



POS SECURITY GUIDE

Achieving effective, efficient security
for critical payment systems

usa.kaspersky.com

CONCERNS

Embedded systems present specific security concerns. They are generally geographically scattered, they can be challenging to manage and they are rarely updated. Operating as they do with real money and credit card credentials, Point of Sale devices are the targets of choice for cybercriminals. As a result, they require the highest levels of focused, intelligent protection.

Obsolete software is a very common problem, and it's not just consumer operating systems that are affected. It's a well-known fact that some still-functioning space satellites are running on decades-old hardware and software. Industrial control systems, too, have a problem with very old operating systems and long renewal cycles.

Windows XP families are still the most popular operating systems for POS devices. The ending of support for this operating system has affected vast numbers of businesses and government bodies. Retail sectors have been particularly impacted. The fact is, though, that this system actually ceased to be supported back in April 2014, along with consumer versions of Windows XP.

The overall replacement of POS systems software is a long, expensive, and painful process. Besides which, replacing software often means also having to replace still-functional, if technically obsolete, hardware.

THE THREAT LANDSCAPE

POS systems, capturing verified personal data and credit card details, are inevitably high on the hit-list, for cybercriminals.

Since 2009 the quantity and quality of attacks has increased dramatically year by year. 2015 has seen attacks on POS systems reaching a new high, with malware including vSkimmer, Dexter, Alina, Backoff, JackPOS, among others.

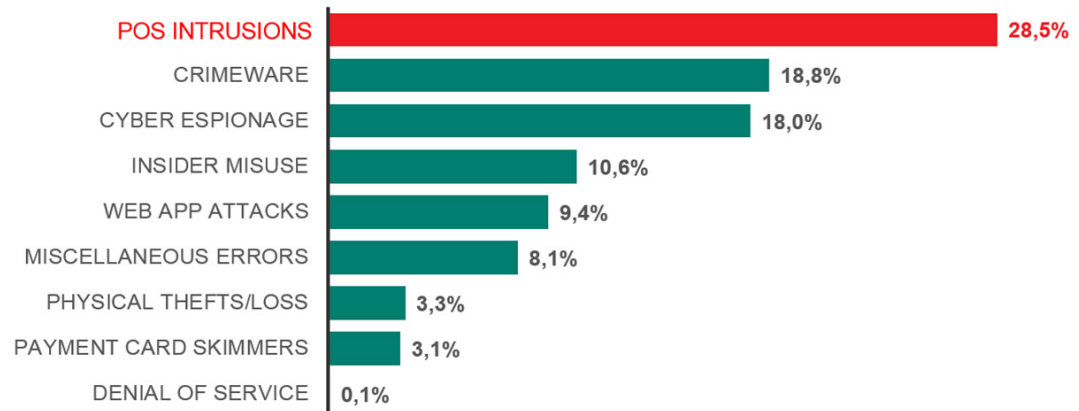
Conventional antivirus software cannot effectively protect against all these threats. The limitations of POS systems – weak channels, low-end hardware and obsolete software – make its installation and deployment challenging and often impractical. As a result, these viruses continue to succeed in penetrating the POS systems of major and retailers on a daily basis.

Meanwhile, increasing volumes of highly targeted POS malware are being created by professional developers; they are supported by the very latest and most powerful systems and hardware.

POS BASED THREATS

FREQUENCY OF IT SECURITY INCIDENTS

CLASSIFICATION OF CONFIRMED DATA BREACHES

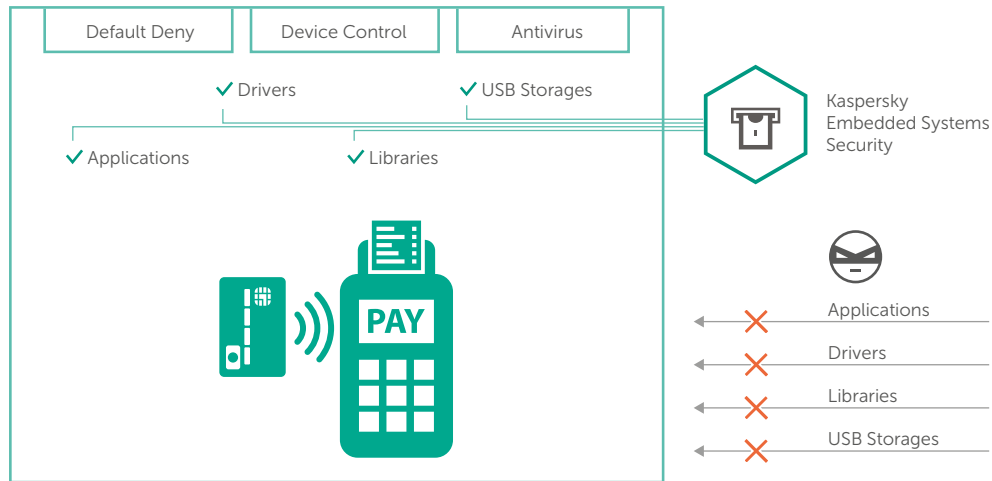


*VERISON 2015 DATA BREACH INVESTIGATION REPORT

A specific area of vulnerability for Point of Sale (POS) systems is the middleware they depend on. This middleware tends to be created by small third-party vendors or in-house. Functionality may well take precedence over security as a design consideration. Easy access to USB ports and CD/DVD drives may be seen as a convenience, rather than a security weakness.

Most POS systems operate with credit/debit cards are subject to PCI DSS regulation. All, without exception work with personal customer data. The protection of the customers' data is the responsibility of the POS system's owner. All of them are connected to an intranet, making the POS both an easily reachable target and a useful entry point for a targeted attack.

KASPERSKY EMBEDDED SYSTEMS SECURITY



Kaspersky Lab has created a security solution specifically for organizations operating POS systems and the threat environment they face. This reflects their unique functionality and OS, channel and hardware requirements, while fully supporting the Windows XP family.

Kaspersky Embedded Systems Security mitigates the security risks inherent in embedded systems. The solution has been designed specifically for POS systems, protecting the attack surfaces unique to these architectures. The solution respects related hardware and efficiency considerations. A single intuitive console gives you the control and visibility you need to manage effective multi-layered security for your endpoints, your critical systems and your whole IT infrastructure.

Implementing Default Deny for Applications, Drivers and Libraries, boosted by Device Control functionality, is the only approach which can ensure the safety of technically 'obsolete' systems in continuing use.

Kaspersky Embedded Systems Security offers a 'Default Deny only' operational mode, with system requirements starting from 256Mb of RAM and 50Mb HDD space – ideal for Windows XP based systems running on low-end hardware. On-demand scanning is supplied through an optional Antivirus module powered by the Kaspersky Security Network; it also provides Patch Management facilities as required.

This single solution meets three key objectives:

- Efficiently securing 'difficult to manage' systems
- Compliance with PCI DSS requirements 5.1, 5.1.1, 5.2, 5.3 and 6.2
- Enabling a soft timeline for obsolete systems and hardware replacement.

Default Deny

Most traditional antivirus solutions cannot fully defend against the advanced, targeted, malware threats the industry is currently facing. Default Deny functionality, takes a different, more fundamental, approach. No executable files, drivers and libraries, are able to run on any POS endpoint without explicit approval from the security administrator.

Device Control

Device Control from Kaspersky Lab provides administrator with the ability to control USB storage physically to systems hardware. This prevents access to the POS unit by any unauthorized device. As a result, these vulnerable systems entry-points, used regularly by cybercriminals as the first step in a malware attack, are blocked.

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 separately-installed antivirus module is designed to use hardware resources only during manual or scheduled 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 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. This prevents and mitigates exploit-based security risks and minimizes reaction time.

PCI DSS COMPLIANCE

Kaspersky Security for Embedded Systems functionality meets and exceeds all security standards laid out in PCI DSS v3.1 sub-points:

5.1: Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).

5.1.1: Ensure that antivirus programs are capable of detecting, removing, and protecting against all known types of malicious software.

5.2: Ensure that all antivirus mechanisms are kept current, perform periodic scans, and generate audit logs which are retained per PCI DSS Requirement 10.7.

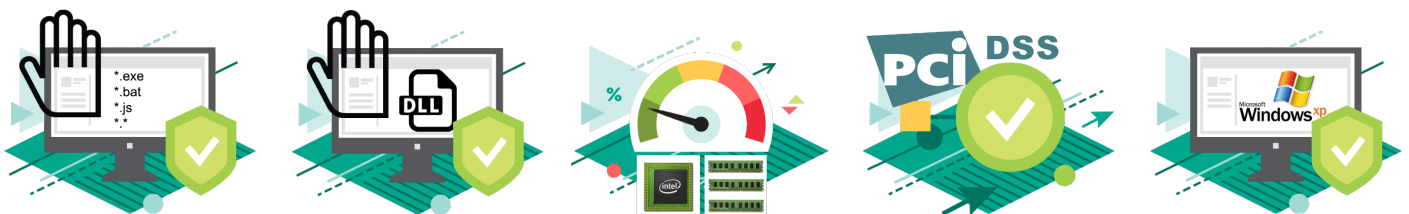
5.3: Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

6.2: Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

BEYOND ANTIVIRUS

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. As aforementioned, an approach that's purely antivirus-based has limited effectiveness against current POS threats. Now is the time to apply Device Control and Default Deny—already well-proven in other security contexts—to critical embedded systems.

To learn more about securing your critical payment systems endpoints more effectively, please contact the Kaspersky Lab Enterprise Sales Team.



AO Kaspersky Lab
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com
To learn more visit us at: usa.kaspersky.com

© 2016 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

