NIPPER InfraSight
BY TITANIA

Nipper InfraSight (Compliance)

Low-impact compliance reporting for faster, more defensible audits

At a glance

Trusted by 100+ elite cybersecurity teams and 1,000+ users worldwide.

Best for
Teams that need faster, more defensible evidence for audits and remediation planning

Assessment mode
Point-in-time compliance assessment

Deployment
Self-installing executable (Windows or Ubuntu)

Inputs
Exported network device configuration files for offline or credentialed assessment workflows

Outputs
Mapped compliance evidence, prioritized findings, and device-specific remediation guidance in human- and machine-readable formats

Audit and compliance teams are under pressure to produce defensible evidence faster while minimizing disruption to production environments. For many organizations, network device assessments remain slow and inconsistent, increasing audit risk, delaying remediation, and adding avoidable manual effort.

Nipper InfraSight (Compliance) accelerates audit preparation with mapped reporting for CMMC, NIST, PCI DSS, and DISA STIG-aligned assessments. It supports low-impact assessment approaches, including offline and credentialed methods, without agents or active network scans, while strengthening network hardening by exposing configuration vulnerabilities, control gaps, and remediation priorities. It can reduce compliance assessment time by up to 80% compared with manual processes.

Control-mapped compliance reporting
Produce mapped reports for PCI DSS 4.0, NIST SP 800-53, NIST SP 800-171, DISA STIGs, CIS Benchmarks, and CMMC.

Pass/fail control evidence
Generate device-level evidence that supports risk-prioritized remediation and strengthens audit defensibility.

Low-impact assessment options
Support offline and credentialed assessment approaches without agents or active probing of production systems.

Firewall complexity reporting
Surface shadowed rules, redundant objects, and structural complexity that obscure intent, increase change risk, and slow reviews.

Risk-prioritized remediation guidance
Rank findings by impact and exploitability, and provide clear, step-by-step remediation in human- and machine-readable reports.

How it works

1. **Configuration file import**
2. **Low-impact assessment execution**
3. **Audit-ready report export**

Who is it designed for?

Designed for organizations with formal compliance obligations, and for teams hardening routers, switches, firewalls, and wireless access points to reduce misconfiguration-driven exposure.

Common use cases

Preparing for audits and assessments
Generate mapped evidence per device to support internal audit preparation and external assessment.

Prioritizing non-compliant device fixes
Use pass/fail results per control to focus remediation effort on the issues that matter most.

Hardening devices against misconfiguration risk
Reduce exposure by fixing the configuration weaknesses that drive business-critical audit findings and incidents.

What makes Nipper solutions different?

Up to 80% faster assessments
Cut manual assessment effort and accelerate compliance with human-readable and risk-prioritized evidentiary reporting and faster, repeatable analysis.

Low-friction deployment
Deploy as a lightweight Windows or Ubuntu executable without adding infrastructure or changing established workflows.

Broader device and benchmark coverage
Extend assessment coverage across multivendor routers, switches, firewalls, Cisco Meraki, wireless access points, and DISA STIG requirements.

Attacker-style configuration validation
Evaluate device configurations the way an attacker would to uncover gaps many tools never inspect.

Risk-prioritized findings
Rank issues by exploitability, impact, and ease of remediation to focus effort where it matters most.

Control-mapped audit documentation
Produce structured outputs aligned to audit and assurance workflows, reducing manual evidence collation.

Deployment and data handling

Nipper InfraSight (Compliance) runs as a lightweight Windows or Ubuntu executable on a laptop or admin workstation. Teams can complete point-in-time assessments using offline or credentialed methods, without introducing additional infrastructure, agents, or active network scans.

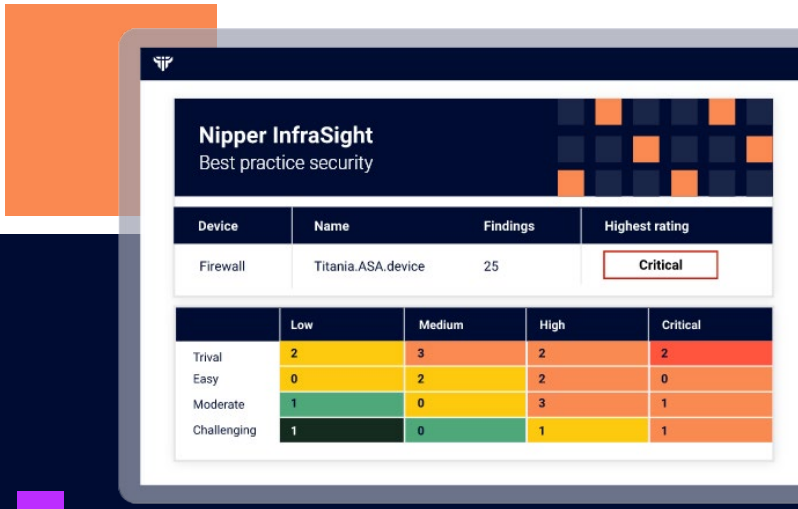
These low-impact assessment workflows fit easily into existing audit, security, and governance processes. Teams can review, hand off, and act on findings without changing established remediation and assurance workflows.

Supported devices

Nipper InfraSight (Compliance) assesses more than 180 network device types using current vendor guidance, including routers, switches, firewalls and wireless access points across multivendor environments and Cisco Meraki.

About Titania

UK-engineered. Trusted globally.
Titania Nipper solutions provide the configuration-validation layer most security architectures are missing, helping security, network, and audit teams reduce misconfiguration-driven exposure, accelerate assurance workflows, and strengthen compliance readiness. Built on virtual device modeling and adversary-style testing, Nipper InfraSight and Nipper OmniSight automate the assessment of device configurations to deliver prioritized findings, device-specific remediation guidance, and defensible reporting for high-assurance environments.



See for yourself

Request a demo to see how Nipper InfraSight (Compliance) speeds compliance reporting and reduces manual evidence collection.

Get in touch