



Cyber Essentials and Cyber Essentials Plus – Your guide to compliance through identity protection

Whitepaper



Executive summary

In this whitepaper, you will learn how the Silverfort Identity Security Platform can help organisations comply with the latest iteration of the Cyber Essentials and Cyber Essentials Plus certification assessment. Silverfort's key mitigations in both frameworks focus on restricting user access and enforcing multi-factor authentication. Silverfort also provides additional advanced capabilities within these two groups that go beyond the scope of Cyber Essentials and Cyber Essentials Plus.

Security stakeholders that need to comply with both Cyber Essentials and Cyber Essentials Plus can learn how to:

- Implement identity security controls with Silverfort
- Strengthen their security posture following the frameworks
- Gain insights into key attack surfaces, such as ransomware, lateral movement and service account protection

Part 1: Overview

What is the Cyber Essentials Model?

The Cyber Essentials model was introduced in 2014 as part of the UK government's National Cyber Security Strategy. It is a cybersecurity certification framework aimed at providing a clear set of guidelines and best practices for organizations to protect themselves against common cyber threats. Its primary goal is to help organizations implement essential cybersecurity controls and improve their overall cybersecurity resilience, regardless of their size or industry.

The Cyber Essentials model has five “core control” areas that provide a baseline level of protection against common cyber threats. By implementing these controls effectively, organisations can significantly reduce the risk of successful cyber attacks.

These core controls include:

- 1 Boundary firewalls and internet gateways
- 2 Secure configuration
- 3 Access control
- 4 Malware protection
- 5 Patch management

What is Cyber Essentials Plus?

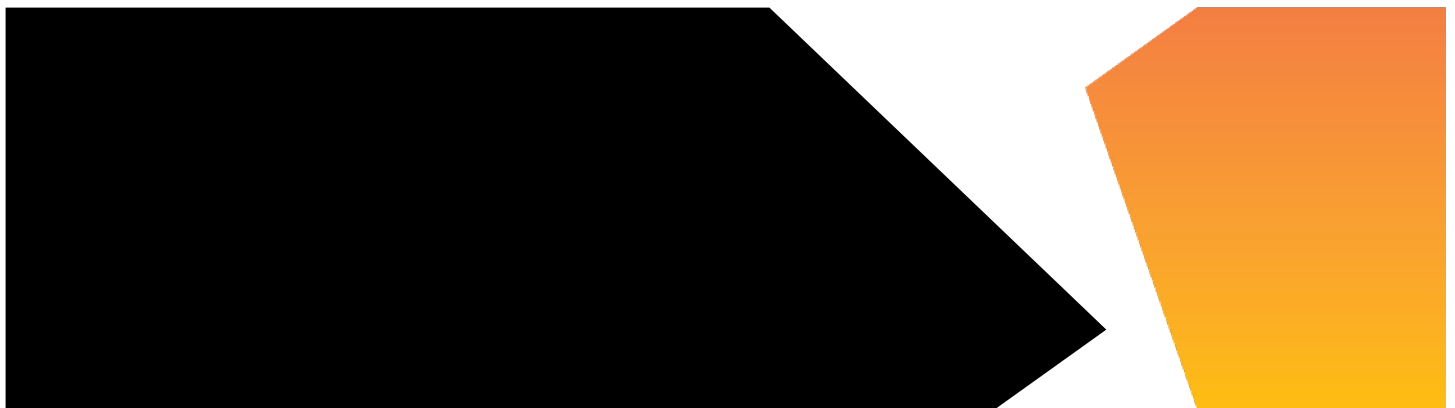
Cyber Essentials Plus is an advanced level of certification within the Cyber Essentials scheme. It builds upon the requirements of the basic Cyber Essentials certification and includes additional verification through independent testing and vulnerability assessments.

To achieve Cyber Essentials Plus certification, organisations must undergo a more rigorous evaluation of their cybersecurity posture.

Here's an overview of the process:

- 1. Cyber Essentials:** Organisations must first meet the requirements of the basic Cyber Essentials certification.
- 2. Independent testing:** In addition to meeting the basic Cyber Essentials controls, organizations must undergo independent testing of their systems and networks. This testing is typically performed by a certified external cybersecurity provider or an internal team that meets the necessary requirements.
- 3. Vulnerability assessment:** The independent testing includes a vulnerability assessment of the organisation's systems and networks. This assessment aims to identify potential vulnerabilities or weaknesses that could be compromised by attackers. The assessment may involve a combination of automated tools and manual techniques to thoroughly analyse the organisation's security posture.
- 4. On-site assessment:** In most cases, Cyber Essentials Plus certification also involves an on-site assessment. A qualified assessor visits the organisation's premises to validate the implementation of cybersecurity controls, conduct interviews with personnel, and gather evidence to support the certification process.

By achieving Cyber Essentials Plus certification, organisations can demonstrate a higher level of cybersecurity maturity and assurance. It provides an additional layer of confidence to stakeholders, clients, and partners, indicating that the organization has undergone more extensive testing and evaluation of its cybersecurity measures.



What is the difference between Cyber Essentials and Cyber Essentials Plus?

Cyber Essentials is based on a self-assessment questionnaire where organizations evaluate their compliance with essential technical controls. It focuses on implementing five core controls to protect against common cyber threats. The certification is verified by a certification body, but there is no independent testing or on-site assessment.

Cyber Essentials Plus provides a higher level of assurance by involving independent testing and on-site assessments conducted by qualified assessors. In addition to the essential technical controls, Cyber Essentials Plus includes rigorous evaluation through vulnerability scans and penetration testing. This thorough assessment verifies the effectiveness of the implemented controls and provides enhanced assurance regarding an organization's cybersecurity defences and resilience. Cyber Essentials Plus is often chosen by organizations seeking a more comprehensive certification or when working with clients or contracts that require a higher level of cybersecurity assurance.

While Cyber Essentials is a valuable starting point for basic cybersecurity practices, Cyber Essentials Plus provides an extra layer of validation and assurance. It is particularly beneficial for organisations that handle sensitive data, work with government contracts, or want to showcase a robust cybersecurity posture where a more rigorous certification is required. Cyber Essentials Plus certification demonstrates a proactive commitment to cybersecurity and can provide a competitive advantage in the marketplace.

What parts of the Cyber Essentials and Cyber Essentials Plus does Silverfort address?

The Silverfort Identity Security Platform assists organisations in complying with two sets of mitigation strategies:

- **Access control** – Silverfort's continuous authentication capabilities monitors and analyses user behaviour during active sessions. Silverfort can detect anomalous actions or suspicious activities in real time. If any unauthorised or abnormal behaviour is identified, the system can take immediate action, such as terminating the session or requesting additional authentication.
- **Multi-factor authentication** – Silverfort fully addresses all the required access controls outlined in the Cyber Essentials framework. Moreover, there are some specific controls that Silverfort alone can provide, such as MFA for privileged and admin users. Organisations that have prioritised this control in their security architecture roadmap can rely on Silverfort to check all the required boxes.

What protection do these controls provide?

The objective of protecting access control and implementing MFA is to prevent the spread of an attack that has gained access via a user's compromised credentials. A common example is an attacker who has managed to gain access to an employee's machine with their target (ideally an admin or privileged user) helping them move laterally while being undetected. By placing access controls and restricting privileges, organisations can prevent attackers from using compromised credentials for malicious access. MFA across all users and resources will provide an additional security protection layer, so even if the credentials used are valid, they cannot be used to access any resource without the approval of the legitimate user.

Part 2: Silverfort Cyber Essentials mapping






Objective

The following is an excerpt from Cyber Essentials. The parts that correspond to restricting access controls is bolded:

"Compared to normal user accounts, **accounts with special access privileges have enhanced access to devices, applications, and information**. If these accounts are compromised, an attacker could take advantage of their greater access to corrupt information on a large scale, disrupt business processes or **gain unauthorised access to other devices in the organisation**. All types of administrators will have this kind of account, including domain administrators and local administrators. This is important because if a user opens a malicious URL or email attachment, the malware would typically be executed with the same privilege level of the user's account. This is why it's important to take special care allocating and using privileged accounts."

Compliance table

Access controls

Mitigation strategy	Silverfort protection
User accounts are assigned to authorised individuals only	
User accounts provide access to only those applications, computers, and networks the user needs to carry out their role	
Have in place a process to create and approve user accounts	
Authenticate users with unique credentials before granting access to applications or devices	
Remove or disable user accounts when they're no longer required (for example, when a user leaves the organisation or after a defined period of account inactivity)	
If you're using externally managed services (such as remote administration), you must be able to confirm that the Cyber Essentials technical controls are being met	

Part 2: Silverfort Cyber Essentials mapping (continued)

The following is an excerpt from Cyber Essentials. The parts that correspond to multi-factor authentication is bolded:

“As well as providing an extra layer of security for passwords that aren’t protected by the other technical controls, **you should always use multi-factor authentication to give administrative accounts extra security**, and accounts that are accessible from the internet.”

Compliance table

Multi-factor authentication

Mitigation strategy	Silverfort protection
Implement MFA where available; authentication to cloud services must always use MFA	✓
Always use MFA to give administrative accounts extra security, and accounts that are accessible from the internet	✓
Throttle the rate of attempts, so that the number of times the user must wait between attempts increases with each unsuccessful attempt; you shouldn’t allow more than 10 guesses in 5 minutes	
A managed/enterprise device, an app on a trusted device, a physically separate token, and a known or trusted account should be protected with MFA	✓
Lock devices after no more than 10 unsuccessful attempts	



Recommended controls to have in place

Combining multi-factor authentication (MFA) protection and the restriction of administrative access significantly strengthens an organization's defence against cyber attacks. By adhering to these strategies, businesses can enjoy several security benefits and mitigate potential risks. The following points elaborate on the advantages of implementing MFA and restricting administrative privileges:

Enhanced security through MFA

Multi-factor authentication (MFA) significantly reduces the risk of credential-based attacks. According to Microsoft, MFA can block over 99% of account compromise attacks. Similarly, data from the UK's National Cyber Security Centre (NSCS) and Cybersecurity and Infrastructure Security Agency (CISA) has consistently shown that enabling MFA is one of the most effective actions organizations can take to prevent unauthorized access. By requiring multiple forms of authentication, including smart card, biometric factor, or one-time passcode, MFA ensures that even if credentials are compromised, access to sensitive systems is still protected.

Restricting administrative privileges

Over 70% of breaches involve the misuse of privileged credentials, according to Verizon's 2024 Data Breach Investigations Report (DBIR). Attackers frequently exploit excessive access to move laterally and escalate privileges undetected. To mitigate the risk, organisations should apply the principle of least privilege by giving users access only to the resources they need to perform their job functions.

Regular review of controls

To maintain the effectiveness of MFA and administrative access restrictions, regular review and monitoring of controls are essential. Organisations should periodically assess and update access policies, review user privileges, and evaluate the implementation of MFA mechanisms. By staying proactive and responsive, businesses can identify and address any vulnerabilities or gaps promptly.

Monitoring and logging

All privileged user activity should be monitored and logged to detect any suspicious activity. This should include the use of a security information and event management (SIEM) system.

Education and training programs

While implementing MFA and restricting administrative access is crucial, educating and training privileged users is equally important. Organisations should conduct comprehensive cybersecurity awareness programs to educate employees about the importance of strong authentication practices, the risks associated with administrative privileges, and the potential consequences of security breaches. By fostering a culture of security awareness, organizations can enhance their overall cybersecurity posture.

Part 3: Silverfort: Your one-stop identity protection solution for compliance needs

While the Cyber Essentials and Cyber Essentials Plus main goal is to assist organisations with their overall cybersecurity posture, it highlights the importance of implementing MFA across all types of users and resources. In the following section, we will shed light on three places where the implementation of the Cyber Essentials and Cyber Essentials Plus models doesn't cover, and we will introduce how the Silverfort platform addresses these gaps to ensure your environment is fully protected.

Lateral movement and ransomware protection

While the standard MFA solution can help UK-based organisations become Cyber Essentials and Cyber Essentials Plus certified, Silverfort is the only solution that provides proactive prevention of lateral movement and ransomware propagation by extending MFA protection across all users, all resources, and all on-prem and cloud environments.

To conduct remote access between machines within the enterprise perimeter, common MFA solutions typically address access via Remote Desktop Access (RDP) to prevent attackers from using it for malicious access. However, most attacks make use of command line tools, such as PsExec, Remote PowerShell, WMI, and others, which are beyond the scope of these solutions. While the Cyber Essentials and Cyber Essentials Plus framework does not mention applying access controls to these interfaces as a requirement, organisations should include them when implementing MFA protection across their environment.

Silverfort enforces MFA across all protocols and access interfaces within the protected environment. When an attacker attempts to perform a malicious act from the initially compromised machine to others in the environment, they'll encounter an MFA barrier—regardless of what access interface was used.

Advanced risk engine for access policies

Cyber Essentials and Cyber Essentials Plus do not mention that organisations should base the MFA policies on a risk analysis. Common MFA solutions that are dependent on preset rules typically experience different challenges that surround protection needs with user experience and minimising work disruption. Silverfort's risk engine supports adaptive access policies that can be triggered by either an overall risk score or any specific risk indicators (brute force, kerberoasting, malicious MFA activity, lateral movement, etc.). This allows users to be prompted with MFA only when an actual risk is detected.

Part 3: Silverfort: Your one-stop identity protection solution for compliance needs (continued)

Non-Human Identity (NHI) security

The need to secure non-human identities (NHIs), especially on-prem service accounts, was excluded from the scope of access controls in the Cyber Essentials and Cyber Essentials Plus frameworks. Similar to admin or privileged users, on-prem service accounts are an attractive target for attackers and are used extensively in lateral movement attacks. Silverfort automates the discovery, access control, and protection of all on-prem service accounts in the environment, providing organisations with granular visibility into every NHI and machine-to-machine authentication, as well as its sources, destinations, authentication protocols, and activity volume. Silverfort monitors the behaviour of every on-prem service account and, upon detection of a risky deviation, can trigger a real-time response of either alert or real-time blocking.

Privileged access security

While the Cyber Essentials and Cyber Essentials Plus frameworks emphasize user account access controls, they do not fully address the unique risks posed by privileged access—a frequent target in identity-based attacks. Silverfort Privileged Access Security (PAS) solution helps close this gap by automatically discovering and classifying privileged users, enforcing least privilege access policies, and restricting the access to only authorised systems. Silverfort PAS secures admin access with Just-In-Time Policies and can enforce MFA protection across all privileged authentication paths. This allows organisations to control when, where, and how privileged accounts are used, ensuring they are only activated when necessary and for their indented purpose.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.

[Learn more](#)