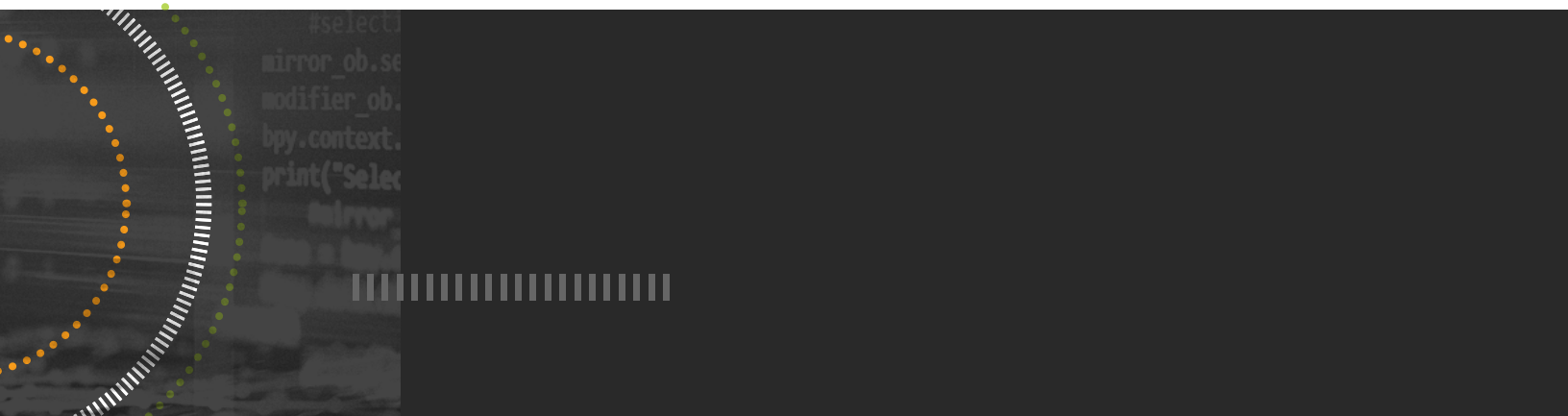
solarwinds government

WHITEPAPER

The Ultimate Guide to Federal IT Compliance



Learning SolarWinds to Solve Your Security Challenge

Every federal IT pro is familiar with cybersecurity, its importance, and its challenges. That said, an ultimate understanding can be gained by taking a historic perspective, and bringing it forward: knowing how—and by whom—cybersecurity rules and regulations were created, then connecting this information to today's solutions. This perspective can help provide a broader understanding of one of the federal IT pros greatest challenges.

THE COMPLIANCE CHALLENGE

Federal Guidelines

Today's security standards for computing systems owned or operated by and for the US Government have been set by two principle overarching entities: the US Congress and the National Institutes of Standards and Technology (NIST).

In 1996, Congress directed NIST to develop and issue best practices and other guidance for secure operation of US Government systems; in response, NIST developed the Federal Information Processing Standards Publications (FIPS PUB) standards. The most relevant publications, "Standards for Security Categorization of Federal Information and Information Systems" (FIPS PUB 199) and "Minimum Security Requirements for Federal Information and Information Systems" (FIPS PUB 200) require federal agencies to categorize the security levels of their information systems based on the types of information the systems will process and/or store.

Agencies must categorize their information systems as low-, moderate-, or high-impact for each of three primary information security objectives: confidentiality, integrity, and availability (CIA). The overall impact categorization of a system is usually equal to the highest impact assigned to any of the three objectives. In other words, a system categorized as "low-moderate-low" based on the CIA security objectives will carry an overall impact categorization of "moderate." Each system will need this defined categorization before one can begin the process of selecting security controls, as the controls are dependent on the categorization (higher-impact systems will have more stringent security controls).

Six years later, Congress further strengthened requirements for US Government systems by enacting the Federal Information Security Management Act (FISMA) of 2002. FISMA has since been implemented across the Federal Government through a variety of named processes and procedures, guided by NIST standards and agency-specific guidance. FISMA requires Federal agencies to safeguard systems based on the impact categorization (FIPS 199) such that residual information security risk is mitigated to an acceptable level.

The principal guidance documents that support FISMA implementation again come from NIST: Special Publications 800-53, and 800-37. NIST SP 800-53 outlines the method for selecting baseline security controls for the chosen system based on its impact categorization; 800-37 outlines a FISMA-compliance process called the Risk Management Framework, or RMF, and the six high-level tasks required to ensure a system meets federal IT compliance standards.

The fifth iteration (Revision 5) of NIST 800-53 was published in September 2020, and was updated in December 2020.

New requirements for contractors:

Cybersecurity Maturity Model Certification (CMMC)

In 2020, contractors and service providers to the Department of Defense (DoD) were required to demonstrate compliance with the Cybersecurity Maturity Model Certification (CMMC) framework to remain eligible to bid and perform work for the DoD. Certification implementation is being phased in over five years, and interim rules require vendors to assess and report scores on their 800-171 compliance.

In 2015, NIST published an additional type of guidance—NIST SP 800-171—to help protect Controlled Unclassified Information (CUI).

Unlike previous NIST guidance, which was focused primarily on ensuring government systems are FISMA compliant, 800-171 requires security compliance initiatives on the part of the government contractors who process, store, and use government-provided CUI in non-government systems. In other words, security compliance requirements now extend beyond federal agencies' systems to include federal contractors' systems.

What comprises CUI? For starters, it encompasses common and expected privacy information like PII and other data identifying government personnel. CUI may also comprise government acquisition information, including quantity and pricing data inherent to acquisitions processes.

The government initially required 800-171 compliance for DoD contracts and contractors; this requirement was expanded and includes civilian agency contractors who generate, store, and process CUI. In other words, all contractors must be aware of this relatively new requirement. Of particular note is the potential cost of meeting the requirement, which will have to be factored into bidding strategies and overall corporate expenses.

Security Controls and STIGs

The federal IT security pro is required to implement a particular set of security controls based on the impact categorization of a given system. A high-impact system can have more than 1,700 possible security controls and sub-controls, also called "enhancements," necessary to secure—or harden—that system. Since each control can be its own set of tasks based on the variables of the system and its components, the government has created further guidance and tools for ensuring these controls are chosen and implemented correctly.

The DoD, through the Defense Information Systems Agency (DISA) Field Security Operations (FSO), has created hundreds of highly detailed guides for a wealth of systems components including operating systems, application servers, database servers, switches, firewalls, and other common computing system components. These guides are known as the Security Technical Implementation Guides, or "STIGs" for short.

How do agencies use STIGs? Let's take a common system component as an example: a STIG for a Cisco® router will not only mandate using passwords to restrict router access, but also provide iOS® configuration instructions for how to properly configure password authentication. Government and industry have developed automated and manual tools for testing STIG compliance for each system component to ensure the component is hardened such that it maintains a baseline security configuration that meets the requirements of the chosen impact level.

Additional Guidance

The government's Executive Branch also offers guidance, in several different forms.

In March 2021, the White House released its Interim National Security Strategic Guidance, and in May 2021, they issued an Executive Order on improving the nation's cybersecurity, both designed to confront a range of the nation's cybersecurity challenges.

Prior, in September 2018 the White House issued the National Cyber Strategy, a relatively high-level memorandum with a four-pillar approach to protecting the nation's data. The objective of each of these pillars, according to the White House, is:

- **Pillar 1:** Manage cybersecurity risks to increase the security and resilience of the Nation's information and information systems.
- **Pillar 2:** Preserve United States influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency.
- **Pillar 3:** Identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace.

» **Pillar 4:** Preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is reinforced by United States interests.

As mentioned, the Executive Branch also issues executive orders. These memorandums require specific additional security efforts such as encryption standards for data-at-rest and data-in-transit, as well as identity management requirements through the issuance of smart cards to US Government personnel and their contractor partners.

The memorandums further define the types of collected and stored information that require additional security safeguards, such as Personally Identifiable Information (PII). Office of Management and Budget (OMB) Memorandum M-07-1616 defines PII as information sufficient to identify an individual alone, or when combined with other identifying information. PII is protected by The Privacy Act of 1974. Another form of such protected information is Electronic Protected Health Information (ePHI), information that is protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Cybersecurity is clearly complex and is guided by an equally complex series of concepts, processes, guidelines, and requirements. Every effort is of critical importance. Consider the current threat landscape comprising bad actors, data breaches, insider threats, poorly configured software, and system components that require the regular application of vendor security patches to ensure a baseline security configuration is maintained.

Now let's add the inevitable staffing shortages from lengthy hiring and acquisition processes, competition from the private sector, and all the skills and certifications required to qualify for security work in the US Government. Securing an agency against cybersecurity threats is a difficult situation and only grows more challenging by the day.

Despite the complexity of the challenge, there are best-practice solutions and basic steps Federal IT pros can implement to help secure systems and data within a timeline that supports agency IT initiatives.

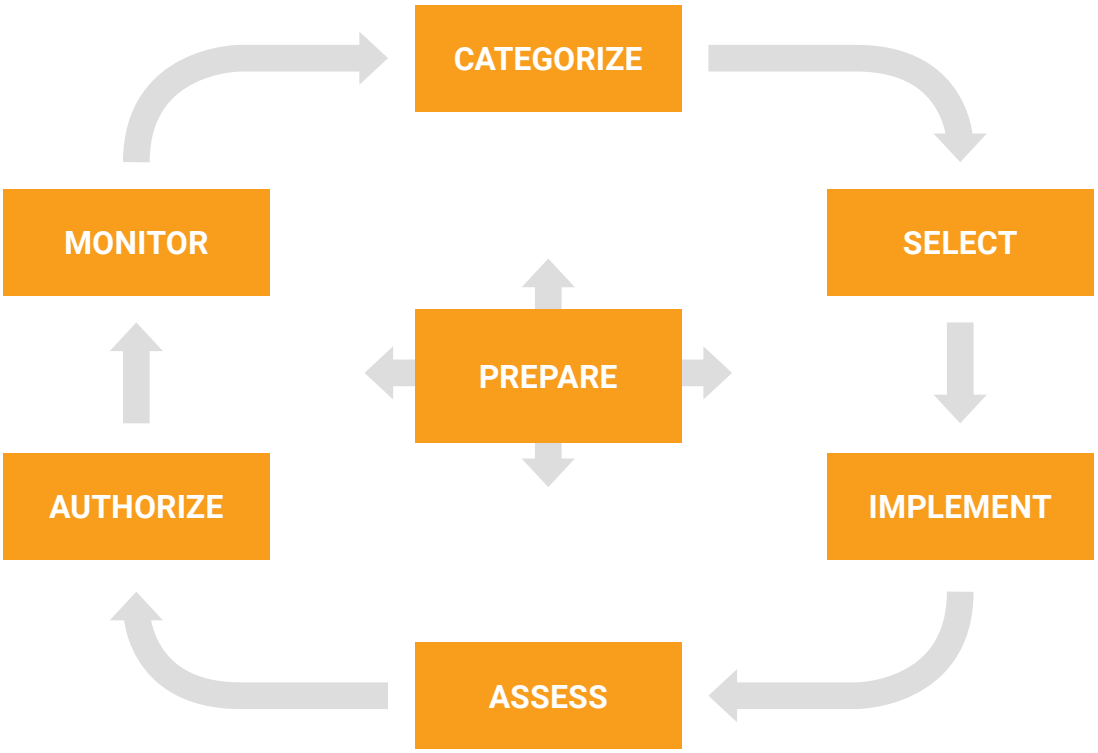
CYBERSECURITY BEST PRACTICES: RMF AND BEYOND

RMF Compliance

FISMA requires each federal agency to implement information security safeguards, audit these safeguards annually, and report the results to the Office of Management and Budget (OMB). The OMB, in turn, prepares an annual compliance report for Congress. This concerted effort taken together strengthens the cybersecurity of US Government systems and data and dramatically reduces risk.

RMF has traditionally mapped out six steps toward compliance and risk reduction:

» Step 1: Categorize Risk. Meet this need by applying the standards outlined in FIPS 199 and 200. The end result should be an impact categorization of low, moderate, or high.



Source- NIST Publication RMF 2.0 Risk Management Framework

» Step 2: Select Security Controls. Choose a set of security controls from NIST SP 800-53 based on the categorization chosen in step 1.

» Step 3: Implement Security Controls. Begin the process of applying controls to a given system. Some controls may be met by policies and management decisions, others by technical efforts. Automated tools can dramatically speed up these processes.

» Step 4: Assess Security Controls. Begin to test that the security controls chosen have been applied correctly. Automated tools really shine here, especially for those controls with a technical test mechanism.

» Step 5: Authorize Information System. Now that controls have been implemented and validated, it's time to get approval for the system to operate.

» Step 6: Monitor Security Controls. A key differentiator of the Risk Management Framework over previous security compliance processes is the notion of continuously monitoring the system and its controls to ensure the system remains secure across the system life cycle.

The newest revision (NIST SP 800-37 Revision 2) of RMF also includes a "Prepare" step organizations should take before beginning the six-step process outlined above. At a high level, this new step focuses on assigning risk management roles, developing a risk-management strategy, and conducting enterprise-level risk assessments. The goal

is to encourage more effective communication between executives and operational staff; identify common controls and tailored control baselines; reduce complexity of the infrastructure; and increase emphasis on the protection of high-value assets.

According to NIST: "Without adequate risk management preparation at the organizational and system levels, security and privacy activities can become too costly, demand too many skilled security and privacy professionals, and produce ineffective solutions."

Released in December 2018, RMF 2.0 includes Prepare as the first step, followed by the "Categorize Step" and continuing through seven steps all together.

FISMA compliance efforts for government systems must adhere strictly to all RMF steps to minimize risk to government systems, data, and the business processes reliant on secure computing. And, yes, RMF provides a framework combining IT security and risk management to enable a more dynamic approach to managing agency risk.

Successfully reducing risk goes beyond RMF and FISMA compliance.

Beyond RMF

First and foremost, ensure good cyber hygiene. Make sure all systems are up to date on all hardware and software updates and patches. New malware is introduced every day; ensuring all systems are up to date should be the agency baseline.

In addition to standard cyber hygiene, there are also several fundamental steps every federal IT pro should take to help ensure a strong security foundation.

1. Create an information security framework. This should encompass a series of well-documented policies, guidelines, processes, and procedures about how best to implement and manage ongoing security within your agency. There are several established security frameworks, but the US government most closely follows the guidelines set forth in NIST SP 800-53 to comply with the FIPS 200 requirements.
2. Develop a consistent training program. Train the team to understand how to recognize potential vulnerabilities quickly and how to find the gems of important information within a sea of security-related alerts and alarms. Train developers on secure coding methodologies. And, train end users on things like creating strong passwords, identifying phishing emails and other social-engineering attacks, and what information can and cannot leave the confines of the agency.

3. Monitor and maintain IT systems. Day-to-day security monitoring and maintenance is the key to successful day-to-day risk and vulnerability mitigation. Having a strong backup system in place is part of this maintenance. If a breach occurs and data is compromised, a good backup system will ensure minimal data and productivity loss.

Next, even with a solid program for cyber hygiene and a solid security foundation, there are additional things the federal IT pro can do to help reduce agency risk, particularly in light of unique challenges that come with federal security.

» Complexity: Agency environments can be quite large and quite complex. Tools that can help determine the perimeter of your network boundary and account for all devices communicating on the network are invaluable.

» Change: Federal environments change over time. Tools that can capture an existing environment and its baseline configuration settings and then capture changes over time allow analysts and architects the ability to find and resolve performance issues and vulnerabilities related to misconfiguration in the environment based on real, quantifiable evidence.

» Too much information: System components generate vast quantities of data in the form of logs. A SIEM tool can help your team wade through these details and find anomalies indicative of device misconfiguration, improper data or location access, privilege escalation, compromise, and more. The use of a SIEM can provide actionable insight and meet access management and other security controls under RMF.

Finally, an organization called the Center for Internet Security (CIS) can provide even further assistance. Specifically, CIS provides a comprehensive security framework called The CIS Critical Security Controls (CSC) for Effective Cyber Defense that provides agencies with a set of clearly defined controls to reduce the risk of cyberattack and improve IT security posture. The framework consists of 20 controls. According to CIS, implementation of the first five controls provides effective defense against 85% of the most common cyberattacks.

Those first five controls are:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges

CIS provides guidance on how to implement the controls and which tools to use to reduce the burden on security teams.

Auditing and Automation

Security audits are a core component of ongoing security best-practices and are part of agency FISMA requirements. The goal of the audit is to ensure compliance requirements are being met.

So, what should federal IT security pros expect for the audit process?

First, expect the audit to take place on-site. The auditor will need a place to work as well as one or more sets of temporary credentials to access the target system or network as well as associated documentation.

For most of the audit, the auditor will perform a range of verifications to ensure compliance requirements are being met. For example, the auditor likely will verify:

- A security categorization has been chosen for the target system (per FIPS 199 and 200) and the security categorization is accurate
- The security controls selected for the system align with the chosen security categorization (low/moderate/high) impact level and controls detailed in NIST SP 800-53, Appendix D, for the corresponding impact level (low/moderate/high)
- Security controls have been accurately selected and implemented

Auditors may choose to create one or more vulnerability and risk reports as outputs for their testing efforts. Based on this report, identified vulnerabilities may require a mitigation tracking document (e.g., a Plan of Actions and Milestones, or POA&M) identifying the severity of each vulnerability and the responsible parties for ensuring the vulnerability is addressed, a timeline for addressing the vulnerability, and the level of effort for the mitigation activities.

Based on this, what should the federal IT security pro do to prepare? Here are a few tips:

- Ensure all necessary personnel are available on the audit date(s) during core testing activities, and be sure all personnel contact information is accurate and up to date
- Ensure all system function and security documentation exists, is up to date, and is available on the audit date
- Validate that an accurate security categorization has been chosen for each application in the environment
- Validate that security controls have been selected and implemented based on that categorization level
- Verify the security control validation schedule for those systems

- Verify how and when system and data backups occur and at least one regular backup is maintained offline (on a device unattached to the network and/or on an external backup resource)
- Verify the system patch schedule with technical personnel, obtain current patch status, and quantify all known patches that have yet to be applied

Meeting compliance requirements—particularly in advance of an audit—can be incredibly time consuming. Automation can go a long way toward meeting these requirements while saving valuable federal IT personnel time.

Automating continuous monitoring is the first and likely most helpful aspect of compliance automation. In fact, automation is a core intent of continuous monitoring as this approach can dramatically streamline security processes.

Many aspects of continuous monitoring can be automated through the use of tools designed specifically for this task. For example, the federal IT security pro can automate attack-surface discovery by regularly scanning for open ports, protocols used, and services available from multiple network locations inside and outside the network. Automated scans can ensure patches are applied in a timely manner and security controls continue to be implemented.

Federal IT security pros can also automate log aggregation and other event details in a SIEM, which provides actionable business intelligence on current security status. Automation tools can also provide incident response support and evidence of Indicators of Compromise (IoCs).

Reporting is a critical part of compliance and can be automated. When scans are run, for example, many tools automatically provide output in a report format tied directly to security control validation. These automated reports can provide information on missing patches, non-permitted ports, which protocols or services are available at any network location, and more. Some directly address security controls in NIST 800-53 and other compliance requirements.

All sounds, good, right? But there are still a large amount of security controls to choose, implement, and validate successful implementation. And then there's the accompanying documentation. So let's look at the SolarWinds tools designed to help reduce the federal IT pro's risk exposure and enhance the path toward FISMA and RMF compliance.

SolarWinds Compliance Solutions

Solar Winds has several products designed to facilitate security control implementation, management, and oversight. For example,

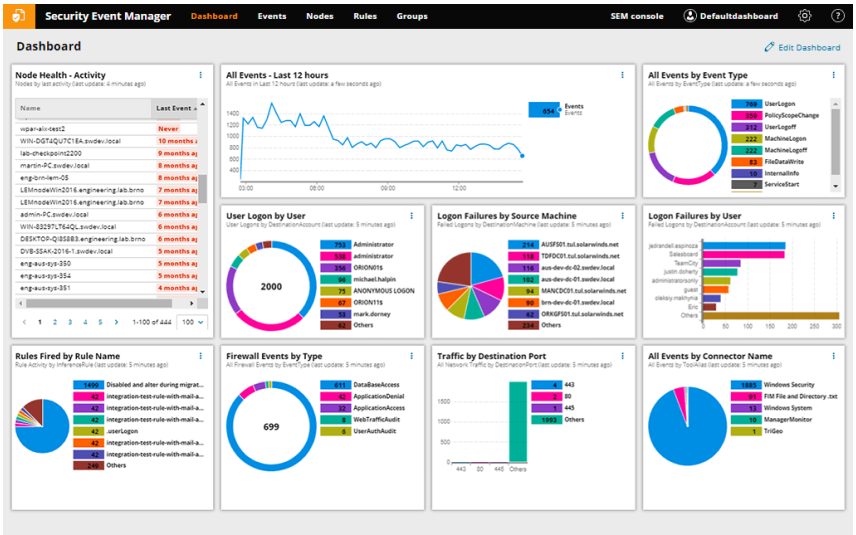
- RMF Step 3, Implement controls: Several SolarWinds products, including Network Configuration Manager (NCM) and Patch Manager, can be used to help satisfy controls or to help implement and manage implementation of controls.

- RMF Step 4, Assess controls are working correctly: SolarWinds security product portfolio, including NCM, and SolarWinds Security Event Manger (SEM) can be used to help make sure controls have been implemented correctly.
- RMF Step 6, Monitor: Several SolarWinds products including SEM, Network Performance Monitor (NPM) and NCM can be used to help make sure controls are working as expected, bypasses aren't attempted, and produce reports that can be used to prove controls have been correctly implemented.

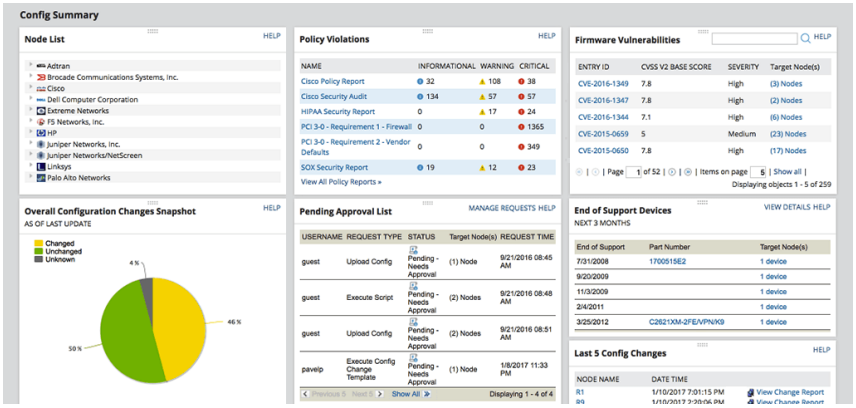
NCM and SEM

Let's start by examining two of the most critical tools SolarWinds offers for helping federal IT pros meet FISMA and RMF compliance demands.

- SolarWinds Security Event Manger (SEM): SIEM tools can make it easier to use event logs for security, compliance, and troubleshooting and simplify many aspects of FISMA compliance. SEM comes bundled with hundreds of built-in reports, many of which are designed to directly support FISMA compliance efforts. These reports rapidly address the Assess/Monitor activities by helping look for exceptions to controls, unexpected changes or activity, or attempts to bypass controls. In addition, SEM includes dozens of correlation rules categorized for compliance initiatives, including FISMA. SEM additionally supports file integrity monitoring, USB device monitoring, automated threat remediation, advance search, and forensic analysis. The tool improves operational security at the same time it streamlines RMF tasks.



» SolarWinds Network Configuration Manager (NCM): NCM includes templates designed to help meet NIST and DISA STIG requirements for network components. These templates can identify services exposed on network devices, identify where and how remote access is enabled on these devices, identify the management protocols used by these devices, and identify key access control lists (ACLs) that should be present to ensure compliance with the relevant security controls. NCM then helps close known vulnerabilities on devices and keeps updated on Cisco devices by accessing the National Vulnerability Database (NVD). The tool supports initial and ongoing network security requirements that dovetail with RMF.



Other SolarWinds tools designed to help with navigating and implementing 800-53, in addition to NCM and SEM, are:

» User Device Tracker (UDT) to detect device usage in classified environments

» Patch Manager to help implement and manage controls

» Network Performance Monitor (NPM) to ensure controls are working as expected

» NetFlow Traffic Analyzer (NTA) to help monitor communications

» Server & Application Monitor (SAM) for enterprise-wide continuous monitoring

» Storage Resource Monitor (SRM) to help detect denial of service (DoS) and resource/performance issues

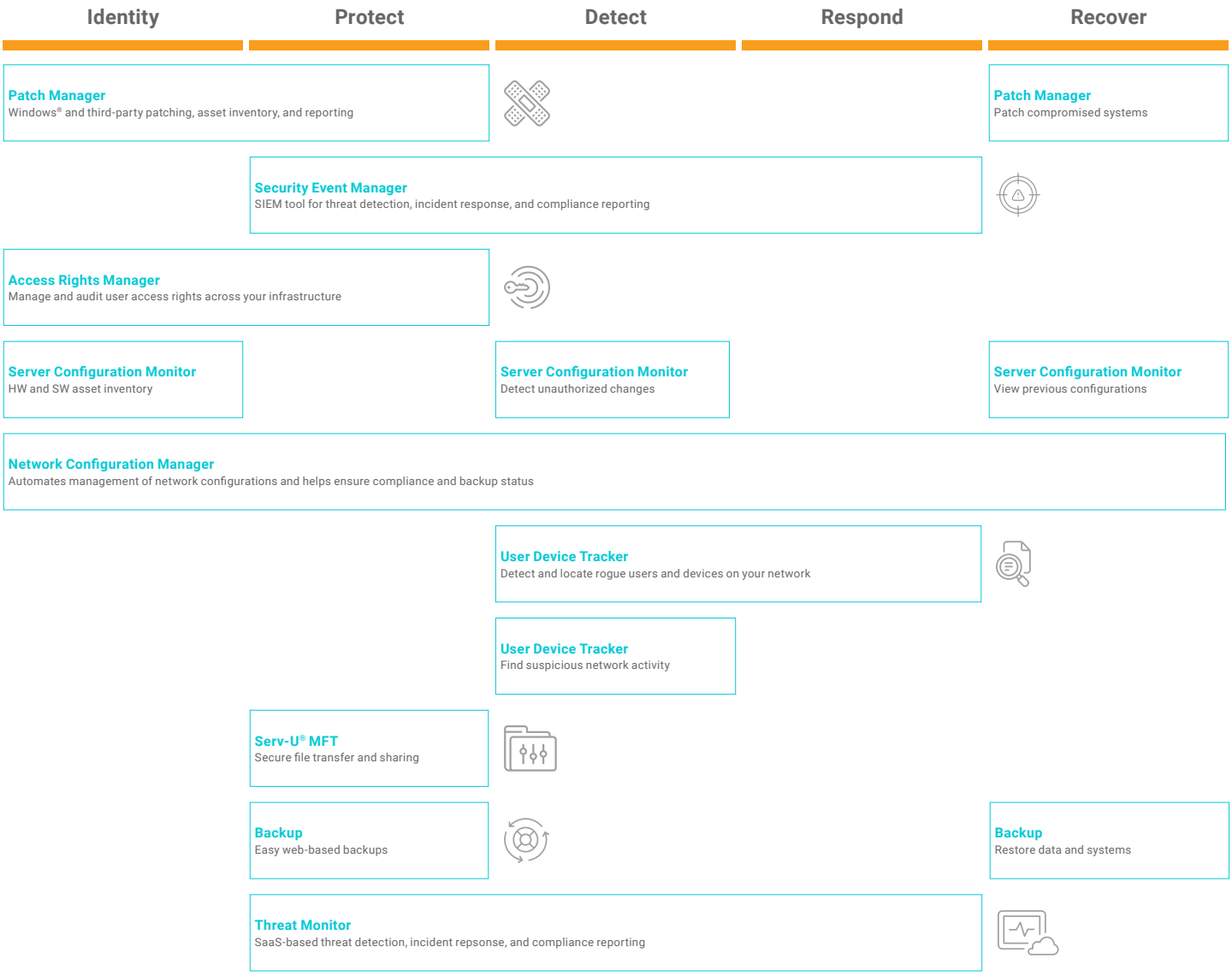
» Database Performance Analyzer (DPA) to identify large queries or unexpected database activity

Next, let's look at SolarWinds Access Rights Manager (ARM) and SolarWinds Server Configuration Monitor (SCM), two SolarWinds products designed to automate monitoring and reporting of common system components and configuration settings over time:

» Access Rights Manager (ARM): This tool monitors user and system account access for common access control components such as Active Directory® and Microsoft® Exchange™. The tool additionally supports auditing of Windows® File Shares a we well as user provisioning, management, and permissions analysis. Lastly, the tool can generate custom reports useful to support compliance reporting and RMF activities.

» Server Configuration Monitor (SCM): This tool monitors system and application changes, server configuration settings and changes for online and offline systems, has a rules engine to support compliance. SCM also includes templates designed to help meet DISA STIG requirements for system components. The tool additionally permits the comparison of configuration changes over time and informs how these changes may have impacted performance. This kind of real-time and historical detail is invaluable when implementing RMF.

SolarWinds Security Products Overview



Other tools, produced by SolarWinds, competitors, and the open-source community can swiftly automate the implementation of other controls by detecting when a restricted port or protocol is in use, whether a critical patch has been applied to close a security flaw, and the like. The shared goal is to allow federal IT personnel to rapidly assess the current security posture of a system, identify flaws, and mitigate those flaws to maintain the security posture for a given system in a manner commensurate with the risk categorization identified.

Enhancing Compliance and Reducing Risk With SolarWinds

IT security threats posed by careless or untrained agency insiders and foreign governments are at an all-time high, according to the 2020 SolarWinds Federal Cybersecurity Survey Report. That said, compliance mandates or regulations and a greater awareness of the sources of security risks have had the greatest impact on the evolution of public sector IT security policies and practices.

Sources of Federal Security Threats - Trend

All sources of security threats have increased since 2014. Six of the eight threat sources are at am all time high.

	2014	2015	2016	2017	2018	2019
Careless/untrained insiders	42%	53%	48%	54%	56%	52%
Foreign governments	34%	38%	48%	48%	52%	48%
General hacking community	47%	46%	46%	38%	48%	40%
Hacktivists	26%	30%	38%	34%	31%	26%
Malicious insiders	17%	23%	22%	29%	36%	29%
Terrorists	21%	18%	24%	20%	25%	22%
For-profit crime	11%	14%	18%	17%	15%	20%
Industrial spies	6%	10%	16%	12%	19%	16%

Note: Multiple responses allowed N=200 ● *= top three sources* ▭ *= statistically significant difference from 2017*

The survey uncovered even more evidence that training and good cyber hygiene all help contribute to a more secure environment. Previous survey respondents cited the following reasons that insider threats have improved or remained in control within their agency environments:

- End-user security awareness training (47%)
- Network access control (45%)
- Patching (43%)
- IT configuration management and reporting (41%)
- Identity and access monitoring tools (39%)
- IT asset management and reporting (31%)

Compliance played an even greater role. According to the survey, 60% of respondents cited "NIST Framework for Improving Critical Infrastructure Cybersecurity" as a contributing factor in managing risk as part of the agency's overall security posture; 55% cited FISMA as a contributing factor; and 52% cited DISA STIGs.

SolarWinds can help federal agencies with all of these, whether basic cyber hygiene or compliance requirements. SolarWinds has the tools, expertise, and experience-based knowledge of the federal space to help any agency enhance its security posture, reduce risk, and more effectively protect agency data—and in turn, the agency mission.

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT management software. Our products give organizations worldwide—regardless of type, size, or complexity—the power to monitor and manage their IT services, infrastructures, and applications; whether on-premises, in the cloud, or via hybrid models. We continuously engage with technology professionals—IT service and operations professionals, DevOps professionals, and managed services providers (MSPs)—to understand the challenges they face in maintaining high-performing and highly available IT infrastructures and applications. The insights we gain from them, in places like our THWACK community, allow us to solve well-understood IT management challenges in the ways technology professionals want them solved. Our focus on the user and commitment to excellence in end-to-end hybrid IT management has established SolarWinds as a worldwide leader in solutions for network and IT service management, application performance, and managed services. Learn more today at www.solarwinds.com.

CONTACT US

PHONE

877.946.3751
+353 21 233 0110

WEB solarwinds.com/government

EMAIL

Federal: federalsales@solarwinds.com
State and Local: governmentsales@solarwinds.com
Education: educationsales@solarwinds.com
National Government: nationalgovtsales@solarwinds.com

solarwinds government

© 2021 SolarWinds Worldwide, LLC. All rights reserved

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.