SILVERFORT

How to Comply with CMMC's Identity Security Requirements with Silverfort

WHITEPAPER

Executive Summary

The Cybersecurity Maturity Model Certification (CMMC) is a framework created by U.S. Department of Defense (DoD) in 2020 to enhance security control implementation within the Defense Industrial Base (DIB) sector. It provides a set of security requirements for contractors and subcontractors for protecting unclassified sensitive data such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) that is processed within the entire DIB supply chain. CMMC compliance is mandatory for any DIB organization, ensuring security measures are in place to protect national interests.

The CMMC framework defines several compliance levels with gradually increasing security requirements to protect unclassified and sensitive information. Organizations engaged in defense-related activities should comply with CMMC standards to protect critical systems from cyberattacks and to ensure their integrity. By achieving CMMC certification, an organization demonstrates its commitment to maintaining a secure environment and safeguarding sensitive government information.

In this whitepaper, we focus on the CMMC model 1.0. The CMMC 2.0 framework is expected to be released to the public in Q4 2024 – Q1 2025.

Addressing the Identity Security Aspects of CMMC

CMMC emphasizes the need for strong authentication measures like MFA to protect sensitive government data such as FCI and CUI. Through its identity authentication requirements, CMMC ensures that only authorized users can access critical information, reducing the risk of compromised credentials.

In addition, the CMMC framework requires strict access control standards, such as the principle of least privilege to limit user permissions and minimize cyber threat exposure. An organization's ability to detect and respond to malicious behavior in real time is enhanced through continuous monitoring, logging, and auditing of user activity. By taking such a proactive approach to identity security, users and privileged accounts are protected from malicious attacks.

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 CMMC Protection 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 continuously monitored to detect anomalies and prevent malicious access in real-time.

Strong Access Control
Apply strong security access controls by enforcing MFA across all sensitive resources, ensuring only authorized users can access critical systems and data.

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 CMMC

Access Control (AC)

CMMC Regulation	Silverfort Security Controls
AC.1.001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Silverfort provides centralized access control policy enforcement on each data access attempt, based on the administrator's policy settings and configurations. With Silverfort, administrators can define access control policies based on specific user roles, risk scenarios, and organizational security policies. These policies can enforce alerting, MFA, or block access upon insecure authentication to protected systems.
AC.1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Silverfort enables administrators to assign access control policies to each user, defining which resources, devices or services the user can access. Silverfort enforces these policies in real time, so only authorized users and devices can gain access to the resources they are assigned to. As a result, alerting, MFA, or blocking access to all users defined in the policy can be enforced.
AC.1.003 Verify and control/ limit connections to and use of external information systems.	Silverfort's access control policies apply to every authentication via the organization's directory services infrastructure, regardless of whether the device or resource is internal or external.
AC.2.007 Employ the principle of least privilege, including for specific security functions and privileged accounts.	Silverfort enables administrators to assign access control policies to each user, including privileged accounts, defining which resources, devices, or services the user can access. Additionally, administrators can monitor all authentications carried out by privileged accounts.
AC.2.008 Use non-privileged accounts or roles when accessing non-security functions.	Silverfort can be used to prevent privileged accounts from performing insecure activities by enforcing access controls and requiring adaptive MFA for all users. Silverfort continuously monitors privileged account activity and applies real-time risk-based policies, preventing unauthorized or insecure actions based on user behavior, device, and location.

CMMC Regulation	Silverfort Security Controls
AC.2.009 Limit unsuccessful logon attempts.	Silverfort employs an adaptive blocking policy which locks authentication following a configurable number of unsuccessful logon attempts. Additionally, Silverfort has a built-in brute force detection module.
AC.2.013 Monitor and control remote access sessions.	Silverfort access control policies apply to every authentication via the organization's directory services infrastructure, regardless of whether internal or remote. Additionally, Silverfort monitors all remote access attempts and supports exporting them in the form of a dedicated report.
AC.2.015 Route remote access via managed access control points.	Silverfort supports access control policies that limit the number of remote access control points. Silverfort ensures that all remote connections are properly authenticated and authorized before granting access. By doing so, Silverfort secures remote access pathways and prevents unauthorized users from bypassing security controls, ensuring compliance with approved access routes.
AC.3.018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Silverfort supports creation of access control policies that limit non-privileged users from accessing defined resources. In addition, Silverfort monitors each authentication attempt and enables administrators to generate activity reports for each user group.
AC.3.019 Terminate (automatically) user sessions after a defined condition.	Silverfort monitors and controls each authentication separately so that even if an initial login to the network was verified, further resource access that poses a risk will be blocked.
AC.4.023 Control information flows between security domains on connected systems.	Silverfort access control policies include the ability to define where each account is allowed to authenticate, creating a segmented system-to-system communication, based on the administrator's definitions.
AC.4.032 Restrict remote network access based on organizationally defined risk factors such as time of day, location of access, physical location, network connection state, and measured properties of the current user and role.	Silverfort restricts remote network access by continuously monitoring access activity and applies risk-based policies, preventing unauthorized or insecure actions based on risk factors such as location, user behavior, role and device.

Asset Management (AM)

CMMC Regulation	Silverfort Security Controls
AM.4.226 Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.	Silverfort provides in-depth visibility of systems within the entire environment, including specific attributes such as firmware level and OS type.

Audit And Accountability (AU)

CMMC Regulation	Silverfort Security Controls
AU.2.041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	Silverfort provides the ability to authenticate every user access request for each system. It ties all actions, including access attempts and resource usage, to individual user identities. By enforcing MFA and logging all user activities, Silverfort allows for precise tracking of each user's actions, ensuring accountability.
AU.2.042 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Silverfort generates comprehensive audit logs of all authentication and access activities across all systems. It captures detailed records of user actions, including logins, access attempts, and privileged account usage, enabling real-time monitoring, analysis, and reporting of unauthorized or suspicious behavior. These logs are centrally stored and can be integrated with SIEM tools for enhanced investigation and compliance reporting, ensuring full visibility into system activity for security audits.
AU.2.044 Review audit logs.	Silverfort supports this functionality with a dedicated investigation interface as well as exporting audit logs to third-party systems.
AU.3.045 Review and update logged events.	Silverfort provides real-time logging of authentication and access events across all systems. It integrates with SIEM tools to continuously monitor, and review logged events, ensuring logs are regularly analyzed for anomalies or security incidents. It is possible to customize and update the audit log policies using Silverfort, ensuring new types of events or threats are captured and the audit logs are in line with evolving security requirements.

CMMC Regulation	Silverfort Security Controls
AU.3.046 Alert in the event of an audit logging process failure.	Silverfort supports multiple monitoring options, enabling the user to configure alerts for various system disconnections and failures, including any related to the logging process.
AU.3.048 Collect audit information (e.g., logs) into one or more central repositories.	Silverfort can act as the central repository itself or export the data to a third-party system.
AU.3.049 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Silverfort secures all audit logs and logging tools with granular access controls and MFA protection. Only authorized users can access or manage audit logs, preventing unauthorized individuals from viewing, modifying, or deleting critical audit data. Silverfort strengthens protection by continuously monitoring access attempts and applying real-time policies to prevent unauthorized modifications, ensuring the integrity and confidentiality of audit information.
AU.3.050 Limit management of audit logging functionality to a subset of privileged users.	Silverfort enforces role-based access controls that restrict audit logging management to a subset of privileged users. It ensures only authorized, privileged users can configure, modify, or access audit logging tools, while other users are prevented from making changes. By applying MFA protection and continuous monitoring of privileged activities, Silverfort ensures that sensitive logging functions are managed securely and in compliance with established policies.
AU.3.051 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Silverfort provides complete visibility into all user activities in audit records based on all authentication and access activities, enabling you to correlate and analyze them in real time. It integrates with SIEM systems to facilitate comprehensive review and investigation of suspicious or unauthorized activity. By identifying patterns and anomalies across environments, Silverfort facilitates efficient reporting of investigations and incident response.
AU.3.052 Provide audit record reduction and report generation to support on-demand analysis and reporting.	Silverfort enables audit record reduction and efficient report generation by filtering and prioritizing key security events, reducing the volume of audit logs while retaining critical data for analysis. Silverfort's integration with SIEM tools allows for on-demand reporting and detailed investigations, providing actionable insights into user activities and access patterns. When audits of security reviews are required, this streamlined approach facilitates faster analysis and reporting.

CMMC Regulation	Silverfort Security Controls
AU.4.053 Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/ or organizationally defined suspicious activity.	Silverfort supports this functionality by detecting and preventing various initial access and lateral movement techniques.
AU.4.054 Review audit information for broad activity in addition to per-machine activity.	Silverfort supports various correlations and analysis based on user, machine, authentication protocol, etc., providing unique contextual insights into the activity within the network and enabling investigators to unveil and mitigate a wide range of hidden attacks.

Awareness And Training (AT)

CMMC Regulation	Silverfort Security Controls
AT.2.056 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	Silverfort assigns an adaptive risk score to all accounts and authentications and support email notifications to alert administrators when an user's risk score changes.

Configuration Management (CM)

CMMC Regulation	Silverfort Security Controls
CM.3.067 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Silverfort supports this functionality, providing logical access restrictions based on its access control policy engine.

Identity And Authentication (IA)

CMMC Regulation	Silverfort Security Controls
IA.1.076 Identify information system users, processes acting on behalf of users, or devices.	Silverfort provides an in-depth identity inventory that displays 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 behavior. Silverfort provides full visibility into all user accounts' authentication trails, while alerting on any excessive access requests and malicious activity.
IA.1.077 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Silverfort can enforce MFA on any access request, whether on-prem, remote, or third-party, and for every level, from regular users to administrators. 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.
IA.3.083 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Silverfort authenticates each user's identity by enforcing strong MFA across all systems, even those that don't natively support modern authentication protocols. This ensures every user must verify their identity before accessing resources.
IA.3.084 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Silverfort assigns a unique ID to each incoming access attempt, which is associated with step-up identification request. Therefore, an attacker cannot replay a step-up authentication message used for one access attempt to bypass step-up authentication for a second access attempt.

Incident Response (IR)

CMMC Regulation	Silverfort Security Controls
IR.2.092 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Silverfort assists with incident analysis by providing detailed logs of all authentication and access activities. This allows security teams to understand what occurred during an incident and determine the root cause. Using comprehensive data on user access requests and behaviors, Silverfort facilitates a comprehensive investigation and understanding of the events leading up to and during a security incident. Silverfort's real-time monitoring capabilities enable it to detect anomalies and suspicious activities, providing insights into the course of an incident. As a result of this detailed analysis, it is possible to pinpoint the exact nature and origin of the problem, thereby facilitating effective remediation and strengthening security overall.
IR.2.093 Detect and report events.	Silverfort supports this functionality by detecting real-time authentication and access events across all systems. With SIEM tools integration, all the logs are regularly analyzed, enabling regular logged events reporting in case of any anomalies or security incidents.
IR.2.094 Analyze and triage events to support event resolution and incident declaration.	Silverfort supports this functionality by assigning an adaptive risk score for each authentication attempt, facilitating the response prioritization for the IR team.
IR.2.097 Perform root cause analysis on incidents to determine underlying causes.	Silverfort provides the relevant data to perform root cause analysis of identity-based attacks.
IR.5.106 In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.	Silverfort gathers the relevant forensic data for identity-based attacks, stores it internally, and supports secure data transfers to SIEM.
IR.5.102 Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.	Silverfort supports real-time response to threats by either alerting, blocking or requiring MFA based on manual policies or automated risk analysis, as well as empowering the security team with relevant forensic data.

Maintenance (MA)

CMMC Regulation	Silverfort Security Controls
MA.2.113 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete	Silverfort enforces MFA for all non-local maintenance sessions over external network connections. It ensures only authenticated and authorized users can establish these sessions, adding an extra layer of security.

Media Protection (MP)

CMMC Regulation	Silverfort Security Controls
MP.2.120 Limit access to CUI on system media to authorized users	Silverfort enforces access control policies for network access to system media containing CUI. It ensures only authorized users can access or interact with CUI by validating user identities through MFA and applying real-time access controls. By continuously monitoring user activities and restricting access to sensitive data based on roles and permissions, Silverfort ensures that only those with approved authorization can access CUI on system media.

Personnel Security (PS)

CMMC Regulation	Silverfort Security Controls
PS.2.128 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	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 organization.

Risk Management (RM)

CMMC Regulation	Silverfort Security Controls
RM.2.141 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Silverfort's risk assessment report creates a summary of an organization's identity security posture in a single click. This provides security teams with clear insights into issues that need resolving. Silverfort provides detailed guidance for mitigating every detected risk. Organizations can also configure access policies that prevent risky authentications from taking place.
RM.2.142 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Silverfort risk assessments detect password weaknesses and authentication-related vulnerabilities across organizational systems. It continuously monitors authentication mechanisms, identifying weak and compromised passwords and poor authentication practices. This ensures organizations can proactively detect and mitigate weaknesses while maintaining secure access controls across their systems.
RM.3.144 Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.	Silverfort's risk reports enable organizations to prioritize risks according to defined risk categories, sources and measurement criteria. With a more data-driven approach, organizations can make more informed decisions on where to focus security efforts.
RM.3.147 Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.	Silverfort discovers older operating systems within the network. These, as well as other EOL products, can be grouped and assigned a dedicated access policy that considers their higher risk exposure.

Security Assessment (CA)

CMMC Regulation	Silverfort Security Controls
CA.3.161 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Silverfort enables administrators to define which of its security controls to monitor, by providing a reach interface to examine the different access events and the policies that took place and apply filters.

Situational Awareness (SA)

CMMC Regulation	Silverfort Security Controls
SA.4.171 Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.	Silverfort provides detection capabilities and an investigation interface, which is used by its customers for threat hunting. The user can investigate the network activities of the entities involved, discover compromised entities, and define policies to prevent further expansion.

System And Configuration Protection (SC)

CMMC Regulation	Silverfort Security Controls
SC.3.181 Separate user functionality from system management functionality.	Silverfort can enforce identity-based segmentation between the different interfaces of a single system. Silverfort's granular policy engine allows the creation of policies that prohibit the access of standard users to administrative interfaces of a system while enabling the access of the administrators to these interfaces.
SC.3.183 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Silverfort integrates with identity-aware firewalls and other network security vendors to provide risk, threat context, and MFA capabilities to these products. These integrations can be used to require step-up authentication or a risk assessment before network communication is permitted.
SC.3.190 Protect the authenticity of communications sessions.	Silverfort protects the authenticity of any communication session by enforcing MFA protection and risk-based threat-aware authentication.
SC.4.197 Employ physical and logical isolation techniques in the system and security architecture and/or where deemed appropriate by the organization.	Silverfort supports logical isolation through configuration of identity-based segmentation rules.
SC.4.228 Isolate administration of organizationally defined high-value critical network infrastructure components and servers.	Silverfort supports logical isolation through identity-based segmentation rules and can enhance existing network segmentation by adding a secure authentication layer.

CMMC Regulation	Silverfort Security Controls
SC.5.230 Enforce port and protocol compliance.	Silverfort assists enforcement by discovering users and devices using weak authentication protocols.
SC.1.175 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Silverfort monitors any access event, including access at the external and internal boundaries of the information systems. Silverfort provides visibility into these access events and allows configuration of policies to control and protect these communications with advanced access controls and secure authentication.
SC.5.208 Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.	Silverfort assists enforcement by discovering users and devices using weak authentication protocols.

System And Information Integrity (SI)

CMMC Regulation	Silverfort Security Controls
SI.2.216 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Silverfort monitors access to organizational systems, including inbound and outbound access, and automatically detects indicators of attacks and vulnerabilities.
SI.2.217 Identify unauthorized use of organizational systems.	When Silverfort detects malicious activity, it provides information regarding the targeted system as well as the compromised system that was used to target the system.
SI.5.223 Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	Silverfort profiles each network entity, automatically detecting anomalies, deviations, and suspicious access patterns typical of an attack.

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.

For more information, visit silverfort.com