WHITEPAPER

Meet the Requirements of the UK Government Cyber Essentials Scheme

BeyondTrust

Table of Contents

What is the Cyber Essentials Scheme?

Businesses are at greater risk than ever before from cyberattacks, but a lack of resources, expertise and awareness has left them vulnerable. Yet small businesses have largely considered themselves to be at less risk than large corporations or government, either because they don't believe they have any information of value, or that they are not high-profile enough to warrant interest from hackers.

Recognizing the potential losses that a security breach can involve for SMEs, the UK government has launched a simplified version of its 10 Steps to Cyber Security, providing five achievable goals that it believes both small and large businesses should implement to secure their IT systems.

Cyber Essentials Plus

The Assurance Framework provides two certifications, Cyber Essentials and Cyber Essentials Plus, that SMEs can obtain with minimum effort and at low cost. Cyber Essentials Plus offers greater assurance through external testing of the implemented controls, and both certifications involve completing a questionnaire that is approved by a company executive, and then verified by an independent certification body.

The five clear goals outlined in the Cyber Essentials scheme are:

1. Use a firewall to secure your internet connection - personal or boundary firewalls are devices designed to prevent unauthorized access to or from private networks, but good setup of these devices either in hardware or software form, is important for them to be fully effective.

2. Choose the most secure settings for your devices and software - full administrator rights are often the default setting on new devices, but not the most secure. Default passwords should be changed, and MFA implemented where possible.

3. Control who has access to your data and services - ensuring only those who should have access to systems have access and at the appropriate level without increasing risk. IT systems should have full audit trails and session playback capabilities.

4. Protect yourself from viruses and other malware - ensuring that virus and malware protection is installed and is up to date.

5. Keep your devices and software up to date – ensuring all devices are kept up to date for security and functionality of the application or device. These updates should be applied as soon as they are released.

Mapping BeyondTrust Solutions to Cyber Essentials

This guide can be used by IT and Security Administrators to quickly understand how BeyondTrust solutions for privileged password management, secure remote access and endpoint privilege management map into the UK government recommendations outlined in the Cyber Essentials/ Cyber Essentials Plus scheme.

1. Use a firewall to secure your internet connection

Devices that protect the network edge, such as routers and firewalls, can fail to provide adequate protection if configured incorrectly. Factory settings, such as blank or default administrator account passwords, can provide an easy point-of-entry for hackers. Additionally, network rules that allow inbound traffic should always be approved and documented by a qualified member of IT staff, and rules that are no longer required removed as soon as possible.

Access to the administrative interface, whether via a web GUI or command-line console, should be restricted to approved devices on the internal network. If external access to the admin interface is required, additional precautions should be used, such as SSL encryption and SSH with certificates to authenticate hosts and clients.

BeyondTrust Privileged Remote Access is designed to secure access to these critical systems for Internal Staff or Vendors. Privileged Remote Access provides a powerful web-based platform where users can sign in and only access the endpoints required to do their job. Give users access, not a VPN. In addition, no software is required. Privileged credentials can be managed and injected into the session from the built in Vault. Each session that takes place is fully recorded and documented within the appliance to provide that full detailed audit trail.

2. Choose the most secure settings for your devices and software

Many Operating Systems are often shipped in a fairly secure state in terms of configuration, but as soon as default settings are changed or third-party software installed, the potential attack surface may increase significantly. Following some simple best practices can ensure that Windows, Mac, Linux, and Unix based devices stay secure.

These devices are often used outside the protection of the corporate network, so an endpoint firewall is critical for ensuring devices remain secure when connected to the public internet or untrusted network. Native, built in Firewalls, or a third-party firewall that's part of an endpoint security suite, should always be enabled on each device, following the same advice about approving the addition of firewall security rules that applies to network-edge security devices.

Guest user accounts should be disabled, and accounts should be properly secured with strong, unique passwords.

Many devices come set up with administrator or sudo rights, and many organizations choose to leave these unchecked for ease and to maintain user productivity. On the contrast, if IT removes administrator rights, they usually see an increase in IT incidents requesting elevation to install software, or even make basic changes to the endpoint like changing the power settings. This practice introduces risk, as users may attempt to find workarounds.

BeyondTrust Password Safe is designed to discover, manage, audit, and monitor privileged accounts of all types. Privilege accounts are pretty much everywhere, and they are growing. Examples of privileged accounts could be Windows domain or local administrators. In the *nix environment these are root users. In addition, there are also privileged accounts within infrastructure devices like Routers, Switches and Servers. That's without mentioning application privileges too.

Password Safe continuously and automatically discovers privileges across your estate. Using Smart Rules, administrators can automate the onboarding and management of these credentials to keep them secure. Checkout requests can be performed in native tools like Putty or Remote Desktop Manager, where full session recording and keystrokes are captured.

3. Control who has access to your data and services

The hardest goal to achieve on the list, the Cyber Essentials Scheme requirements state that administrative accounts should not be used on devices with internet access, or for reading email, which rules out assigning administrative privileges to most employees. But this can pose a challenge when running legacy applications, and sometimes admin rights are required to perform system tasks.

BeyondTrust Endpoint Privilege Management enables organizations to remove excessive privileges across their estate, and only elevate the tools and processes required for an individual to complete their task based on flexible working styles. Applications and processes can be assigned the necessary rights, while leaving logged in users with standard user privileges. This ensures a much higher level of security, meeting the scheme requirements as well as ensuring that users remain productive.

Additionally, exception-handling capabilities such as Challenge/ Response codes can be used to ensure users have flexible options to request the access they need, with auditing and reporting options that can be used to ensure policy rules are created to suit individual users or groups.

4. Protect yourself from viruses and other malware

The Cyber Essentials scheme strongly advocates whitelisting. This can be used to prevent users installing and running applications that may contain malware. Just as is the case with firewalls, misconfiguration of antivirus software can render it ineffective.

The Cyber Essentials Scheme necessitates that all devices connected to the internet be protected by malware protection software, and that the software and signature files should be updated at least daily.

The whitelisting process involves an administrator creating a list of applications allowed on a device. Any application not on this list will be blocked from running. This is a strong protection as it works even if the malware is undetectable to anti-virus software.

According to Ponemon's Study on the State of Endpoint Security Risk, anti-virus software misses 60% of malware, a risk that can be mitigated by removing admin rights.

BeyondTrust Endpoint Privilege Management Quick Start policy delivers rapid time-to-value in achieving this and reduces business disruption - meaning you have the ability to implement least privilege overnight, with minimal ongoing maintenance required thereafter.

5. Keep your devices and software up to date

Manufacturers and developers release regular updates which not only add new features, but also fix any security vulnerabilities that have been discovered. Applying these updates (a process known as patching) is one of the most important things you can do to improve security. Operating systems and applications should all be set to 'automatically update' wherever this is an option.

The importance of timely patching (and the removal of admin rights mentioned in number three) is explained in detail in our annual Microsoft Vulnerabilities Report. Vulnerabilities are constant, and over the last five years, our report shows that vulnerabilities have increased by 64%, hitting a record high in 2019.

The Cyber Essentials Scheme also requires that the operating system and third-party software be licensed, supported, and updated automatically, or within thirty days of a patch being released; with the exception of security patches, which must be installed within fourteen days of release.

Case study: University of Derby Achieves Cyber Essentials Certification with BeyondTrust

University of Derby is a public university based in the city of Derby, United Kingdom. With more than 7,000 Windows and Mac machines and 500 mobile devices, University of Derby relies on BeyondTrust Endpoint Privilege Management to help manage privileges on these devices campus wide.

The university has achieved Cyber Essentials Certification by using BeyondTrust Endpoint Privilege Management. Ransomware vulnerability has been reduced to zero, and they have empowered their users to be able to run software updates securely.

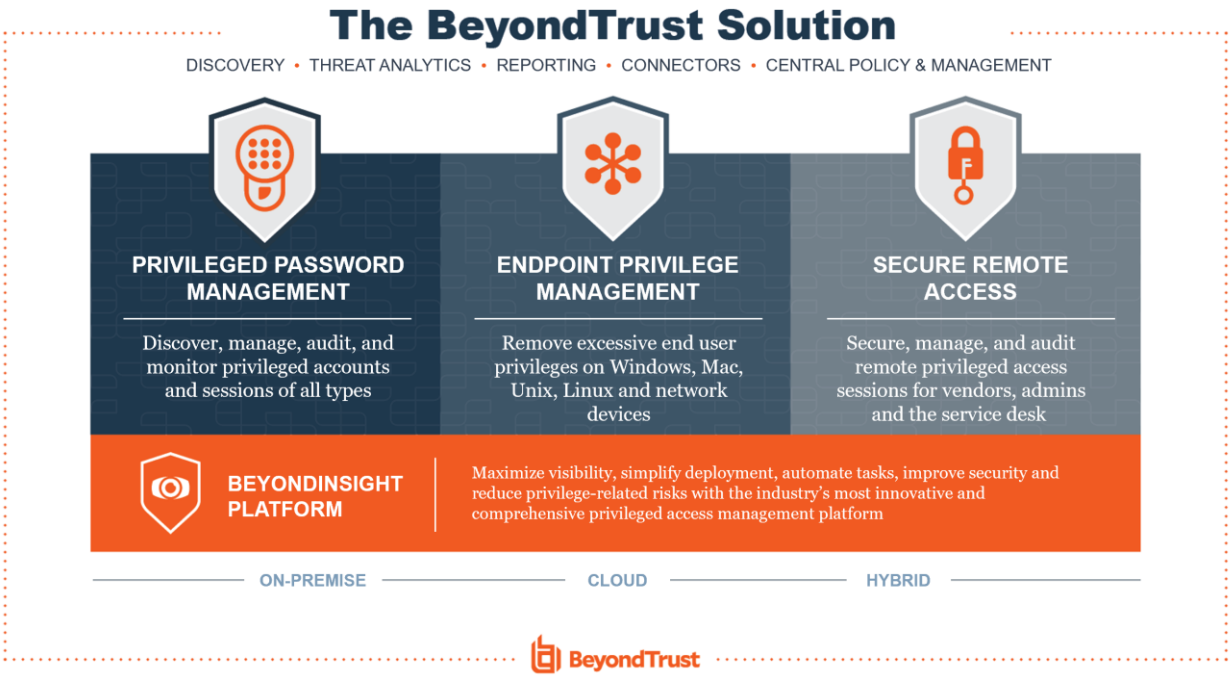
Ryan Powell, Operations & Response Centre Manager, states that "We've got a team of six engineers who manage the entire desktop and mobile estate, so we needed something that was really going to empower them to get the job done in as quick and efficient way as we can."

View the full case study video here.

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the Forrester Wave Privileged Identity Management, Q4 2020, BeyondTrust is named as a leader and ranked as the top Vendor in the strategy category.
BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.