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.While the number of attacked devices in the first 10 months of 2019 was slightly lower than the previous year, the number of ATM/POS infections had already exceeded those for all of 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.

As support for Windows 7 winds down – ending on 12 January 2020 – there is still time for companies to update the OS in their embedded systems, and take any additional protection measures necessary. However, older Windows XP - still an extremely popular OS for embedded systems – is still being overlooked, even though support for that OS ended in 2016. This is an open invitation to hackers.

Cybercriminals are increasingly turning their attention to these embedded devices as a door into the corporate network, and 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 for even Low-End Hardware

Kaspersky Embedded Systems Security has been built specifically to operate effectively even on low-end hardware. Efficient design delivers powerful security with no risk of systems overload. Requirements start from only 256MB RAM for the Windows XP family, with around 50MB space required on the system hard drive when operating in 'Default Deny only' mode.

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

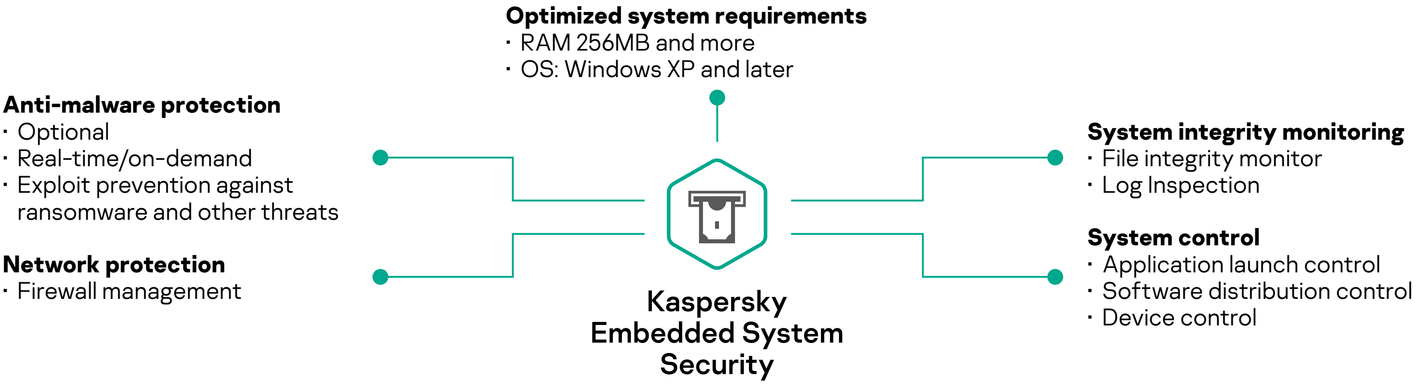
Most embedded systems still run on the now-unsupported Windows® XP OS. Kaspersky Embedded Systems Security has been optimized to run with full functionally on the Windows XP platform as well as the Windows 7, Windows 8 and Windows 10 families.

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

Compliance

The unique, comprehensive set of protection components (anti-malware, application and device control, firewall management, File Integrity Monitoring and log audit) within Kaspersky Embedded Systems Security identifies and blocks malicious actions against your system, and detects different indicators of a security breach, in compliance with regulations (including PCI/DSS, SWIFT, etc.).

ATMs **POS** **Ticketing machines** **Cashier** **Old PCs** **Medical equipment**



Optimized system requirements
- RAM 256MB and more
- OS: Windows XP and later

Anti-malware protection
- Optional
- Real-time/on-demand
- Exploit prevention against ransomware and other threats

Network protection
- Firewall management

System integrity monitoring
- File integrity monitor
- Log Inspection

System control
- Application launch control
- Software distribution control
- Device control

Kaspersky Embedded System Security

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 (KSN)

KSN is Kaspersky cloud-assisted, global threat intelligence network. Millions of globally distributed nodes constantly feed real-world threat intelligence to our systems, ensuring 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

Device Control from Kaspersky gives you the ability to 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 are not in domain and Windows firewall settings can't be configured centrally.

File Integrity Monitoring*

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

Log Audit*

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

Kaspersky Embedded Systems Security can be managed from the command line, local GUI, or the centralized policy-based management via Kaspersky Security Center. 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 any local console – 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 tommorow.

Know more at kaspersky.com/transparency

Proven. Transparent. Independent.