Kaspersky Embedded Systems Security

kaspersky

All-in-one security designed for embedded systems (and more)

Embedded systems are all around us, and we interact with them every day. We depend on them for everything from PoS systems and ATMs to medical devices and automated fueling stations. As the embedded systems market grows, cybercriminals follow, honing their tactics, techniques and procedures to suit the specifics of these widespread systems.

Embedded security challenges

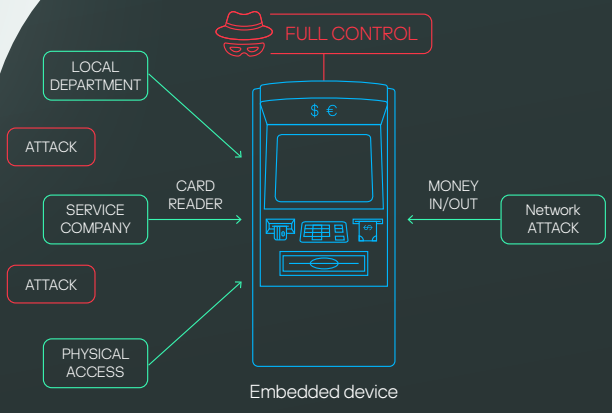
1. **Obsolete, vulnerable software.** Long lifecycles can mean running out-of-support for operating systems and apps which contain unpatched vulnerabilities just waiting to be exploited.
2. **Erratic security updates.** Even when the software is still supported, there can be patching gaps. Problems around updating multiple geographically dispersed devices, having to take them offline to be updated (thereby creating a temporary Denial of Service), and the need to test updates before deploying them can all contribute to patching delays.
3. **Process continuity.** Taking certain types of devices out of service even temporarily – such as medical equipment, for example – can be highly problematic, further increasing the patching gap timeframe.
4. **Public locations.** Many embedded devices operate in open public spaces, which significantly increases the risk of tampering. Network-level defenses can't protect against direct physical infection of the device.
5. **Inherently risky nature.** Because they're so often directly associated with financial operations, and process sensitive personal information, embedded devices are especially attractive targets for cybercriminals.

Threat landscape

New criminal business models like Malware-as-a-Service continue to emerge, lowering the skills bar for would-be attackers. While older Windows versions have long reached end of support, they remain in service (Windows XP is still the most widespread OS used in embedded devices). Millions of embedded devices and PCs continue to run old, vulnerable OSs that for whatever reason, aren't upgraded. This is an open invitation to hackers.

In the meantime, Linux-based embedded systems are rapidly gaining in popularity, and cybercriminals are taking note, adapting their techniques and creating entirely new instruments to the specifics of Linux-based embedded systems. Overestimating Linux's inherent security is dangerous – and while attackers have only been turning their attention to Linux-based embedded devices relatively recently, they're making up for lost time. It doesn't help that current cybersecurity offerings for Linux-based embedded devices are limited compared to what's available for Windows.

Businesses need to be smarter than ever to keep their systems and data safe. Featuring powerful threat intelligence, opt-in malware detection and exploit prevention, comprehensive system hardening controls and flexible management, Kaspersky Embedded Systems Security is all-in-one security designed specifically for embedded systems. It provides a unique level of protection for legacy systems that are no longer supported by most cybersecurity vendors, and now also offers the same level of protection for more modern devices running the Linux OS.



Over half of all successful attacks on embedded systems involve 'insider activity' - by an employee or a third-party service provider

Physical-level attacks

- Black-box attacks
- PIN pad changes/skimmers
- Hidden cameras
- Explosions

Software-level attacks

- Remote/local malware installation
- Memory sniffers/OS attacks
- Middleware infection/changes

Network-level attacks

- VPN vulnerabillities
- Bruteforcing of RDP
- RCE-allowing network exploits
- Remote installation

Embedded systems: typical attack vectors

Embedded security challenges

6 **Strict regulations.** Due to the financial and personally identifiable information they tend to process, many embedded devices operate under regulations mandating a particularly diligent approach to security.

7 **Insider threats.** According to Kaspersky data, over 50% of all successful attacks on embedded systems involve 'insider activity' – either by an employee or a third- party service provider.

8 **Linux spreading.** Embedded platforms are rapidly gaining momentum, offering greater flexibility and allowing use of a broader range of configurations. Cybercriminals are taking note, and the choice of modern, specialized security solutions is much more limited compared to what's available for Windows.

Highlights

Optimum protection for any embedded scenario:
Kaspersky Embedded Systems Security offers multilayered protection to deliver optimum security for devices with differing power levels and implementation scenarios. This includes support for platforms based on different Operating Systems such as Windows and Linux

Protects legacy as well as new systems
Kaspersky Embedded Systems Security has been optimized to run with full functionally on Windows XP, 7, 8, 10, and 11. Kaspersky will continue to support Windows XP for the foreseeable future, giving customers enough time to upgrade when they're ready. Kaspersky Embedded Systems Security also supports the latest architectures running either Windows or Linux OS.

Low resources, high levels of protection
Kaspersky Embedded Systems Security has been built to operate effectively even on low-end hardware.

ATM & PoS attacks increase
According to Kaspersky research data, the number of attacks against ATMs and PoS systems grew significantly during 2022, and continues growing, with 19% growth compared to 2020 and 4% up on 2021.

Key features

System hardening (security controls). Comprising application, device and update controls, these system hardening technologies allow the use of only trusted applications, peripherals and update sources. This prevents unauthorized programs from launching and running, including malware and apps which could be used maliciously.

Opt-in anti-malware. An opt-in security layer detects known, unknown and advanced threats with precise detection logic, using local or cloud-based threat intelligence as well as heuristics and machine-learning models, running on-prem or in the cloud.

Exploit prevention[1]. Prevents the exploitation of vulnerabilities in running Windows system components and third-party apps, helping to counter more advanced attacks, including attacks designed to sidestep Default Deny mode application control, and those using fileless techniques.

Network threat protection. Prevents any intrusion into the operating system, protecting against port scanning and brute force attacks, and cyberattacks exploiting network-related vulnerabilities to compromise the targeted device. By doing this, you're blocking one of the principal attack vectors directed against embedded systems.

Integrity monitoring & compliance support. File integrity and registry access monitoring superscript track actions performed on specified registry keys, files and folders, and can block any unwanted changes. This helps to detect not only malware-based intrusions, but also direct access/offline modifications to critical resources. These countermeasures are often specifically recommended in data protection regulations – enabling them helps maintain compliance.

Supports underpowered & legacy systems. Supports even low-powered embedded systems running on outdated hardware and unsupported operating systems, right down to Windows XP SP2. You can continue running older devices or legacy desktops securely until you're ready to upgrade.

Log Inspection[1]. Possible protection violations are detected based on monitoring and inspecting Windows event logs. The application notifies the administrator when it detects any abnormal behavior that may indicate an attempted cyberattack.

Flexible management – on-prem or in the cloud. Depending on your needs, your corporate embedded systems security can be managed either from an on-premise management server or from the Kaspersky Security Center SaaS cloud console, alongside other Kaspersky solutions. While on-prem management is useful where strict privacy is needed, the vendor-run cloud SaaS console helps save on both CAPEX and OPEX, enabling a fast-start for secure working processes and requiring less maintenance hassle.

[1] for Windows OS only

Firewall management. Operating System's Firewall can be configured directly from Kaspersky Security Center, giving you the convenience of local firewall management through a single unified console. This is essential when embedded systems aren't in domain and Windows/Linux firewall settings can't be configured centrally.

Poor connectivity tolerance. Because many kinds of embedded devices are often remotely located, poor connectivity – as a result of poor cellular coverage, interference from close radio sources, etc. – is not unusual. Kaspersky Embedded System Security remains stable even at very low bandwidth, maintaining reliable protection even during prolonged periods of no connectivity.

Professional Services & Premium Support

Proper maintenance of a security solution's lifecycle takes effort, and due to the specifics of embedded devices which differentiates them from regular endpoints, maintaining embedded systems security can be especially laborious. Kaspersky Professional Services offers assistance with every stage of this lifecycle, from deployment and updating, configuration and performance optimization, to migration to newer hardware. And our Premium Support guarantees prioritized, expert resolution of incidents, with a dedicated technical account manager backed-up by unmatched expertise.

Related products and services

Kaspersky Threat Intelligence: A versatile selection of services that delivers a comprehensive view of cyberthreats targeting your organization, combining intelligence sources, threat data feeds, and in-house research, analyzed by our security experts.

Payment Systems Security Assessment: Comprehensive analysis of your ATMs and POS devices gives you a clear picture of your current security levels, enabling you to further boost your security, optimize its configuration, and close any security gaps.

Kaspersky Endpoint Security for Business: Globally renowned endpoint protection platform that secures your endpoints, servers, workstations and mobiles with the most tested, most awarded security. All managed via a single console.

Industries

- Financial Services
- Transportation & Tourism (Ticketing)
- Retail
- Restaurants & Hospitality
- Healthcare
- Government & Non-commercial
- Entertainment

Devices

- ATMs
- Ticketing machines
- Fuel dispensers
- Checkouts
- Point-of-Sale
- Medical equipment
- Legacy endpoints
- Slot & arcade machines

Industries using embedded devices

Cyber Threats News: securelist.com
Kaspersky Technologies: kaspersky.com/technowiki
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer **tomorrow**.

Learn more at kaspersky.com/about/transparency

Proven. Transparent. Independent.