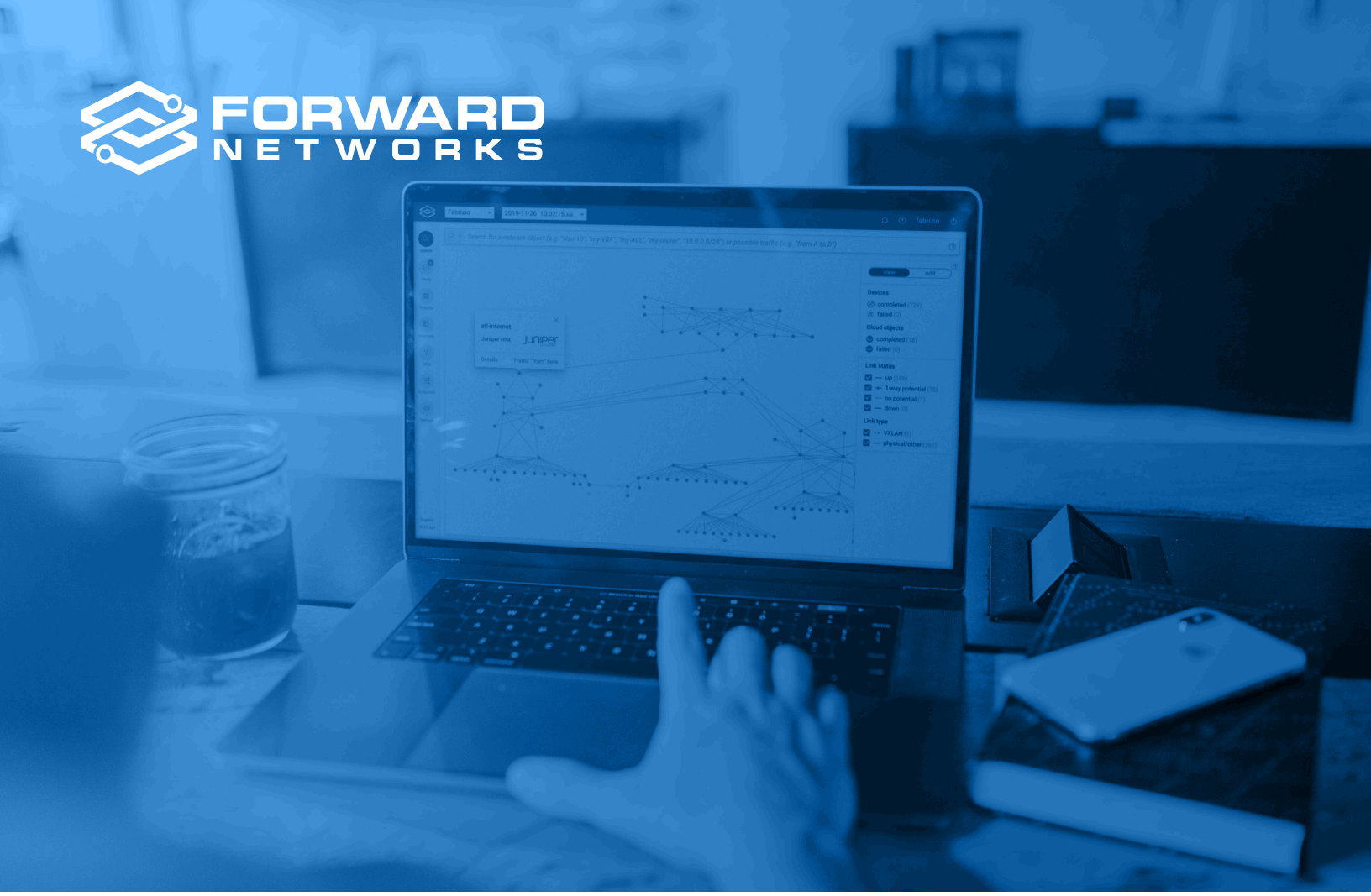
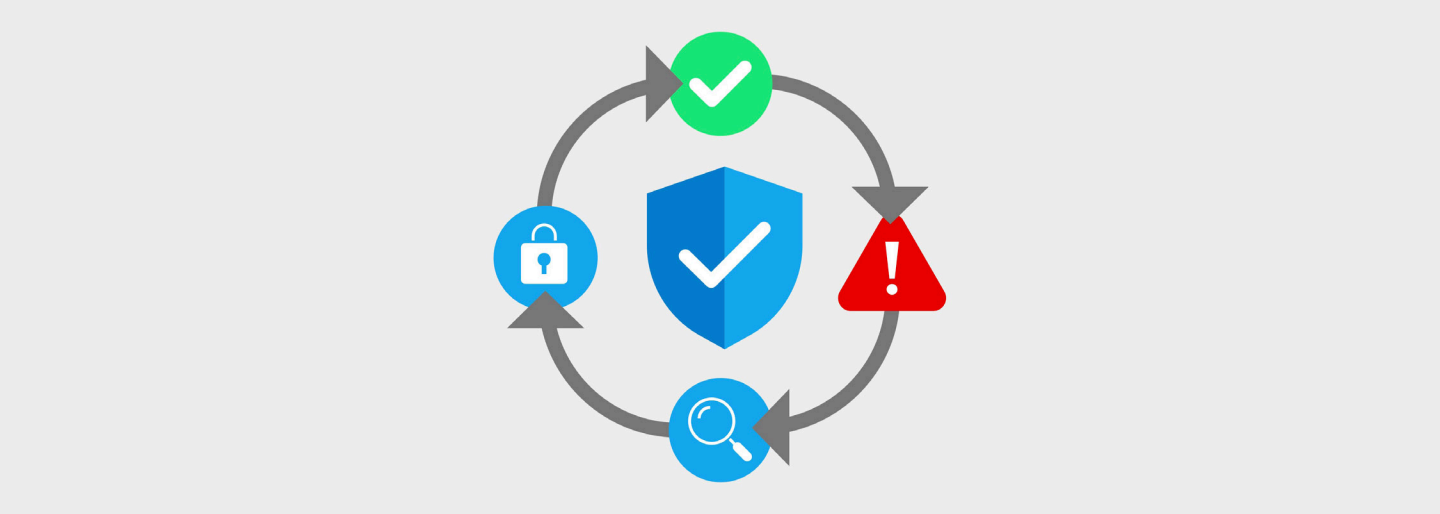
FORWARD NETWORKS



USE CASE

Automated Secure Application Provisioning



Businesses are developing and deploying applications at an increasingly rapid pace in a quest to deliver the best customer experience. At the same time, network and security operations teams struggle to securely provision these applications as it is typically a time-consuming and labor-intensive process. Manually verifying that new applications adhere to security policies before deployment often takes days, or weeks. That slows down the business and frustrates users — worse yet, security risks still slip through the cracks.

When provisioning new applications, security teams rely on their SecOps playbook (or security matrix) to determine what security and network connectivity policies to apply to every new application or device added to the enterprise network. Forward Enterprise curates firewall security rules in an easy-to-read matrix that enables rapid compliance assessment.

Empower Developers to Conduct Intent Checks and Enable Continuous Monitoring

Many malicious actors specifically target security vulnerabilities in applications to launch their attacks. So, it's essential for businesses to streamline the process and reduce the potential for errors when verifying that new applications adhere to security policies prior to provisioning. An effective solution that can ease the burden on network and security teams and improve accuracy in the verification process is to give application developers a self- service tool for verifying that applications are compliant.

Using Forward Enterprise, rather than examine each prospective application individually, security teams can write an intent check to automatically ensure that the application is within policy. Once the intent check is written, the application development team can use the automated intent check as a self-service verification that their application meets security policy connectivity guidelines. So, if their application:

- **Passes the intent check**, confirming that all appropriate security and networking connectivity policies are in place and working as intended, they can deploy the app confidently and without delay.

- **Fails the intent check**, indicating that the security policies need to be updated. Developers will get information on why the application failed the security check enabling them to quickly adjust the application.

Automated secure application provisioning in Forward Enterprise helps speed up the deployment of secure apps by automating policy checks and helping teams to pinpoint and quickly remediate issues. Developers don't need to have advanced networking knowledge to verify that their application is in-policy; in fact, they can use a Slack Bot to perform the check thanks to the Forward Enterprise API integration.

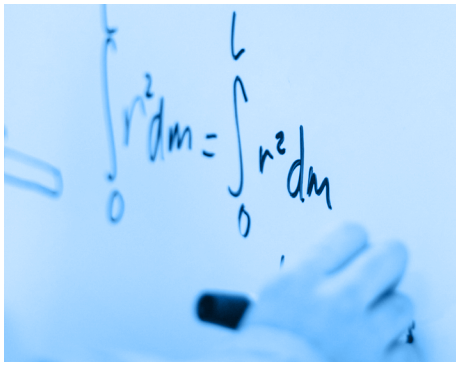
Deploy New Apps and Services Faster — Without the Need to Expand Teams

Automated secure application provisioning in the Forward Enterprise platform not only reduces the burden that network and security teams face when receiving many tickets, but it also allows application developers to perform their role much more efficiently. One customer we work with told us this functionality enabled them to launch a new credit card business in 3 months vs 1 year.

Forward Enterprise identifies all potential traffic paths for the new application across the entire network which includes tens of thousands of devices. The customer combined the Forward API with custom internal software which is used to securely update impacted firewalls. Policy compliance and a correct deployment for all new flows is guaranteed and there is no delay between when application developer flows are requested and approved.

> We haven't added people, but we've been able to grow the scope of our operations. Deploying a new business unit at this speed would have required many, many, many bodies — and without Forward Enterprise, it would've been impossible.
>
> Forward Networks Customer

Verify Your Security Posture With Mathematical Certainty



Forward Networks is the industry leader in network assurance and intent-based verification. Our mathematical model creates a complete and always-current digital twin of your physical, virtual, and cloud network estate, including config and state information for all devices.

The digital twin provides a complete view of all network behavior, with visibility into every possible path in your network. It brings mathematical certainty to verifying zone-to-zone connectivity and security postures for applications and devices by enabling network and security teams to:

VISUALIZE network layer 2 – 4 topology and all possible traffic paths within a single-pane view for on-premises, cloud (AWS, Microsoft Azure, and Google Cloud Platform), and virtualized environments. Then, drill down to specific devices and traffic flows, including configuration and state data.

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

VERIFY that the security controls in the network are working as intended by using purpose-built (custom) intent checks. Continuously audit the network and receive actionable alerts for noncompliance with your security policies.

PREDICT the effect of proposed changes so that you can deploy updates without the fear of unintended connectivity changes by using the network digital twin as a sandbox.

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 snapshots of network configurations, topology, and device state. 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.

See for yourself how automated secure application provisioning in Forward Enterprise can help you expedite the app deployment cycle, while also reducing security risks for your users — and your organization — through continuous monitoring and validation of the app's security posture post-deployment, including adherence to zero trust policy. For a first hand look at how Forward Enterprise can enhance your security posture, request a personal demo.

Getting Started With Forward Networks

Are you ready to deliver new capabilities through the network, reduce outages, enhance security, and save time?

Request a personal demo ›

FORWARD NETWORKS

www.forwardnetworks.com