TITANIA

titania.com

Establishing a Defendable Network and Automating RMF Compliance

Combining continuous misconfiguration detection and auto-mitigation with risk-focused compliance analysis

Abstract

Critical network devices (firewalls, routers and switches) are pivotal to the security of all networks. Each device is managed through a complex configuration. Errors arising in the configuration can result in critical security risks to the network, its data, applications and the mission.

It's why DISA ACAS augments its scanning capabilities by incorporating vulnerability and configuration assessment modules in its solution as well as traffic monitoring and reporting modules. The vulnerability scanning module provides information on vulnerabilities associated with the software/ firmware version whilst the configuration module looks at the device configuration.

However, the ACAS configuration module is designed to look at each device setting individually, not in conjunction with other settings, leading to well-known accuracy issues and reports of significant time being wasted investigating false-positives findings. As a result, since 2013, elite cyber teams across Department of Defense and Fourth Estate have complemented their network vulnerability analysis with Titania's highly accurate configuration auditing software, Nipper InfraSight – resulting in time savings of up to 80% for a base configuration assessment compared to using ACAS.

This whitepaper summarizes how Nipper InfraSight is able to achieve unrivalled accuracy in configuration assessment by virtually modelling the entire configuration as a single entity to consider interdependencies and suppress irrelevant findings. It will also demonstrate how this approach to detecting misconfigurations is enabling cyber teams to prioritize remediation workflows for firewalls, routers and switches, based on network risk criticality – viewed through either Nipper InfraSight's security and/or compliance lenses, such as NIST 800-53 or CMMC.

Moreover, as configurations change daily and these advanced cyber teams have a need for continuous assessment as a foundational component of establishing a defendable network and meeting the DoD's zero trust architecture objectives – this whitepaper focuses on how Titania will provide them with continuous detection and remediation capabilities with Nipper OmniSight.

Comparison: Network Security Assessment Methodologies

Before looking at the challenges in assuring network security it is useful to swiftly consider and compare the assessment methodologies which are currently used by cyber protection teams.

Penetration Testing

Penetration testing is the expert process of using a variety of tools to probe and examine, in detail, how the network has been configured. In the case of firewalls, routers, switches and other infrastructure devices, this involves reviewing the configuration file, line-by-line, and comparing it to a secure configuration. Pentesters typically provide independent audits of systems. These systems are installed and maintained by experienced teams who apply their own methods and technologies for protecting their networks.

Vulnerability Scanning

Vulnerability scanning includes the assessment of a device by probing its external interface (scanning it). This process only provides a subset of the security checking required. The scans retrieve the version number of the firmware and look it up in publicly available tables from NIST or the manufacturer to list known Common Vulnerabilities and Exposures (CVE) against the firmware version. Neither of these techniques reveal risks in the device configuration, which can result in undetected misconfigurations in the network that pose critical risks.

Configuration Assessment

Configuration assessment is sometimes referred to as a ‘build review’ by penetration testers. It involves a line-by-line granular assessment of the internal system instructions (configuration or O/S) of a physical or virtual device. As these instruction sets determine a system’s actual security response, it is regarded as the least intrusive, most accurate and detailed way of determining the system’s security and compliance status. There are two types of configuration assessment technologies:

- **‘Find and match’ text string analysis (grep) tools (e.g. Tenable Nessus)**
- **Solutions with built-in virtual modelling of device configurations and interactions (e.g. Nipper InfraSight)**

Requirement Description	Nipper InfraSight	Scanners
Authentication & Authorization Configuration	✓	-
Account & Logging Configuration	✓	-
IDS & IPS Configuration	✓	-
Password Strength & Encryption Analysis	✓	-
Timeout Configuration	✓	-
Physical Port Audit	✓	-
Routing Configuration	✓	-
VLAN Configuration	✓	-
Network Address Translation	✓	-
Network Protocols	✓	-
Device Specific Options	✓	-
Time Synchronization	✓	-
Network Filtering (ACL) Audit	✓	-
Wireless Networking	✓	-
Warning Messages (Banners)	✓	-
Network Administration Services	✓	-
Network Service Analysis	✓	-
Software Vulnerability Analysis	✓	-
VPN Configuration	✓	-
Network Discovery and Topology	✓	-
Availability Monitoring	✓	-

Grep configuration auditing is prone to false positives and false negatives, whereas virtual modelling provides the high levels of granular auditing accuracy needed for SIEM solutions and Security Orchestration Automation and Response (SOAR) enabled playbook controlled risk prioritization and auto-mitigation.

The challenge: accurately auditing and assuring every device, every day

Modern military and federal networks can contain hundreds or thousands of firewalls, routers and switches. This represents an enormous attack surface to defend as all the devices must maintain a secure configuration that matches both network policy and functional intent. Over time, these configurations can change, with a range of people altering them for differing purposes, leading to configuration drift.

Configuration drift is where the device configuration drifts out of compliance with policy, resulting in unintended security risks. Most of this activity is not malicious in intent but results in potentially critical security and operational problems nevertheless, largely through the unwitting interaction of configurable items – for example, routing changes or firewall rules.

> **"Human error creates the biggest threat. Technicians can inadvertently misconfigure devices, opening up holes. We need to go back and validate configs."**
>
> **Source:** DISA Emerging Technologies Directorate, Steve Wallace

Traditional approaches to assessing the security status of a network involves personnel penetration testing the devices. This is a skilled and time-consuming job. The combination of network scale and the number of trained penetration testers available – even when using best of breed, on demand, configuration assessment software to automate the process – means that only a sample of devices can be tested and/or the cadence of testing reduces to testing the devices once per year. This can result in any security risks, including critical risks, persisting in the network and exposing the mission.

Indeed, military and federal security risk management programs now reflect that sampling is insufficient to protect networks.

Moreover, RMF for DoD and DHS CDM (both based on NIST 800-53) stipulate that the agenicies must implement continuous assessment. To protect critical vendors in agency supply chains, CMMC and NIST 800-171 also recommend continuous monitoring for security risks.

If regulatory and mandated compliance was not enough of a driver already, recent events have emphasized how easily network security can be breached, and the far reaching consequences of those breaches. It has long been recognised that a determined attacker will gain access to a network eventually using one of a variety of techniques. Once in the network, it is important that their progress to their goal is made as difficult as possible, inhibiting lateral movement. This means that security within the network perimeter is as important as the security on devices forming the perimeter.

It's why network architects are increasingly adopting a zero trust approach to securing networks. Particularly since DISA released its Zero Trust Reference Architecture, emphasizing its importance, and the Presidential Executive Order from May 2021 specifically called out the adoption of zero trust paradigms to mitigate risks.

There are many aspects to zero trust, but at its heart lies the principle that no entity should be implicitly trusted due to the application, device or location that they appear to be using. The second principle is to understand your estate and ensure every node in the network is configured correctly and has no security holes. As networks mature towards higher levels of zero trust implementation, it becomes necessary to perform continuous assessments to assure the network remains secure and that any inadvertent or deliberate acts are discovered quickly and the risk remediated.

This is why network and security teams need a solution with the capability to accurately assess the security configuration and compliance status of every device in a network, preferably on a continuous basis, ensuring that any misconfigurations are identified quickly and remediated as soon as practicable.

Network security challenges

- **Large complex networks**
- **Insufficient resource**
- **Ad hoc audits and sampling**
- **Unmonitored configuration drift**
- **Exposure due to critical risks**
- **Incomplete compliance reports**
- **Remediation not prioritized by risk**
- **Excessive mean time to remediate**
- **Low confidence in network security**

Network security challenges

Used across the US Department of Defense since 2013, Nipper InfraSight offers unrivalled accuracy in detecting security and compliance issues in firewalls, routers and switches, and is used for configuration analysis over and above ACAS. In this environment, Nipper InfraSight has been proven to deliver higher accuracy and to reduce false-positive findings significantly, providing a superior, network-centric risk score, and offering detailed remediation instructions. It is reported that using Nipper InfraSight instead of ACAS to assess the network reduced base audits from 10 working days to 2, through not wasting time investigating false-positive findings generated by ACAS.

Nipper InfraSight achieves this superior accuracy through its virtual modelling of the entire configuration as a single entity.

By adopting this approach, the analysis can consider the interdependencies of the configuration settings and supress findings that are irrelevant, for example, because they are not enabled elsewhere in the configuration. The same is true for complex configurations within firewall devices, where overlapping rules can cause security issues, but all of the rules must be ingested and analysed simultaneously to discover them.

Not only does Nipper InfraSight provide accuracy, it also provides a network risk context for any issues it finds. Competitor products use
CVSS severity rather than risk scoring, but Nipper InfraSight also takes into account other factors representing risk to the network, not just to
the device.

Nipper solutions take in factors representing risk to the network, not just to the device. This includes:

- **The impact of an exploitation of the misconfiguration**
- **How easy it is to exploit it, i.e. to assess risk likelihood**
- **How easy it is to remediate**

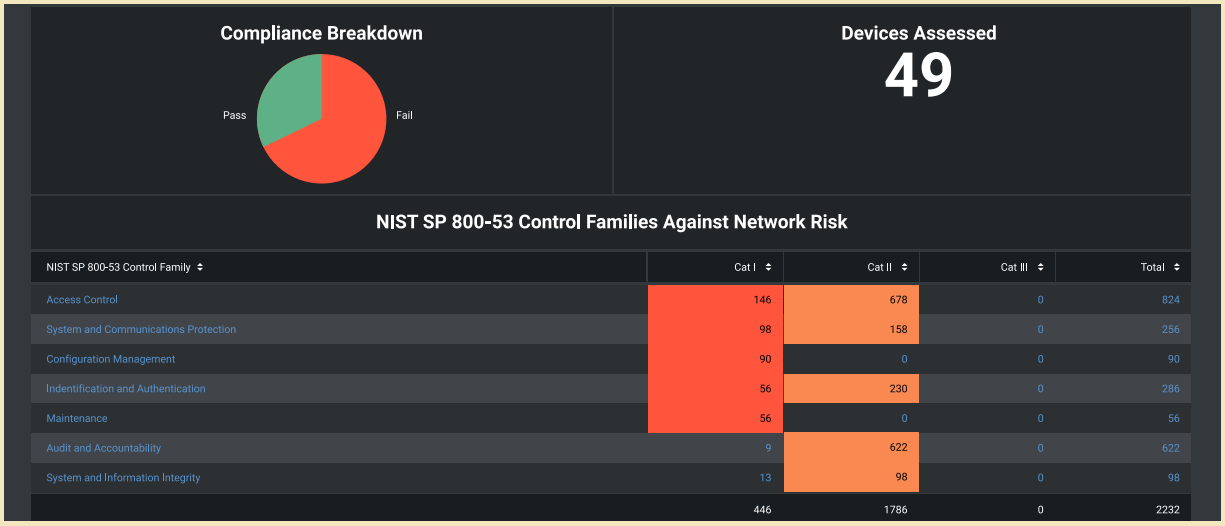
The Nipper InfraSight findings report then automatically prioritizes the risks identified by criticality to the network. Alternatively, the risk can be viewed through a compliance lens. For example, by assessing the 34 automatable NIST 800-53 controls across 10 control families, Nipper InfraSight categorizes any misconfigurations found, prioritized by risk for remediation against the NIST 800-53 control and control family to accurately prioritize RMF remediation by risk criticality.

In addition to scoring risk by security and/or compliance, Nipper InfraSight also provides detailed remediation advice, with command line syntax instructions, allowing network professionals to remediate issues quickly.

This information is invaluable to the SOC and NOC to inform remediation strategies and workflows. It allows them to reduce the risks in the network, to the greatest extent, as quickly as possible as well as proving RMF assurance.

However, until recently Nipper InfraSight could not provide continuous configuration assessments, as it relied on a human to drive the process.

Titania's Nipper OmniSight product now solves this problem, by automating the whole security and compliance assessment process for the network.



NIST SP 800-53 Control Family	Cat I	Cat II	Cat III	Total
Access Control	146	678	0	824
System and Communications Protection	98	158	0	256
Configuration Management	90	0	0	90
Indentification and Authentication	56	230	0	286
Maintenance	56	0	0	56
Audit and Accountability	9	622	0	622
System and Information Integrity	13	98	0	98
	446	1786	0	2232

RMF/NIST 800-53 compliance assessment prioritized by network risk

The shift from ad hoc to continuous assessment with Nipper OmniSight

Nipper OmniSight is a web application using a set of containerized Nipper InfraSight instances that scale up and automate the assessment of the configuration of every network device, every day. This brings the power and accuracy of Nipper InfraSight to the whole network and enables the continuous audit and compliance assessment against mandated risk frameworks, such as RMF and CMMC, that advanced cyber teams need.

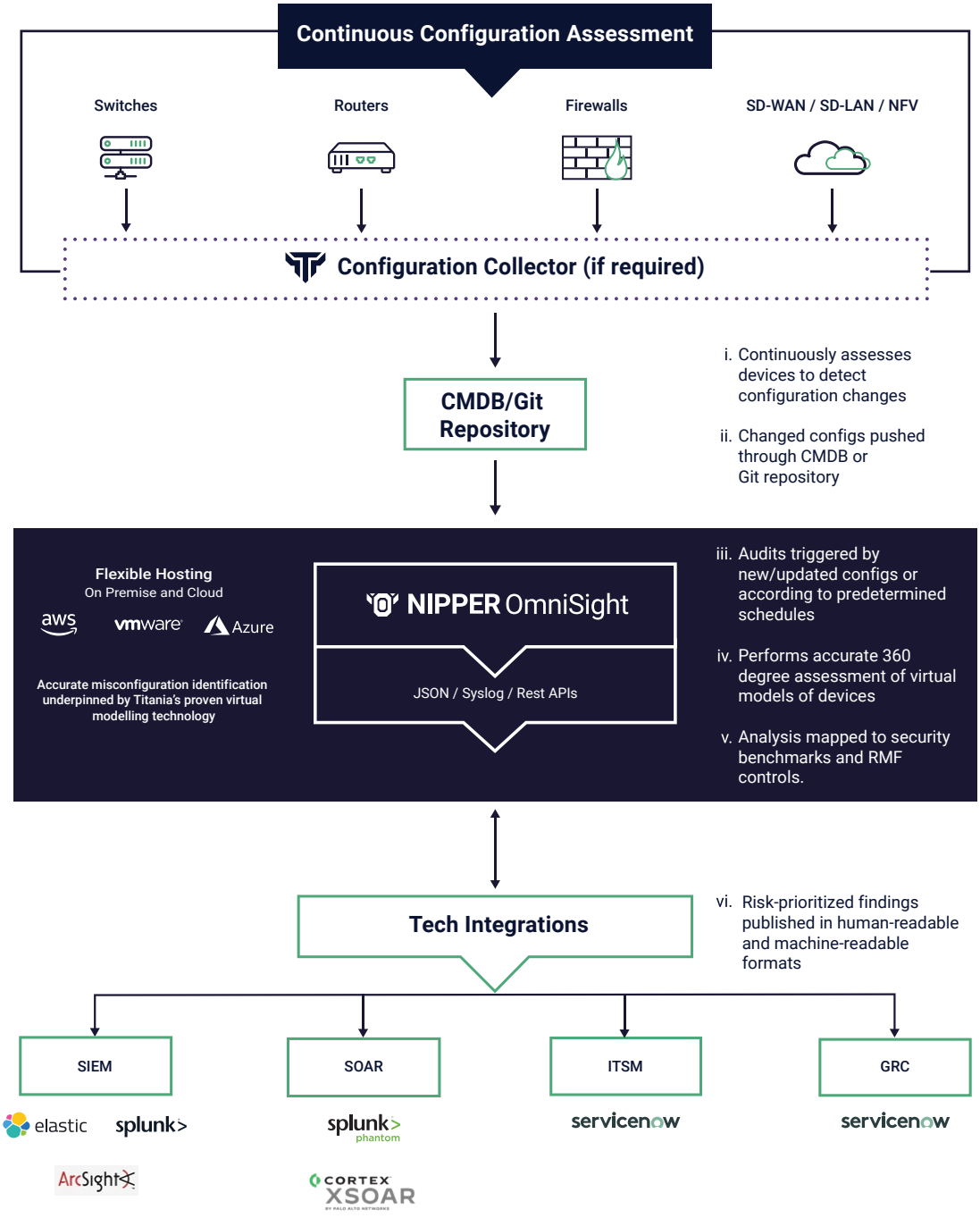
By ingesting configuration files, Nipper OmniSight can be used in situations where security professionals or auditors do not have direct access to the devices but are provided with the configurations or they are available from a CMDB. The file-based Nipper OmniSight mode facilitates auditing every device in the network at a single point in time, so as to produce and compare RMF posture assessments for the network.

Alternatively, the configuration collection layer with Nipper OmniSight can be enacted to auto-populate and maintain the organisation's configuration repository. This allows configuration changes to be detected, validated and impact assessed in near-real time.

Enacting the configuration layer also provides the additional benefit of allowing users to manage configuration as code, using a digital twin of the repository to test pre-production configuration changes, ahead of deploying them to live environments..

In either deployment, Nipper OmniSight is not tethered to external cloud systems in any of its modes, so no security or compliance data leaves the product, except through explicit secure integrations to trusted existing systems, for example to SIEM, SOAR, GRC systems. In the case of integrations with SIEM systems, such as Splunk and Elastic, the findings are shipped to these products as JSON records, either directly or via data lakes using SYSLOG as a transport.

Titania has built dashboards in these products, using the powerful analysis and visualization capabilities of the systems to provide on-demand and continuous network compliance and risk views for the NOC and SOC professional respectively.



Technical Specifications

Titania Nipper OmniSight is a horizontally scalable application and can be applied to the largest networks, operating at an hourly audit cadence if required.

The application can be hosted in a VMWare environment as a virtual appliance, or within an AWS VPC. The application does not ship data to any cloud services, and can be deployed in air-gapped environments.

Nipper OmniSight accesses device configurations flexibly, to allow for a range of deployments. Firstly, device details can be provisioned into the application, and then Nipper OmniSight will reach out securely to the device over the client network to retrieve the configuration for analysis. The configuration is retrieved either as a single action, or on a regular scheduled cadence from every hour, to quarterly.

Nipper OmniSight has successfully assessed and reported on over 300,000 device configurations daily, and, due to its horizontally scalable nature, this can be increased further as required.

Key to minimizing the attack surface and developing operational resilience, deploying Nipper OmniSight so that it then proactively monitors configuration changes between assessments, provides a practical way to manage network risks in near-real time.

All Nipper reports produce tagged security findings that Titania has mapped to Risk Management Frameworks; for example, NIST 800-53 dashboards have been developed in Splunk to visualize the RMF compliance across the network, applying a risk lens through which to prioritize actions.

Nipper OmniSight is also future proof, supporting a wide range of enterprise integrations, including SIEM and SOAR systems, to facilitate automatic remediation where this is appropriate.

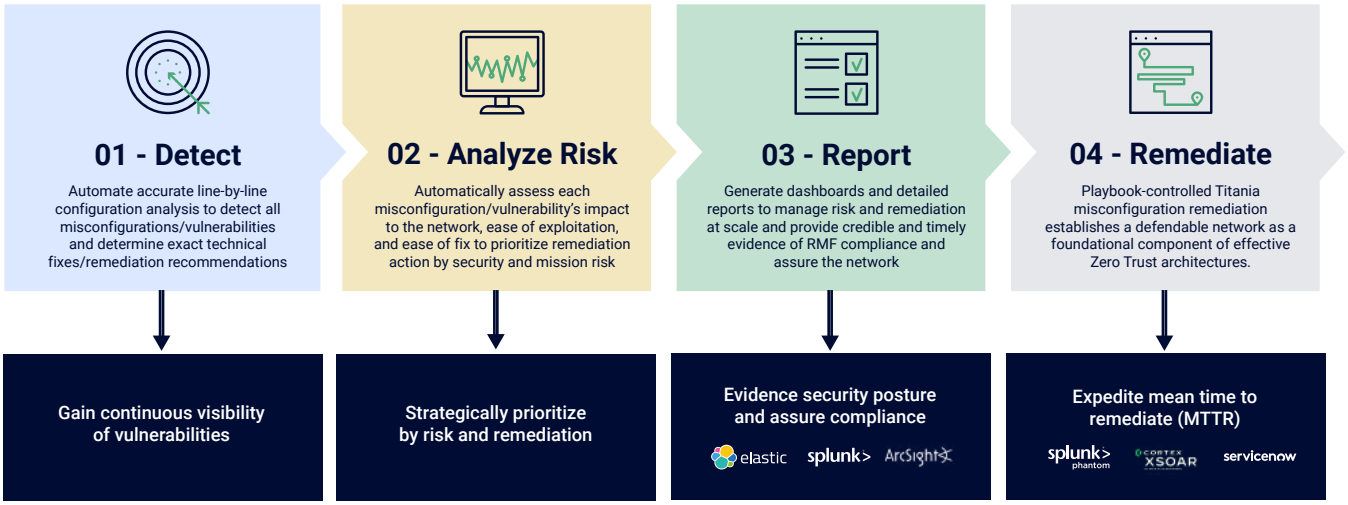
Significantly reducing MTTR and playbook controlled auto-mitigation

Virtually modelling and analysing the entire configuration as a single entity, in the way that Nipper InfraSight and Nipper OmniSight do, provides accuracy and granular detail about where the actual configuration differs from the desired secure configuration. This means that the findings can be reported with remediation recommendations and where possible complete with command line syntax instructions to remediate any misconfiguration risks found.

This means that Nipper OmniSight can produce reports suitable for ingest by workflow tools, such as ServiceNow, or automatic playbook controlled remediation tools, such as SOAR, incluing Splunk Phantom and Cortex XSOAR.

Integrating Nipper OmniSight's detailed findings with SOAR systems not only allows configuration security and compliance data to be visualized and prioritized in those products, it can also be used in playbooks that step through the remediation processes, enabling playbook controlled automatic remediation capability for a variety of risk classes.

So Titania's software is not only proven to reduce the mean time to detect (MTTD) network misconfigurations, it also addresses the mean time to repair (MTTR) and remediate risks, supporting users in their missions to establish a defendable network.



Conclusion

Increasingly sophisticated methods of attack, the sheer size of networks, and the volume of interdependent configurations that need to be checked daily, means network security is no longer considered a case of 'finding and fixing' every vulnerability. Rather, best practice is to find and fix the misconfigurations that pose any critical risk first and to inform remediation workflows, ensuring the prioritization of the work that is required to most significantly improve the security and compliance posture of the network.

Reducing the mean time to remediate a vulnerability that has low impact on the network if exploited cannot be considered an effective benchmark of security. In order to prioritize remediation effectively, network owners need to be able to:

- **Accurately identify misconfigurations and interdependencies between network settings**
- **Analyze the impact if it is exploited**
- **Understand how easy it is to exploit the misconfiguration**
- **Assess the risk in terms of both security and compliance**
- **Calculate how easy it is to remediate (with a time to fix)**
- **Determine and advise the remediation recommendation**

Only then, equipped with the accurate data they need, can network teams implement considered remediation workflows that provide a roadmap to security compliance and configuration confidence.

So whilst on the surface, vulnerability detection software for the network might appear equal – in reality, the way in which the software detects vulnerabilities has a significant impact on the efficacy of the findings and on a network team's ability to remediate critical misconfigurations and reduce risk.

Vulnerability scanners with configuration management modules that use GREP analysis can find firmware and software quality issues, but cannot accurately identify and prioritize network misconfigurations based on risk

Complementary to their analysis, Titania's Nipper solutions provide:

- **Audit accuracy – saving significant time not investigating false positives and identifying misconfigurations others don't to improve MTTD**
- **Risk scoring and prioritization – with a security and/or compliance lens**
- **Remediation advice – with exact technical fixes that can be used in playbook-controlled auto-mitigation, reducing MTTR**

Furthermore, Titania has augmented Nipper software and associated visualizations to specifically address the DoD network and report against the RMF compliance framework. By generating a unique network risk assessment, Nipper InfraSight's NIST 800-53 compliance report is prioritized to help network owners decide what actions to take first to reduce RMF risk as soon as possible.

These are the primary reasons that the DoD and approximately 30 other federal agencies complement their DISA ACAS (Tenable Nessus) analysis with Nipper InfraSight configuration analysis for firewalls, routers and switch devices. It's also the reason that Titania has developed Nipper OmniSight, to deliver the market-leading configuration assessment accuracy that the DoD depends on, at scale, every day.

TITANIA

At the forefront of proactive network security, Titania's multi-award-winning vulnerability and exposure management solutions are trusted by NOC, SOC, Incident Response and Cyber Protection teams to safeguard critical infrastructure and commercial entities, globally. Whether organizations need real-time visibility and analysis of every network change to get ahead of threats, segmentation violations, and potential network disruptions. Or scheduled network posture and device vulnerability assessments to enhance attack surface security and demonstrate compliance. We have a solution for every stage of the journey to network readiness and resilience.

USA
Suite 600,
2451 Crystal Dr, 6th Floor,
Arlington, VA 22202

UK
167-169 Great Portland Street,
London, England,
W1W 5PF