Application Whitelisting

Malware increases in volume and variety every day, causing widespread damage and disruption. Malware infects victim systems in a multitude of ways, such as through email, websites, and removable media. Moreover, malware authors are in a never-ending arms race with security professionals. They continuously modify their code to avoid detection, while antivirus vendors update their software daily to detect new variants.

Even the installation of non-malicious, but unauthorized, software applications poses a risk as these may not be included in an organization's regular security configuration and patch management program.

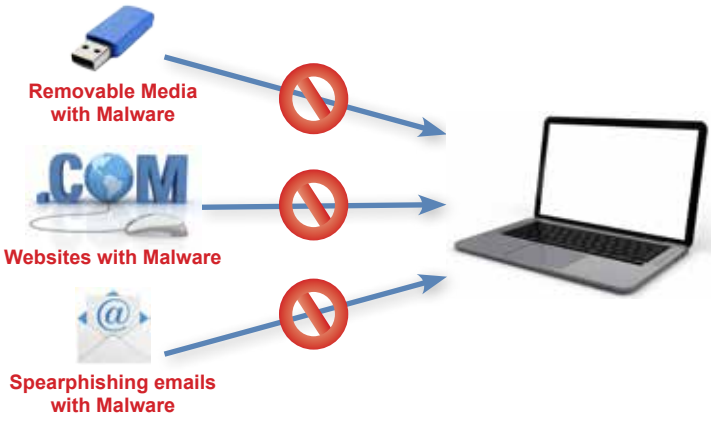
Defending against these threats by blocking all known malware and unauthorized applications arriving via all possible means, a technique known as blacklisting, is a reactive technique that does not scale well and does not protect against unknown malware.

Ultimately, organizations must balance the need to allow users to execute known, trusted applications with the ability to block potentially harmful applications. As part of a multi-layered network defense strategy, Application Whitelisting is an effective, flexible technique for doing just that.

What is Application Whitelisting?

Application Whitelisting is a proactive security technique that only allows a limited set of approved programs to run, while blocking all other programs (including most malware) from running by default. In contrast, the standard policy enforced by most operating systems allows all users to download and run a wide variety of unauthorized (and potentially malicious) applications. Application Whitelisting enables only the administrators, not the users, to decide which programs are allowed to run.

Application Whitelisting is not a replacement for traditional security software, such as antivirus and host firewalls, and should be used as one layer in a defense-in-depth strategy.



Benefits

Application Whitelisting offers tremendous security value:

- Blocks most current malware
- Prevents the use of unauthorized applications
- Does not require daily definition updates
- Requires standardized processes for administrator installation and approval of new application

Location-Based Application Whitelisting

For the best balance of performance, security, and manageability, NSA's Information Assurance Directorate (IAD) recommends employing locationbased Application Whitelisting, which allows execution of programs only from specific locations in the file systems. This approach precludes the need to identify each individual program and executable library. The locations must be protected so that only authorized administrators can install or modify the files to prevent standard users and malicious activities from circumventing the Application Whitelisting policy. These rules have a minimal impact on system performance and allow most program updates and patches to be applied without requiring any rule changes, while preventing the execution of new unauthorized programs and most current malware.

Implementing Application Whitelisting

For Microsoft Windows® operating systems, AppLocker® is a built-in feature that enforces an administrator-defined Application Whitelisting policy. AppLocker policies can be created and managed through standard Windows Group Policy management applications and techniques. AppLocker is available in certain editions of Windows Server® 2012, Windows Server 2008 R2, Windows 8, and Windows 7. It primarily enhances the functionality of the Software Restriction Policies (SRP)® feature included in Windows XP[1]. Some Host Intrusion Prevention System (HIPS) products and host-based security suites also include application control capabilities.

There are several vendors that offer enterprise Application Whitelisting solutions (for example McAfee®, Bit9®)[2]. Most solutions make management of the whitelist easy for administrators, such as enabling the updating of applications, and monitoring and reporting attempted violations of the policy.

When determining an Application Whitelisting deployment strategy and timeline, consider the following potential issues and allow adequate time to investigate and customize your implementation:

- May require performance overhead to enforce the whitelist (varies greatly depending on implementation)
- May require regular maintenance of the whitelist to add new applications and remove ones that are no longer approved
- Requires a change in user behavior because they can no longer download and run applications at will

Additional Information

The Information Assurance Directorate provides Application Whitelisting guidance that contains detailed instructions for developing an appropriate whitelist for a Windows network, configuring AppLocker or SRP, applying the rules across the network, maintaining the whitelist over time, and monitoring the policy enforcement.

For additional information as to how this mitigation relates to a full-spectrum IA plan for your environment, see the System Protection capability in the NSA Community Gold Standard (CGS) (**www.iad.gov/iad/cgs/cgs.cfm**). For technical guidance, see the Executable Content Restrictions network security task in the CGS Technical Guidance: Manageable Network Plan (available at the same link).

[1] Windows®, AppLocker®, Windows Server®, and SRP® are registered trademarks of Microsoft Corp.

[2] McAfee® is a registered trademark of McAfee, Inc. Bit9® is a registered trademark of Bit9.