SPOTLIGHT

Sponsored by: Cisco

User access decisions must be based on the most secure route for a seamless user experience across *all* private and public applications and resources.

Flexibility in Convergence: Delivering on the Promise of Security Service Edge

August 2024

Written by: Christopher Rodriguez, Research Director, Security and Trust, and Pete Finalle, Research Manager, Security and Trust

Introduction

The security needs of the modern digital business are vastly complex, spanning various devices, user groups, and locations. Users need secure access to enterprise applications and resources via a consistent, frictionless experience — whether they are onsite, in a branch office, at home, or on the road. Business benefits of remote and hybrid work models include increased productivity and job satisfaction. Unsurprisingly, connectivity and security systems for these remote and in-office users remain a top priority as business leaders hope to foster greater communication and collaboration.

In recent years, applications and data have left the confines of the datacenter. Users require flexible work models more now than ever, and the proliferation of cyberthreats is driving a necessary change in networking and security architecture. Enterprise IT organizations use multiple clouds in hybrid models to balance the privacy, scalability, performance, and cost considerations that come with aggressive digital expansion. Web and software-as-a-service (SaaS) applications are also increasingly playing a role in enterprise IT architecture. Overall, the rapid adoption of SaaS applications, cloud computing, BYOD, and remote access use cases has increased complexity, expanded the attack surface for cybercriminals, and introduced a slew of specialized security concerns.

AT A GLANCE

KEY STATS

Risk is unlikely to abate as businesses continue to invest in the cloud and hybrid work environment. In detail:

- 31% of businesses noted "flexible work models" as the most important investment for continued business growth, according to IDC's March 2024 *SSE/SASE Buyer Adoption Survey.*
- The top challenge for supporting flexible work models was "securing across endpoints, networks, and cloud" (37%), according to IDC's March 2024 *Future Enterprise Resiliency and Spending Survey, Wave 3.*
- 84.7% of SSE/SASE buyers prefer or strongly prefer a single vendor solution for all components of an SSE/SASE solution, according to IDC's March 2024 *SSE/SASE Buyer Adoption Survey.*

KEY TAKEAWAY

By approaching security modernization strategies such as ZTNA and SSE in a smart manner, businesses can unlock performance and security benefits.

The traditional approach to cybersecurity has been to invest in one-off security tools to address the ever-changing threat landscape. This point product approach has started to produce diminishing returns over time. Specialized security tools operate in silos, with each new tool requiring a subsequent investment in time and personnel to deploy and operate properly. The point product approach introduces inconsistencies in protections and policies across use cases and environments. Without standardization, security gaps appear, the risk of a data breach increases, and the user experience suffers.

Converging and consolidating these security technologies is a strategic step toward modernizing network security architecture to meet the dynamic needs of modern digital businesses. Security service edge (SSE) is a security platform that unifies key network security technologies such as zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateway (SWG), and firewall as a service (FWaaS), in addition to optional capabilities such as data loss prevention (DLP), remote browser isolation (RBI), digital experience monitoring (DEM), and sandboxing. These critical network security functions are integrated into a single coherent cloud service for effective, all-encompassing protection. Furthermore, when combined with software-defined wide area network (SD-WAN) capabilities, the technology stack is referred to as secure access service edge (SASE). IDC's 2024 *SSE/SASE Buyer Adoption Survey* found that 84.7% of SSE/SASE buyers prefer or strongly prefer a single vendor solution for all components of an SSE/SASE. The addition of DEM for performance and optimization purposes helps elevate SSE from a security-only solution toward a comprehensive networking and security platform.

While there is no "magic pill" for cybersecurity, the SSE approach addresses key security and business concerns in a modern world. SSE consolidates several critical network security technologies into a single security solution, leveraging a common cloud architecture to perform necessary edge security functions. This eliminates the need for hair-pinning traffic back to a datacenter for inspection or to multiple security clouds for specific functions. The single pass, single cloud approach reduces latency and improves performance. It also provides the opportunity to apply zero trust principles across multiple use cases to reduce the attack surface and the risk of lateral movement.

Zero Trust Principles Are an Essential Part of SSE

SSE uses ZTNA to provide secure access to protected enterprise applications. Zero trust principles of least privileged access, complete segmentation and separation of protected assets from the internet, strong authentication, granular contextual policies, and continuous threat detection underpin ZTNA. ZTNA evolved in response to the limitations of a VPN, improving both security efficacy and user experience.

However, the path to ZTNA has not been without its challenges. Traditional VPNs are good for network-level access but not for app-level control. As a result, traditional VPNs offer opportunities for threat actors to move laterally throughout a network after an initial compromise. So organizations increasingly looked to ZTNA for app-level control. But existing, industry-defined ZTNA solutions do not work well with applications that are server initiated or feature dynamic protocols such as VoIP. Latency-sensitive and legacy apps can also cause issues for ZTNA. Ideally, ZTNA should allow users to work as if they were in the office with secure, frictionless access to all applications (not just some). For the security professionals who manage ZTNA policies, the ease of management, implementation, and usage is a necessary consideration.

The Trends Driving the Core Themes of SSE

The network security market is undergoing much-needed convergence. Security vendors have shifted their focus from à la carte, individualized security services to SSE — a consolidated, cloud-delivered, network security service. SSE has four essential capabilities: SWG, CASB, ZTNA, and FWaaS. These core capabilities address the following key use cases, which are frequently cited as top-of-mind concerns for securing users, their access, and devices:

- The protection of users, data, and devices accessing the web from malware, phishing, and other data theft, risky, or unapproved activities
- The security and privacy of users accessing internal applications
- The control and privacy of data accessed and generated in cloud applications

Convergence does not happen overnight, and the definition of SSE continues to evolve. Vendors also incorporate existing network security technologies adapted to the demands of a cloud delivery model. FWaaS is a pertinent example because it provides the ability to extend security controls to users, resources, device types, and use cases beyond what is possible with SWG, CASB, and ZTNA. To further boost the security posture, SSE also includes optional add-on services such as sandboxing, RBI, DLP, web application firewall, and deception. These additional capabilities are available as add-on subscriptions or built-in features, and they assist buyers in addressing specific use cases.

On a strategic level, SSE vendors strive to not only deliver consolidation and bundled pricing but also provide customers with greater value as competitive differentiators. True integration of key technologies such as SWG, CASB, and ZTNA delivers notable improvements in capabilities. For example, a unified agent simplifies the deployment process and updates, while consuming fewer resources on the device. A unified console provides simplified management and policy implementation and streamlined reporting. When implemented correctly, SSE delivers improved security posture and outcomes, as well as performance benefits that support business productivity and security goals.

However, even during convergence cycles, enterprise IT buyers face a practical need to focus on specific security use cases. These buyers will often prioritize certain functions over others at various points in their security maturity cycles. As enterprises work to modernize their cybersecurity systems, opportunistic SSE adoption will accelerate. Furthermore, despite SSE's promotion of a single-solution approach, vendors have found significant success by offering an entry point into the solution, such as SWG or ZTNA, which provides a foundational level of protection against modern threats. As their clients' renewal cycles allow, the strategy allows SSE vendors to eventually displace their competition.

Considering Cisco

Cisco has long offered a broad portfolio of security essentials such as firewall, SWG, and VPN, before introducing the Cisco Security Cloud in 2022. Cisco Security Cloud is a cloud-native platform with a comprehensive set of integrated security and networking services: unified management and policies, generative AI, detection and response services including threat intelligence, endpoint detection and response (EDR), extended detection and response (XDR), and open APIs to enable third-party solutions, as well as a security marketplace. Cisco offers an SSE solution (Cisco Secure Access) built on the Cisco Security Cloud, so customers can take advantage of the platform's many value-added capabilities on top of a completely re-architected and fortified SSE solution.

Cisco Secure Access Overview

Cisco Secure Access intelligently enables a seamless user experience for all private and public applications and resources, using the most secure connectivity — zero trust access or fallback catchall VPN as a service (VPNaaS) — as defined by the centralized access policy. The solution leverages capabilities from Cisco's security and networking portfolio, including embedded internet and cloud network visibility from Cisco ThousandEyes.

The solution contains a broad set of capabilities including:

- Secure web gateway
- Cloud access security broker
- ZTNA (client-based and clientless)/VPNaaS
- Firewall as a service
- DEM
- DNS security
- Remote browser isolation (RBI)
- Data loss prevention (DLP), including GenAI visibility and control
- Sandboxing/advanced malware protection
- Talos threat intelligence
- AI assistant: GenAI guided help for IT admins

In addition, the Cisco portfolio includes networking and operations functionality such as:

- **Digital Experience Assurance:** Beyond the DEM capability included in Secure Access, customers with ThousandEyes licenses can get extended visibility across networks and the internet.
- **SD-WAN:** Catalyst and Meraki are available for a single vendor SASE environment with advanced networking capabilities to optimize reliability, performance, and cost.

This converged solution enables improved efficiency through a single agent (called Secure Client), a single management console for viewing traffic, setting policies, and analyzing risks; a single identity and posture assessment; and a single policy management system. It is also part of the Cisco Security Cloud, which provides a comprehensive cloud-native management platform and unified dashboard — complete with an identity, posture, unified policy, design system, and service-level agreement — that enables better threat protection and easier realization of benefits across the Cisco portfolio. Consolidated licensing enables lower costs, requires fewer people for management, and reduces or eliminates the need for hardware.

Delivering SSE with Flexible ZTNA Advantages

Secure Access consolidates and innovates Cisco's deep portfolio of technologies to provide secure, identity-based access for all users and private applications in the cloud or on premises. It also supports client-based or clientless scenarios.

Unlike traditional ZTNA that is built with a reverse proxy architecture, Cisco takes a unique approach through a more modern zero trust access (ZTA) relay architecture. This architecture reduces the attack surface and enables an enhanced level of enterprise privacy by giving organizations more control over their data and inspection points. It enables them to easily create policies that enforce whether specific traffic is routed through cloud security or routed directly to their edge security device.

The unified agent in Cisco Secure Access offers a single, consistent, and powerful solution for access control of all applications and network protection. This single agent supports several subservices — zero trust access, VPNaaS, health agent, DEM, and network visibility monitoring (process, user, and network telemetry to XDR) — thus reducing the burdensome configuration and management tasks required to support multiple security agents. In addition, a unified console, from which all policy configuration and management is done, enables device posture-based controls and provides a single dashboard for managing ZTNA, VPNaaS, and other SSE security components. These two unification elements — the single agent and single console — reduce risk, streamline the user experience, and improve management efficiency.

Importantly, Cisco offers implementation flexibility such as support for ZTNA resource connectors or backhaul VPNaaS, lowering adoption barriers for organizations with complex environments that want to migrate at their own pace. Deployment flexibility is further achieved through support for integration with both Cisco and third-party SD-WAN solutions, as well as flexible tiered packaging to aid customers on their zero trust journey.

Characteristics and Capabilities

Cisco Secure Access offers several advanced capabilities to meet the steep demands of a ZTNA and SSE transformation:

- **Performant protection:** The solution enables multiple connection methods, including the Multiplexed Application Substrate over QUIC Encryption (MASQUE) framework, which provides a fast and secure end-to-end zero trust ecosystem. The technology also allows for relaying through multiple hops without any added encryption. Proxying improves client privacy by concealing a client's IP address from the target server.
- **Device-level zero trust control:** MASQUE enables OS vendors to enable zero trust access directly from the device, eliminating the need for a vendor-specific ZTNA or VPN software implementation. Cisco integrates with Samsung's and Apple's support for MASQUE relays to enable the secure access feature in Android and iOS, respectively. The ability to bring microsegmentation all the way to the application running on the device is an advantage of these new OS-native zero trust access implementations. It provides a better experience for both the user and IT staff by reducing the number of agents and agent-related management tasks.
- **AI for productivity enhancement:** The GenAI assistant can convert natural language phrases directly into security policy, helping admins to save time, reduce complexity, and prevent possibility of "human error."
- **Identity-based approach:** Integration with Duo deepens posture assessment and streamlines user authentication tasks for improved security and user experience. Cisco's focus on identity is shown by augmented capabilities being rolled out that use additional identity attributes and behavioral analytics to detect compromised accounts and limit the "blast radius" of an identity incident. These capabilities are powered by integrations with key Cisco technologies (Duo, Identity Services Engine, and Cisco XDR) and third-party identity tools.
- **End device performance:** The new OS-native implementations of zero trust access improve performance by removing the need for the kernel-to-user-mode bump that ZTNA and VPN clients require. This not only enables zero trust microtunnels to exist entirely within the applications but also eliminates the need for context switching to encapsulate application traffic.
- **DNS security:** The solution starts with a powerful DNS security function, allowing Cisco Secure Access to effectively identify and block the majority of malicious traffic very early in the process (before engaging the many other layers of inspection). Cisco security services process over 600 billion DNS requests and 2.8 million malware samples per day, blocking over 170 million malicious domains daily. This level of visibility enables Cisco to discover and block new threats quickly and share that protection across a range of security functions.
- **Simplified troubleshooting:** DEM capabilities significantly reduce the time to resolve remote or hybrid worker issues by quickly providing key performance insights to the IT help desk team. IDC's 2024 *SSE/SASE Buyer Adoption*

Survey found that only 20% of companies with a mature SSE/SASE adoption (ZTNA, SWG, CASB, and optional components) with adequate visibility into the network were not utilizing some form of DEM. Rapid resolution of user problems improves the productivity of both end users and the IT staff that supports them.

Challenges

One challenge that organizations face is getting the full visibility and deep insights needed to optimize all environments their customers and employees depend on, across clouds, the internet, and enterprise networks. With DEM, Cisco Secure Access provides a significant portion of that, with a focus on visibility into the user's experience and endpoint performance. However, more is needed. Customers need an end-to-end view of the data path from the user to the application to isolate performance problems. To address this, Cisco is continuously building deeper integration with ThousandEyes to bring intelligent insights into the native Secure Access dashboard. In the meantime, customers can optionally purchase a ThousandEyes license for that fuller capability.

Conclusion

Modern SSE buyers are expecting more than just a change in form factor, and with expanding security feature sets and capabilities, vendors are answering the call. However, with increased functionality comes additional complexity, and helping customers get to the finish line is an important measurement of success for any SSE product. Cisco has made significant strides in not only providing a full-featured SSE product but providing the necessary tools for customers to successfully deploy and manage it. Seamless integration of a cutting-edge AI assistant and advanced DEM visibility allows customers to actively pinpoint and remediate configuration issues, policy complexities, and network architecture deficiencies that have historically plagued large-scale network security migrations. With the recent progress and continuing development efforts that are underway, Cisco has a significant opportunity for continued success in this market.

Seamless integration of a cutting-edge AI assistant and advanced DEM visibility allows customers to actively pinpoint issues and actively remediate them.

About the Analysts

	Christopher Rodriguez, *Research Director, Security and Trust* Christopher Rodriguez is a research director for IDC's Security and Trust research practice focused on the products designed to protect critical enterprise applications and network infrastructure. IDC's Security and Trust research services to which Chris contributes include network security products and strategies as well as active application security and fraud.
	Pete Finalle, *Research Manager, Security and Trust* Pete Finalle is a Research Manager for IDC's Security and Trust team, currently responsible for the Trusted Access and Network Security coverage area. Pete's core research coverage is focused on network security hardware, software, and public cloud services, spanning foundational components like firewall, IDS/IPS, VPN, NAC, SWG, and CASB, as well as new concepts like ZTNA and SSE.

MESSAGE FROM THE SPONSOR

Security convergence and the adoption of zero trust architectures are driving many organizations to rethink their security strategy. At the same time, organizations are still adapting to hybrid work environments. They need a security stack that simplifies operations, blocks threats, and provides zero trust–based access to *all* public and private applications and resources, and it needs to do all this regardless of where users are located.

Cisco Secure Access facilitates this goal by consolidating twelve security technologies into one unified, cloud-delivered platform. It is designed to connect end users seamlessly and securely to anything from anywhere, while simultaneously reducing the management burden on IT operations. It mitigates risk by applying zero trust network access (ZTNA) principles and enforcing granular security policies. It simplifies and automates IT operations through a single, cloud-managed console and client, centralized policy creation, and aggregated reporting.

Learn more about Cisco Secure Access.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or an opinion about the licensee.

External Publication of IDC Information and Data—Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.