WHITE PAPER

Security Simplified: NIST

Practical tools for practical problems.

solarwinds

Introduction

IT security and compliance doesn't have to be complicated or out of reach for all but the largest organizations. At SolarWinds, we recognize you need practical solutions to solve practical problems, so we've created a set of tools built around the NIST Cybersecurity Framework. We call it Security Simplified.

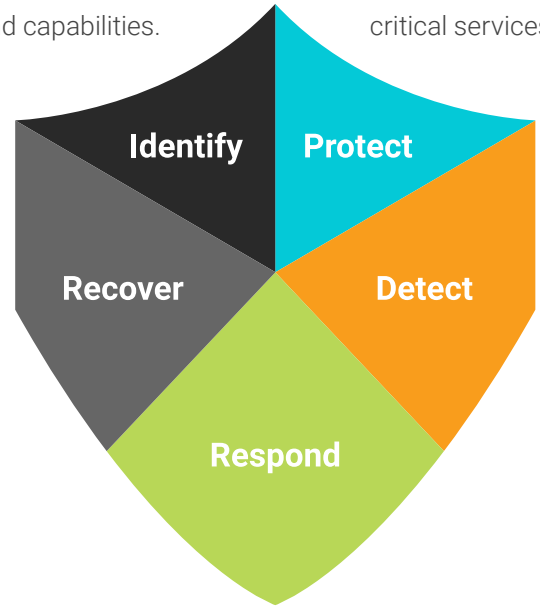
The NIST framework is a risk-based approach to managing cybersecurity risk and is not intended to be a one-size-fits-all set of guidelines. The decision of how to apply it is left to the implementing team.

In this paper, we will explore the functions, categories, and subcategories of the framework core as it relates to IT security and illustrate how SolarWinds tools, specifically, can help your organization demonstrate compliance with the NIST guidelines.

NIST FRAMEWORK

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Develop and implement appropriate safeguards to help ensure delivery of critical services.



Develop and implement appropriate activities to help maintain plans for resilience and restoration.

Develop and implement appropriate activities to help identify the occurrence of a cybersecurity event.

Develop and implement appropriate activities to take action regarding a detected cybersecurity event.

FUNCTION	CATEGORY	SUBCATEGORY	HOW SOLARWINDS CAN HELP
Identify (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to operations.	**ID.RA-2:** Cyberthreat intelligence is received from information-sharing forums and sources.	**SolarWinds Security Event Manager (SEM)** is a security information and event management (SIEM) tool that provides a continuously updated threat intelligence feed that monitors IP address for behavior from known bad actors. solarwinds.com/sem
Protect (PR)	**Identity Management, Authentication, and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistently with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. **PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	**SolarWinds Access Rights Manager (ARM)** helps improve security posture and mitigate insider threats by providing management and auditing of user access rights to Active Directory®, Exchange™, SharePoint®, and file servers. With ARM, users can audit access, permissions, and authorizations of users and devices based on the principle of least privilege. Custom compliance-ready reports can be easily generated in minutes. solarwinds.com/arm
		PR.AC-5: Network integrity is protected.	SolarWinds Network Configuration Manager (NCM) automated network configuration tools provide the ability to establish baseline configurations and bulk-deploy throughout your infrastructure. Compare configurations side-by-side to quickly identify differences, detect unauthorized changes, and back up for restore or disaster recovery. NCM also integrates with the National Vulner- ability Database to aid in the identification of vulnerabilities. solarwinds.com/ncm
	Data Security (PR.DS): Information and records (data) are managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availibility of information.	**PR.DS-1:** Data at rest is protected. **PR.DS-5:** Protections against data leaks are implemented.	SolarWinds Access Rights Manager (ARM) helps protect data at risk and prevent data leaks by monitoring and managing access to sensitive data. The ARM permissions visualization and activity log book make it easy to identify at-risk data. solarwinds.com/arm
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SolarWinds Patch Manager automates patching of software for Microsoft® servers, workstations, and third-party software applications. With Patch Manager, users can easily verify software integrity. solarwinds.com/patch-manager

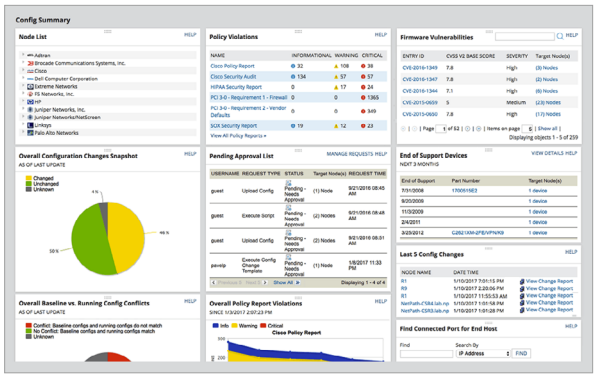
FUNCTION	CATEGORY	SUBCATEGORY	HOW SOLARWINDS CAN HELP
Protect (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (addressing purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**IPR.IP-1:** A baseline configuration of information technology/ industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality). **PR.IP-3:** Configuration change control processes are in place.	**SolarWinds Network Configuration Manager (NCM)** automated network configuration tools provide the ability to establish baseline configurations and bulk-deploy throughout your infrastructure. Compare configurations side-by-side to quickly identify differences, detect unauthorized changes, and back up for restore or disaster recovery. NCM also integrates with the National Vulnerability Database to aid in the identification of vulnerabilities. solarwinds.com/ncm
		PR.IP-4: Backups of information are conducted, maintained, and tested.	SolarWinds Backup is a unified, cloud-based backup service that provides fast backup and rapid restore with built-in compression and deduplication. solarwinds.com/backup
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	SolarWinds Access Rights Manager (ARM) allows for simple provisioning, modification, and deprovisioning of users and their access permissions. solarwinds.com/arm
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	Log auditing and compliance reporting are at the heart of **SolarWinds Access Rights Manager and Security Event Manager (formerly Log & Event Manager)**. Customizable reports are easily generated to help demonstrate compliance across industry-specific IT regulatory frameworks. solarwinds.com/arm solarwinds.com/sem
		PR.PT-2: Removable media is protected, and its use is restricted according to policy.	S**olarWinds Security Event Manager (SEM)** is an on-premises SIEM tool that helps make it easy to use logs for security, compliance, file integrity, and USB device monitoring. The SEM built-in USB analyzer provides insight into USB device and file activity. solarwinds.com/sem
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected, and the potential impact of events is understood.	DE.AE-2: Detected events are analyzed to understand attack targets and methods. DE.AE-3: Event data are collected and correlated from multiple sources and sensors	SolarWinds Security Event Manager is a SIEM tool to monitors, responds to, and reports on security threats in near real time. It receives continuously updated threat intelligence and log data from multiple sources, and correlates data to detect and analyze external threats. solarwinds.com/sem

FUNCTION	CATEGORY	SUBCATEGORY	HOW SOLARWINDS CAN HELP
Detect (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.	SolarWinds Security Event Manager monitors your network and helps protect against potential cybersecurity events. It includes near real-time event correlation, automated threat remediation, and advanced search and forensic analysis. solarwinds.com/sem
Respond (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated.	SolarWinds Access Rights Manager and Security Event Manager include advanced alerting and notification engines, so you'll be the first to know when issues arise. solarwinds.com/arm solarwinds.com/sem
		RS.AN-3: Forensics are performed.	Perform forensic analysis to support recovery activities with archives and correlation engines. solarwinds.com/arm solarwinds.com/sem
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained. **RS.MI-2:** Incidents are mitigated.	Contain and mitigate risks using the advanced detection and analysis capabilities of SolarWinds Access Rights Manager, Security Event Manager, and Patch Manager. solarwinds.com/arm solarwinds.com/sem solarwinds.com/patch-manager

SOLARWINDS TOOLS SUPPORTING NIST

SolarWinds Network Configuration Manager

Automated network configuration and compliance management

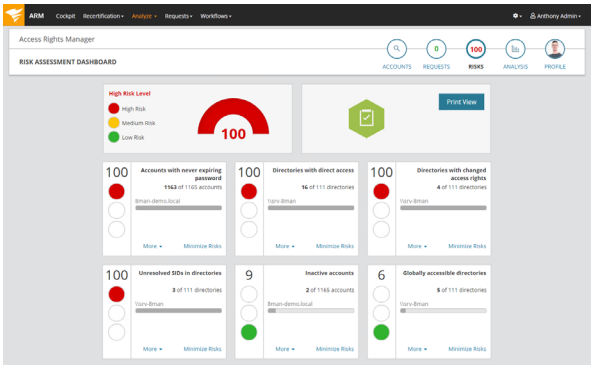


Key Features

- Network automation
- Network compliance
- Configuration backup
- Vulnerability assessment
- Network Insights for Cisco® ASA and Cisco Nexus®
- Integration with Network Performance Monitor

SolarWinds Access Rights Manager

Manage and audit user access rights across your IT infrastructure



Key Features

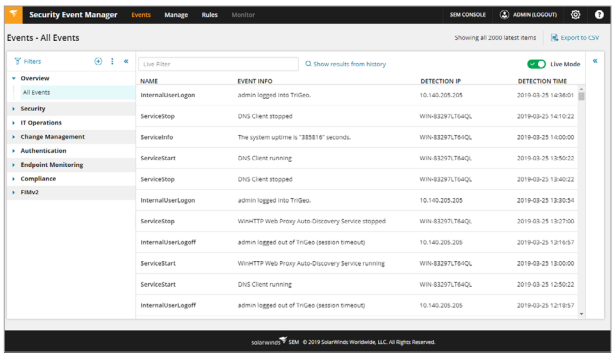
- Monitoring of Active Directory®
- Auditing for Windows File Share
- Monitoring of Microsoft Exchange™
- SharePoint® access monitoring and management
- User provisioning and management
- User permissions analysis

SolarWinds Security Event Manager

Use event logs for security, compliance, and troubleshooting

Key Features

» Integrated compliance reporting tools
» Event-time correlation of security events
» Automated threat response
» Advanced search and forensic analysis
» File integrity monitoring
» USB device monitoring

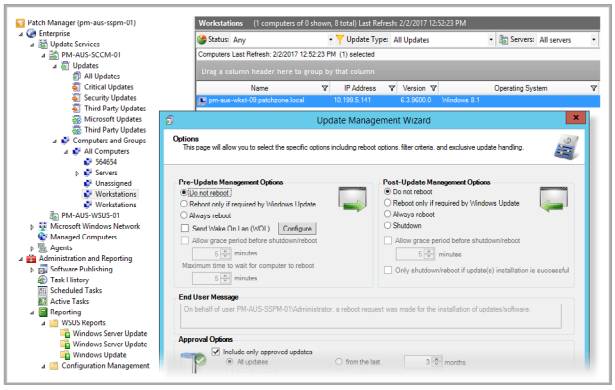


SolarWinds Patch Manager

Patch management software designed for quickly addressing software vulnerabilities

Key Features

» Microsoft WSUS patch management
» Integrations with SCCM
» Vulnerability management
» Prebuilt/pretested packages
» Patch compliance reports
» Patch status dashboard



SolarWinds is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size, or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premises, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals—IT operations professionals, DevOps professionals, and managed service providers (MSPs)—to understand the challenges they face maintaining high-performing and highly available IT infrastructures. The insights we gain from engaging with them, in places like our THWACK online community, allow us to build products that solve well-understood IT management challenges in ways that technology professionals want them solved. This focus on the user and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as a worldwide leader in network management software and MSP solutions.

Learn more today at solarwinds.com