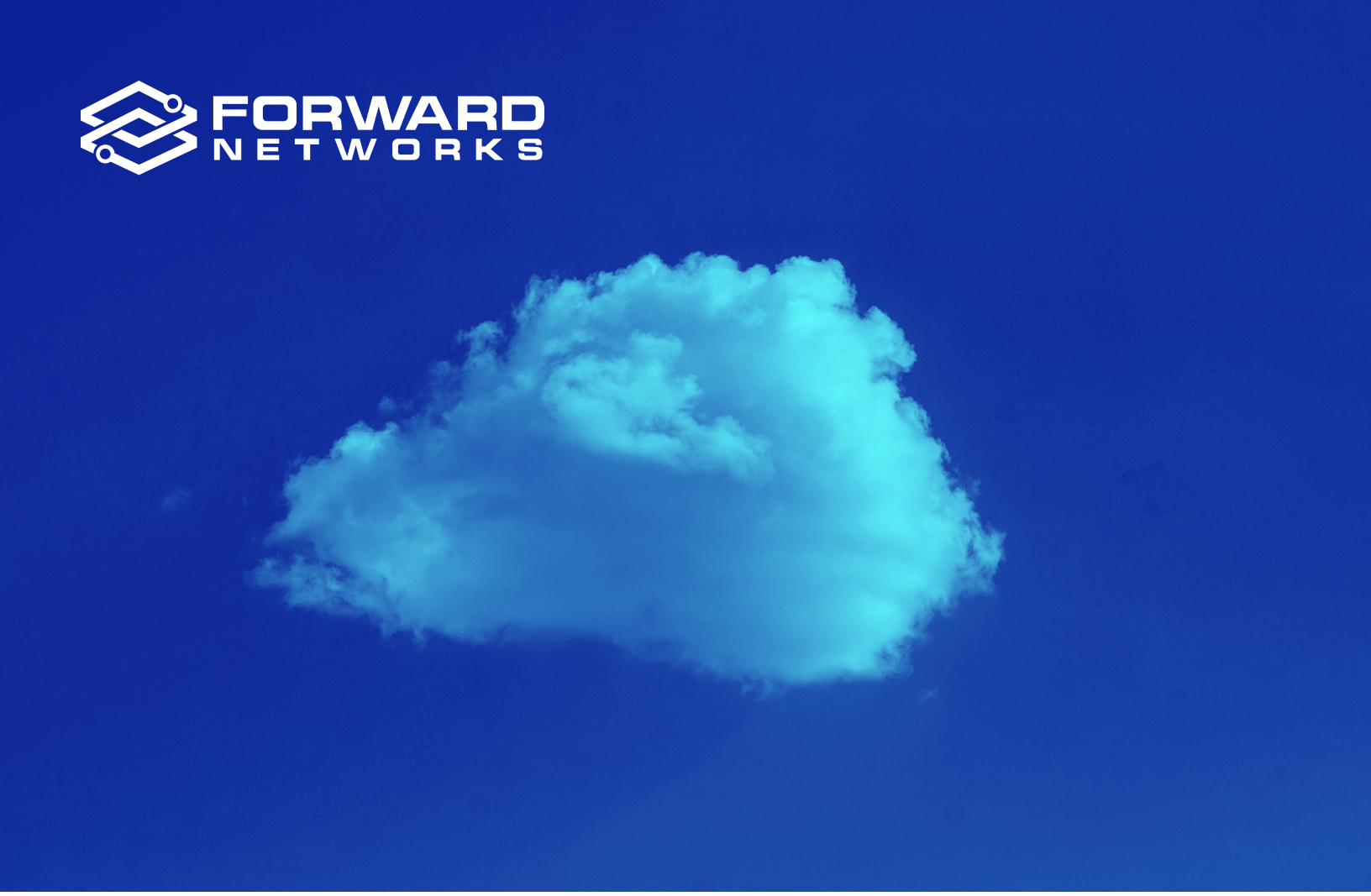
FORWARD NETWORKS



USE CASE

# Verify Security Policies in the Cloud with Confidence

# Visibility That Can Uncover Otherwise Undetected Agency Risks

As workloads move to and between clouds, agencies need to continually verify whether security policies are being effectively executed. Despite the scalability and agility that the cloud delivers, moving to the cloud often comes with unpredictable costs, enhanced complexity, and increased difficulty enforcing security policies.

Hybrid cloud has become the de facto strategy for agencies needing to scale mission-ready services while keeping sensitive workloads on-premises to meet security and regulatory mandates. Cloud Smart policies are providing more options for hybrid clouds, such as blueprints for deploying shared and unique private clouds in various combinations. Whatever strategy your agency is pursuing, the need to manage across on-premises and cloud platforms, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure, is fundamental to everyday operations within federal agencies.

A standard configuration to maintain security policies seems simple but rationalizing and validating traffic flows – from on-premises to the cloud and intercloud – can be almost impossible without full visibility. The tools used by network and security operations to validate on-premises or cloud connectivity and security are different from those used for cloud. Each cloud provider also has its own terminology, methodology, visualization, and toolset (see Figure 1). The release of new services and features further complicates the picture, making it even harder for teams to understand flow visibility. Deploying traditional security controls proves ineffective in this complex environment since defensible perimeters are erased, component virtualization and decentralization obscures visibility, and automated configuration tools are required at scale.

| | L2 | L3 | ACCESS CONTROL (STATEFUL) | ACCESS CONTROL (STATELESS) | EXTERNAL CONNECTIVITY | TROUBLE-SHOOTING |
|---|---|---|---|---|---|---|
| **On-Prem Networking** | Traditional Network Switches and Overlays | Traditional Routing protocols (BGP/ OSPF/ISIS/etc) | Traditional Firewalls | ACLs/Firewall Rules | BGP connection + firewalls | Ping/traceroute |
| **Amazon Web Services (AWS)** | VPC Subnet (native L2) | Route tables and Peering (BGP optional) | Security Groups/ AWS Network Firewall | Network ACLs | Transit Gateway/ VPN Gateway/ Internet Gateway | VPC Reachability Analyzer |
| **Google Cloud Platform (GCP)** | GCP Subnet | Cloud Router and Peering (BGP optional) | GCP Firewall | GCP Firewall | NCC/VPN Gateway/ NAT Gateway | GCP Connectivity Test |
| **Microsoft Azure** | VNET Subnet | Route Serve/ Route Tables | Network Security Groups | Azure Firewall | Virtual WAN/VPN Gateway | Azure Network Watcher |

*Figure 1: Securing a hybrid multi-cloud environment is complex due to differing protocols and processes*

# A Unified Approach to Verifying Security Posture in the Cloud

An inflection point has been reached where already stretched IT resources need a new approach to more efficiently navigate the silos, different operational dynamics, and growing toolsets around agency cloud environments. A grade of C- from U.S. Senate investigators on the Homeland Security Committee for failing to implement basic safeguards against cyberattacks underscores the urgency to find a better approach to ensure consistent governance and security across on-premises and cloud estates.
There's a better way to understand how networks behave. The first step is gaining visibility.

With Forward Networks' multi-vendor network model, agencies can use a mathematically accurate network digital twin of the agency's physical, virtual, and cloud networks to understand their cloud environment. Forward Enterprise delivers complete visibility into all possible traffic paths with automated analysis to scale the complexity of federal environments to instantly verify security policies and quickly identify misconfigurations.

Using a digital twin, network, security, and cloud teams can take a holistic and more proactive approach to enforce security policies and verify compliance with cloud security postures. Forward Networks provides:

- A single source of truth for complete visibility across on-premises and multiple clouds
- Automated intent checks to instantly verify the compliance of cloud security policies
- Zone-to-zone connectivity matrix to provide insight into the agency's security posture at a glance

# SINGLE SOURCE OF TRUTH FOR COMPLETE VISIBILITY

The Forward Enterprise platform unifies visibility across distributed, hybrid agency environments. Network engineers can now visualize on-premises data centers, private and public clouds (AWS, GCP, and Microsoft Azure), and high-side and low-side environments in a single, easy-to-navigate view. By gathering and normalizing data into an intuitive digital twin, the platform helps make sense of the cloud estate so that agency teams can see that the same policies used on-premises are being enforced in the cloud.

Figure 2 shows how network, security, and cloud teams can use a network digital twin for clutter-free navigation that cuts through silos and drills down into specific pathways or scales to view the environment and understand connectivity holistically.

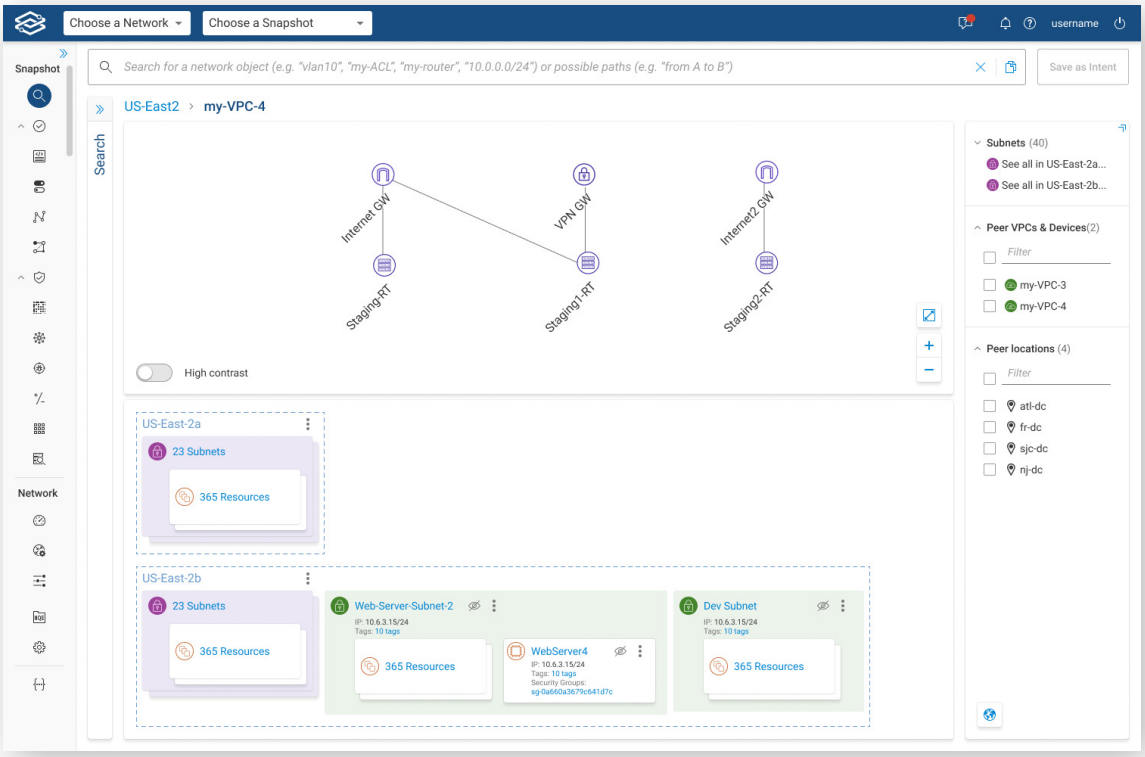



*Figure 2: Normalized view of virtual private clouds within Forward Enterprise*

For more detail about a specific element within the network, such as a cloud platform, a click on that element provides this information. For example, clicking on a platform from a major cloud provider could show four virtual private cloud instances (VPCs), one transit VPC, and several subnets related to that platform (see Figure 3).

And if at any time visibility is needed into which cloud platforms Forward Enterprise is pulling and collecting this data from, click on “Cloud Objects” in the Cloud Security Posture Management (CSPM) dashboard to see all the details.

Forward Networks collects configuration and state data from all on-premises devices, such as routers, switches, and firewalls, and uses publicly available APIs to gather similar read-only information from various cloud accounts to create a network digital twin that incorporates physical, virtual, and cloud estates. Forward Enterprise needs only a basic set of API connectivity to access the data required to model and visualize all possible traffic paths in specified cloud environments. All permissions used to collect data are read-only (see Figure 4).

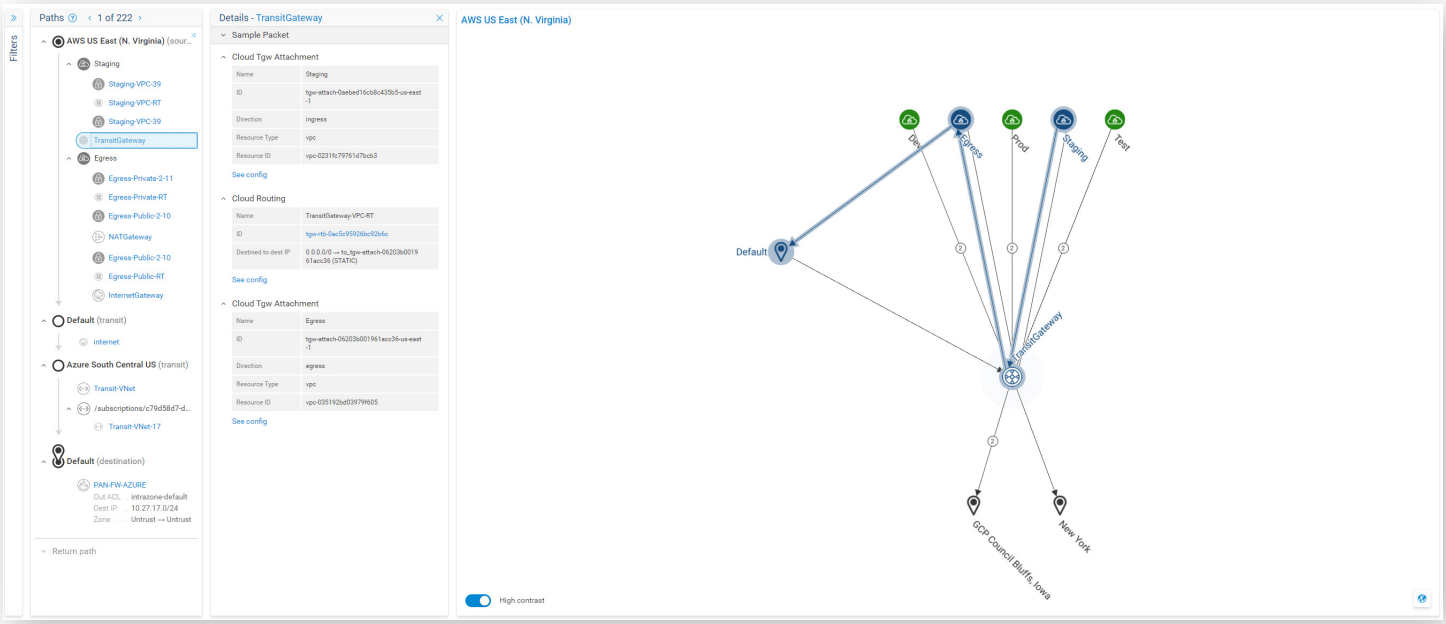



*Figure 3: Detailed view of cloud resources*

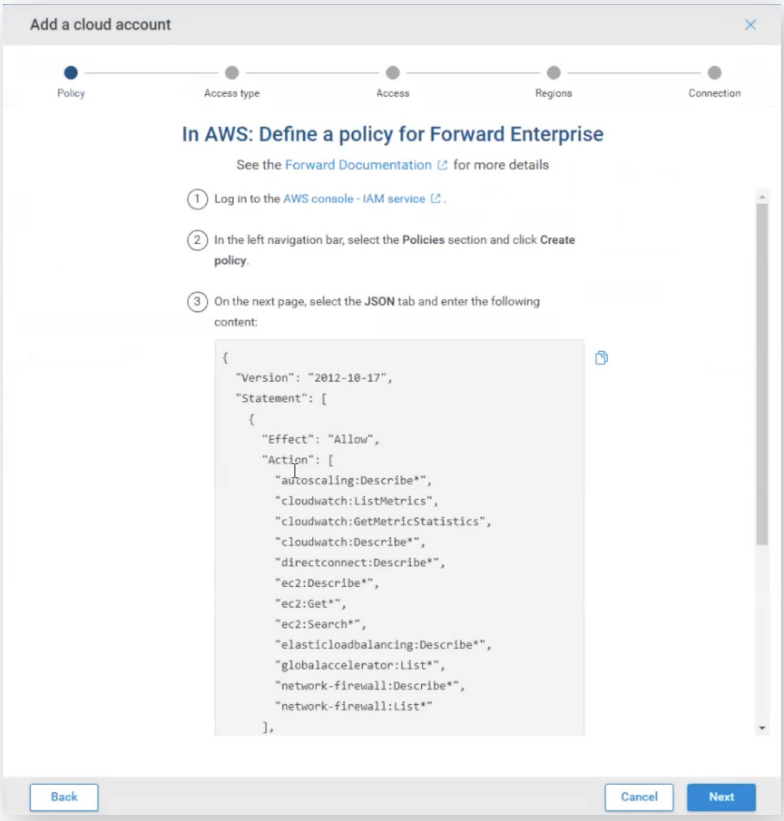



*Figure 4: Required permissions for snapshot collection*

# Automated Intent Checks Instantly Verify Compliance of Security Policies in the Cloud

Forward Enterprise's mathematical model normalizes disparate data across agency estates and creates a digital twin for exhaustive analysis and verification of current network behaviors. The digital twin simplifies and augments CSPM efforts by allowing automated verification checks in the cloud to prove that safeguards remain in place for sensitive workflows. This allows network and security teams to move away from time-consuming manual processes while maintaining compliance with zero trust security and DISA STIGS.

Agencies can jump-start verification using Forward Enterprise's library of intent checks. Or teams can customize intent checks for a specific mandate, such as validating zero trust, that will run in an automated fashion and ensure permanent compliance of agency security policies in the cloud. Mathematically certain documentation proves that all traffic flows are going through authorized security chokepoints to continuously enforce barriers between segmented, mission-critical networks.

Anytime a non-compliant change is detected within the cloud estate, the appropriate teams will receive specific, actionable information about which instantiation is non-compliant and why. This enables rapid resolution. Intent checks can also be used to identify costly routing errors with mathematically certain proof for accountability.

Furthermore, Forward Enterprise supports regular data collection that creates stored network snapshots, allowing teams to see exactly what changes occurred over a specified period of time. These snapshot collections provide an always up-to-date forensic audit tool in the case of a security event.

## Zone-to-Zone Connectivity Matrix to Validate Agency Security Postures at a Glance

Given the unique mission and security requirements of many federal agencies, the ability to instantly assess true, up-to-date connectivity across estates can enable more proactive protection of sensitive work like workloads with CUI or PII or warfighter and classified operations where critical network barriers must be enforced for complete isolation.

Forward Enterprise supports CSPM efforts by providing a visual connectivity matrix, including any hybrid connectivity (e.g., a virtual firewall) that may have been set up in cloud platforms, but it's more than just a firewall manager. Forward Enterprise provides a complete view of the entire network estate. Up-to-date connectivity details are provided for all IP addresses, ports, and protocols between sites identified as key bases, communities of interest (COI), and data centers in the network that includes NATs and tunneling.

At a glance, IT security, network, and cloud managers gain the ability to drill down into specific rules between any zones, regions, sites, and subnets. They can examine connectivity to see whether the activity is permitted between the various zones and set up intent checks to continuously verify that desired security controls are working as intended. If something changes, actionable alerts are automatically sent about non-compliance with security policies (see Figure 5), proving the segmentation of high-side networks or individual applications that require isolation protection.

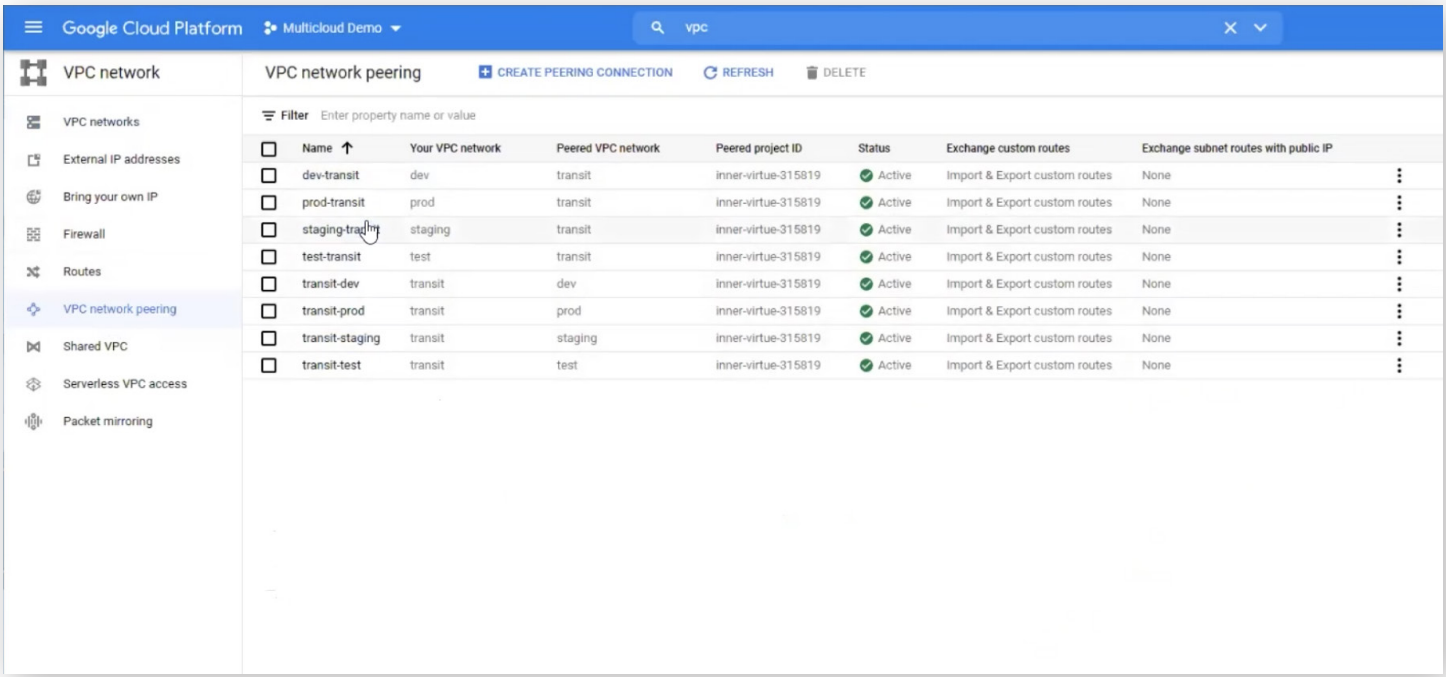



*Figure 5: Cloud zone security matrix*

# A Single Source of Truth for Your On-Premises, Hybrid, and Multi-Cloud Estate

Forward Networks' mathematical model creates a complete and always current digital twin of your physical, virtual, and multi-cloud network estate, including config and state information for all network elements and your hybrid or multi-cloud environment. The digital twin provides a comprehensive view of all network behavior with visibility into every possible path a packet can take. It brings mathematical certainty to network security validations by enabling security operations teams to:

**VISUALIZE** network layer 2 – 4 topology and all possible traffic paths within a single pane of glass including on-premises, Cloud (AWS, GCP, and Microsoft Azure), and virtualized environments. Then, drill down to specific devices and traffic flows, including configuration and state data. View the global network in a single view or drill down to a single device.

**SEARCH** the entire estate as simply as a database. Our browser-like search feature performs the industry's most in-depth, complete end-to-end path analyses across the network for both on-premises and cloud infrastructure. This also enables you to locate devices and access detailed information on their location, configuration, and state in milliseconds.

**VERIFY** that the security policies are extended to the cloud using purpose-built (custom) intent checks. Forward Enterprise offers the most advanced network segmentation tool available with support for multi-vendor on-prem, hybrid cloud, and multi-cloud environments. Continuously audit the network and receive actionable alerts for non-compliance with your security policies. Know that applications are compliant before provisioning them.

**COMPARE** network changes over time to understand their impact on the network and prevent incidents from reoccurring. The network collector frequently scans the network, taking and saving network configurations, topology, and device state snapshots. These "snapshots" become a searchable historical record of network behavior and compliance at any point in time. And the behavior diffs feature makes it easy to quickly find and compare snapshots to identify changes that may violate your security policy.

# Explore All Aspects of Your Compute Environment With Forward Enterprise

Are you seeking a more proactive stance without adding additional specialized expertise? See how the Forward Enterprise digital twin can help your agency network and security teams monitor and verify estate-wide controls through a single pane of glass and explore any object in the cloud environment to ensure everything is working as intended. Regardless of which cloud strategy is most important for your agency, keeping data safe and meeting zero trust mandates will depend on understanding what's in the full agency network estate and how connectivity behavior can be visualized to keep connections safe.

Learn more at forwardnetworks.com/cloud. To see the Cloud Smart feature and the power of a network digital twin in action, watch the Forward Cloud video. Request a personal demo today, contact us at forwardnetworks.com/federal.

## ABOUT FORWARD NETWORKS

Forward Networks' mission is to de-risk and accelerate network operations by increasing efficiency, reducing outages, and verifying network intent. Built on a series of breakthrough algorithms, the Forward Platform provides enhanced network visibility, policy verification, and change modeling for legacy, SDN, or hybrid environments.

Forward Networks is headquartered in Santa Clara, California, and funded by top-tier investors, including Andreessen Horowitz, DFJ, A.Capital, SV Angel, and several luminaries in the networking and systems space.