

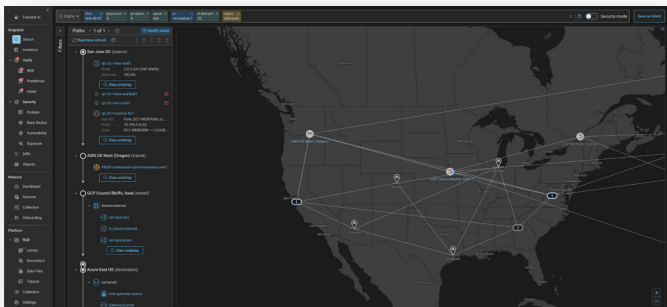
Forward Enterprise

Run and Secure Your Network with Mathematical Certainty

Overview

Your network should be your most trusted asset. Forward Enterprise builds a mathematically accurate digital twin of every router, switch, firewall, load balancer, and cloud instance across your hybrid environment, delivering a single verified source of truth to every network, security, cloud, and compliance team. Read-only by design, Forward Enterprise never risks production and gives teams the certainty to act without guesswork.

The result is a network that becomes the verified foundation your organization builds on. Network problems surface before production, not after users feel them. Changes ship with evidence. Security and compliance run continuously. And AI agents act on verified truth at machine speed.



The Outcome

When you trust a mathematically accurate digital twin, everything changes. Not incrementally, but fundamentally. Change windows shrink because impact is verified before anything touches production. Security gaps close because every possible path is visible, not assumed. Compliance stops being a quarterly fire drill. The teams carrying the weight of your network's complexity finally have something solid beneath them. That's not a promise; that's what verified truth delivers.

Capabilities

Network Digital Twin

Builds a mathematically accurate model of every router, switch, firewall, load balancer, and cloud instance across 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 against the digital twin, verifying every proposed action before it executes.

Forward Enterprise Use Cases

- **Accelerated Troubleshooting:** Eliminate the discovery phase of troubleshooting. Replace tribal knowledge and stale diagrams with a vendor-agnostic digital twin. Instantly trace packet paths, query complex policies, and resolve connectivity tickets across your hybrid estate using a mathematically accurate model of your live network.
- **Security Posture Verification:** Stop assuming isolation. Map every potential attack vector to surface reachable vulnerabilities that scanners miss. Move beyond static audits to active path verification, proving defenses block threats.
- **Change Management:** Turn the CAB from a subjective debate into a data-driven gate. Swap best-guess impact assessments for mathematical proof. Test every routing, NAT, and ACL change against the digital twin to catch catastrophic errors in staging and ship with a definitive pass/fail record.
- **Agentic operations, without the risk:** Run complex network workflows at machine speed, without putting production at risk. Every action teams, and AI agents take is verified against the digital twin before it executes, catching unintended consequences before they reach the network.

In Practice

NetOps

Operate the hybrid network with full visibility

Replace fragmented monitoring and tribal knowledge with end-to-end path analysis, authoritative inventory, and a vendor-agnostic digital twin. Trace traffic flows across on-premises and cloud environments in seconds.

CloudOps

Take hybrid workloads live faster

Verify new paths across AWS, Azure, GCP, IBM Cloud, and on-premises networks end-to-end before deployment. Resolve connectivity issues that stall cloud migrations and application deployments before reaching production.

SecOps

Know and eliminate your attack surface

Trace every reachable path from exposure point to critical asset, across on-prem and cloud. Surface permissive rules, implicit trust, and unintended access, and catch new exposure the moment a change introduces it, before it can be exploited.

Compliance

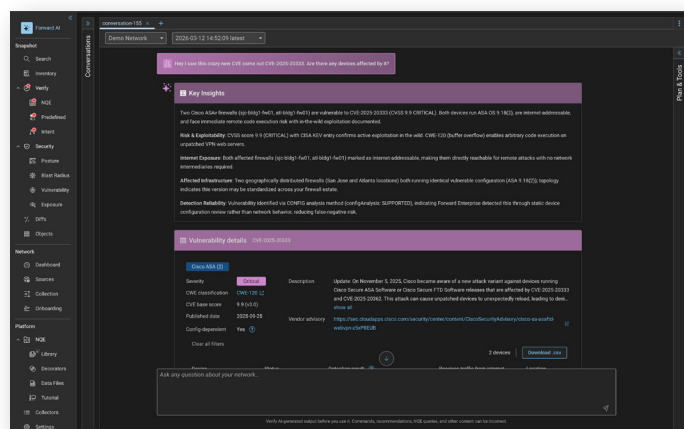
Stay audit-ready, continuously

Verify cloud and on-premises regulatory policies on every change, across every vendor and zone. Identify policy drifts and violations before deployment, maintaining a full audit trail of exactly what was tested and when.

Forward Enterprise: Delivering Strategic Value

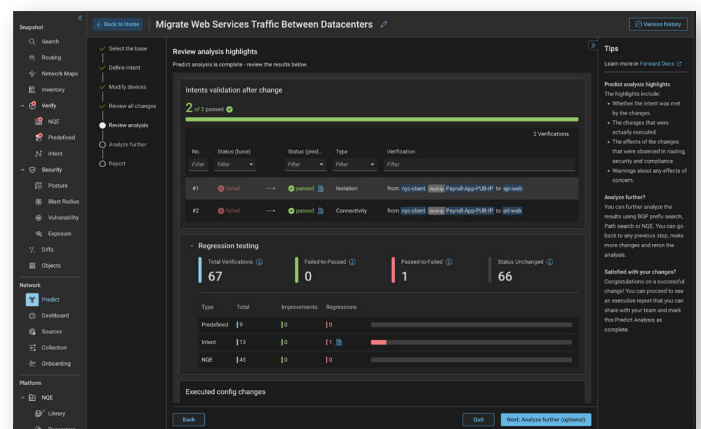
Verified truth, at AI speed

Forward AI delivers the power of a mathematically accurate and trust-worthy digital twin to every operator and automated agent, eliminating guesswork and manual analysis. Teams instantly understand network behavior and act with confidence across complex environments. By making expert-level knowledge accessible without requiring deep domain expertise or constant escalation, Forward AI enables teams to ask complex questions and receive verified, evidence-backed answers in seconds.



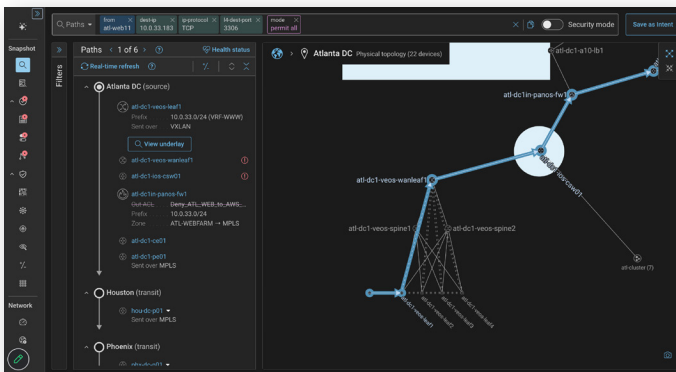
Verify before you deploy

Forward Predict verifies every proposed network and security change against the digital twin before a single command reaches production. It evaluates routing updates, firewall rules, ACL changes, and segmentation policies end-to-end to determine their impact on security, connectivity, and compliance. By shifting CAB approvals from subjective judgment calls to evidence-backed decisions, Forward Predict compresses delivery cycles from weeks to days and ensures higher first-attempt success rates.



Instant visibility and path tracing

Path Search acts as a Google-like engine for your infrastructure. By querying the digital twin, engineers instantly visualize hop-by-hop paths across multi-vendor on-prem and cloud environments. It eliminates manual CLI tracing, allowing users to search for IPs, MACs, or application paths to see exactly how traffic interacts with routing, NAT, and security policies.



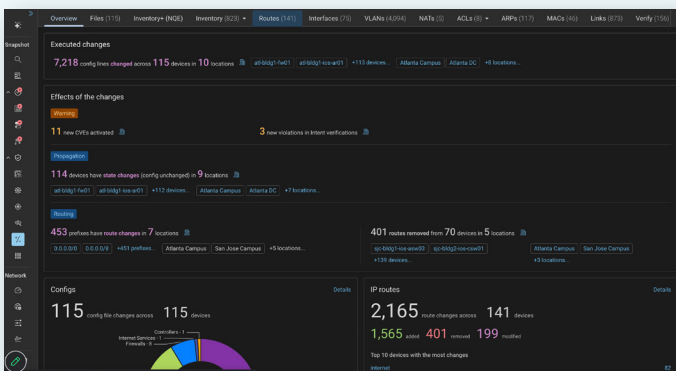
Continuous compliance with business rules

Network Verification and Policy Intent ensures network behavior aligns with business goals. By defining Intent, such as isolating Production from Development, the platform continuously audits the network state. Any configuration drift or change that violates these rules triggers an immediate alert, shifting security from periodic audits to real-time, proactive enforcement.

Active	Name	Type	Intent	Tags	Query	Verification status	Health
☒	Atlanta Webfarm to AWS DB	Existential	Verify that Atlanta Webfarm ...	from atl-dc1-web-ho	from atl-dc1-web-ho	passed	disabled
☒	Atlanta Webfarm to MySQL DB	Existential	Verify that Atlanta Webfarm ...	from atl-dc1-web-ho	from atl-dc1-web-ho	failed	n/a
☒	Atlanta Webfarm to MySQL DB	Existential	Verify that Atlanta Webfarm ...	from atl-dc1-web-ho	from atl-dc1-web-ho	failed	n/a
☒	Atlanta Webfarm to MySQL DB	Existential	Verify that Atlanta Webfarm ...	from atl-dc1-web-ho	from atl-dc1-web-ho	failed	n/a
☒	Atlanta Web to AWS App Cluster	Existential	Verify that Atlanta Web ...	from atl-dc1-web-ho	from atl-dc1-web-ho	failed	n/a
☒	Backend Instances	Isolation	Verify that Backend Instances ...	from atl-dc1-web-ho	from atl-dc1-web-ho	failed	n/a

Rapid troubleshooting of unintended changes

Snapshot-based digital twin acts as a network time machine by continuously capturing full-state snapshots of the network over time. Behavior Diff then allows engineers to compare any two snapshots to instantly identify the root cause of issues, including exactly which configuration lines changed, which routes were withdrawn, or which security policies were modified.



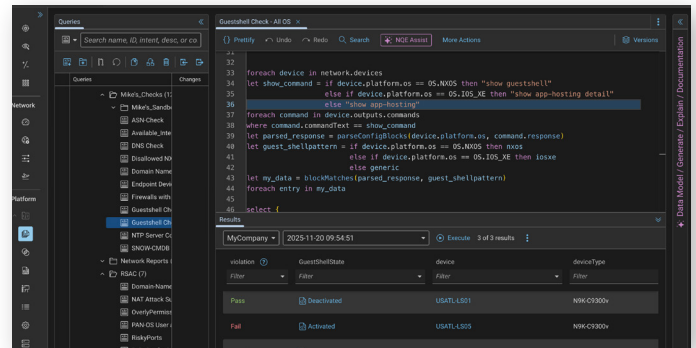
Exposure and vulnerability containment

Security Posture & Blast Radius visualizes the reachability of compromised assets to uncover hidden vulnerabilities. By mathematically calculating every possible path, it maps the "blast radius" of a potential breach. This ensures segmentation remains intact and minimizes the attack surface across the entire hybrid cloud.

Source	Target	Name	Security zones	IP protocol	L4 dest port
10.55.101.11	10.30.10.4	azure-01	Any	Any	
10.55.101.11	10.30.10.11	sp-dc1-web-host1	sp-dc1-panos-fe ...	6	80
10.55.101.11	10.55.101.11	atl-web11	atl-dc1-panos-fe ...	Any	Any
10.55.101.11	10.51.101.11	sp-dc2-web-host1	sp-dc1-panos-fe ...	6	Any
10.55.101.11	10.51.103.31	sp-dc2-web-host31	sp-dc1-panos-fe ...	6	Any
10.55.101.11	10.50.100.22	sp-dc1-web-host22	sp-dc1-panos-fe ...	6	80

Custom automation and standardized reporting

Network Query Engine (NQE) transforms fragmented, multi-vendor CLI data into a structured JSON model, and provides a powerful, flexible network-wide query language for analyzing infrastructure state at scale. This enables “network as code” workflows, allowing teams to run custom queries that verify configurations, automate inventory audits, and ensure global consistency without ever logging into a device.



30+
Supported
Vendors

35+
Vendor Operating
Systems

900
Versions of
Operating Systems

4 Public Clouds



Google Cloud



15+ Technology Integrations



ARISTA



infoblox



RAPID7



servicenow



Get started

Request a demo at www.forwardnetworks.com/request-a-demo