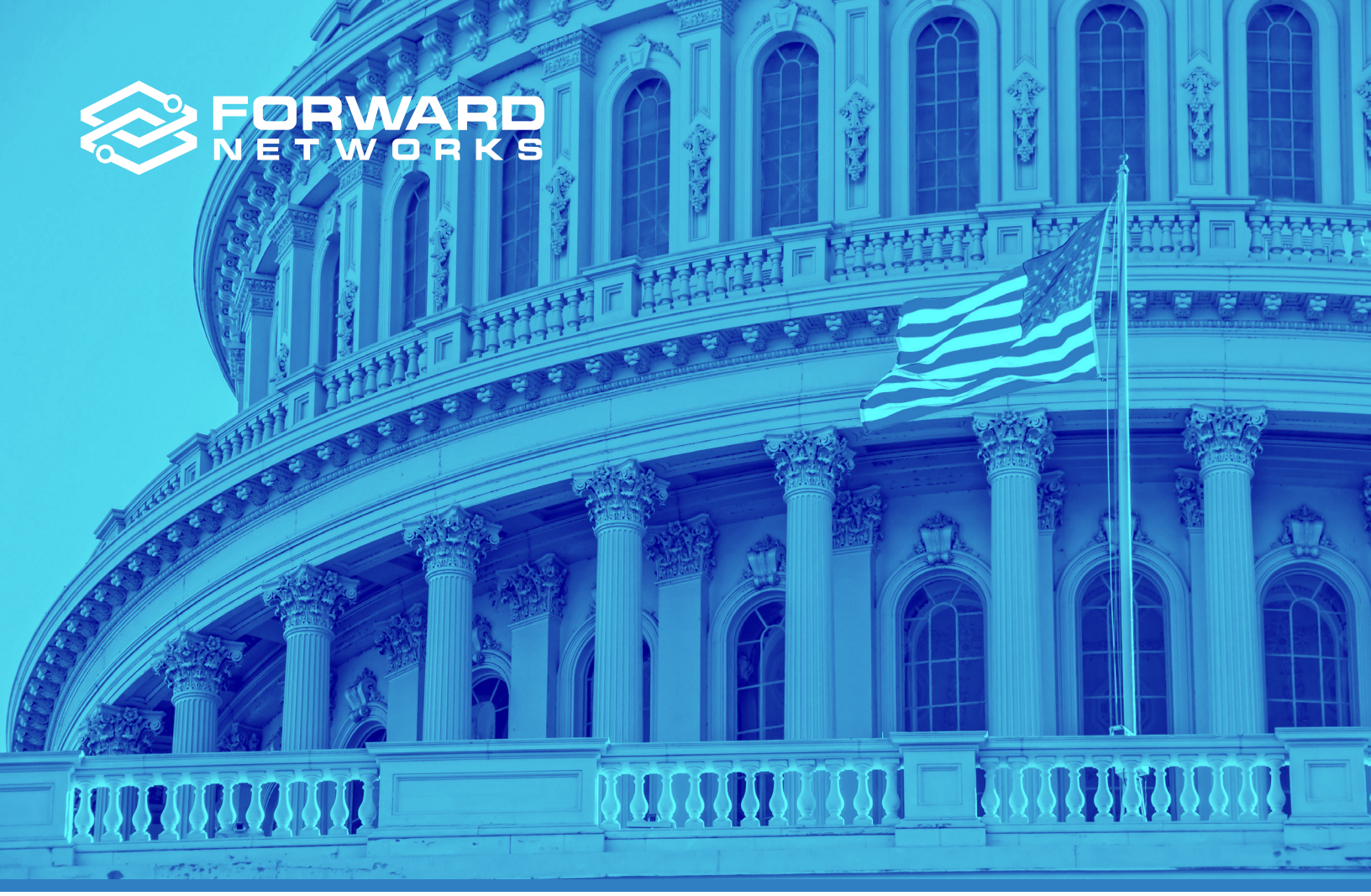


CASE STUDY

Solving Complex Network Challenges with Forward Networks When Lives Hang in the Balance

The customer, a federal organization responsible for ensuring the safety of U.S. citizens and the world at large, relies on vast amounts of data to fulfill its mission and ensure the safety of its employees.

The Challenge

The network is the backbone of the organization and essential to its mission, safeguarding national security and conducting field operations. When lives are on the line, it's paramount that the network delivers:

RELIABILITY: Ensuring seamless communication between global operations, people in the field, and policymakers, even in the most challenging environments. In this context, outages endanger lives.

SECURITY: Protecting classified data from cyber threats, unauthorized access, and adversarial interference is paramount to maintaining operational integrity and national security.

SCALABILITY AND AGILITY: Supporting a wide range of operations, from real-time intelligence gathering to large-scale data analysis, often requiring rapid adaptation to evolving global threats.

Without a resilient, secure, and agile network, the mission-critical functions of such an organization would be significantly hindered, exposing vulnerabilities and compromising national safety.

The Challenge

Like many large organizations, this agency faced the challenges of managing an expansive and complex network. Their network consisted of devices across different life stages, from newly deployed to end-of-life, and varied security statuses ranging from fully patched to vulnerable. Two critical priorities—Recapitalization/Refresh and Vulnerability Management—were falling behind their high standards because it was nearly impossible to prioritize efforts and ensure nothing was missed. Traditional network and security tools proved insufficient for their efforts. What they needed was a comprehensive data platform capable of aggregating network information and delivering intuitive, actionable results that could easily be shared across the team.

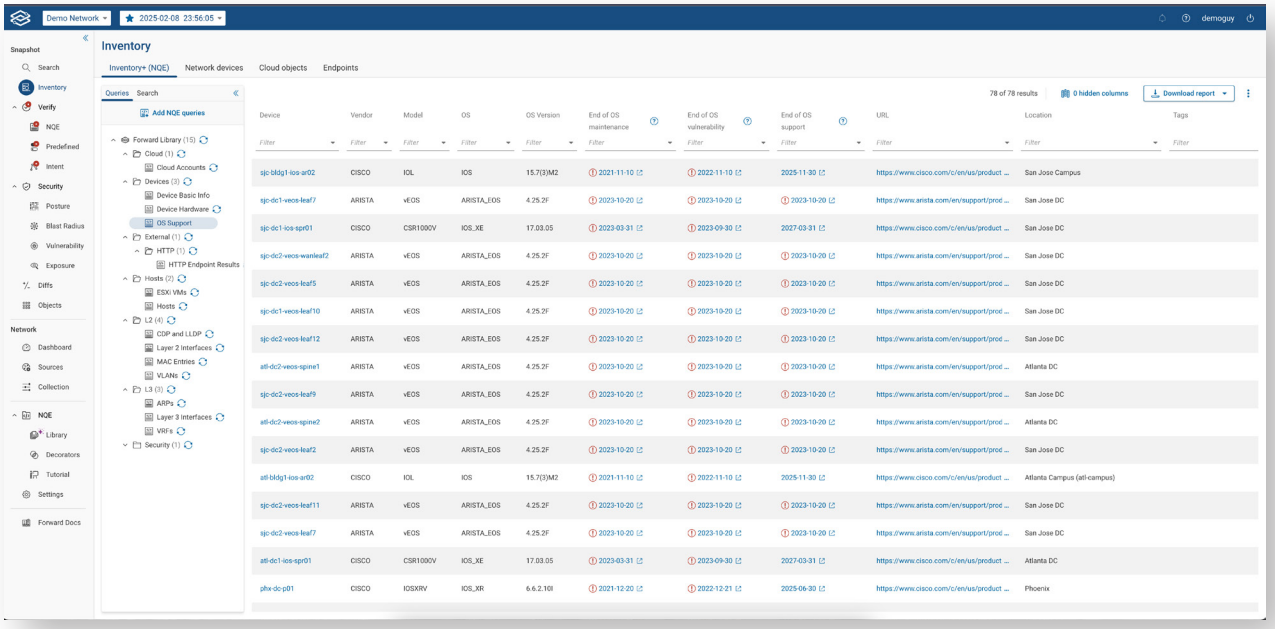
The Selection Process

A key leader summarized their requirements succinctly: "If a solution can tell me where to focus my effort and spending to maximize my results, I'll leverage it everywhere." In an effort to replace their existing solution, they evaluated several vendors. Forward Networks' digital twin technology emerged as the clear leader due to its superior data aggregation, analysis, and actionable insights. Unlike RedSeal, which relies primarily on configuration-based attack surface management and visualization, Forward Networks provides a mathematically accurate model of the network, capturing both state and configuration data. This capability ensures the data is always accurate down to exact configuration code within the devices, enabling the agency to make informed, impactful decisions while ensuring their efforts are focused and efficient.

The Solution

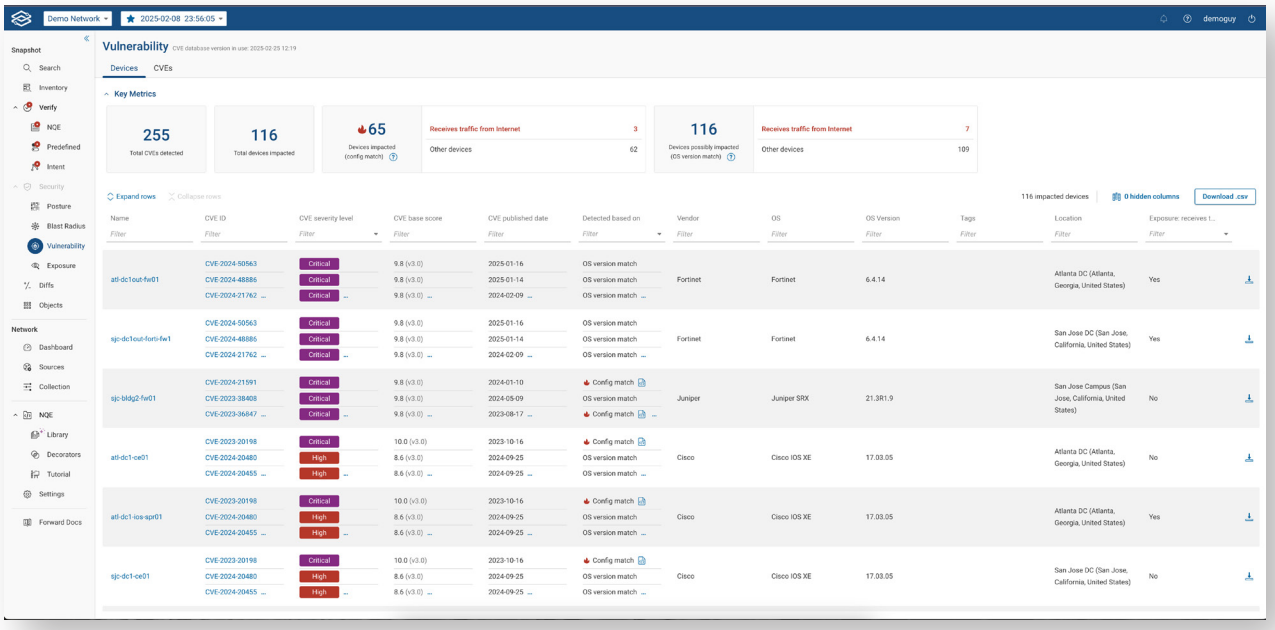
The Forward Enterprise network digital twin delivered on their requirements by providing a unified repository spanning multiple separate enclaves and offering:

COMPREHENSIVE PRIORITIZATION:
Automatically prioritizing device refresh based on aggregated data from all devices at a given location across all enclaves.



ADVANCED VULNERABILITY MANAGEMENT:

Delivering the most comprehensive CVE management solution available. The platform integrates with NIST and vendor databases and combines that information with the configuration and state data collected by the platform to deliver a customized list of vulnerabilities present in the network according to devices, features, and OS. This data is delivered in an exportable, prioritized remediation plan with vulnerabilities ranked by severity and exposure.



FLEXIBLE DATA INTEGRATION:

Consuming data from various sources, including CMDB, IPAM, custom APIs, and command-line interfaces.

API ACCESSIBILITY:

Exposing all collected data via APIs for seamless integration into business intelligence platforms, enabling holistic risk assessment and funding prioritization.

Aggregating Data with Precision

Forward Networks offered two key capabilities that directly addressed the agency's needs:

ALWAYS-CURRENT CUSTOM SOURCES:
The platform's ability to configure the collection of nearly any API or CLI allowed the agency to integrate data from disparate systems, including spreadsheets stored in S3.

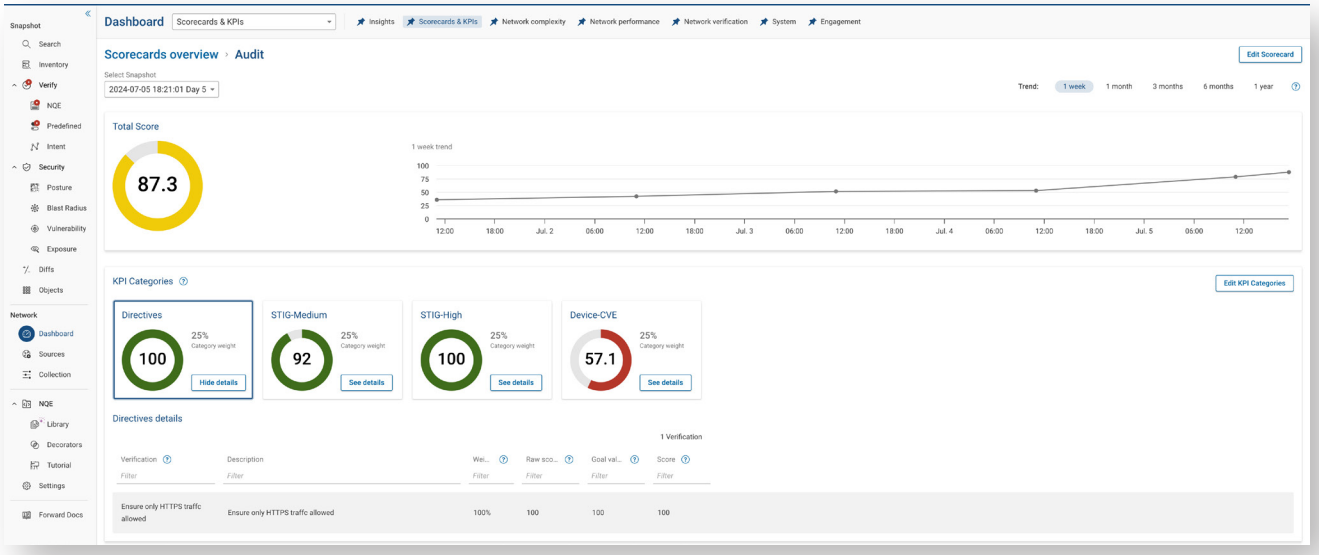
PORTABLE SNAPSHOTS:
The agency leveraged Forward's portable snapshots to merge data from isolated networks into a single Forward instance, creating an enterprise-wide view. This capability, combined with native CVE and End-of-Life (EoL) data, enabled the agency to prioritize network refresh efforts effectively across its entire infrastructure.

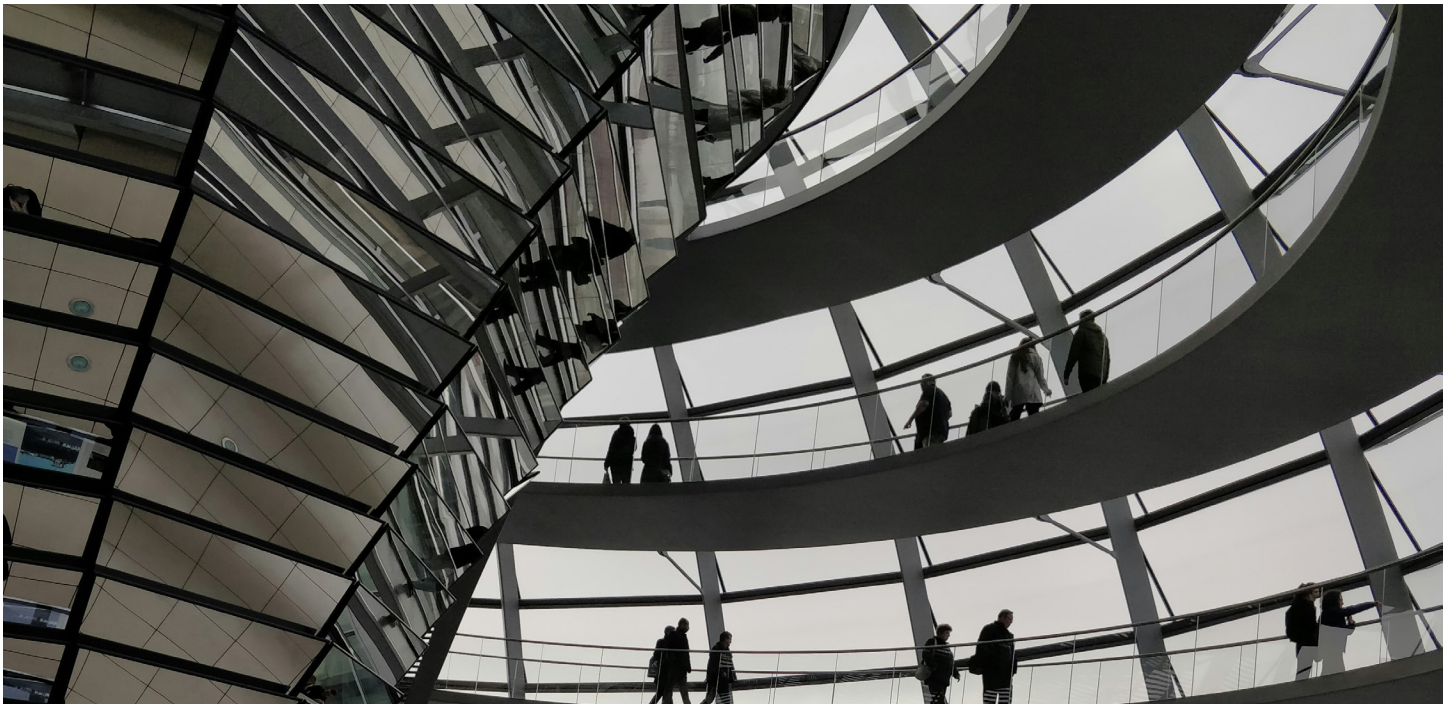
By comparison, RedSeal's reliance on static configuration data and limited state analysis left gaps in visibility and operational accuracy, making Forward Networks the more robust solution.

Exposing Actionable Insights

With Forward Networks, the agency consolidated all network data into a single platform. This allowed them to:

- Extract actionable insights for use in business intelligence platforms.
- Enumerate mission-critical risks and allocate time and funding where they would deliver maximum impact.
- Utilize snapshot comparison capabilities for trending analysis, forensic investigations, and configuration validation.





Expanding Use Cases

Because Forward Enterprise was able to deliver on the requirement of focusing time and spending, the agency leadership is looking to extend its use cases. The initial success with Forward Networks led other teams within the agency to adopt the platform for their specific needs:

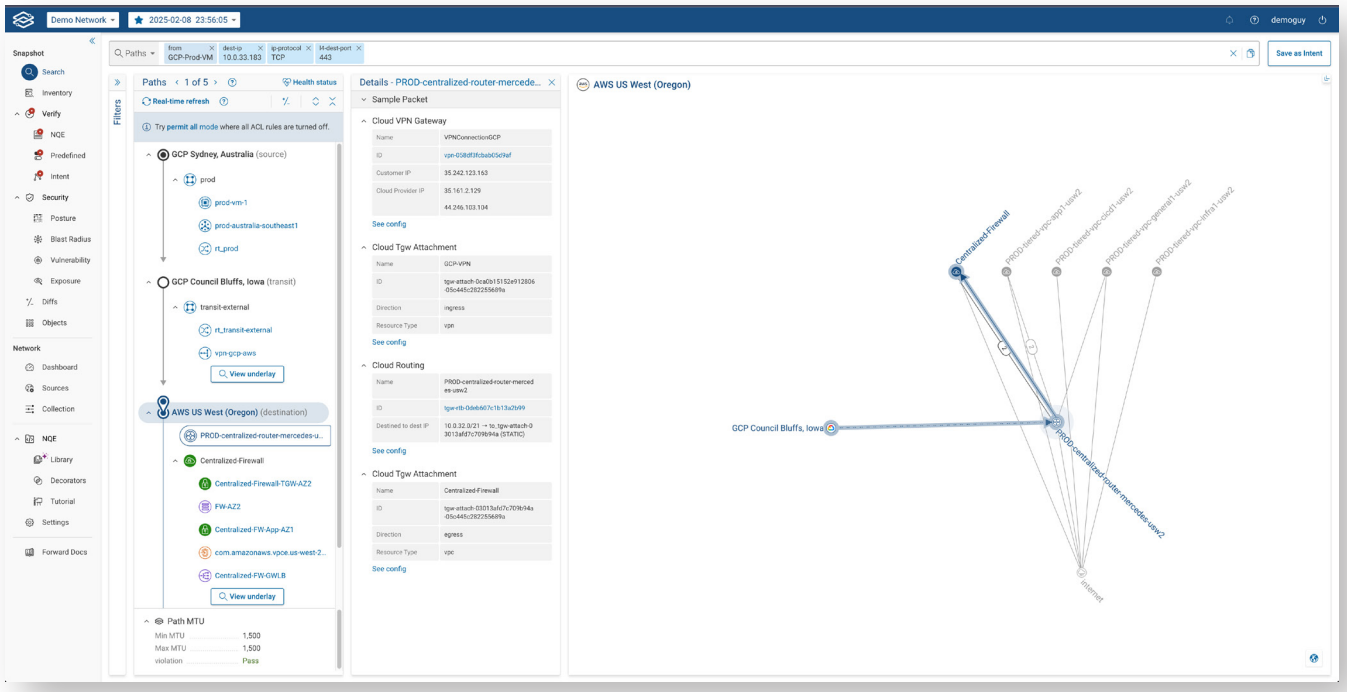
CONFIGURATION MANAGEMENT:
Automatically feeding accurate, up-to-date data into the CMDB with every new collection.

CYBERSECURITY TEAMS:
Leveraging the platform's wealth of data for threat hunting and enhanced defense strategies, supported by Forward's sophisticated mathematical model.

OPERATIONAL EFFICIENCY:
Utilizing thousands of built-in best practices, data calls, and health checks to proactively identify and resolve network issues, generating trouble tickets automatically.

Hybrid Cloud Extension

The agency is now extending Forward Networks' capabilities to its hybrid cloud environments, including AWS, GCP, and Azure. Unlike RedSeal, which offers limited cloud visibility, Forward provides hop-by-hop path analysis from on-premises networks through the cloud to the internet. This unified view enhances security policy enforcement and reduces costs, delivering a single pane of glass for managing the entire hybrid, multi-cloud network.



Looking Forward

Forward Networks has enabled this Global Federal Agency to transform its approach to network management and security. By offering unparalleled visibility, actionable insights, and seamless integration across systems, Forward Networks has proven to be a critical partner in achieving the agency's mission. The scalability and flexibility of the platform continue to drive innovation and efficiency, making Forward Networks the superior choice over RedSeal for solving complex network challenges.

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 2025 "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.