



Kaspersky[®]
Embedded Systems
Security

All-in-one security designed for embedded systems

The embedded systems market is growing steadily, with its global value expected to hit \$114-billion by 2024 – up from \$86 billion in 2017. And cybercriminals are taking note. In the first seven months of 2018 alone, malware directed at ATMs/PoS systems infected 57% more targets than in the whole of 2017.

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.

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 business 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 protected 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.

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 functionality on the Windows XP platform as well as the Windows 7, Windows 2009 and Windows 10 families.

Most leading endpoint security vendors are ending their support of Windows XP. Kaspersky Embedded Systems Security is committed to providing 100% support for the Windows XP family for the foreseeable future.

Compliance

The unique, comprehensive set of protection components 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.).

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 anti-malware component is available which can be disabled if using low-end hardware or slower communications channels, to ensure it doesn't take up too much bandwidth or impact on productivity.

Real-time Malware Detection with Kaspersky Security Network (KSN)

KSN is Kaspersky Lab's 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 new and unknown malware 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 normal way.

Device Monitoring and Control

Device Control from Kaspersky Lab 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 key point of entry, used regularly by cybercriminals as the first step in a malware attack. All USB device connections are monitored and analyzed 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 by specified files and folders within scope. You can also configure file changes to be tracked during periods when monitoring is interrupted.

Log Audit

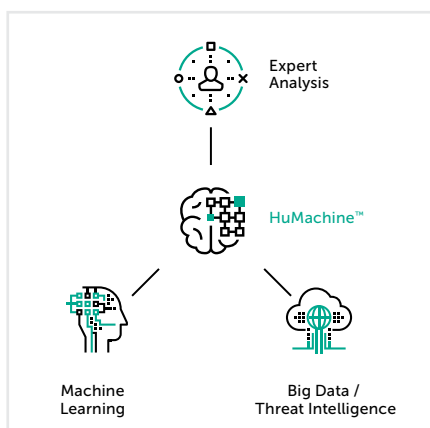
Kaspersky Embedded Systems Security monitors the integrity of the protected environment based on inspecting Windows Event Logs. The application notifies the administrator when it detects abnormal behavior that may indicate an attempted cyber-attack.

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 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. All agents in a local area network can be managed through any local console – particularly useful when working with the isolated, segmented networks typical of embedded systems.



How to buy

Kaspersky Embedded Systems Security can be purchased as separate licenses:

- Kaspersky Embedded Systems Security
- or
- Kaspersky Embedded Systems Security Compliance Edition

It's not included in any bundle

www.kaspersky.com

© 2018 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.