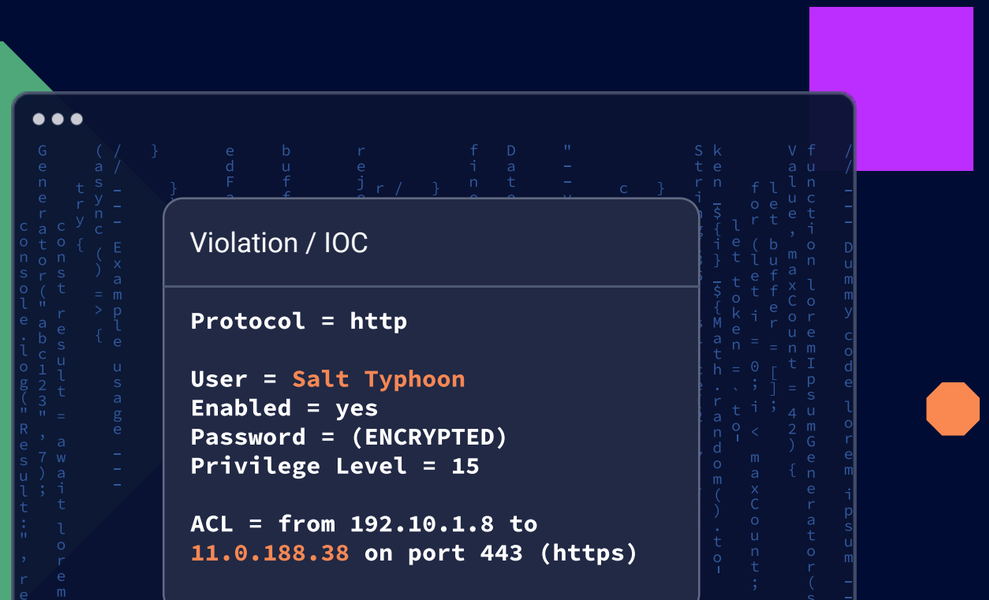
TITANIA | Use case titania.com

How to limit lateral movement with network segmentation and access control

Lateral movement inside the network is now one of the biggest risks

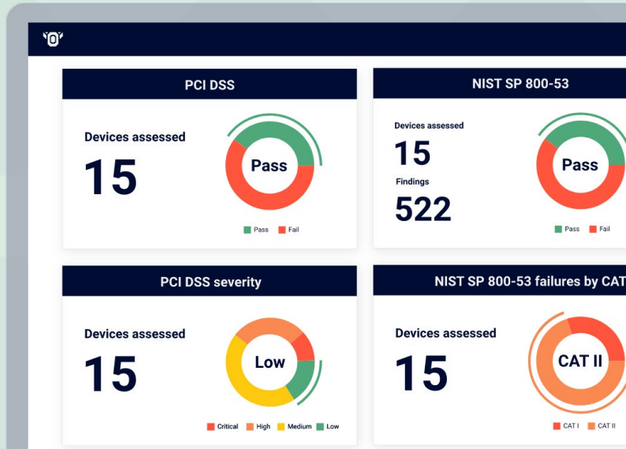
The emergence of advanced persistent threats (APTs) like Salt Typhoon – which targeted telecom, government and military networks across the US, UK, Australia, Canada and other allied nations – signaled a new approach to cyber attacks.

Instead of focusing on short-term gain, adversaries are seeking to quietly penetrate the weakest links in defenses. Then, they will move laterally within the network to reach key targets, whether to exfiltrate data or cause significant operational disruption. To help constrain this lateral movement, organizations need to adopt segmentation, supported by robust access controls. Together, these approaches help contain attacks around the point of breach.



NIPPER OmniSight can help by:

- **Identifying the routes attackers can currently use to reach key assets like Operational Technology (OT)**
- **Informing risk-based decision-making about where to segment and what access controls to adopt**
- **Confirming whether your segmentation and access policies are being enforced correctly across your entire network**
- **Pinpointing weak spots, from misconfigured devices to conflicting access rules, that could undermine segmentation**
- **Enabling continuous monitoring of changes to network access, in line with Zero Trust principles.**



Why limiting lateral movement is vital

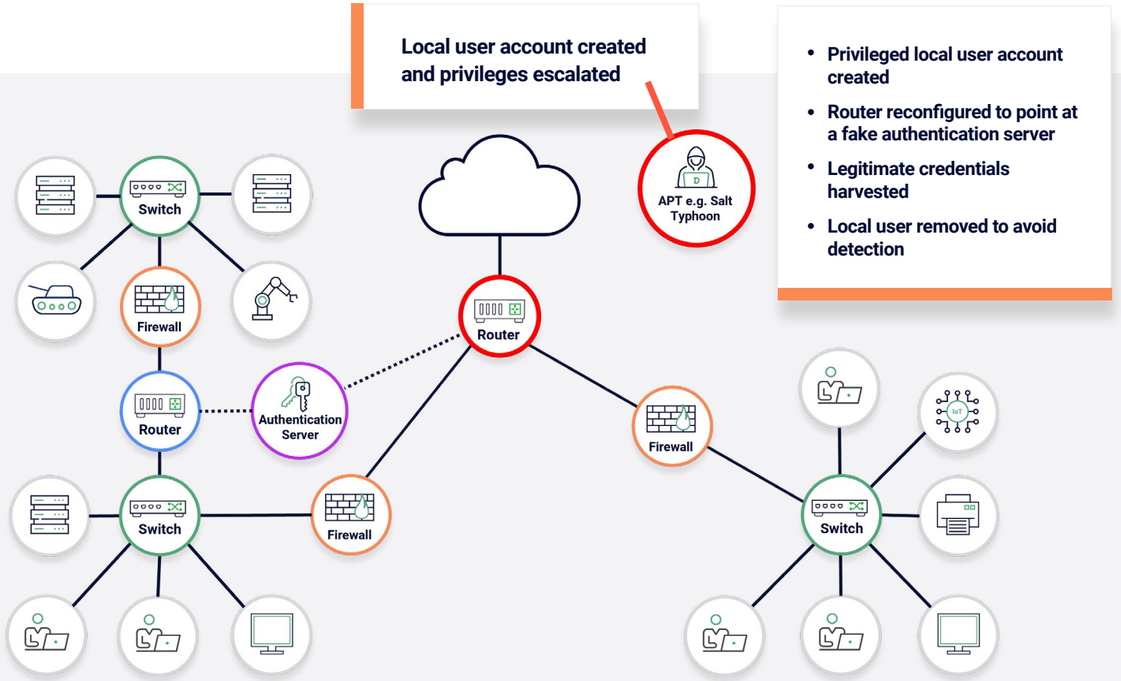
Perimeter defense is now a race against attackers. With automated scanning powered by AI, the attackers are winning.

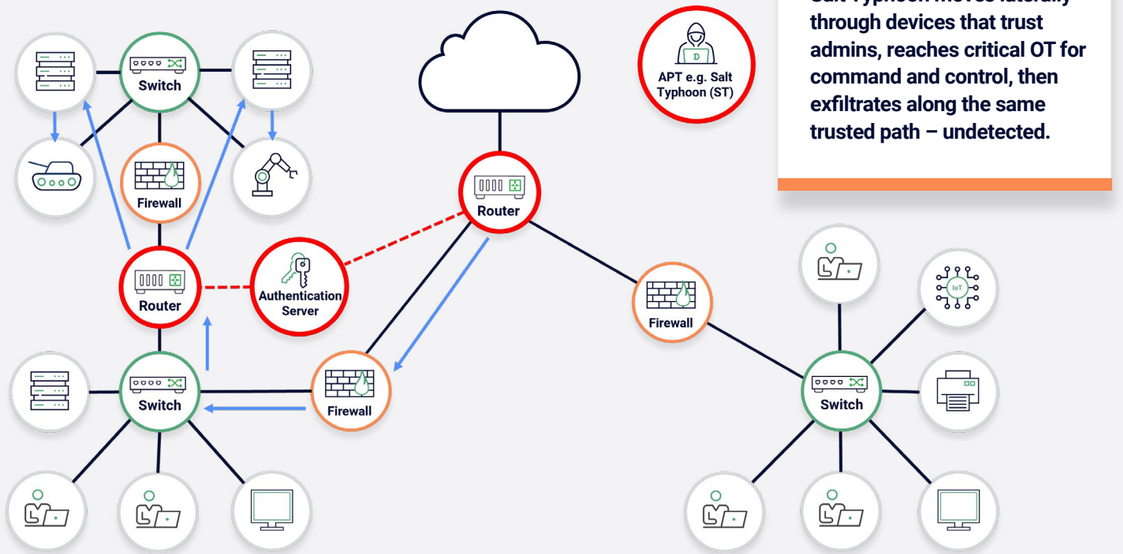
These technologies enable them to find vulnerabilities in network devices, such as default passwords, open ports and insecure admin interfaces at speed: far faster than security teams, responsible for hundreds or thousands of devices and endpoints, can patch and harden device configurations. As a result, the risks of them breaching the network are far higher than ever before.

That's where the real damage can be done.

Once on the inside, APTs can stay undetected for long periods of time, as Salt Typhoon and Volt Typhoon both proved across multiple allied nations. And then they can move laterally, gradually accessing large volumes of data, from customer information to intellectual property. They can secure additional access rights or even administrator privileges, allowing them to take control, compromise or even shut down essential systems.

Organizations in all sectors – but particularly those responsible for critical infrastructure, defense, financial services and global manufacturing or distribution – know they need new ways to help constrain this kind of lateral movement. Limiting it effectively doesn't just protect data from being exfiltrated but also protects everyday operations: you need to know that the right users are able to access the right systems to do their jobs.





The core defense: segmentation…

The main strategic defense organizations can apply to constrain lateral movement is segmentation: dividing the overall network into specific sections typically around key systems, locations or user groups, then putting in place security controls that limit the traffic flow between segments.

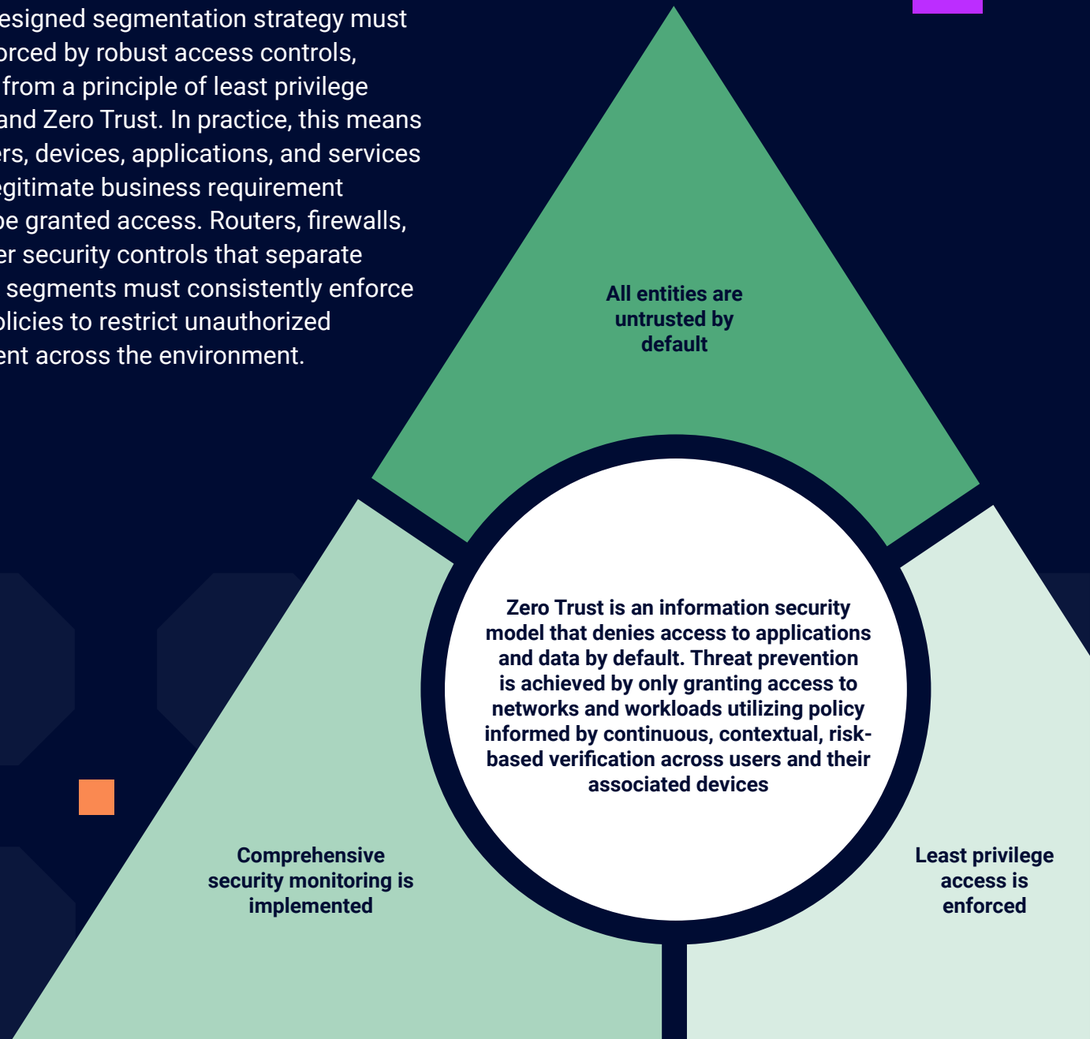
Sometimes, there can even be a demilitarized zone (DMZ) between internal networks and publicly accessible servers (e.g., web, email, and DNS servers), increasing the separation.

This approach effectively closes off routes to key assets such as OT, cyber physical systems and sensitive customer or financial data, with only authorized users, devices and services granted permission. So even when an attacker breaches an external-facing device, their routes to the key assets are limited, or even fully blocked.

The value of segmentation is demonstrated by the fact that regulators increasingly view it as a key compliance requirement. For example, the ISA/IEC 62443 standard – the international benchmark for OT and Industrial Control Systems security – includes a DMZ as a foundational requirement for separating IT networks from OT environments.

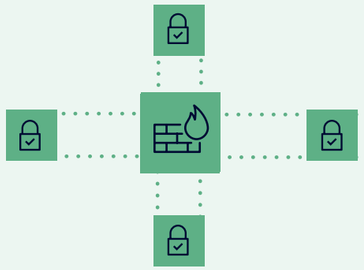
… supported by access controls

A well-designed segmentation strategy must be reinforced by robust access controls, starting from a principle of least privilege access and Zero Trust. In practice, this means only users, devices, applications, and services with a legitimate business requirement should be granted access. Routers, firewalls, and other security controls that separate network segments must consistently enforce these policies to restrict unauthorized movement across the environment.

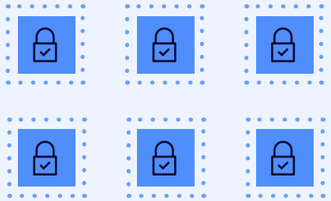


Macro and microsegmentation

There are two different approaches to segmentation:



Macrosegmentation divides the network into sub-networks, where everything within that segment is inaccessible to unauthorized users. It's the equivalent of creating secure corridors in a building; unauthorized users can see the corridor exists but can't see what rooms are inside it.



Microsegmentation involves additional authentication to access specific assets. Using the same analogy, it's putting locks on the doors of each room. The problem is that anyone with access to the building can find exactly where a specific room is, then focus on breaking that lock.

The ideal is to combine both, to provide defense in depth. Macrosegmentation is a higher-impact first step, closing off access to key assets faster. However, it can seem more difficult because it requires deeper analysis of risk and potentially investment in additional devices and security measures.

The challenges around segmentation

There are three fundamental challenges around effective segmentation:

Determining how to segment the network: what is the most effective way to split the overall network, without affecting performance?

Adopting strict access policies: how do you persuade leaders to introduce controls that may remove access rights to key applications and systems, including for leaders themselves?

Ensuring that the organization's policies are being correctly enforced: how do you monitor whether routers and firewalls are functioning as intended, to check they haven't been compromised by bad actors or bad practice?

This latter challenge applies to organizations that have already adopted segmentation, as well as those just starting on their journey.

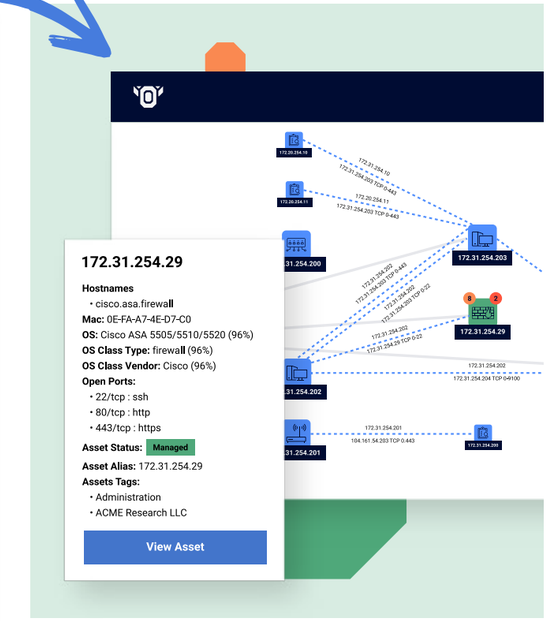
How Nipper OmniSight can help

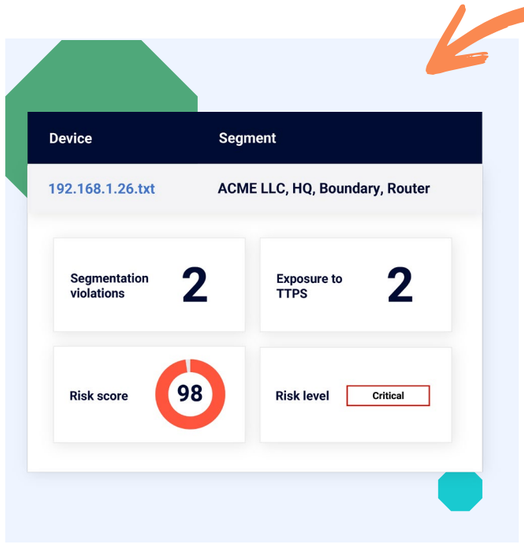
Nipper OmniSight uses configuration files to build a behaviorally accurate model of each device on your network. It then runs configuration-led checks across 180+ device types from 20+ vendors to pinpoint misconfigurations and control gaps. And it does so fast. Nipper OmniSight (Continuous) can assess up to 250,000 devices within 24 hours against known threats (such as MITRE ATT&CK TTPs) to build a network-wide view of risk.

Based on this core assessment, Nipper OmniSight can:

Inform macrosegmentation strategy with attack path mapping.

Using read-only configuration collection and offline analysis, Nipper OmniSight can map internet-facing exposures, so you can visualize exactly how adversaries could move laterally across your network to reach key assets. It also allows you to model the impact of different segmentation approaches, so you can make informed decisions about the most effective and/or least disruptive strategies.



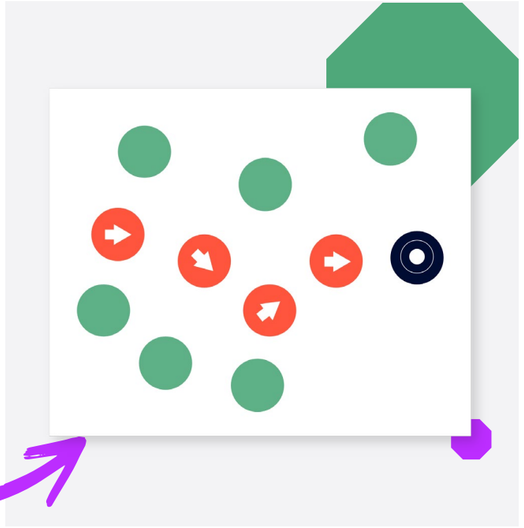


Risk-score and rank exposures to demonstrate the need for robust controls.

Nipper OmniSight provides a risk assessment for each exposure it identifies, based on exploitability and potential impact. Reports then rank the exposures from highest risk first, helping you prioritize remediation, but also providing independent evidence of the need for implementing strict access policies.

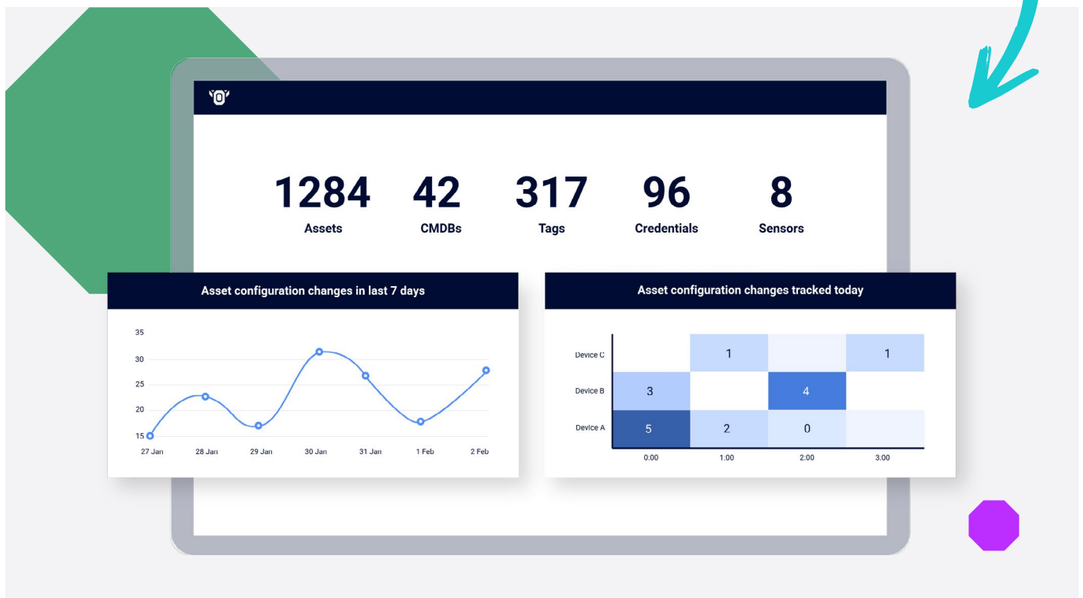
Validate whether devices are enforcing segmentation and access policies correctly.

The analysis, which requires no scanning or live device interaction, compares how routers, switches, and firewalls are managing traffic and access with what the policies state they should be doing, to spot any gaps or conflicts. Where issues are found, you get clear alerts and remediation guidance, so you can promptly resolve them.



Monitor policy adherence, alerting you to any configuration drift.

Routine day-to-day changes across your network, such as user access requests and firewall rule sprawl, can undermine the integrity of your segmentation and quietly reopen paths between segments. Use Nipper OmniSight (Standalone) on a regular basis to check devices are still adhering to the policies and validate any intentional changes against segment-by-segment allow lists. Or, for organizations facing the most severe threats, adopt Nipper OmniSight (Continuous) to monitor networks 24x7 and alert you to every device configuration change: users, rules, permissions.



About Nipper OmniSight

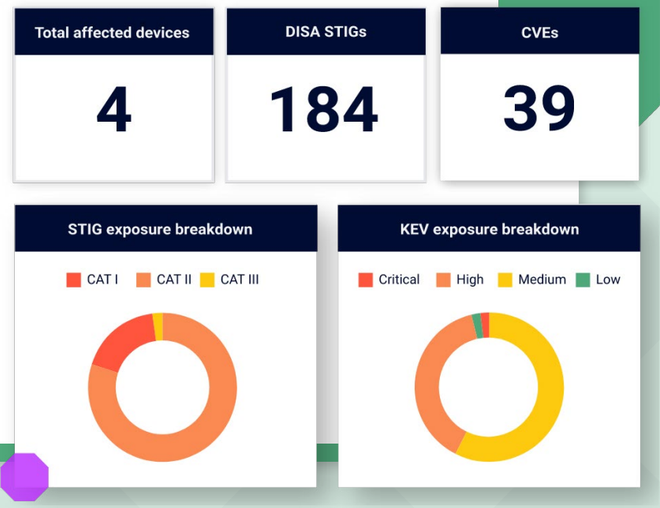
Nipper OmniSight is Titania's enterprise-scale configuration assessment solution, built for validating segmentation, least-privilege access, and exposure reduction across complex networks.

It analyzes device configurations directly – without agents, live network scanning, or cloud access – enabling safe assessment in air-gapped, on-premises or virtual private cloud (VPC) environments.

Nipper OmniSight (Standalone) delivers scheduled, repeatable assessments across more than 200 devices without requiring a Configuration Management Database (CMDB).

Nipper OmniSight (Integrated) adds CMDB or configuration storage ingestion and Security Information and Event Management (SIEM) workflow integrations to automate assessment orchestration across distributed environments.

Nipper OmniSight (Continuous) provides real-time configuration monitoring, supporting assessment of up to 250,000 devices within 24 hours – helping teams detect drift, validate Zero Trust segmentation, and limit unauthorized lateral movement as networks change.



Titania secures the networks society depends on by finding what adversaries exploit and defenders can’t see.

Our Nipper solutions – Nipper InfraSight and Nipper OmniSight – analyze router, switch, firewall and wireless access point configurations, with expanding coverage for SD-WAN and software-defined network (SDN) environments, to reveal hidden exposure, without scanning the live network, installing agents, or sending data to the cloud. This makes it possible to safely assess sensitive and air-gapped networks without disrupting production systems, and to help teams harden devices, prove compliance, validate segmentation, and prepare for audits faster.

More than 700 organizations trust Nipper technology, including 30+ US federal agencies and 100+ critical infrastructure providers, spanning sectors such as defense, financial services and manufacturing.

700+

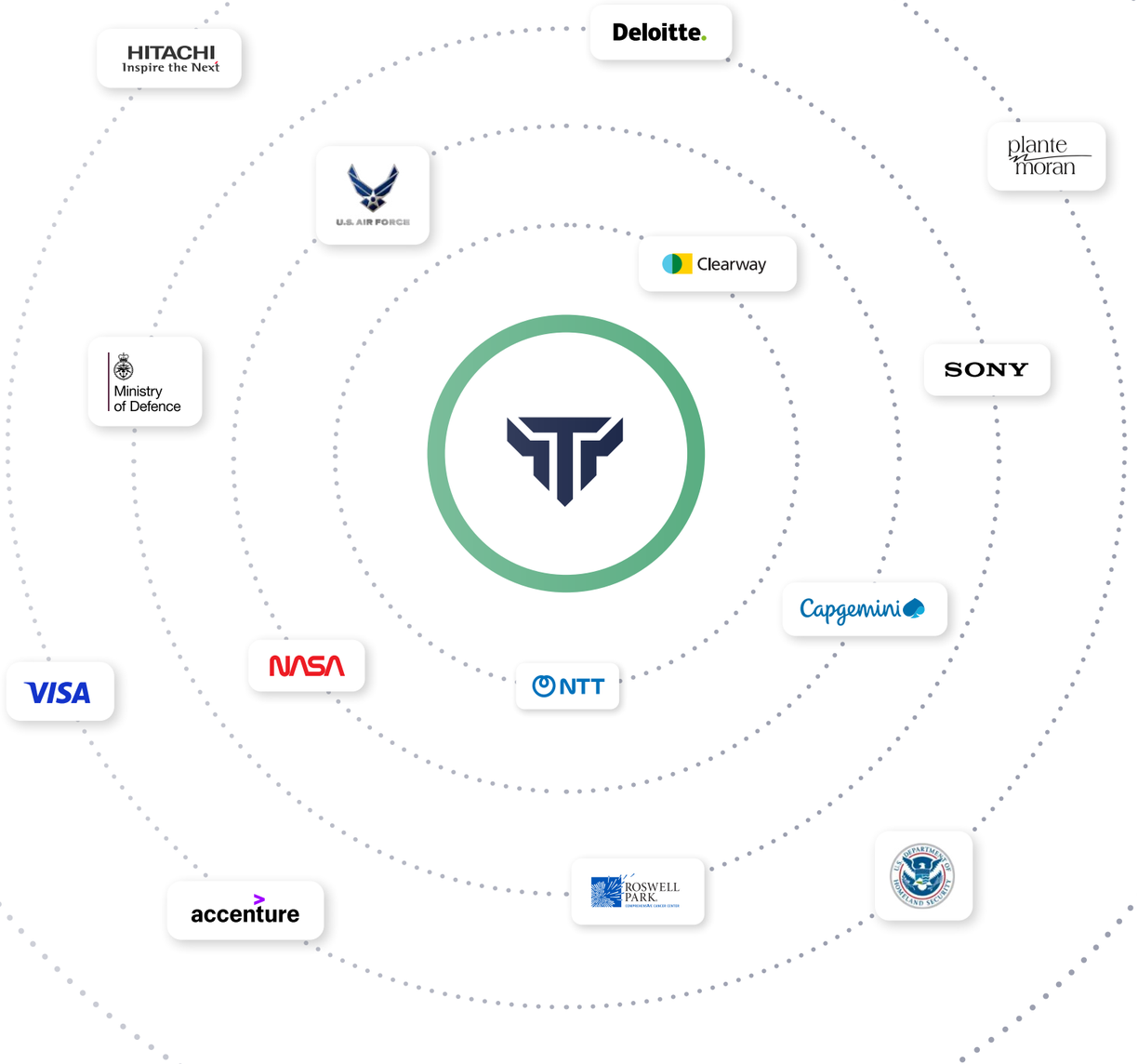
organizations trust Nipper technology

30+

US federal agency customers

100+

critical infrastructure providers



Seeing is believing

Based on technology used by more than 100 elite cyber teams across critical infrastructure, defense, financial services and manufacturing, Nipper OmniSight can be a crucial ally in the fight against APTs.

We'd love to show you how it can underpin your segmentation strategy and help constrain lateral movement on your network.

To arrange a demo, or speak to one of our experts

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

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

titania.com/try/demo