WHITE PAPER

Choosing the Right Network Observability Platform for Highly Distributed Environments

By Bob Laliberte, Principal Analyst

December 2022

This Enterprise Strategy Group White Paper was commissioned by Progress Software and is distributed under license from TechTarget, Inc.

Contents

Executive Summary

Modern IT environments are highly distributed and dynamic, with applications deployed across private data centers, multiple public clouds, and edge locations. Hybrid work and IoT require employees and devices to be connected from home offices or other remote locations. This new environment places more emphasis on organizations to deliver secure connectivity between all applications, employees, and IoT devices.

To ensure optimized and secure network operations, operations teams need to transition from network monitoring tools that sample data at regular intervals to a network observability platform. Given the dynamic nature of modern applications, this transition entails network observability platforms continuously collecting deep, granular data (including metrics, events, logs, and traces) from network traffic, network devices, and devices attached to the network to detect and fix issues in an ephemeral modern application environment. These highly distributed environments also have increased risk due to their larger attack surfaces. However, organizations can mitigate that risk by leveraging data collected from the network traffic to find issues and ensure a secure environment. Leveraging network detection and response (NDR) capabilities enables organizations to detect anomalous behavior and to quickly respond to it. Lastly, the ability to identify specific application traffic will provide context to prioritize and accelerate troubleshooting for business-critical applications.

As the IT landscape has evolved, organizations need to consider transitioning from individual monitoring tools to a network observability platform that collects granular, end-to-end network data, enhances their security posture, provides application context, and can easily share information with other IT or business systems.

Modern IT Environments Are Highly Distributed

IT environments have been rapidly evolving to become more agile and responsive to the business. Much of this progress has been accomplished by leveraging public cloud services. In fact, research from TechTarget's Enterprise Strategy Group (ESG) highlights that 96% of organizations are using the public cloud (IaaS or SaaS).[1] Utilizing public clouds to create hybrid cloud environments that connect private data centers to public clouds has now evolved to the point where 86% of organizations indicate that they currently use two or more public cloud services (IaaS and PaaS).[2]

However, the rapid adoption of cloud services doesn't mean that all applications are in the cloud. In fact, the majority of applications and workloads are still in private data centers, with 62% of organizations reporting that 50% or less of their applications are in the cloud.[3] Increasingly, organizations are taking advantage of data generated at edge environments to derive real-time business insights, ensure high-quality products, and optimize processes, and they are deploying applications there was well. ESG research shows that 94% of organizations believe that edge computing is one of their top ten investment priorities (see Figure 1).[4]

The majority of applications and workloads are still in private data centers, with 62% of organizations reporting that 50% or less of their applications are in the cloud.

[1] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.
[2] Source: Enterprise Strategy Group Complete Survey Results, *Distributed Cloud Series: Application Infrastructure Modernization Trends*, March 2022.
[3] Ibid
[4] Source: Enterprise Strategy Group Complete Survey Results, *Distributed Cloud Series: Digital Ecosystems*, August 2022.

Figure 1. State of Modern IT Environments

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As a result, applications and workloads are now distributed across several private data centers, multiple public clouds, and numerous edge environments. This has two important implications: First, it means that secure network connections are more critical to ensuring smooth business operations and differentiated customer experiences. Second, new application development is typically cloud-native, leveraging microservices architectures. This requires organizations to transition from monitoring or visibility tools that passively sample data at regular intervals (typically measured in minutes) to observability solutions that collect granular-level network traffic data or metrics all the time, as well as other data sources, such as logs, application traces, and events. This enables organizations to understand the state of the system and address the inherent complexity of an environment that is constantly changing, often in the span of just a few seconds. Concurrently, IT teams also have to contend with a highly remote workforce, as hybrid work models have taken hold, and operations teams now have to support these remote workers and their connections.

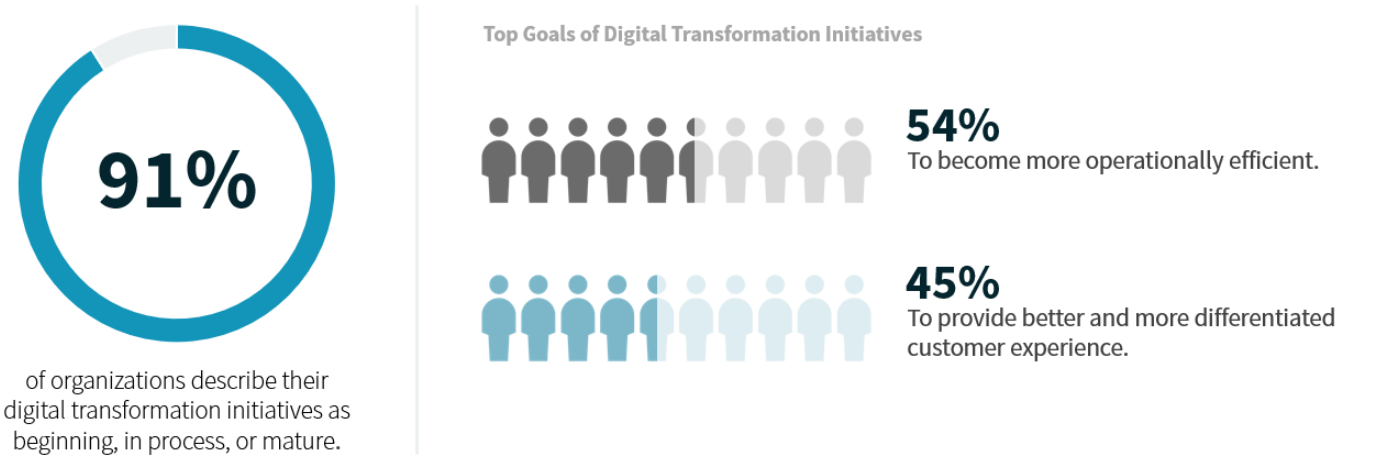
This also places more emphasis on securing the network, as the distributed environment represents an increased attack surface and risk to the business. When asked in an ESG research survey which technologies organizations used for threat detection and response, 93% of the respondents selected network detection and response.[5] This highlights the importance of leveraging the network to mitigate risk and enhance an organization's security posture.

These highly distributed environments are also more complex to manage, as validated by ESG research, with more than half of respondents (54%) citing that the network environment is now more or significantly more complex than it was just two years ago.[6]

Nine out of ten organizations are currently engaged in digital transformation initiatives to some degree, which is driving the creation of highly distributed environments. And some of the top IT goals for these transformations are to become more operationally efficient (54%) and to provide a better and more differentiated customer experience (45%) (see Figure 2).[7]

[5] Source: Enterprise Strategy Group Research Report, *Network Threat Detection and Response Trends*, December 2022.
[6] Source: Enterprise Strategy Group Research Report, *Network Modernization in Highly Distributed Environments*, November 2021.
[7] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

Figure 2. Digital Transformation Initiatives and Top Goals



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

To reach those goals, organizations need to leverage the information available in the underlying network infrastructure and network traffic used to ensure secure connectivity between highly distributed modern applications, remote workers, and edge devices. This information needs to span from the physical network layer two up to application layer seven and should include NetFlow/IPFIX, SNMP, Logs, events etc. In addition, data needs to be collected from on-premises, cloud-based services or colocation centers and remote locations. More importantly, it needs to be available in a single, unified data source and not isolated in individual tools.

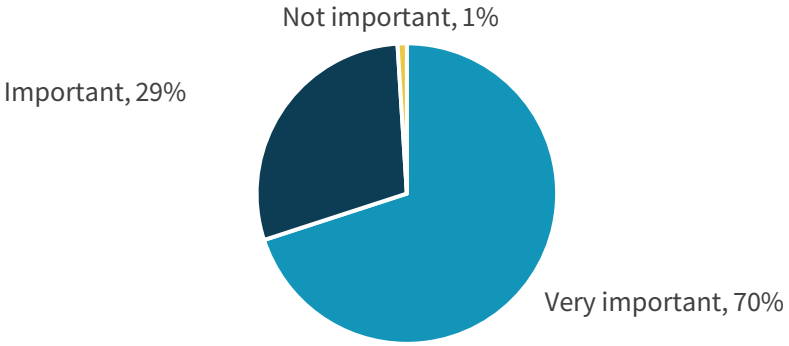
The Value of Comprehensive Network Information

The key to effectively managing these highly distributed, yet connected, environments is the ability to have granular, end-to-end network visibility and the ability to collect and correlate this data. Enterprise Strategy Group (ESG) research highlights that virtually all organizations (99%) believe that having end-to-end visibility is either important (29%) or very important (70%)[8]—which includes visibility to remote sites and employees (see Figure 3).

[8] Source: Enterprise Strategy Group Complete Survey Results, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased*, December 2021.

Figure 3. Importance of End-to-end Visibility

How important will it be to have end-to-end visibility into and for all remote locations and employees? (Percent of respondents, N=613)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why is that visibility so important? Organizations need to understand what is going on across private data centers, multiple public clouds, edge environments, and even remote workers. End-to-end visibility is an important stepping stone to delivering on network observability, where collecting every piece of information is important (i.e., no sampling) and the more granular the better. The transition to observability dictates that every piece of data be collected to detect those "unknown" network problems created by modern application architectures. These are ephemeral environments that can spin new services up and down in a matter of seconds. The information collected from the network devices and traffic can play a critical role in enabling organizations to understand what happened and when. Specifically, operations teams (and the business owners) want to know:

- How are the applications performing? Application performance is critical for the success of most businesses. However, given the distributed nature of modern IT environments, it can be challenging to ensure optimized availability and performance. While application outages are easy to determine, applications that suffer a degradation in performance can be much harder to recognize and even harder to diagnose, especially when the problem is intermittent. Even more importantly, organizations need to have insight into their application users' experience.

- Are cloud resources utilized and performing well? Organizations are making significant investments in public cloud resources, but getting complete, concise information regarding servers, storage, and cloud devices, especially when leveraging multiple public cloud vendors, can be a challenge.

- What is connected to the network? Am I at risk? Today, organizations deploy physical and virtual resources across public clouds, edges, data centers, and home offices. Every end user and IoT and IT device on the network represent a potential vulnerability, yet most organizations can't get an accurate picture of what is actually connected, how it is connected (wired/wireless), and the potential risk.

It is important to understand the critical role the network can play in helping to answer these questions, especially in highly distributed environments. It can do this by providing comprehensive, granular information, including:

- Network performance and bandwidth consumption across every location, by application. Application-aware network performance monitoring and management solutions enable organizations to get detailed information on the performance of their applications, including the ability to identify which applications are impacted by a network

outage. But these solutions can also pinpoint the cause of intermittent network performance issues that are creating poor experiences for users, down to individual network links.

- Network detection and response (NDR) capabilities. Organizations understand the need to ensure secure connectivity to all applications and users or devices. Fortunately, analyzing network traffic can be extremely beneficial to improving security posture. Leveraging network detection and response (NDR) protects against ransomware, insider threats, and even unknown threats. As malware is continuously modified to elude advanced perimeter solutions, advanced AI/ML tools can be used to analyze network footprints to identify any potential anomalies and quickly alert security operations teams. In fact, as ESG research highlights, organizations cite the top two benefits of AI/ML capabilities are to improve detection accuracy (61%) and detection speed (59%).[9]

- Detailed information regarding wireless networks. This includes the ability to understand performance or issues when users and or devices (IoT) are connecting to the network. Keep in mind that with the hybrid work model, observability of the wireless network could also extend to the home. Wireless networking is playing a more important role at corporate locations since these spaces may be reimagined to provide more collaboration areas than dedicated cubicles. This transition requires voice and video applications to be increasingly accessed over wireless connections and not just dedicated rooms with wired connections.

- Configuration management. Rolling out new equipment can be a daunting task; organizations have to ensure that devices consistently have the correct configuration. Increasingly this requires a centralized, typically cloud-based management system to centralize policies for configuration. It also ensures that any updates are performed across the environment without the need for time-consuming and error-prone manual updates.

- Log management. Collecting logs from network devices can be highly valuable for organizations to perform trend analysis, aid in incident response, and assess operational health. Plus, log assessment and archiving can be instrumental for compliance audits or for performing post-intrusion assessments. Also, for organizations building out network observability solutions, logs are an important leg of the stool.

- Sharing details with other platforms. Network solutions with REST APIs can drive greater operational efficiencies by interacting with other IT platforms. This includes collecting deep telemetry data to integrating with ticketing solutions like ServiceNow or automation platforms like Ansible to ensure an optimized workflow with the ability to centralize data.

Taking a Platform Approach to Network Observability

Given the complexities associated with these highly distributed environments and the reliance on the network to connect them, organizations need to take a more comprehensive approach to collecting data from the network that can be transformed into valuable information and knowledge.

Because technology is evolving faster than ever, organizations must take a long-term approach to network observability. Network operations teams need to move beyond monitoring known metrics and events and look to capture as much data as possible to find the future "unknown" events that will arise with the new application and network architectures that are gaining traction (i.e., microservices apps or multi-cloud networking).

This mentality dictates that network operations teams don't focus on buying a single technology product but rather look to adopt a platform approach that can provide network observability and adapt to a rapidly changing and highly distributed

[9] Source: Enterprise Strategy Group Research Report, *Network Threat Detection and Response Trends*, December 2022.

network environment. The switch to a platform approach requires organizations to form strategic partnerships rather than just buying products from a vendor. This will require a longer commitment, and organizations need to make sure there is an expectation that the technology vendor will continue to invest in innovation and develop the platform as the environment and technology landscape changes. For example, the rise in remote employees and IoT devices at the edge has extended the requirements for network observability platforms to be flexible to accommodate those changes.

Top characteristics to look for in an end-to-end network observability platform include:

- Support for heterogeneous network environments. Most organizations adopt a dual vendors strategy to avoid vendor lock-in or take a best-of-breed approach to deploying network hardware. This can result in different vendors in the data center than in the campus, branch, or WAN. Even those organizations that standardize on a single vendor may have different OSes or technology based on acquisitions. Organizations need to collect and correlate data from all network devices regardless of the logos on the outside. And for those in multiple public clouds, this capability will be important as well.

- End-to-end support. This extends from the application to the end user, regardless of where the application or user are located. The platform must provide insights into and between any of an organization's private data centers; public clouds; or campus, branch, or even home office locations. It must also include wired and wireless technologies and end user devices as well.

- Collection of metrics, events, logs, and network traces. It will be important to collect as much data as possible from the network devices and network traffic to accelerate problem identification and resolution. This data will also provide a clear picture of the entire environment that can be leveraged to build AI/ML functionality or create historical data to provide a more predictive approach to managing the network.

- Support for application-level monitoring. It will be critical to prioritize problem resolution to support mission-critical and production applications in the event of an outage or degradation of service. The ability to correlate application traffic to specific network environments will greatly aid in optimization and problem resolution.

- The ability to enhance security posture with NDR. These highly distributed environments represent a much larger attack surface and greater risk to the business. Once a threat actor gets past traditional perimeter security and is inside the network, organizations need to leverage data collected from the network to help detect anomalous traffic and take immediate action. The key is ensuring that the platform has role-based access to ensure security operations teams have access to this data as well.

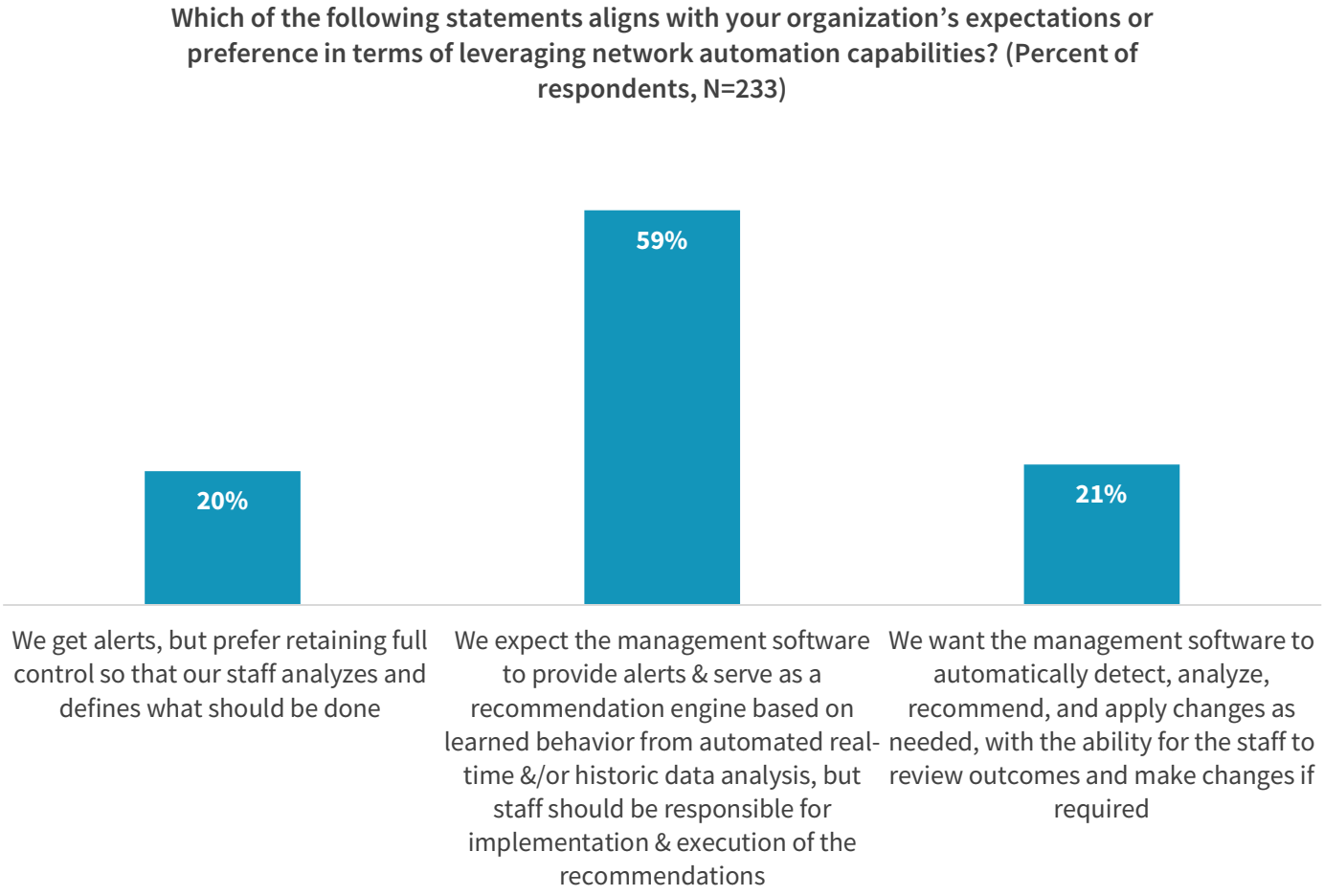
- Tight integration with other applications. The network plays a critical role providing secure connectivity in these distributed environments but does not exist in a vacuum. Therefore, it is imperative that network platforms are tightly integrated into organizations' trouble-ticketing and workflow systems, as well as other security or IT systems tools. This would include publishing and supporting APIs to accelerate integration.

- Centralized management. To drive operational efficiency, organizations need to take advantage of a single management console. Increasingly, these systems are cloud-based to facilitate connectivity when working remotely and to provide a centralized data repository that can be used to enhance AI/ML models and algorithms. Plus, being cloud-based streamlines lifecycle management (LCM) efforts and reduces spending for on-premises hardware and maintenance.

- A robust roadmap and commitment to invest. Technology is evolving at a rapid pace, so organizations must have visibility into an observability platform's roadmap. Does the vendor understand where the market is going, and does it have a plan to incorporate the appropriate functions and technologies to keep its customers on the leading edge?

- AI/ML and automation. Intelligent systems will be required to manage these ever-changing and expanding network environments. Organizations need to understand the level of intelligence and automation that is currently available and what will be available in the near future. Enterprise Strategy Group (ESG) research examines enterprise adoption of network automation and indicates that the majority of organizations (59%) expect network automation capabilities to both alert them to problems and provide recommendations to fix them. Just over one-fifth of organizations state they would like to deploy fully automated solutions, while one-fifth just want to get an alert and find and fix the problem on their own.[10] The key is to ensure that these intelligent systems provide a feedback loop to include the operations teams in any of the scenarios.

Figure 4. Leveraging Intelligence to Drive Network Automation



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[10] Source: Enterprise Strategy Group Research Report, *Network Modernization in Highly Distributed Environments*, November 2021.

The Bigger Truth

Modern IT environments are becoming more distributed and complex. Applications are being deployed across private data centers, multiple public clouds, and edge locations. Simultaneously, employees and IoT devices accessing those apps are doing so from their home or other remote location. As a result, the network has become the critical component to ensure secure connectivity regardless of where employees and devices are located.

To retain control over these environments, operations teams must deploy network platforms that can provide deep, granular visibility into network devices and network traffic to ensure optimized experiences, provide enhanced levels of security, and drive operational efficiencies. Given the reliance on the network in a distributed environment, NDR capabilities and granular data collection will play an important role in organizations' defense strategies. In addition, organizations need an awareness of the applications running over their networks and the ability to provide insights into them. This, in turn, will enable them to prioritize problem resolution based on the importance of the applications and accelerate troubleshooting times. Having this level of visibility will also help them reduce operational costs and optimize day-two activities.

Given the highly distributed nature of current environments, it will be very difficult for individual tools to provide the requisite end-to-end view. Instead, organizations should think strategically and adopt a platform that provides comprehensive, end-to-end network observability with the ability to easily integrate into other business systems.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188