Avecto

Achieve HIPAA compliance

The Health Insurance Portability and Accountability Act was passed by US Congress in 1996. In this short article, we take a look at the requirements of HIPAA / HITECH with a simple guide to achieving compliance via the COBIT framework.

About HIPAA compliance

Applying to any organization which processes, stores or manages PHI electronically, HIPAA's security rule requires that access controls are put in place to ensure authorized users only have access to the minimum amount of information needed to perform their job role.

Additionally, the Final Rule of HITECH legislates that any instance of PHI being disclosed without permission is reported to the individuals affected. Should this affect more than 500 individuals the media must also be notified. 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 a commonly adopted framework by IT departments to meet HIPAA compliance.

HIPAA Violating the requirements of HIPAA can prove extremely costly. In 2014, the penalties for noncompliance were reviewed and the Final Rule under the HITECT Act increased the maximum penalty to $1.5 million per year. Penalties are based on the level of negligence and can range from $100 to $50,000 per violation (or per record).

How Defendpoint maps to 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 personnel are performing only authorised duties relevant to their respective jobs and positions.

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

If a user does not have access to an elevated account, there are thousands of applications that will simply not run. In addition, the user will be unable to carry our the most basic of administrative tasks and software installations or updates are limited to portable applications.

Avecto

In most cases, these applications that the user can install are not authorized by the business. Even applications installed to the users profile can still de-stabilize the build.

Windows User Account Control (UAC) was introduced by Microsoft to make it easier to run Windows under a standard user account. However, UAC is a consumer oriented technology which denies organizations the control to manage security effectively to meet a compliance mandate, effectively offering a yes/no solution with limited user flexibility.

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 HIPAA/ HITECH compliance

Avecto Defendpoint allows organizations to remove administrative privileges from end users and block unauthorized applications while retaining confidence that all operational needs can be met.

IT can 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 notebook 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.

01 > 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. This is done by ensuring application and process compatibility with standard user accounts is known before least privilege is deployed.

02 > 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 it helps differentiate genuine messages from those that might be generated by malware. Defendpoint messaging also has multi-lingual support.

03 > Challenge response authorization

One of the biggest challenges of any least privilege project is how to manage remote 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 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.

04 > 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 HIPAA compliance

Whether you choose the Group Policy, McAfee 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 HIPAA 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.