Kaspersky® Embedded Systems Security

KESS 2.0 What's new

Top 5

Memory protection

Protects the process memory from vulnerabilities

Kaspersky Embedded Systems Security now protects the process memory against exploits A dynamically loaded Process Protection agent is inserted into protected processes, monitoring their integrity and reduce the risk of vulnerabilities being exploited.

File integrity monitor (FIM)

Audits file changes that may indicate a security breach on the protected computer

The File Integrity Monitor task tracks actions performed by specified files and folders in the monitoring scope. You can also configure file changes to be tracked during periods when monitoring is interrupted.

Log inspection

Analyzes activity within a protected system via the Windows Event Log

Kaspersky Embedded Systems Security now monitors the integrity of the protected environment based on inspecting Windows Event Logs. The application notifies the administrator on detecting abnormal behavior that may indicate attempted cyber-attacks. The solution examines the Window event log and identifies breaches based on rules specified by the user or by Heuristic Analyzer settings used by the task to inspect logs.

SIEM integration

Exports application logs to the external Security Information and Event Management (SIEM) systems via the syslog protocol

Kaspersky Embedded Systems Security can now convert events in application logs into formats supported by the syslog server, so these can be transmitted and successfully recognized by SIEM.

USB connections monitoring

Notifications about all the connections to a protected computer via the USB ports for various device types

Kaspersky Embedded Systems Security can control USB storage devices. In version 2, all USB device connections are monitored for further analysis. Inappropriate USB use can be detected as a possible attack source or during the incident investigation and response processes.

Powerful Threat Intelligence

Based on unequalled sources of real-time threat intelligence, our technologies continually evolve to protect your business from even the latest, most sophisticated threats, including zero-day exploits. By aligning your security strategy with the world leaders in advanced threat discovery, you are choosing to adopt best of breed endpoint protection, now and in future. There is no better security posture for your organization.

Centralized Management

Security policies, signature updates, antivirus scans and results collection are easily managed through a single centralized management console – Kaspersky Security Center. All the agents in a local area network can be managed through any local console – particularly valuable when working with the isolated, segmented networks typical of Embedded systems.

Optimized Efficiency – Integrated Management

Kaspersky Embedded Systems Security provides your security teams with full visibility and control over every Embedded node.

Infinitely scalable, the solution provides access to inventories, licensing, remote trouble-shooting and network controls, all accessible from one console – the Kaspersky Security Center.

The security specialist can manage all agents within an area network through any local console.

Maintenance And Support

Operating in more than 200 countries, from 34 offices worldwide, our 24/7/365 commitment to global support is reflected in our Maintenance Service Agreement (MSA) support packages.

Our Professional Services teams are on standby to ensure that you derive maximum benefit from your Kaspersky Lab security installation.

To learn more about securing your Embedded systems more effectively, please visit www.kaspersky.com/enterprise

Firewall and CD/DVD management

Due to the nature of some embedded systems attacks, protection against malicious insider activity is essential. Embedded systems operating outside the domain perimeter must always be protected by centrally managed Device Controls for both internal CD/DVD and USB storage drives, as well as by a firewall.

Windows XP – Windows 10 Ready

After 12 years, support for Windows XP Embedded ended on January 12, 2016 and for Windows Embedded for Point of Service on April 12, 2016. There will be no more security updates or technical support for the Windows XP operating system.

Even more importantly, most leading endpoint security vendors are also now ending their support of Windows XP. Kaspersky Embedded Systems Security is absolutely committed to providing 100% support for the Windows XP family, for the foreseeable future.

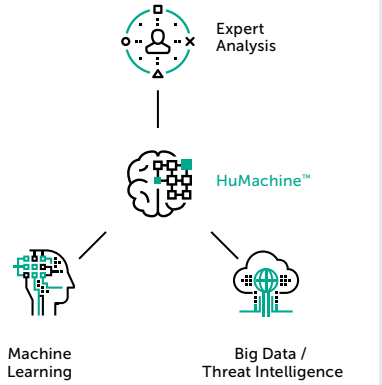
Designed for Embedded Systems Hardware

Kaspersky Embedded Systems Security is designed to be fully effective on the low-end systems which are a feature of most Embedded systems hardware. 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. The antivirus module is designed only to use hardware resources during manual or scheduled antivirus scans.

Antivirus and Kaspersky Security Network

Antivirus is provided as an optional module. Using a classic "antimalware approach" is impractical due to of the limitations of low-end hardware, and is anyway largely ineffective in this unique threat landscape. Once Kaspersky Embedded Systems Security is installed in Device Control and Default Deny mode, additional antivirus is not always necessary, but can be added as a further security level where needed.

Kaspersky Lab also recommends applying intelligent security in the form of the Kaspersky Security Network knowledge base, to prevent and mitigate exploit-based security risks and minimize reaction time.



Kaspersky Lab
Enterprise Cybersecurity: www.kaspersky.com/enterprise
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.com