

Titania named finalist in the coveted Top InfoSec Innovator Awards 2026

Recognition highlights Titania's approach to preemptive network exposure assessment in the Top InfoSec Innovator Awards, part of the 14th Annual InfoSec Awards



TITANIA

Titania, a global leader in network security and compliance assurance

LAS VEGAS, NV, UNITED STATES,

September 29, 2026 /EINPresswire.com/ -- (CYBERDEFENSEWIRE) – Titania is proud to announce that during BlackHat USA 2026 it was named a finalist in the Top InfoSec Innovator Awards 2026 by Cyber Defense Magazine (CDM), the industry's leading electronic information security magazine.



This recognition reflects what our customers already know: security teams don't need more findings – they need to understand which exposures create a real path to critical systems and data.”

Ian Robinson, Chief Product Officer, Titania

Titania has been named a finalist in two categories: Exposure Assessment Platform for [Nipper OmniSight](#) and [Vulnerability Management](#) for [Nipper InfraSight](#). The recognition recognizes Titania's innovation in helping organizations identify and reduce hidden exposure across complex network infrastructure.

Nipper OmniSight, Titania's enterprise-scale preemptive exposure assessment platform for network infrastructure. Nipper OmniSight directly assesses the configurations of routers, switches, firewalls and other network devices to

identify weaknesses that can create attack paths, undermine segmentation and enable lateral movement – assessing configurations across 180+ device types from 20+ vendors.

Nipper InfraSight brings the same configuration-led approach to vulnerability management, uncovering misconfigurations, ineffective rules and access exceptions that traditional vulnerability tools can miss, and helping teams prioritize the weaknesses that pose the greatest risk.

The recognition comes as organizations rethink how they manage cyber exposure. Traditional vulnerability management has largely focused on identifying vulnerabilities across endpoints, applications and cloud environments. But whether an attacker can reach and exploit those

vulnerabilities often depends on the configuration of the underlying network.

Titania is addressing this gap through the company's preemptive exposure assessment platform, bringing evidence-based assessment to the network devices responsible for enforcing access, segmentation and trust boundaries.

"We're thrilled to be named among this coveted group of finalists in Cyber Defense Magazine's 14th Annual InfoSec Awards. We knew the competition would be tough, with leading InfoSec experts from around the globe judging the entries, so we couldn't be more pleased," said Ian Robinson, Chief Product Officer at Titania. "This recognition reflects what our customers already know: security teams don't need more findings – they need to understand which exposures create a real path to critical systems and data. That's where Nipper technology is different. By directly validating network configurations and the controls they enforce, we provide teams with deterministic evidence of where exposure exists, which instances represent the greatest risk to their organization, and the guidance they need to fix them fast – cutting audit preparation time by up to 80% along the way."

Gary S. Miliefsky, Publisher of Cyber Defense Magazine, said: "Titania embodies three major features we judges look for with the potential to become winners: understanding tomorrow's threats, today, providing a cost-effective solution and innovating in unexpected ways that can help mitigate cyber risk and get one step ahead of the next breach."

Nipper OmniSight uses virtual device modeling and adversary-style assessment to analyze network configurations from the inside out, directly validating the routers, switches and firewalls that control access and segmentation. It is built on established Nipper InfraSight technology and extends this approach to scheduled and continuous enterprise-scale exposure assessment, identifying configuration changes and drift, mapping attack paths and helping teams understand what is reachable, what matters most and where to remediate first.

Because Nipper solutions can assess network infrastructure without agents, live network scanning or sending sensitive configuration data to the cloud, this makes them particularly valuable for government, critical infrastructure and other organizations where networks need to remain secure and operational – a capability already trusted by 100+ critical infrastructure providers and 169 government and defense organizations.

Judging continues through October 2026, where winners will be announced online, in print and during CyberDefenseCon 2026, taking place October 20-21, 2026 at The Ritz-Carlton in Orlando, Florida, USA. A select group of winners will be given the opportunity to showcase their innovative solutions to the Top Global CISOs during their invitation only conference at <https://www.cisoconference.com>.

Beth Fichtel/Cassandra Hegarty
The Hoffman Agency

+1 914-588-2695

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/945764255>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.