



ESG WHITE PAPER

Forward Networks: The Power of Visibility

How a Network Digital Twin Drives Agility, Security, and Availability

By **Bob Laliberte**, Senior Analyst; and **Leah Matuson**, Research Analyst

September 2021

This ESG White Paper was commissioned by Forward Networks and is distributed under license from ESG.

Contents

Highly Distributed IT Environments	3
The Challenges of Highly Distributed Environments.....	3
IT Complexity is Increasing	4
The Network is Clearly Impacted	4
Lack of Visibility and Evolving Security Requirements	4
Forward Enterprise Empowers Organizations to Regain Control.....	5
Forward Networks’ Digital Twin	5
An Exact Duplicate of the Entire Network Environment	6
Customer Value	6
The Bigger Truth	8

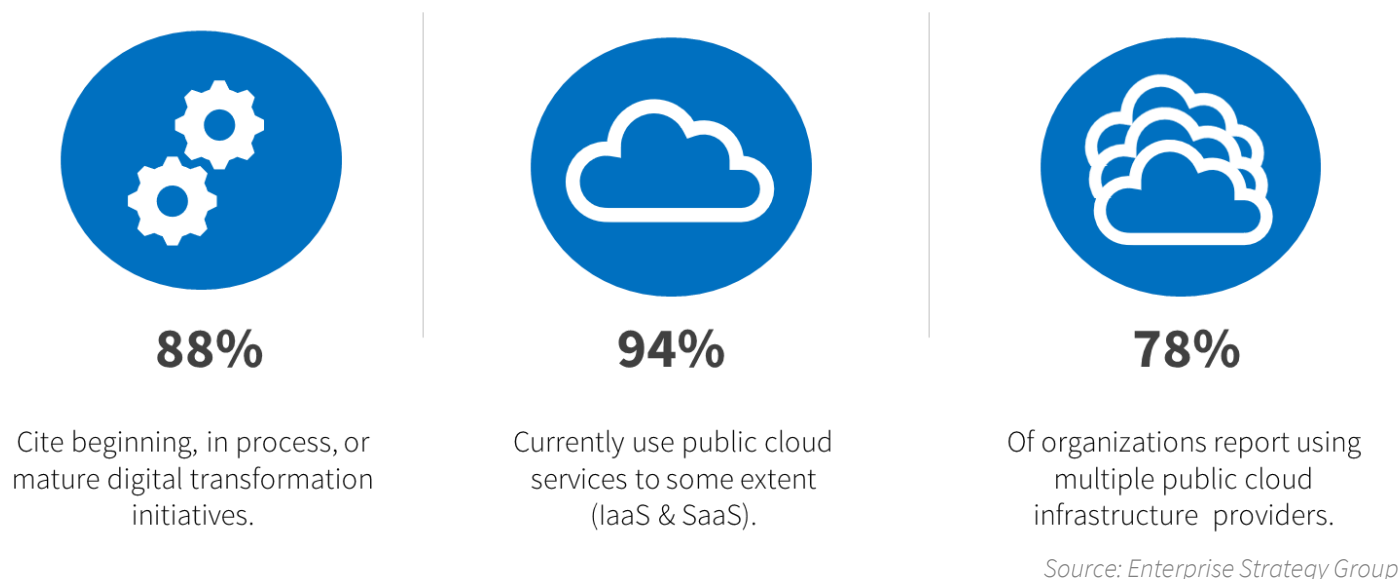
Highly Distributed IT Environments

The IT pendulum is swinging towards highly distributed, modern environments. More than ever before, employees are working remotely, and vast numbers of applications are being distributed across data centers, multiple public clouds, and edge locations.

Driven by these highly distributed application and employee environments, it is not surprising that organizations across industries are rapidly evolving their environments. In fact, ESG research shows that digital transformation initiatives are becoming mainstream, revealing that almost nine out of ten organizations are currently in the process.¹

As part of digital transformation, organizations are adopting public cloud and multi-cloud environments. According to ESG research, cloud adoption is nearly ubiquitous, with 94% of organizations currently using public cloud services to some extent (IaaS and SaaS), while more than three-quarters (78%) of organizations are leveraging multiple public cloud infrastructure providers (see Figure 1).

Figure 1. Data Transformation and Cloud Adoption



The Challenges of Highly Distributed Environments

With highly distributed environments, organizations are looking to gain greater operational efficiency. According to ESG research, several of the top goals of digital transformation reported by respondents are to become more operationally efficient, ensure users can interact and collaborate in new ways, and provide a better and more differentiated customer experience.

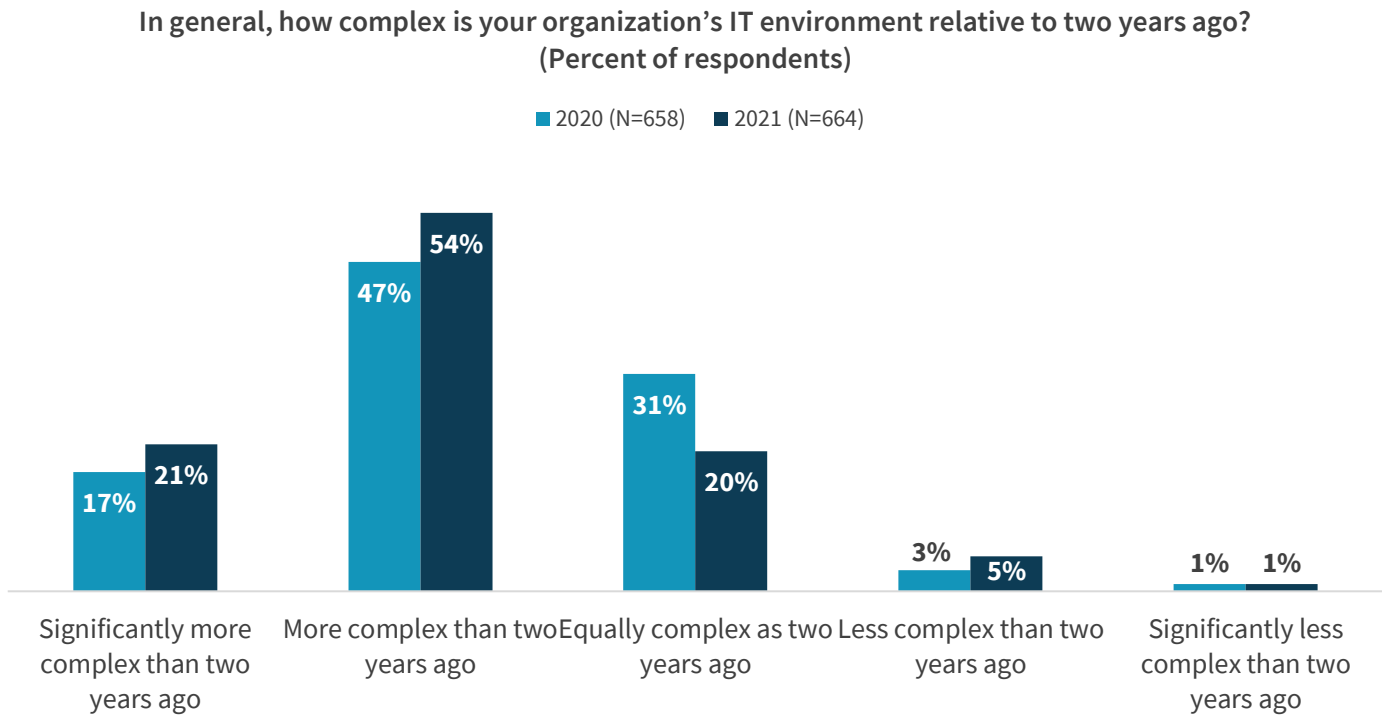
Thus, while organizations are looking to attain better operational efficiency, they must focus on the health and performance of the network, as they are central to meeting the goals of digital transformation.

¹ Source: ESG Research Report, [2021 Technology Spending Intentions Survey](#), January 2021. All ESG research references and charts in this white paper have been taken from this research report.

IT Complexity is Increasing

IT has grown increasingly complex, especially with rising numbers of organizations leveraging highly distributed IT application environments. In fact, according to ESG research, three-quarters (75%) of respondents believe that IT has become more or significantly more complex than just two years ago (see Figure 2).

Figure 2. IT Complexity is on the Rise



Source: Enterprise Strategy Group

The Network is Clearly Impacted

The network is clearly impacted. While many organizations currently employ a multi-vendor strategy, merger and acquisition (M&A) activity can further increase complexity as this type of activity potentially introduces additional network vendors into the existing mix. In addition, this, combined with supporting multiple public cloud infrastructure providers, has resulted in creating an environment where it is virtually impossible for humans to keep up or effectively manually manage.

Lack of Visibility and Evolving Security Requirements

Modern application environments and development methodologies are also creating challenges for network teams, as the network is highly dynamic and changes frequently—and this means that every network environment is going to be unique.

The scale, hybrid nature, and volume of adds, moves, and changes in these highly dynamic environments produce increasingly difficult conditions for network operations teams to prevent outages and, when an outage does occur, make it extremely challenging to quickly locate the root cause. It should come as no surprise that lack of visibility negatively impedes progress, especially since many network teams still use Visio and CSVs (i.e., plain text files containing a list of data) or rely on tribal knowledge, which is often used reactively to attempt patchwork fixes.

In addition, organizations working in highly distributed environments must constantly deal with swiftly evolving security requirements, such as zero trust infrastructure (i.e., only authorized individuals can access certain information and resources) to keep the business and customers safe.

To drive operational efficiency, enhance network availability, and ensure policy compliance, organizations require innovative tools that can provide them with comprehensive visibility into modern, hybrid, and multi-cloud environments. In order to maintain a competitive edge, grow the bottom line, and provide employees with a secure, enhanced experience, organizations must take action. Enter Forward Networks.

Forward Enterprise Empowers Organizations to Regain Control

Forward Networks was founded to provide organizations with visibility into highly distributed and complex modern network environments. Forward Enterprise, the vendor's full-featured platform, visualizes, searches, verifies, and predicts the behavior of an organization's network by creating a digital twin (an exact mathematical model).

Forward Enterprise helps engineers by providing easy-to-understand, actionable L2 – L4 information in the following areas:

- Configuration correctness: Using custom intent checks, Forward Enterprise will alert engineering if a device is configured in a non-compliant manner to protect network health and maintain the security posture.
- Support for all major network equipment vendors and cloud suppliers: Understanding that network environments are heterogeneous, Forward Networks' coverage consists of more than 30 network and cloud vendors. Plus, it has the ability to extract and share data effectively via APIs and CLIs.
- Network paths: The solution can help organizations discover all possible traffic paths, ensure security policy compliance, and determine the potential blast radius of compromised devices in a single click.

Forward Networks' Digital Twin

Forward Networks' digital twin is based on a powerful mathematical network model created through years of development by a team of PhDs to provide organizations with the ability to proactively validate network configuration, security posture, and behavior patterns and ensure compliance and consistency. This mathematical model allows Forward Enterprise to compute all possible paths that traffic can take—not just those paths that are being used. In addition, Forward Enterprise's validation of network configuration can help organizations avoid outages by finding errant configurations before an outage occurs.

Leveraging these capabilities, network operations and security operations teams can regain control of increasingly complex, highly distributed environments, quickly allowing organizations to:

- View complex information in a vendor-agnostic and easy-to-understand manner. This allows new or junior engineers to quickly solve problems and frees up senior staff to work on more value-added initiatives.
- Create a single source of truth that improves the ability for SOC/NOC/Apps teams to work better together. This means faster application deployment and quicker revenue recognition. Organizations can enforce complex rules without increasing staff or training, which avoids added expenditures and mitigates security risks.
- Rapidly scale the implementation. A single instance of Forward Enterprise is capable of supporting up to 50,000 devices, and clustering allows support for even more devices.

- Roll out network-wide changes with confidence by using the digital twin to determine how configurations will impact traffic before they are pushed live.
- Deploy new applications more quickly using automated secure application provisioning, driving faster revenue recognition.
- Detect network traffic anomalies, ensuring compliance with security policies.
- Identify the blast radius for compromised servers and locate errant configurations in seconds.

An Exact Duplicate of the Entire Network Environment

Unlike a test lab environment, Forward Networks' digital twin precisely duplicates an organization's entire network environment, accurately predicting how the environment will respond when making any moves, adds, or changes. Given that, the ability to create a digital twin is extremely powerful compared with trying to create a shadow network environment.

It's important to note that creating a shadow network environment that only samples the production environment (not the entire environment) is extremely time consuming and costly—plus there is no guarantee that the predictions are 100% accurate.

Forward Networks' digital twin can be created for highly complex network environments, scaling tens of thousands of devices across a distributed environment with a cluster architecture, allowing network, security, and development teams to access a single source of truth for the network. This, in turn, drives greater operational efficiencies, increases availability, strengthens security, and allows applications to be deployed faster.

Customer Value

ESG heard from several of Forward Networks' customers to better understand the value derived from the solution—and found consistent themes across these customers, including:

- Deriving value with initial deployment:
 - Customers gained visibility into network paths and network topology. Customers have reported that “It's like magic,” referring to the first time the solution was deployed, and others asserted that it was able to reveal a complete inventory of network devices, many of which were unknown to the business. Another benefit derived from working with an accurate view was that the network team was able to demonstrate to the executive team the level of network complexity and use those results to justify modernization efforts.
 - Customers could respond to security team requests with accurate network information. With the convergence of network and security accelerating, Forward Networks can provide value to the security team by identifying network device vulnerabilities and reducing technical debt.
 - Customers no longer needed to maintain a matching test lab environment. Organizations indicated that having an accurate digital twin of the network enabled them to save both time and money by not having to build out a matching test environment.

- Customers uncovered unauthorized internet connections. Often, initial discovery uncovered devices that were connected to the internet but should not have been. These unauthorized connections can have significant implications on an organization's security posture.
- Accelerating new initiatives:
 - Customers enhanced security and agility. By having a complete understanding of the network environment, including network paths and connection points, organizations can accelerate the adoption of zero trust environments. This visibility also enables organizations to validate hybrid, multi-cloud environments (distributed clouds) and take advantage of infrastructure as code.
 - Customers enhanced their visibility. Forward Networks can map and provide complete visibility between network and application points. Seeing all actual and potential paths enables organizations to deploy with confidence and allows them to test new policies before they are implemented. This ensures new initiatives work correctly the first time.
- Greater agility:
 - Highly distributed IT environments and modern applications require greater agility. Customers stated that leveraging Forward Networks has enabled them to deploy new applications in just a few months, not a year—*without* adding resources. The same team was able to manage a more complex, distributed environment.
- Stronger relationships between application development and security teams:
 - Customers could bridge gaps and reduce or eliminate friction. Having a single source of truth for the network environment and being able to share that information uncovers the real bottlenecks. Organizations can leverage this solution to create a bridge between the network team and other functions, such as developers and security teams.
 - Customers could provide security teams with direct access. Role-based access enables security teams to directly query network information to streamline the troubleshooting process. Organizations reported shaving hours off their troubleshooting times.
 - Customers could validate firewall rules/policies. Security teams can leverage the digital twin to validate new firewall rules or policies prior to deployment in production to ensure they will produce a positive effect and not create new vulnerabilities.
- Operational efficiency for network, security, and application teams:
 - Customers could monitor both modern and legacy environments. While established organizations are rapidly deploying new technology, they must still support many legacy environments. It is important to map out both environments to obtain a complete picture.
 - Customers could eliminate silos. Forward Enterprise creates a single repository of data, making it easier for the security and application teams to access. This democratization of data can lead to tool and process consolidation and create change assurance.

- One customer stated that “application developers have embraced the tool, and [it] provides a capability we did not have before.” Forward Networks delivers the actual discovered source of truth and not the intended source of truth, often derived from a Visio diagram.
- Scalability with cluster architecture:
 - One large enterprise offered that they had “started with a modest environment, but are now covering over 40M flows across tens of thousands of devices.” More importantly, Forward Networks is able to consistently collect a complete topology in minutes, not days. This ensures organizations can work with current data. The best testament to Forward Networks’ value to the company was the proclamation that the “true value of Forward Networks is realized when deployed across the entire network, not just part of it.”
- Return on Investment:
 - According to one customer, “We justified Forward Networks by examining last year’s Sev-1 incidents and realized if Forward Networks had been deployed, we would have eliminated about 90% of them. In fact, if the company had just eliminated one of the events, it would have paid for the entire deployment.”

The Bigger Truth

IT and application environments are becoming highly distributed, straining agility, and creating additional security risks. The network is becoming more complex, and a distributed environment is critical to ensure application availability and positive customer experiences. New application development architectures, methodology, and security frameworks are driving the convergence of network operations teams with developers and security professionals. Fortunately, the network has a wealth of data that can be leveraged to create a more secure, agile, and operationally efficient environment—if it can be kept up to date and easily accessed.

Forward Networks has created technology that allows organizations to rapidly collect this wealth of network data and construct a digital twin of their exact network environments—allowing them to effectively leverage their data across network, security, and application development teams to deliver a highly available, secure, and agile network environment.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.