USE CASE

Reduce Audit Effort by 99% with Automated Compliance Validation

Financial institutions operate under some of the world's most stringent regulatory frameworks—PCI DSS, SOX, GLBA, DORA, GDPR—and face increasing scrutiny from both regulators and customers. Yet ensuring continuous compliance across sprawling, hybrid IT environments remains an ongoing challenge. Networks built over decades, often through mergers and acquisitions, lack consistent documentation, centralized visibility, and scalable mechanisms to enforce policy. This complexity results in configuration drift, audit delays, and significant regulatory risk.

Non-Compliance is Nearly Triple the Cost, Zero the Confidence

The business case for proactive compliance is clear. According to the Ponemon Institute, the average annual cost of non-compliance for a U.S. financial services firm is $14.82 million, nearly triple the $5.47 million it costs to remain compliant. In other words, non-compliance costs 2.71 times more than maintaining a compliant environment. These costs are driven not only by regulatory fines, but also by operational disruptions, reputational damage, and lost customer trust.

Maintaining compliance in financial services is especially difficult due to the size and heterogeneity of the network. Devices from dozens of vendors, legacy infrastructure, and rapid cloud adoption make consistent enforcement and verification nearly impossible without automation. Teams often rely on outdated spreadsheets, tribal knowledge, and manual CLI commands to assess security posture—a process that introduces risk and cannot scale.

The Multi-Million Dollar Burden of Audit Readiness

Audit readiness remains a persistent challenge for financial institutions. Compared to pre-financial crisis spending levels, operating costs spent on compliance have increased by over 60 percent for retail and corporate banks according to Deloitte. For large institutions, this translates to millions of dollars annually in labor, compliance software, and external consulting fees. These costs are driven by the need to document controls, validate policies, test compliance, and remediate gaps across complex, hybrid networks.

Preparing for an audit often demands thousands of person-hours, particularly in global banks and insurers with highly federated environments. In many cases, audit teams must coordinate across dozens of internal systems, line-of-business applications, and legacy infrastructure—frequently relying on fragmented data sources and manual processes. According to industry estimates, responding to a major audit can consume 5,000 to 10,000 worker hours across network, security, compliance, and legal teams over several weeks.

Bank Slashes Audit Time by 99% — Saving $200K Annually

A large global bank required constant monitoring of over 1,000 interconnects with financial partners to ensure operational efficiency and regulatory compliance. Manual auditing by dedicated engineers was time-consuming and often failed to detect broken links in a timely manner. Using the Forward Enterprise Network Query Engine (NQE), the bank created a configuration auditor that automatically scans all interconnects daily, immediately flagging misconfigurations for prompt remediation. This eliminated tedious manual audits and produced tangible business results:

- Audit time reduced from 84 hours per month to just minutes daily
- $200K annual labor savings
- Engineers freed for higher-value tasks
- Improved compliance and operational assurance at scale

Proven Cost Benefits Across Institutions

In one IDC study, organizations using Forward Networks reported compliance teams were 10.4% more efficient—equal to four FTEs—and saved nearly $400,000 annually based on an average salary of $100,000. (See Figure 1)
By replacing error-prone, unscalable processes with Forward's automated solution, enterprises dramatically reduce audit time and labor costs while strengthening regulatory confidence.

	BEFORE/WITHOUT FORWARD NETWORKS	WITH FORWARD NETWORKS	DIFFERENCE	BENEFIT
Total FTE count	38.3	**34.3**	4.0	10.4%
Value of staff time per year	$3,831,250	**$3,433,330**	$397,920	10.4%

Figure 1 IDC Estimates of Regulatory Compliance Benefits with Forward Enterprise

The stakes are high. Regulatory agencies including the SEC, OCC, FDIC, and CFPB can impose fines, sanctions, or consent orders if an institution fails to demonstrate compliance. Penalties vary widely but can be severe: in 2022, the SEC fined 16 Wall Street firms a combined $1.8 billion for recordkeeping and compliance failures. Beyond the immediate financial impact, failed audits often lead to enhanced oversight, reputational damage, and forced operational changes, driving up long-term costs and disrupting business continuity.

What is a Network Digital Twin?

Forward Enterprise is the industry's only true network digital twin, delivering a mathematically accurate model of the network—on-premises, cloud, or hybrid. The platform supports 30+ hardware vendors, 35+ operating systems, and over 900 OS versions across AWS, Azure, and GCP environments. By modeling every possible path a packet can take, Forward Enterprise provides comprehensive, actionable insight into network behavior, security posture, and compliance status.

Its passive, read-only approach eliminates security risk while enabling teams to continuously verify configurations, segmentations, and access policies. Forward Enterprise integrates with CMDBs and discovers unknown devices, ensuring a complete and continuously updated inventory. It can scale to over 50,000 devices without requiring heavy server infrastructure, and serves as a single source of truth across NetOps, SecOps, and Cloud teams.

How a Network Digital Twin Streamlines Compliance

Continuous compliance monitoring is essential to ensure that networks remain compliant at all times—not just during scheduled audits. Even small configuration updates or policy changes can inadvertently break compliance, creating risk exposure that may go unnoticed until an incident or audit occurs. Forward Enterprise addresses this challenge by automating the validation of security and regulatory controls in real time, closing the gap between change and assurance.

This need is amplified by the sheer scale of modern financial networks, which often consist of tens of thousands of devices and millions of lines of configuration code. At this magnitude, manual audits are impractical and error-prone. Forward Enterprise replaces these resource-intensive processes with automated "intent checks" that run continuously. Each check captures the current network state and validates it against policy, so that if drift is detected, teams receive clear, actionable alerts and can immediately remediate issues before they escalate. Snapshots also provide on-demand, point-in-time evidence for auditors, giving organizations confidence that their networks are always operating within compliance.

REGULATORY COMPLIANCE ✓

Agencies impose **fines and sanctions** for violations

ENHANCED OVERSIGHT ✓

Greater scrutiny **financial regulators** for compliance

REPUTATIONAL DAMAGE ✓

Non-compliance can lead to **loss of trust**

LONG-TERM COSTS ✓

Financial institutions face **increased operational expenses**

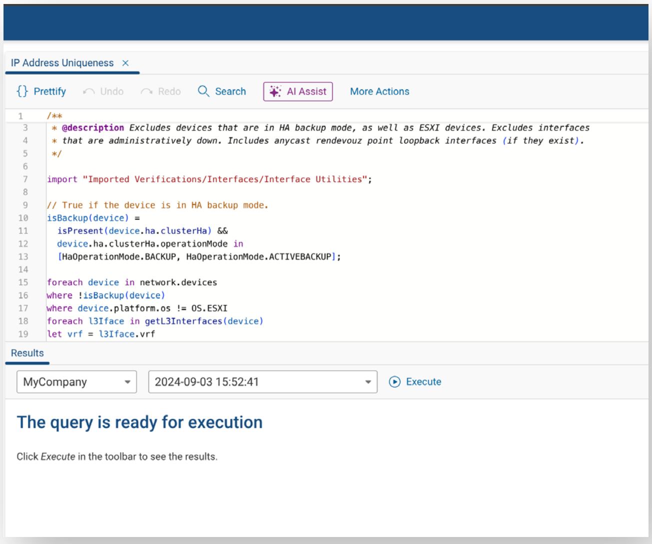
OPERATIONAL CHANGES ✓

Increased costs and **business disruption** are likely

4 Steps to Continuous Network Compliance Monitoring with a Digital Twin

1. Search the Entire Network

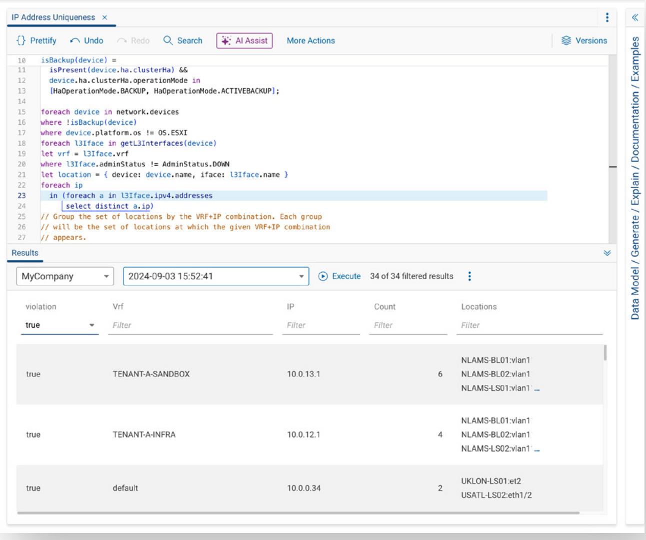
The Network Query Engine (NQE) enables teams to search network assets as if querying a database—by device type, configuration, IP/MAC address, or other parameters. Hundreds of prebuilt checks are available, or custom queries can be written or generated using Forward's AI Assist with natural language prompts.



```
/**
 * @description Excludes devices that are in HA backup mode, as well as ESXI devices. Excludes interfaces
 * that are administratively down. Includes anycast rendevouz point loopback interfaces (if they exist).
 */

import "Imported Verifications/Interfaces/Interface Utilities";

// True if the device is in HA backup mode.
isBackup(device) =
  isPresent(device.ha.clusterHa) &&
  device.ha.clusterHa.operationMode in
  [HaOperationMode.BACKUP, HaOperationMode.ACTIVEBACKUP];

foreach device in network.devices
where !isBackup(device)
where device.platform.os != OS.ESXI
foreach l3Iface in getL3Interfaces(device)
let vrf = l3Iface.vrf
```

The query is ready for execution

Click *Execute* in the toolbar to see the results.



```
isBackup(device) =
  isPresent(device.ha.clusterHa) &&
  device.ha.clusterHa.operationMode in
  [HaOperationMode.BACKUP, HaOperationMode.ACTIVEBACKUP];

foreach device in network.devices
where !isBackup(device)
where device.platform.os != OS.ESXI
foreach l3Iface in getL3Interfaces(device)
let vrf = l3Iface.vrf
where l3Iface.adminStatus != AdminStatus.DOWN
let location = { device: device.name, iface: l3Iface.name }
foreach ip
  in (foreach a in l3Iface.ipv4.addresses
      select distinct a.ip)
// Group the set of locations by the VRF+IP combination. Each group
// will be the set of locations at which the given VRF+IP combination
// appears.
```

34 of 34 filtered results

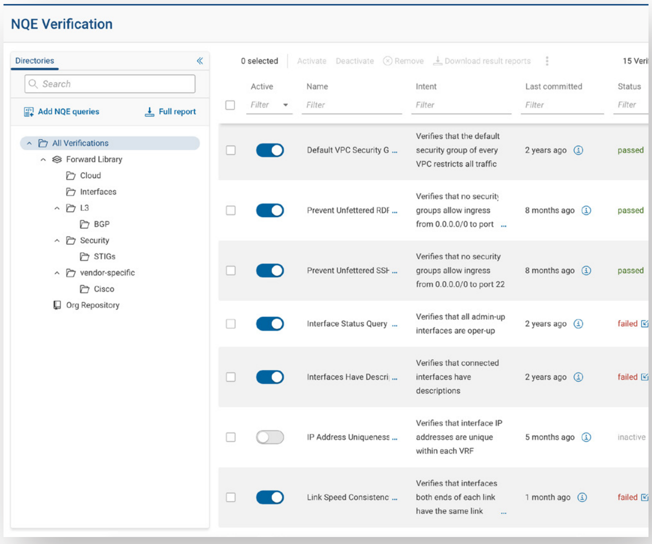
violation	Vrf	IP	Count	Locations
true	Filter	Filter	Filter	Filter
true	TENANT-A-SANDBOX	10.0.13.1	6	NLAMS-BL01:vlan1 NLAMS-BL02:vlan1 NLAMS-LS01:vlan1 ...
true	TENANT-A-INFRA	10.0.12.1	4	NLAMS-BL01:vlan1 NLAMS-BL02:vlan1 NLAMS-LS02:vlan1 ...
true	default	10.0.0.34	2	UKLON-LS01:et2 USATL-LS02:eth1/2

2. Identify Non-Compliant Configurations

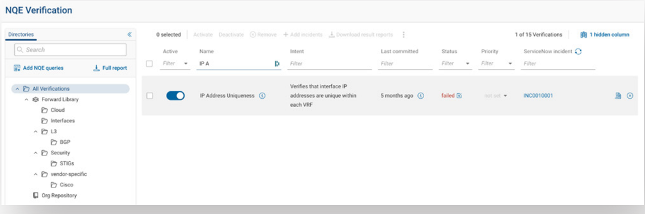
NQE parses raw device data and displays it in a normalized format, allowing engineers to identify misconfigurations and policy violations in seconds—without manual data wrangling.

3. Create Automated Intent Checks

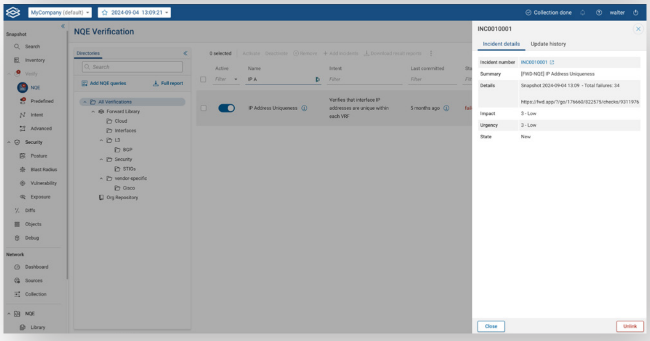
Once verified, any query can be turned into an intent check to enforce policy continuously. For example, teams can be alerted anytime firewall rules are modified in a way that violates compliance controls. These continuous checks not only streamline audit readiness but also reduce cybersecurity risk by ensuring that misconfigurations or policy violations are detected and addressed before they can be exploited.



Active	Name	Intent	Last committed	Status
Filter	Filter	Filter	Filter	Filter
●	Default VPC Security G ...	Verifies that the default security group of every VPC restricts all traffic	2 years ago	passed
●	Prevent Unfettered RDF ...	Verifies that no security groups allow ingress from 0.0.0.0/0 to port ...	8 months ago	passed
●	Prevent Unfettered SSH ...	Verifies that no security groups allow ingress from 0.0.0.0/0 to port 22	8 months ago	passed
●	Interface Status Query ...	Verifies that all admin-up interfaces are oper-up	2 years ago	failed
●	Interfaces Have Descri ...	Verifies that connected interfaces have descriptions	2 years ago	failed
○	IP Address Uniqueness ...	Verifies that interface IP addresses are unique within each VRF	5 months ago	inactive
●	Link Speed Consistenc ...	Verifies that interfaces both ends of each link have the same link ...	1 month ago	failed



Active	Name	Intent	Last committed	Status	Priority	ServiceNow incident
Filter	IP A	Filter	Filter	Filter	Filter	Filter
●	IP Address Uniqueness	Verifies that interface IP addresses are unique within each VRF	5 months ago	failed	not set	INC0010001



Incident number	INC0010001
Summary	[FWD-NQE] IP Address Uniqueness
Details	Snapshot 2024-09-04 13:09 - Total failures: 34 https://fwd.app/?/go/176660/822575/checks/9311976
Impact	3 - Low
Urgency	3 - Low
State	New

4. Integrate with Collaboration and ITSM Tools

Forward integrates with platforms like Slack, Microsoft Teams, Webex, and ServiceNow to escalate alerts, open tickets, and keep audit stakeholders aligned—all using a shared, validated data source.

Audit Confidence and Cost Savings

With rich, continuously updated network snapshots, compliance teams can prove adherence to regulatory controls at any point in time—whether for internal audits, regulator inquiries, or board reporting. Forward Enterprise eliminates the guesswork and last-minute scramble of traditional audit preparation. It closes compliance gaps before they form and gives IT leadership the assurance that they can respond to audits quickly, accurately, and confidently.

> “*Our IT department is obligated to communicate with regulators. Forward Networks helps us by delivering data that shows we comply with various regulations. We would need to hire one or two additional FTEs to replace this functionality.”*
>
> **FINANCIAL SERVICES EXECUTIVE**

> “*We were unable to comply with regulatory requirements until we implemented Forward Networks. Without it, we would have needed to double or triple our team size to remain compliant.”*
>
> **LEADER IN FINANCIAL TECHNOLOGY**

> “*We're able to avoid a number of audit items because we can provide compliance information with certainty and validate remediation progress. We can demonstrate to auditors that we have validated, real-time information.”*
>
> **FINANCIAL SERVICES CUSTOMER**

Together, these benefits translate into fewer audit findings, reduced staffing costs, and the confidence to face regulators and auditors with real-time, verifiable compliance data.

Why Forward Networks

Forward Networks is pioneering the networking digital twin, transforming how the world's largest organizations manage and secure their infrastructure. Forward Enterprise delivers customers an average of $14.2 million in annual benefits by enhancing staff productivity, preventing unplanned downtime, and improving operational efficiency. It creates a mathematically precise digital replica of the entire hybrid, multi-cloud network, modeling every device, configuration, and possible path from L2 through L7.

This single source of truth gives NOC, Cloud, and SOC teams unmatched visibility and verification capabilities, ensuring security policies are enforced, compliance is maintained, and the network operates reliably. By collecting and analyzing configuration and state data across all major networking vendors and cloud providers—including AWS, Azure, and Google Cloud Platform—Forward Enterprise simplifies critical but tedious tasks that traditionally drain resources and introduce risk.

Trusted by Fortune 100 enterprises and federal agencies, Forward Networks empowers organizations to reduce risk, streamline compliance, and prepare their infrastructure for the demands of AI and the next wave of digital transformation. Learn more at www.forwardnetworks.com.

ABOUT FORWARD NETWORKS

Forward Networks is revolutionizing the way large networks are managed. The Forward Enterprise platform delivers a vendor-agnostic “digital twin” of the network, based on a mathematical model. The platform scales to support hundreds of thousands of network devices, whether cloud, hybrid cloud, or on-prem. It serves as a single source of truth for the network, enabling network operators to instantly verify security posture, accelerate troubleshooting, avoid outages, and modernize network management.

Over the past few years, Forward Networks has received tremendous industry recognition, including “Cool Vendor in Enterprise Networking” by Gartner and “Product of the Year” by Cloud Computing, and has been named to Fortune Magazine’s 2024 Cyber 60 as well as Fortune’s 2024 “Best Workplaces in the Bay Area” list.

The company was founded by four Stanford PhD graduates who saw a massive opportunity to improve network operations. Investors include Andreessen Horowitz, Threshold Ventures, and Goldman Sachs.