Technical FAQ

Maintain PCI Retail Compliance for Systems No Longer Supported

Protect end-of-life operating systems with application whitelisting.

In April 2014, Microsoft ended support for Microsoft Windows XP, an operating system (OS) used by many installed retail systems, including point-of-sale (POS) terminals, ATMs, and back office servers. This means that Microsoft will no longer release new security patches intended to eliminate threat vulnerabilities in this OS version. Eventually, retailers must take alternative action to ensure systems handling customer credit card information remain compliant to the Payment Card Industry Data Security Standard (PCI DSS).[1]

Example of OS Vulnerability

As advanced persistent threats evolve, a legacy OS may become vulnerable, presenting a huge risk for retailers. One example is the Conficker worm, which targeted the Windows XP and Windows 2000 operating systems and took control of systems without users suspecting that anything was happening. The worm exploited vulnerabilities in the networking stack kernel drivers and propagated as a dynamically linked library (DLL), an issue that only the OS vendor can remedy. Conficker-type worms continue to infect systems and can read out data, like customer credit card information.

Whitelisting Ensures System Integrity

Retailers can prevent the execution of malware, like Conficker, by controlling what runs on their retail systems and protecting memory in those devices. This is achievable when retail IT departments can specify which programs (EXEs, DLLs, and scripts) are permitted to execute, a capability supported by McAfee® Embedded Control with whitelisting. As part of the Intel® Security product offering, McAfee Embedded Control automatically creates a whitelist of the “authorized code” on the embedded system. Once the whitelist is created and enabled, the system is locked down to the known good baseline, no program or code outside the authorized set can run, and no unauthorized changes can be made. Whitelisting prevents worms, viruses, and other malware from executing illegitimately on systems used in retail, industrial control, medical, and other industries.

Performance Impact

If a retail system is running an unsupported OS, there's a good chance it's based on older computer technology and may be slow. It may also be running traditional antivirus security, which requires significant computing resources. The good news is that whitelisting has a negligible impact on performance because its primary task is to control the loading of software code—there are no malware signature files to download and run. For retail systems running a pre-defined set of applications, whitelisting offers better protection than antivirus alone, while using fewer resources. When a system has ample resources, like a high-end POS, the best solution is to implement both whitelisting and antivirus.

Q&A

Q: What is the risk posed by an OS that is no longer supported with security patches?

A: Over time, hackers may develop new malware capable of exploiting OS vulnerabilities, compromising system operation, and enabling hackers to access critical data and intellectual property. The ramifications could be severe, such as malware instructing an automated teller machine (ATM) to dispense all its cash.

Q: I'm using a firewall. Isn't that sufficient?

A: Firewalls control the communication ports applications are able to use, but they are not capable of stopping malware that has already infected the system, perhaps via a USB Flash drive. For instance, firewalls cannot stop zero-day attacks, whereas whitelisting can.

Q: Will antivirus software compensate? In what areas may antivirus be deficient?

A: Antivirus software cannot stop malware that attacks the operating system seeking to attain full system privileges. On the other hand, antivirus is a highly effective approach to protecting applications on systems with sufficient computing resources.

Q: How will this impact PCI DSS?

A: The Payment Card Industry (PCI) has specified that a system running an OS no longer supported by the vendor violates the standard unless there are compensating controls, such as whitelisting, to mitigate the risks.[2]

Q: How does whitelisting help?

A: It prevents any unauthorized program that is on disk or injected into memory from executing and prevents unauthorized changes to an authorized baseline. This includes safeguarding against malware designed to attack the operating system.

Q: Do I need antivirus software if I am using whitelisting?

A: Antivirus detects and remediates malware; it works to remove the offending software from the system, whereas whitelisting prevents malware or any unauthorized files or changes from executing. The prudent approach is to run both antivirus and whitelisting, which provides layered security protection when systems have ample computing resources.

Q: Which systems require whitelisting?

A: Install the software on all retail devices (POS terminals, ATMs, kiosks, and sales assistants) that store, transmit, or track credit card data, as well as the back office systems that connect to these devices.

Q: How hard is it to install and support whitelisting?

A: It's not difficult at all. McAfee Embedded Control is a small-footprint, low-overhead, application-independent solution that provides "deploy-and-forget" security.

Q: PCI DSS requires change monitoring. How is this done with whitelisting?

A: McAfee Embedded Control integrates with McAfee® ePolicy Orchestrator® (McAfee ePO™) software, which retailers can use to make system updates, monitor changes, and create Qualified Security Assessor (QSA) audit reports for individual systems.

Q: I'm using a shared hosting provider. Does this change anything?

A: No. Retailers are still responsible for ensuring the systems they use for credit card transactions are PCI DSS compliant.

Q: How will my DSS compliance change with whitelisting?

A: Retailers should verify that their QSA recognizes whitelisting as a compensating control for addressing the risks posed by operating systems without vendor support. Retailers should also follow industry best practice guidelines (IBPG) that further lock down firewalls, BIOS, ports, user access, and more beyond the protection provided by whitelisting.

Q: How does whitelisting address PCI DSS Requirement 5: Use and regularly update antivirus software or program?

A: Whitelisting provides complete malware protection without the need for updates. It does this by providing memory protection for all binaries on the system regardless of the vendor.

Q: How do I test a system with whitelisting, per PCI DSS Requirement 11?

A: No changes to security test procedures are necessary.

More Information

For more information or to learn more visit: **www.mcafee.com/embeddedcontrol.**

[1] PCI DSS is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands.

[2] Dave Shackleford, *How to Choose a Qualified Security Assessor*, a SANS white paper, November 2010, p. 5, **http://www.sans.org/reading_room/analysts_program/secureworks_11_2010_2.pdf**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com