NIPPER OmniSight
BY TITANIA

Nipper OmniSight (Continuous)

Preemptive exposure assessment for network infrastructure

At a glance

Best for
Highly regulated, fast-changing environments needing continuous exposure assessment for network infrastructure.

Assessment mode
Continuous change discovery, drift detection, exposure and Zero Trust compromise assessments, attack path mapping, and remediation mobilization.

Deployment
OVA in your environment with supported integrations and add-ons.

Inputs
Device configurations, topology context, CMDB data, and operational sources.

Outputs
Risk- and asset-criticality-prioritized findings, drift alerts, segmentation assurance evidence, and device-specific remediation guidance to reduce exposure, speed investigation, and support audit readiness.

Nipper OmniSight (Continuous) is Titania's flagship preemptive exposure assessment platform for network infrastructure. It discovers assets and changes and prioritizes the exposures that matter most. It supports continuous exposure assessment and segmentation assurance, and mobilizes remediation and response through integration-ready workflows to help organizations operationalize CTEM, strengthen Zero Trust, and reduce attack surface, disruption, and loss.

Continuously discover change, assess impact and contextualize exposure
Normalize native and operational data to map attack paths and prioritize exposure across security, operations, and compliance.

Detect drift and policy-breaking change early
Identify authorized and unauthorized changes quickly so teams can contain exposure before it expands.

Assure foundational Zero Trust segmentation and Least Privilege Access (LPA)
Assess every change against LPA allow lists (ports/services, CIDR ranges, and users/privileges) to surface indicators of compromise and limit lateral movement and access to essential functions.

Mobilize remediation
Accelerate risk-prioritized, device-specific remediation and response through trusted SIEM, SOAR, ITSM, and GRC integrations and keep CMDBs updated for every network change.

Enable preemptive validation and resilience
Maintain trusted configuration history that supports posture trending, recovery, and stronger validation over time.

How it works

1. **Detect change, collect configs, and update CMDBs and network maps**
2. **Contextualize exposure and compromise, and identify attack paths to critical data and services**
3. **Mobilize risk-prioritized remediation and response**

Who is it designed for?

Security, network, cyber operations, architecture, and GRC teams where change can introduce immediate risk of business disruption and loss.

Common use cases

Reduce configuration drift risk
Identify policy-breaking changes early so teams can contain drift before it weakens security, operations, or audit readiness.

Prove segmentation remains intact
Highlight where NAT, ACL, firewall, and hardening changes create exposure or open unintended access to critical systems and data.

Improve incident recovery speed
Use trusted history and change diffs to investigate unauthorized changes faster and restore safer states.

What makes Nipper solutions different?

Domain-specialized for network infrastructure
Purpose-built for the routers, switches, and firewalls that shape attack paths and segmentation risk.

Contextualized, not just collected
Normalize and correlate configuration, topology, and operational context to improve prioritization.

Assessment-led and attack-path aware
Automate configuration drift, posture, and exposure assessment while highlighting the control weaknesses that matter most.

Continuous evidence for Zero Trust
Show whether segmentation policy and least-privilege controls remain enforced as the environment changes.

Built to mobilize action
Provide the detail needed for faster ticketing, assignment, and workflow integration.

Aligned to high-assurance and on-prem environments
Support critical national infrastructure, OT, and other settings where cloud-only approaches are not viable.

Deployment and data handling

Nipper OmniSight (Continuous) is deployed as an OVA within your environment and connects with supported systems through integration services. This suits organizations needing continuous, change-aware exposure and compromise assurance without a cloud-only model or manual reviews.

It collects trusted configuration records, preserves history for comparison, and highlights the changes and control weaknesses that introduce exposure. This supports investigation, remediation, recovery, and stronger validation over time.

Supported devices

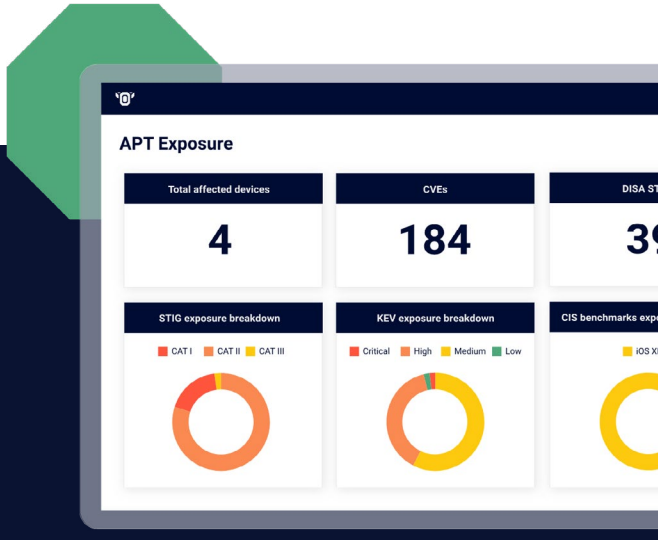
Nipper OmniSight (Continuous) supports 180+ network device types using current vendor guidance. For organizations already using Nipper InfraSight, core device support carries across the OmniSight tiers.

Integrations

Supported integrations include SYSLOG-enabled SIEM, SOAR, GRC, ITSM, CMDB, and configuration repositories, with add-ons for asset visibility, mapping, backup automation, and recovery workflows.

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 for yourself

See how Nipper OmniSight (Continuous) helps your team identify, prioritize, and reduce exposure. Request a demo or speak to one of our experts.

Get in touch