TITANIA
Assured Accuracy

Product Overview

Nipper Enterprise

Accurate configuration security and RMF compliance at scale

Configuration assessment accuracy is critical

Core network devices (firewall, routers and switches) are pivotal to the security of all networks. Each device is managed through a complex configuration, and misconfigurations (either accidental or deliberate) can result in critical security risks to the network, its data, applications and ultimately the agency's mission.

The only way to accurately detect these misconfigurations is to virtually model the configuration as a single entity to consider interdependencies across the core network.

As core networks can change on a daily basis, trusted USG security programs and risk management frameworks increasingly mandate continuous monitoring and assessment as foundational components of establishing a defendable core network and meeting DoD's zero trust architecture objectives.

This requires a risk-focused approach to misconfiguration detection and remediation that is accurate, timely, and scalable.

By virtually modelling configurations, Nipper Enterprise accurately assesses the security risk posture of up to 300,000 firewalls, routers and switches daily from trusted manufacturers like Cisco, Fortinet, Juniper and Palo Alto amongst others. The solution significantly reduces the mean time to detect vulnerabilities and misconfigurations, delivering deterministic results on an up-to-hourly basis.

Nipper Enterprise not only prioritizes security risks according to expert pentest criticality ratings – based on ease of exploitation and network impact, but also provides remediation recommendations and command line fixes where possible.

Securing your core network through RMF assurance

To help deliver security from compliance with trusted risk and control frameworks, Nipper Enterprise's security risk assessment can be automatically overlaid onto NIST 800-53 and DISA STIG assessments, and therefore, onto RMF for DoD agencies and CDM for civilian agencies, or onto CMMC and/or NIST 800-171 for supply chains.

Integrations with trusted SIEM, ITSM and SOAR tools enable both snapshot RMF posture assurance and/or continuous RMF monitoring of the actual state of core network configuration - prioritized by network security risk criticality.

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

SOC and NOC Benefits

Deliver network security and RMF assurance
By providing an accurate RMF snapshot of the entire core network, Nipper Enterprise empowers compliance and security teams to agree and monitor a Plan of Action and Milestones (POA&M), prioritized by network risk, to deliver and maintain network security and RMF assurance.

Continuous configuration drift monitoring and management
By assessing every device daily, Nipper Enterprise quickly identifies configuration drift as it arises, allowing SOC/NOC teams to prioritize risk remediation of any critical risks detected within existing POA&Ms.

Zero Trust Architecture Baselining
Providing both snapshot RMF assurance and continuous monitoring, the solution enables an agency to evidence their adherence to baseline zero trust capabilities for the core network of (i) being segmented with deny all/permit by exception and (ii) devices being managed and compliant to IT security policies as identified in the DoD's 2021 ZTA reference architecture.

Significantly improved security and financial ROIs
Nipper Enterprise's accuracy and risk and remediation focus significantly improves the security return from existing SOC/NOC investments in terms of MTTD and MTTR, as well as financial terms by saving thousands of labor years per annum not investigating false positives and ensuring cyber teams prioritize remediation by network risk criticality.

Architected for the Enterprise

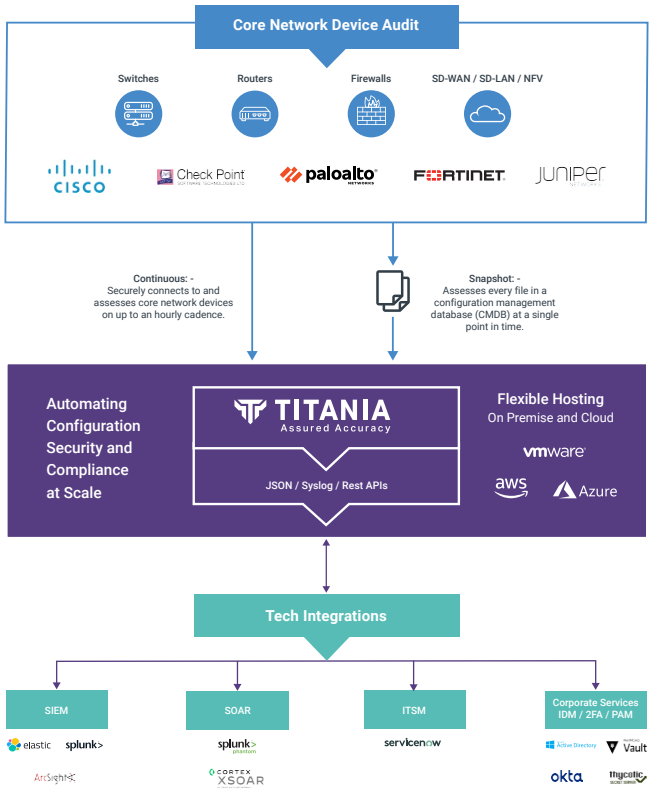
Nipper Enterprise is a horizontally scalable, agentless web-based application, hosted on a VSphere platform or AWS VPC.

Fitting easily into any corporate network infrastructure, whether on-premises or cloud-based environment, by scaling the unrivalled accuracy of Titania Nipper's proven configuration assessment virtual modelling, the solution accurately assesses a wide range of core network devices against trusted risk management and control frameworks.

Nipper Enterprise is capable of directly connecting to network devices to access the configuration file or ingesting previously extracted configurations. The analysis performed is identical regardless of the configuration source. Risk findings are produced in a variety of formats, including JSON and syslog, enabling integration with existing SIEM, SOAR and ITSM SOC and NOC solutions.

Integrations with trusted Active Directory, 2FA, PAM and IDAM providers ensure Nipper Enterprise meets operational security requirements.

NIPPER ENTERPRISE: TECHNOLOGY & DEVICE INTEGRATIONS



"Automatically prioritize RMF remediation by security and mission risk, and reduce mean time to repair with device specific remediation advice."

Snapshot mode: Nipper Enterprise assesses every file in a configuration management database (CMDB) at a single point in time, accurately reporting actual RMF posture prioritized by network risk criticality to meet compliance assurance requirements and ensure POA&Ms deliver security from RMF compliance.

Continuous mode: By allowing Nipper Enterprise to securely connect to and assess core network devices on up to an hourly cadence, critical RMF misconfigurations in particular can be identified and remediated on a daily basis in support of agreed POA&Ms.

Key Features

Secure deployment
Integrations with trusted 2FA, Active Directory, PAM and IDAM providers ensure Nipper Enterprise can meet stringent operational security requirements.

Air-gapped Auditing
Nipper Enterprise can ingest device configurations from pre-extracted configuration files within repositories to assess the security and RMF compliance of the most secure networks in the world.

Risk Visualization, Prioritization & Exploration
Machine-readable JSON and syslog outputs enable integration with dynamic visualization, prioritization, enrichment and exploration SIEM and GRC tools.

Remediation Workflow Enhancement
Integrations with SOAR and ITSM platforms enable risk prioritized playbook-controlled remediation automation workflows to improve MTTR.

Flexible Device Labelling and Audit Scheduling
Devices can be labelled as required by, for example, network criticality, geographic location, manufacturer, device type, etc. Using labels then enables audit cadence scheduling flexibility based on network or device risk profiles.

About Titania
Since 2013, Titania Nipper's accurate configuration assessment has been trusted by elite DoD vulnerability assessment teams to complement DISA ACAS analyses. Nipper's unrivalled accuracy allows audits to be reduced by up to 80% as a result of not wasting time investigating ACAS false positives.

Utilizing the trusted Nipper sensor that delivers this industry-leading accuracy in configuration security and compliance assurance, Nipper Enterprise now delivers accurate security assessment and RMF monitoring and assurance at scale to support USG cyber teams in their efforts to establish a defendable core network.

For more information on any of our products or services, visit us on the web at: www.titania.com