Maintain Security for XP Systems

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 systems, including point-of-sale (POS) terminals, ATMs, medical devices, back-office servers, and industrial control systems. What this means is Microsoft will no longer release new security patches intended to eliminate code vulnerabilities in this OS version. OEMs must take alternative action to ensure that systems handling mission-critical data or that require high availability remain compliant to the respective regulatory or auditing body.

Example of OS Vulnerability

As advanced persistent threats evolve, a legacy OS may become vulnerable, thus presenting a huge risk for OEMs. One example is the Conficker worm, which targeted the Windows XP and Windows 2000 OS and took control of systems without users knowing 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 personal identification information (PII) and mission-critical information.

Whitelisting Ensures System Integrity

OEMs can prevent the execution of malware like Conficker by controlling what runs on their systems and protecting the memory in those devices. This is achievable when IT/OT departments are able to specify exactly which programs (exes, dlls, and scripts) are permitted to execute, a capability supported by McAfee® Embedded Control with whitelisting. As a 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, spyware, and other malware from executing illegitimately on embedded systems used in any industry.

Performance Impact

If a system is running an unsupported operating system, there's a good chance it's based on older computer technology and is a bit slow. It may also be running traditional antivirus security, which requires a significant amount of 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 systems running a pre-defined set of applications, whitelisting can offer better protection than antivirus alone, while also using fewer computer resources. When a system has ample computing 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 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. Even Microsoft has acknowledged that the Windows XP operating system is vulnerable to security breaches.[1] The ramifications could be severe, such as malware instructing an 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 alone cannot stop zero-day attacks, whereas whitelisting can.

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

A: Antivirus software cannot stop all malware that attacks the OS seeking to attain full system privileges. However, antivirus is highly effective as a layered approach to protect applications against malicious code and data 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 operating system no longer supported by the vendor violates the standard unless antivirus is used. McAfee antivirus can be tuned for performance if used in conjunction with 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, meaning it works to remove the offending software from the system, whereas whitelisting prevents malware or any other unauthorized files or changes from executing on the system. 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 devices that store, transmit, or track PII, or have a high availability requirement, 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 on most fixed function devices.

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, the asset owners are still responsible for ensuring the systems they use for mission-critical operations are compliant with any regulations or compliance requirements.

Q: How will my DSS compliance change with whitelisting?

A: With the advent of PCI DSS 3.0, antivirus is no longer optional. However, antivirus can be tuned for performance for lower resource devices if used in conjunction with application whitelisting. OEMs should also follow industry best practice guidelines that further lock down firewalls, BIOS, ports, and user access beyond the protection provided by whitelisting.

Q: How does whitelisting protect system without patches?

A: Whitelisting locks down the runtime environment and automatically creates a dynamic 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. This solution enables manufacturers to enjoy the benefits of using a commercial operating system without incurring additional risk or losing control over how systems are used in the field.

Q: Will using McAfee Embedded Security increase the ROI of devices on XP?

A: Yes, by applying McAfee whitelisting technology, OEMs extend the life of XP systems by avoiding capital expenditure of new systems while providing internal compensating controls for these devices.

1. **http://gigalaw.com/2013/10/29/microsoft-warns-of-security-threats-to-windows-xp/**
2. 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

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