

Silverfort Identity Security for the NIST Cybersecurity Framework 2.0

WHITEPAPER

Executive Summary

The NIST Cybersecurity Framework 2.0 is an updated version of the original framework developed by the National Institute of Standards and Technology (NIST) to provide guidelines for organizations to manage and reduce cybersecurity risk. The original version of the framework was created in 2014 in response to Executive Order 13636, which aimed to improve critical infrastructure cybersecurity.

The framework is structured around five core functions: Identify, Protect, Detect, Respond and Recover, helping organizations develop a holistic and effective cybersecurity strategy. The NIST 2.0 standards are not mandatory, which means that they do not dictate what security controls you must implement. Rather, it provides a means to assess your cybersecurity risks and develop controls to mitigate them.

Addressing the Identity Security Aspects of NIST 2.0

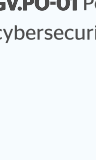
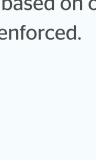

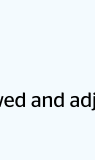
The growing use of compromised credentials for malicious access underscores the importance of protecting the identity attack surface. NIST 2.0 addresses this issue by recommending access policies and procedures for the entire identity lifecycle management process, strong authentication such as multi-factor authentication (MFA), and role-based access control (RBAC) to minimize privileges.

As part of the framework, special attention is given to the need to secure privileged users through strict controls and continuous monitoring and response to cyber threats.

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 (ISMP), advanced MFA, service account protection, and Identity Threat Detection and Response (ITDR).

Silverfort for NIST 2.0 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 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 attacks, privilege escalation, and lateral movement attacks, and respond automatically with real-time blocking.

Mapping Silverfort Capabilities to NIST 2.0

GOVERN (GV)

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Policy (GVPO)

Organizational cybersecurity policy is established, communicated, and enforced.

NIST Regulation	Silverfort Security Controls
GVPO-01 Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	Silverfort enables organizations to apply and enforce cybersecurity in their policies, processes, and procedures. 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. Silverfort enforces these policies in real-time, so only authorized users and devices can gain access to the resources they are assigned to.
GVPO-02 Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	Silverfort's access policies are configured based on the users, groups, and OUs from the directories in the environment, ensuring only authorized users have access to their privileges and organizational classifications, always replacing access policies on the user's login or log files to detect malicious or irregular activity.

Oversight (GVOV)

Results of organization wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.

NIST Regulation	Silverfort Security Controls
GVOV-01 The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	Silverfort provides a Risk Report functionality that enables organizations to create a summary of the entity's identity security posture in a single risk, detailing security items with clear insights into issues that need resolving. This allows detailed guidance on the mitigation and actions for every detected risk and the ability to configure an access policy that prevents many authentications from taking place.

Roles, Responsibilities, and Authorities (GVRR)

Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.

NIST Regulation	Silverfort Security Controls
GVRR-02 Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	Silverfort enables organizations to define and enforce specific access policies based on user roles and responsibilities, ensuring only authorized users have the appropriate level of access. By ensuring clarity and consistency in roles and responsibilities, Silverfort can help enforce cybersecurity controls such as MFA protection or deny access upon login or remote access to on-prem and cloud systems and on any third-party application accessed on-prem or via a cloud directory.

Cybersecurity Supply Chain Risk Management (GVSC)

Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.

NIST Regulation	Silverfort Security Controls
GVSC-01 A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	Silverfort provides organizations with the ability to manage and control all third-party and service chain access by enforcing access policies to all third-party users. Silverfort ensures that all third-party users can access critical systems and data by enforcing precise access controls and multi-factor authentication for third-party access.
GVSC-02 The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.	Silverfort monitors and provides risk analysis of every incoming authentication and access attempt. This enables Silverfort to detect identity threats and act on malicious activity. Silverfort can also enforce security controls such as MFA protection or deny access upon login or remote access to on-prem and cloud systems and on any third-party application accessed on-prem or via a cloud directory.

IDENTIFY (ID)

The organization's current cybersecurity risks are understood.

Asset Management (ID.AM)

Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

NIST Regulation	Silverfort Security Controls
ID.AM-02 Inventories of hardware, services, and systems managed by the organization are maintained.	Silverfort provides an in-depth identity inventory that studies 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 behavior. Silverfort provides full visibility into all user accounts' authentication trails, while alerting on any unauthorized access requests and detected malicious activity.
ID.AM-03 Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	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.
	Silverfort's detection and visibility capabilities enable effective asset prioritization. First, a continuous analysis of authentication and access activities, assigning risk scores to users and machines based on their behavior. This risk analysis helps identify critical assets that are being accessed or targeted, allowing for prioritization based on risk level and potential mission impact.
ID.AM-05 Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	Secondly, Silverfort provides comprehensive visibility into all user access across the organization, including service accounts used by non-human resources. By monitoring these access patterns, organizations can identify which resources are most used or potentially overused, helping to prioritize resources based on their importance to ongoing operations. Finally, Silverfort's threat detection capabilities can identify potential security incidents and risks, helping to prioritize assets based on their vulnerability to threats, which could significantly impact the mission if compromised.

Risk Assessment (ID.RA)

The cybersecurity risk to the organization, assets, and individuals is understood by the organization.

NIST Regulation	Silverfort Security Controls
ID.RA-01 Vulnerabilities in assets are identified, validated, and recorded.	Silverfort integrates with all identity providers to seamlessly monitor all identity traffic and authentication activity in real-time. With complete visibility across all user activity, Silverfort's risk engine can determine the risk of every authentication, so organizations can detect and respond to potential security threats in real-time — including blocking the access of any accounts that display anomalous behavior, while alerting on any excessive access requests and detected malicious activity.
ID.RA-03 Internal and external threats to the organization are identified and recorded.	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.
ID.RA-04 Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	With Silverfort, you can detect and identify potential risks associated with risky users. With continuous monitoring and advanced behavior analytics, Silverfort can identify unusual or risky user behavior that may indicate compromised accounts or identity theft. By recording these potential risks in the Log screen, Silverfort provides organizations with valuable insights into the likelihood and impact of threats, enabling proactive measures to mitigate these threats.
ID.RA-05 Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	Silverfort provides comprehensive insights into user behavior and associated security threats through its risk reports. These reports analyze threats, user and authentication activity and impact to continuously monitor user activities and detect anomalies or risky behaviors. Silverfort's risk reports enable organizations to prioritize risks with a more data-driven approach to help them make informed decisions on where to focus security efforts.

PROTECT (PR)

Safeguards to manage the organization's cybersecurity risks are used.

Identity Management, Authentication, and Access Control (PR.AA)

Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access.

NIST Regulation	Silverfort Security Controls
PR.AA-01 Identities and credentials for authorized users, services, and hardware are managed by the organization.	Silverfort provides comprehensive visibility into all user access across the organization, including service accounts used by non-human resources to access various assets. This visibility can help manage identities for monitoring access patterns and identifying any unusual or unauthorized activities.
PR.AA-03 Users, services, and hardware are authenticated.	Silverfort enforces 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 enforce MFA on any access request, whether on-prem, remote, or third-party, and enforce even the most regular users to administer in an Active Directory (AD) environment. Silverfort can enforce MFA and block access policies on any LDAPs, SAML, 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.
PR.AA-04 Identity assertions are protected, conveyed, and verified.	Silverfort provides comprehensive visibility into all user access across the organization, including service accounts used by non-human resources to access various assets. This visibility can help protect identity assertions by monitoring access patterns and identifying any unusual or unauthorized activities. This allows organizations to configure and apply access policies to ensure only authorized users have access to resources in the environment.
PR.AA-05 Access permissions, entitlements, and authorizations are defined in a policy managed, enforced, and renewed, and incorporate the principles of least privilege and separation of duties.	Silverfort enforces flexible access policies, and organizations can embed cybersecurity into their policies, processes, and procedures. Admins can define access control policies based on specific user roles, risk scenarios and organizational security policies. 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.
PR.AA-06 Physical access to assets is managed, monitored, and enforced commensurate with risk.	Silverfort enhances physical access management to assets by leveraging its advanced detection and visibility capabilities. It continuously monitors authentication and access activities, identifying patterns that indicate unauthorized access attempts and assigning risk scores to users and assets based on behavior. This risk assessment approach prioritizes the physical security of high-risk or high-value assets. Additionally, Silverfort integrates with physical security systems for access control and surveillance, enabling real-time monitoring and enforcement of physical access policies.

Platform Security (PR.PS)

The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.

NIST Regulation	Silverfort Security Controls
PR.PS-04 Log records are generated and made available for continuous monitoring.	Silverfort provides admins with detailed logs of all accounts including Active Directory service accounts. Silverfort documents every authentication and access attempt in the environment.

DETECT (DE)

Possible cybersecurity attacks and compromises are found and analyzed.

Continuous Monitoring (DE.CM)

Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.

NIST Regulation	Silverfort Security Controls
DE.CM-01 Networks and network services are monitored to find potentially adverse events.	Silverfort monitors all authentications between endpoints and the other assets of the organization, and alerts on any anomalous activity. This includes but is not limited to attempts of lateral movement.
DE.CM-03 Personnel activity and technology usage are monitored to find potentially adverse events.	Silverfort monitors all identity traffic and authentication activities across an organization's environment, providing visibility into every authentication and access request. With complete visibility across all user activity, Silverfort's risk engine can determine the risk of every authentication, so organizations can detect and respond to potential security threats in real-time — including blocking the access of any accounts that display anomalous behavior.
DE.CM-06 External service provider activities and services are monitored to find potentially adverse events.	Silverfort enables admins to monitor all third-party authentications requests, as well as detect and prevent their abuses by adversaries for malicious access.

Adverse Event Analysis (DE.AE)

Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.

NIST Regulation	Silverfort Security Controls
DE.AE-02 Potentially adverse events are analyzed to better understand associated activities.	Silverfort provides detailed logs of all user access requests and authentication activities. These logs make security teams to investigate and understand the sequence of events leading up to the adverse incident, enabling them to detect adverse events and identify the root cause in real-time. This proactive approach not only enhances incident response capabilities but also supports ongoing security monitoring and compliance efforts effectively.

RESPOND (RS)

Actions regarding a detected cybersecurity incident are taken.

Incident Analysis (RS.AN)

Investigations are conducted to ensure effective response and support forensics and recovery activities.

NIST Regulation	Silverfort Security Controls
RS.AN-01 Analysis is performed to establish what has taken place during an incident and the root cause of the incident.	Silverfort alerts 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. With 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 continuous monitoring capabilities enable it to detect anomalies and suspicious activities, providing insights into the source of an incident. As a result of this detailed analysis, it is possible to pinpoint the exact time and origin of the problem, thereby facilitating effective remediation and strengthening security overall.

Incident Mitigation (RS.MI)

Activities are performed to prevent expansion of an event and mitigate its effects.

NIST Regulation	Silverfort Security Controls
RS.MI-01 Incidents are contained.	Silverfort enables organizations to begin the IR process with a complete malicious access lockdown. Depending on the severity and scope of the response attack, they can determine the level of lockdown and the balance between MFA and block access policies. Most often, MFA would achieve the same level of containment as block access, while allowing legitimate users to continue to access resources. By utilizing both MFA and block access policies with Silverfort, malicious attempts at logging in to additional resources are prevented. MFA is especially effective since it provides a clear indication of which accounts have been compromised, achieving both containment and recovery simultaneously. This will allow you to rapidly shut down an attack by automatically denying users access to resources until the attack has been eradicated and in recovery mode.
RS.MI-02 Incidents are eradicated.	Silverfort helps create conditions to enabling incident response (IR) teams to block lateral movement and detect compromised user and service accounts. Silverfort's capabilities include configuring MFA and access block policies for any user account, especially the ones that have been identified as compromised. Silverfort also offers automated visibility into service accounts, allowing IR teams to create policies that block access or alert deviations from standard behavior, which are indicators of compromise. Additionally, Silverfort's detailed log screen aggregates authentication and access attempts, assigning risk scores to detect malicious activities. These features allow IR teams to contain threats, eliminate the presence of attackers, and restore systems to their original state, effectively eradicating incidents.

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

