TITANIA NIPPER

PRODUCT OVERVIEW

On-demand router, switch and firewall configuration assessments with automated pass/fail evidence of compliance

Delivering security from compliance

Organizations increasingly rely on compliance standards to strengthen their security posture and to protect their networks, customers and supply chains. Failure to assess network infrastructure configurations against trusted risk management frameworks and hardening guides makes networks more vulnerable to breaches - as misconfigurations provide threat actors with known pathways to alter configs and scale attacks.

Non-compliance with mandated controls can also lead to contract losses, reputational damage and even lawsuits. So, it is imperative that assessors have the capability to accurately assess and effectively evidence network security and compliance across routers, switches and firewalls, with:

» Automated security checks mapped to control standards & RMFs,
» Pass/fail evidence for each network check, and
» Prioritized remediation for the most critical non-compliances.

The power of Nipper

Providing complementary analysis to server-centric vulnerability management solutions, auditors and assessors choose Nipper to deliver the level of proactive network risk assessments required to assess:

» **Zero Trust readiness using existing hardening standards**
» **Network segmentation rules and settings**
» **Compliance with control standards and RMFs**

Nipper analyses configurations with the precision of a pentester, providing advanced network contextualization that suppresses irrelevant findings to reduce security audit and compliance assessment times by up to 80% when compared to other automated approaches.

Automating security checks to assess whether configurations adhere to vendor hardening and network infrastructure hardening best practices, Nipper also applies a compliance lens to its findings.

Compliance findings are provided with evidence of ‘passes’ and ‘fails’*, and configuration changes between audits can be tracked with ease to aid further investigation into whether the drift was accidental or deliberate.

**Requires version 3.0 (or later) to generate evidence-based compliance reports.*

Reports provide insight into:

» Specific tests run on the configuration,
» Deviation from the security and/or compliance standard, and
» Remediation required to mitigate the risk.

Nipper simultaneously analyses the misconfiguration for the:

» Impact to the network if exploited,
» Ease of exploitation, and
» Ease of fix.

In-depth findings are then automatically prioritized by risk criticality or ease of remediation, with a summary of non-compliance findings displayed at the top of easy-to-navigate reports.

Demonstrating compliance by automating:

Exception-based security reporting
Nipper’s renowned Security Audit automates configuration checks to report exceptions that fail to adhere to vendor hardening guides and network infrastructure hardening best practices. Separate exception-based reports also check for vulnerabilties against:

» CIS Benchmarks,
» Cisco PSIRT Vulnerability Database, and
» NIST National Vulnerability Database.

Evidence-based compliance reporting
Nipper accurately checks whether a configuration passes or fails to comply with an RMF control or security standard, providing specific information on the test(s) performed to reach this conclusion for:

» Up to 41 (96%) of Cisco NDM STIG checks,
» Up to 55 (60%) of Cisco RTR STIG checks,
» Up to 52 NIST 800-53 controls, across 12 control families, and
» Up to 94% of PCI DSS 4.0 network device procedures.

Risk-prioritized view of configuration vulnerabilities
Prioritizing findings by compliance risk, Nipper visualizes the significance of its findings according to CVSS, STIG, Cisco SIR, and its own trusted risk criticality rating systems.

Remediation analysis to improve security posture
Device-specific guidance on how to fix misconfigurations – including command line scripts in some cases – is provided to decrease the mean time to remediate security and compliance risks and inform POAMs.

Online and air-gapped auditing

Nipper is a downloadable application which is installed on a local machine, enabling deployment in air-gapped environments and offline networks. The configuration assessment methodology does not require direct access to devices.

Installing and activating Nipper on multiple workstations allows users to access the license to audit devices across different teams, departments, or locations as required.

Running the latest available version of Nipper ensures access to the most up to date security policy checks, compliance framework mapping and product enhancements.

Supported devices

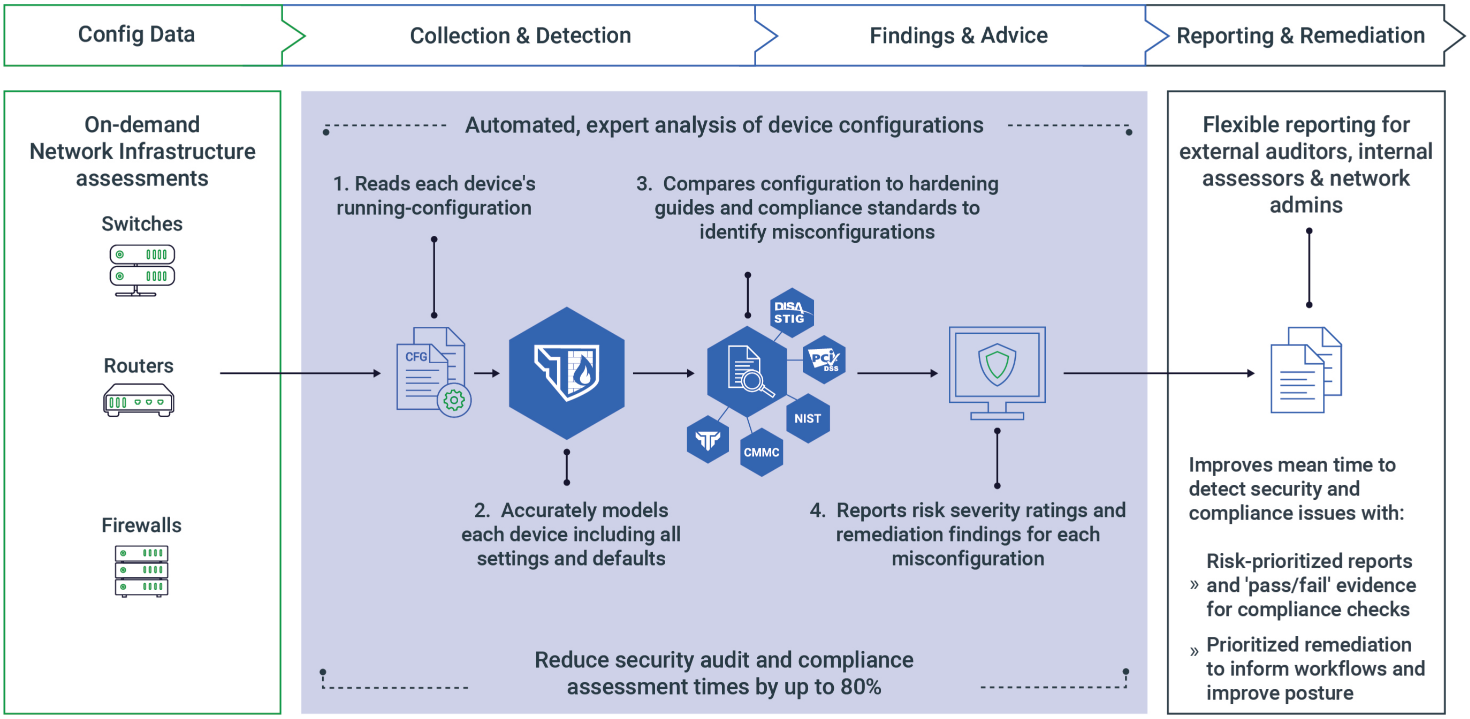
All major device vendors are supported, including:

cisco paloalto NETWORKS JUNIPER NETWORKS
FORTINET CHECK POINT f5

Key Features:

- **Audit scoping**
  Define the scope of the audit by specifying which IP addresses to include/exclude, which audit reports should be scoped, and whether to include/exclude report sections.
- **Configurable check parameters**
  Detailed check descriptions and configurable parameters help ensure network checks reflect organizational policies and risk profile.
- **Reports browser**
  Navigate audit reports with ease, add notes or exclude findings altogether as required. Modified results can be, optionally, remembered and applied each time the same device is audited, or the type of device is audited, or all devices - as required.
- **'Save' formatting**
  Easily read, filter, manage and export findings to a variety of platforms including STIG Viewer (Checklist, CMRS, XCCDF, and CSV), Excel, HTML, SQL, CSV, LaTex, ASCII, and XML.

How Nipper assesses configurations



Config Data → Collection & Detection → Findings & Advice → Reporting & Remediation

On-demand Network Infrastructure assessments

Switches

Routers

Firewalls

Automated, expert analysis of device configurations

1. Reads each device's running-configuration

2. Accurately models each device including all settings and defaults

3. Compares configuration to hardening guides and compliance standards to identify misconfigurations

4. Reports risk severity ratings and remediation findings for each misconfiguration

Reduce security audit and compliance assessment times by up to 80%

Flexible reporting for external auditors, internal assessors & network admins

Improves mean time to detect security and compliance issues with:

- Risk-prioritized reports and 'pass/fail' evidence for compliance checks
- Prioritized remediation to inform workflows and improve posture

Why Titania?

Used by more than 30 federal agencies, US DoD, global telcos, multinational financial institutions, utilities and retail companies for over 10 years, elite cyber teams have complemented their vulnerability analysis with Titania's accurate network configuration assessment software - Nipper.

Accuracy-advantages, a trusted risk criticality rating, and choice of security and compliance lenses make Nipper solutions flexible for both internal and third-party teams, across a range of use cases and industries.