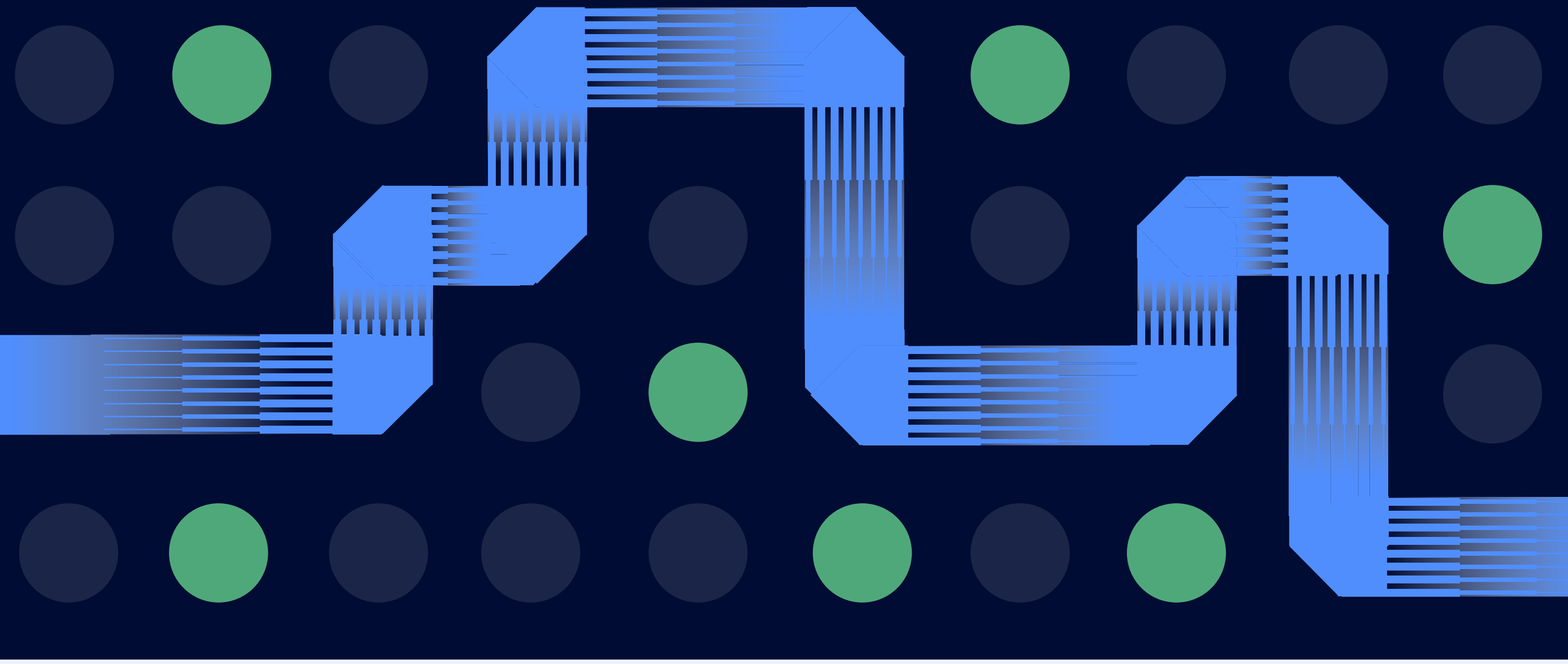
Close the gaps: strengthen your network security against advanced threats



The growing threat to your network infrastructure

Right now, bad actors are systematically targeting organisations like yours.

Successful breaches across the world by Advanced Persistent Threat (APT) groups, such as Salt Typhoon and Volt Typhoon, have proven that network devices - routers, switches, firewalls and wireless access points - are high value targets.

Using Living off the Land (LOTL) tactics, these adversaries exploit vulnerabilities to disrupt, degrade, and destabilize networks over time.

Meanwhile, access brokers are thriving. These threat actors don't break through your defenses; they exploit overlooked gaps like weak segmentation or default settings. They then sell this access to ransomware gangs or nation-state actors. Their marketplace is booming, and your misconfigurations are their inventory.

The reality of network vulnerabilities

#1

Exploits are the #1 attack vector

Mandiant M-Trends 2025

50%

Routers account for more than 50% of the most vulnerable devices

Riskiest Connected Devices of 2025 report – Forescout

70%

70% of vulnerabilities reside deep within the network

2025 OT/ICS Cybersecurity report – Dragos

9.5m

9.5 million cyberattacks were fuelled by misconfigurations in the first half of 2025

Most exposures start at the network layer via misconfigurations, configuration drift and unpatched systems, creating unknown security gaps and compliance blind spots.

The challenge: traditional security techniques are falling short

Many organizations struggle to address exploitable vulnerabilities in network devices because traditional cybersecurity techniques - like network scanning, pattern matching and policy management - fail to see them.

With AI and automation, your adversaries advantage is accelerating. From pre-attack reconnaissance to post-compromise persistence, attackers now operate with unprecedented speed, precision, and reach.

To regain the upper hand, your teams need preemptive capabilities to:

- Identify critical device misconfigurations and vulnerabilities.
- Prioritize remedial actions before they can be exploited.

The Titania Nipper solutions advantage

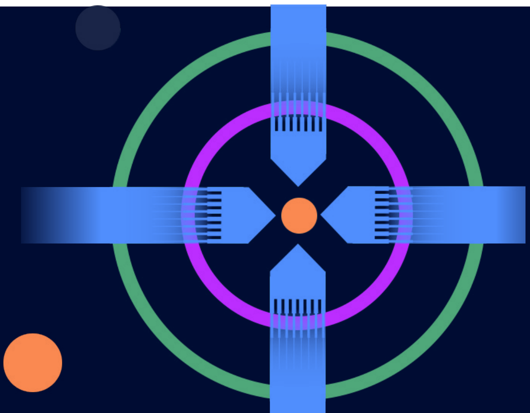
Titania's award-winning Nipper solutions focus exclusively on securing physical and virtual routers, switches, firewalls, and wireless access points.

Powered by proprietary virtual modeling technology and unique penetration-tester methodology, Nipper solutions analyze network device configurations the way APT groups do to identify misconfigurations that create attack paths - regardless of patch status.

Key features:

- Device-specific security settings
- Vendor hardening guidelines
- Configuration-level vulnerabilities
- Common Vulnerabilities and Exposures (CVEs)
- DISA STIG, NIST compliance templates, and federal security requirements

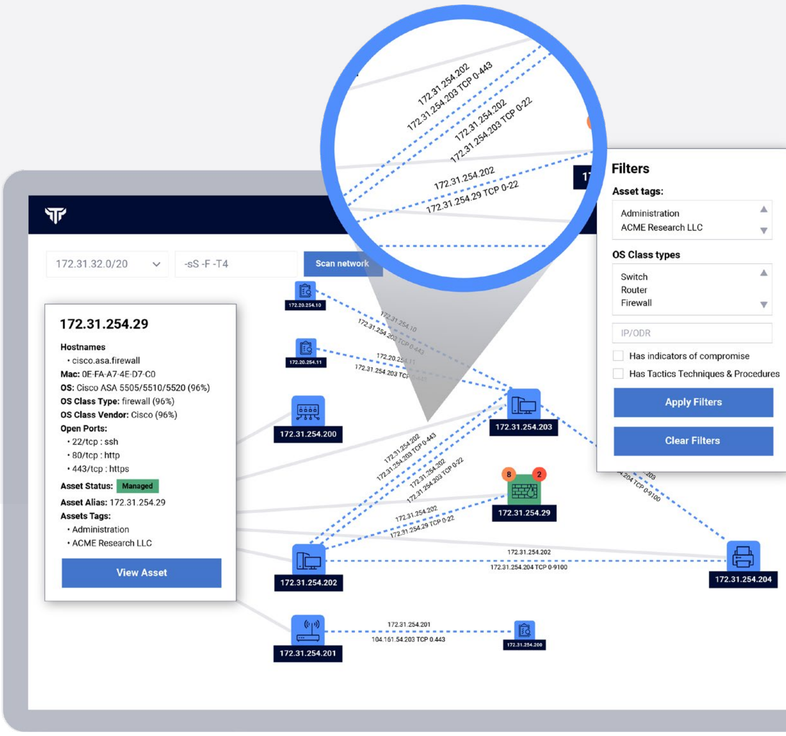
> **“We don’t just identify vulnerabilities; we eliminate attack paths.”**
>
> Ian Robinson, CPO, Titania



Why network devices are the weakest link

Network devices don't just connect to the network - they are the network. A misconfigured router doesn't need to authenticate; it's already trusted. A switch with weak access controls doesn't trigger network access control (NAC) policies; it enforces them.

This is why network devices must be continuously validated, assessed for exposure to active threats, and hardened against adversary tactics.



172.31.32.0/20 -sS -F -T4 Scan network

172.31.254.29

Hostnames
- cisco.asa.firewall

Mac: 0E-FA-A7-4E-D7-C0
OS: Cisco ASA 5505/5510/5520 (96%)
OS Class Type: firewall (96%)
OS Class Vendor: Cisco (96%)
Open Ports:
- 22/tcp : ssh
- 80/tcp : http
- 443/tcp : https

Asset Status: Managed
Asset Alias: 172.31.254.29
Assets Tags:
- Administration
- ACME Research LLC

View Asset

Filters
Asset tags:
Administration
ACME Research LLC
OS Class types
Switch
Router
Firewall
IP/ODR
□ Has indicators of compromise
□ Has Tactics Techniques & Procedures
Apply Filters
Clear Filters

Harden your network security

Nipper solutions are designed to strengthen foundational network security and support your evolution in preemptive cybersecurity through Zero Trust, Continuous Threat Exposure Management (CTEM), and Attack Path Mapping (APM) automation.

Key capabilities:

Compliance automation	Map configurations to industry compliance frameworks (e.g., PCI DSS 4.0, NIST SP 800-53, CMMC, DISA STIGs) to reduce audit times by 80%.
Built-in rating system	Focus resources on critical findings by considering network impact, exploitation difficulty, and remediation effort.
Risk-rated remediation guidance	Includes device-specific CLI commands to reduce time-to-fix.
Automated Attack Path Mapping (APM)	Maps configurations and known CVEs to specific MITRE ATT&CK tactics, techniques, and protocols (TTPs).
Filtering Complexity analysis	Identifies firewall rule conflicts, overlapping rules, and unused objects that create unintended access paths undetectable by vulnerability scanners.

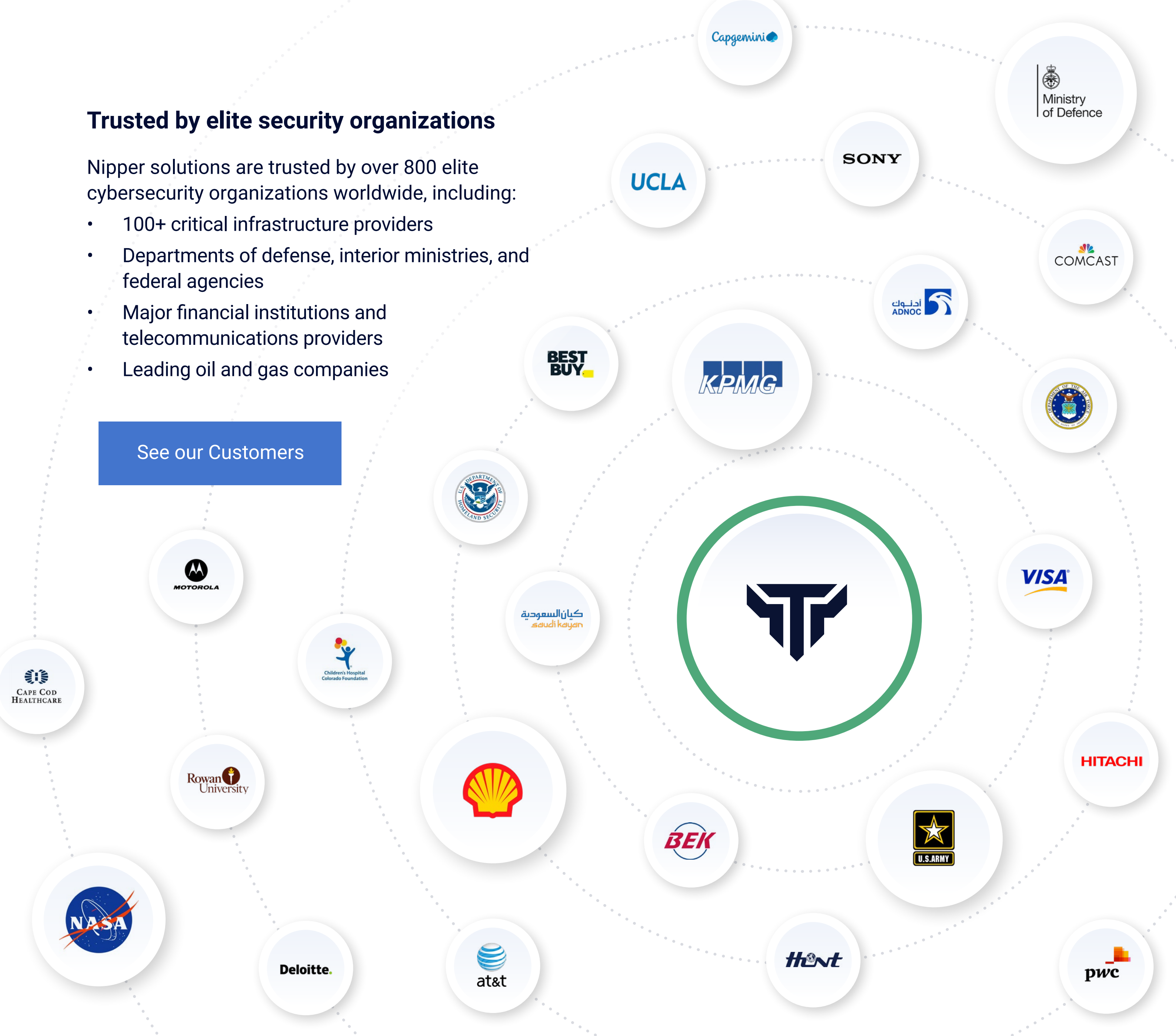
Nipper operates offline, enabling use in classified, sovereign, or highly regulated environments where Internet access is restricted. With assessments performed offline, there's no impact on network operational bandwidth.

Trusted by elite security organizations

Nipper solutions are trusted by over 800 elite cybersecurity organizations worldwide, including:

- 100+ critical infrastructure providers
- Departments of defense, interior ministries, and federal agencies
- Major financial institutions and telecommunications providers
- Leading oil and gas companies

See our Customers



TITANIA

Ready to close your network exposure gaps?

Connect with Titania to learn how to strengthen your foundational network security and evolve your preemptive cybersecurity strategy

Connect with us

titania.com