Kaspersky® Embedded Systems Security

All-in-one security designed for Embedded systems

The threat environment is advancing exponentially, putting critical business processes, confidential data and financial resources at ever-increasing risk from zero-second attacks. To mitigate the risk to your business, you need to be smarter, better equipped and better informed than the cyber-professionals targeting you.

Today we see Embedded systems everywhere: in ticketing machines, ATMs, kiosks, Point of Sale systems, medical equipment... the list goes on. Embedded systems generate particular security concerns as they tend to be geographically scattered, challenging to manage and rarely updated. They also need to be highly fault tolerant and resistant, operating as they do with cash and with credit card credentials. Embedded devices must not only be protected against threats in themselves: they must also be inaccessible by cybercriminals or an inside attacker as an entry point into the corporate network.

Standard security regulations for Embedded devices tend to cover only antivirus based security or system hardening, which is not enough. A purely antivirus approach is of limited effectiveness against current Embedded systems threats, as has been amply demonstrated in recent attacks. Now is the time to apply well-proven technologies like Device Control and Default Deny, with additional antivirus protection applied to critical systems where required.

Solution Highlights

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.

Windows XP Optimized

The majority of Embedded systems still run on the now unsupported Windows® XP family 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 2009 and Windows 10 families.

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.

Default Deny

The last 10 years has seen an increase in malware developed specifically to attack Embedded systems, including Tyupkin, Skimer, Carbanak and their families. Most traditional antivirus solutions cannot fully defend against such advanced, targeted, malware threats. A classical anti-malware solution is not effective against the many targeted threats not based on malware, which use insiders' middleware in a different attack approach. Default Deny functionality means that no executable files, drivers and libraries, other than software protection, can run without approval from the Security Administrator.

Device 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 processes.

SIEM integration

Kaspersky Embedded Systems Security can now 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.

Memory protection

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.

Centralized Management

Security policies, signature updates, antivirus 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 valuable when working with the isolated, segmented networks typical of Embedded systems.

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 should always be protected by centrally managed Device Controls for both internal CD/DVD and USB storage drives, as well as by a firewall.

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

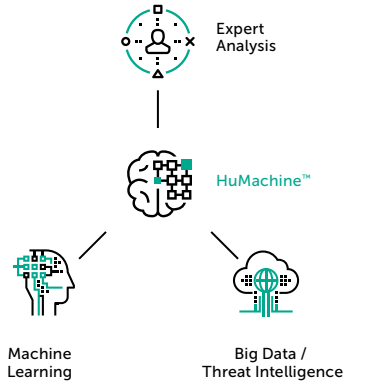
Kaspersky Embedded Systems Security monitors the integrity of the protected environment based on inspecting Windows Event Logs. The application notifies the administrator on detecting abnormal behavior that may indicate an attempted cyber-attack.

The solution examines the Windows event log and identifies breaches based on rules specified by the user or by Heuristic Analyzer settings.

Antivirus and Kaspersky Security Network

Antivirus is provided as an optional module. Using a classic 'anti-malware only 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