

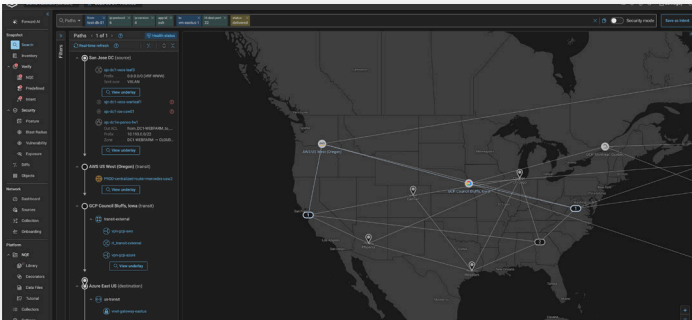
Forward Enterprise

The Platform for Safe Agentic NetOps, Built on Mathematical Certainty.

Overview

Your network should be the trusted foundation for AI and Agentic NetOps. Forward Enterprise builds a mathematically accurate digital twin of every router, switch, firewall, load balancer, and cloud instance across your hybrid environment, giving teams and agents a single verified source of truth to know what's true, predict what's next, and prove what will work. Read-only by design, Forward Enterprise never risks production and gives network, security, cloud, and compliance teams the certainty to act without guesswork.

The result is a network you can understand, predict, and trust. Network problems surface before production, not after users feel them. Changes move forward with evidence. Security and compliance run continuously. And AI agents' reason from verified truth at machine speed.



The Outcome

When your operations run on 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 verified, not assumed. Compliance stops being a quarterly fire drill. Your teams and AI agents have the verified foundation to know what's true, predict what's next, and move with confidence.

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 proposed routing, firewall, ACL, NAT, and segmentation change against the digital twin and returns evidence of impact before anything reaches production.

Security Posture

Traces every reachable path and policy across your hybrid network to surface exploitable vulnerabilities, verify segmentation, and prioritize remediation by real risk.

Built-in, Trusted AI

Answers natural language questions and runs multi-step workflows against the digital twin, grounding AI in verified network truth and the predictive capabilities of the platform.

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 issues across your hybrid network using a mathematically accurate model of what is deployed.
- **Security Posture Verification:** Stop assuming isolation. Map every potential attack path to surface reachable vulnerabilities that scanners miss. Move beyond static audits to continuous path verification, proving whether your defenses actually block threats.
- **Change Management:** Turn the CAB from a subjective debate into a data-driven decision. Replace best-guess impact assessments with mathematical proof. Test routing, NAT, and ACL changes against the digital twin before production, identifying unintended consequences at design time, and providing clear evidence to move forward.
- **Safe Agentic NetOps:** Give teams and AI agents trusted network intelligence without putting production at risk. Investigate complex questions, run multi-step workflows, and predict the impact of proposed changes using a mathematically accurate digital twin, so AI operates from verified network truth rather than assumptions.

Why it matters

01 Replace assumptions with certainty

When teams operate from the same source of truth, response times shrink, troubleshooting cycles shorten, and the cross-team disagreements give way to faster decisions.

03 Continuously verify security and compliance

Audit readiness becomes a continuous state, not a quarterly project. Provable evidence for DISA STIGs, PCI DSS, HIPAA, ISO 27001, and NIST 800-53 reduces regulatory exposure and the operational cost of demonstrating control.

In Practice

NetOps

Operate the hybrid network with verified understanding

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 and troubleshoot from a shared source of truth.

CloudOps

Take hybrid workloads live with confidence

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

02 Accelerate delivery while reducing risk

Change velocity becomes a business advantage rather than an operational risk. Risky changes are caught at design time, not after deployment, compressing change cycles, and turning rollbacks into a rare exception.

04 Safe Agentic NetOps

Give teams the leverage of AI without inheriting a new class of operational risk. Ground AI in verified network truth and use the digital twin to validate proposed changes before they reach production.

SecOps

Know 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 identify how proposed changes could introduce new exposure before they reach production.

Compliance

Stay audit-ready, continuously

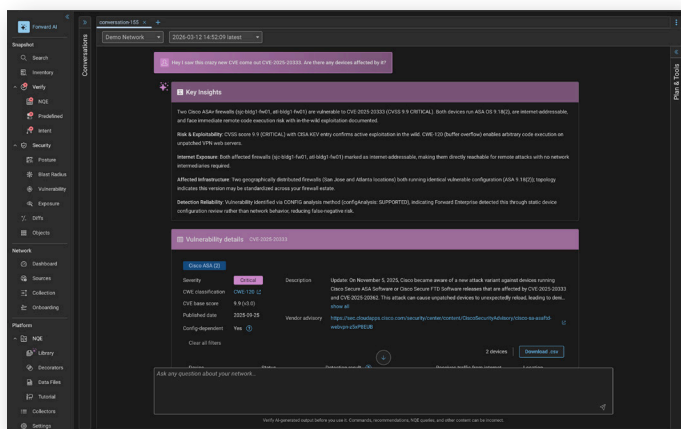
Verify cloud and on-premises regulatory policies across every vendor and zone. Identify policy drift and violations and validate proposed changes before production, maintaining a verifiable audit trail of what was tested and when.

Forward Enterprise: Capabilities in Action

Safe agentic AI, built on verified network truth

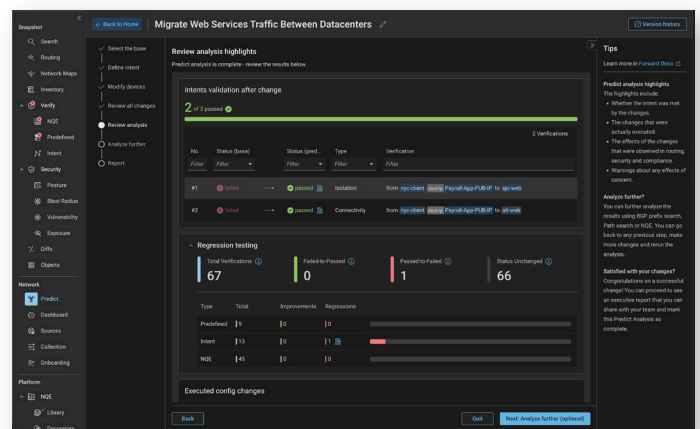
Forward AI brings natural-language interaction and multi-step workflows to the mathematically accurate digital twin at the core of Forward Enterprise. Teams can ask complex questions and receive verified, evidence-backed answers in seconds, grounded in trusted network truth.

Forward MCP extends the same read-only network knowledge to external agents and MCP clients, so teams and their own agents can look up devices, trace paths, and query inventory, and reason over the network using the digital twin.



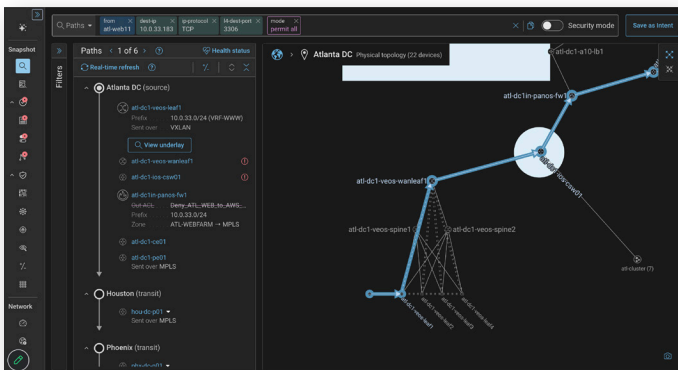
Know before you act

Forward Predict runs proposed network changes against the digital twin at design time, before a single command reaches production. It models the impact of routing, ACL, NAT, firewall, and segmentation changes across the network, identifying potential connectivity, security, and compliance issues before deployment. Teams get evidence to support CAB approvals, compare current and predicted state, and move proposed changes forward with greater confidence. The same predictive insight can inform AI and agentic workflows before anything reaches production.



Instant path analysis across your entire network

Path Search acts as a search engine for your network. By querying the digital twin, engineers can instantly trace 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 and understand how traffic is affected by routing, NAT, and security policies.



Continuous compliance with business rules

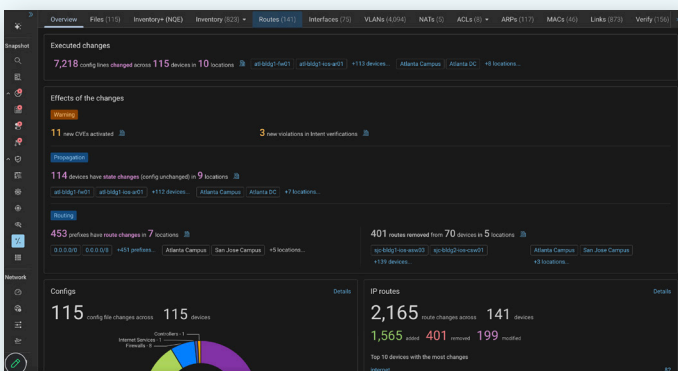
Network Verification and Policy Intent ensures network behavior aligns with business goals. By defining Intent, such as isolating Production from Development, the platform continuously audits network behavior against those rules. Any configuration drift or change that violates defined policy is surfaced immediately, shifting compliance from periodic audits to continuous verification.

The screenshot shows the Intent Verification interface. It features a table with columns for Name, Type, Intent, Tags, Query, Verification status, and Health. The table lists various verification tasks, such as 'Verify that Atlanta Webfarm to AWS DB is Existential', and their corresponding status (e.g., 'passed', 'failed', 'notified').

Name	Type	Intent	Tags	Query	Verification status	Health
Atlanta Webfarm to AWS DB	Existential	Verify that Atlanta Webfarm to AWS DB is Existential	Atlanta	from atl-dc1-web-farm to atl-dc1-aws-db	passed	disable
Atlanta Webfarm to MySQL DB	Existential	Verify that Atlanta Webfarm to MySQL DB is Existential	Atlanta	from atl-dc1-web-farm to atl-dc1-mysql-db	failed	n/a
Atlanta Webfarm to MySQL DB	Existential	Verify that Atlanta Webfarm to MySQL DB is Existential	Atlanta	from atl-dc1-web-farm to atl-dc1-mysql-db	notified	n/a
Atlanta Webfarm to MySQL DB	Existential	Verify that Atlanta Webfarm to MySQL DB is Existential	Atlanta	from atl-dc1-web-farm to atl-dc1-mysql-db	failed	n/a
Atlanta Web to AWS App Cluster	Existential	Verify that Atlanta Web to AWS App Cluster is Existential	Atlanta	from atl-web-farm to atl-dc1-aws-app-cluster	failed	n/a
Backend instances	Isolation	Verify that Backend instances are isolated	Atlanta	from atl-dc1-web-farm to atl-dc1-aws-app-cluster	failed	n/a

Rapidly troubleshoot unintended changes

Snapshot-based digital twin captures full-state snapshots of the network over time. Behavior Diff lets engineers compare any two points in time to quickly isolate what changed, including configuration updates, withdrawn routes, and modified security policies.



Proactive exposure and vulnerability analysis

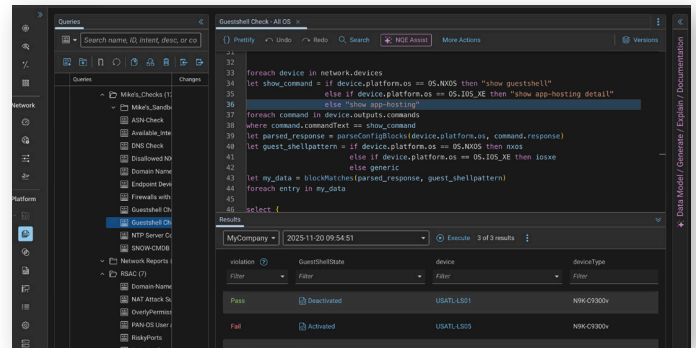
Security Posture and Blast Radius visualize the reachability of compromised assets to uncover hidden vulnerabilities. By mathematically calculating reachable paths across the network, it maps the “blast radius” of a potential breach. This helps teams verify segmentation, understand exposure, and identify where risk could propagate across the hybrid network.

The screenshot shows the Blast Radius interface. It displays a table with columns for Source, Target, Name, Security zones, IP protocol, and L4 dest port. The table lists various reachability results, such as '10.55.101.11' reaching '10.50.10.4' via 'azure-01'.

Source	Target	Name	Security zones	IP protocol	L4 dest port
10.55.101.11	10.50.10.4	azure-01	Any	Any	
10.55.101.11	10.50.101.11	sp-dc1-web-host11	atl-dc1-in-panco-fe...	6	80
10.55.101.11	10.55.101.11	atl-web11	atl-dc1-in-panco-fe...	Any	Any
10.55.101.11	10.51.101.11	sp-dc2-web-host11	atl-dc1-in-panco-fe...	6	Any
10.55.101.11	10.51.101.11	sp-dc2-web-host31	atl-dc1-in-panco-fe...	6	Any
10.55.101.11	10.50.103.22	sp-dc1-web-host22	atl-dc1-in-panco-fe...	6	80

Custom automation and reporting at scale

Network Query Engine (NQE) transforms fragmented, multi-vendor CLI data into a structured JSON model that can be queried consistently across the entire network. This enables “network as code” workflows, enabling teams to verify configurations, automate inventory audits, and ensure global consistency without manually querying individual devices.



30+

Supported
Vendors

35+

Vendor Operating
Systems

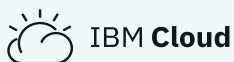
900

Versions of
Operating Systems

4 Public Clouds



Google Cloud



20+ Technology Integrations



Get started

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