Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Implementing Application Whitelisting

JANUARY 2018

Introduction

Application whitelisting is one of the most effective mitigation strategies in ensuring the security of systems. As such, application whitelisting forms part of the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents***.

This document provides guidance on what application whitelisting is, what application whitelisting is not, and how to implement application whitelisting.

What application whitelisting is

Application whitelisting is a security approach designed to protect against malicious code (also known as malware) executing on systems. When implemented properly it ensures that only authorised applications (e.g. programs, software libraries, scripts and installers) can be executed.

While application whitelisting is primarily designed to prevent the execution and spread of malicious code, it can also prevent the installation or use of unauthorised applications.

Implementing application whitelisting across an entire organisation can be a daunting undertaking; however, implementation on at least workstations of high-risk users such as senior managers and their staff; system administrators; and staff members from human resources, sales, marketing, finance and legal areas can be a valuable first step.

What application whitelisting is not

The following approaches, while still valuable for defence-in-depth, are not considered to be application whitelisting:

- providing a portal or other means of installation for authorised applications
- using web or email content filters to prevent users from downloading applications from the Internet
- checking the reputation of an application using a cloud-based service before it is executed
- using a next-generation firewall in an attempt to identify whether network traffic is generated by an approved application.

How to implement application whitelisting

Implementing application whitelisting involves the following high-level steps:

- identifying applications that are authorised to execute on a system
- developing application whitelisting rules to ensure only those authorised applications can execute
- maintaining the application whitelisting rules using a change management program.

When determining the method used to specify application whitelisting rules, the use of cryptographic hashes, publisher certificates (combining both publisher names and product names), absolute paths and parent folders are all considered suitable if implemented correctly.

Note, if application whitelisting rules based on absolute paths are used, particular care should be taken to ensure users do not have the ability to overwrite files that have been whitelisted. Likewise, if parent folders are used, particular care should be taken to ensure users do not have the ability to write content in any path that has been whitelisted. In either case, doing so would enable users to bypass application whitelisting. Furthermore, to ensure the integrity of application whitelisting, users and system administrators should not be able to temporarily or permanently disable, bypass or otherwise be exempt from application whitelisting mechanisms.

To ensure application whitelisting has been appropriately implemented, testing should be undertaken on a regular basis to check for misconfigurations of file system permissions and other ways of bypassing application whitelisting rules or executing unauthorised applications.

In addition to preventing the execution of unauthorised applications, application whitelisting can contribute to the identification of attempts by an adversary to execute malicious code on systems. This can be achieved by configuring application whitelisting to generate event logs for failed execution attempts. Such event logs should ideally include information such as the name of the blocked file, the date/time stamp and the username of the user attempting to execute the file.

Finally, it is important that application whitelisting does not replace antivirus and other security software already in place on systems. Using multiple security solutions together can contribute to an effective defence-in-depth approach to preventing the compromise of systems.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

Contact details

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).