

FEBRUARY 2023

# The Importance of Network Visibility and Analytics for Zero Trust Initiatives

Bob Laliberte, Principal Analyst

**Abstract:** Organizations are embarking on zero trust initiatives to deliver enhanced security postures across highly distributed environments. The network plays an increasingly important role in enabling zero trust by providing granular visibility into application, user, and device traffic on the network, possessing the ability to analyze this data, and automating the response based on the results. The Fortinet Secure SD-WAN solution provides organizations with the requisite functionality to accelerate the implementation of a zero-trust initiative.

### **Current Environment**

Modern IT environments are highly distributed, with applications deployed across private data centers, multiple public clouds, and edge locations. This means that most enterprises have potentially hundreds of applications spreading across a combination of SaaS-based, laaS-based, private DC-based, or edge locations. Adding even more complexity is the fact that shadow IT groups can spin up applications without full knowledge of the IT team.

In addition to a distributed application environment, organizations are embracing hybrid work. In fact, TechTarget's Enterprise Strategy Group research indicates that the majority of organizations believe more than half (57%) of their workforce will be remote in two years. With so many workers continuing to work remotely, a robust business resiliency plan is needed to dictate how all knowledge workers can work remotely while their IT environments remain secure. As a result, organizations must now have the capability to allow employees to securely access applications from wherever they are working.

Unfortunately, this highly distributed environment creates a much larger attack surface, prompting new threats and entry points into the business, with access typically gained through a remote user. One can look at the daily news to track the increase in ransomware attacks for proof of this. Enterprise Strategy Group research indicates that organizations continue to invest to protect themselves from these attacks, with 44% of organizations reporting that they have made significant technology investments specifically tied to ransomware preparedness.<sup>2</sup>

As a result, zero trust initiatives are gaining traction to limit the risk associated with the increased attack surface and ensure that a user's identity is continuously validated, that a user only has access to applications and resources they need, and that the user is blocked from reaching everything else. Essentially, this creates a "never trust, always verify" environment. Enterprise Strategy Group research highlights this shift to zero trust, with 46% of organizations stating they have either implemented or have begun to implement a zero trust initiative across their organization.<sup>3</sup> However, it should be noted that zero trust is a broad topic and can be confusing to fully understand, demonstrated by the fact that 54% of organizations reported that it is difficult for them to find a starting point for zero

<sup>&</sup>lt;sup>1</sup> Source: Enterprise Strategy Group Complete Survey Results, End-to-end Network Visibility and Management Trends, to be published.

<sup>&</sup>lt;sup>2</sup> Source: Enterprise Strategy Group Research Report, <u>2023 Technology Spending Intentions Survey</u>, November 2022.

<sup>&</sup>lt;sup>3</sup> Source: Enterprise Strategy Group Survey Results, <u>The State of Zero Trust Security Strategies</u>, May 2021.



trust.<sup>4</sup> Further complicating the matter, every vendor has a different definition of zero trust and different requirements to implement it.

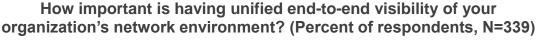
What is clear is that given the role the network has in connecting these distributed environments, organizations must take advantage of the visibility, analytics, and automation capabilities available in modern SD-WAN solutions to enable a zero trust architecture.

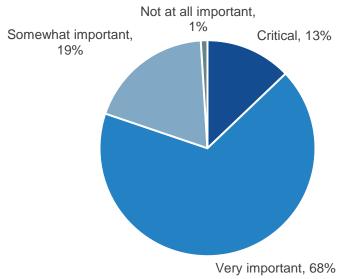
## The Importance of Network Visibility and Analytics

As organizations build out a distributed IT infrastructure, applications, and user environments, it is critical that they have end-to-end visibility of the IT environment and eliminate any blind spots, as it is impossible to manage something that you cannot "see."

Enterprise Strategy Group research validates this and demonstrates the importance of network visibility, as 81% of organizations stated that end-to-end network visibility is either critical or very important, and only one percent stated it wasn't important at all.<sup>5</sup>

Figure 1. Importance of End-to-end Visibility





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

When asked why end-to-end visibility was important for their organizations, respondents reported that it allows them to:<sup>6</sup>

Have a complete view of all network assets (46%) – In a highly distributed environment, the first step to
ensuring security is to find every device that is connected to the network. Having a complete view of all network
assets also ensures that the organization can adhere to the compliance requirements that correspond to their
specific industry (e.g., PCI, HIPAA, GDPR).

<sup>&</sup>lt;sup>4</sup> Ibid.

<sup>&</sup>lt;sup>5</sup> Source: Enterprise Strategy Group Complete Survey Results, *End-to-end Network Visibility and Management Trends*, to be published.

<sup>6</sup> Ibio



- Mitigate risk when making changes (42%) Having visibility enables organizations to dramatically reduce the
  risk of unintended consequences when a change to the network environment is made. Given the number of
  adds, moves, and changes that occur on a daily basis, being able to quickly identify what in the environment
  may be impacted enables organizations to preemptively take the appropriate steps to minimize an impact.
- Gain visibility over remote workers (41%) Given that the most commonly cited reason for increased IT
  complexity is the increase in remote and hybrid work concerns,7 it tracks that organizations want to get visibility
  into these workers. This is especially true, as remote workers dramatically increase the number of endpoints to
  monitor and manage.
- Accelerate troubleshooting (35%) Comprehensive visibility enables operations teams to quickly isolate a
  problem so organizations can focus on fixing the problem instead of trying to find it.
- Better understand vulnerabilities and exposures (34%) In many environments, having blind spots can lead to
  devices not being properly patched and upgraded. This creates vulnerabilities and potentially exposes
  organizations to unwanted threats or attacks.

Furthermore, separate Enterprise Strategy Group research highlights that 91% of organizations agree or strongly agree that they leverage analytics to identify anomalous behavior, and or require additional authentication and ensure that access is restricted when a questionable event occurs.<sup>8</sup>

Enterprise Strategy Group asked organizations that are already implementing or that have begun to implement a zero trust architecture how they prioritized the implementation of capabilities. 44% of respondents reported that network segmentation was the starting point for their zero trust strategy, and 42% cited analytics was their starting point.<sup>9</sup>

## **Fortinet Secure SD-WAN**

Fortinet understands the challenges associated with implementing a zero trust architecture and has developed solutions to enable organizations to jumpstart their zero trust journey. It starts with Fortinet's Secure SD-WAN, which provides organizations with a foundation to provide the visibility, analytics, and automation capabilities that drive operational efficiencies and enhance security postures.

For example, the visibility, analytics and automation are extended across the entire network (LAN, WLAN and WAN [including 4G/5G]) to enhance zero trust initiatives. Furthermore, organizations are able to segment and prioritize application traffic to reduce attack surface and ensure performance. With the purpose-built ASIC, scale and power efficiency are optimized as well. Additional operational efficiencies are achieved using zero-touch provisioning and centralized management combined that enables network, application, and security configurations and policies to be distributed to all sites and hybrid workers correctly and consistently. The solution is comprised of:

- FortiGate solutions. Fortinet provides a wide range of form factors to match the required scale and are
  suitable for use in data center, public cloud, and edge locations, which can accommodate both physical and
  virtual environments (including container environments). This includes fully supported offerings for all major
  public clouds, with bring-your-own-license (BYoL) and pay-as-you-go models available. FortiGate solutions
  include a built-in zero trust network access (ZTNA) application gateway that enforces explicit application access
  and user identity to ensure secure connectivity for remote and hybrid workers.
- The Fabric Management Center that is comprised of FortiManager and FortiAnalyzer to deliver the endto-end visibility, analytics, and reporting across the Fortinet Security Fabric. More specifically:
  - o **FortiManager** provides comprehensive and centralized management of not only the FortiGate solution, but also of FortiSwitch, FortiAP, and FortiExtender solutions to ensure end-to-end visibility across the WAN,

3

<sup>&</sup>lt;sup>7</sup> Source: Enterprise Strategy Group Research Report, <u>2023 Technology Spending Intentions Survey</u>, November 2022.

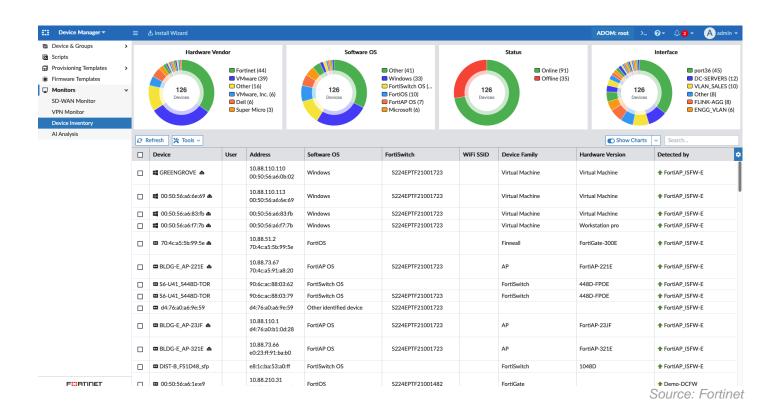
<sup>&</sup>lt;sup>8</sup> Source: Enterprise Strategy Group Research Report, The State of Zero Trust Security Strategies, May 2021.

<sup>9</sup> Ibid



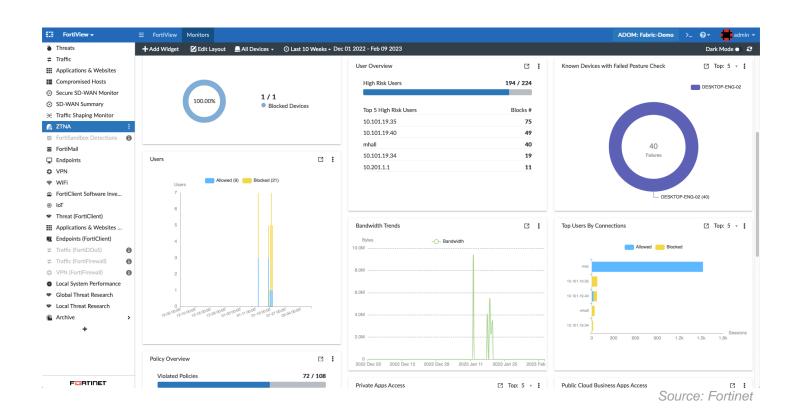
LAN, and WLAN. This unified visibility enables operations teams to drive operational efficiency even though the network and security environment is becoming more distributed and complex. The use of out-of-the-box templates to follow best practices and device blueprints drives additional efficiencies. Having a centralized management platform that provides deep visibility of systems, applications, and interfaces that include items such as network segmentation, performance SLAs, IoT device ID, route tables, IPS templates, and top talkers (see Figure 2).

Figure 2. Centralized Management and Visibility



This visibility enables organizations to mitigate risk and deliver enhanced experiences. Leveraging automation-driven network configuration, visibility, and policy management will enable organizations to be more agile and turn up new locations quickly, while operations teams can spend more time on strategic initiatives and less time performing repetitive manual tasks. To drive additional efficiencies, FortiManager has streamlined workflows that are integrated with almost 500 ecosystem partners.

Figure 3. Policy and Posture Overview of Users and Devices



FortiAnalyzer delivers the requisite visibility, analytics and automation capabilities to enable operations teams to have consolidated and comprehensive visibility into the attack landscape across highly distributed IT and hybrid work environments. As a result, organizations can proactively orchestrate the response (people, process, and technology) to potential or immediate threats. FortiAnalyzer accomplishes this by having tight integration with FortiGate SD-WAN and NGFW solutions, FortiClients, FortiMail, and other solutions to provide detailed reporting on every device, network, user, or application in the environment. This includes collecting all logs and having the ability to perform real-time detection and correlation of problems (Indicators of Compromise [IoC] and advanced threats), which enable operations teams to quickly respond to attacks or threats. FortiAnalyzer allows both the network and security operations team to create dashboards and work from a single source of truth.

In addition to intelligent reporting, operations teams are aided by the ability to leverage automated workflows with APIs, scripts, automation stitches (trigger and response), and connectors. This can dramatically reduce the time required to fix a vulnerability and identify and isolate a threat. Fortinet provides organizations with out of the box "playbook" templates that operations team can quickly customize to fit their environment. By storing all data collected (with public cloud archive options), operations teams also have access to historical analysis and predictive analysis based on trending.

Based on the capabilities outlined above, by deploying Fortinet Secure SD-WAN with FortiManager and FortiAnalyzer, organizations can take significant first steps on their zero trust journeys.

### Conclusion

The reality is that modern IT and application environments are highly distributed, and this creates a significant amount of complexity. Hybrid work initiatives only compound that complexity by adding more corporate endpoints



and creating more risk for an enterprise by having a much larger attack surface. Organizations recognize the increased threat and are beginning their journey to create zero trust architectures.

Because of the distributed nature of IT environments, the network is now playing a bigger role in securely connecting the enterprise. Organizations need to ensure they have the requisite levels of end-to-end visibility and intelligence to leverage the data generated in the network to deliver meaningful insights and enhanced security.

Fortinet Secure SD-WAN, with FortiManager and FortiAnalyzer, will provide organizations with a strong foundation from which to build a zero trust architecture. The comprehensive visibility and detailed analytics and automation capabilities ensure organizations can drive greater operational efficiencies, improve customer experiences, and fortify their security posture.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, 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 TechTarget, 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 Client Relations at <a href="mailto:contact@esg-global.com">contact@esg-global.com</a>.