kaspersky BRING ON THE FUTURE

Kaspersky Embedded Systems Security

All-in-one security designed for embedded systems

The embedded systems market is growing steadily, and cybercriminals are taking note – there were 28% more infection attempts on ATM/PoS systems in 2019 than in 2018.

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 telecommunications. This means more attack vectors than ever before.

With Windows 7 having recently reached its end-of-support, companies should not delay updating the OS in their embedded systems, and must take any additional protection measures necessary. It's worth noting that even though Windows XP became obsolete many years ago, it's still the most common operating system used in embedded systems today. This is an open invitation to hackers.

Cybercriminals are increasingly turning their attention to these embedded devices as a focus of their attacks, with a potential for considerable financial damage. Given this, businesses need to be smarter than ever to keep their systems and data safe. Featuring powerful threat intelligence, real-time malware detection, comprehensive application and device controls and flexible management, Kaspersky Embedded Systems Security is all-in-one security designed specifically for embedded systems.

Highlights

Efficient design even for low-end hardware

Kaspersky Embedded Systems Security has been built specifically to operate effectively even on low-end hardware (from 256MB of RAM, and Pentium III CPU) and old software (from Windows XP), with no risk of systems overload. Weak communication channels (from as low as 56kbps) are also not a problem, even when a mobile modem is the only communications option and works on 2G only due to a poor signal.

Powerful memory protection

Powerful exploit prevention technology watches over critical processes to prevent exploits from attacking unpatched and even zero-day vulnerabilities in applications and system components. This is especially important for protection against widespread ransomware attacks such as WannaCry and ExPetr.

Windows XP-optimized

Most embedded systems still run on the unsupported Windows® XP OS. Kaspersky Embedded Systems Security has been optimized to run with full functionality on the Windows XP platform as well as on Windows 7, Windows 8 and Windows 10.

Kaspersky Embedded Systems Security is committed to providing 100% support for Windows XP for the foreseeable future, giving businesses time to upgrade gradually.

Compliance

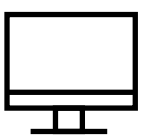
The unique, comprehensive set of protection components in Kaspersky Embedded Systems Security – anti-malware, application and device control, firewall management, File Integrity Monitoring and Log Audit – identifies and blocks malicious actions against your systems and detects various indicators of a security breach. This helps businesses to meet the compliance requirements of regulations such as PCI/DSS, SWIFT, etc.

ATMs

POS

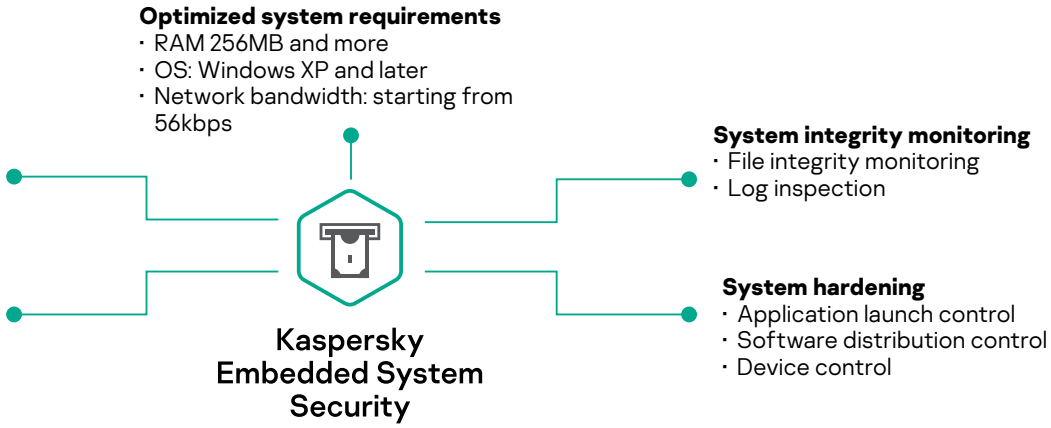
Ticketing machines

Cashier



Old PCs

Medical equipment



Features

Powerful anti-malware

Proactive, cloud-assisted threat detection and analysis work with traditional technologies to provide protection from known, unknown and advanced threats. An optional (but strongly recommended) anti-malware component can be disabled in scenarios with low-end hardware or slow communications channels.

Real-time malware detection with Kaspersky Security Network

Kaspersky Security Network (KSN) is Kaspersky's cloud-assisted, global threat intelligence network. Millions of globally distributed nodes constantly feed real-world threat intelligence to our systems, ensuring a rapid response to even the newest, emerging and evolving threats, including mass attacks.

This constant flow of new data about attempted malware attacks and suspicious behavior creates instant file verdicts, delivering real-time protection against the latest threats.

Application control

Adopting a Default Deny scenario using Application Launch Control optimizes your system's resilience to data breaches. By prohibiting the running of any applications other than specified programs, services, and trusted system components, you can automatically block most forms of malware completely. Software distribution control uses a 'trusted installer' approach, eliminating the need for time-consuming, manual whitelisting of files created or changed during a software update or installation. Just specify the installer as trusted and carry out the update in the usual way.

Device monitoring and control

Kaspersky's Device Control lets you control USB storage devices connected or trying to connect physically to systems hardware. Preventing access by unauthorized devices means you block a common point of entry used by cybercriminals as the first step in a malware attack.

All USB device connections are monitored and logged so that inappropriate USB use can be identified as a possible attack source during the incident investigation and response process.

Windows 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 do not belong to a domain and Windows firewall settings can't be configured centrally.

Network threat protection

Network threat protection helps to prevent network threats, including port scanning, denial-of-service attacks and buffer-overruns. It constantly monitors network activities and, if it detects suspicious behavior, runs a pre-defined response.

File integrity monitoring*

Tracks actions performed on specified files and folders within scope. You can also configure changes to be tracked during periods when monitoring is interrupted.

Log inspection*

Kaspersky Embedded Systems Security monitors possible protection violations based on inspecting Windows event logs. The application notifies the administrator when it detects abnormal behavior that may indicate an attempted cyberattack.

SIEM integration

Kaspersky Embedded Systems Security can convert events in application logs into formats supported by the syslog server, so these can be transmitted to, and successfully recognized by, all SIEM systems. Events can be exported directly from Kaspersky Embedded System Security to SIEM or centrally via Kaspersky Security Center.

Flexible management

Security policies, signature updates, anti-malware scans and results collection are easily managed through a single centralized management console – Kaspersky Security Center. In addition, clients in a local network can be managed through a local GUI console or command line – particularly useful when working in the isolated, segmented networks typical of embedded systems.

* Requires Kaspersky Embedded Systems Security Compliance Edition license

Cyber Threats News: www.securelist.com
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.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.