Solution Brief

McAfee Application Control Extends the Life of Legacy Microsoft Windows XP System

Effective April 8, 2014, Microsoft discontinued its support for the Windows XP operating system. Any vulnerabilities that are discovered in Windows XP will not be addressed by a Microsoft security update. The phase-out of support should be of concern to customers because Windows XP systems are more susceptible to zero-day vulnerabilities in the absence of Microsoft support. More than 30% of businesses still use Windows XP systems, so they have to rely on additional security precautions to stay ahead of threats.

Though Microsoft has encouraged customers to develop a strategy to migrate from Windows XP to a more recent operating system in advance of the April 8, 2014 date, the IT resources needed to do so make it an unrealistic proposition for many organizations. But the inability or unwillingness to shift away from Windows XP does not necessarily have to condemn Windows XP users to security gaps. McAfee® Application Control—part of the Intel® Security product offering—provides an effective way to block unauthorized applications from running. McAfee Application Control incorporates a triple-layered defense strategy to prevent zero-day attacks centered on a whitelisting solution that provides protection with minimal strain on system resources.

Dynamic Whitelisting

Whitelisting is a fairly simple yet effective concept. It creates a list of trusted programs necessary for day-to-day operations and ensures that only those specific applications are allowed to run. This feature reduces overhead by eliminating the need to scan each application individually.

Memory Protection

Whitelisted programs that might contain some inherent vulnerabilities cannot be exploited through a buffer overflow. This feature helps prevent complex threats from circumventing whitelisting.

intel Security

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence is a cloud-based service with knowledge of file reputations used by McAfee Application Control to classify applications as good or bad. This feature indicates whether any malware is being whitelisted inadvertently and also highlights files without a reputation that need to be investigated individually.

Layers that Work Together to Prevent Zero-Day Threats

A typical zero-day attack involves multiple factors. First, it leverages a vulnerability in a piece of software that is already installed on the system. Next, it attempts to use that vulnerability to benefit the attacker. Third, it is very likely that the malware leaves a portion of itself behind in an attempt to keep a persistent presence in the event of a reboot.

Stop Vulnerabilities

McAfee Application Control reduces risk in this area by allowing administrators to specify a subset of binaries that are authorized to run. By controlling applications, the potential attack surface through unknown or unauthorized installed applications is greatly reduced.

While McAfee Application Control does not inherently stop vulnerabilities, it does make exploitation of those vulnerabilities significantly more difficult, if not impossible. While only a patch could truly fix the code, potential breaches can be protected in a way that vastly reduces the risk of an attacker being able to make use of them.

Stop the Compromise

McAfee Application Control uses its memory protection to prevent most types of buffer overflow exploitation. This greatly reduces the chance that zero-day vulnerabilities could be effective in code execution. Additionally, many exploits make external calls to binaries. By allowing only solidified binaries to run, the common attacker technique of downloading new code to the system and executing that is automatically prevented.

Stop the Persistence

Since only solidified binaries can run, any attempt at executing a binary that has not been previously approved and solidified will fail. This works during the same session as the attack or even after a reboot. An attack cannot execute a new binary downloaded on disk, and McAfee Application Control prevents an existing binary from being overwritten.

Conclusion

The phase-out of support for Windows XP creates an increased security risk for the many organizations still running the operating systems. Windows XP users no longer receive security patches and are more vulnerable to targeted attacks as a result. McAfee Application Control provides continued protection for Windows XP systems beyond Microsoft's support phase-out by blocking unauthorized applications from running while only impacting system resources slightly. With an effective whitelisting solution in place, IT administrators can address security threats without a full-scale operating system upgrade.

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