

PRODUCT OVERVIEW

Automated DISA STIG Compliance for OT Endpoints

OT Security Configuration Assessments and Centralized Tracking for DoD and DIB Organizations

Security Technical Implementation Guides (STIGs) are security configuration guides that translate broader cybersecurity requirements for Department of Defense (DoD) systems into specific, product-level configuration checks, helping DoD components and defense industrial base (DIB) organizations comply with NIST SP 800-53 requirements and provide auditable evidence for DoD Risk Management Framework (RMF) and authorization activities.

While STIGs primarily target IT systems, OT systems that run on IT components are also subject to compliance. The challenge is applying and validating detailed configuration requirements to sensitive OT assets, where limited visibility — let alone access to host-level configuration data — makes IT-centric approaches impractical.

DoD and DIB entities need a safe way to perform OT security configuration assessment (SCAs) at scale and centrally track compliance across distributed environments.

Safe, Scalable OT-native SCAs with Nozomi Arc

Nozomi Arc sensors automate DISA STIG compliance in distributed OT environments by assessing Windows-, Linux- and macOS-based OT endpoint security configurations against benchmarks, consolidating proof of compliance and centrally tracking changes over time either on premises using our central management console or in the cloud with Vantage or Vantage for Government, our FedRAMP® Class C (Moderate) SaaS platform.

Benefits



Automated SCAs comparing configuration evidence collected directly from OT endpoint sensor to imported security benchmarks



Centralized results across assets, benchmarks, policies and individuals check so teams can quickly see where configuration risk exists.



Scalability across distributed OT environments, with support for on-premises deployments and centralized workflows



Proof of compliance across assets and rules, with remediation guidance for failed configuration checks

OT Endpoint Security Configuration Assessment on Par with IT SCAs

Accurate OT Configuration Data with Rule-level Findings

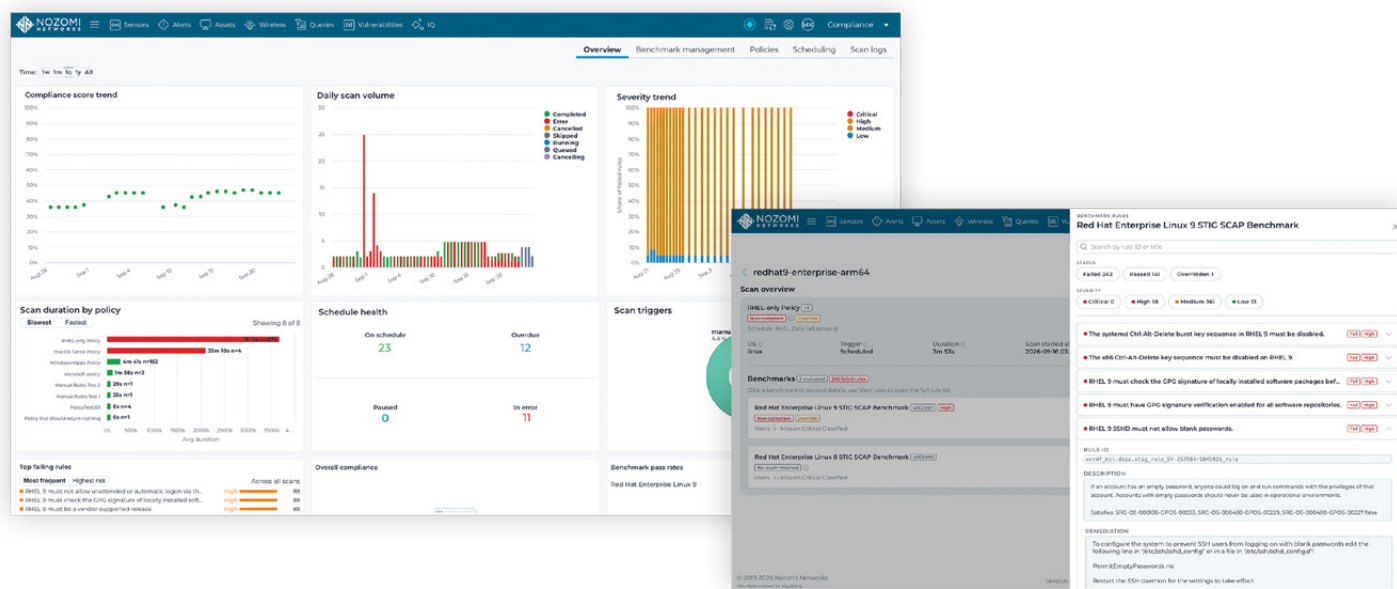
Nozomi Arc sensors collect the host-level configuration data needed to assess DISA STIG checks across OT endpoints and send the results into centralized security and compliance workflows. Security teams can drill into individual DISA STIG checks to understand what failed and why and apply specific remediation guidance.

Easy Benchmark Management, Policy Creation and Assessment Scheduling

Updated DISA STIG benchmarks can be automatically imported upon availability or uploaded when needed. Teams can create policies, assign them to relevant assets and schedule repeatable assessments from one centralized workflow, on premises or in the cloud.

Centralized OT Asset Configuration Review and Tracking

Overall DISA STIG configuration assessment posture can be viewed at-a-glance across benchmarks, policies, scans and assets. Teams can quickly identify failed assessments, view trends over time and focus on the areas that need attention. Individual configuration assessment results can also be viewed within asset profiles in context with identity, vulnerabilities, risk and other security information.



Take the Next Step

Discover how easy it is to identify and respond to cyber threats by automating your OT and IoT asset discovery, inventory and management.

[Request a Demo](#)

nozominetworks.com/demo

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

