Is your network ready?

Adversaries continue to exploit one of the most basic and preventable weaknesses in cybersecurity: exposures created by misconfigured network devices.

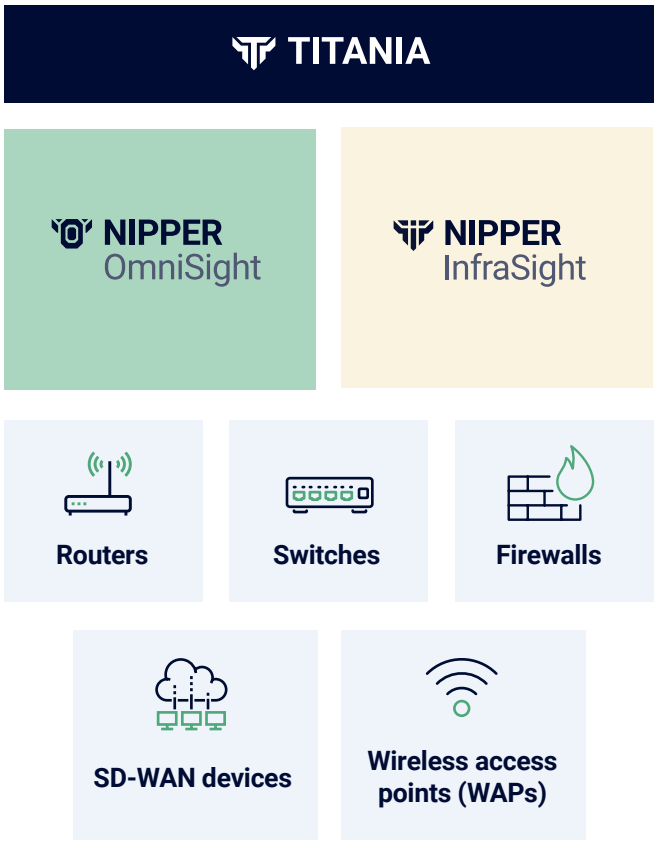
Nipper solutions: Purpose-built for configuration exposure management

Titania Nipper solutions provide high-assurance, configuration-centric security for the routers, switches, firewalls, SD-WAN devices, and wireless access points (WAPs) that underpin every business-critical network.

Built on Titania's trusted virtual-device modelling and adversary-style testing methodology, Nipper solutions identify, prioritize, and help teams remediate the configuration weaknesses that create real attack paths.

Supporting organisations across the exposure management maturity curve

From high-value, point-in-time exposure assessments today to scheduled or continuous exposure management programs tomorrow, Nipper solutions support teams at all maturity levels.



NIPPER InfraSight

Fast, accurate, device-level configuration exposure assessment.

InfraSight (Essential)

- Provides fast, precise, point-in-time, agentless config assessments
- Supports assessments of routers, switches and firewalls
- Performs best-practice audits, NIST NVD and Cisco PSIRT checks, CIS Benchmarks (where supported), and filtering complexity reporting
- Results available in human- and machine-readable formats

InfraSight (Compliance)

- Includes all InfraSight (Essential) capabilities
- Adds structured reporting aligned with NIST 800-53, NIST 800-171, PCI DSS 4.0 and RMF mapping
- Includes pass / fail evidence per control
- Expands coverage through Premium capabilities such as DISA STIG assessments
- Support for Cisco Meraki, SD-WAN and wireless access points (WAPs)

InfraSight (Air Gapped)

- Delivers the full InfraSight (Essential) and InfraSight (Compliance) capability set
- Fully offline for classified, sovereign, OT and mission-critical networks
- Supports DISA STIGs (Premium) and strict operational control environments

Best for: Auditors and assessors needing immediate exposure visibility or preparing for major audits, and teams establishing foundational hardening workflows across critical network devices.

NIPPER OmniSight

Enterprise-scale exposure visibility – scheduled or continuous.

Nipper OmniSight extends the precision of our virtual modelling technology across entire networks, enabling scheduled, repeatable or continuous exposure-management programs.

OmniSight (Standalone)

- Direct offline upload of configs, enabling full, scheduled assessments
- Best-practice + CIS checks, NVD / PSIRT overlays
- Filtering complexity reporting
- PCI / NIST / DISA STIG (Premium) reporting
- Executive insights dashboards
- Holistic and segmentation-level posture visibility (snapshot + trend dashboards)
- MITRE Att&ck and Indicators of Compromise (IOC) threat-context overlays
- IOC through Zero Trust segmentation assurance
- Multi-site trend analysis and device-level attack surface visibility

OmniSight (Integrated)

Includes all OmniSight (Standalone) capabilities, plus:

- Automated scheduling and orchestration
- CMDB read-only ingestion
- Asset discovery (limited via CMDB)
- SIEM integration
- Centralized baselines
- DISA STIG (Premium)

OmniSight (Continuous)

Delivers the full OmniSight (Standalone + Integrated) capability set, plus:

- CMDB full synchronization and change detection
- Continuous configuration-drift detection
- Persistent visibility of device-level attack surface
- Ongoing Zero Trust control validation
- Automated backups
- Asset discovery (not limited to CMDB capability)
- Optional threat-intel context
- Enables continuous exposure visibility, prioritisation and governance

Why configuration exposure matters

Security tools such as policy engines, network detection and response (NDR), endpoint protection, and vulnerability scanners remain vital, but none can confirm whether network infrastructure devices themselves are securely configured.

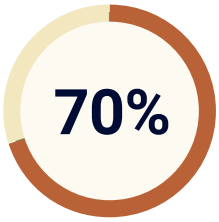
Without configuration-exposure visibility, organizations lack confidence that segmentation, least-privilege access and Zero Trust controls are truly being enforced.

Despite unprecedented investment in detection technologies, the same exposures persist because the root cause remains unaddressed – foundational configuration hygiene across routers, firewalls, and switches.

Misconfiguration-driven exposures are widespread, growing, and disproportionately exploited:

Exploits remain the #1 attack vector

Mandiant M-Trends 2025



70% of exploitable vulnerabilities originate on network infrastructure devices – not endpoints

2025 OT/ICS Cybersecurity report – Dragos

Routers account for over half of today's most vulnerable devices

Riskiest Connected Devices of 2025 report – Forescout

Half of all global ransomware attacks now hit essential sectors

Escalating Ransomware Threats to National Infrastructure – KELA

Unhardened default configurations are the leading cause of misconfigurations

NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations – CISA

Attackers don't need zero-days when basic controls are left undone. Breaches continue to stem from simple, preventable oversights: missed hardening steps, forgotten devices, insecure defaults, and flat, overly permissive architectures.

The time to act is now

Configuration-driven exposure is accelerating due to:

AI multiplying attacker speed and breadth, widening the attack target scope

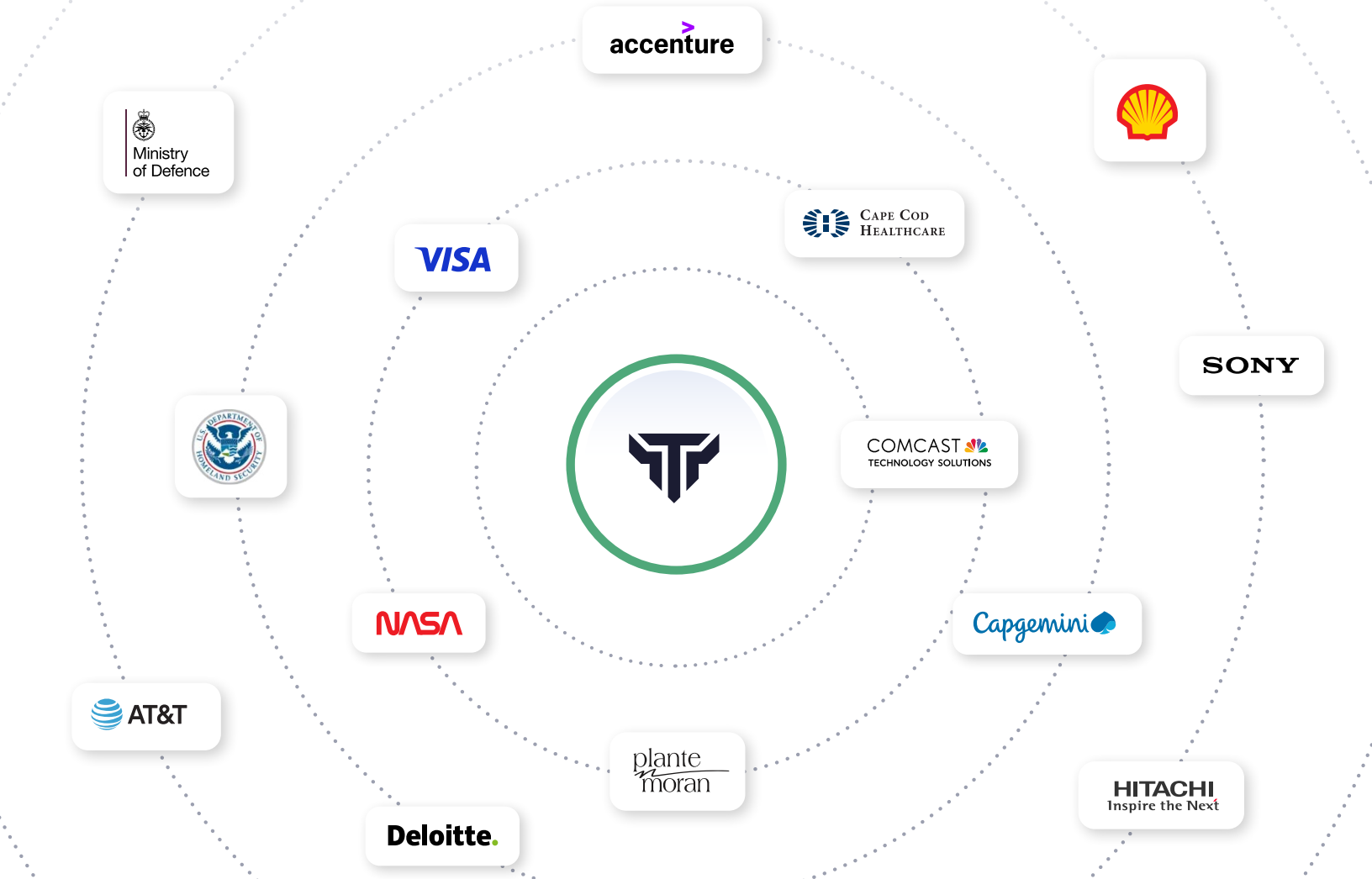
Rising regulatory pressure across CORA, DORA, CMMC, NIS2, PCI DSS 4.0, TSA, and national resilience mandates

IT-OT-cyber-physical convergence, expanding blast radius and operational impact

Misconfigurations remain the path of least resistance for adversaries. For defenders, managing configuration exposure is now central to resilience.

Why organizations choose Titania

- **Pen-tester accuracy** via industry-leading virtual device modelling.
- **Agentless, offline and safe** for sovereign networks, OT, and mission-critical networks.
- **Trusted by 100+ elite cyber teams** and deployed across **800+ organizations worldwide**
- **UK-engineered. Globally trusted.** Built for clarity, confidence and resilience.



About Titania

UK-engineered. Globally trusted. Unmatched in finding and fixing the critical misconfigurations everyone else misses. In an AI-accelerated threat landscape, Titania enables every organization to answer the only question that matters: **Is your network ready?**

Get in touch

TITANIA

USA
Suite 600,
2451 Crystal Dr, 6th Floor,
Arlington, VA 22202

UK
167-169 Great Portland Street,
London, England,
W1W 5PF