Kaspersky® Embedded Systems Security

Powerful protection specifically designed for automated control systems and equipment running on the Windows® OS family

Any automated terminal, whether controlling assembly line processes or orchestrating the flow of goods and traffic, is reliant on the stability and fault-tolerance of the embedded system at its core. Should a device fail, or its performance be disrupted, the 'knock-on' effects can be costly in terms of lost productivity and remediation.

It's easy to forget, too, that these comparatively simple control systems generally sit on the corporate network at some level, and so offer a potential access-point into your organization's overall IT infrastructure. So properly securing these systems is a must.

Insider activity is a key factor in the majority of attacks against embedded systems, and a purely antivirus approach is of limited effectiveness where this is the case, as has been amply demonstrated in recent attacks.

Now is the time to apply approaches like Device Control and Default Deny, already well-proven technologies in other security contexts, to protect your automated operational equipment and terminal based systems against targeted malware attack, cyber-espionage from within, or simple human error.

Kaspersky Lab Has Created a Solution Specifically Designed for Automated Control Systems Running on Windows Embedded Operating Systems

Default Deny

The last 10 years has seen an increase in malware developed specifically to attack embedded devices. Most traditional antivirus solutions cannot fully defend against such advanced, targeted, malware threats when used alone. Default Deny functionality means that no executable files, drivers and libraries, other than software protection, can run without approval from the Security Administrator. Centralized Firewall management provides further enhanced security.

Device Control

Device Control from Kaspersky Lab gives you the ability to prevent an access by unauthorized USB data storage devices – a key point of entry used regularly by cybercriminals as the first step in a malware attack. Internal CD/DVD drives can be controlled centrally even when they are outside of domain.

Optimised Efficiency – Integrated Management

Kaspersky Embedded Systems Security provides your security teams with full visibility and control over every embedded device. 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, a valuable facility when working with isolated and segmented embedded systems as well as operating systems and middleware patch management.

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 ATM and POS endpoints more effectively, please contact the Kaspersky Lab Enterprise Sales Team.

WinXP Ready

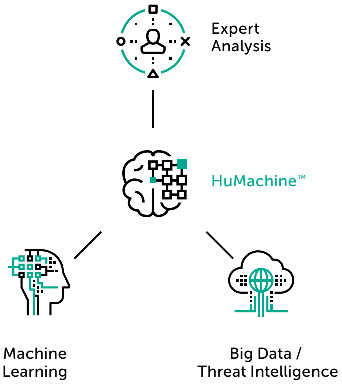
After 12 years, support for Windows XP Embedded ended on January 12, 2016 with product End-of-life. There will be no more security updates or technical support for the Windows XP operating system by Microsoft. Most security vendors do not support Windows XP legacy systems. Kaspersky Embedded Systems Security provides 100% support for the Windows XP family as standard.

Designed for Embedded Systems Hardware

Kaspersky Embedded Systems Security is designed to be fully effective even on low-end 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 'on-demand mode', the antivirus module is designed to use hardware resources only during manual or scheduled antivirus scans.

Antivirus and Kaspersky Security Network

When an embedded system is protected with application control only, there is a serious risk of insider or malware based attack. Kaspersky Embedded Systems Security delivers efficient antivirus protection, together with regular automatic or manual malware signature updates as required. As the majority of attacks on embedded systems are initiated through insiders' activity, Kaspersky Lab also recommends activating the Kaspersky Security Network knowledge base, to prevent and mitigate malware whitelisting and exploit-based attacks.



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