Avecto Whitepaper

Achieving Compliance

Contents

Introduction

As greater emphasis is placed on complying with industry and government regulations, securing data as it passes through personal computer systems is crucial to satisfy auditors and protect systems against data loss and reputational damage.

Organizations can yield quick gains by implementing simple security controls across server and desktop estates. As well as putting your business on the right path to full compliance, total cost of ownership is lowered and end-user productivity improved.

This whitepaper discusses the concept of layered security for desktop computers; why it's needed to meet compliance requirements set out by regulatory bodies and how to overcome implementation challenges to ensure project success.

The best practices outlined in this paper can be used as the foundation for creating baseline security configurations that will be effective at protecting your environment as well as helping you meet these compliance regulations.

Challenges with admin access

Desktop PCs play an important role in Information Systems, allowing users to view, manage, and access critical business data. Therefore, security configuration should be controlled by qualified system administrators or dedicated security teams. If employees log in to PCs with administrative privileges, system-wide settings can be changed that can greatly weaken the organization's security – for example allow the circumventing of security policies, allow the installation of applications, removal of audit trails or the disabling of firewalls.

Admin privileges increase the risk that malware, such as viruses and key loggers, can install without a user's knowledge and steal sensitive information via Internet browsers or other application exploits. Once malware gains administrative access to the network, it can cause far greater damage at the core of the network. The likelihood of unpatched vulnerabilities in the operating system being exploited is greater if users log in with administrative accounts, removing an important layer of defense while updates are queued for deployment.

Challenges with applications

By installing or running applications that are not approved or governed by the business, the risk of software vulnerabilities is increased.

In allowing unknown applications to install and run on a PC you greatly increase the attack surface for malware. The user may unknowingly install malicious software that can steal or encrypt private data. Combined with excessive administrator rights, malware can bury itself deep within the operating system and disable security controls.

Poor quality or unstable applications introduced to the system may also cause issues with performance, and if the IT department is unaware of the software even being installed, they cannot ensure it is legitimate or up to date. Additionally, lack of visibility and control of applications in use across the estate is likely to breach compliance.

Challenges with internet activity

The internet is an essential part of daily business life. However as well as offering opportunities, it presents many challenges in terms of security. With the volume of malware online increasing exponentially, it is often successful in evading anti-virus and firewall defences.

Employees browsing websites carrying hidden threats or opening untrusted documents are becoming direct targets for attackers. Vulnerabilities in Java, Silverlight and Adobe Reader can result in an employee being unknowingly compromised just by viewing a site or document.

So that user productivity is unrestricted, there is a need for internet sites and documents to be isolated from sensitive private data while still being viewable by the user – so that online activity is protected by a safety net.

Approaching defense in depth

When it comes to securing the endpoint it's best to focus on the quick wins first. These are the areas, layered together, that can provide the greatest benefit in the shortest timeframe to produce a defense in depth solution.

Least privilege security

Least privilege security is the principle of granting users only the permissions necessary to carry out their job roles. Least privileged user accounts, sometimes known as standard user accounts, help to mitigate the risks associated with administrative accounts. The use of standard user accounts rather than local administrator accounts not only decreases the risk of data loss and unauthorised access, but improves productivity and reduces costs through better manageability.

The Windows operating system includes a set of technologies under the umbrella of User Account Control (UAC), and are designed to encourage the development of applications that work without the need for administrative privileges. UAC prompts users to give consent or enter administrative credentials when a process needs elevated access to the OS. While UAC is a welcome addition to Windows for home and small business users, it is unsuitable as a business security measure. Due to its inflexibility, UAC prompts cause frustration for users as they are often restricted from performing their day-to-day activities. Additionally, it creates challenges for the IT department when the user tries to complete a task that affects the operating system in some way, resulting in an influx of helpdesk calls or tickets.

Application control

Application control reduces security risk and aids compliance by allowing or blocking applications from running based on defined rules. This allows trusted business applications to run freely while unknown or malicious applications are restricted.

Traditionally it has been difficult to implement whitelisting solutions as all the applications on a system must be individually identified. In the same vein, blacklists can target known problem applications directly and block them from executing.

Application control works best when combined with the removal of admin rights, as it allows the operating system and installed applications to be trusted with simple, broad rules. With a default deny policy that will stop all other user applications from running, IT teams need only deal with exceptions. By controlling the applications allowed to run on an endpoint, you greatly reduce the ability of malware to run and install.

Sandboxing

With the internet representing the greatest window of opportunity for outside threats, malware's stealthy approach often requires no interaction with the user to gain entry. If malware gains entry to the system, any data accessible by the user can be compromised or stolen.

Sandboxing isolates web browsing and downloaded documents so that any malicious threats cannot gain access to the user's data. This technique deals with a variety of common drive-by download and targeted phishing attacks. Because the sandbox prevents malware gaining persistence on the endpoint, it protects organisations from data breaches and provides a last line of defense against web-borne threats.

Meeting compliance standards

The following regulations and mandates are primarily intended to improve security to protect sensitive information from unauthorized access, uphold data integrity and prevent data leakage.

The most commonly implemented regulations can be divided into two categories:

Those that explicitly demand the use of least privilege, application controls or anti-malware/sandboxing security on PCs:

> Payment Card Industry Data Security Standard (PCI DSS)
> MAS Technology Risk Management
> US Government Configuration Baseline (USGCB)
> UK Government PSN Standards

And those that suggest it:

> Sarbanes-Oxley Act (SOX)
> Health Insurance Portability Accountability Act (HIPAA)

In the latter case, auditors interpret the regulations as to require least privilege.

Payment Card Industry Data Security Standard (PCI DSS) v3.0

The current version of PCI DSS, for businesses that process or store credit card data, contains a directive in requirement 7: Restrict access to cardholder data by business need to know, that specifically requires the use of least privilege user accounts. The mandate also specifies preventing users altering or disabling anti-virus software in directive 5, which can be also be achieved with least privilege.

5.3	Ensure anti-virus mechanisms are actively running and cannot be disabled or altered by users
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

MAS Technology Risk Management

The Monetary Authority of Singapore (MAS) Technology Risk Management document specifically refers to the use of least privilege:

11.0.1c	Only grant access rights and system privileges based on job responsibility;
11.2.3c	Restrict the number of privileged users;
11.2.3d	Grant privileged access on a “need-to-have” basis;

Also discussed in the document is the ‘never alone’ principle, which requires at least two people to be present when privileged accounts are used on business-critical systems.

US Government Configuration Baseline (USGCB)

All federal agencies and government contractors are required to comply with the USGCB and is mandated by the Office of Management and Budget (OMB). All users must log on with a standard user account.

PSN Standards

The UK government's Public Services Network (PSN) Standards are based on ISO 27001 and contain six configuration controls that apply to Windows PCs and servers.

Table 2 – PSN Standards configuration controls

01	Hardware and software shall be locked-down in accordance with the organizations lock down policy and is part of an overall risk managed approach so that functionality is limited to what is required for the provision or consumption of the PSN service.
02	The execution of unauthorised software shall be prevented
03	Organizations shall have in place a configuration control process which prevents unauthorized changes to the standard build of network devices and hosts
04	Users shall use accounts with the least privilege required to perform their roles.
05	Customers allowing active content shall be able to demonstrate that this is done as part of an overall risk managed approach. Therefore risks from allowing Active Content shall be understood and appropriate controls shall be implemented.
06	The customer shall implement controls to ensure that executable content shall not be run without the user's active consent' and within the organisation's control.

PSN Standard controls one to three cannot be achieved without control four. Removing administrative privileges, and the use of application whitelisting can satisfy controls one to four. Application whitelisting is necessary to comply with controls five and six by blocking not only executables, but also VBscripts, batch files, PowerShell commands, registry files and Active X Controls.

Sarbanes Oxley (SOX) and Health Insurance Portability and Accountability Act (HIPAA)

SOX and **HIPAA** are high-level directives, so **COBIT** (Control Objectives for Information and Related Technology) is generally used as the technical framework for compliance. There are four controls that pertain to least privilege security:

01 DS 5.3 Identity Management – Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities.

02 DS 5.4 User Account Management – Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

03 DS 5.7 Protection of Security Technology – Make security related technology resistant to tampering.

04 DS 5.9 Malicious Software Prevention, Detection and Correction – Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

Least privilege, application control and sandboxing can be used to achieve compliance of these four Deliver and Support (DS) controls. DS 5.3 talks about business needs, which rarely require users to have administrative access to PCs.

DS 5.7 covers security-related technology, which includes antivirus software, and event logs on PCs that can be tampered with if users have administrative privileges.

Lastly, least privilege, application control and sandboxing are effective preventative measures that defend against malware.

Emerging guidance based on real attack data

The Australian Department of Defence's **Top 35 Strategies to Mitigate Targeted Cyber Intrusion** report, first published in 2011 and updated in 2014, and the SANS Institute/CSIS **20 Critical Security Controls**, represent the first security guides developed from actual attack data gathered by public and private organizations. With this valuable research, improved compliance standards are emerging.

Australian DoD Top 35 Strategies to Mitigate Targeted Cyber Intrusion Report

Based on research of attack techniques carried out from 2010 to 2013, the Australian DoD concluded that at least 85% of cyber-attacks could have been prevented if its top four recommendations had
been followed.

The top four strategies are:

- Use application whitelisting to help prevent malicious software and other unapproved programs from running.
- Patch applications such as PDF readers, Microsoft Office, Java, Flash Player and web browsers.
- Patch operating system vulnerabilities.
- Minimize the number of users with administrative privileges.

The Australian government has initiated programs based on the report's advice to great effect. Government employees are now only allowed to run authorized (whitelisted) applications and administrative rights have been removed where possible.

> "In a properly designed, administered and maintained environment there is no requirement for any user to have administrative privileges on their day-to-day account. When properly planned and executed, minimizing administrative privileges can have significant flow on benefits to the stability and consistency of the computing environment, simplifying administration and support of that environment."
>
> Australian DoD

10 Steps to Cyber Security –published by GCHQ, BIS and CPNI
The UK Government and intelligence agencies provide advice for helping private sector businesses minimise the risks to company assets. Their report states that around 80% of known attacks would be defeated by embedding basic information security practices to manage people, processes and technology.

The report recommends businesses should take steps to review, and invest where necessary, to improve security in 10 key areas. This advice includes managing user privileges, monitoring and malware protection.

10 Steps to Cyber Security

01 Home & mobile working
02 User education & awareness
03 Incident management
04 Information risk management regime
05 Managing user privileges
06 Removable media controls
07 Monitoring
08 Secure configuration
09 Malware protection
10 Network security

SANS Institute/CSIS – 20 Critical Security Controls
Many compliance codes are based on the SANS/CSIS 20 Critical Security Controls. While the controls do not represent a specific compliance mandate, the controls were created to help organizations prioritize and reinforce the technical aspects of existing regulations and in no way contradict current mandates.

CIOs can use the 20 controls as a foundation for creating a secure baseline configuration for devices in an organization, and as a starting point for adopting the information security recommendations outlined in **NIST** (National Institute of Standards and Technology) Special Publication 800-5.

> “Managing User Privileges: Establish account management processes & limit the number of privileged accounts. Limit user privileges & monitor user activity. Control access to activity & audit logs.”

10 Steps to Cyber Security

Table 1 – SANS/CSIS 20 Critical Security Controls

01	Inventory of authorized and unauthorized devices
02	Inventory of authorized and unauthorized software
03	Secure configurations for hardware and software on laptops, workstations, and servers
04	Continuous vulnerability assessment and remediation
05	Malware defences
06	Application software security
07	Wireless device control
08	Data recovery capability
09	Security skills assessment and appropriate training to fill gaps
10	Secure configurations for network devices such as firewalls, routers, and switches
11	Limitation and control of network ports, protocols, and services
12	Controlled use of administrative privileges
13	Boundary defence
14	Maintenance, monitoring, and analysis of security audit logs
15	Controlled access based on the need to know
16	Account monitoring and control
17	Data loss prevention
18	Incident response and management
19	Secure network engineering
20	Penetration tests and red team exercises

Steps to achieving compliance

As there are many common threads in the guidance available, the top four strategies from the Australian DoD Top 35 Mitigation Strategies report represent a good starting point for organizations embarking on compliance or for reviewing /validating security controls.

Patching applications and the operating system

Reports on mitigating security risk often single out the particular importance of patching common applications that are frequently targeted due to their ubiquitous nature. All applications listed can be installed with their own proprietary patching mechanisms enabled, but this often requires user intervention to approve updates. The exceptions are Microsoft Office and Internet Explorer, which can be patched using Microsoft's robust and manageable Windows Update service. In Windows 8, Flash Player is integrated into Internet Explorer, so is automatically patched by Windows Update.

Minimizing the number of users with administrative privileges

Just as many information assurance policies grant access to data on a 'need to know' basis, in system security, we should grant access based on a least privilege approach, or 'need to do' basis. As such, standard users should not be granted administrative privileges they don't need to perform for everyday computing tasks. This approach not only prevents accidental change to critical system configuration, which could render a device insecure or unstable, but also prevents cyber-attacks, blocking over 90% of attack vectors on known critical vulnerabilities in Windows 7.

Application whitelisting

Least privilege security is not limited to the removal of administrative rights; to be completely effective, users must also be prevented from running code that hasn't been tested and approved internally. It is all too easy for programs to be downloaded from the Internet, sometimes without a user's knowledge or consent, and for them to sit silently in memory without being detected or requiring administrative privileges to run.

Application control (or whitelisting) allows organizations to restrict users to running programs from a portfolio of tested and supported software, reducing the risk of malware and allowing the IT department to regain control and visibility of application usage in the business. In much the same way as the curated app store on an iPad provides a superior user experience by supplying only secure, quality applications for everyday tasks and entertainment purposes, application whitelisting can help provide the same assurances in the enterprise.

Meeting compliance requirements with Avecto Defendpoint

Avecto's modular endpoint protection suite, Defendpoint, uniquely combines the technologies of privilege management, application control and sandboxing to protect the operating system, software environment and user data from unknown cyber threats.

Defendpoint empowers employees to be free, without security compromise. Complementing existing patching and antimalware strategies, it offers strength and depth across both desktops and servers as a holistic solution to endpoint security.

Privilege Management
Eliminate admin rights
Assign privileges directly to applications
Protect against insider threats

Application Control
Block unauthorized applications
Handle diverse user needs flexibly
Defend against zero day and targeted attacks

Sandboxing
Capture web-borne threats
Isolate untrusted activity
Secure your data from malware

Implementing security with confidence

IT departments can remove administrative rights from user accounts with confidence in the knowledge that Defendpoint can be used to quickly and easily elevate privileges for specific processes. If additional programs are needed, the user can request access easily and if a malicious document is opened from the internet the threat is contained. Defendpoint's pre-built templates allow Windows tasks to be quickly located and privileges granted as required. For example, you could allow a remote worker to change network settings or add a printer while still preventing them from downloading and installing untrusted applications.

Benefits

- Line-of-business applications continue to work correctly
- Users can change system configuration required for everyday tasks
- Updates and approved software can be installed without helpdesk intervention
- Device Manager can be run to install device drivers
- Users can complete approved everyday tasks that require admin rights in Windows (e.g. installing a printer)
- Advanced users can request access to complete advance tasks or run new software
- Unknown and untrusted applications are detected and blocked
- Unknown websites and documents are contained within a sandbox
- Positive user experience with clear customizable messaging and flexible options for requesting access

Conclusion

Least privilege, application control and sandboxing strategies are critical components in any regulatory compliance project. Microsoft's effort to reduce the reliance on administrative privileges and improve application compatibility with standard user accounts via User Account Control has been successful to a point, but challenges persist for organizations that require additional flexibility. Without a flexible solution to manage applications on the endpoint, efforts often result in reduced productivity for the user and resource implications for IT.

Layering security technologies is an effective means of achieving compliance as part of an organization's wider security strategy, protecting PCs against malware, unwanted changes to standard system images, and curbing unwanted software. By taking a proactive, positive approach to endpoint control, security can become an enabler of creativity, productivity and profitability.

About Avecto

Avecto is an innovator in endpoint security.

Founded in 2008, the company was established to challenge the status quo that effective security leads to user lockdown. This philosophy of security + freedom promotes a positive user experience across every software implementation, allowing organizations to strike just the right balance.

Its unique Defendpoint software makes prevention possible, integrating three proactive technologies to stop malware at the endpoint. This innovative software has been implemented at many of the world's most recognizable brands, with over 8 million licenses deployed.

Attention to detail is paramount, with a team of qualified and experienced technology consultants to guide clients through a robust implementation methodology. This consultative approach provides clients with a clearly mapped journey against measurable objectives to ensure project success.

The company has placed in the top four of the Deloitte Fast 50 for the last two consecutive years, making it one of the UK's fastest growing software companies as well on the global stage.

Deloitte. Technology Fast50 UK 2014

UKtech awards 2015

winner Cyber Security Awards

intel Security Innovation Alliance

Microsoft Partner Gold Application Development