carahsoft

TITANIA

.ŜűűŜNJ ¢2ƎŜűKŜNJY l2ø C2NJŜăŎ2dzű l-yŘ ¢ƛűl-yƛl-

5ŜfƛØŜNJ tNJŜπSYLJűƛØŜ ¢KNJŜl·ü 9ËLJ2ădzNJŜ a l·yl·ƎŜYŜyű

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASA SEWP V, ITES-SW2, The Quilt and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Titania, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/TitaniaResources

Join Events & Webinars:
carah.io/TitaniaEvents

Discover Technology Solutions:
carah.io/titania

Learn About Procurement:
carah.io/TitaniaContracts

Connect With Our Team:
Titania@carahsoft.com
(844) 445-5688

TITANIA | FORESCOUT | carahsoft

Better Together: How Forescout and Titania Deliver Pre-emptive Threat Exposure Management

Meet your Comply-to-Connect (C2C), Cyber Operational Readiness Assessment (CORA), and Zero Trust mandates with seamless orchestration across asset visibility, access control, and network device configuration security.

The transition to CORA and Zero Trust has changed the rules for how cyber readiness is assessed across the defense landscape.

Department of Defense (DoD) organizations must move beyond traditional compliance checklists to proactive threat exposure management – identifying and closing the specific vulnerabilities that adversaries are actively exploiting before they can be weaponized. They also need to ensure that their devices are configured to provide insight into their usage, access and configuration changes.

Foundational security gaps

Successful breaches by APT groups like Salt Typhoon and Volt Typhoon demonstrate that network devices are prime targets for establishing persistent access, lateral movement, and data exfiltration.
Yet many organizations have dangerously poor visibility into actual device configurations. As a result, they miss critical vulnerabilities in physical and virtual devices such as firewalls, switches, routers and wireless access points. This creates cascading security failures:

- Zero Trust policies fail when underlying network segmentation is misconfigured
- SIEM alerts become meaningless when network devices themselves are compromised
- Incident response teams lack the foundational data needed to understand lateral movement
- CORA assessments reveal critical Key Indicators of Risk (KIORs) that could have been prevented

The consequences extend beyond technical risk. Organizations failing CORAs face accountability reviews, remediation mandates, and increased likelihood of repeat assessments. More critically, every CORA finding represents an exploitable weakness that adversaries can leverage for initial access, persistence, or privilege escalation.

Delivering defensible architecture

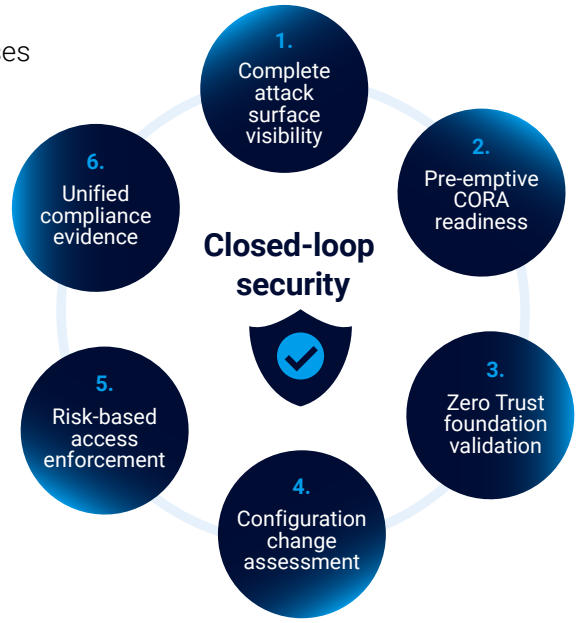
For DoD organizations navigating CORA requirements and Zero Trust implementation, Forescout and Titania provide an integrated solution that delivers the visibility, validation, and automation needed to secure the network foundation before adversaries can exploit it.

Titania Nipper Resilience integrates with Forescout through the eyeExtend Connect module available on the Forescout Marketplace and ensures that the network infrastructure enforcing security policies is itself continuously validated and hardened. This creates a defensible architecture where:

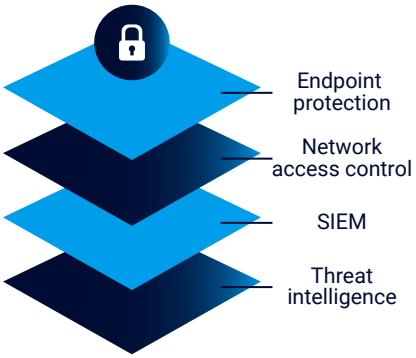
- Adversaries can't leverage network device misconfigurations for initial access
- Lateral movement is blocked by properly configured segmentation
- Security tools receive accurate data from trusted infrastructure
- Zero Trust policies are enforced by validated controls

Closed-loop security

The integration creates a closed-loop security architecture that addresses both endpoint compliance and infrastructure hardening:



- **Complete attack surface visibility** – Forescout continuously discovers all connected assets, including network infrastructure devices. This inventory feeds directly into Nipper Resilience assessment scope, ensuring every network device undergoes configuration validation against DISA STIGs.
- **Pre-emptive CORA readiness** – Nipper Resilience analyzes device configurations against the latest DISA STIGs and maps findings directly to CORA KIORs. This is more than generic vulnerability scanning – it provides threat-specific analysis through MITRE ATT&CK framework alignment that shows exactly how misconfigurations enable adversary tactics.
- **Zero Trust foundation validation** – When Forescout detects unauthorized lateral movement attempts, Nipper Resilience provides the context: which network device configurations allowed that movement.
- **Configuration change assessment** – When Forescout detects a network device configuration change – whether planned maintenance or unauthorized modification – Nipper Resilience assesses the new configuration for security implications.
- **Risk-based access enforcement** – When Nipper Resilience identifies critical misconfigurations or CORA KIORs on network infrastructure devices, Forescout can automatically adjust access controls, restrict traffic flows, or trigger security orchestration workflows until remediation is complete.
- **Unified compliance evidence** – For CORA assessments, Nipper Resilience provides device-specific evidence of STIG compliance and KIOR status, while Forescout delivers continuous posture data across all connected assets. Together, they create the comprehensive security posture documentation required for successful assessments.



Become exponentially more effective

Modern security architecture depends on layered defenses that work together. Endpoint protection, network access control, SIEM, and threat intelligence all play critical roles. But these capabilities become exponentially more effective when the foundational network infrastructure is properly secured.

For organizations operating in the DoD Information Network (DoDIN) or preparing for CORA assessments, the Forescout + Titania combination delivers the foundational visibility and continuous validation required for successful outcomes and improved mission readiness:

- **Unified visibility** – See every device and know its security configuration status in near real time
- **Faster compliance** – Reduce manual audit cycles with automated, continuous validation against STIGs
- **Proactive risk reduction** – Block non-compliant or misconfigured devices before they become attack vectors
- **Operational efficiency** – Minimize manual checks and free personnel for higher-priority security tasks
- **Zero Trust alignment** – Verify device compliance continuously before and during network access

Ready to close your network infrastructure exposure gaps?
Connect with Forescout and Titania to learn how leading defense organizations are achieving preemptive security posture through complementary technology integration.