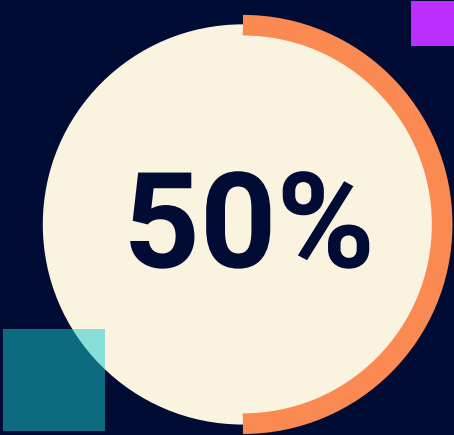


How Nipper InfraSight cuts firewall review time by up to 50%

A global professional services Firm uses Nipper InfraSight and Nipper OmniSight to accelerate firewall security assessments



50%

A global professional services Firm has put Nipper solutions at the heart of its highly respected firewall assessment service. It has used Nipper InfraSight for several years to automate the initial analysis – enabling the Firm to deliver detailed reports to its customers at speed. It estimates Nipper InfraSight reduces the review effort by

approximately half compared with a fully manual review.

Now, it is introducing Nipper OmniSight to support more frequent assessments, reflecting the increased pace of change in the cyber threat landscape and expanding the potential customer base.

At a glance: how Nipper solutions support the Firm

- ✓ **Reduces the time to conduct a firewall review by up to 50%** compared to doing it manually
- ✓ **Delivers consistent, reliable analysis of devices from major vendors** including Palo Alto Networks, Fortinet, WatchGuard and Cisco
- ✓ **Accelerates assessment of compliance against key regulatory frameworks** including CMMC and PCI DSS
- ✓ **Frees up consultants' time to focus on adding value to customers**, through enhanced reporting that reflects the customers' needs
- ✓ **Enables the Firm to offer the service at an attractive price-point** for growing organizations.
- ✓ **Provides the foundation for new more regular assessment services** such as monthly security posture reviews, using Nipper OmniSight (Standalone).

The client: the Cybersecurity Consulting practice of a specialist advisory Firm

Over 60 years ago, the Firm expanded from its heritage in financial advisory services to become a broader consulting Firm.

It is trusted by its customers – primarily growing organizations across the United States – to offer an independent, expert view on key strategic and specialist issues. So, it was a logical step to add cybersecurity consulting to its portfolio of services in 1996.

How Nipper InfraSight powers firewall security assessments

Some of the most in-demand services the Firm provides are firewall configuration reviews and network security assessments, as its customers recognize the need to validate the robustness of their network's "front door". The emergence of AI-enabled threats has magnified the risk and led to greater awareness of the need to ensure that network devices are themselves protected and that they are correctly enforcing access controls.

Increasingly, the impetus for this is coming from C-level executives, underlining the shift in the way cyber breaches are now viewed, from purely a technological risk to a substantial business one.

Today, the Cybersecurity Consulting group provides security assessments, firewall and network architecture reviews, penetration testing, cloud security services, and compliance-related assessments. Though it supports customers across all sectors, a significant portion of its current workload is for financial institutions.



But in-depth analysis of firewall configuration takes time: as rules have been added over the years and short-term policies incorporated to address specific needs, the complexity of the code grows.

Examining this manually is a major challenge, even for security experts; multiply that by the number of devices on a growing organization's business network, and the task very quickly becomes too great to deliver. It would also become a very high professional services cost.

Automating firewall configuration analysis with Nipper InfraSight

The Firm has used Nipper InfraSight for several years to speed up analysis without compromising accuracy or consistency, having concluded that no other option matches it on accuracy, speed and usability

It works like this: customers provide configuration files for all their firewalls, whether from the same vendor or multiple providers, to the Cybersecurity Consulting team. One of the team then uploads these to Nipper InfraSight, running on air-gapped machines in its own environment. This offline access is a major benefit from the Firm's perspective, because it eliminates the risk of affecting customer network performance and provides a secure environment for analysis.

Nipper InfraSight analyzes the configuration file against the latest best practice and vendor hardening advice, checking the firewall has been patched to recommended standards and whether it is operating in line with business rules.

"Nipper InfraSight excels at vulnerability tracking," confirms a Manager within the Cybersecurity Consulting team. "It is extremely accurate and provides details from the vendor website to confirm compliance with latest releases or pinpoint anything that has not been done."

Turning Nipper InfraSight analysis into customer-ready reports

The team members then review the report from Nipper InfraSight, add or apply customer context where relevant, and produce their own report that frames the findings in the best way for each customer organization.

These reports are typically delivered around a week from the initial upload of configuration files; the team commits to a timeline in advance. They include clear descriptions of the different risks and vulnerabilities found, prioritizing the most urgent, and guidance – often drawn from the Nipper InfraSight report – around how to address them.

Reflecting the C-level interest, the Firm ensures each report begins with a short executive summary that covers the overall assessment and the biggest risks, explaining in non-technical terms why these are problematic and how they can be resolved.



The screenshot displays the Nipper InfraSight interface. At the top, it says "Nipper InfraSight Best practice security". Below this is a summary table with columns: Device, Name, Findings, and Highest rating. The data row shows "Firewall", "Titania.ASA.device", "25", and "Critical". Below the summary table is a detailed findings table with columns: (empty), Low, Medium, High, and Critical. The data rows are: Trivial (2, 3, 2, 2), Easy (0, 2, 2, 0), Moderate (1, 0, 3, 1), and Challenging (1, 0, 1, 1). The cells are color-coded: green for Low, yellow for Medium, orange for High, and red for Critical.

Device	Name	Findings	Highest rating
Firewall	Titania.ASA.device	25	Critical

	Low	Medium	High	Critical
Trivial	2	3	2	2
Easy	0	2	2	0
Moderate	1	0	3	1
Challenging	1	0	1	1

The Nipper technology advantage: fast, accurate, reliable analysis

Nipper InfraSight is integral to the process. “Its depth of checks, broad vendor support, vulnerability and CVE analysis, compliance-related information, reporting structure, and repeatable analysis give our consultants the key insights, while allowing us to retain control of the final conclusions,” a Senior Manager says.

Crucially, it provides these reliable findings across firewalls from almost all major vendors (following the recent addition of Meraki) at speed: far faster than the team could operate if it had to analyze configuration files manually.

“We estimate that Nipper InfraSight can reduce our review effort by approximately half compared with a fully manual review,” the Senior Manager confirms. “Because it automates a significant portion of the initial review and applies consistent analysis across technologies, Nipper InfraSight reduces repetitive work and gives our consultants more time for validation, higher-risk investigation, and remediation guidance.”

The team is acutely aware of how pivotal Nipper InfraSight is to the commercial aspects of the offer. “Nipper InfraSight enables us to provide the analysis at a price point our customers are comfortable with, and to deliver at a speed fast enough for the business to back the service,” the Senior Manager adds.

The team currently conducts around 25-35 firewall assessments a year, and its recommendations are highly valued by its customers. Sometimes, the Client can apply the same recommendations to similar firewalls beyond the original scope. The analysis also identifies unnecessary rules or open ports that were configured and later forgotten, or local device settings that have been overlooked.

These high-quality insights lead most customers to agree to a review cycle, where the firewalls are fully reassessed on a scheduled basis: typically every year for higher risk organizations, or every three years.

“Nipper InfraSight reduces repetitive work and gives our consultants more time for validation, higher-risk investigation, and remediation guidance.”

Offline analysis: a unique feature of Nipper solutions

One of the most important factors for the professional services Firm is that Nipper solutions operate offline, with no need to link to its customer networks. Instead, team members upload the relevant configuration files into an air-gapped environment. This has multiple benefits: it is more secure, with no external access to the customer device data. It means there's no impact on the customer networks. And it gives the team full control of the analysis process.

The Senior Manager recalls: "When I joined the Firm, I was invited to review the service and look at whether other tools could be more effective. I examined a range of options but concluded very quickly that Nipper InfraSight was the best for us: as well as providing swift, reliable analysis, it was already safely installed in an air-gapped environment that cut out risks."

The next steps: expanding the offer with Nipper OmniSight

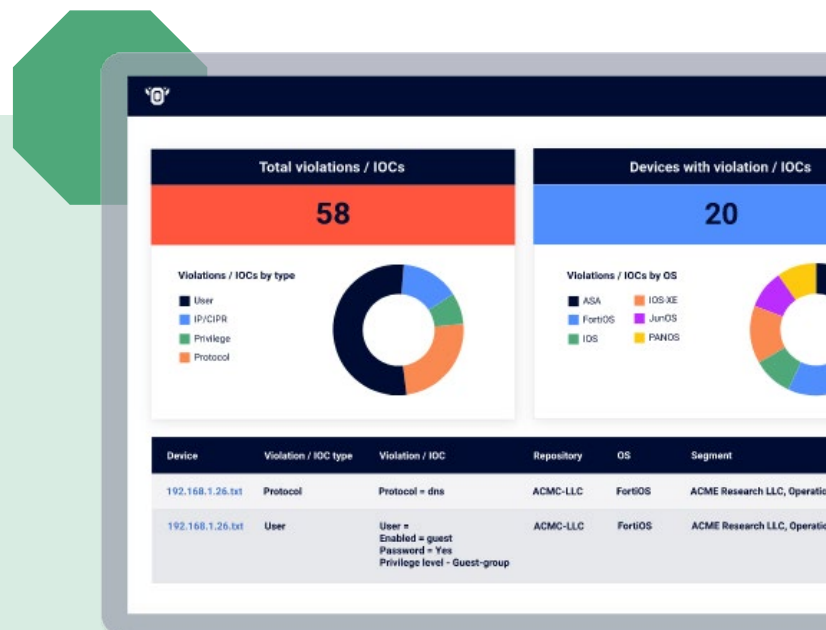
With regulators focusing more closely on networks, the Firm is now also increasingly using Nipper InfraSight as a tool to support CMMC and PCI compliance reviews, confirming that network devices are correctly configured and enforcing relevant policies.

But the team sees even greater potential from the adoption of Titania's exposure management platform, Nipper OmniSight, which will allow it to scale up the existing analysis, deliver faster and underpin new service offerings.

Nipper OmniSight offers bulk import of configuration files, automated report execution and a dashboard providing executive insights and trends over time. "We like the advanced dashboard, that offers an alternative to the output files," the Manager

continues. "As well as visualizing trends, it allows easy drill down to find the exact issue and its remediation. We're looking forward to using Nipper OmniSight on a regular basis for more customers."

One further advantage is how quickly Nipper OmniSight compares configuration files pre-assessment and post-remediation, giving customers the assurance that the steps they have taken have improved their cybersecurity posture



Nipper OmniSight enables monthly cybersecurity posture reviews

The ability to scale up assessments without sacrificing speed also offers a new opportunity. “We’ve been using Nipper InfraSight for point-in-time reviews, but Nipper OmniSight allows us to automate the process,” the Manager notes. “That means we can offer a more frequent service: a monthly touchpoint looking at current cyber posture.”

The option of a more frequent assessment against the latest CVEs is an advantage for larger organizations, who are being challenged by regulators to move to more regular monitoring.

However, the team sees a major opportunity to offer a new service for smaller organizations with less IT staff. The rapid posture check through Nipper OmniSight will identify priority issues for them to tackle that month or quarter; that in turn enables them to deliver continuous improvement of their cybersecurity, without overwhelming them with huge numbers of tasks.

Titania and the Firm’s partnership: ongoing product support and collaboration

The Firm will be one of the first to use Nipper OmniSight commercially, a testament to its trust in Titania’s solutions and support. The Senior Manager comments: “We have a great partnership. Titania has supported us through product demonstrations, technical enablement, responsive support, product discussions, and assistance with questions or issues.”

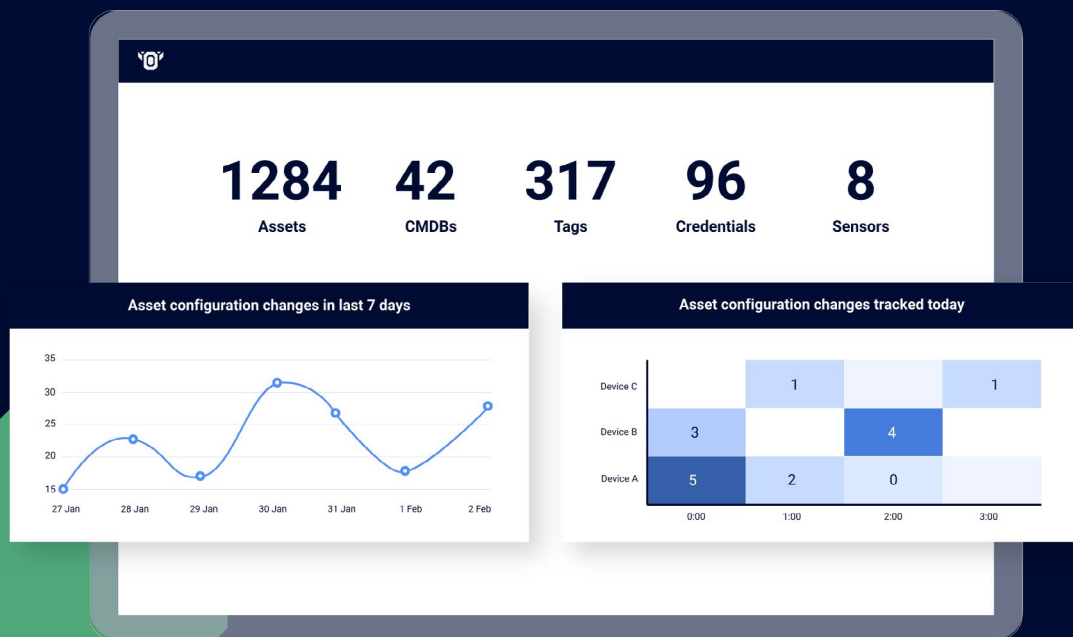
That collaboration has led to several new capabilities within Nipper solutions, reflecting Titania’s understanding of the Firm’s needs – and it’s why Nipper remains central to how the Firm delivers cybersecurity assurance to its customers.

“We have a great partnership. Titania has supported us through product demonstrations, technical enablement, responsive support, product discussions, and assistance with questions or issues.”

Senior Manager, Cybersecurity Consulting

Find out how you can accelerate and automate configuration analysis.

Contact us



Learn more about Nipper solutions

Vulnerability management with Nipper InfraSight

[Learn more](#)

Network configuration and change monitoring with Nipper OmniSight

[Learn more](#)

Put Nipper solutions at the heart of your cyber consulting and managed security service provision.

[Find out more about partnering with 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