos equipos sin sistema operativo), o a través de tareas de Kaspersky Vulnerability and Patch Management (para instalar imágenes de sistema operativo en los equipos cliente gestionados). Mediante el envío de señales Wake-on-LAN a los equipos, puede distribuir automáticamente las imágenes fuera del horario normal de oficina. La compatibilidad con UEFI también está incluida.