Powerful protection for medical equipment running Windows® OS

kaspersky BRING ON THE FUTURE

Kaspersky Embedded System Security

kaspersky BRING ON THE FUTURE

Kaspersky Embedded System Security

Powerful protection for medical equipment running Windows® OS

In July, 2019, Springhill Medical Center in Alabama was hit by a ransomware attack that disabled many of the hospital's computer systems. This resulted in lost access to patients' historical data as well as a severe lack of diagnostic information, as most of the monitoring equipment was made offline. The latter was the reason for a wrong decision, resulting in a traumatic birth of a baby girl who suffered hypo-oxygenation brain damage and later died because of it. The mother filed a lawsuit against the hospital – which, in turn, presented the information about the then-ongoing ransomware attack. The trial is currently set for November 2022; if the court accepts the hospital's data as the proof of innocence, it will be the first officially confirmed death caused by ransomware.

Source: Wall Street Journal

Hospitals around the world have hundreds of thousands of Internet-enabled devices connected to their networks, covering almost every aspect of patient care from medical records to pacemaker implants. Medical equipment must be fault-tolerant, stable and available 24/7, yet these devices face risks associated with being part of the corporate network, as well as those unique to the embedded systems which they're based on. Embedded healthcare systems are targets of sabotage that directly impacts connected equipment – and can even manipulate patient data.

Medical devices generally have a lifecycle of around 20 years, and it's estimated that over 60%[1] of medical devices have reached end of life, making it more likely that they're running on outdated, unsupported operating systems. Cybercriminals use vulnerabilities in these outdated systems to gain access to the healthcare network.

Add to this the fact that the number of connected medical devices globally is set to rocket from around 10 billion today to over 50 billion in the next decade[2] and it's not hard to see why the healthcare industry faces more ransomware attacks than nearly any other sector. And these types of attack are growing rapidly, as is the number of networked devices. More devices mean more attack vectors, and old devices can't be properly secured with outmoded protection.

The Covid-19 pandemic has exacerbated the situation. Healthcare practitioners and operators have had to accelerate their digital transformation almost overnight. Suddenly, there are waiting lists for online medical consultations across the board, and more digital devices, medical equipment and connected monitors than ever before are being used to collect and share data to be stored and analyzed. When these devices and systems aren't protected, it's great news for cybercriminals – and bad news for healthcare. Cybercriminals' claims that they would not damage healthcare institutions have proven empty, and they have caused plenty of disruption to medical facilities. The consequences of a ransomware attack on health monitoring systems or diagnostic equipment can't only be measured in unanticipated costs, but in human lives. The protection for these systems must be as powerful as their often below-average specs allow.

A purely anti-malware-based or purely system hardening[3] -based approach is not enough to deal with threats to embedded systems. Only multi-layered protection specifically designed to address these unique challenges can deliver reliable, effective protection. Of course, not all medical equipment has the same computing power. Some devices, especially newer ones, are close to regular workstations, and some configurations can restrict the scope of the protective layers. Ideally, the security solution must be able to adapt to devices with any power levels within any medical facility.

[1] https://www.sensato.co/post/endless-terrifying-possibilities-call-for-a-good-medical-device-cop

[2] https://linchpinseo.com/trends-medical-device-industry/

[3] Including Application control, device control and other technologies capable of utilizing the Default Deny scenario

Efficient design even for low-end hardware

Kaspersky Embedded Systems Security has been built specifically to work smoothly even on low-end hardware. The efficient design delivers powerful security with no risk of systems overload. Requirements start from only 256MB RAM for Windows XP, with around 50MB space required on the system hard drive when operating in 'Default Deny only' mode.

Easy 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 the single centralized management console. 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.

Flexible licensing

Kaspersky Embedded Systems Security is available in two commercial licenses:

- Kaspersky Embedded Systems Security standard
- Kaspersky Embedded Systems Security Compliance Edition, an extended license that includes File Integrity Monitor and Log Inspection.

Protection against the latest threats

Kaspersky Embedded Systems Security is all-in-one security designed specifically for embedded systems. It delivers multiple layers of essential security technologies, including application and device control, anti-malware, exploit prevention and network protection to protect embedded systems from attacks.

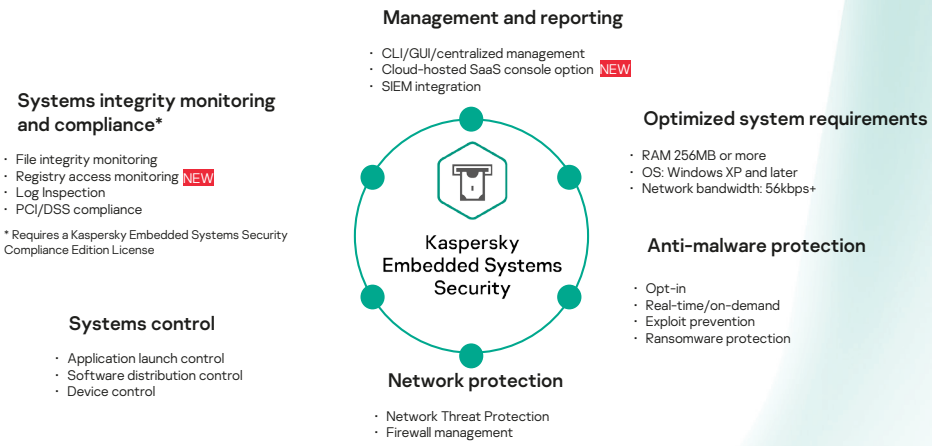
The solution supports an opt-in approach for its protection layers, offering the highest level of protection for the broadest possible range of Windows-based embedded systems.

Optimized for Windows XP

Most embedded systems still run on the obsolete Windows® XP OS. Kaspersky Embedded Systems Security has been optimized to run with full functionally on Windows XP as well as on Windows 7, Windows 8 Windows 10 and even Windows 11 families. Kaspersky Embedded Systems Security is committed to providing 100% support for Windows XP for the foreseeable future, giving organizations plenty of time to upgrade when they're ready.

Features and benefits

Kaspersky 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. When it comes to medical equipment, these capabilities can literally be the difference between life and death.



System hardening

Using 'allow list' principles, system hardening prevents the use of unsolicited applications and external devices. This helps to prevent malware attacks and stops unwanted utilities and storage from connecting to your systems. It also ensures that apps on the allow list can be easily and safely updated, in default deny mode.

Opt-in anti-malware and exploit prevention/ memory protection

Proven cloud-assisted protection from the industry's leading antivirus engine, capable of detecting even the most aggressive attacks. Anti-malware protection offers both real-time and on-demand scanning, instant, reputation-based protection from the Kaspersky Security Network cloud, and exploit prevention. This is essential for all systems but especially those running an unsupported OS. You can enable or disable this component depending on your device type and deployment scenario.

Network threat protection

Embedded systems are highly vulnerable to network attacks. Kaspersky Embedded Systems Security offers centralized management of the OS embedded firewall as well as network threat pretention to counter a broad range of attack scenarios, including DoS and network-related vulnerability exploitation. Network threat protection is particularly important for medical embedded devices because cyberattacks that start by infecting a regular endpoint can move laterally, using network vulnerabilities to compromise highly specialized medical machines.

Application and device controls

Application and device controls are the foundation of effective protection for embedded systems, where everything (apps drivers, libraries, USB drives) not explicitly permitted is blocked, making direct infection highly unlikely.

Optimized system requirements

Embedded systems can vary significantly in terms of resources, age and usage scenarios. Kaspersky Embedded Systems Security offers flexible configuration and selection options, so that security can be tailored to any system, regardless of its age and use. This optimize performances and delivers rock-solid stability.

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.

File Integrity and Registry Access Monitoring[4]

Most embedded systems are single-purpose devices, so interference with their components may indicate an intrusion. Tracking changes in critical system areas and monitoring abnormalities in system logs is crucial for system integrity – especially when compliance is at stake. File integrity monitoring and Registry Access monitoring in Kaspersky Embedded Systems Security tracks actions performed on specified registry keys, files and folders, and can be configured either to alert or block the undesired changes.

Log Inspection[5]

Kaspersky Embedded Systems Security monitors possible protection violations based on Windows Event Logs. The application notifies the administrator when it detects behavior that may indicate an attempted cyberattack.

[4] Available in Kaspersky Embedded Systems Security Compliance Edition

[5] Available in Kaspersky Embedded Systems Security Compliance Edition

On-prem or cloud-based management

Fast deployment and remote operation options have become essential, so Kaspersky Embedded Systems Security can be administered from an on-premise management infrastructure or from the cloud via Kaspersky Security Center. This enables a fast start, without the need to set up a management server, and brings easy availability of management instruments from anywhere. The solution is managed from the same management console as other Kaspersky products, delivering better visibility and control and consistent, more effective security policies.

Life-saving stability and security

The smooth, uninterrupted functioning of embedded medical devices is critical for the delivery of effective healthcare, allowing medical staff to do much more, and ultimately save more lives. Even if the functioning of a particular device isn't threatened, a leak of confidential medical information can be disastrous for medical services and patients alike. Kaspersky Embedded Systems Security delivers reliable security and rock-solid stability so that the medical fraternity can focus on the most critical task of all: keeping people well and alive.

To find out more about how Kaspersky Embedded Systems Security can secure your healthcare facilities and systems, **contact us now**

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Kaspersky technologies in details: kaspersky.com/technowiki
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

www.kaspersky.com