kaspersky BRING ON THE FUTURE

Kaspersky Embedded Systems Security

Seguridad todo en uno diseñada para sistemas embebidos

El mercado de los sistemas integrados crece a un ritmo constante y los cibercriminales están al acecho: en 2019 hubo un 28 % más de intentos de infección de sistemas de puntos de venta y cajeros automáticos que en 2018.

Estamos rodeados de sistemas integrados que influyen en todos los aspectos de nuestra vida diaria. Dependemos de ellos para todo, ya que se encuentran tanto en sistemas de puntos de venta y cajeros automáticos como en dispositivos médicos y de telecomunicaciones. Esto se traduce en más vectores de ataque que nunca.

Puesto que Windows 7 ha alcanzado recientemente su fin de soporte, las empresas no deben retrasar la actualización del sistema operativo de sus sistemas integrados, y es imperativo que tomen todas las medidas de protección adicional que sean necesarias. Cabe destacar que, aunque Windows XP se haya quedado obsoleto hace muchos años, sigue siendo el sistema operativo más común que utilizan los sistemas integrados en la actualidad. Esto es dejarles las puertas abiertas a los hackers.

Cada vez con mayor frecuencia, los cibercriminales centran sus ataques en estos dispositivos integrados, y esto tiene un gran potencial de ocasionar daños financieros. Por este motivo, las empresas deben ser más inteligentes que nunca y mantener sus sistemas y datos seguros. Kaspersky Embedded Systems Security se caracteriza por una potente inteligencia sobre amenazas, detección de malware en tiempo real, controles exhaustivos para los dispositivos y aplicaciones, y una gestión flexible. Es un sistema de seguridad todo en uno diseñado específicamente para los sistemas embebidos.

Aspectos destacados

Diseño eficaz incluso para hardware de gama baja

Kaspersky Embedded Systems Security se ha diseñado específicamente para que funcione de forma eficaz incluso con hardware de gama baja (desde 256 MB de RAM y CPU Pentium III) y software antiguo (desde Windows XP) sin riesgo de sobrecargar los sistemas. Los canales de comunicación débiles (desde tan solo 56 kbps) tampoco son un problema, incluso cuando un módem móvil es la única opción de comunicación y funciona solo en 2G debido a una señal deficiente.

Protección potente de la memoria

La potente tecnología de prevención de exploits supervisa los procesos críticos para evitar que los exploits ataquen las vulnerabilidades a las que no se han aplicado parches e incluso de día cero en aplicaciones y componentes del sistema. Esto es especialmente importante para la protección frente a ataques de ransomware masivos como WannaCry y ExPetr.

Optimización para Windows XP

La mayoría de los sistemas integrados se ejecuta aún en Windows® XP, para el que ya no se ofrece soporte. No obstante, Kaspersky Embedded Systems Security se ha optimizado para que funcione plenamente en la plataforma Windows XP, así como en Windows 7, Windows 8 y Windows 10.

Kaspersky Embedded Systems Security se compromete a proporcionar soporte total para Windows XP en un futuro próximo, lo que proporciona a las empresas el tiempo necesario para actualizarse gradualmente.

Cumplimiento

El exclusivo y completo conjunto de componentes de protección de Kaspersky Embedded Systems Security (antimalware, control de aplicaciones y dispositivos, gestión de firewalls, supervisión de la integridad de los archivos y auditoría de registros) identifica y bloquea las acciones maliciosas en contra de sus sistemas, y detecta los diferentes indicadores de una brecha de seguridad. Esto ayuda a las empresas a satisfacer los requisitos de cumplimiento de normativas como PCI/DSS, SWIFT, etc.

Cajeros automáticos

POS

Máquinas de venta de tickets

Cajas registradoras

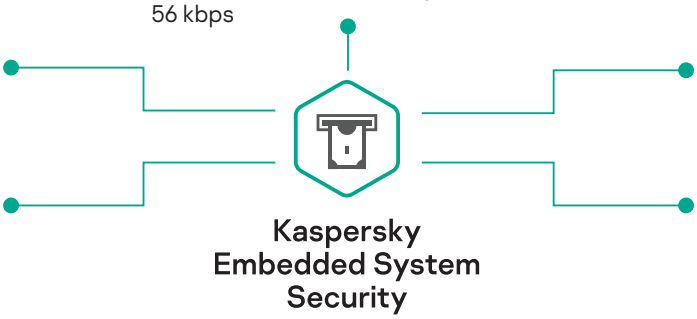
Ordenadores antiguos

Equipo médico

Requisitos optimizados del sistema
- RAM de 256 MB y más
- SO: Windows XP y posterior
- Ancho de banda de red: a partir de 56 kbps

Protección antimalware
- Opcional
- Tiempo real/a petición
- Prevención de exploits contra ransomware y otras amenazas

Protección de redes
- Gestión de firewalls
- Protección contra amenazas de red



Supervisión de la integridad del sistema
- Supervisión de la integridad de archivos
- Inspección de registros

Refuerzo del sistema
- Control de inicio de las aplicaciones
- Control de distribución de software
- Control de dispositivos

Funciones

Potente antimalware

Análisis y detección proactiva de amenazas con asistencia en la nube en combinación con tecnologías tradicionales para garantizar la protección contra amenazas conocidas, desconocidas y sofisticadas. Existe un componente antimalware que es opcional, aunque se lo recomendamos encarecidamente. Este se puede desactivar en escenarios con hardware de gama baja o canales de comunicación lentos.

Detección de malware en tiempo real con Kaspersky Security Network

Kaspersky Security Network (KSN) es la red de inteligencia contra amenazas global con asistencia en la nube de Kaspersky. Millones de nodos distribuidos globalmente alimentan constantemente nuestros sistemas con inteligencia contra amenazas procedente del mundo real, y garantizan una respuesta rápida incluso frente a las amenazas más recientes, emergentes o en evolución, incluidos ataques masivos.

Este flujo constante de nuevos datos sobre los intentos de ataques de malware y los comportamientos sospechosos crea veredictos instantáneos de los archivos, ofreciendo así protección en tiempo real frente a las amenazas más recientes.

Control de aplicaciones

La adopción de un escenario de denegación predeterminada, mediante el control de inicio de las aplicaciones, optimiza la resiliencia de su sistema para las fugas de datos. Al prohibir la ejecución de las aplicaciones que no se correspondan con determinados programas, servicios y componentes del sistema de confianza, puede bloquear automáticamente la mayoría de las formas de malware completamente. El control de distribución de software utiliza un enfoque de "instaladores fiables" que elimina la necesidad de invertir tiempo en el proceso manual y tedioso de marcado en lista blanca de los archivos creados o modificados durante una actualización o instalación de software. Solo tiene que especificar que el instalador es fiable y realizar la actualización de la forma habitual.

Supervisión y control de dispositivos

El control de dispositivos de Kaspersky le permite controlar los dispositivos de almacenamiento USB conectados físicamente al hardware de los sistemas o que intentan conectarse. Al impedir el acceso de los dispositivos no autorizados, se bloquea el punto de acceso común que suelen usar los cibercriminales como punto de partida a la hora de lanzar un ataque de malware.

Se supervisan y registran todas las conexiones de dispositivos USB para poder identificar el uso inapropiado de un dispositivo USB como el posible inicio de un ataque durante la investigación de incidentes y el proceso de respuesta.

Gestión del firewall de Windows

El firewall de Windows puede configurarse directamente desde Kaspersky Security Center, lo que permite una gestión de firewalls local a través de una única consola unificada. Esto es esencial cuando los sistemas integrados no pertenecen al dominio y la configuración del firewall de Windows no se puede llevar a cabo de forma centralizada.

Protección contra amenazas de red

La protección contra amenazas de red ayuda a prevenir las amenazas de la red, incluidos el análisis de puertos, los ataques de denegación del servicio y las saturaciones del búfer. Supervisa constantemente las actividades de la red y, si detecta un comportamiento sospechoso, ejecuta una respuesta predefinida.

Supervisión de la integridad de archivos*

Realiza el seguimiento de las acciones llevadas a cabo por los archivos y las carpetas especificados dentro de un marco determinado. Además, puede configurar que se realice el seguimiento de las modificaciones durante los periodos en los que la supervisión se interrumpe.

Inspección de registros*

Kaspersky Embedded Systems Security supervisa las posibles infracciones en relación con la protección mediante la inspección de los registros de eventos de Windows. La aplicación envía una notificación al administrador cuando detecta comportamientos anormales que pueden indicar un intento de ciberataque.

Integración con SIEM

Kaspersky Embedded Systems Security puede convertir los eventos de los registros de aplicación en formatos admitidos por el servidor syslog, de modo que estos se puedan transmitir y reconocer correctamente en todos los sistemas SIEM. Los eventos pueden exportarse directamente desde Kaspersky Embedded Systems Security a SIEM, o bien de forma centralizada a través de Kaspersky Security Center.

Gestión flexible

Las políticas de seguridad, las actualizaciones de firmas, los análisis antimalware y la recopilación de resultados se gestionan fácilmente mediante una única consola de gestión centralizada: Kaspersky Security Center. Además, los clientes que tengan una red local pueden gestionarlos a través de una consola de interfaz de usuario local o una línea de comandos, lo que resulta especialmente útil al trabajar en las redes segmentadas y aisladas típicas de los sistemas integrados.

---

* Requiere la licencia Kaspersky Embedded Systems Security Compliance Edition.

Noticias de ciberamenazas: www.viruslist.es
Noticias de seguridad de IT: business.kaspersky.com
Seguridad de IT para pymes:
https://www.kaspersky.es/small-to-medium-business-security
Seguridad de IT para grandes empresas: kaspersky.es/enterprise-security

www.kaspersky.es

Seguridad probada, independiente y transparente.
Nos comprometemos a construir un mundo más seguro en el que la tecnología nos mejore la vida. Por eso la protegemos, para que todas las personas del mundo puedan beneficiarse de las oportunidades que brinda la tecnología. Proteja su futuro gracias a la ciberseguridad.

Más información en kaspersky.es/transparency

Probada.
Transparente.
Independiente.