ivanti

How Ivanti® Security Controls Can Help You Achieve Cyber Essentials Certification

Contents

Introduction

Cyber Essentials (https://www.cyberessentials.ncsc.gov.uk/) is a UK Government-backed certification scheme designed to help you better protect your organisation, whatever its size, against a broad spectrum of the most common cyber-attacks, as well as demonstrate your commitment to cyber-security.

The truth, however, is that meeting the requirements of Cyber Essentials can be time consuming and costly. The purpose of this white paper is to help ease the headache by providing information about Ivanti® Security Controls, a set of proven security capabilities or basic technical controls that help organizations in their efforts to protect themselves against common online security threats—and that help simplify the achievement of Cyber Essentials certification.

Cyber Essentials certification requires that you implement these five key controls as advised by the National Cyber Security Centre:

1. Configure and use a firewall to protect all your devices, particularly those that connect to public or other untrusted Wi-Fi networks.
2. Ensure only necessary software, accounts, and applications are used.
3. Control:
    a. access to your data through user accounts;
    b. that administration privileges are only given to those that need them; and
    c. that what an administrator can do with those accounts is controlled
4. Implement at least one of anti-malware, whitelisting, or sandboxing to defend against malware.
5. Keep your devices, software, and apps up to date, also known as ‘patching’.

Controls 1 and 2 above are not the main focus of this white paper, but are discussed briefly in this introduction:

1. Configure and use a firewall to protect all your devices, particularly those that connect to public or other untrusted Wi-Fi networks.

Firewalls are included by default as part of the Windows Operating System and, in a typical enterprise, will be supplemented by network-based firewalls. This effectively creates a ‘buffer zone’ (closes doors) between your IT network and other external networks. Firewall settings can be managed locally on each endpoint or centrally via an endpoint management solution.

2. Ensure only necessary software, accounts, and applications are used.

Within this context, it’s important to choose the most secure settings for your devices and software applications. Manufacturers often set the default configurations of new software and devices to be as open and multi-functional as possible. They come with ‘everything on’ to make them easily connectable and usable. Unfortunately, these settings can also provide cyber attackers with opportunities to gain unauthorised access to your data, often with ease. Reviewing and remediating these settings is a part of typical security housekeeping. Cyber Essentials recommends that you:

- Check the settings of new software and devices.
- Make changes which raise your level of security (for example, by disabling, controlling, or removing any functions, accounts, or services which you do not require).
- Configure password-complexity levels and expiry dates.

Mapping Ivanti Security Controls to Requirements 3, 4 and 5 of Cyber Essentials

The balance of this white paper focuses on Cyber Essentials Requirements 3, 4, and 5—and how Ivanti Security Controls can support your efforts to achieve Cyber Essentials certification.

Ivanti Security Controls brings together best-in-breed technology from across the Ivanti security portfolio into a single platform. Building on decades of market experience, Ivanti Security Controls delivers:

- A layered, modular defence-in-depth security solution to provide a solid baseline protecting against security threats
- Simplified workflow with automated security processes that reduce the burden on system administrators while also improving response times for security issues
- Security without adversely impacting user or business productivity

Requirement 3: Control Who Has Access to Your Data and Services

Privilege Management refers to the process of managing who or what has administrative privileges on the network. The misuse of these privileges is a primary method for attackers to spread inside the target enterprise.

Giving users full admin privileges introduces several costly IT challenges, when the original reason for providing admin rights may be trivial. By providing users with full administrative privileges, IT effectively gives the user 'the keys to the endpoint'. This makes endpoint management incredibly difficult, as the user now has complete control over their own system. Any applications that run do so with admin-level privileges. If the user introduces malware inadvertently, for example, by clicking on a link in a phishing email, this malware also runs with administrative privileges, which can be far more damaging than if it runs with standard privileges.

To minimise the potential damage that could be done if an account is misused or stolen, staff accounts should have "least privilege" or just enough access to software, settings, online services, and device connectivity functions for them to perform their role. Extra permissions should only be given to those who need them. "Least privilege" needs to be done in a balanced way to minimize the impact on end users.

Ivanti Security Controls provides privilege management capabilities within the Application Control features of the Security Controls solution. Privilege management helps control who has access to your data and services.

Capability	What It Does
Elevate user privileges for running specific applications	There are two schools of thought when it comes to Windows privilege management. The first is to remove admin-level access and elevate standard users, where needed, which is the approach Ivanti recommends. This functionality allows IT admins to specify which applications can run with admin privileges for specific users. Full admin privileges can then be removed from the user, yet the user can continue to perform needed tasks, with elevated privileges only where required.
Elevate user privileges for running specific Control Panel applets and system controls	Windows privilege management also allows Control Panel applets and system controls to run with elevated privileges. This means that in instances where full admin rights may have been given previously, the user's privileges can now be elevated so that a task such as stopping or starting a service can still be carried out without users being Admins.

Reduce privileges to restrict the rights that applications can run with	The other approach to Windows privilege management is to reduce privileges so users can retain the rights they have currently, but also ensuring that certain applications don't run with admin credentials. While removing admin credentials is a security best practice, this isn't always possible for practical or political reasons. Reducing privileges can be a simpler option in the short term to removing admin rights across the board and can help with a phased rollout of privilege management.

Requirement 4: Protect Yourself from Viruses and Other Malware

Viruses and other malware are an ever-present danger in today's complex computing environment. There are many types of malicious software that can cause damage ranging from the trivial to the catastrophic.

Without question, the threat is constantly evolving, with new forms of malware being identified on a daily basis. The source of the threat is also changing. Previously, creators of malware were often misguided enthusiasts keen to prove how clever they were. Much of today's malware is created by people with a more sinister agenda, including cyber-criminals who want to access corporate and personal data for financial gain. There are, however, well-defined technologies and strategies for dealing with the threat posed by malware.

You may have an antivirus solution already**, yet Ivanti Security Controls enables you to further reduce your risk through Application Control—one of the most effective defences against viruses and other malware.**

Capability	What It Does
Application Control	Ivanti Application Control prevents attacks, including advanced persistent threats (APTs) by providing visibility into, and control over, what applications can execute in your environment, and prevents modified applications from executing. It protects endpoints automatically without the need for complex configurations and constant management. It achieves this through a technique called Trusted Ownership checking that enables you to block ransomware, spyware, malicious mobile code, and other web-based threats, including executable-borne viruses, Trojan horses, worms, keylogging, script attacks, and rogue internet code.

More about Trusted Ownership checking	Application Control reduces the manual overhead of traditional whitelisting. Trusted Ownership checking provides enterprise-wide desktop/laptop protection both inside and outside of the corporate network, providing a valuable layer of security for a mobile workforce. It prevents user-introduced, unauthorized applications, preserves the integrity of gold-build images, and increases user productivity by refocusing resources back on business applications. It alleviates the IT burden associated with other application control solutions that require ongoing maintenance of whitelists, such as Microsoft AppLocker.

Requirement 5: Keep Your Devices and Software Up to Date (Patching)

With security breaches the new normal, the rush is on to implement effective security practices and ensure proper patch compliance. With the rising number of vulnerabilities in third-party applications, this includes implementing solutions that

install critical security updates for more than just Microsoft products. Writing for *Intelligent CISO*, 25 July, 2019, Jess Phillips reports: "According to research, 60% of organizations that experienced data breaches in the last two years attributed the breach to an unpatched vulnerability—so it has never been more necessary to stress the important of good patch management."

But whether your machines are behind the firewall or remote, physical or virtual, patching your critical operating systems and applications quickly and cost-effectively remains challenging—due in part to the sheer number of vulnerabilities being disclosed currently. For example, according to a report from Risk Based Security in 2018, around 22,000 vulnerabilities were disclosed and this number has continued to grow each year.

To be successful, you must have a systematic approach to applying patches and employ automation where possible.

Once a vulnerability is disclosed, it's a race against time between the time it takes to apply the associated patches in your environment and the time for that vulnerability to be exploited. That risk of exploitation increases over time and, after just two weeks, it starts to increase significantly.

In 2018, according to the Verizon Data Breach Investigation Report, within two to four weeks of a vulnerability being disclosed, 50% of vulnerabilities that would eventually be exploited already had been. However, the average time to patch in 2018 was 34 days.

That gap from 14 days to 34 days (or longer) creates opportunities for systems to be compromised through phishing attacks and other techniques. In the case of WannaCry in 2017, Microsoft released security bulletin MS17-010 on March 14th that year to fix a vulnerability in the Server Message Block for its supported operating systems. Many organisations went ahead and applied this patch as part of their normal patching cycle over the following weeks. However, on May 12th, more than eight weeks later, WannaCry infected more than 230,000 computers across at least 150 countries in less than one day. If these systems had been patched, these infections would not have been possible.

Ivanti Security Controls provides industry-leading automated patching that spans not only physical and virtual Windows servers but workstations as well. The solution also features patch support for Red Hat Enterprise Linux and CentOS.

Capability	What It Does
Patch your virtual servers	Finds online and offline workstations and servers, scans for missing patches, and deploys them. Patches everything from the OS and apps to virtual machines (VMs) and even the ESXi hypervisor with the product's deep integration with VMware. Even offline virtual images can be kept in a constant state of readiness to be deployed. (You don't want to go through the two-step process of creating a VM and having to patch it. If offline templates are always kept current, you can deploy a VM without worrying if it's up to date.)

Patch without an agent	Agentless technology lets you assess and deploy patches to the workstations and servers connected to your network while minimizing the impact on both your team and system workloads. Alternatively, you can use the agent to create as many different agent policies as necessary to manage your network, offering significant patching flexibility, and to provide a higher degree of patch accuracy in environments where devices aren't connected to the network continuously. Assign different agent configurations to different devices in your organization.

Patch your Windows and Linux machines	Having patch management software that can handle today's heterogenous environments is a necessity. Extending patching beyond Windows is a must. And doing this efficiently, using a single interface and automated tool, frees up IT and reduces human error while enhancing your defenses.

Patch your applications	What do hackers target most? Third-party applications and browser add-ons such as Adobe Acrobat Flash and Reader, Google Chrome, Mozilla Firefox, and Oracle Java. Ivanti Security Controls provides the largest catalog of tested patches in the industry, saving you time to focus on core business goals.

By utilising a set of patch best practices, you can ensure you're covered—with reporting to back it up. Here is a full list of vendors and applications which can be patched by Ivanti Security Controls.

Ways to Learn More

Please visit the Ivanti Security Controls web page for more information. Register here if you would like to see a live demo of Ivanti Security Controls delivered by one of our security experts. Or, if you would like to try it out for yourself, you can request a 60-day trial licence.