Kaspersky Embedded Systems Security

kaspersky

Desafíos de la seguridad integrada

1. **Software vulnerable y obsoleto.** Los ciclos de vida largos pueden dar pie a la utilización de sistemas operativos y aplicaciones sin soporte, que contienen vulnerabilidades sin parches que están esperando ser aprovechadas.
2. **Actualizaciones de seguridad erráticas.** Incluso cuando sigue habiendo soporte para el software, es posible que existan brechas en los parches. Los problemas para actualizar distintos dispositivos dispersos geográficamente, el hecho de tener que desconectarlos para la actualización (lo que crea una denegación de servicio temporal) y la necesidad de probar las actualizaciones antes de implementarlas puede contribuir a demoras en los parches.
3. **Proceso de continuidad.** Quitar de servicio determinados dispositivos (por ejemplo, equipos médicos), incluso temporalmente, puede ser muy problemático y aumentar aún más el período de brecha en los parches.
4. **Lugares públicos.** Muchos dispositivos integrados funcionan en espacios públicos abiertos, lo que aumenta significativamente el riesgo de manipulación. Las defensas a nivel de red no pueden proteger contra la infección física directa del dispositivo.
5. **Carácter riesgoso por naturaleza.** Debido a que, con mucha frecuencia, están directamente relacionados con operaciones financieras y procesan información personal confidencial, los dispositivos integrados son objetivos especialmente atractivos para los ciberdelincuentes.

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

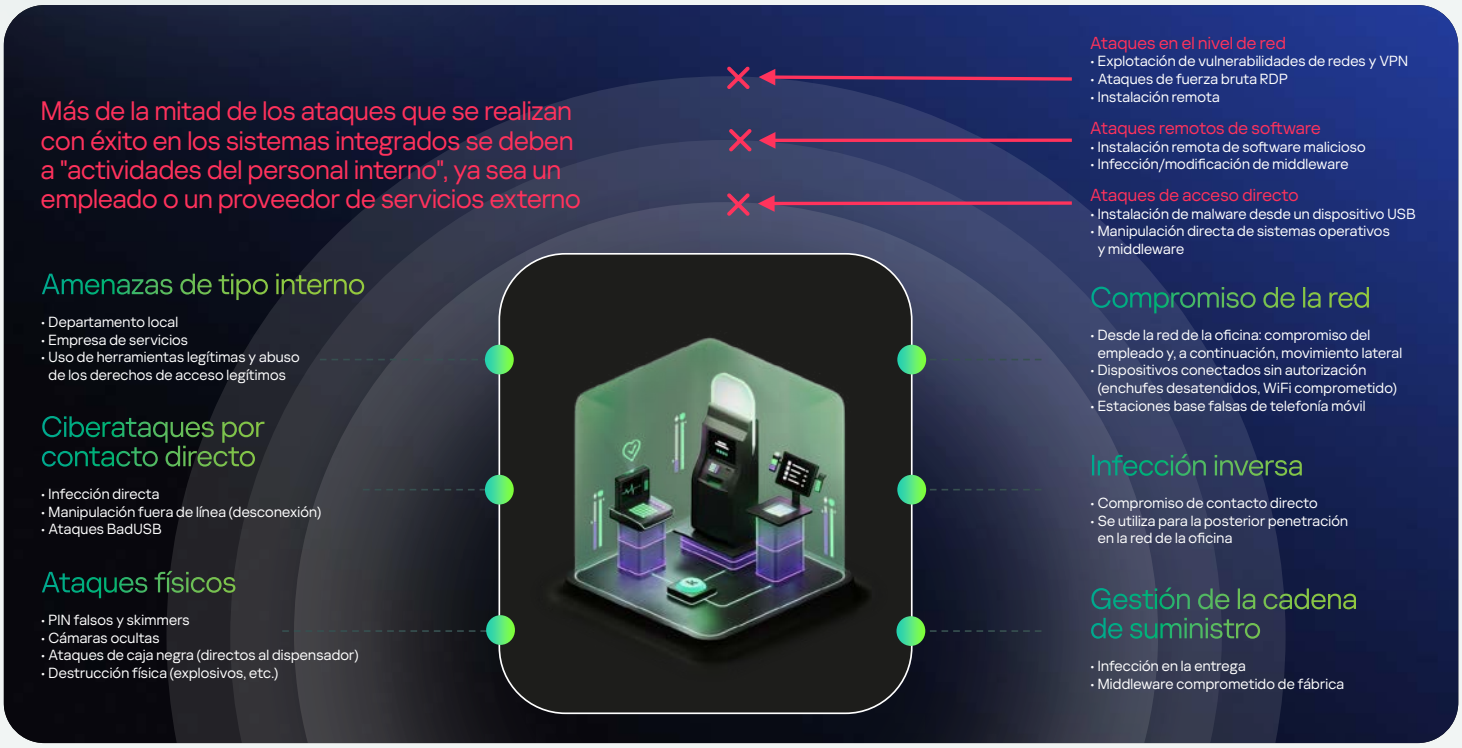
Los sistemas integrados están en todas partes e interactuamos con ellos todos los días. Dependemos de ellos para todo, desde los sistemas de punto de venta y los cajeros automáticos hasta los dispositivos médicos y las estaciones de servicio automatizadas. A medida que crece el mercado de sistemas integrados, los ciberdelincuentes hacen lo propio y refinan sus tácticas, técnicas y procedimientos para adaptarlos a los aspectos específicos de estos sistemas omnipresentes.

Panorama de amenazas

Siguen surgiendo nuevos modelos de negocio criminal, como el software malicioso como servicio, y esto reduce el nivel de conocimientos que necesitan los posibles atacantes. Aunque las versiones más antiguas de Windows han llegado a su fin de soporte, siguen en servicio. Y Windows XP sigue siendo el sistema operativo más usado en los dispositivos integrados. Millones de dispositivos integrados y PC siguen ejecutando sistemas operativos antiguos y vulnerables que, por alguna razón, no se actualizan. Esto es una invitación directa para los hackers.

Mientras tanto, los sistemas integrados Linux son cada vez más populares, y los cibercriminales toman nota de esto para adaptar sus técnicas y crear instrumentos completamente nuevos en función de los aspectos específicos de estos sistemas. Sobrestimar la seguridad inherente de Linux es peligroso. Y aunque el fenómeno de que los atacantes dirijan su atención a sistemas integrados Linux es relativamente reciente, están compensando el tiempo perdido. No ayuda que los productos de ciberseguridad actuales para dispositivos integrados Linux sean limitados si se los compara con los disponibles para Windows.

Las empresas deben ser más inteligentes que nunca para mantener la protección de sus sistemas y datos. Con una potente inteligencia frente a amenazas, detección de software malicioso y prevención de exploits opcionales, controles integrales de fortalecimiento de sistemas y administración flexible, Kaspersky Embedded Systems Security proporciona seguridad "todo en uno" diseñada de manera específica para sistemas integrados. Proporciona un nivel único de protección para sistemas heredados que ya no tienen soporte por parte de los principales proveedores de ciberseguridad, y 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 **Estrictas regulaciones.** Debido a la información financiera y de identificación personal que tienden a procesar, muchos dispositivos integrados operan conforme a normas que exigen un enfoque de seguridad particularmente diligente.

7 **Amenazas del personal interno.** Según los datos de Kaspersky, más de la mitad de los ataques que se realizan con éxito en los sistemas integrados se deben a "actividades del personal interno", ya sea un empleado o un proveedor de servicios externo.

8 **Propagación en Linux.** Las plataformas integradas están obteniendo protagonismo rápidamente, ya que ofrecen una mayor flexibilidad y permiten utilizar una gama más amplia de configuraciones. Los ciberdelincuentes están tomando nota de esto, y la opción de soluciones de seguridad modernas y especializadas es mucho más limitada que la disponible para Windows.

Aspectos destacados

Protección óptima para cualquier escenario de integración:
Kaspersky Embedded Systems Security ofrece protección multicapa para ofrecer seguridad óptima a 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 se ha optimizado para ejecutarse con todas sus funcionalidades en Windows XP, 7, 8, 10 y 11. Kaspersky seguirá brindando soporte para Windows XP durante el futuro próximo, para que los clientes tengan tiempo suficiente para llevar a cabo una actualización cuando llegue el momento. Kaspersky Embedded Systems Security también brinda soporte para las arquitecturas más recientes que ejecutan sistemas operativos Windows o Linux.

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

Parte de un ecosistema unificado
La seguridad de sistemas Kaspersky Embedded funciona como parte orgánica de una familia de soluciones, se gestiona 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 principales

Refuerzo del sistema (controles de seguridad). Estas tecnologías de fortalecimiento del sistema, compuestas por controles de aplicaciones, dispositivos y actualizaciones, permiten utilizar únicamente aplicaciones, periféricos y fuentes de actualización de confianza. Esto evita el inicio y la ejecución de programas no autorizados, incluido el software malicioso y aplicaciones que pueden utilizarse de forma maliciosa.

Antimalware opcional. Una capa de seguridad opcional detecta las amenazas conocidas, desconocidas y avanzadas con una lógica de detección precisa mediante inteligencia de amenazas local o basada en la nube, así como modelos heurísticos y de aprendizaje automático, que se ejecutan en las instalaciones o en la nube. La tecnología anticifrado especializada garantiza que tus dispositivos no sufrirán los efectos del ransomware.

Prevención de exploits. Evita el aprovechamiento de las vulnerabilidades en los componentes de sistemas Windows en ejecución y en las aplicaciones de terceros, lo cual ayuda a contrarrestar los ataques más avanzados, como los diseñados para eludir el control de las aplicaciones en modo de denegación predeterminada y aquellos que utilizan técnicas sin archivos.

Protección contra amenazas de red. Impide intrusiones en el sistema operativo para proteger contra ataques de análisis de puertos y fuerza bruta, y contra ciberataques que aprovechan las vulnerabilidades relacionadas con la red para comprometer el dispositivo objetivo. De este modo, bloqueas uno de los principales vectores de ataque dirigidos contra los sistemas integrados.

Supervisión de la integridad y respaldo para el cumplimiento. La supervisión[1] de la integridad de los archivos y del registro de accesos realiza un seguimiento de las acciones ejecutadas en el registro de claves, archivos y carpetas específicos y puede bloquear cualquier cambio no deseado. Esto no solo ayuda a detectar las intrusiones basadas en software malicioso, sino también el acceso directo o las modificaciones sin conexión a los recursos esenciales. Estas contramedidas a menudo se recomiendan específicamente en las normativas de protección de datos, por lo que activarlas ayuda a mantener el cumplimiento.

Soporte para sistemas de bajo consumo y heredados. Brinda soporte incluso para sistemas integrados de bajo consumo que funcionan con hardware obsoleto y sistemas operativos sin soporte, hasta Windows XP SP2. Puedes seguir utilizando dispositivos antiguos o equipos de sobremesa heredados de forma segura, hasta que llegue el momento de realizar una actualización.

Inspección de registros[1]. Las posibles infracciones 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 en las instalaciones o en la nube. En función de tus necesidades, la seguridad de los sistemas corporativos integrados puede manejarse desde un servidor de administración local o desde la consola SaaS de Kaspersky Security Center en la nube, junto con otras soluciones de Kaspersky. Aunque la opción local es útil cuando se necesita una estricta confidencialidad, la consola SaaS en la nube que ejecuta el proveedor ayuda a ahorrar tanto gastos de capital como operativos, lo que permite un inicio más rápido de los procesos de trabajo seguros y menos problemas de mantenimiento.

[1] solo para SO Windows

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

Tolerancia a la mala conectividad. Debido a que muchos tipos de dispositivos integrados suelen estar en una ubicación remota, la mala conectividad (como consecuencia de cobertura móvil deficiente, interferencia de fuentes de radio cercanas, etc.) no es inusual. Kaspersky Embedded System Security conserva la estabilidad incluso con banda ancha muy escasa, para mantener una protección fiable aun durante periodos prolongados sin conectividad.

Integración de detección y respuesta gestionadas: La solución se integra con el Centro de Operaciones de Seguridad de Kaspersky para una supervisión 24/7 y una respuesta rápida. Esto permite la detección temprana y la contención 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 requiere esfuerzo. Y, debido a los aspectos específicos de los dispositivos integrados que los diferencian de los endpoints regulares, el mantenimiento de la seguridad de sistemas integrados puede ser especialmente trabajoso. Kaspersky Professional Services ofrece asistencia en cada etapa de este ciclo de vida, desde la implementación y actualización, la configuración y la optimización de rendimiento, hasta la migración a hardware más reciente. Además, nuestro soporte premium garantiza la resolución priorizada y experta de incidentes, con un administrador técnico de cuenta exclusivo, con el respaldo de una experiencia inigualable.

Productos y servicios relacionados

Kaspersky Threat Intelligence: Una variedad de servicios versátil que permite acceder a un panorama integral de las ciberamenazas dirigidas a tu organización y combina fuentes de inteligencia, orígenes de datos de amenazas e investigaciones internas, analizadas por nuestros expertos en seguridad.

Evaluación de la seguridad de los sistemas de pago: El análisis integral de tus cajeros automáticos y dispositivos PoS te brinda una idea clara de los niveles de seguridad actuales y te permite mejorar aún más la seguridad, optimizar su configuración y cerrar todas las brechas de seguridad.

Línea de productos Kaspersky Next: Combina una protección excepcional de los endpoints y potentes controles de seguridad con la transparencia y velocidad de EDR y la visibilidad y potentes herramientas de XDR, en una línea de productos flexible por niveles.

Industrias

- Servicios financieros
- Transporte y turismo (venta de billetes)
- Minoristas
- Hospitality
- Asistencia sanitaria
- Entidades gubernamentales y no comerciales
- Entretenimiento

Dispositivos

- Cajeros automáticos
- Máquinas de venta de tickets
- Surtidores de combustible
- Puntos de pago
- Punto de venta
- Equipo médico
- Terminales heredados
- Tragaperras y máquinas arcade

Industrias que utilizan dispositivos integrados

www.kaspersky.com

Seguridad probada. Somos independientes. Somos transparentes. Nos comprometemos a construir un mundo más seguro en el que la tecnología mejore nuestras vidas. Por eso la protegemos, para que todas las personas del mundo puedan beneficiarse de las oportunidades que brinda la tecnología. Protege tu **futuro** gracias a la ciberseguridad.

Más información en kaspersky.es/about/transparency

Proven. Transparent. Independent.