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 assist UK organisations in managing their cyber security risks and improving their cyber 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 (EU) 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) and security of privileged accounts, in addition to requiring the implementation of best practices for monitoring, detecting, and responding to cyber threats, which include a significant aspect of identity security.

Silverfort Unified Identity Security Platform

The Silverfort 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 user's authentication and access attempts. Using these capabilities, Silverfort provides Identity Security Posture Management (ISPM), advanced MFA, service account protection, and Identity Threat Detection and Response (ITDR).

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.

Securing Privileged Users

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

Detect and Respond to Identity Threats

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

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 in a single click, arming security teams with clear insights into issues that need resolving.
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. Organizations can also configure access policies that prevent risky authentications from taking place.
(1) recover from cybersecurity events and restore normal operations and services. and	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 B1a 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 compliance requirements. Silverfort enforces these policies in real time, so only authorized 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 roles for both on-prem and cloud environments. These policies can enforce alerting, MFA, or block access upon insecure authentication to protected systems.
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 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 onprem or via a cloud directory.
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).	The Silverfort platform MFA functionality is a reasonably equivalent or more secure compensating control in case the company cannot apply such a solution
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.	Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers, and leavers process.
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.

B2.d Identity and Access Management (IdAM)

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.
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/enforces 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 centralized 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.

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 a patented technology that natively integrates with your entire IAM infrastructure, Runtime Access Protection™ (RAP). 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