FORWARD ENTERPRISE FOR NETWORK SECURITY

Prove Your Network Security

Modern networks are too complex to secure using intuition, manual audits, or point-in-time scans. Security teams need proof that segmentation policies, access controls, and network paths behave exactly as intended across the hybrid infrastructure. Forward Enterprise provides proof. It collects configuration and state from routers, switches, firewalls, load balancers, and cloud environments to build a precise behavioral model of your entire network. Using this digital twin, security teams can analyze every possible traffic path, verify segmentation policies, identify unintended exposure, and continuously detect configuration drift. The result is provable network security posture without agents, traffic mirroring, or disruption to production environments.

KEY CAPABILITIES

WHAT FORWARD ENTERPRISE SOLVES

End-to-End Path Analysis
See exactly how traffic can move between any two points.

Segmentation Validation
Prove that your segmentation strategy works as intended.

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 and compliance by providing near real-time provable evidence.

USE CASES

FOUR CRITICAL SECURITY CHALLENGES

01 Attack Surface & Exposure Analysis

THE CHALLENGE
Security teams lack visibility into attack paths from the exposure points through to the physical assets, leaving critical systems unknowingly exposed.

Customer Value
- Reduced attack surface
- Verify security architecture matches intent
- Faster breach investigation and mitigation
- Attack path trimming

02 Vulnerability Management

THE CHALLENGE
Organizations are overwhelmed by thousands of CVEs affecting network devices, with no network context to determine which device has the most risk.

Customer Value
- Reduce vulnerability noise
- Focus remediation on exploitable risk
- Improve prioritization with CISA KEV integration
- Avoid time-consuming authenticated scans

03 Continuous Network Compliance

THE CHALLENGE
Audits consume weeks of manual effort. Static, point-in-time checks fail to capture the dynamic reality of hybrid network infrastructure.

Customer Value
- Faster audits with continuous, near real-time evidence
- Continuous compliance visibility
- Reduced risk of misconfiguration

04 Firewall Rule Optimization

THE CHALLENGE
Firewall rule sets grow unmanageable over time, creating hidden risk through unused rules, redundant policies, and unreviewed access paths.

Customer Value
- Reduce attack surface from unused rules
- Simplify firewall rule audits
- Improve firewall rule lifecycle management

FORWARD ENTERPRISE FOR NETWORK SECURITY

Prove Your Network Security

SUPPORTED COMPLIANCE FRAMEWORKS

AUDIT READY ACROSS MAJOR STANDARDS

DISA STIGs | HIPAA | ISO 27001 | PCI DSS | NIST 800-53 | Internal Security Standards

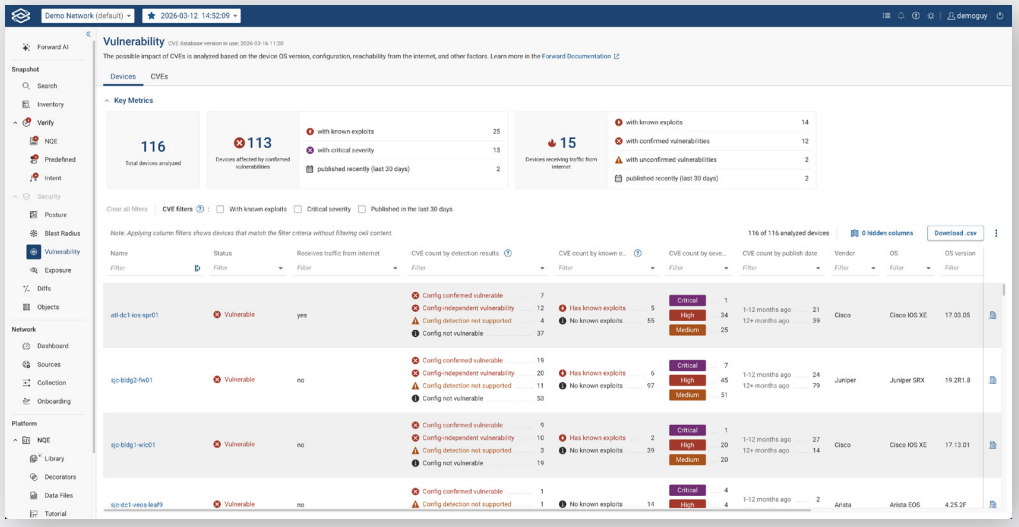
Auditors ask questions. Forward Enterprise answers them, instantly and comprehensively, with provable evidence instead of manual attestations.

FORWARD AI

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 manually tracing configurations across devices, analysts can ask complex security questions and receive answers validated against a mathematically accurate digital twin of the network. Determine the true blast radius of a CVE by analyzing reachable network paths instantly.

- Identify whether a device or service is exposed to the internet and what security devices it passes through.
- Detect policy violations and perform gap analysis against compliance or segmentation requirements.



Security Vulnerabilities Discovered by Forward Enterprise

WHY FORWARD ENTERPRISE

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.

Vendor Agnostic

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

Read-Only by Design

Never pushes changes into the environment.
Zero impact to production.

Security You Can Explain

Clear, defensible answers you can take to leadership, auditors, and incident reviewers.