Application Whitelisting Explained
IT Security Bulletin for the Government of Canada

ITSB-95

Last Updated: March 2015

1 Introduction

Application whitelisting is one of the Top 10 Security Actions in CSE’s Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information (ITSB-89 Version 3). Implementing the Top 10 Security Actions as a package would prevent the vast majority of the intrusions to which CSE currently responds.

This document provides high-level guidance on what application whitelisting is, what it is not, and how to apply it effectively in a Windows-based environment.

2 Why Implement Application Whitelisting?

Application whitelisting is designed to prevent the execution of unauthorized and malicious programs. It aims to ensure that only specifically selected programs (EXEs) and software libraries (DLLs) are able to run, while no others are allowed to execute.

While application whitelisting is primarily implemented to minimize the execution and spread of malicious software (malware), whitelisting can also prevent the installation or use of unauthorized software.

Implementing application whitelisting across an entire organization can be a challenging undertaking. However, deployment to high-value and often targeted employees can be a valuable first step. High-value and often-targeted employees might include:

- senior executives and their assistants;
- help desk staff, system administrators, and other users with administrative privileges or privileged access;
- users who have access to sensitive information;
- users with remote access; and
- users whose job role involves interacting with unsolicited e-mails from members of the public and other unknown Internet users (e.g., human resources staff, who regularly open e-mail attachments such as job applications).

Additionally, high-value enterprise services such as core application servers (e.g., Domain Controllers, Primary Active Directory, Database servers) could also be considered during the initial deployment of application whitelisting.

3 What is Application Whitelisting?

Application whitelisting comprises the following technical steps:

- identifying specific executables and software libraries that should be permitted to execute on a given system;
- preventing any other executables and software libraries from functioning on that system; and
- preventing users from being able to change which files can be executed.

A less demanding intermediate approach to application whitelisting is identifying entire directories from which users should be allowed to execute programs, such as C:\Windows, C:\Program Files, or even C:\Program Files\Specific Application. This provides some measure of protection from applications executing outside the specified directories but it does not take into account a number of possible scenarios for compromise. This technique is better than not applying application whitelisting at all, but a more comprehensive approach should be considered at the earliest opportunity, such as at the next Standard Operating Environment (SOE) refresh.

4 Common Whitelisting Myths

Providing a portal or other means of installation of a restricted list of approved software (for example, in the way iTunes operates) is not application whitelisting. This does not stop users from running software not listed on the portal, and will not prevent malware from executing and compromising a system.

Application whitelisting is not accomplished by simply disallowing users from writing to locations such as C:\Windows or C:\Program Files. While this may stop a user from installing some software, it does not prevent the execution of software residing in locations such as a user’s desktop or temporary directories. These locations are commonly used by malware to infect a computer.
5 How do you Implement Application Whitelisting?

Application whitelisting is commonly implemented using the combination of a software product that identifies and approves necessary executable and library files, and Access Control Lists that prevent users from changing the approved files. There are various whitelisting programs, also referred to as application control programs, available on the market. For example, some antivirus products are capable of whitelisting applications by cryptographic hash. Free products to whitelist applications are provided with recent versions of Microsoft Windows.

It is crucial that the software selected and the configuration used cover both executables and software libraries, as an omission of either of these could negate the security afforded by whitelisting. Research should be conducted on the different products available to determine the most effective software based on implementation and reviews.

Before implementing a chosen product, it is advantageous to engage in planning and pre-deployment activities; for instance, policy should outline which applications are allowed to run. Additionally, there should be restrictions in place as to which users are permitted to run certain applications. These restrictions should be based on the requirements of each user’s role and responsibilities in the organization.

The most challenging aspect of whitelisting is determining which applications to whitelist by identifying which applications are imperative for business. Once this task is completed, the whitelist software should not require significant upkeep and can be revised as required.

The whitelist’s rules are adaptable and can be edited to match an organization’s needs. They can be automatically generated by the product or created manually. In general, the rules should be applied to a test computer first, and then deployed to a pilot user group. Equally important, whitelisted executables should be positively identified via means other than merely file name or directory location in order to capture malware masquerading as legitimate software.

To assist in implementation, it would be beneficial to initially deploy a test in Audit Only mode. In the Audit Only mode, events that would have been blocked by the application whitelisting, had it been enabled, are logged. In this way, the results can be analyzed to determine whether the proposed application whitelisting design is effective. These event logs include valuable information (application fingerprints) which could also be used during an incident and recovery phase.

Application whitelisting impacts the user’s ability to operate within the computer environment. Thus, users should be made aware of the security reasons behind these changes and provided with support to adapt to their new working environment. Support staff should be advised on how to assist users and respond to their requests and concerns.
The computer environment changes over time (is constantly changing), and it is important to update application whitelisting rules accordingly in order for the application control program to remain effective.

6 Additional Information

The full list of CSE’s Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information as well as a range of supplementary advice can be found at https://www.cse-cst.gc.ca/en/group-groupe/its-advice-and-guidance.

7 Contacts and Assistance

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca