FORWARD

Forward Enterprise for Federal Agencies

Mission-ready at any scale

Overview

Federal agencies and DoW organizations must meet the Zero Trust mandate, earn and maintain Authority to Operate (ATO), and continuously evaluate networks that can't wait for a manual audit cycle.

Forward Enterprise turns your network into evidence. It models every vendor, cloud, and tactical IP network into one mathematically accurate digital twin, so every enforcement point, every path, and every policy is provable on demand.

Not a map. Not a diagram.

A continuously verified model, with every enforcement point, path, and policy provable on demand.

The outcome

ATO timelines compress from years to months. Compliance evidence moves from a yearly scramble to a continuous, audit-ready record. Mission teams work from one verified truth instead of tribal knowledge.

Federal Use Cases

- **Zero Trust:** validate enforcement points, segmentation, and policy alignment against a vendor-agnostic model of the network.
- **Continuous ATO evidence:** automate STIG checks and generate audit-ready proof multiple times a day, not once a year.
- **Mission resilience:** map blast radius from any compromised asset and prove segmentation end-to-end, across hybrid and tactical environments.
- **Cyber command readiness:** enter CORA inspections with verified network state.

Capabilities

Network Digital Twin

Models every router, switch, firewall, load balancer, and cloud instance into one mathematically accurate representation of the entire hybrid network.

Change Verification

Tests every routing, firewall, ACL, NAT, and segmentation change against the digital twin and returns pass/fail evidence before anything reaches production.

Security Posture

Traces every reachable path and policy across your hybrid network to surface the vulnerabilities an attacker could exploit.

Trusted AI

Answers natural language questions and runs multi-agent workflows, verifying proposed changes before they run. Available as SaaS.

Why it matters

Proven at mission scale

From the DoW combatant commands to civilian agencies, Forward Enterprise models every major vendor, operating system, and public and government cloud. No proprietary agents. No gaps in coverage. Read-only by design, it never disrupts production.

Zero Trust you can validate

Replace perimeter assumptions with a deterministic model that shows exactly how segmentation and enforcement behave, continuously.

Continuous ATO, by design

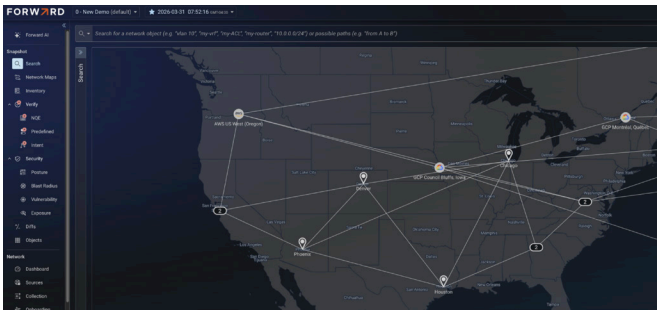
Prepare, assess, authorize, and continuously monitor, with evidence at every stage. Evidence is continuously gathered and processed with every snapshot, removing the yearly bottleneck of post-ATO operations.

Audit-ready, every day

Give assessors immediate access to the verified network state and path evidence. Stand beside inspectors with confidence, not dread.

FORWARD

Prove Zero Trust before the Change Board



The DoW has mandated aggressive Zero Trust adoption timelines. Forward Enterprise supports these mandates directly: validating enforcement points, enabling continuous ATO, and reducing the risk of misconfiguration across large, multi-vendor environments.

- **Comprehensive asset discovery:** build hardware and software inventory, discover end-of-life and end-of-service hardware, and run host inference across every connected device.
- **STIG and CVE compliance:** automate STIG checks and prioritize vulnerabilities by exposure.
- **Segmentation assurance:** validate the posture matrix and enforcement point coverage before an assessor asks.

Prove segmentation and STIG compliance hold before the CAB, not after the audit.

Test the change, before the mission

Forward Enterprise tests every proposed change against a production-equivalent digital twin and returns pass/fail evidence before the change reaches production.

- **Pre-CAB verification:** test proposed routing, firewall, ACL, and segmentation changes against the digital twin at design time.
- **Zero Trust preservation:** prove segmentation and enforcement points survive the change, before it ships.
- **Audit-ready evidence:** catch STIG regressions and attach verification reports to the CCB packet, ready for assessors.

Every change earns approval on evidence, not opinion. Federal teams walk into the Change Board with the proof the change is safe, and leave with an approved deploy, no post-audit surprises, and no mission-day reviews.

Modeled without gaps, across every environment

30+
Supported network vendors

35+
Vendor operating systems

4
Public clouds modeled

15+
Technology integrations

Built for every mission

Civilian agencies
Modernize hybrid IT with full visibility and continuous compliance evidence.

CORA readiness
CORA-ready every day, not just inspection week, with evidence assessors can trust.

DoW
Validate Zero Trust enforcement, segmentation, and STIG posture at mission scale

Mission partners
Secure interoperability across coalition and joint environments.

GET STARTED Request a demo at **www.forwardnetworks.com/request-a-demo**