Avecto

How to simply achieve Sarbanes-Oxley (SOX) Compliance

In this article, security guru Russell Smith provides an overview of the requirements of SOX and how Defendpoint helps organizations achieve compliance.

Introduction

In response to major accounting scandals such as those that affected Enron, Sarbanes-Oxley (SOX) was passed into US law in 2002. Put simply, it requires that public companies verify the accuracy of their financial information. Specifically, SOX section 404 states that organizations must demonstrate confidence in IT systems that store, transport and process data.

The Act itself doesn't determine what internal controls organizations should use, but COBIT (Control Objectives for Information and Related Technology) outlines best practice and is the most commonly adopted framework by IT departments to meet SOX compliance.

COBIT

COBIT control PO4.11 Segregation of Duties requires organizations to ensure that users' roles are defined in such a way as to minimize the likelihood of a critical process being compromised. Additionally, employees must be prevented from using systems for activities not related to their assigned duties. The removal of administrative privileges and use of application control are critical in achieving these goals.

PO4.11 Segregation of Duties: Implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. Make sure that personnel are performing only authorised duties relevant to their respective jobs and positions.

The Information Systems Audit and Control Association (ISACA), which is responsible for certifying auditors, carried out a study to determine the most important controls required for SMEs to meet SOX compliance. File access privilege controls was ranked in the top five controls and least privilege was identified as the technology required to meet the control requirement.

COBIT Quickstart, a guide to implementing the most critical COBIT controls for SMEs with small IT shops, is available from the ISACA website.

Windows and least privilege security

Least privilege security has been shown to significantly reduce virus and malware infection rates on Windows. Additionally, application whitelisting is necessary to prevent users from installing unauthorized software that could lead to a computer being compromised. Portable applications, some scripts and batch files cannot be blocked by simply removing administrative rights.

To achieve effective least privilege security, organizations need to:

- Remove users from built-in Windows groups, such as Administrators and Power Users.
- Implement application whitelisting to prevent users running unauthorized software.

User Account Control

In the past, users on Windows were assigned administrative privileges because some software didn't work correctly when run by a standard user. Furthermore, some Windows features,

Avecto

such as Disk Defragmenter, can only be started by a user with administrative rights.

Starting in Windows Vista, User Account Control (UAC) brings together a set of technical changes that make it easier to run Windows under a standard user account. Fewer Windows features in Vista (and later operating systems) require administrative privileges; Protected Administrator (PA) accounts remove administrative privileges most of the time, requiring users to confirm the use of admin rights in an elevation prompt in some scenarios. However, UAC is a consumer-orientated technology which denies organizations the control to manage security effectively and meet compliance mandates.

Application control

Software Restriction Policies (SRP), which were first introduced in Windows XP, are difficult to implement and manage, thus preventing widespread adoption. AppLocker in Windows 7 (and later) is a replacement for SRP that provides more flexibility, the ability to scan the OS for installed software and automatic rule creation.

While AppLocker is an improvement over SRP, it doesn't offer the comprehensive control and automation of thirdparty application whitelisting solutions.

Using Defendpoint to meet SOX compliance

Defendpoint's Privilege Elevation and Delegation Management features allow organizations to remove administrative privileges from end users and block unauthorized applications while retaining confidence that all operational needs can be met.

IT can utilize Defendpoint to assign rights to individual processes, applications, scripts, batch files, control panel applets, etc. As a result, if the removal of administrative privileges from users' accounts causes a legacy application to stop functioning correctly, or remote users can no longer perform a maintenance task, the required rights are transparently added to the required process according to centralized policy set by the IT department.

Monitoring privilege use

Defendpoint can monitor PCs and servers to determine which applications and processes are being used and what privileges are required to run them. Gathering this data in advance reduces the chances of users experiencing problems when administrative rights are removed, by ensuring application and process compatibility with standard user accounts is known before least privilege is deployed.

Custom messaging

Unlike UAC elevation prompts, Defendpoint messages can be customized and branded. Not only is this useful for providing users with more information, but helps differentiate genuine messages from those generated by malware. Defendpoint messaging also has multi-lingual support.

Challenge response authorization

One of the biggest challenges of any least privilege project is how to manage notebook users that don't have connectivity to the corporate network. Defendpoint's challenge response authorization feature lets users elevate applications or processes on receipt of an authorization code from IT, ensuring that support can be provided in any situation and unforeseen changes can be authorized by IT even when it's not possible for a device to receive a policy update.

Application control

The combination of privilege management and application control makes whitelisting simple. By removing admin rights and making all users standard users, you can trust the build. This means that trusted locations e.g. program files, operating system are simply allowed to run. Trusted applications e.g. line of business apps, are automatically enabled. Untrusted and unknown applications are blocked, with exceptions managed by highly customized messages to enhance the end user experience.

Reducing the cost of SOX compliance

Whether you choose the Group Policy, ePO (ePolicy Orchestrator) Edition or iC3, Defendpoint can streamline your efforts to remove administrative privileges from end users on PCs and servers. Removing administrative privileges is required for SOX compliance and for the wider aim of delivering an effective security strategy. Least privilege is one of the most effective measures that can be taken against malware, helping to reduce downtime related to unwanted configuration changes, and improving productivity.

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.