Kaspersky® Embedded Systems Security

Powerful protection for medical equipment running on the Windows® OS family

Security is a major consideration for medical equipment vendors and health providers alike. Medical equipment must be fault-tolerant, stable and available 24x7. But these critical devices face both the risks associated with being a part of the corporate network, and those unique to the embedded systems on which they're based.

A purely antivirus approach is of limited effectiveness against current threats to embedded systems, including medical equipment, as has been amply demonstrated in recent attacks.

A more effective solution, and this is particularly true where stability and continuity is such a critical factor, is one based on a combination of Default Deny with Device Control. These technologies also offer effective protection against insider attack – always a possibility in busy, highly-populated hospital environments.

Kaspersky Lab has created a solution specifically designed for medical equipment running on Windows Embedded Operating Systems.

Optimized 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.

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 or 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 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 the domain.

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 based medical equipment more effectively, please contact the Kaspersky Lab Enterprise Sales Team.

Windows XP Compatible

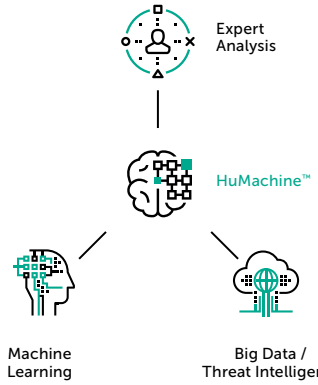
After 12 years, support for Windows XP Embedded ended on January 12, 2016 with product End-of-life. There will be no more security updates or technical support for the Windows XP operating system from Microsoft. Most security vendors do not support Windows XP legacy systems. Kaspersky Embedded Systems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