FORWARD

Forward Enterprise for Network Security

Confidence, built on proof.

Overview

Modern networks have outgrown intuition, manual audits, and point-in-time scans. Security teams need proof, not assumptions; that segmentation policies, access controls, and network paths behave exactly as intended across the hybrid network infrastructure.

Forward Enterprise delivers that proof. It pulls configuration and state from routers, switches, firewalls, load balancers, and cloud environments, and into a mathematically accurate digital twin of the entire network.

Not a scan. Not a snapshot.
A continuously verified model, with exposure, segmentation, and compliance provable on demand, across every path and policy in the network.

The outcome
Exposure stops hiding in blind spots. Segmentation stops being assumed and starts being proven. Compliance evidence moves from static, point-in-time checks to continuous, defensible proof. Security teams work from one verified model instead of chasing configurations across devices.

Network Security Use Cases

- **Attack surface and exposure analysis:** trace attack paths from exposure points through to critical systems, before they are exploited by someone else.
- **Vulnerability management:** prioritize CVEs by network context and exploitability instead of severity score alone.
- **Continuous network compliance:** replace static, point-in-time checks with continuous, near real-time evidence.
- **Firewall rule optimization:** remove unused rules and overly permissive policies that grow hidden risk over time.
- **Shadow IT and asset discovery:** find unmanaged or forgotten devices that never made it into the CMDB.
- **Pre-deployment risk verification:** with Forward Predict, catch outcomes with proposed policy changes before they reach production.

Capabilities

End-to-end path analysis
See exactly how traffic can move between any two points on the network.

Segmentation validation
Prove that the segmentation strategy works as intended, not just as designed.

Attack surface reduction
Identify exposed services, permissive rules, and implicit trust relationships.

Vulnerability management
Detect network device vulnerabilities and prioritize those actively being exploited.

Continuous drift detection
Detect when the network drifts away from approved security intent, automatically.

Compliance verification
Simplify audits by providing near real-time, provable evidence.

Why it matters

Attack surface and exposure analysis
Security teams lack visibility into attack paths from exposure points through multiple NAT translations to physical assets, leaving critical systems unknowingly exposed. Forward Enterprise reduces attack surface, verifies that architecture matches intent, and speeds breach investigation and mitigation.

Vulnerability management
Organizations are overwhelmed by thousands of CVEs affecting network devices, with no network context to determine which device carries the most risk. Forward Enterprise reduces vulnerability noise and focuses remediation on exploitable risk, with CISA KEV integration.

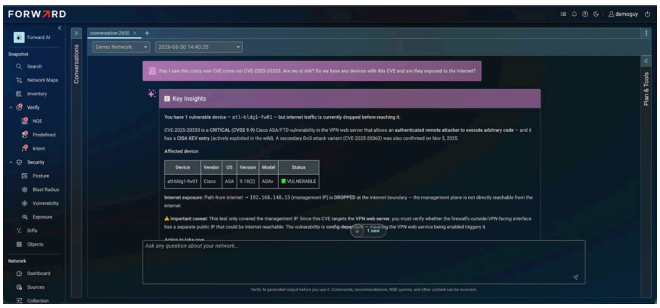
Continuous network compliance
Audits consume weeks of manual effort. Static, point-in-time checks fail to capture the dynamic reality of hybrid network infrastructure. Forward Enterprise delivers continuous compliance visibility and faster audits, backed by near real-time evidence.

Firewall rule optimization
Firewall rule sets grow unmanageable over time, creating hidden risk through unused rules, redundant policies, and unreviewed access paths. Forward Enterprise simplifies rule audits and improves firewall rule lifecycle management.

FORWARD

Security analysis at AI speed

Forward AI enables security teams to investigate network risk using natural language queries grounded in the verified Forward Enterprise network model. Instead of tracing configurations across devices, analysts ask complex security questions and receive answers validated against a behaviorally accurate digital twin of the network.



Blast radius analysis: determine the true blast radius of a CVE by analyzing reachable network paths instantly.

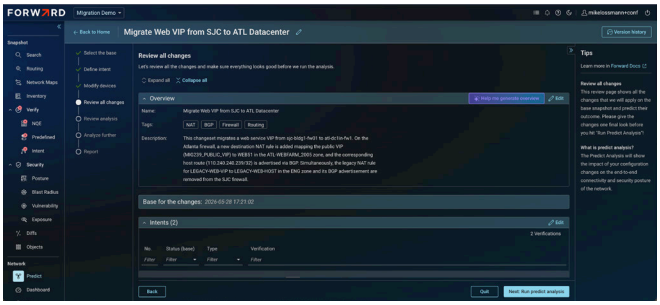
Exposure mapping: identify whether a device or service is exposed to the internet, and what security devices it passes through.

Policy gap analysis: detect policy violations and perform gap analysis against compliance or segmentation requirements.

Verify change before it ships

Forward Predict tests proposed routing, firewall policies, and ACL, changes against a mathematically accurate, network digital twin, before they reach production. Teams get a verified answer, not a guess, with security, connectivity, and compliance risks identified at design time.

Intent validation: test proposed changes against intent. Pass or fail, no guesses.



Regression testing: surface unexpected outage risk, and exposure risks of an urgent security update before deployment.

Accelerated CAB approval: move change reviews from months to days, backed by verified evidence.

Audit-ready across major standards

DISA STIGs **HIPAA** **ISO 27001** **PCI DSS** **NIST 800-53**

Built for the way security teams work

Complete visibility
Analyze all paths, not just observed traffic. If a path across the network exists, Forward Enterprise knows about it.

Read-only by design
Never pushes changes into the environment. Zero impact to production.

Vendor agnostic
Works across multi-vendor on-premises networks, multi-cloud environments (AWS, GCP, Azure, IBM), and hybrid architectures.

Security you can explain
Clear, defensible answers for leadership, auditors, and incident reviewers.

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