SOLARWINDS
WHITEPAPER

Daily Federal Compliance & Continuous Cybersecurity Monitoring

solarwinds
The Power to Manage IT

INTRODUCTION

Governments have a critical need for information security. The many agencies that comprise government require and amass great quantities of information. Much of this information is vital to national, economic, and security interests and must be vigorously defended from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction. Therefore, government agencies must comply with strict standards and controls designed to offer these protections.

Defense Information Systems Agency (DISA) is a combat support agency that provides, operates, and ensures command and control, information-sharing capabilities, and a globally-accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of its operations. DISA-managed IT supports some of the most critical programs in the U.S. government, and therefore requires the highest levels of confidentiality and availability.

To achieve its operational objectives, DISA has developed the Security Technical Implementation Guides (STIGs) for securing information and systems under its control. The STIGs are specific to operational and device-level technical controls and how to configure those controls on specific hardware. For 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.

The Department of Defense (DoD), through adoption of the DISA STIGs, was doing a reasonable job of IT security in 2002. However, Congress decided that the civilian agencies were not taking IT security seriously enough, so they created the Federal Information Security Management Act (FISMA) to help the civilian agencies secure their IT systems.

FISMA requires each federal agency to implement information security safeguards, audit these safeguards annually, and make an accounting to the Office of Management and Budget (OMB). The OMB, in turn prepares an annual compliance report for Congress. FISMA standards and guidelines are developed by the National Institute of Standards and Technology (NIST).

FISMA is a risk-based approach and requires every U.S. federal agency to adopt the following process:

1. Categorize information and systems according to confidentiality and availability
2. Design operational and technical controls based on categorization
3. Construct policies mandating what systems and information assets are to be protected using specified controls
4. Verify that controls and policy mitigate risks
5. Implement policies and controls and maintain compliance through regular certification
6. Continuously monitor systems and controls to prevent compliance drift and to update operating and technical controls

As illustrated in this methodology, a risk-based approach requires an organization to identify what information assets require safeguards to:

- Protect information from unauthorized use (e.g., confidentiality)
- Ensure information is available—with integrity—when needed (e.g., availability)

Confidentiality safeguards are typically implemented in layers. Measures are taken to broadly restrict outside access and specifically restrict internal access only to those who have specific permissions. These confidentiality controls are implemented across many IT devices, including firewalls, routers, switches, and servers. Therefore, it should be specifically noted that "network" security—that is, security controls on routers and switches—is an integral part of the larger security strategy and must not be overlooked.

Another important aspect to remember is that policy can mandate both technical and operational controls. A technical control is implemented through hardware or software. It is typically a "feature" controlled by a configuration setting. Operational controls, on the other hand, have more to do with work processes and ensure that proper analysis, planning, and testing have occurred to guarantee that technical controls yield expected results. Both are equally important.

NIST and DISA have been working to consolidate the DISA STIGs and FISMA NIST security controls. The merging of these two sets of similar security guidelines and controls has been going on for years and will likely take years more to complete.

THE PROBLEM

There are a number of challenges that government agencies face to achieve and maintain FISMA and DISA STIG compliance, especially in the area of network security. These are:

- Routers and switches are complex devices and require many commands to properly configure. Routinely examining these configurations and verifying all required technical controls are present and properly implemented (such as DISA STIGs in the case of DoD protected systems) can be daunting.
- Even when technical controls are initially implemented, unless the operational controls are also in place, vulnerabilities will soon appear. IT systems are dynamic and constantly changing, as are the methods attackers use to breach defenses. Therefore, there must be strict management controls in place to manage inevitable change. Unfortunately, there are few specialized tools to help network managers adequately manage operational controls.

THE CONSEQUENCES

The consequences of noncompliance far exceed the threat of simple inconvenience or sanctions. While punitive sanctions are undesirable, the true cost of loss is often measured in human lives, weakening of national security, interruption of crucial services to citizens, or significant economic losses.

For example, Mandiant, a security research firm in Virginia, recently reported that APT1, an alleged cyber-espionage unit of the Chinese People's Liberation Army, had systematically compromised 141 companies across 20 industries and stolen valuable intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, partnership agreements, emails, and more. APT1 is only one example of well-funded organizations that will not only target commercial industries vital to national security, but also directly cyber-attack federal targets.

Another important example is that of Edward Snowden, the computer analyst who provided the Guardian with classified National Security Agency (NSA) documents leading to revelations about U.S. surveillance on phone and Internet communications.

Snowden, by using his knowledge of the NSA's poor control over its SSH and private keys and self-certificates, was able to turn those security assets against the NSA and steal valuable and top secret information. The need for continuous monitoring to stay compliant with information assurance standards like FISMA and the DISA STIGs has never been greater.

Fortunately, even seemingly small measures can have a significant impact. Sustained attacks always rely on finding holes in the defenses. The FISMA/NIST guidelines and DISA STIGs both serve to close those avenues for easy exploit and greater access.

SOLUTION

A recent **SolarWinds® federal cybersecurity survey** showed that:

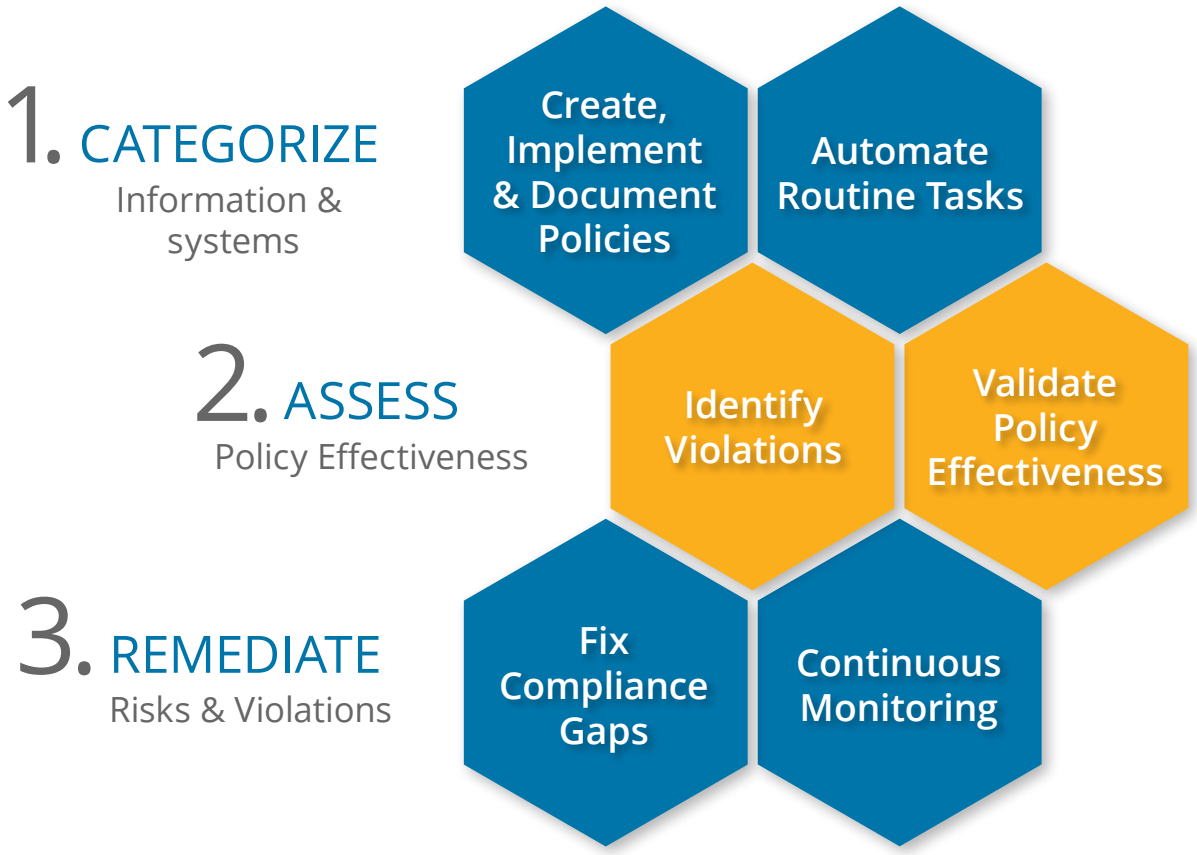
- 47% percent of respondents said the general hacking community is first to blame for cybersecurity breaches. Careless and untrained insiders are a close second at 42%, indicating that insiders may inadvertently pose nearly as many risks as deliberate, malicious hackers.
- 53% of DoD IT pros named careless and untrained insiders as their top security threat sources—more than named foreign governments (48%) or terrorists (31%) as the top threat.

DISA STIGs and FISMA/NIST standards require each federal government agency to develop minimally-acceptable system configuration requirements and ensure compliance with the configuration requirements. Systems with secure configurations are less vulnerable and better able to thwart network attacks.

The exploitation of vulnerabilities must be evaluated at the level of the network device being reviewed. A router, for example, is a standalone device for some purposes and part of a larger system or network for others. All these risk factors are to be considered when developing mitigation strategies at the device and system level:

- Risks to the device
- Risks to the device in its environment
- Risks presented by the device to the environment

Categorizing, Assessing, and Remediating Security Risks



Steps in the process of categorizing, assessing and remediating security risks in accordance with the DISA STIGs and FISMA/NIST standards. Source: SolarWinds

Compliance for your network can be achieved through three simple steps.

1. Categorize Information Systems
2. Assess Policy Effectiveness
3. Remediate Risks and Violations

Let us examine in detail the tasks involved in each step, its significance, and best practices for execution.

INFORMATION SYSTEMS

The first step in this process is to review and inventory all devices in the network. Then, assess compliance requirements and devices that need to be brought into compliance.

For those devices out of compliance, make the required changes and bring them under regulatory controls. Clearly document the applied policies and steps taken to comply with regulatory controls. This is helpful for audit proofs and to maintain an audit trail of what changes were made to the network and when.

Next, automate routine tasks like bulk password changes, perimeter device hardening, configuration backup and archival, configuration changes (e.g., SNMP configuration, VLAN configuration, access control list changes), or even interface configuration changes.

Automation helps reduce human error and systematically conduct routine tasks required to maintain compliance. Network administrators—especially those handling very large networks with hundreds of devices—are finding it increasingly difficult to carry out these repetitive but important tasks manually. Yet, ignoring these everyday jobs or putting them off for extended periods of time can be disastrous to your network.

ASSESS POLICY EFFECTIVENESS

Once security controls are in place, it is important to ensure that they are enforced and followed. Devices need to be continuously monitored and changes tracked. Any new device configuration or change in configuration must conform with internal and external polices documented for the agency.

To ensure continuous compliance, regular audits need to be conducted to assess and identify violations. Validate policy effectiveness separately through analysis and by conducting penetration tests.

Compliance assessment can also be automated with the use of tools that run reports and list policy violations.

Despite the tedium of these tasks, it's very important that they be carried out regularly and effectively. A few steps that help administrators ensure compliance include:

1. Establish baseline configurations so that they can be used in the case of aconfiguration issue.
2. Generate compliance reports that can help verify compliance and point out policy violations.
3. Ensure that security and risk management controls are exercised and practiced.

REMEDIATE RISKS AND VIOLATIONS

Once assessment is complete and security gaps and policy violations listed, the next and most important step is to close these vulnerabilities that put the network at risk.

This is called remediation, and all steps taken need to be documented. All proposed changes must be reviewed and approved by authorized personnel. This helps reduce the chance of errors or misconfigurations.

Use of a tool can help automate the change management approval process with the help of role-based controls. It also provides an audit trail that tracks users who uploaded configurations so the right people can be involved in fixing problems.

The use of an automated tool also simplifies configuration management and can save hours of troubleshooting. In a given scenario, an administrator makes changes to a router one evening and runs through the test plan where all looks fine. However, the next day, the helpdesk is swamped with phone calls related to a problem caused by that change. So, remediation also includes the provision to be able to quickly roll back a bad or unauthorized change.

Finally, continuously monitor devices to know whenever device configurations are changed, even if changes are made directly on the device. This eliminates the problem of mystery changes that haven't been approved and aren't discovered right away, which can reduce downtime.

In short, **continuous monitoring** encourages timely awareness of vulnerabilities, allows faster detection of a possible security incident, ensures latest **compliance** guidelines are in place, and provides clear visibility into compliance status on the network.

Along with increasing requirements from regulatory agencies and a growing awareness of security risks of nonconformity, agencies now implement compliance as an integrated part of their daily operations. To do so successfully, they need the support of easy-to-use technology.

BENEFITS AND SUMMARY

Manual execution is certainly not advisable to carry out the above compliance tasks. It is recommended that you invest in an automated solution that offers a single interface to manage all the devices in your multivendor environment. A **recently-conducted study** by Market Connections and SolarWinds indicates that IT pros are using continuous monitoring tools to detect network issues and vulnerabilities within minutes.

Time to Detect and Analyze Compliance

	Time Taken	Total Respondents	Continuous monitoring user	Continuous monitoring non user
How long does it typically take your organization to detect and/or analyze network device configurations out of compliance?	Within minutes	20.0%	24.0%	13.3%
	Within hours	28.0%	27.2%	29.3%
	Within one day	21.0%	23.2%	17.3%
	More than one day	17.0%	14.4%	21.3%
	No ability to detect	1.5%	0%	4.0%
	Don't know/unsure	12.5%	11.2%	14.7%

Twenty percent of federal IT pros are now able to detect noncompliant configurations within minutes. Source: Market Connections and SolarWinds

Continuous monitoring users point out that most practices and technologies are of essential and priority investments significantly more than non-users of automation tools.

Importance of Security to Continuous Monitoring Users

	Continuous Monitoring User	Non-User
Firewall configuration and security continuous monitoring	53%	33%
Intrusion detection and prevention	52%	31%
Improving system defenses e.g. anti-virus, HIPS	46%	32%
Network configuration security compliance continuous monitoring	46%	31%
Database security	44%	17%
Vulnerability management	41%	25%
Technologies and processes to monitor and block use of removable media (USB, etc.)	37%	23%
Secure remote system administration	36%	20%
Security information and event management	34%	20%
Patch management	33%	19%

= statistically significiant difference

Users of continuous monitoring consider compliance and vulnerability management more essential than do non-users. Source: Market Connections and SolarWinds

Compliance policies and controls can be implemented at any time. However, to enforce them, you need specialized tools to help manage device configurations according to FISMA and STIG guidelines.

The survey results above illustrate the importance of using automation for continuous monitoring. Consider consolidating the management of tasks with configuration backup, configuration change, device inventory, and compliance checks through a single automated solution.

SolarWinds Network Configuration Manager (NCM) saves time and gives you visibility into compliance management and adherence across the entire network. Use of tools such as NCM for continuous monitoring gives agencies faster detection times over non-users.

With NCM you can:

- Easily download all device configurations
- Create baselines and automatically compare configurations
- Run compliance policy checks and obtain reports on violations
- View graphs on compliance details for each device
- Leverage user-tested STIG and FISMA policy templates
- Take advantage of options for immediate compliance remediation

The cost of noncompliance is high. If vulnerabilities are present, unwarranted entities can penetrate and gain access to confidential data, putting essential agency missions and lives in danger. Don't let a security threat or breach put you or your agency in jeopardy.

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide, from Fortune 500 enterprises to nearly every civilian agency, DoD branch, and intelligence agency. In all market areas, the SolarWinds approach is consistent—focusing exclusively on IT pros and striving to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors.

SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale.

Each solution is rooted in the company's deep connection to its user base, which interacts in an online community, thwack®, to solve problems, share technology and best practices, and directly participate in the product development process.

SolarWinds provides IT management and monitoring solutions to numerous common public-sector IT challenges, including continuous monitoring, cybersecurity, network operations, compliance, data center consolidation, cloud computing, mobile workforce and devices, and scaling to the enterprise.

SolarWinds software is available on the U.S. General Services Administration (GSA) Schedule, Department of Defense ESI, and numerous other contract vehicles. For more information and fully-functional free trials, visit http://www.solarwinds.com/federal.