Kaspersky® Embedded Systems Security

Powerful protection for Ticket Vending Machines and POS terminals running on the Windows® OS family

Ticket Vending Machines (TVMs), electronic kiosks and similar Point of Sale (POS) devices are at particularly high risk of cyberattack, as they:

- usually run on the obsolete Windows XP OS family
- handle financial transactions
- are geographically scattered and rarely updated
- sit inside an internal network
- offer a classic entry point for Targeted Attacks

As targets of choice for cybercriminals, POS devices like Ticketing Machines 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 Point of Sale devices appear to cover only antivirus based security. A purely antivirus approach is of limited effectiveness against current 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.

Kaspersky Lab has created a solution specifically designed for POS devices including Ticket Vending Machines.

Optimized 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 TVM and POS networks.

Default Deny

The last 10 years has seen an increase in malware developed specifically to attack vending machines, 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 or 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 prevent access by unauthorized devices, blocking a key point of entry used regularly by cybercriminals as the first step in a malware attack.

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

Windows XP – Windows 10 Ready

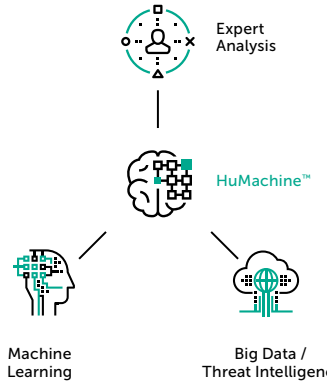
After 12 years, support for Windows XP Embedded ended on January 12, 2016 and for Windows Embedded for Point of Service on April 12, 2016. There will be no more security updates or technical support for the Windows XP operating system. Kaspersky Embedded Systems Security provides 100% support for the 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 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

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 POS systems has entered through zero-day/ zero-second exploits, Kaspersky Lab also recommends 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