

Product Overview

Foundational network configuration security for Zero Trust and PCI DSS 4.0 assurance at scale

Configuration assessment accuracy is critical

Devices, such as firewalls, 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 organization'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 network.

As networks can change on a daily basis, trusted compliance standards and risk management (RMF) frameworks such as PCI DSS 4.0 increasingly mandate continuous monitoring and assessment of all network devices as foundational components of delivering security from compliance. This is in line with the Zero Trust security best practice identified by NSA and DISA in the DoD's Zero Trust reference architecture.

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 manufacturers including Cisco, Fortinet, Juniper, Check Point and Palo Alto amongst others. The solution significantly reduces the mean time to detect and remediate 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 CDE and wider network by adopting PCI DSS 4.0 best practice

To help deliver security from compliance with trusted risk and control frameworks, Nipper Enterprise's security risk assessment can be automatically overlaid onto PCI DSS 4.0 requirements, as well as NIST 800-53, NIST 800-171 and CMMC 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 network configuration - with results prioritized by network security risk criticality.



PCI DSS 4.0 compliance assessment prioritized by network risk

SOC and NOC Benefits

Deliver network security and PCI 4.0 assurance

By providing an accurate RMF snapshot of the network, as well as CDE, Nipper Enterprise empowers compliance and security teams to agree action and monitor the effectiveness of remediation plans prioritized by network risk, to deliver and maintain network security and PCI DSS 4.0 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.

Zero Trust architecture baselining

Providing both snapshot RMF assurance and continuous monitoring, Nipper Enterprise enables an organization to evidence their adherence to baseline zero trust capabilities for the network (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 zero trust reference architecture.

Significantly improved security and financial ROIs

Nipper Enterprises accuracy and risk and remediation focus significantly improves the security return from existing SOC/NOC investments. In terms of both MTTD and MTTR, as well as in financial terms, the solution saves thousands of labor years per annum through not investigating false positives and ensuring cyber teams prioritize remediation by network risk criticality.

Architected for the Enterprise

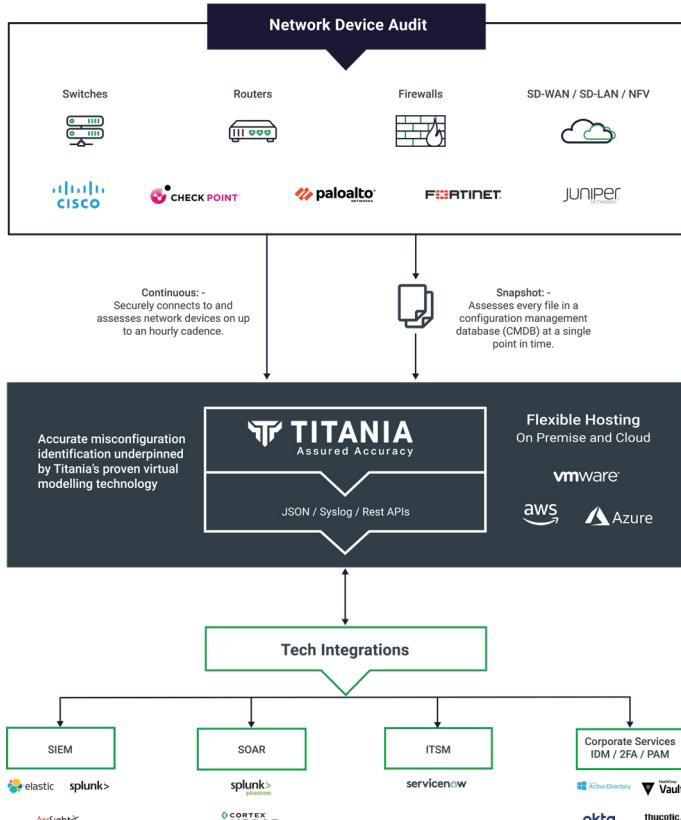
Nipper Enterprise is a horizontally scalable, agentless web-based application, hosted on a VSphere platform or AWS VPC.

The application fits 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 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 PCI DSS 4.0 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 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 2012, Titania Nipper's accurate configuration assessment has been trusted by expert vulnerability assessment, PCI QSA and ISA teams to automate security and PCI assurance. Nipper's unrivalled accuracy allows audits to be reduced by up to 3 hours per audit by not wasting time investigating 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 PCI DSS 4.0 monitoring and assurance at scale whilst simultaneously delivering effective foundational zero trust capabilities.

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