SILVERFORT

WHITE PAPER

Cyber Essentials and Cyber Essentials Plus – Your Guide to Compliance Through Identity Protection

Table of Contents

Foreword 3

Part 1 – Overview 4

What is the Cyber Essentials Model? 4

What is Cyber Essentials Plus? 5

What is the difference between Cyber Essentials and Cyber Essentials Plus? 5

What Parts of the Cyber Essentials and Cyber Essentials Plus Does Silverfort Address? 6

What Protection Do These Mitigations Provide? 6

Part 2 – Silverfort Cyber Essentials Mapping 7

Compliance Table: Access Controls 7

Compliance Table: Multi-factor Authentication 8

Recommended Controls to Have in Place 9

Part 3 – Silverfort: Your One-Stop Identity Protection Solution for Compliance Needs 10

Lateral Movement and Ransomware Protection 10

Advanced Risk Engine for Access Policies 10

Service Account Protection 11

About Silverfort 12

Foreword

In this whitepaper, you will learn how organisations can integrate the Silverfort Unified Identity Protection platform to help comply with the Cyber Essentials and Cyber Essentials Plus certification assessment per its latest update in April 2021. Silverfort mitigations in both frameworks focus on restricting both user access control and the enforcement of multi-factor authentication. Silverfort also provides additional advanced capabilities within these two groups, that while being beyond the scope of Cyber Essentials and Cyber Essentials Plus are nevertheless imperative for sound protection against today's evolving threat landscape.

Security stakeholders that are looking to be compliant with both Cyber Essentials and Cyber Essentials Plus certification assessment can learn how Silverfort can enable them to implement identity security controls to strengthen their security posture following the frameworks, as well as gain insights into key attack surfaces that Silverfort is uniquely positioned to address, such as lateral movement and service account protection.

How to use this document?

The document is divided into three parts:

1. **Overview:** The objective, what mitigation strategies Silverfort covers, and what actual protections these strategies translate to when implemented.
2. **Silverfort's Cyber Essentials and Cyber Essentials Plus Mapping:** A table that lists the various strategies Silverfort checks within the user access controls and multi-factor authentication groups.
3. **Your One-Stop Identity Protection Solution for Compliance Needs:** How Silverfort delivers protection to three key attack surfaces that Cyber Essentials and Cyber Essentials certification does not cover.

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. The Cyber Essentials model is a cybersecurity certification framework aimed to provide a clear set of guidelines and best practices for organizations to protect themselves against common cyber threats. Its primary goal is to help organizations, regardless of their size or industry, implement essential cybersecurity controls and improve their overall cybersecurity resilience.

These five areas constitute the core controls of The Cyber Essentials model has five areas which constitute as the core controls which 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.

The framework requires organisations to implement five essential technical controls:

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 fundamental 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.

On the other hand, 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 defenses 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 Unified Identity Protection platform assists organisations in complying with two sets of mitigation strategies:

- **Access Control –** Silverfort's continuous authentication capabilities monitors and analyses user behavior during active sessions. Silverfort can detect anomalous actions or suspicious activities in real-time. If any unauthorised or abnormal behavior 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 Mitigations Provide?

The objective of protecting access control and implementing multi-factor authentication is to prevent the spread of an attack that has gained access via a user's compromised credentials in the targeted environment. 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 some restrictions on privileges users will deteriorate the ability of an attacker to utilise compromised credentials for malicious access. While implementing MFA across all users and resources will provide an additional; security protection layer to ensure that even if the credentials used are valid, they cannot be used to access any resource without the explicit verification 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	V
User Accounts provide access to only those applications, computers, and networks the user needs to carry out their role	V
Have in place a process to create and approve user accounts	V
Authenticate users with unique credentials before granting access to applications or devices	V
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	V

The following is an excerpt from Cyber Essentials. The parts that correspond to Mult-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	V
Always use multi-factor authentication to give administrative accounts extra security, and accounts that are accessible from the internet	V
Throttling' 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 multi-factor authentication	V
Locking devices after no more than 10 unsuccessful attempts	

Recommended Controls to Have in Place

The combined implementation of multi-factor authentication (MFA) protection and the restriction of administrative access significantly strengthens an organization's defense 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 adds an extra layer of security by requiring users to provide multiple forms of identification before accessing sensitive systems or data. This authentication method can include using a smart card, biometric authentication, or a one-time code sent to a mobile device. By leveraging MFA, organisations can mitigate the risk of unauthorized access resulting from compromised or weak passwords.

Restricting Administrative Privileges

Limit access to privileged accounts to only those who need it to perform their job functions. Access should be granted based on the principle of least privilege, which means that users should only have access to the resources they need to do their job.

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 in increasing their resilience to cyberattacks, 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 organsations 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 access interfaces in the on-prem environment.

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 utilizing it for malicious access. While industry-accepted, this is not enough since 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. Resulting when an attacker attempts to perform a malicious act from the initially compromised machine to others in the environment encounters an MFA barrier – regardless of what access interface was used.

Advanced Risk Engine for Access Policies

Cyber Essentials and Cyber Essentials Plus did not mention that organsations 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.

Service Account Protection

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

About Silverfort

Silverfort has pioneered the first-ever Unified Identity Protection platform, which protects enterprises against identity-based attacks that utilize compromised credentials to access enterprise resources. Using innovative agentless and proxyless technology, Silverfort natively integrates with all existing IAM solutions, to extend secure access controls such as Risk-Based Authentication and MFA across all on-prem and cloud resources. This includes assets that could never have been protected in this way before, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access, and more. Silverfort continuously monitors all access attempts by users and service accounts and analyzes risks in real-time using an AI-based engine to enforce adaptive access policies.

To learn more, visit www.silverfort.com