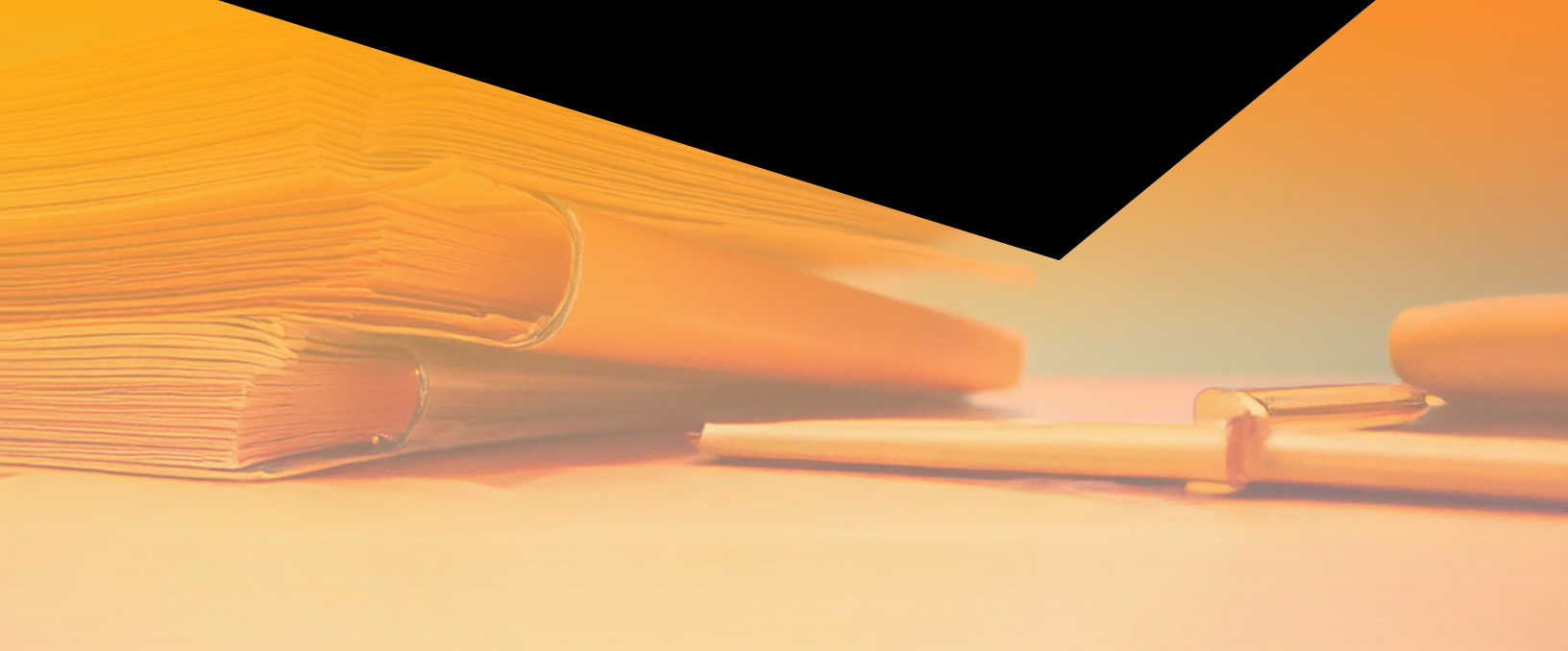
Silverfort

Silverfort Identity Security for NIST SP 800-171

Whitepaper



Executive summary

The National Institute of Standards and Technology (NIST) published NIST Special Publication 800-171, Protecting Controlled Unclassified Information (CUI) in Non-Federal Systems and Organizations, in June 2015. It is designed to provide federal contractors and non-federal organizations with a comprehensive framework for safeguarding sensitive information, otherwise known as Controlled Unclassified Infor-mation (CUI), when it is stored or processed outside of federal systems.

CUI is information that requires protection due to its sensitive nature in areas such as defense, healthcare, or critical infrastructure, despite not being classified. NIST SP 800-171 is intended for contractors, subcontractors, and organizations that handle or store CUI on behalf of the U.S. government. Organizations working with government agencies like the Department of Defense (DoD) and other federal agencies, especially those engaged in defense-related activities, are required to comply with NIST SP 800-171.

Addressing the identity security aspects of NIST SP 800-171

Cyberattacks have shifted their focus from exploiting purely technical vulnerabilities to making use of com-promised credentials, weak authentication mechanisms, and poorly managed access controls. Identity se-curity is now at the forefront of protecting Controlled Unclassified Information (CUI), especially for non-fed-eral organizations that work with federal agencies.

NIST SP 800-171 emphasizes the importance of authenticating users and devices and controlling access to ensure only authorized personnel can interact with CUI. Requirements such as multi-factor authentication (MFA), regular auditing, and limiting access to all user and service accounts based on the principle of least privilege, directly address the identity security vulnerabilities attackers love to exploit.

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 NIST SP 800-171 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 to NIST SP 800-171

3.1 Access control

NIST regulation	Silverfort security controls
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, admins 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.
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 is allowed to 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 of these policies, alerting, MFA, or blocking access to all users who were defined in the policy can be enforced.
3.1.3 Control the flow of CUI in accordance with approved authorizations.	Silverfort enforces centralized access control policies across all environments, ensuring only authorized users can access CUI. Silverfort continuously validates user identities with MFA protection, providing granular control and real-time monitoring of access to CUI.
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Silverfort enforces role-based access controls and segments users' access across all resources. In this way, each role has distinct permissions, and no single user has access to all resources, reducing the possibility of malicious activity. Through centrally managed and monitored access activities and security controls, Silverfort prevents unauthorized users from escalating privileges or combining duties, thereby reducing collusion risks.
3.1.5 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 is allowed to access. Additionally, Silverfort enables administrators to monitor all authentications carried out by privileged accounts.
3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.	Silverfort can be used to limit 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.
3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Silverfort supports the 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.
3.1.8 Limit unsuccessful logon attempts.	Silverfort employs an adaptive blocking policy that locks authentication following a configurable number of unsuccessful logon attempts. Additionally, Silverfort has a built-in brute force detection module.

3.1 Access control (continued)

NIST regulation	Silverfort security controls
3.1.11 Terminate (automatically) a user session after a defined condition.	Silverfort monitors and controls each authentication separately so that even if an initial login to the network is verified, further resource access that poses a risk will be blocked.
3.1.12 Monitor and control remote access sessions.	Silverfort access control policies apply to every access that entails an authentication via the organization's directory services infrastructure, whether internal or remote. Additionally, Silverfort monitors all remote access attempts and supports exporting them in the form of a dedicated report.
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.
3.1.20 Verify and control/limit connections to and use of external systems.	Silverfort access control policies can be applied to any user access that requires authentication via the directory services infrastructure of the organization, regardless of whether the device or resource is internal or external.

3.3 Audit and accountability

NIST regulation	Silverfort security controls
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.
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 through its platform. It ensures that all actions, including access attempts and resource usage, are tied to individual user identities. By enforcing MFA and logging all user activities, Silverfort allows for precise tracking of each user's actions, ensuring accountability.
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.

3.3 Audit and accountability (continued)

NIST regulation	Silverfort security controls
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 that are related to the logging process.
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 the reporting and response process for unlawful or unusual activities, supporting efficient investigations and incident response.
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 or security reviews are required, this streamlined approach facilitates faster analysis and reporting.
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, ensuring unauthorized individuals cannot view, modify, or delete 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.
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 that 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 sensitive logging functions are managed securely and in compliance with established policies.

3.5 Identification and authentication

NIST regulation	Silverfort security controls
3.5.1 Identify system users, processes acting on behalf of users, and devices.	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 access from any accounts that display anomalous behavior. Silverfort provides full visibility into all user accounts' authentication trails, while alerting on any excessive access requests and detected malicious activity.

3.5 Identification and authentication (continued)

NIST regulation	Silverfort security controls
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 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.
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, even those that don't natively support modern authentication protocols. This ensures every user must verify their identity before accessing resources.
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.	Silverfort assigns each incoming access attempt a unique ID which is bound to the step-up authentication 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.

3.6 Incident response

NIST regulation	Silverfort security controls
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.
3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Silverfort provides real-time tracking and logging of security incidents related to authentication and access activities. It can automatically document incidents and generate detailed reports, which can be shared with designated internal and external members of an organization. Silverfort integrates with incident response systems and SIEM tools, ensuring incidents are reported promptly to the appropriate authorities. This facilitates timely investigation and response while maintaining compliance with organizational policies.

3.7 Maintenance

NIST regulation	Silverfort security controls
3.7.5 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 that only authenticated and authorized users can establish these sessions, adding an extra layer of security.
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, even those that don't natively support modern authentication protocols. This ensures every user must verify their identity before accessing resources.
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.	Silverfort assigns each incoming access attempt a unique ID which is bound to the step-up authentication 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.

3.8 Media protection

NIST regulation	Silverfort security controls
3.8.2 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 that 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 CUI on system media is accessible only to those with approved authorization.

3.9 Personnel security

NIST regulation	Silverfort security controls
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.

3.11 Risk assessment

NIST regulation	Silverfort security controls
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.
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 or compromised passwords and poor authentication practices. This ensures organizations can proactively detect and mitigate authentication weaknesses while maintaining secure access controls across their systems.

3.12 Security assessment

NIST regulation	Silverfort security controls
3.12.3 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 rich interface to examine the different access events and the policies that took place and apply filters.

3.13 System and communications protection

NIST regulation	Silverfort security controls
3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Silverfort monitors any access event, including access at the external and internal boundaries of the information systems. Silverfort provides visibility to these access events and allows the configuration of policies to control and protect these communications with advanced access controls and secure authentication.
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 administrators to these interfaces.

3.13 System and communications protection (continued)

NIST regulation	Silverfort security controls
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.
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.

3.14 System and information integrity

NIST regulation	Silverfort security controls
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.
3.14.7 Identify unauthorized use of organizational systems.	If Silverfort detects malicious activity, it provides information regarding the targeted system as well as the compromised system that was used to target the system.