Esprida LiveControl™
Endpoint Device Management Platform

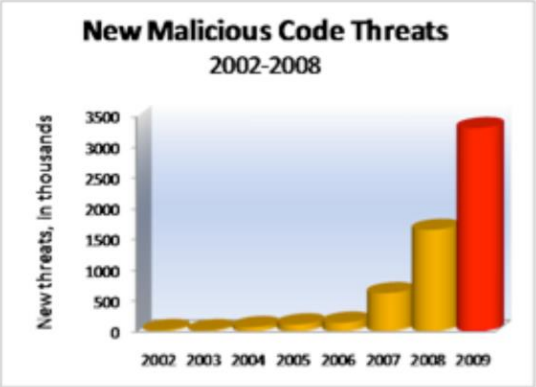
Meeting PCI DSS Requirements for Retail Kiosks

Moving From Compliance to Security

The retail industry is challenged as never before. While the slowing economy reduces consumer spending, the increasing number and sophistication of computer attacks that result in security breaches can create serious consequences.

Loss of consumer confidence, tarnished brand image, negative sales impact, increased fees and potential fines 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.



Sources - Symantec 2009 and Savant Protection Estimate - Ponemon Institute, 2009

Savant Protection and Esprida provide a new class of PCI compliance solutions designed for 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. Esprida delivers increase customer satisfaction while reducing operational costs.

Esprida and Savant Integrated Solution

Esprida and Savant Protection have teamed to deliver a highly secure and automated content management solution. Our joint solution guarantees that all software changes are approved and are centrally managed by Esprida's Remote Device Management Software and authorizes (whitelists) these changes on the devices protected by Savant.

No other executables or changes to the applications or operating system are allowed except for those distributed through Esprida or other trusted change processes. Our solution ensures that only those executable files whitelisted on the device will execute. Further, no new files, modification or deletions to existing files are permitted when the device is locked down by Savant Protection.

"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

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. 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.

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. In 2009 the number of new malicious code threats exceeded 3 million 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.

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.

Security Assessors 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.

Features

- Secure content management – guaranteed automated delivery and guaranteed security
- Automated Distribution capabilities + auditing + security policy enforcement
- Secure configuration management
- 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 via Esprida
- 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 via Esprida
- USB device lockout prevents use of USB mass storage device

Esprida Corporation
1301 Shotgun Road
Weston, FL 33326
Email: info@esprida.com
Phone: 1-877-267-4968
Website: www.esprida.com

Savant Protection
9 Commercial Street
Hudson, NH 03051
Email: sales@savantprotection.com
Phone: 1-603-889-0944
Website: www.SavantProtection.com