Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Implementing Application Control

JUNE 2020

Introduction

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

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

What application control is

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

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

What application control is not

The following approaches are not considered to be application control:

- providing a portal or other means of installation for approved 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 to identify whether network traffic is generated by an approved application.

How to implement application control

Implementing application control involves the following high-level steps:

- identifying approved applications
- developing application control rules to ensure only approved applications are allowed to execute
- maintaining the application control rules using a change management program.

When determining how to enforce application control, the following methods are considered suitable if implemented correctly:

- cryptographic hash rules
- publisher certificate rules (combining both publisher names and product names)
- path rules (ensuring file system permissions are configured to prevent unauthorised modification of folder and file permissions, folder contents and individual files).

Conversely, the use of file names, package names or any other easily changed application attribute is not considered suitable as a method of application control.

To ensure application control 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 control rules or executing unapproved applications.

In addition to preventing the execution of unapproved applications, application control can contribute to the identification of attempts by an adversary to execute malicious code. This can be achieved by configuring application control 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 control 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. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.