

Moving From Compliance to Security

Meeting PCI DSS requirements through Application Whitelisting

"I do want to dispel the myth once and for all that PCI compliance is enough to keep a company secure. It is not, and the credit card companies acknowledge that."

*Rep. Yvette Clarke (D-N.Y.), Chairwoman, House Subcommittee on Emerging Threats, Cybersecurity, Science and Technology
March 2009*

Retailers are challenged like never before. While the economy slows consumer spending, the increasing number and sophistication of computer attacks resulting in security breaches can create serious consequences.

Loss of consumer confidence, tarnished brand image, negative sales impact, increased fees and potential fines together can put a retailer out of business. While PCI compliance has become a high priority, retail IT security experts realize that even the most PCI compliant retailers are still not secure

Recent high-profile attacks on PCI-compliant credit card processors, retailers and other "secure" organizations make it clear that while PCI compliance is important to satisfy auditors and shareholders, its security standards do not keep pace with organized crime's ability to compromise an organization.

Savant Protection is a class of new application whitelisting technology that allows retailers to comply with PCI standards while improving security. Savant Protection stops attacks, eliminates the need for antivirus and reduces the cost of compliance and management.

POS Environment, PCI and Antivirus

Retail Point of Sale systems (POS) and back-office servers process credit card information and are the targets of criminal attacks. The goal of the attacker is use is to gain an initial foothold on an endpoint (POS system, wireless entry point), migrate through a network to locate cardholder information, then collect and transmit that information to the attacker while avoiding detection. In an effort to "enhance payment account data security", in 2004 the Payment Card Industry created its Data Security Standards (PCI DSS). Contrary to popular belief, PCI compliance applies to ALL organizations or merchants, regardless of size or number of transactions, that accept, transmit or store any cardholder data.

Antivirus software has been the primary end-point defense used by retailers to prevent malicious software from executing and comply with Section 5 of the PCI DSS. As seen in the many breaches against retailers relying on antivirus, this strategy provides a simple method that allows organizations to achieve compliance, but clearly does not meet the security objective of the standards. In other words, organizations need to move beyond simple compliance to protect their customers' information.

"We have to get beyond check box security. It provides a false sense of security for everyone involved, and it is ineffective in reducing the real threats."

*Bennie G. Thompson (D-MS)
Chairman, Committee on Homeland Security*

The challenges faced by antivirus vendors are not simple to overcome. To be successful, the vendors must first identify all malicious software that exists "in the wild", reverse engineer these attacks and create a unique signature or hash for each "known bad" application. New signatures, added to an update file, are then distributed to customers, often several times each day. On the end-point, each time the device accesses a file the antivirus end-point application compares the signature of that file with the antivirus signature database.

Criminals Easily Bypass Antivirus

Aside from the processing overhead resulting from antivirus on end-points and the administrative burden of managing centralized solutions, the vendors' ability to identify and track all malicious software has become practically impossible. According to Symantec, the number of new malware threats was over 1,600,000 in 2008. In 2009, some believe we will see *over 10,000 new malware threats each day*. While antivirus must identify all possible attacks to be effective, attackers need only create new ones that do not match the signatures of "known bad" software.

"These are incredible technical programs often designed by organized crime syndicates with technical resources that dwarf those of the average company. And with just one inside source in a company they can be made virtually invisible."

*Mr. Michael Jones
Chief Information Officer, Michaels Stores Inc.*

Criminals understand the weaknesses of antivirus *and* retailers' reliance on antivirus as their primary endpoint protection. In many ways, this makes the criminals' task easier. Criminal organizations will invest the effort necessary to test their attacks against multiple antivirus solutions and create unique attacks that bypass antivirus for each target retailer.

These "targeted attacks" are effective; once the attack is deployed, the criminals are confident the attack will not be detected. Since antivirus solutions rely on a centralized database of all known bad software, if a single attack signature is missed, every device in the environment is exposed.

Application Whitelisting is a Compensating Control for Antivirus

POS and retail systems typically perform a limited and specific set of functions. In practice, the only software that should execute and update on these devices are the applications required for the devices to perform required tasks. There is no need to identify the "intent" of any other executable on the device, or whether unknown software is "known bad". No other software, whether malicious or not, is required or should run.

QSA's recognize that antivirus will only stop "known attacks". Savant Protection stops all unauthorized software from reaching the CPU, whether it is known malware, unidentified or simply unwanted on an end-point. Savant provides the ability to approve or whitelist known applications for any Windows POS implementation, whether designed in-house or purchased from a third-party provider.

Savant's Distributed Application Whitelisting solution allows trusted software to run and update normally while preventing all other software from executing, effectively locking down the retail environment. Savant is extremely easy to implement and manage, and automatically "learns" existing POS environments in minutes. Protection of the end-points against intentional or accidental changes begins immediately, regardless of the local operating system privileges of the users and managers.

In addition, if your QSA insists on antivirus despite its shortcomings, Savant Protection can link to an open source antivirus product to identify and clean "known" malware.



No Single Point of Failure

Savant eliminates the single point of failure associated with antivirus and centralized or rules-based solutions. With Savant's unique distributed architecture, the components of the POS system do not rely upon access to centralized servers in order to protect end-points. Instead, each POS, server or device maintains its own unique set of Savant "keys" that allow only authorized software to execute. Since the key that allows an application to run on one device will not work on any other device, even a deliberate attack by a privileged user that is approved on one device cannot spread to any other device.



Low Overhead, Low Total Cost of Ownership

Retail organizations must provide high levels of control and security, but minimize management overhead. Savant installs in minutes and begins protecting systems immediately. Because of its distributed architecture, no updates to "known good" or "known bad" centralized databases are required.

Not all applications are static, some need to update to run effectively. Savant allows organizations to designate trusted applications, such as Windows Updates, to update automatically without user interaction. POS updates can be pushed normally and no other software or malware will execute.

Savant also integrates with desktop management systems such as Altiris and SMS to automatically whitelist applications. This makes deployment and management of end-points even simpler, and can ensure that the only software running in your organizations are those deployed through the desktop management system.

Savant's Enterprise Management System provides all of the alerting, reporting, management and configuration needs of a retail environment without introducing the potential for coercion or single points of failure. Managed or unmanaged, POS servers and devices remain protected by Savant.

Features

- Lockdown POS devices to eliminate unauthorized software and updates
- Stop viruses, Trojans, Bots and other malware from executing
- Trusted applications may operate and update normally
- Small footprint is ideal for POS environment
- Reduce IT overhead from system rebuilds due to malware infection
- Reduce management and updating of centralized antivirus/whitelist databases
- Compensating control for PCI Section 5
- Centralized alerting, reporting and configuration management
- USB device lockout prevents use of USB mass storage devices
- Active Directory synchronization
- Remote control of all systems through an individual secure console
- Compliments or replaces legacy anti-virus solutions

Platforms Supported

- Windows 2000 (client and server)
- Windows 2003 (client and server)
- Windows XP
- Windows XP Embedded
- WEPOS