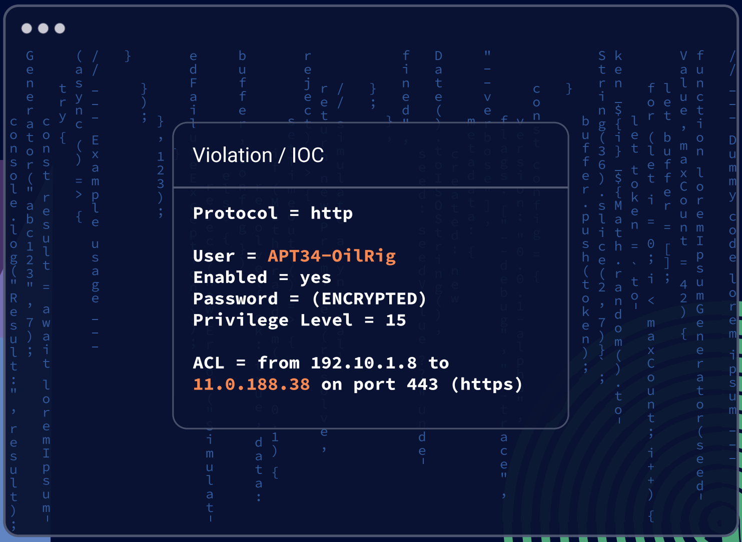
TITANIA | Solution overview titania.com

Nipper and Nipper Resilience

Built for network, security and cyber operations teams who need to assure operational resilience, network readiness and compliance through proactive defense against cybersecurity threats.



Violation / IOC

```
Protocol = http

User = APT34-OilRig
Enabled = yes
Password = (ENCRYPTED)
Privilege Level = 15

ACL = from 192.10.1.8 to
11.0.188.38 on port 443 (https)
```

You can't defend against what you can't see

Gartner predicts there will be more than one million documented vulnerabilities and exposures within five years, while threat intelligence experts at Mandiant currently track more than 4,000 threat groups globally.

Finding and fixing the few vulnerabilities that pose a critical threat to your network is the difference between resilience and risk when you are defending against:

- **Systematic targeting of network devices** by Advanced Persistent Threat (APT) and ransomware groups
- **Living off the Land (LOTL) tactics** used by adversaries to disrupt, degrade, or destabilize networks over time
- **Configuration drift and misconfigurations** that create unknown security gaps and compliance blind spots

#1 Attack vector

Exploits are the most frequently observed initial infection vector

Mandiant M-Trends 2025

11 days

The average amount of time an attacker is present in an environment before they are detected

Mandiant M-Trends 2025

68%

The share of breaches with a human-error component

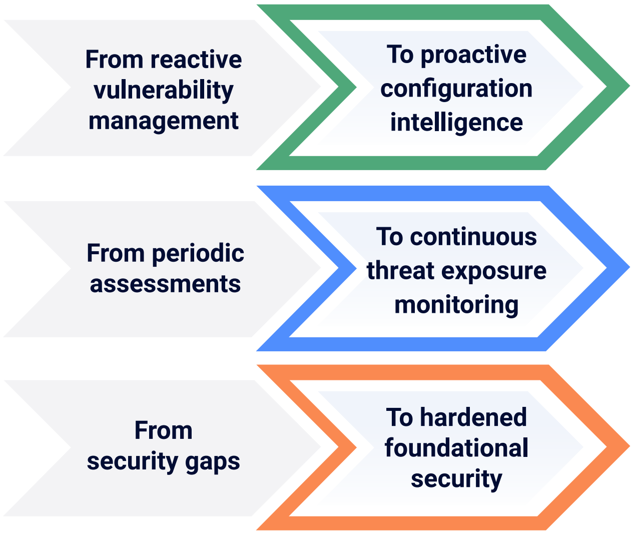
2024 Data Breach Investigations Report (DBIR) - Verizon

Harden your foundational security for continuous threat exposure management

Maintaining an up-to-date, authoritative configuration management database (CMDB) is key to operational resilience. It enables you to monitor how configuration changes occur, who makes them, and whether they introduce risk. But if it is not on your digital transformation roadmap right now, we can still help you on that journey towards resilience and provide threat exposure management (TEM) capabilities at a regular cadence.

While others react to breaches, Nipper Resilience helps you target and fix exposure to critical network threats before attackers can exploit them.

Transform your approach:



From reactive vulnerability management → To proactive configuration intelligence

From periodic assessments → To continuous threat exposure monitoring

From security gaps → To hardened foundational security

Key capabilities and outcomes

Maintain operational resilience

Reduce risk by prioritizing your most critical exploitable threats with penetration tester-level accuracy, segment-by-segment analysis, and automated prioritization by criticality and exploitability.

Unique capability to deploy to air-gapped environments and operate with minimal effect on the network operational bandwidth for sovereign and maximum-security environments.

Protect your entire attack surface with end-to-end visibility across on-premises, operational technology (OT), industrial control system (ICS) and multi-cloud environments.

Ensure network readiness

Continuous configuration monitoring of routers, switches, firewalls, and wireless access points.

Pre-empt exploits by identifying and mapping vulnerabilities and misconfigurations automatically to specific CISA Known Exploited Vulnerabilities (KEVs) and MITRE ATT&CK tactics, techniques and procedures (TTPs).

Enhance decision making with intuitive threat dashboards including strategic risk trending, business impact analysis, and historical attack surface analysis.

Recover fast

Speed up disaster recovery and prevent incidents with a digital twin.

Manage configurations as code (CaC) and maintain backup of configs.

Restore configs as easily as the hardware in the event of an incident and test config changes before they go live.

Assure compliance

Simplify compliance reporting with the latest readiness and resilience mandates, including:

- **DoD CORA** – Cyber Operational Readiness Assessment
- **EU DORA** – Digital Operational Resilience Act
- **NIS2** – Network and Information Security (NIS) Directive
- **CIS Benchmarks** – Center for Internet Security
- **NCSC CAF** – Cyber Assessment Framework
- **PCI DSS 4.0** – Payment Card Industry Data Security Standard

Readiness is the best defense

Nipper Resilience provides continuous real-time visibility of network changes, threat exposure, and indicators of compromise. These critical capabilities support proactive security and assure foundational Zero Trust network segmentation and least privilege access principles, compliance with regulatory mandates, and are core to achieving operational resilience, network readiness and recoverability.

80%	10x	250k^{+}	100
Reduction in network security assessment time	**Faster critical threat identification and remediation**	**Network devices that can be assessed continuously at enterprise scale**	**Critical Infrastructure providers across government and commercial industry verticals trust Nipper**

Use cases and capabilities

Titania Nipper Resilience is an enterprise grade platform with Nipper as the engine.

Nipper

- Point in time assessments of foundational security, compliance and vulnerability, with device-specific remediation guidance
- Agentless (Direct connectivity to devices or pre extracted configs), virtual modelling of the device for unmatched accuracy and performance
- Comprehensive human readable report with evidence, risk prioritization

Nipper Resilience for security operations

- Automated scheduled credentialed assessments at scale, enhanced risk prioritization, risk prioritized remediation guidance
- Holistic or segmentation posture visibility (snapshot and trends) through dashboards, threat (TTP/APT) exposure, IOC exposure
- Integration with CMDB or direct upload, offline assessment without affecting network operational bandwidth

Nipper Resilience for network operations

- Asset discovery, network terrain and attack path mapping, asset inventory (population of an external configuration storage e.g. CMDB), asset validation
- Network change detection
- Visibility of change (planned vs unplanned)

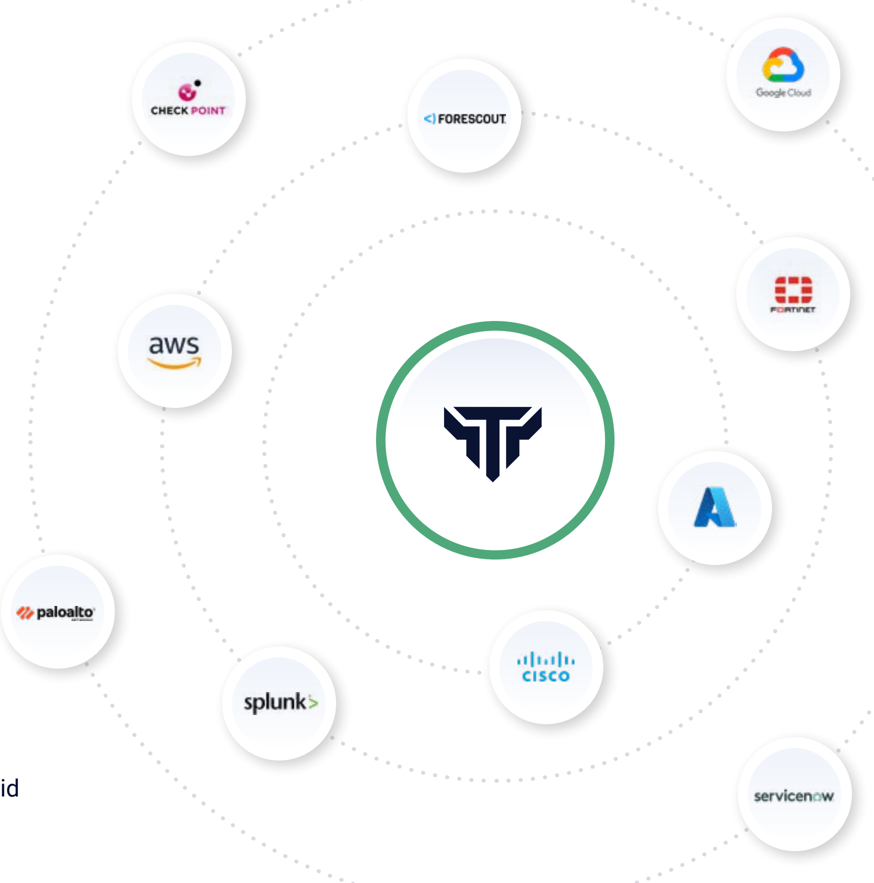
Nipper Resilience for cyber operations

- Integration with a SIEM (single pane of glass), integration with ITSM/GRC/SOAR
- Visibility of contextual change (integration with CMDB)
- Overlay attack path mapping with TTP/IOC exposure, overlay attack path mapping with external cyber ops data for endpoints and cyber physical systems (OT, IOT)

Nipper Resilience with CMDB

- Disaster recovery (restore to a last known secure configuration)
- Visibility of contextual change, audit trail
- Ability to test pre-production changes (configuration as code)

Technical overview



Comprehensive coverage

- **180+** devices from **20+** network vendors (including Cisco, Juniper, Palo Alto, Fortinet, Check Point).
- **Multi-cloud deployment support** (AWS, Microsoft Azure, GCP configurations).
- **Legacy to modern** infrastructure assessment.

Enterprise integration

- **SIEM/SOAR workflows** for automated response
- **API-first** architecture for custom integrations
- **Deployment options** for on-premises, cloud, and hybrid environments.

Partner integrations

- **Elastic** – ECS-normalized data feeds with purpose-built, intuitive dashboards.
- **Forescout** – eyeExtend Connect for Nipper Resilience on Forescout Marketplace.
- **ServiceNow** – Nipper Resilience is certified for the ServiceNow CMDB app available within the ServiceNow app store.
- **Splunk** – Native CIM-compliant data ingestion with pre-built, intuitive dashboards.

> "At AmiViz, we're focused on delivering real value—not just products. With Titania, we're enabling enterprises to take a more proactive approach to cybersecurity, which is critical as digital transformation accelerates across the region."
>
> **Ilyas Mohammed, COO, AmiViz**
>
> AmiViz Enterprise Marketplace

TITANIA

Ready to see what you've been missing?

Join the elite security organizations who trust Titania Nipper and Nipper Resilience to defend their most critical networks.

Book your network security assessment

titania.com