NIPPER InfraSight
BY TITANIA

Nipper InfraSight (Essentials)

Foundational hardening through inside-out device assessments

At a glance

Trusted by100+ elite cybersecurity teams and 1,000+ users worldwide.

Best for
Teams building foundational hardening workflows across critical network devices

Assessment mode
Point-in-time

Deployment
Self-installing executable (Windows or Ubuntu)

Inputs
Network device configuration files

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

Nipper InfraSight (Essential) helps teams harden routers, switches, and firewalls by turning exported configuration files into actionable security insight. It reveals misconfigurations, risky services, and control gaps that many scanners, policy tools, and NDR platforms are not designed to uncover.

The Essential tier of Nipper InfraSight provides fast, precise, point-in-time, agentless configuration assessments through a self-installing executable on Windows or Ubuntu. It delivers prioritized findings and device-specific remediation guidance to help teams strengthen hardening, validate changes, and reduce misconfiguration-driven exposure across critical network devices.

Vendor best-practice hardening audits
Run repeatable checks to uncover weak settings, risky services, and control gaps before they increase security and operational risk.

CIS Benchmark alignment
Assess against CIS Benchmarks, where supported, to strengthen baselines and reduce configuration drift.

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

NVD and PSIRT exposure checks
Use NIST NVD and Cisco PSIRT checks to highlight configuration-relevant exposure and focus remediation on the issues most likely to increase risk.

Device-specific remediation guidance
Produce clear, device-specific guidance in human- and machine-readable formats so teams can move from review to risk remediation faster.

How it works

1. **Import exported device configurations**
2. **Run a point-in-time offline assessment**
3. **Review prioritized findings and remediate issues**

Who is it designed for?

Designed for teams that need fast, point-in-time insight to strengthen device hardening, validate changes, and run consistent security reviews across critical network infrastructure.

Common use cases

Baseline hardening and review
Establish stronger baselines, expose security gaps, and prioritize fixes across critical network infrastructure.

Post-change validation
Reassess devices after updates or major changes to confirm improvements and reduce the risk of new weaknesses.

Firewall cleanup and assurance
Identify redundant objects, shadowed rules, and ineffective configurations to reduce complexity and increase confidence in change.

What makes Nipper solutions different?

Offline virtual device modeling
Analyze exported configuration files without interrogating live devices or generating disruptive traffic.

Adversary-style validation approach
Apply tester logic to uncover exploitable misconfigurations, control gaps, and hidden weaknesses many other tools are not designed to inspect.

Deeper configuration visibility
Reveal the real security state of network devices through configuration-led analysis, including issues policy-only and scan-led approaches may miss.

Prioritization for action
Rank risk issues by exploitability and impact so teams can focus effort where it reduces risk fastest.

Device-specific remediation guidance
Provide clear, vendor-specific remediation steps to help teams fix issues faster across multivendor environments.

Consistent, repeatable and risk-focused results
Produce structured findings and remediation guidance that teams can review, share, and act on with less manual effort.

Deployment and data handling

Nipper InfraSight (Essential) runs as a self-installing executable on Windows or Ubuntu. It performs agentless, point-in-time assessments using exported configuration files, helping teams validate device posture without probing production systems.

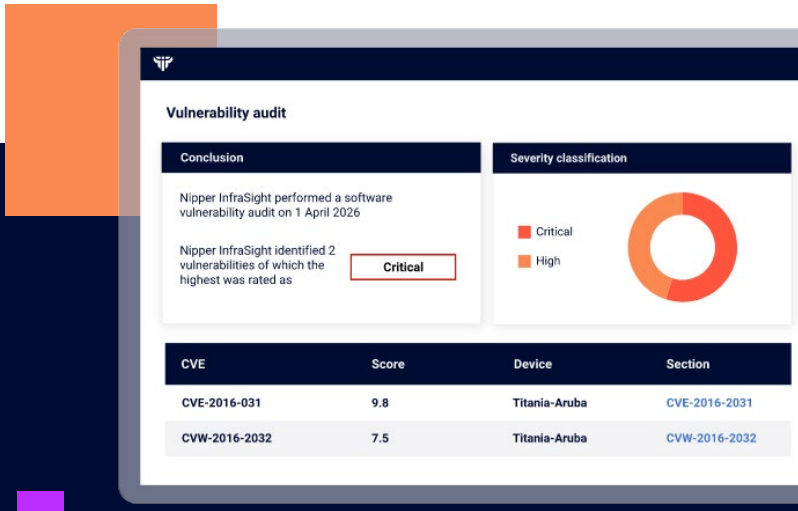
Assessments generate prioritized findings and clear remediation guidance for existing hardening, review, and governance workflows. Teams can run them on demand, for example after major changes, to validate improvements and reduce misconfiguration-driven exposure.

Supported devices

Nipper InfraSight (Essential) assesses more than 180 network device types using current vendor guidance, including routers, switches, and firewalls across multivendor environments. It helps teams apply consistent hardening reviews across core network infrastructure.

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 (Essential) helps teams harden critical network devices faster and with greater confidence.

Get in touch