NIPPER OmniSight
BY TITANIA

Nipper OmniSight (Standalone)

Scaled network exposure and compliance assessments

At a glance

Best for
Security operations, network security, and exposure management teams

Assessment mode
Scheduled point-in-time assessments

Deployment
(air-gapped, on-premises, or VPC)

Inputs
Network device configuration files

Outputs
Prioritized findings, remediation guidance, and exposure and LPA assessment outputs (where licensed)

Routers, switches, and firewalls enforce access and segmentation, but many security programs still miss a key risk: exposure created by network device misconfigurations.

Nipper OmniSight (Standalone) delivers point-in-time exposure assessment through scheduled, repeatable runs – without touching live systems. It uses penetration-tester methodology to turn configurations into prioritized findings and remediation guidance, helping teams take the first step toward scaled TEM and Zero Trust posture assessment (where licensed).

Reduce configuration-driven exposure
Find misconfigurations and control gaps, then map them to APT-linked TTPs.

Prioritize remediation with risk context
Focus teams on the findings that matter most based on impact, exploitability, and real-world attacker TTPs.

Validate segmentation and least privilege (LPA)
Confirm segmentation boundaries and expose paths that break least privilege (where licensed).

Review firewall complexity
Expose exploitable paths and rule-set complexity offline, without scanning or live traffic inspection.

Assess risk posture at scale
Measure enterprise-wide exposure and prioritize action with TEM-focused risk context.

How it works

1. **Ingest configuration data and asset labels at scale**
2. **Assess risk posture across the enterprise and by segment**
3. **Prioritize and remediate**

Who is it designed for?

Nipper OmniSight (Standalone) is designed for teams that need repeatable, point-in-time assessment across large estates – without adding a CMDB dependency or interrogating production devices.

Common use cases

Risk posture assessment
Measure enterprise-wide exposure, surface control gaps, and prioritize action with TEM-focused risk context.

Segmentation and LPA validation
Validate segmentation boundaries and expose unintended access paths that weaken least privilege (where licensed).

Audit preparation and evidence collection
Map outputs to PCI DSS 4.0 and NIST requirements to reduce manual effort and support audit preparation.

What makes Nipper solutions different?

Nipper OmniSight (Standalone) applies adversary-style testing to deliver point-in-time exposure assessment across your network estate – creating a practical starting point for scaled TEM and Zero Trust posture assessment.

Virtual device modeling
Analyze configuration files offline, without interrogating live devices.

Penetration-tester methodology
Run 200+ penetration-style tests across routers, switches, and firewalls.

See what VM platforms miss
Surface configuration-driven exposures that vulnerability management (VM) platforms and many NDR / policy tools don't validate.

Prioritization for action
Rank exposures by impact, exploitability, and mapped TTPs linked to APT activity (where licensed).

Run on schedule or on-demand
Assess after change, ahead of audits, or as part of regular exposure reviews.

Dashboards for operational decision-making
See exposure trends and segmentation weaknesses, enriched with IOC detection and threat-intelligence overlays (where licensed).

Supports exposure benchmarking and compliance reporting

Benchmark exposure against DISA STIGs, PCI DSS 4.0, NIST SP 800-53, and NIST SP 800-171 reporting requirements, and validate against NIST NVD, CIS Benchmarks, and Cisco PSIRT (where licensed).

Deployment and data handling

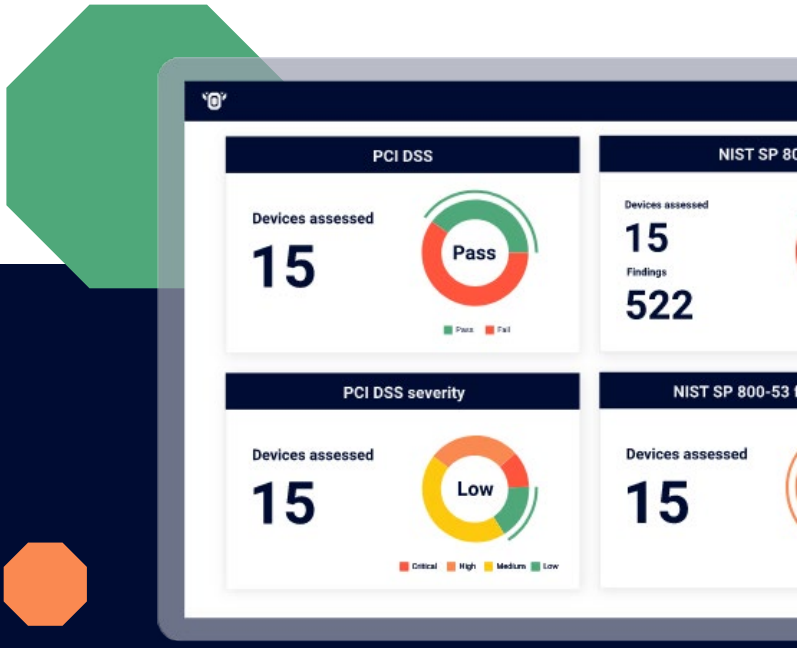
Nipper OmniSight (Standalone) is delivered as an open virtual appliance (OVA) for fast deployment and scale. Deploy as an OVA in customer-controlled infrastructure (air-gapped, on-premises, or VPC) and assess configuration data without interrogating production devices. Use it to run scheduled assessments and on-demand checks – for example after patching, provisioning, or major network change.

Supported devices

Nipper OmniSight (Standalone) assesses more than 180 network device types using current vendor guidance, helping teams scale exposure assessment across complex estates.

About Titania

UK-engineered. Trusted globally.
Titania Nipper solutions provide the configuration-validation layer many security architectures are missing, helping security and network teams reduce misconfiguration-driven exposure and assess risk posture with greater clarity. 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 reporting for complex enterprise environments.



See Nipper OmniSight in action

Book a demo or speak with one of our experts to see how Nipper OmniSight (Standalone) can help you scale exposure assessment across complex estates.

Get in touch