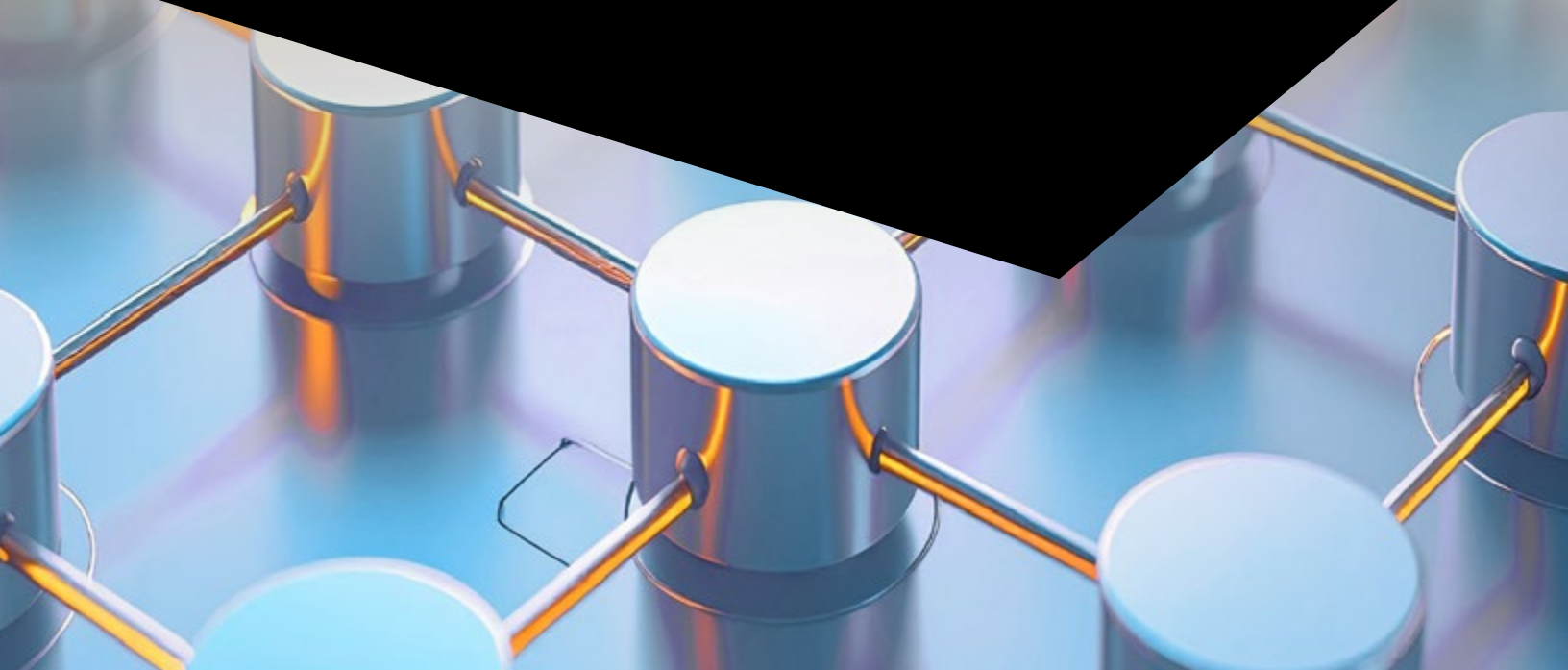
Silverfort

Cyber Assessment Framework (CAF) compliance with Silverfort

Whitepaper



Executive summary

The Cyber Assessment Framework (CAF) was developed by the National Cyber Security Centre (NCSC) to help UK organisations manage their cyber security risks and improve their resilience. The CAF was produced to support the implementation of the Network and Information Systems (NIS) Regulations 2018, which are based on the European Union Directive on Security of Network and Information Systems (NIS Directive).

CAF provides a systematic approach for evaluating an organisation's cybersecurity posture, identifying vulnerabilities, and implementing effective risk mitigation strategies. In contrast to most other standards and guidelines, CAF is applicable to both Information Technology (IT) and Operational Technology (OT). The framework is designed to be flexible and adaptable to different sectors and contexts, and to align with existing cybersecurity standards and guidelines.

Addressing the identity security aspects of CAF

Recent ransomware attacks have revealed an alarming increase in the use of compromised credentials for malicious access, highlighting the importance of protecting the identity attack surface. A key component of CAF is the requirement for organisations to enforce Multi-Factor Authentication (MFA), secure their privileged accounts, and implement best practices for monitoring, detecting, and responding to cyber threats.

Managing privileged accounts is the cornerstone of protecting an organisation's most valuable resources. However, traditional PAM solutions are subject to inherent blind spots that prevent them from providing security to all privileged users. These solutions often entail lengthy and complex deployment cycles and rely on manual account discovery, making it difficult to quickly identify all privileged users. They also cannot enforce least privilege access, prevent admins from bypassing the PAM, or eliminate privileged access abuse, leaving critical security gaps in place.

The Silverfort Identity Security Platform

Silverfort's platform integrates with all Identity and Access Management (IAM) infrastructures in the entity's environment to provide continuous monitoring, risk analysis, and active enforcement of every authentication and access attempt. Using these capabilities, Silverfort provides Identity Security Posture Management (ISPM), advanced MFA, service account protection, and Identity Threat Detection and Response (ITDR).

Silverfort's Privileged Access Security (PAS) offers a new approach to overcoming the limitations of traditional PAM solutions through its unique architecture, which integrates directly with Active Directory. This allows for the instant discovery and classification of privileged accounts, ensuring no account goes unnoticed. Silverfort PAS provides comprehensive security capabilities designed to protect privileged users from being compromised, whether used alongside existing PAM solutions for full coverage or as a standalone solution.

Your PAS journey made simple with Silverfort

DISCOVER

Automatically discover privileged accounts based on their authentications.

CLASSIFY

Prioritize and implement security controls based on privilege tiers.

FENCE

Apply least privilege policies by fencing privileged accounts according to their access permissions.

JUST - IN - TIME (JIT)

Remove standing privileges with JIT policies by granting access rights only when necessary.

Silverfort for CAF highlights

Multi-factor authentication

Extend MFA protection to command-line access, legacy apps, IT infrastructure and other critical resources that couldn't be protected before.

Continuous monitoring

All access requests are monitored to detect anomalies and prevent malicious access in real time.

Detect and respond to identity threats

Detect common credential access, privilege escalation and lateral movement attacks, and respond automatically with real-time blocking.

Secure privileged users

- Automatically discover and classify all privileged accounts based on actual authentication activity
- Enforce MFA or access block policies on all your privileged users, both human admins and service accounts
- Fence privileged accounts to their intended purpose by restricting admin account usage to specific sources, destinations, and protocols
- Enforce Just-In-Time (JIT) access policies to ensure privileged accounts only receive permissions when needed and for a limited duration
- Achieve Zero Standing Privileges at scale to eliminate the risk of privileged credential theft and misuse

Silverfort for CAF highlights

Multi-factor authentication

Extend MFA protection to command-line access, legacy apps, IT infrastructure, and other critical resources that couldn’t be protected before.

Detect and respond to identity threats

Detect common credential access, privilege escalation, and lateral movement attacks, and respond automatically with real-time blocking.

Securing privileged users

Enforce MFA or access block policies on all your privileged users, both human admins and service accounts.

Continuous monitoring

Monitor all access requests to detect anomalies and prevent malicious access in real time.

Protect your privileged accounts without compromising security

Automated discovery and classification

See all privileged accounts and classify them to different tiers based on the actual privileges they use. Determine if regular accounts are being used with privileged intent.

Virtual fencing

Allow admin accounts to only access the resources they need while blocking access to all other resources.

Seamless Just-In-Time access

Enforce JIT access policies on domain privileged accounts with a single click to decrease unnecessary access and reduce the identity attack surface.

Mapping Silverfort capabilities to Cyber Assessment Framework V3.2 based on the achieved level

CAF Objective A: Managing security risk

A2.a Risk management process

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of your essential function(s) and communicating associated activities.

CAF Regulation	Silverfort Security Controls
Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed.	With Silverfort's risk report functionality, organisations can create a summary of their identity security posture with a single click, arming security teams with clear insights into issues that need resolving. Silverfort PAS automatically discovers and classifies all privileged accounts based on user activity, enabling organisations to gain comprehensive visibility into risky privileged access patterns.
Your risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to network and information systems, change of use and new threat information.	Silverfort continuously updates risk assessments based on information gathered from user logs. It detects suspected threats by analysing the behaviour patterns and authentication attempts of entities such as users and resources. Silverfort shows the sequence of events detected in an incident, including details of authentications that occurred during it, changes in the risk level of the main entity, and changes in the status of the incident. This timeline can be filtered by user, source, destination, risk and more.
You perform detailed threat analysis and understand how this applies to your organisation in the context of the threat to your sector and the wider CNI.	The Silverfort platform provides detailed guidance for mitigating every detected risk. Organisations can also configure access policies that prevent risky authentications from taking place. Silverfort PAS enables organisations to prioritize and implement security controls tailored to each privileged tier while detecting privilege escalation potential.
(5) recover from cybersecurity events and restore normal operations and services.	N/A

CAF Objective B: Protecting against cyber attack

Proportionate security measures are in place to protect the network and information systems, supporting essential functions from cyber attack.

Principle B1.a Service protection policies, processes and procedures

The organisation defines, implements, communicates, and enforces appropriate policies, processes and procedures that direct its overall approach to securing systems and data that support operation of essential functions.

CAF Regulation	Silverfort Security Controls
You fully document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is integrated and embedded throughout policies, processes and procedures and key performance indicators are reported to your executive management.	Silverfort enforces flexible access policies, and organisations can embed cybersecurity into their policies, processes, and procedures. Admins can define access control policies based on specific user roles, risk scenarios and organisational security policies. Silverfort enforces these policies in real time, so only authorised users and devices can gain access to the resources they are assigned to.
Policies, processes, and procedures that rely on user behaviour are practical, appropriate and achievable.	With Silverfort, organisations can configure access policies based on user rules for both on-prem and cloud environments. These policies can enforce alerting, MFA, or block access upon insecure authentication to protected systems. PAS enables organizations to simplify security controls by eliminating the need for complex security measures like password rotation and vaulting, and instead applying strict access policies to all privileged users.
You review and update policies, processes and procedures at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident.	Silverfort continuously analyses user behaviour, devices, locations, security events, and other risk factors to easily adjust any access policies when needed. This allows for the review and update of policies, processes, and procedures at regular intervals to ensure the applied access policies remain relevant.

Principle B2: Identity and access control

The organisation understands, documents and manages access to network and information systems supporting the operation of essential functions. Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.

B2.a Identity verification, authentication and authorisation

You robustly verify, authenticate and authorise access to the network and information systems supporting your essential function(s).

CAF Regulation	Silverfort Security Controls
Your process of initial identity verification is robust enough to provide a high level of confidence of a user's identity profile before allowing an authorised user access to network and information systems that support your essential function(s).	Silverfort can enforce MFA on any access request, whether on-prem, remote, or third-party, and for every level, from regular users to admins. In an Active Directory (AD) environment, Silverfort can enforce MFA and block access policies on any LDAP/S, NTLM, and Kerberos authentications. This expands the scope of MFA protection to a wide array of resources and access methods that couldn't have been protected before, such as command-line tools, legacy applications, IT infrastructure and more. Silverfort ensures no access is granted based on passwords alone, and users are required to authenticate through MFA to verify that they are who they claim to be.
The number of authorised users and systems that have access to all your network and information systems supporting the essential function(s) is limited to the minimum necessary.	Silverfort detects user behaviour, devices, locations, and other risk factors to calculate the risk score of each user authentication request. This allows the organisation to configure and apply access policies to ensure only authorised users have access to resources in the environment. Silverfort PAS enables organizations to reduce the attack surface by decreasing the number of standing privileges through its Just-in-Time access capabilities.
You use additional authentication mechanisms, such as multi-factor (MFA), for all user access, including remote access, to all network and information systems that operate or support your essential function(s).	Silverfort can enforce MFA protection across all users and resources, both on-prem and in the cloud. This applies to all Active Directory authentications, including those that couldn't be protected by MFA before, such as legacy applications, command-line access, databases, networking infrastructure and many others. Silverfort can also enforce MFA protection on all remote access to on-prem and cloud systems and on any third-party application that is accessed on-prem or via a cloud directory.
The list of users and systems with access to network and information systems supporting and delivering the essential function(s) is reviewed on a regular basis, at least every six months. Your approach to authenticating users, devices and systems follows up to date best practice.	Silverfort provides an in-depth identity inventory that displays the types of users and resources in the environment as well as security weaknesses. This enables you to detect and respond to potential security threats, including blocking the access of any accounts that display anomalous behaviour. Silverfort provides full visibility into all user accounts' authentication trails, while alerting on any excessive access requests and detected malicious activity. This allows admins to perform scheduled, continuous, and as-needed security reviews.

B2.c Privileged user management

You closely manage privileged user access to network and information systems supporting your essential function(s).

CAF Regulation	Silverfort Security Controls
Privileged user access to network and information systems supporting your essential function(s) is carried out from dedicated separate accounts that are closely monitored and managed.	Silverfort PAS offers automated discovery and classification of all privileged accounts based on actual authentication activity. This allows organizations to know exactly which accounts have privileged access and monitor their usage patterns in real-time. PAS enforces frictionless Just-in-Time (JIT) access policies that remove standing privileges by granting access rights only when necessary, significantly enhancing security posture.
The issuing of temporary, time-bound rights for privileged user access and/or external third-party support access is in place.	Silverfort PAS implements temporary, time-bound access through its Just-in-Time (JIT) privileged access management capabilities. The solution automatically provisions privileged access rights only when necessary and for the minimum duration required, eliminating standing privileges. For both internal privileged users and external third-party support personnel, Silverfort enforces session-based access controls with predefined expiration periods. Access rights are automatically revoked when the approved time window expires, ensuring no persistent privileged access remains. This approach significantly reduces the attack surface by minimizing the timeframe during which privileged credentials could potentially be compromised or misused.
Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers, and leavers process.	Silverfort continuously monitors user activities and access rights across the network, including privileged users. This monitoring ensures that any changes in access rights or user roles are promptly detected. Silverfort PAS allows organizations to “fence” privileged accounts to their intended purpose, limiting the misuse of admin accounts outside their intended purpose and blocking lateral movement attempts.
The number of authorised users and systems that have access to all your network and information systems supporting the essential function(s) is limited to the minimum necessary.	Silverfort continuously monitors user activities and access rights across the network, including privileged users. This monitoring ensures that any changes in access rights or user roles are promptly detected. Silverfort access policies can dictate the appropriate level of access for different users based on their roles and responsibilities. With PAS, organizations can reduce the risk of overexposure and unnecessary access by enforcing strict privilege limitations and access boundaries.

B2.d Identity and access management (IAM)

You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting your essential function(s).

CAF Regulation	Silverfort Security Controls
You follow a robust procedure to verify each user and issue the minimum required access rights, and the application of the procedure is regularly audited.	Silverfort can enforce MFA protection across all users and resources, on-prem and in the cloud. This applies to all Active Directory authentications, including those that couldn't be protected by MFA before, such as legacy applications, command-line access, databases, networking infrastructure and many others. Silverfort ensures no access is granted based on passwords alone, and users are required to authenticate through MFA to verify that they are who they claim to be. PAS enables organizations to implement Zero Standing Privileges at scale by eliminating privileged standing permissions and implementing Just-in-Time access rights.
User access rights are reviewed both when people change roles via your joiners, leavers, and movers process and at regular intervals - at least annually.	Silverfort continuously monitors all user activities and access requests across the environment. This monitoring ensures that any changes in access rights or user roles are promptly detected. Silverfort access policies can dictate the appropriate level of access for different users based on their roles and responsibilities. The JML process allows these policies to be flexibly adjusted to reflect changes in user status within the organisation.
You regularly review access logs and correlate this data with other access records and expected activity.	Silverfort provides admins with a detailed log screen that documents every authentication and access attempt in the environment. The log screen includes optional filters to detect insecure authentications, suspicious activity, misconfigurations, and other anomalies. Silverfort detects and alerts against invalid access attempts that appear to be malicious.
Attempts by unauthorised users, devices, or systems to connect to the systems supporting the essential function(s) are alerted, promptly assessed and investigated.	Silverfort monitors all authentications and access requests across the organisation and alerts/denies anomalous activity, including attempts at lateral movement. Furthermore, Silverfort requires MFA on every "hop," or move from one asset to another, so that stolen credentials cannot be used to progress in the attack path.

CAF Objective C: Detecting cyber security events

Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential function(s).

Principle C1 Security monitoring

The organisation monitors the security status of the network and information systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

C1.a Monitoring coverage

The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).

CAF Regulation	Silverfort Security Controls
Your monitoring data provides enough detail to reliably detect security incidents that could affect the operation of your essential function(s).	Thanks to its native integrations with all identity providers, Silverfort monitors all identity traffic and authentication activities in one place and provides centralised visibility into every authentication and access request across all users and resources in the hybrid environment. With complete visibility across all user activity, Silverfort's analysis engine can determine the risk of every authentication, so organisations can detect and respond to potential security threats in real time — including blocking the access of any accounts that display anomalous behaviour.
Extensive monitoring of user activity in relation to the operation of your essential function(s) enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.	Silverfort provides organisations with a detailed log screen that documents every authentication and access attempt carried out in the environment. When malicious access occurs, Silverfort detects and alerts console admins of security threats. Silverfort PAS detects actual access usage patterns and behavior to classify different user tiers and identify when regular accounts are being used with privileged intent.

Silverfort PAS can be deployed in three distinct ways to support organisations at different stages of their CAF compliance journey:

PAM alternative

- Single solution to protect all privileged users in the environment
- Ideal for mid-to-small organisations that can't afford or don't have the resources for traditional PAM
- Rapid deployment with minimal setup time and effort

Complementing PAM

- Protecting privileged users that are temporarily or permanently not in the PAM
- Designed for organisations that are within a PAM journey and acknowledge its limitations
- Fills the security gaps in existing PAM implementations

Enhancing PAM

- Additional protection layer on top of the privileged users already in the PAM
- Perfect for mature organisations with PAM fully onboarded
- Provides additional security controls and monitoring capabilities

Why Silverfort PAS is Invaluable for CAF Compliance

- **Achieve zero standing privileges at scale:** Reduce the risk of misuse by eliminating privileged standing permissions and implementing Just-in-Time access rights
- **Limit misuse of accounts:** Ensure accounts are only used for their intended purpose, reducing the possibility of misuse
- **Reduce the attack surface:** Minimize your attack surface by decreasing the number of standing privileges
- **Simplify security controls:** Eliminate the need for complex security measures like password rotation and vaulting, and instead apply strict access policies to all privileged users
- **Comply with regulations and cyber insurance:** Assists you in significantly reducing the time and effort to comply with regulations as well as renewing your cyber insurance policy
- **Rapid deployment:** Silverfort's unique architecture deploys seamlessly into existing environments for rapid time-to-value and a streamlined user experience

About Silverfort

Silverfort secures every dimension of identity. We are the first to deliver end-to-end identity security across the entire IAM infrastructure, eliminating gaps and blind spots, giving businesses visibility into their identity fabric and extending protection to resources that previously could not be protected. This is all done via Runtime Access Protection (RAP), a patented technology that natively integrates with your entire IAM infrastructure. It is lightweight, easy to use and deploy, and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline to stop lateral movement, ransomware propagation, and other identity threats.

To learn more, visit www.silverfort.com