Brought to you by Informa Tech
OMDIA

Publication date:
20 Jul 2022
Author:
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: Titania assesses config on switches, routers, and firewalls for security, compliance

Summary

Catalyst

Titania develops and markets technology that assesses the configuration of network elements (switches and routers) and firewalls from both a vulnerability management and a compliance perspective. Its flagship product is Nipper Enterprise, which is designed to build on the success of the formerly open source Nipper technology, created by the company's founder.

Omdia view

There is a marked growth in proactive technologies on offer in the cybersecurity market as even the most advanced reactive technologies in the extended detection and response (XDR) spectrum face challenges scaling to address all the threats now coming at organizations.

Vulnerability management and, in particular, its more evolved variants should be in the forefront of this trend, and Titania's ability to cover both network elements and firewalls represents a nice complement to the more conventional scanner technologies, which focus on servers.

Why put Titania on your radar?

Titania adds a level of proactive vulnerability management / risk assessment, focused on network elements and firewalls, which can nicely complement the kind of server-centric vulnerability assessment enabled by the likes of Qualys and Tenable. Its ability to integrate with the leading security information and event

management (SIEM) and security orchestration, automation, and response (SOAR) products, in addition to IT service management (ITSM) platforms, for remedial action will be particularly welcome.

Market context

Vulnerability management is a venerable segment of the security market, with its foremost proponents dating from around the turn of the millennium (Qualys was founded in 1999, Rapid7 in 2000, and Tenable in 2002). In that time it has gone through considerable evolution and generational change, and today it sits alongside a wave of other proactive security technologies emerging to complement the reactive approaches of detection and response (EDR, NDR, XDR, etc.) that have held sway in the market for the last decade.

The first generation of vulnerability management/assessment platforms centered around scanners, technology that inspected the servers on which applications and databases resided to detect vulnerabilities. These might be the result of misconfiguration or code that was in the app when it first shipped but had subsequently been found to be susceptible to cyberattack (a recent example would be the likes of Log4j). The scanners would compile a list of all the vulnerabilities found in an organization's environment, enabling security teams to address them as they saw fit.

However, as application infrastructures mushroomed thanks to cloud adoption, vulnerability management customers began to face the challenge of scale: scanners drew up ever-longer Excel spreadsheets of vulnerabilities, and resource-constrained SecOps teams then had to decide which of the many issues on them to address first. Which were the most critical, and which could comfortably be left unpatched or without remediation for the time being?

Thus a second generation of vendors arose to deliver the prioritization of vulnerabilities that has become a key requirement. RiskSense was founded in 2006, while both Kenna and Brinqa were founded in 2009. They prioritized vulnerabilities based on

- Their knowledge of the current threat landscape (i.e., which vulnerabilities were being weaponized at that time)
- Their understanding of how their customers' infrastructure worked: where the most sensitive and confidential information resided, and which systems had access to the greatest number of others

To achieve this, they used predictive modeling, machine learning, and expert analysis. Two of these vendors were acquired in 2021: Kenna by Cisco in June and RiskSense by Ivanti in August.

However, the server-centric view of the world shared by both the first and second generations of vulnerability management is now itself considered insufficient. Firewall management vendors such as Firemon, Tufin (recently taken private for $570m by Turn/River), and AlgoSec proclaim the importance of performing similar optimization on these core security assets. Meanwhile, Titania adds switches and routers to the mix.

Product/service overview

Nipper Enterprise's approach to security and compliance assurance is an "inside out" one, which can operate in one of two ways. The customer either provides it with the configuration file for all network elements (switches, routers, and firewalls) for it to audit or gives the platform permission to pull the

configuration data off the network elements in a secure fashion and without leaving any trace on the device. It then produces a virtual model and recommends actions, based on best practices, to harden the device's security posture.

This is done automatically, with Titania layering on top its pentesting expertise to gauge the exploitability of a given misconfiguration and thus the risk it represents to an organization, that is, how likely that misconfiguration is to be exploited. It then proceeds to offer remediation advice, complete with an assessment of how easy that misconfiguration should be to fix.

Nipper Enterprise fits within the parameters of the US federal government's Continuous Diagnostics and Mitigation (CDM) program, launched in 2012 to help federal agencies improve cybersecurity and provide visibility across the federal government. The program delivers cybersecurity tools, integration services, and dashboards that help participating agencies improve their security posture by

- Reducing agency threat surface
- Increasing visibility into the federal cybersecurity posture
- Improving federal cybersecurity response capabilities
- Streamlining Federal Information Security Modernization Act (FISMA) reporting

In addition, Titania notes that the Zero Trust Framework of the US Department of Defense (DoD), which was issued in February 2021, establishes three criteria for gauging how well a defense contractor is implementing zero trust, and Nipper Enterprise enables companies to assess two of them on a daily basis.

The Enterprise platform is designed to be overlaid on whatever framework a customer is using to deliver accurate and timely risk prioritization, together with recommendations for how to remediate.

Compliance

The program enables federal agencies to meet key compliance requirements such as the payments industry's PCI DSS and to achieve Cybersecurity Maturity Model Certification (CMMC), which is a unified standard for the DoD for implementing cybersecurity across the defense industrial base and includes more than 300,000 companies in the supply chain.

Nipper is mainly deployed on customers' premises, typically running on the laptop of a security or compliance professional who runs the program. Nipper Enterprise, on the other hand, is licensed software that runs as a horizontally scalable web application that extracts data, either from a configuration management database (CMDB) or from the devices themselves in continuous mode. It integrates with any privileged access management (PAM) platform operating within a customer's environment to enable secure access to the device on a daily basis.

Use cases

Nipper Enterprise gives security operations centers a snapshot, prioritized for risk and remediation, of the security and compliance posture of every firewall, switch, and router in a CMDB on a monthly basis or at a more frequent cadence as required.

For network operations centers, Nipper Enterprise can check the CMDB for file changes and automatically trigger an audit of those changed configurations. It provides a proactive way to assess for configuration drift as it occurs, without the need for direct, credentialed device access, thereby delivering foundational zero-trust capabilities.

Company information

Background

Titania was founded in 2009 by Ian Whiting, a former pentester who remains on the board of the company. Its current CEO is Phil Lewis, previously CEO of Telesoft, a vendor of network visibility technology.

The vendor raised an initial £2.5m ($3.1m) in a private equity funding round from the Foresight Group in January 2021.

Current position

The original Nipper technology was open source software whose initial raison d'être was to automate pentesting. After some 30,000 downloads of the product, it was retired in 2011 to make way for the commercial version of Nipper, which focuses on providing on-demand security and compliance audits and assurances. Nipper Enterprise was launched into the defense sector in September 2021 and is now on general availability for all commercial customers.

The platform's remit has expanded to offering continuous, on-demand security and compliance audits and assurance, checking the configuration of core network elements (switches, routers, and firewalls) both for software vulnerabilities that require patching and for misconfigurations that should be remediated, with its primary focus being on the latter.

Titania currently has 600–700 customers using Nipper, including the US DoD. Aside from organizations in the critical national infrastructure (CNI) segment, the vendor also targets high-end customers with large and complex networks. This typically means enterprises with more than 5,000 employees, since that level of user base indicates a large and complex corporate network. It also sells into systems integrators and private contractors and some specialist pentesting companies that serve small and medium-sized businesses.

In terms of its competitive landscape, Titania acknowledges that the likes of vulnerability management vendors Tenable and Qualys are in the same market segment, but both those companies started from a scanning perspective. This is an "outside in" approach, pinging messages at the network and awaiting a response, whereas Nipper works outward from the inside and as such it can be and often is used in collaboration with those scanning tools.

Titania also points out that vendors such as Qualys are often too cloud-focused for many DoD agencies, which tend to operate airgapped networks and be particularly security conscious. Meanwhile, others such as AlgoSec, Tufin, and Firemon focus entirely on the firewall side of the problem, whereas Nipper takes in switch and router data too. A significant differentiator is the fact that Nipper operates continuously on configuration data, whereas many competing products operate by sampling data.

Future plans

The current version of Nipper Enterprise provides detailed remediation instructions for any misconfigurations found, which can be used by network teams to prioritize remediation workflows and expedite fixes based on risk. To make the most of this capability, Titania's roadmap for future versions includes extended integration with ITSM and SOAR systems including ServiceNow, Splunk Phantom, and Cortex XSOAR. Users will be able to visualize and prioritize the risks that Nipper Enterprise finds in those

platforms as they can now but can also orchestrate risk-prioritized plan of actions and milestones (POAM) playbooks to further reduce mean time to remediate.

Titania expects to see an ever-increasing impact from the zero-trust approach to cybersecurity on how its technology is used. Today, Nipper Enterprise provides organizations with a risk-prioritized view of their compliance posture together with a plan of actions to be taken and the milestones against which they can measure their progress. It typically delivers these views monthly or, occasionally, weekly.

However, with zero trust becoming a requirement mandated by the likes of the DoD, it sees both plans of actions and milestones being superseded as organizations move to daily assessments, resulting in a list of high and critical risks for them to work through in real time. Nipper Enterprise will support this with remediation prioritization and automatic mitigation where possible.

Key facts

Table 1: Data sheet: Titania

Product/service name	Nipper Enterprise	**Product classification**	Vulnerability assessment: configuration assessment, risk prioritization, and remediation for firewalls, switches, and routers
Version number	1.0.19	**Release date**	2022
Industries covered	Enterprises with hundreds of firewalls, switches, and routers in their network Customers with critical national infrastructure: military, civilian federal, education, commercial telcos, utilities, and finance	**Geographies covered**	Customers primarily in US and Europe, Middle East & Africa
Relevant company sizes	Enterprise, typically with more than 5,000 employees (because this drives the size of the network)	**Licensing options**	Subscription Snapshot license Continuous license Compliance subscriptions for NIST 800-53, NIST 800-171, PCI, CMMC, and NERC-CIP
URL	www.titania.com/products/nipper-enterprise/	**Routes to market**	Direct, primes, systems integrators, MSSPs, value-added resellers/distributors
Company headquarters	Worcester, UK and Arlington, Virginia, US	**Number of employees**	50–100

Source: Omdia

Analyst comment

While there is a tendency in tech circles to say that the future is the cloud, the reality is that the foreseeable future is hybrid, with some application functionality moving to the cloud while other parts continue to reside on organizations' premises. And of course, in certain highly sensitive areas such as the defense sector, the vast majority of applications may need to remain on premises forever. The same can be said for huge swathes of operational technology in the CNI sector.

This being the case, Titania's technology will be relevant for a very long time. Its ability to work in tandem with the "outside in" technology of mainstream vulnerability management vendors and its focus on network elements and firewalls give it a compelling differentiation in the market.

This situation should guarantee the vendor a relatively free run in the market, since none of the other players in this segment boast its mix of target devices: the scanners look at servers and endpoints, while the firewall management vendors limit themselves to firewalls without extending to network elements, and networking vendors do not offer scanning of heterogeneous switch or router environments.

The challenge Titania faces, in fact, is one of visibility. While open source Nipper is relatively well known in its space, both the company and its Enterprise product are still relatively unknown, and there is a clear need to raise the profile of both in the market. Some of this can be the result of marketing efforts by the vendor itself, while another part can come through partnerships with major players in the tech sector, whether they be other vendors whose platforms can integrate with Nipper Enterprise and benefit from it or channel partners with an interest in taking the product to market.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Blockchain Technology and Adoption Trends (December 2019)

Service Provider Routers & Switches Market Tracker – 4Q19 (February 2020)

"Blockchain is good for more than just Bitcoin" (September 2019)

"CenturyLink goes 'colorless' and takes on the edge cloud" (February 2020)

US Cybersecurity & Infrastructure Security Agency, "Federal Information Security Management Act," available at www.cisa.gov/federal-information-security-modernization-act, retrieved July 2022

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com