Enterprise Strategy Group™ by TechTarget

WHITE PAPER

Moving Beyond Users: The Case for Zero Trust SASE

By John Grady, Principal Analyst
Enterprise Strategy Group

January 2024

Contents

Executive Summary

Software-defined WAN (SD-WAN) has seen increasing adoption to enable network modernization and address the issues created by increasingly distributed enterprise environments. But while traditional SD-WAN has helped achieve some network-centric goals, it does not address the security challenges organizations face. Secure access service edge (SASE) seeks to remedy this by converging network and security capabilities in a single solution, but in most cases it only bolts traditional SD-WAN onto security tools.

To better facilitate true network transformation, organizations should look for SASE solutions built on a zero-trust architecture. In a zero-trust SASE model, security is decoupled from network transport, implementing a default-deny posture across the communications of all users, devices, clouds, and physical locations; a wide range of security capabilities are converged to improve security outcomes and promote efficiency; and user experience is prioritized to ensure productivity. Zscaler's Zero Trust SASE solution supports zero-trust-based network transformation across users, workloads, SD-WAN, and IoT/operational technology (OT) to help businesses achieve these outcomes.

To better facilitate true network transformation, organizations should look for SASE solutions built on a zero-trust architecture.

Traditional SD-WAN Alone Cannot Facilitate Network Transformation

Enterprise environments have fundamentally changed, becoming highly distributed and increasingly complex. In fact, nearly three-quarters (73%) of respondents to a research survey by TechTarget's Enterprise Strategy Group (ESG) agree that the network environment has become more complex than it was two years ago.[1] There are a variety of reasons for this, but the prevalence of multi-cloud strategies, the sprawl of connected devices, and the need to support hybrid work stand out (see Figure 1).

Nearly every organization uses cloud resources of some kind, but whether due to self-service expansion over time, acquisition activity, or specific business rationale, multi-cloud usage continues to increase. Specifically, ESG has found that, among organizations using public cloud IaaS, 91% use two or more cloud service providers.[2] As a result, east-west traffic now often travels north-south across what was the traditional perimeter, making secure connectivity more important yet more difficult than ever.

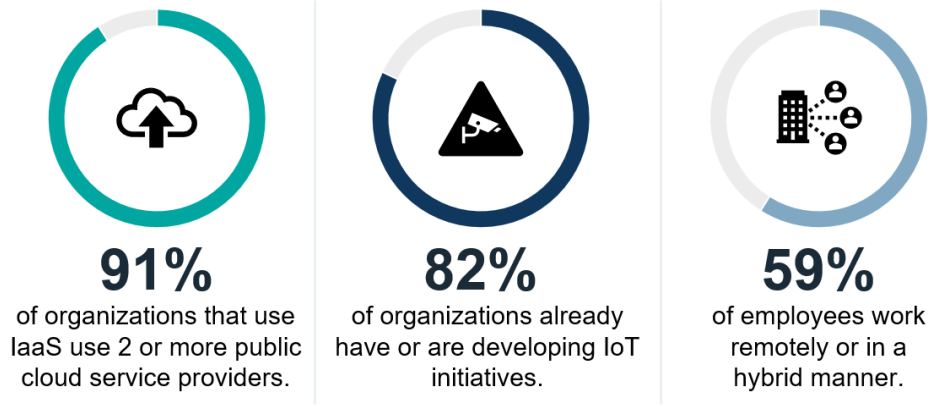
At the same time, the on-premises network looks drastically different than just a few short years ago, with IoT becoming mainstream. Among ESG research respondents, 42% said they have IoT initiatives underway, 28% are developing IoT initiatives that will launch in the next year, and 12% are developing initiatives to launch in the next 24 months or later.[3] While connected devices are clearly a reality and offer a variety of benefits to organizations, attackers can exploit them to gain a foothold in the IoT environment.

Finally, flexible work remains in place for most organizations. Employees across a variety of sectors have pushed back on a full-time return to the office, and a majority of organizations continue to support fully remote or hybrid models. ESG research has found that 28% of employees remain fully remote, while 31% work in a hybrid manner. This, again, creates complexity with regard to consistently providing secure and performant connectivity between users and corporate resources.

---

[1] Source: Enterprise Strategy Group Research Report, *A Network Perspective on SASE and SD-WAN*, November 2023. All Enterprise Strategy Group research references are from this report unless otherwise noted.
[2] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.
[3] Ibid.

Figure 1. The Distributed Modern Enterprise



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

All these factors have rendered traditional castle-and-moat, data-center-centric network architectures obsolete. The typical method of backhauling branch and remote traffic to the data center via VPNs is inefficient and can introduce latency, especially when traffic is ultimately destined for the cloud. Securely connecting the myriad of users, devices, applications, and locations is now exceptionally difficult.

SD-WAN Was Positioned to Enable Network Transformation, but Challenges Remain

SD-WAN has seen increasing adoption to enable network modernization and address some of the issues created by increasingly distributed enterprise environments. Traditional SD-WAN enables organizations to better utilize multiple transport methods; shift to unified, cloud-based management consoles; and enable direct internet access from branch locations.

But while traditional SD-WAN has helped to an extent, it only partially addresses the core challenges security and network teams face in securing connections, managing costs, and reducing complexity. At a foundational level, SD-WAN alone does not solve the underlying security issue with traditional network architectures, which is that flat networks are prone to compromise. Once an attacker gains initial entry onto a flat network, they have free reign to map the environment, do reconnaissance, and find high-value data for exfiltration.

While traditional SD-WAN has helped to an extent, it only partially addresses the core challenges security and network teams face in securing connections, managing costs, and reducing complexity.

Additionally, SD-WAN still relies on site-to-site VPN to secure connections from one location to another, but it does nothing to ensure that the entity being connected accesses only what it is entitled to. While true that traditional SD-WAN solutions can provide some coarse-grained segmentation and steer traffic based on location, application, or other characteristics, it cannot provide the granular control to facilitate the direct entity-to-entity connectivity needed in today's enterprise.

For these reasons, organizations using traditional SD-WAN solutions must layer on additional security tools, adding complexity and cost. While many organizations have moved forward with traditional SD-WAN, gaps remain, and a number are seeking alternative solutions. In fact, 52% of ESG research respondents indicated they are likely to change SD-WAN vendors. This could be due to the challenges organizations continue to face even after deploying traditional SD-WAN. In fact, based on some of the top reasons cited for interest in changing SD-WAN vendors, it is

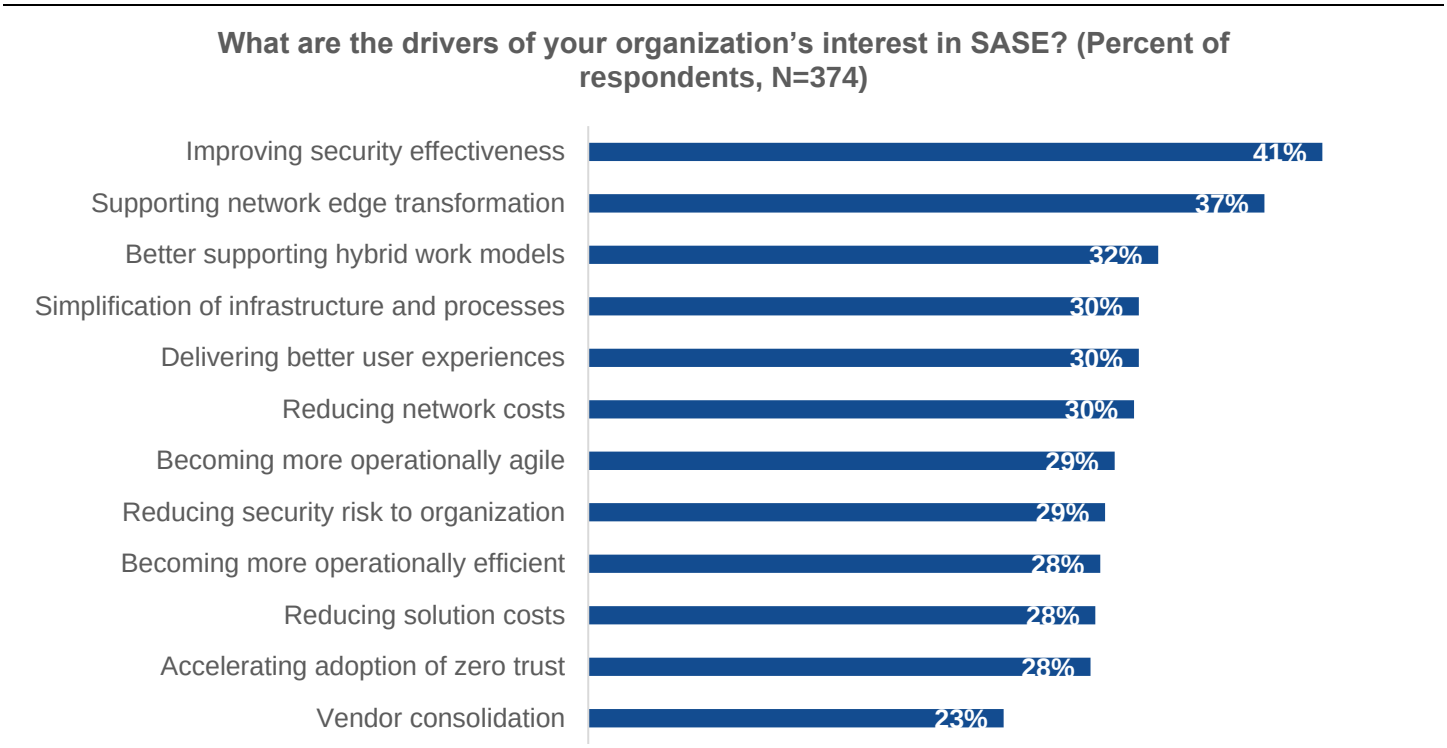
clear that organizations are not seeing the outcomes they expected from traditional SD-WAN solutions. Reasons for interest in changing include reducing operational complexity (33%), connecting directly to applications (32%), and reducing cost as well as providing better ROI (32%).

SASE Aims to Converge SD-WAN and Security but Can Fall Short

To address many of these issues, organizations are beginning to explore SASE, which converges network and security capabilities in a single, cloud-centric solution. While the list of capabilities is long, some of the core functionality includes SD-WAN and autonomous digital experience management on the network side, and zero-trust network access, secure web gateway, cloud access security broker, and firewall as a service on the security side.

Many of the top drivers cited for SASE interest align directly with the challenges previously discussed (see Figure 2). Supporting network edge transformation (37%), better supporting hybrid work models (32%), simplifying infrastructure and processes (30%), and becoming more operationally efficient (28%) all feature prominently on the list. However, when traditional SD-WAN is simply bolted onto security capabilities—even when converged—achieving these desired results becomes much more difficult.

Figure 2. Top Drivers for SASE



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

SASE Must Incorporate Zero Trust That Extends Beyond Users

So, what's needed? Zero-trust architectures continue to gain traction at a wide range of organizations to improve security outcomes. The breadth of zero trust results in a vast array of starting points and drivers, some tactical and others strategic. A tactical example, and one of the most common zero-trust drivers, is enabling secure remote

access for employees and/or third parties, which was cited by 41% of ESG research respondents.[4] On the other end of the spectrum is an example of a strategic driver: cybersecurity program modernization, which 51% of organizations cited. With so many organizations taking a broad view of zero trust, it becomes clear that the initiative must expand much more broadly beyond users.

Expanding Zero Trust to All Connectivity Through Zero Trust SASE

To better facilitate true network transformation, organizations should consider a zero-trust networking model through SASE. As was shown in Figure 2, 28% cited accelerating the adoption of zero trust as a SASE driver. However, these initiatives must be more closely aligned to support network and security transformation.

In an environment built around zero-trust networking, security is decoupled from network transport. The network simply becomes the plumbing, while zero-trust networking provides the intelligence to enforce policy. Most importantly, this default-deny model must be extended across all communications, including users, clouds, and physical locations. Through this non-routable architecture, malicious insiders or curious employees can be prevented from accessing anything to which they are not entitled, attackers can be blocked from moving laterally from workloads and locations across the environment, and granular segmentation can be enforced to ensure connected devices are not exploited.

In an environment built around zero-trust networking, security is decoupled from network transport. The network simply becomes the plumbing, while zero-trust networking provides the intelligence to enforce policy.

In addition to preventing lateral movement and extending across all communication paths, zero-trust SASE architectures should reduce operational complexity and cost. By centralizing a range of capabilities, security teams can more efficiently apply policy that is consistent across all parts of the organization, leveraging multiple threat-detection mechanisms such as intrusion prevention, sandboxing, behavioral analysis, and data loss prevention, and ideally achieving cost savings by consolidating with a trusted vendor partner.

Finally, security teams today must protect the business but do so while enabling productivity and supporting users. So, while security capabilities are paramount, supporting a strong user experience is critical for zero-trust SASE solutions as well. This requires understanding the normal performance of networks, applications, devices, and connections; quickly diagnosing when issues occur; and providing remediation so that users can get back to work quickly.

Through these capabilities, zero-trust SASE solutions can help organizations close security gaps and achieve the benefits traditional SD-WAN deployments could not deliver.

Zscaler Zero Trust SASE

Zscaler is well known as a leader in securing user access to the internet and applications. It has expanded well beyond those roots and now provides comprehensive zero-trust SASE through the Zscaler Zero Trust Exchange. The Zscaler Zero Trust Exchange is a cloud-native platform that connects users, workloads, and locations without putting them on the corporate network, helping organizations support holistic zero-trust initiatives. The Zero Trust Exchange runs across more than 150 data centers worldwide, putting the service close to users and applications and using the shortest path between users and their destination to provide consistent security and performance for a strong user experience.

[4] Source: Enterprise Strategy Group Research Report, *The State of Zero-trust Security Strategies*, April 2021.

Zscaler's Zero Trust SASE solution supports zero-trust-based network transformation across four key areas:

- **Zero Trust SD-WAN.** Zscaler's newest capability, Zero Trust SD-WAN, provides branches and data centers with fast, reliable access to the internet and private applications without the implicit trust present in traditional SD-WAN, offering strong security and simplified operations. Branch communications are securely forwarded to the Zero Trust Exchange, where Zscaler Internet Access (ZIA) or Zscaler Private Access (ZPA) policies can be applied. This includes full security inspection and identity-based access controls for all branch and data center communications.
- **Zero Trust for Users.** To address the user-to-application use case, Zero Trust for Users provides secure and performant internet and SaaS access while protecting against advanced threats and data loss via ZIA. It connects users seamlessly and securely to private applications, services, and OT devices through ZPA. Further, it ensures a strong user experience to optimize performance and quickly identify and remediate application, network, and device issues via Zscaler Digital User Experience (ZDX).
- **Zero Trust for Workloads.** Shifting to non-user connectivity, Zero Trust for Workloads helps organizations securely enable application-to-application communications across clouds, the internet, and on-premises environments. It is deployed via virtual machines called Cloud Connectors, which forward traffic to the Zscaler Zero Trust Exchange. The Cloud Connectors apply least-privilege access to enforce zero-trust policies by forwarding data from the workloads to the Zero Trust Exchange. Policies for cloud workloads are managed centrally in the same ZIA and ZPA consoles administrators use to protect users, helping to improve operational efficiency and reduce the likelihood of human error when writing policies.
- **Zscaler for IoT and OT.** Finally, Zscaler for IoT and OT provides device visibility across all connected devices, servers, and unmanaged devices across the business. Based on this visibility, organizations can create zero-trust policies to secure connectivity to OT equipment from any location, secure access for IoT devices to the internet, secure device-to-device communications, and protect device-to-application connections.

Conclusion

While most recognize the importance of modernization initiatives such as SASE and zero trust, the perceived complexity of such undertakings can cause organizations to take pause. Determining where to begin, choosing the correct tools to support both short- and long-term needs, and ensuring those tools work in concert and do not introduce friction for users can all be difficult. This makes identifying solutions that can help unify these projects and specifically address these challenges critical.

Platforms that provide native integration across a range of capabilities to promote efficiency, cover a range of use cases to provide flexibility and help expand initiatives over time, and ensure both strong security and a seamless user experience should be prioritized. Zscaler's Zero Trust SASE approach checks each of these boxes by supporting zero-trust-based network transformation across users, workloads, SD-WAN, and IoT/OT. Any organization moving forward with a zero-trust or SASE implementation would be well served to consider Zscaler.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

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