Kaspersky Embedded Systems Security

kaspersky

Desafíos de la seguridad integrada

1. **Software vulnerable y obsoleto.** Los ciclos de vida largos pueden indicar el uso de sistemas operativos y aplicaciones sin soporte, que contienen vulnerabilidades sin parches que pueden aprovecharse en cualquier momento.
2. **Actualizaciones de seguridad erráticas.** Incluso cuando el software todavía es compatible, puede que aún existan vacíos en los parches. Los problemas relacionados con la actualización de varios dispositivos dispersos geográficamente, la necesidad de tener que desconectarlos para su actualización (que produce una denegación de servicio temporal) y la necesidad de probar las actualizaciones antes de desplegarlas son factores que pueden contribuir a los retrasos en la implementación de parches.
3. **Continuidad de procesos.** Desconectar ciertos tipos de dispositivos (como equipamiento médico), incluso de forma temporal, puede ser muy problemático e incrementar aún más el tiempo de implementación de parches.
4. **Ubicaciones públicas.** Muchos dispositivos integrados funcionan en espacios públicos abiertos, lo que aumenta demasiado el riesgo de manipulación. Las defensas a nivel de red no pueden brindar protección contra la infección física directa del dispositivo.
5. **Naturaleza peligrosa de por sí.** Debido a que, en muchos casos, están asociados de manera directa a operaciones financieras y procesan información personal confidencial, los dispositivos integrados son objetivos muy atractivos para los ciberdelincuentes.

Seguridad todo en uno diseñada para los sistemas integrados (y más)

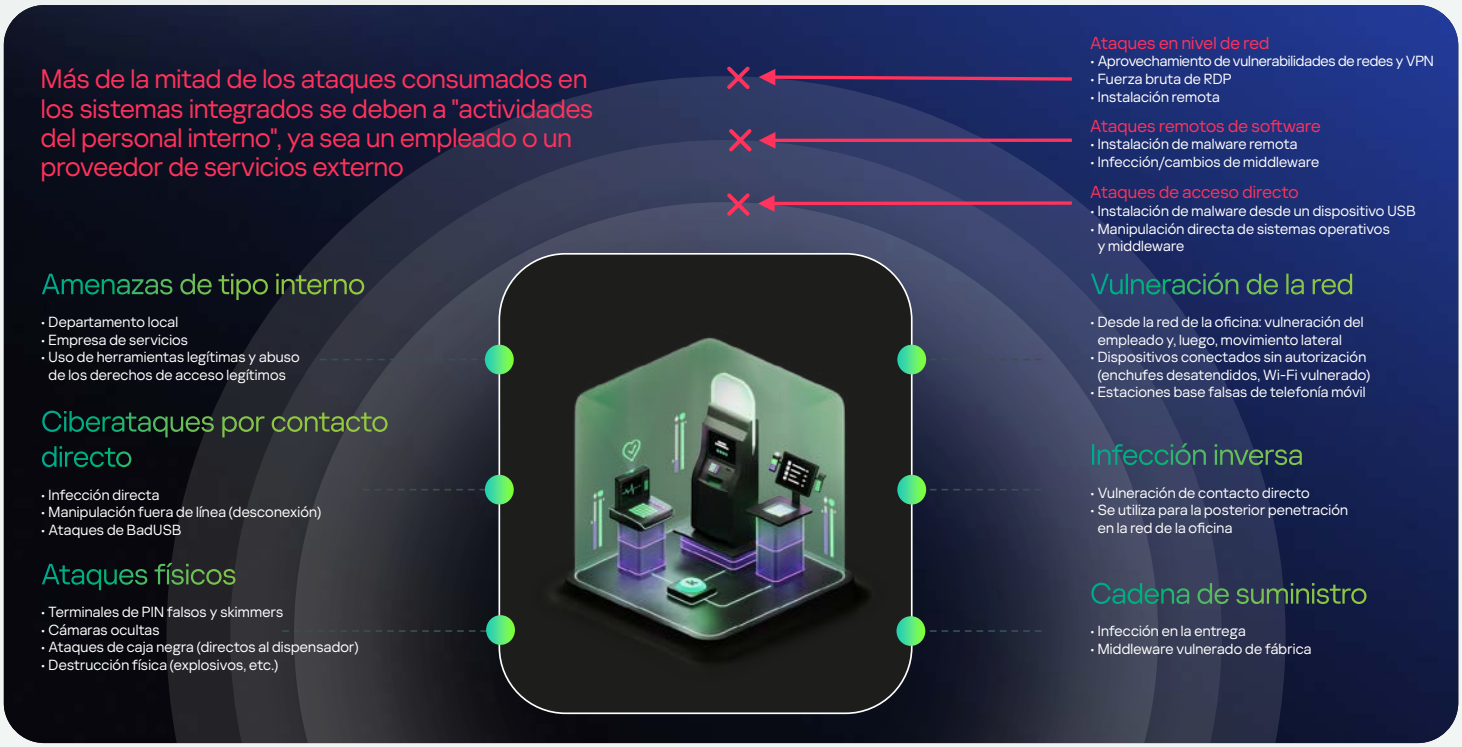
Los sistemas integrados son omnipresentes e interactuamos con ellos todo el tiempo. Dependemos de ellos para todo, desde los sistemas de punto de venta y los cajeros automáticos hasta los dispositivos médicos y las estaciones de servicio automatizadas. A medida que el mercado de sistemas integrados crece, los ciberdelincuentes tomarán nota y perfeccionarán sus tácticas, técnicas y procedimientos para adaptarse a las características de estos sistemas extensos.

Panorama de amenazas

Todo el tiempo surgen nuevos modelos de negocio criminales (por ejemplo, el malware como servicio) para reducir el nivel de conocimientos que necesitan los posibles atacantes. Las versiones más antiguas de Windows se siguen usando, a pesar de que ya no cuentan con soporte técnico (Windows XP sigue siendo el sistema operativo más usado en los dispositivos integrados). Millones de PC y dispositivos integrados siguen ejecutando sistemas operativos antiguos y vulnerables que, por alguna razón, ya no se actualizan. Esto es una invitación abierta a los hackers.

Mientras tanto, los sistemas integrados basados en Linux están ganando popularidad rápidamente y los ciberdelincuentes están al tanto de esto, por lo que adaptan sus técnicas y crean instrumentos completamente nuevos para adecuarse a las características de los sistemas integrados basados en Linux. Sobrestimar la seguridad inherente de Linux es muy peligroso y, si bien los atacantes han puesto su atención en los dispositivos integrados basados en Linux de manera reciente, están avanzando rápidamente. Tampoco es de gran ayuda que la oferta actual de soluciones de ciberseguridad para dispositivos integrados basados en Linux sea limitada, en comparación con las soluciones disponibles para Windows.

Las empresas deben ser más inteligentes que nunca para mantener seguros sus sistemas y datos. Al brindar inteligencia avanzada frente amenazas, detección de malware y prevención de exploits opcionales, y controles integrales de fortalecimiento de sistemas y administración flexible, Kaspersky Embedded Systems Security proporciona seguridad "todo en uno" diseñada de manera específica para los sistemas integrados. Proporciona un nivel único de protección para sistemas heredados que ya no reciben soporte técnico por parte de la mayoría de los proveedores de ciberseguridad. Ahora también ofrece el mismo nivel de protección para dispositivos más modernos que ejecutan el sistema operativo Linux.



Sistemas integrados: modelo de amenaza

Desafíos de la seguridad integrada

6 **Regulaciones estrictas.** Debido a la información financiera y de identificación personal que suelen procesar, muchos dispositivos integrados operan conforme a normas que exigen un enfoque de seguridad particularmente diligente.

7 **Amenazas de personal interno.** Según datos de Kaspersky, más de la mitad de los ataques consumados contra los sistemas integrados se deben al uso de "información privilegiada", ya sea por parte de un empleado o de un proveedor de servicios externo.

8 **Propagación de Linux.** Las plataformas integradas están ganando impulso rápidamente al ofrecer una mayor flexibilidad y permitir el uso de una gama más amplia de configuraciones. Los ciberdelincuentes están al tanto de esto y la selección de soluciones de seguridad especializadas y modernas es mucho más limitada en comparación con la disponibilidad de soluciones para Windows.

Aspectos destacados

Protección óptima para cualquier sistema integrado:
Kaspersky Embedded Systems Security ofrece protección de múltiples capas, que proporciona una seguridad óptima para dispositivos con diferentes niveles de potencia y escenarios de implementación. Esto incluye soporte para plataformas basadas en diferentes sistemas operativos, como Windows y Linux.

Protege sistemas heredados y nuevos
Kaspersky Embedded Systems Security está optimizado para ejecutarse con una funcionalidad completa con Windows XP, 7, 8, 10 y 11. Kaspersky seguirá brindando soporte a Windows XP en el futuro a fin de darles a los clientes el tiempo suficiente para actualizar cuando estén listos. Kaspersky Embedded Systems Security también es compatible con las últimas arquitecturas que ejecutan sistemas operativos tanto de Windows como de Linux.

Bajos recursos, altos niveles de protección
Kaspersky Embedded Systems Security se desarrolló para operar de manera efectiva incluso con hardware de baja gama.

Parte de un ecosistema unificado
Kaspersky Embedded Systems Security funciona como parte orgánica de una familia de soluciones, se administra a través de la misma consola junto con otros productos Kaspersky y se beneficia de una visibilidad única y un flujo de trabajo unificado.

Características clave

Controles de seguridad (fortalecimiento de sistemas). Estas tecnologías de fortalecimiento de sistema, compuestas por controles de aplicaciones, dispositivos y actualizaciones, permiten el uso exclusivo de aplicaciones, periféricos y fuentes de actualización de confianza. Esto evita que se lancen y ejecuten programas no autorizados, incluidos malware y aplicaciones que podrían utilizarse con fines maliciosos.

Antimalware opcional. Un nivel de seguridad opcional detecta las amenazas conocidas, desconocidas y avanzadas con una lógica de detección precisa, por medio de la inteligencia de amenazas local o de nube, así como el modelo heurístico y de aprendizaje, que se ejecutan en las instalaciones o en la nube. La tecnología anticifrado especializada garantiza que sus dispositivos no sufrirán los efectos del ransomware.

Prevención de exploits. Impide la explotación de vulnerabilidades en los componentes de sistemas de Windows en ejecución y en las aplicaciones de terceros, lo cual permite contrarrestar ataques más avanzados, como los diseñados para eludir el control de aplicaciones en modo de denegación predeterminada y aquellos que usan técnicas sin archivos.

Protección contra amenazas de red. Impide cualquier intrusión en el sistema operativo, protegiéndose del análisis de puertos y los ataques de fuerza bruta y de los ciberataques que aprovechan las vulnerabilidades relacionadas con la red para comprometer el dispositivo objetivo. Esto bloquea uno de los principales vectores de ataque dirigidos contra los sistemas integrados.

Monitoreo de la integridad y apoyo para el cumplimiento. El monitoreo de integridad de archivos y de acceso al registro[1] lleva a cabo un seguimiento de las acciones realizadas en el registro de claves, archivos y carpetas específicas, y puede bloquear cualquier cambio no deseado. Esto no solo permite detectar las intrusiones basadas en malware, sino también el acceso directo o las modificaciones fuera de línea a los recursos críticos. Estas contramedidas a menudo están recomendadas en el reglamento de protección de datos, por lo que habilitarlas permite mantener el cumplimiento.

Compatible con sistemas heredados y de baja potencia. Compatible incluso con sistemas integrados de baja potencia que funcionan con hardware obsoleto y sistemas operativos no compatibles, hasta Windows XP SP2. Puede continuar ejecutando dispositivos antiguos o PC heredadas de forma segura, hasta que tenga todo listo para actualizarlos.

Inspección de registros[1]. Las posibles violaciones de la protección se detectan a partir de la supervisión e inspección de los registros de eventos de Windows. La aplicación notifica al administrador cuando se detecta cualquier comportamiento anormal que pueda indicar un intento de ciberataque.

Administración flexible: local o en la nube. En función de sus necesidades, la seguridad de sus sistemas corporativos integrados puede administrarse desde un servidor de administración en las instalaciones o desde una consola SaaS de Kaspersky Security Center en la nube, junto con otras soluciones de Kaspersky. Mientras que la administración en instalaciones es útil cuando se necesita proteger la confidencialidad, la consola SaaS que mantiene el proveedor de la nube permite ahorrar tanto en CAPEX como en OPEX, lo que genera un inicio rápido de los procesos de trabajo seguros, con menos molestias de mantenimiento.

[1] solo para sistemas operativos de Windows

Administración de firewall. El firewall del sistema operativo puede configurarse directamente desde Kaspersky Security Center, lo que permite administrar el firewall local a través de una consola unificada. Esto es esencial cuando los sistemas integrados no se encuentran en dominio y la configuración de firewall de Windows/Linux no se puede llevar a cabo de forma centralizada. En el caso del sistema operativo Windows, se dispone de un firewall propietario a nivel de la aplicación, que reduce aún más la superficie de ataque mediante una administración más granular de las conexiones de red de las aplicaciones.

Tolerancia hacia mala conectividad. Ya que muchos tipos de dispositivos integrados suelen estar localizados en ubicaciones remotas, la mala conectividad (como resultado de una mala cobertura celular, interferencia con fuentes de radio cercanas, etc.) es frecuente. Kaspersky Embedded Systems Security se mantiene estable incluso con una mala conectividad a Internet, lo que preserva la integridad de la protección, incluso durante períodos prolongados sin conectividad.

Integración de detección y respuesta administradas: La solución se integra con el Centro de Operaciones de seguridad de Kaspersky para una supervisión ininterrumpida y una respuesta rápida. Esto permite la detección y la contención tempranas de ataques sofisticados a dispositivos integrados, y evita pérdidas financieras significativas para la empresa.

Servicios profesionales y soporte premium

El mantenimiento adecuado del ciclo de vida de una solución de seguridad lleva tiempo y, debido a las características de los dispositivos integrados que los diferencian de los endpoints normales, el mantenimiento de la seguridad de los sistemas integrados puede ser aún más complicado. Kaspersky Professional Services ofrece asistencia en cada etapa de este ciclo de vida, desde el despliegue y la actualización, la configuración y la optimización del rendimiento, hasta la migración a un hardware más actualizado. Nuestro soporte premium garantiza una resolución experta y prioritaria de incidentes, con un administrador técnico de cuenta dedicado, respaldado por una experiencia inigualable.

Productos y servicios relacionados

Kaspersky Threat Intelligence: una selección versátil de servicios que ofrece una visión integral de las ciberamenazas que tienen a su organización como objetivo. Combina fuentes de inteligencia, fuentes de datos de amenazas e investigación interna, con análisis llevados a cabo por nuevos expertos en seguridad.

Payment Systems Security Assessment: el análisis integral de sus cajeros automáticos y dispositivos de puntos de venta le brinda un panorama claro sobre los niveles de seguridad actuales, lo que permite mejorar la protección, optimizar su configuración y cerrar cualquier brecha existente.

Línea de productos de Kaspersky Next: Combina una protección excepcional para endpoints y controles de seguridad poderosos con la transparencia y la velocidad de EDR y las herramientas poderosas de XDR, en una línea de productos escalonada y flexible.

Sectores

- Servicios financieros
- Transporte y turismo (venta de boletos)
- Comercio
- Hostelería
- Salud
- Gobierno y no comercial
- Entretenimiento

Dispositivos

- Cajeros automáticos
- Máquinas de venta de tickets
- Surtidores de combustible
- Cajas
- Punto de venta
- Equipo médico
- Endpoints heredados
- Tragamonedas y máquinas recreativas

Industrias que utilizan dispositivos integrados

latam.kaspersky.com

Hemos pasado pruebas. Somos independientes. Somos transparentes. Estamos comprometidos con la creación de un mundo más seguro, donde la tecnología mejore nuestras vidas. Por eso que lo protegemos, para que cada quien, sin importar de dónde sea, tenga las infinitas oportunidades que nos brinda. Proteja su **futuro** gracias a la ciberseguridad.

Obtenga más información en kaspersky.com/about/transparency

Proven. Transparent. Independent.