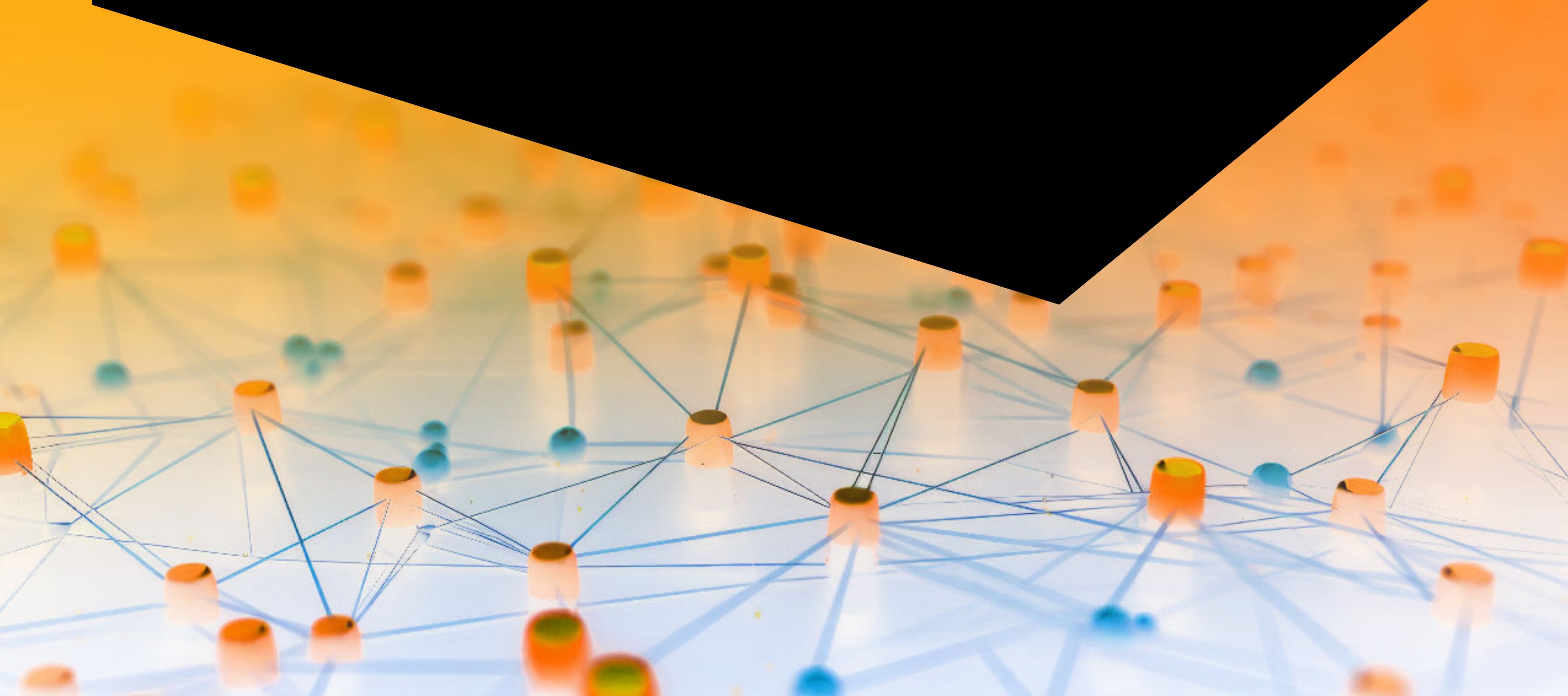
Silverfort

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 latest CMMC 2.0 model. It was released to the public in October 2024.

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 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.

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.

Continuous monitoring

Gain comprehensive visibility into all authentication and access attempts, monitor and review them continuously 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.

Mapping Silverfort capabilities to CMMC

Access Control (AC)

CMMC regulation	Silverfort security controls
AC.L2-3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other 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.L2-3.1.2 Limit 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.L2-3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	Silverfort enables administrators to automatically discover and classify all privileged accounts based on user's actual authentications activity. With Silverfort, organizations gain comprehensive visibility into all privileged accounts and cross-tier authentications and access requests to identify whether regular accounts are being used with privileged intent. Additionally, with virtual fencing restricts admin accounts usage to specific sources, destinations and protocols to minimize risk and by enforcing Just-in-Time (JIT) access policies, grants access rights only when necessary.
AC.L2-3.1.6 Use non-privileged accounts or roles when accessing non-security functions.	Silverfort enables administrators to automatically discover and classify all privileged accounts based on user activity. With Silverfort, organizations can utilize Just-in-Time (JIT) access policies to ensure that privileged accounts only receive the necessary permissions when needed and for a limited duration to further reduce identity attack surface.
AC-L2-3.1.7 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.L2-3.1.8 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-L2-3.1.11 Terminate (automatically) user sessions after a defined condition.	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.

Access Control (AC) (continued)

CMMC regulation	Silverfort security controls
AC-L2-3.1.12 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-L2-3.1.14 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.L2-3.1.20 Verify and control/limit connections to and use of external 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.L3-3.1.2e Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	Silverfort enforces access policies across systems to ensure only authorized users have access. 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.L3-3.1.3e Employ secure information transfer solutions to control information flows between security domains on connected systems.	Silverfort ensures secure authentication for system access, reducing the risk of unauthorized access during data transfer.

Audit and Accountability (AU)

CMMC regulation	Silverfort security controls
AU.L2-3.3.1 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.L2-3.3.2 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.

Audit and Accountability (AU) (continued)

CMMC regulation	Silverfort security controls
AU.L2-3.3.3 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.
AU.L2-3.3.4 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.L2-3.3.5 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.L2-3.3.6 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.
AU.L2-3.3.8 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.L2-3.3.9 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.

Awareness and Training (AT)

CMMC regulation	Silverfort security controls
AT.L2-3.2.1 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.
AT.L3-3.2.1e Provide awareness training upon initial hire, following a significant cyber event, and at least annually, focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.	Silverfort's identity tracking can support management's identification of high-risk users who may need additional training.
AT.L3-3.2.2e Include practical exercises in awareness training for all users, tailored by roles, to include general users, users with specialized roles, and privileged users, that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.	Silverfort's monitoring may aid in recognizing who needs practical training, but Silverfort does not provide training exercises.

Configuration Management (CM)

CMMC regulation	Silverfort security controls
CM.L2-3.4.5 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.
CM.L3-3.4.1e Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.	Silverfort provides visibility into users and their associated access, aiding in component tracking.

Identity and Authentication (IA)

CMMC regulation	Silverfort security controls
IA.L2-3.5.1 Identify system users, processes acting on behalf of users, and 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.L2-3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational 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.L2-3.5.3 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, event those that don't natively support modern authentication protocols. With Silverfort, administrators can automatically discover and classify privileged accounts to enforce Just-in-Time (JIT) access policies with granular allow/deny rules. This ensures privileged users receive the necessary permissions only when needed, minimizing risk and strengthening security posture.
IA.L2-3.5.4 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.L2-3.6.1 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.L3-3.6.1e Establish and maintain a security operations center capability that operates 24/7, with allowance for remote/on-call staff.	Silverfort provides real-time monitoring and alerting that supports incident response.
IR.L3-3.6.2e Establish and maintain a cyber incident response team that can be deployed by the organization within 24 hours.	Silverfort's SIEM integration and adaptive risk scoring allow for analysis of alerts.

Maintenance (MA)

CMMC regulation	Silverfort security controls
MA.L2-3.7.5 Require multi-factor 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.L2-3.9.2 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 Assessment (RA)

CMMC regulation	Silverfort security controls
RA.L2-3.11.1 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.
RA.L2-3.11.2 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.

Security Assessment (CA)

CMMC regulation	Silverfort security controls
SC.L2-3.13.1 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.L2-3.13.3 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.L2-3.13.6 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.L2-3.13.15 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.L3-3.13.4e Employ physical isolation techniques or logical isolation techniques or both in organizational systems and system components.	Silverfort can enforce logical isolation via authentication firewall policies, without requiring endpoint agents.

System and Information Integrity (SI)

CMMC regulation	Silverfort security controls
SI.L2-3.14.6 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.L2-3.14.7 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.

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