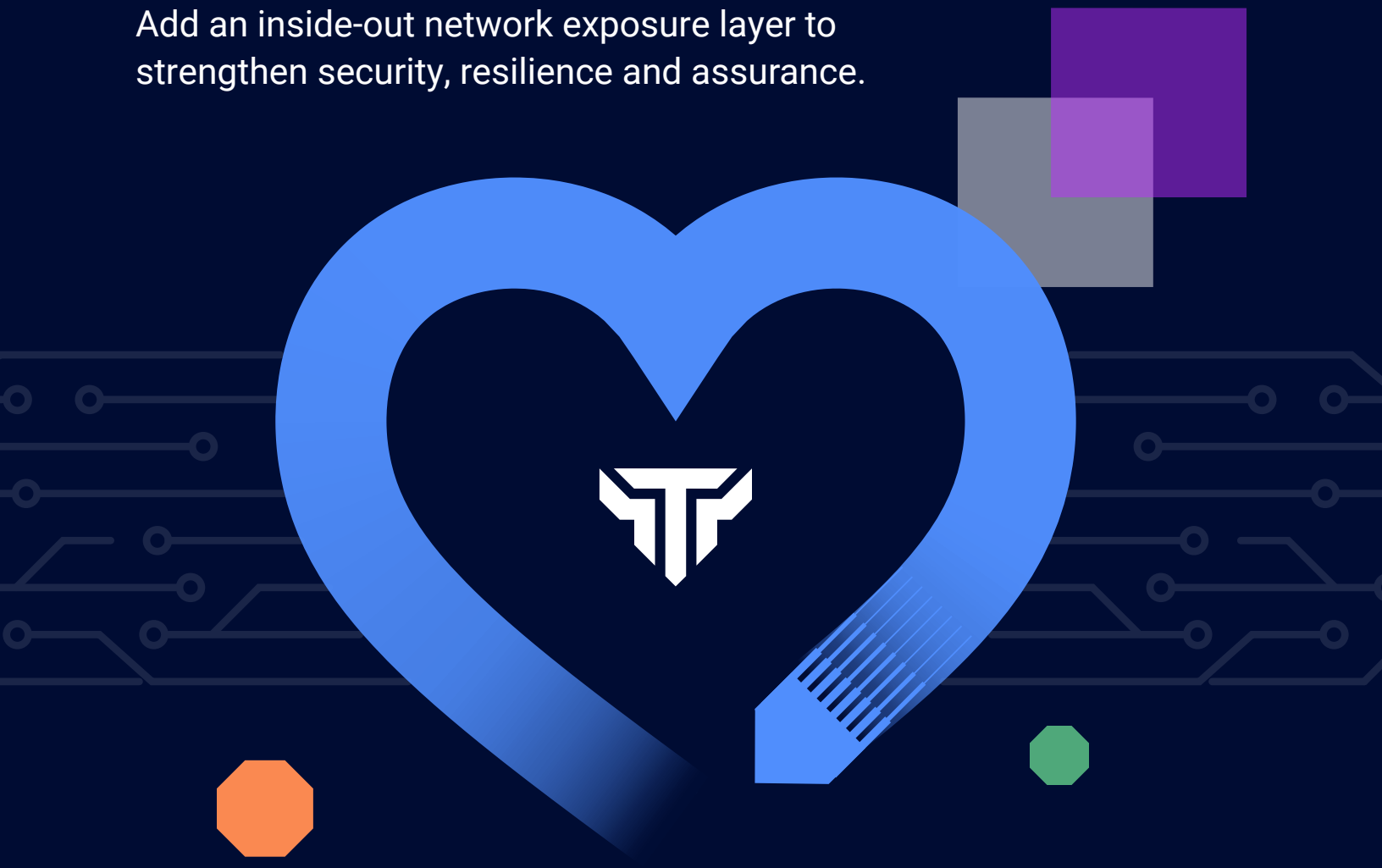
TITANIA | Solution overview titania.com

Five reasons to put Nipper solutions at the heart of your cybersecurity stack

Add an inside-out network exposure layer to strengthen security, resilience and assurance.



Introduction

Segmentation and least privilege access (LPA) assurance are the bedrock of a network that is ready, resilient, and recoverable.

As advanced persistent threats (APTs) and AI-fueled attacks compress the gap between finding and exploiting zero day vulnerabilities, organizations need more than broad visibility. They need to know whether the routers, switches, and firewalls enforcing segmentation, access, and trust are configured to hold.

Device configurations matter because a cyber breach can threaten national security, public safety, and economic resilience.

For example, the Salt Typhoon campaign infiltrated major communications providers, while the cyber incident at Jaguar Land Rover halted production and contributed to a £1.5 billion UK government-backed loan guarantee.

That is why organizations are adding an inside-out network exposure layer: to limit the impact of fast-moving attacks, strengthen resilience, and support faster, more confident recovery.

The need for a different approach

Titania's Nipper solutions provide that inside-out approach by analyzing device configurations directly.

Rather than inferring risk from scans, signals, or what responds on the network, they validate how the network is configured to behave, helping teams uncover misconfigurations, enforcement gaps, and exploitable paths other tools cannot see.

This guide tells you more - setting out five compelling reasons to add Nipper solutions to your security stack.

See what other solutions miss

Prioritize the exposures and IOCs that matter most

Get compliant faster with defensible evidence

Support faster recovery with accurate network configuration records

Detect risky network change to defend against machine-speed adversaries

What are Nipper solutions?

Nipper solutions form the configuration-validation layer many security architectures are missing.

They analyze configuration files for routers, switches, and firewalls to uncover misconfigurations, control gaps, rule conflicts, and latent attack paths and IOCs, then provide device-specific remediation guidance prioritized by risk and business impact.

Nipper solutions are trusted by 1000+ organizations, including 100+ critical infrastructure providers, and support 180+ device types across 20+ vendors.

NIPPER InfraSight

Nipper InfraSight delivers point-in-time hardening and compliance assessments for individual devices across the Essential, Compliance, and Air Gapped tiers.

NIPPER OmniSight

Nipper OmniSight extends these capabilities to enterprise scale across the Standalone, Integrated, and Continuous tiers.

The following pages demonstrate the capabilities Nipper solutions bring to stregthen security, resilience and assurance.

Reason one

See what other solutions miss

Broad exposure, vulnerability, and policy platforms can show what is visible from the outside or infer which issues may matter.

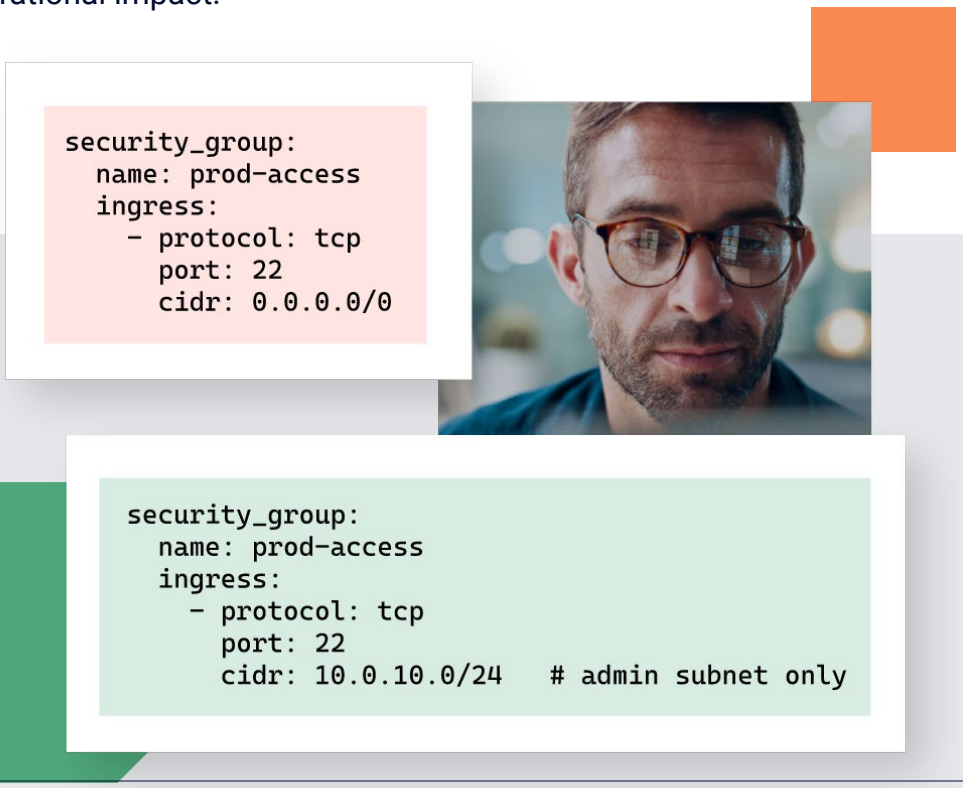
What they often cannot prove is whether the network devices enforcing segmentation, access, and trust are configured to behave as intended, or whether least privilege access (LPA) is still holding where it matters most.

Using Titania's virtual device modeling, Nipper solutions analyze configurations directly to uncover misconfigurations, control gaps, rule conflicts, and latent attack paths that scan-led or policy-only approaches may miss.

That gives teams a more deterministic view of how the network is set to behave and whether segmentation and LPA controls are strong enough to limit attacker movement and reduce operational impact.

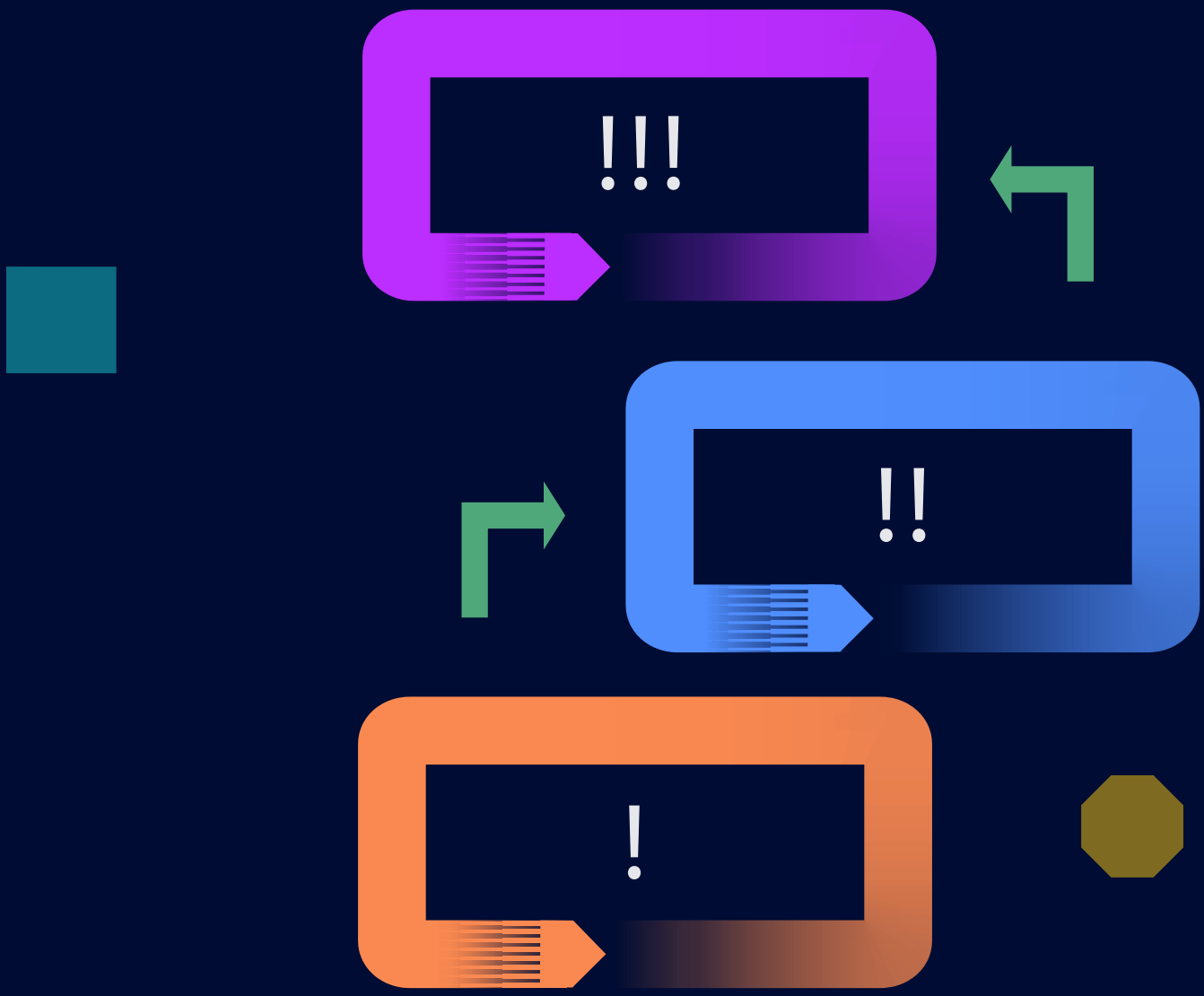
Nipper solutions also support environments where live scanning, cloud-only analysis, or intrusive collection methods are not appropriate or are restricted. With offline, air-gapped, and customer-controlled deployment options, they fit high-assurance, sovereign, classified, operational technology (OT), and other tightly regulated environments.

The result is not another broad exposure platform, but a complementary inside-out network exposure layer that validates the network behavior other tools assume is working and helps teams build networks that are more ready, resilient, and recoverable when attacks hit.



Reason two

Prioritize the exposures and IOCs that matter most



On complex networks, teams rarely lack findings. What they often lack is clarity on which exposures and IOCs create the greatest business risk. That slows effective remediation and response and leaves high-impact risks unresolved for longer.

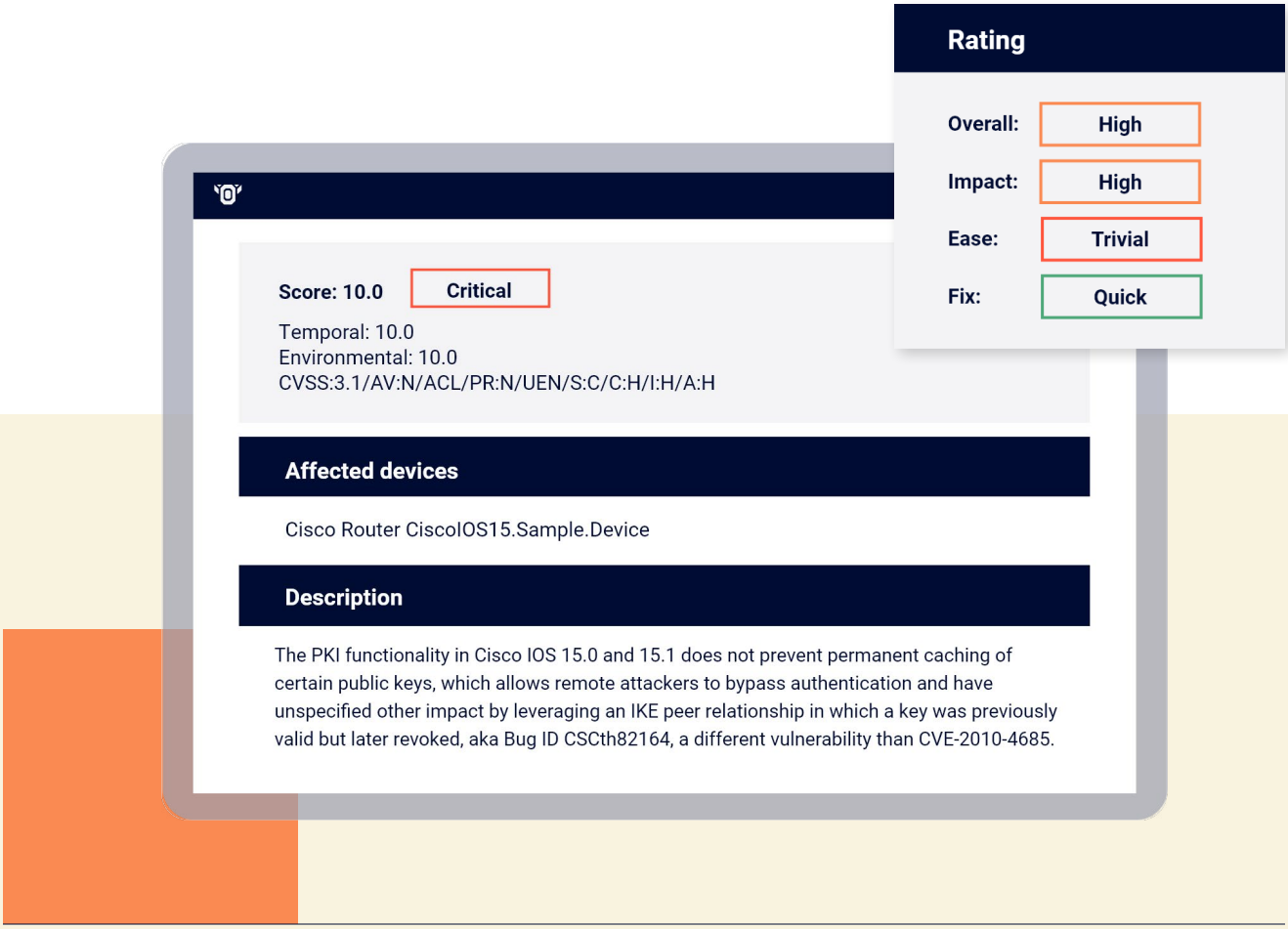
Nipper solutions help prioritize what matters by grounding findings in network truth: how devices are configured, how controls interact, and where exploitable weaknesses could affect critical assets, services, or audit outcomes.

They combine asset and configuration context, recurring issue trends, and supported threat intelligence to help teams separate urgent exposure from background noise.

Instead of treating every issue alike, security and network teams can focus effort where it reduces risk fastest.

Nipper InfraSight supports device-level prioritization for hardening and compliance, while Nipper OmniSight adds wider estate and segment-level posture context, including change, trend, and path insight, where supported by tier.

The result is faster, risk-prioritized remediation and response supported by evidence teams can trust and act on.



Reason three

Get compliant faster with defensible evidence

As cyber regulation tightens, organizations need faster ways to prove that network controls are configured to hold. Manual evidence gathering is slow, inconsistent, and difficult to repeat under pressure.

Nipper solutions help by assessing device configurations against supported standards and producing audit-ready, device-level evidence alongside prioritized findings and remediation guidance.

Crucially, findings are deterministic by design, because they are obtained from running device configurations and apply explicit logic, not inference.

Nipper InfraSight supports mapped reporting for frameworks such as PCI DSS 4.0, NIST SP 800-53, NIST SP 800-171, CMMC, DISA STIGs, and CIS Benchmarks, while also validating against sources such as NIST NVD and Cisco PSIRT, where supported by tier.

Nipper OmniSight extends this with broader exposure and compromise assurance insight to support ongoing control review, remediation planning, and audit readiness in line with Zero Trust and continuous threat exposure management (CTEM) best practice.

Teams can identify what to fix and respond to first, rerun assessments, and show exposure and compromise posture improvement with clearer evidence.

For organizations already using broad vulnerability or exposure tools, Nipper solutions add the inside-out network evidence needed for a fuller, more defensible view of risk.

Reason four

Support faster recovery with accurate network configuration records

When incidents, outages, or unauthorized changes affect the network, recovery is only as fast as the records teams can trust. If configuration history is incomplete, outdated, or scattered across systems, response slows and risk of business-critical disruption and loss rises.

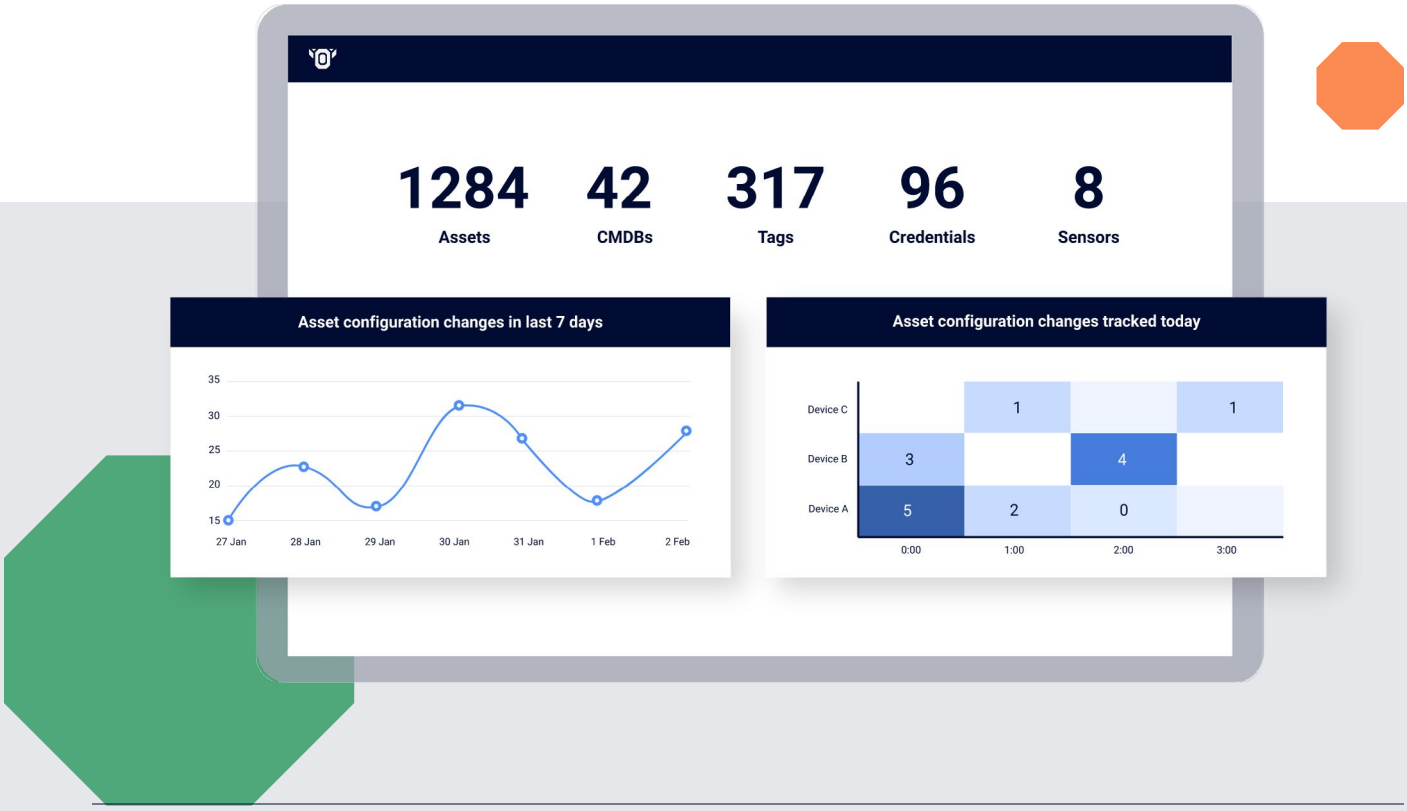
Accurate network configuration records help teams understand what changed, identify safer, known-good states, and support faster recovery planning. They also reduce the risk of restoring the wrong configuration, overlooking the control gap that caused the issue, or losing the network source of truth that underpins effective digital transformation.

This is where current configuration records and connected operational context matter.

Nipper OmniSight supports tier-aligned integration with configuration repositories, configuration management databases (CMDBs), and related systems to help teams maintain more reliable records for assessment, investigation, recovery, and resilience workflows.

That means resilience is not just about knowing what should be on the network. It is about having accurate configuration evidence teams can use to restore service, validate recovery steps, and reduce repeat exposure.

Policy automation tools can help define intent at scale. Nipper solutions help confirm the network devices enforcing that intent remain configured to support resilience and recovery.



Reason five

Detect risky network change sooner to defend resilience against machine-speed adversaries

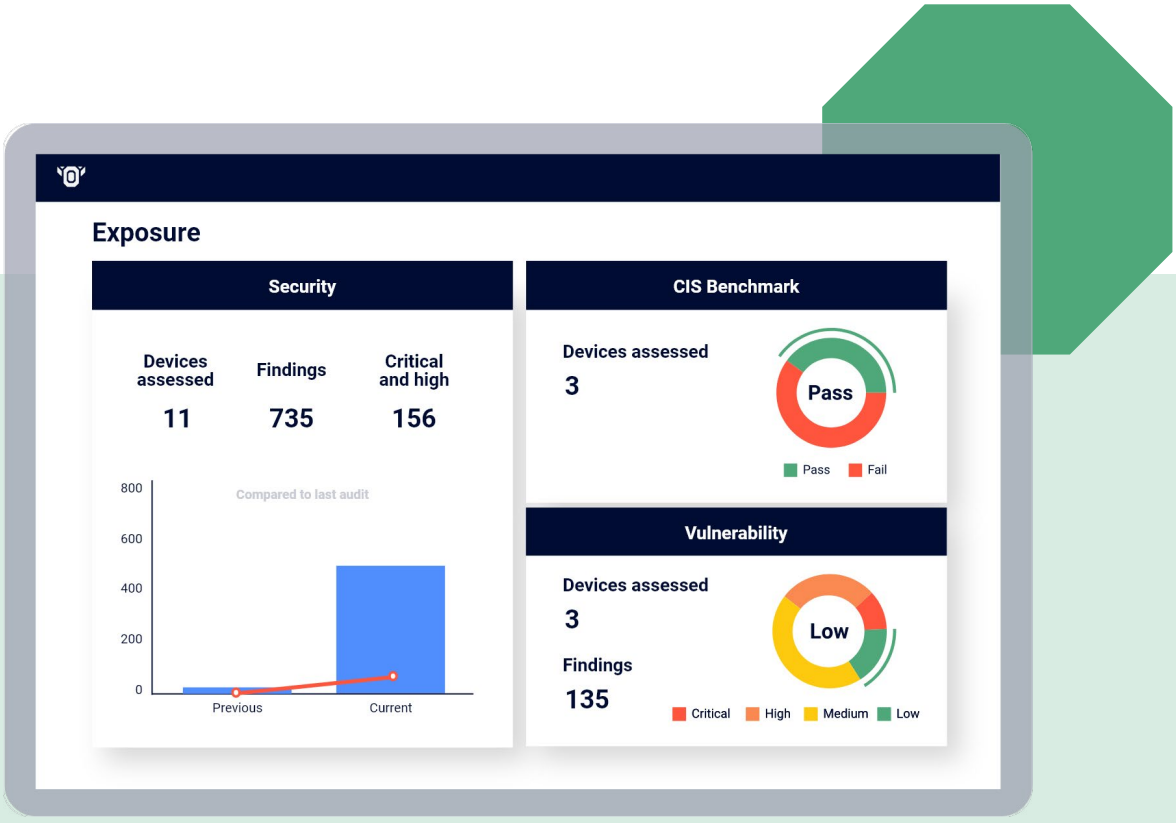
As AI accelerates attacks to machine speed, the time between exposure being introduced and exploited can shrink dramatically. Organizations need to identify risky change and emerging vulnerabilities earlier so they can contain impact, protect resilience, and respond with more confidence.

Nipper OmniSight (Continuous) is designed for that challenge. It supports continuous change discovery, drift detection, exposure and compromise assessment, attack path mapping, and remediation mobilization across fast-changing or high-assurance environments.

By preserving trusted configuration history and highlighting policy-breaking or unexpected changes, it helps teams investigate whether a change is expected, identify IOCs sooner, and understand potential consequences before exposure spreads and recovery becomes harder.

That enables security and network teams to connect change with risk, validate segmentation and LPA controls, and move faster from detection to containment and risk-prioritized remediation and response.

It is a proactive, and in the case of OmniSight (Continuous), preemptive model built to reduce uncertainty, disruption, and loss while helping networks stay ready, resilient, and recoverable as environments change and attackers move faster.



The Nipper solutions family

The Nipper solutions family includes six tiers designed to match different operating models, assurance requirements, and levels of automation.

NIPPER InfraSight

Essential

Point-in-time, agentless configuration assessment with best-practice hardening checks, exposure insight, firewall complexity reporting, and device-specific remediation guidance.

Compliance

Adds mapped compliance reporting and pass/fail evidence for supported frameworks to accelerate audit preparation and remediation planning.

Air Gapped

Delivers hardening and compliance capabilities in a fully offline mode for isolated, sovereign, classified, OT, and other high-assurance environments.

NIPPER OmniSight

Standalone

Scheduled, repeatable configuration risk posture assessment across larger estates without requiring continuous collection or a CMDB dependency.

Integrated

Adds trusted context from repositories, CMDBs, and connected systems to support recurring assessment, prioritization, and workflow alignment.

Continuous

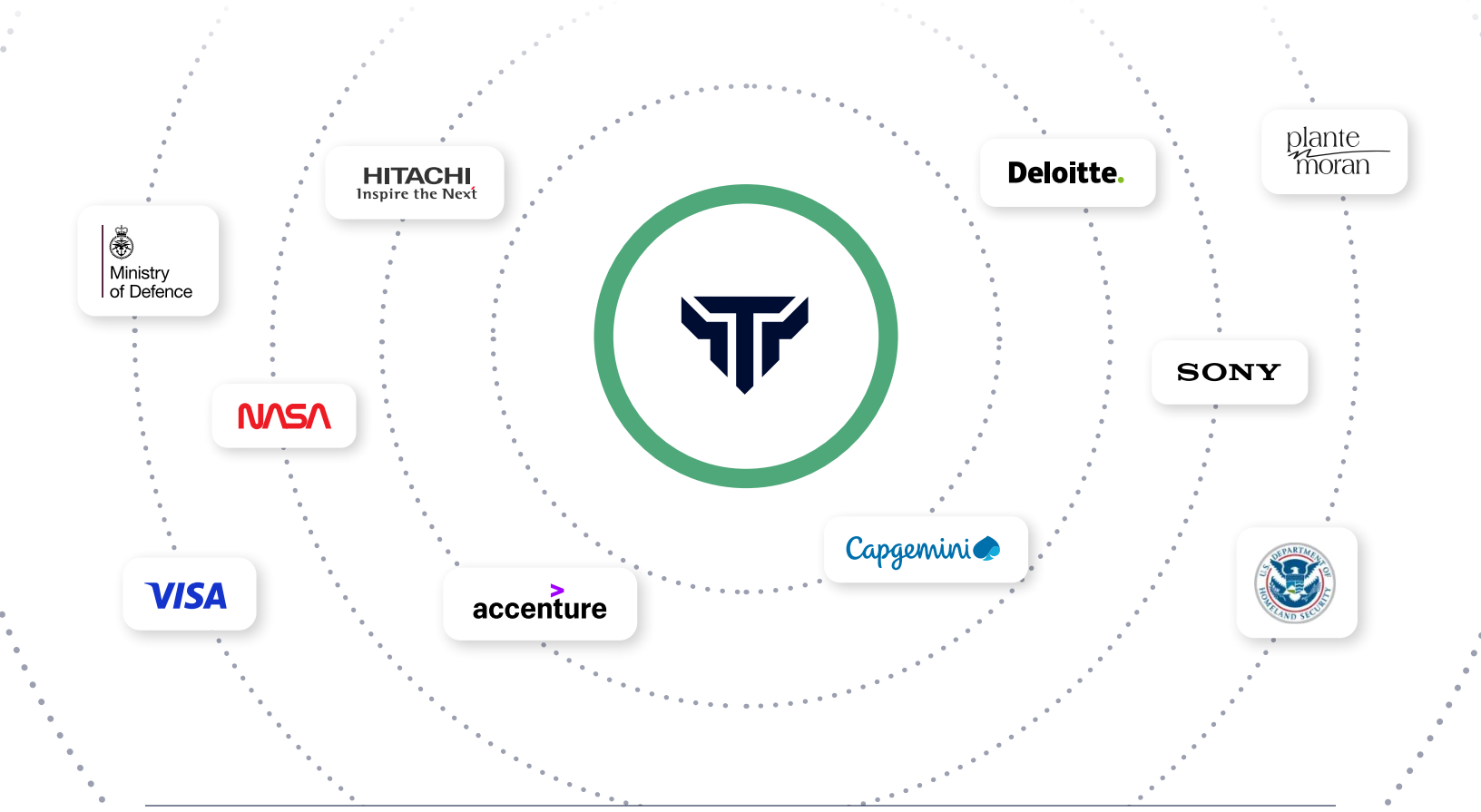
Provides continuous change discovery, drift detection, segmentation assurance, attack path insight, and remediation and response mobilization for fast-changing or high-assurance networks.

About Titania

Securing the networks society depends on

Titania helps governments, defense, critical infrastructure, and enterprise organizations reduce risk by uncovering configuration-level exposures attackers exploit. Built on virtual device modeling and adversary-style testing, Nipper solutions help teams identify hidden exposure faster, prioritize remediation with greater confidence, and generate audit-ready evidence.

The Nipper portfolio supports teams from point-in-time hardening and compliance assessment to ongoing, change-aware exposure assessment. Headquartered in the UK with operations in Arlington, VA, Titania is trusted by 1000+ organizations, including 30+ U.S. federal agencies and 100+ critical infrastructure providers.



Find out more

Whether you want to uncover exposure other tools miss, generate stronger audit evidence, or improve resilience and recovery, Nipper solutions can help. Contact Titania to learn more or arrange a demo.

Book a demo

TITANIA

USA
Suite 600,
2451 Crystal Dr, 6th Floor,
Arlington, VA 22202
enquiries@titania.com

UK
167-169 Great Portland Street,
London, England,
W1W 5PF
enquiries@titania.com