NIPPER InfraSight
BY TITANIA

Nipper InfraSight (Air Gapped)

Offline configuration assurance for isolated environments

At a glance

Trusted by 100+ elite cybersecurity teams and 1,000+ users worldwide for safe assessment in air-gapped, OT, and high-assurance

Best for
High-assurance offline configuration analysis

Assessment mode
Offline point-in-time

Deployment
Self-installing executable (Windows or Ubuntu)

Inputs
Exported or retrieved network device configurations

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

Nipper InfraSight (Air Gapped) helps teams validate network device configurations safely in isolated environments using a fully offline deployment model. It supports secure local assessment workflows where cloud-based analysis is not permitted, helping teams strengthen hardening, accelerate reviews, and generate defensible results while keeping data within the air-gapped boundary.

The Air Gapped tier of Nipper InfraSight combines hardening and compliance capabilities in a fully offline deployment model for isolated, sovereign, classified, and OT environments. It runs on Windows or Ubuntu and supports secure review workflows across routers, switches, firewalls, Cisco Meraki, and wireless access points.

Operate safely in isolated environments

Assess configurations offline within the air-gapped environment, with deployment options that support secure local review workflows.

Accelerate assurance and audit preparation

Generate mapped reporting and pass/fail control evidence for selected controls and reporting requirements across frameworks such as NIST SP 800-53, NIST SP 800-171, PCI DSS 4.0, DISA STIGs, CMMC, and CIS Benchmarks, helping teams complete assessments up to 80% faster than manual methods.

Reveal gaps traditional tools may overlook

Identify attacker-relevant misconfigurations, control gaps, risky services, and weaknesses that policy tools, scanners, and NDR platforms are not designed to validate.

Firewall complexity reporting

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

Turn findings into action faster

Prioritize risk by severity and exploitability, with device-specific remediation guidance to help teams fix what matters first.

How it works

1. **Import or retrieve device configurations within the air-gapped environment**
2. **Run a fully offline assessment**
3. **Review prioritized findings, evidence, and remediation guidance in human-readable reports**

Who is it designed for?

Designed for teams responsible for securing and assuring network devices in isolated, sovereign, classified, and OT environments.

Common use cases

Validate devices safely before formal review
Review critical routers, switches, and firewalls without scanning, probing, or adding operational risk.

Produce evidence for hardening and compliance assessments
Generate consistent device-level evidence and mapped reporting for formal assessments in isolated environments.

Strengthen mission-critical network resilience
Identify and remediate configuration weaknesses that increase exposure and undermine operational confidence across critical environments.

What makes Nipper solutions different?

Fully offline virtual device modeling
Build a virtual model from device configurations to validate hardening, controls, and exposure without relying on cloud services or live network scanning.

Adversary-style configuration validation
Apply tester logic to uncover exploitable control gaps, hidden access paths, and misconfigurations many tools are not designed to inspect.

Designed for environments where live assessment is restricted or not appropriate
Support isolated, sovereign, classified, and OT environments where cloud services or live assessment methods are not appropriate.

Risk-prioritized findings for elite teams
Rank issues by exploitability, impact, and ease of remediation so teams can focus effort where it will reduce risk fastest.

Repeatable reporting for audit and assurance workflows
Produce consistent outputs for audits, reviews, and remediation workflows while fitting into established operational processes.

Deployment and data handling

Nipper InfraSight (Air Gapped) runs as a self-installing executable on Windows or Ubuntu. Customers may still use Nipper's SSH connectivity to retrieve and assess running configurations within an air-gapped environment, provided that connectivity is permitted.

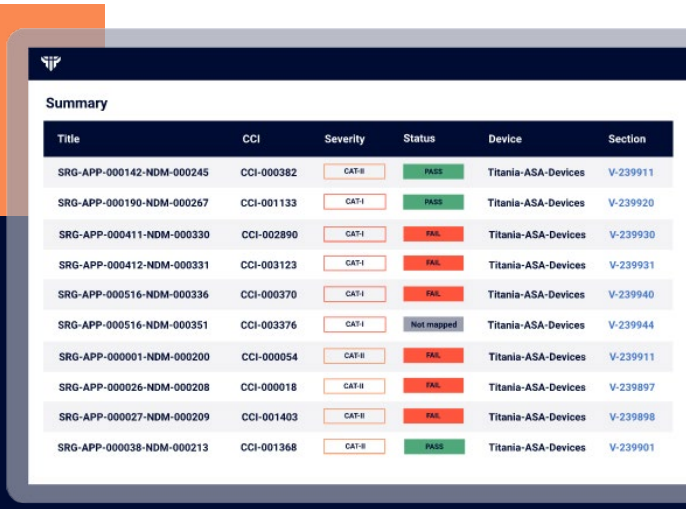
The key benefit is that Nipper InfraSight (Air Gapped) can be installed on a secure, authorized laptop, taken into the isolated environment, used to perform assessments locally, leave reports behind, and then be wiped so that no configuration data or results leave the air-gapped boundary.

Supported devices

Nipper InfraSight (Air Gapped) 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 (Air Gapped) helps teams automate offline configuration reviews, strengthen hardening, and simplify compliance preparation in isolated environments.

Get in touch