kaspersky BRING ON THE FUTURE

Kaspersky Embedded System Security

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

Embedded systems are all around us and impact on every part of our daily lives. 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, improving their tactics, techniques and procedures to better suit such devices' specifics. New criminal business models like Malware-as-a-Service emerge to lower the skills bar for would-be attackers. While older Windows versions have long reached their end of support, they still remain in service, Windows XP still being the most widespread OS used in embedded devices. And it is not about only embedded devices; there are still millions of PCs running the old and vulnerable OS, avoiding being upgraded for different reasons. This is an open invitation to hackers.

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 – and offers unique level for protection for legacy systems that are no longer supported by most cybersecurity vendors.

Key security challenges

Embedded devices, though very similar to regular computers, present a number of specific challenges. Some of these are common to all embedded devices, while others are characteristic of particular devices types. These challenges include:

Obsolete, vulnerable software. Long lifecycles can mean running out-of-support operating systems and apps, containing unpatched vulnerabilities that can be exploited.

Irregular security updates. Even where the software's supported, there can be patching gaps. Problems with updating multiple geographically-dispersed devices or taking them offline for update purposes (and thus creating a temporary Denial of Service), and the need to test the updates before deploying them in production can all contribute to patching delays.

Process continuity. Taking certain types of device – such as medical equipment – out of service temporarily for updating can be especially undesirable, further increasing the patching gap timeframe.

Public space placement. Many embedded devices operate in open public spaces, which greatly increases the risk of tampering. Network-level defenses can't protect against the direct physical infection of the device.

Inherently risky context. Embedded devices are particularly attractive to cybercriminals, as so many are directly involved in financial operations and/or process sensitive personal information.

Subject to strict regulations. Because of the financial and personally identifiable information they may process, many embedded devices operate under regulations mandating a particularly diligent approach to security.

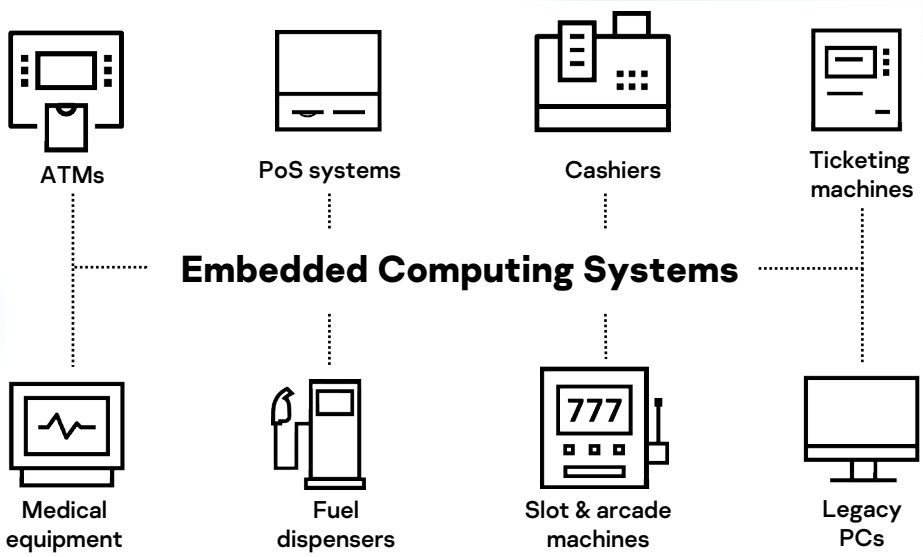
Insider threats. According to Kaspersky data, over 50% of all successful attacks on embedded systems involve 'insider activity' – by an employee or a 3rd party service provider

Highlights

Best protection for any embedded scenario:
Kaspersky Embedded Systems Security is a true multi-layered solution, offering an optimal selection of protective layers to provide the best security level possible for devices of differing power and with different implementation scenarios.

Older systems receive the most up-to-date protection
Kaspersky Embedded Systems Security has been optimized to run with full functionally on the Windows XP platform as well as on the Windows 7, 8, 10 and even the newest Windows 11 families. Kaspersky solution is committed to providing total support for the Windows XP family for the foreseeable future, giving customers enough time to upgrade when appropriate.

Low resources but high security levels
Kaspersky Embedded Systems Security has been built specifically to operate effectively even on low-end hardware.



Key features

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
Prevents the exploitation of vulnerabilities in running system components and 3rd party apps, helping counter more advanced attacks - including those designed to sidestep Default Deny mode application control, and those using fileless techniques.

Security controls
Comprising Application, Device and Updating controls, these system hardening technologies allow the use of only trusted applications, peripherals and update sources. This prevents the loading and launch of programs the device should not be running- including malware and apps which could be used maliciously

Network threat protection
Prevents any intrusion into the operating system, protecting against cyber-attackers who use port scanning and brute force attacks, and those who exploit networkrelated vulnerabilities to compromise the targeted device. By doing this, you're blocking one of the principal attack vectors directed against embedded computing systems.

Integrity monitoring & compliance support[1]
File integrity and registry access monitoring track actions performed on specified registry keys, files and folders, and can block any undesired changes. This helps 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 - so enabling them helps maintain compliance.

Underpowered & legacy systems support
The solution supports even low-powered embedded systems running on out-dated hardware and unsupported operating systems, right down to Windows XP SP2. You can continue running older devices or legacy desktops securely until such time as upgrading becomes practicable.

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

On-prem or cloud management
Depending on your business needs, your corporate embedded systems security can be managed either from an on premises management server or from a cloud SaaS Kaspersky Security Center 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, allowing a faster start for secure working processes and less maintenance hassle

Firewall management
Windows 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 firewall settings can't be configured centrally

[1] Available only in Kaspersky Embedded Systems Security Compliance Edition

Request a call
Still feel you need more information?
Request a call now!

Buy via a trusted partner
Feel like you're ready to buy?
Find a reseller in your region!

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

Known more at kaspersky.com/transparency

Proven. Transparent. Independent.