

KASPERSKY EMBEDDED SYSTEMS SECURITY

Powerful protection specifically designed for critical payment 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 critical financial and payment systems, you need to be smarter, better equipped and better informed than the cyber-professionals targeting you.

Embedded systems are a particular security concern as they tend to be geographically scattered, challenging to manage and rarely updated. Operating as they do with real money and credit card credentials, ATMs and Point of Sale devices are targets of choice for cybercriminals, so require the highest levels of focused, intelligent protection.

The Payment Card Industry Data Security Standard (PCI DSS) regulates many technical requirements and settings for credit card data based systems. However, security regulations for ATMs and Point of Sale devices appear to cover only antivirus based security. A purely antivirus approach is of limited effectiveness against current ATP/POS threats, 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 your critical embedded systems.

SOLUTION HIGHLIGHTS

LOW PERFORMANCE 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.

WINDOWS XP OPTIMIZED

With around 90% of ATMs still running on the now-unsupported Windows® XP family OS, Kaspersky Embedded Systems Security has been optimized to run with full functionality on the Windows XP platform as well as the Windows 7, Windows 2009 and Windows 10 families.

ISOLATED SECURED NETWORKS READY

Malware signatures can be updated automatically through the internet, or manually for the isolated secured networks typical of ATMs and often of POS systems. For 'Default Deny only' installation, no updates are needed.

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 ATM and POS installations.

Default Deny

The last 10 years has seen an increase in malware developed specifically to attack ATMs and POSs, including Tyupkin, Skimer, Carbanak and their families. Most traditional antivirus solutions cannot fully defend against such advanced, targeted, malware threats. 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. The prevention of access by unauthorized devices blocks a key point of entry used regularly by cybercriminals as the first step in a malware attack.

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. Kaspersky Embedded Systems Security provides 100% support for the Windows XP family.

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 ATM and POS 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 only to use hardware resources during manual or scheduled antivirus scans.

Antivirus and Kaspersky Security Network

PCI DSS regulations specify that all systems interfacing with credit or debit cards must have antivirus installed and regularly updated. Kaspersky Embedded Systems Security delivers efficient antivirus protection, together with regular automatic or manual malware signature updates as required. As over half of all malware found in ATM and POS systems has entered through zero-day/zero-second exploits, 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.



OPTIMISED EFFICIENCY - INTEGRATED MANAGEMENT

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

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 ATM and POS networks.

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.