Avecto

How to simply achieve PSN compliance

In this article, security guru Russell Smith reviews the requirements of the UK Public Services Network (PSN) to satisfy audit and compliance requirements.

Introduction

In November 2012, the UK government Public Services Network (PSN) Code of Practice replaced the Government Secure Intranet Code of Connection (GSi CoCo). Based on ISO 27001, the new code is outcome based so that government departments can comply how they see fit, rather than check a list of technical requirements.

The requirements

As a core requirement of the new code, least privilege security is the practice of assigning only the permissions users require to perform their roles. Though least privilege security is widely accepted as best practice, Windows users often work with full administrative rights because of the difficulties associated with running legacy applications, adding new hardware and working with some Windows features under a standard user account.

The PSN Code of Practice includes configuration controls that require government departments to:

- Lockdown software according to policy, and assign the minimum privileges required to use a PSN service
- Prevent the execution of unauthorized software
- Prevent unauthorized changes to the standard build of network device
- Ensure that users give permission before active content can be executed

Step one > Lockdown policy and least privilege security

Least privilege security and OS lockdown can be achieved by removing administrative permissions from end users. Least privilege can also be achieved by using Protected Administrator (PA) accounts in Windows Vista and later, but neither of these solutions can fully satisfy the PSN requirements. Protected Administrator accounts offer some protection by removing administrative privileges from end users most of the time, but Windows User Account Control (UAC) doesn't provide any centralized policy-based control of how elevated privileges are used.

There are many scenarios where removing administrative rights can prove problematic for end users, especially where there is no direct access to IT support, as is increasingly the case with many local authorities and government departments which prefer to issue notebooks to facilitate mobile working. Legacy applications often fail to run without administrative permissions, applications cannot be patched manually, hardware with unsigned drivers cannot be installed, and some Windows features cannot be run.

Microsoft's Application Compatibility Toolkit (ACT) can be used to deploy compatibility shims that solve some of the issues encountered with legacy applications running under standard user accounts. However, compatibility shims require testing and development time, and cannot be used to solve privilege-related issues on the fly.

Avecto Defendpoint enables government departments to overcome the limitations of Windows privilege management to set sophisticated policies that modify the privileges of running processes. Applications, Windows features, Windows Store Apps (previously Metro apps), scripts, batch files, and ActiveX Controls can all be launched with a unique set of assigned rights,

Avecto

without giving users administrator accounts. Defendpoint can be deployed and managed using Active Directory Group Policy, McAfee ePolicy Orchestrator or the cloud-based iC3.

Whilst Microsoft modified UAC, starting in Windows 7, to minimize the number of prompts users see when running as a Protected Administrator, standard users will continue to be confronted by these UAC prompts, generated by Explorer from applications using Component Object Model (COM). Defendpoint's auditing feature can be used to eliminate generic UAC prompts and either replace them with informative, branded messaging or silently elevate processes so that users can continue working without contacting IT.

The difficulties of supporting notebook users when away from the office has traditionally been a block to the adoption of least privilege security. For example, notebook users don't always have connection to the network but may need to perform an operation that is blocked by policy. The challenge/response authorization feature in Defendpoint provides a mechanism that allows IT to respond in situations where policy can't be updated, giving government departments confidence they can meet users' needs in any situation.

Step two > Remove admin rights

Application whitelisting is a technology that blocks the execution of software not listed in a centrally defined policy. Removing administrative privileges from end users is not enough to block all unauthorized software, as a lot of applications are packaged to install to user profiles (sometimes referred to as portable applications), rather than the protected Program Files folder and restricted parts of the system registry. Additionally, application whitelisting enables government departments to be sure that only authorized scripts, batch files and other types of active content can run.

Software Restriction Policy (SRP), which was first introduced in Windows XP, provides basic application whitelisting functionality but has never been widely adopted as it is considered difficult to deploy and manage. Windows Vista introduced a new technology called AppLocker, which considerably reduces the effort required to implement and manage application whitelisting. AppLocker in Windows 10 includes support for Universal Windows Apps (UWAs). Defendpoint's application whitelisting feature offers IT several advantages over AppLocker. Not only does Defendpoint have more flexible creation of rules to match authorized software, it provides a unified system for all supported versions of Windows and a means to monitor the software run on a network and the privileges in use. These features combine to increase the prospect of a successful application whitelisting project, and reduce costs with simplified management.

Step three > Dealing with active content

The ActiveX Installer Service (AxIS) was introduced in Windows Vista and provides on demand installation of permachine ActiveX Controls, using elevated privileges on the user's behalf. The concept of per-user ActiveX Controls was also introduced, allowing IT to package in-house controls so that they can be installed by standard users. The Windows ActiveX Installer Service limits IT to specifying trusted host URLs from which users are able to install all available controlsFor example, if Adobe is listed in policy as a trusted host URL, users can install Flash, Shockwave and any other controls Adobe publishes. AxIS can't be restricted to the installation of specific ActiveX Controls from a given host.

Defendpoint allows IT to define exactly which controls can be installed, and in conjunction with Defendpoint's challenge/response authorization feature, IT can quickly allow users to install controls that are not defined in policy. Other active content, such as scripts and batch files can also be allowed or blocked at a granular level.

Software Restriction Policy (SRP), which was first introduced in Windows XP, provides basic application whitelisting functionality but has never been widely adopted as it is considered difficult to deploy and manage. Windows Vista introduced a new technology called AppLocker, which considerably reduces the effort required to implement and manage application whitelisting. AppLocker in Windows 10 includes support for Universal Windows Apps (UWAs).

Defendpoint's application whitelisting feature offers IT several advantages over AppLocker. Not only does Defendpoint have more flexible creation of rules to match authorized software, it provides a unified system for all supported versions of Windows and a means to monitor the software run on a network and the privileges in use. These features combine to increase the prospect of a successful application whitelisting project, and reduce costs with simplified management.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world's biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto's Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.