kaspersky

Kaspersky®
Embedded Systems Security

Powerful protection for automated control systems and equipment running Windows® OS

Any automated terminal, whether controlling assembly line processes or orchestrating the flow of goods and traffic, relies on the stability and fault-tolerance of the embedded system at its core. If a device fails or its performance is disrupted, the impact can be devastating. Planned downtime – for scheduled maintenance, for example – is disruptive enough, but the cost of unplanned downtime as a result of a cyberattack can take down a manufacturer for good.

Embedded systems in automated control systems are prime targets for cybercriminals looking to cause maximum disruption and financial losses, and steal intelligence. Financially motivated breaches against the manufacturing industry have increased in recent years, and the sector suffers more espionage-related breaches than any other. According to US ICS CERT classification, in 2018 there were more vulnerabilities in various automated controls system components in manufacturing than in any other industry.

Embedded systems used in manufacturing usually run on the obsolete Windows XP OS, are rarely updated, and typically reside within an internal network. They present a classic entry point for targeted attacks in particular – and the vast majority of cyberattacks against the manufacturing industry are targeted attacks…

It's clear that preventing unplanned downtime as a result of a cyberattack is a top priority for manufacturers, and that embedded devices in manufacturing need the highest levels of protection. Traditional forms of protection - anti-malware only, or application/device control only - are not enough to secure them. This is why we developed Kaspersky Embedded Systems Security.

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.

Efficient design even for low-end hardware

Kaspersky Embedded Systems Security has been built specifically to operate effectively even on low-end hardware. The 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.

Protection against the latest threats

Kaspersky Embedded Systems Security delivers multiple layers of essential security technologies (including application and device control, antimalware and network protection) to protect embedded systems from the latest threats.

Optimized for Windows XP

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 on 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, allowing enough time to gradually upgrade.

Flexible Management

Kaspersky Embedded Systems Security can be managed from the command line, the local GUI or the centralized policy-based management of 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.
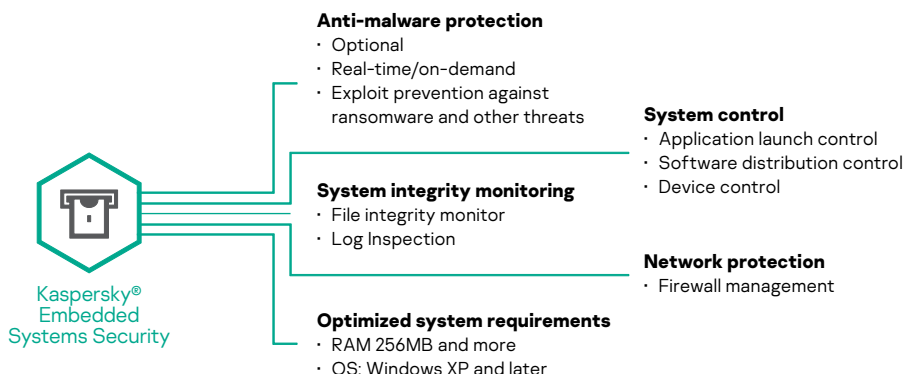
Licensing Options

Kaspersky Embedded Systems Security is available in two types of commercial licenses:
· Kaspersky Embedded Systems Security standard
· Kaspersky Embedded Systems Security Compliance Edition, an extended license that includes File Integrity Monitor and Log Inspection.

Kaspersky Embedded Systems Security

Kaspersky Lab Embedded Systems Security has been specifically designed for organizations operating embedded systems, and the threat environment they operate in. It protects the attack surfaces unique to these architectures, reflecting their unique functionality and OS, channel and hardware requirements, while fully supporting the Windows XP family.

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

System control
· Application launch control
· Software distribution control
· Device control

Kaspersky®
Embedded
Systems Security

System integrity monitoring
· File integrity monitor
· Log Inspection

Network protection
· Firewall management

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

Anti-Malware and Memory Protection

Proven cloud-assisted protection from the industry's leading antivirus engine, capable of detecting even the most aggressive attacks.

Application and Device Controls

The basis of effective protection for embedded systems, where everything (apps drivers, libraries, USB drives) not explicitly permitted is blocked.

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 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.

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.

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.

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.