IDC

SPOTLIGHT

Sponsored by: Cisco

The need for enhanced security that is business-friendly and respects the importance of the user experience is accelerating demand for integrated security service edge platforms.

Extending SSE Benefits with a More Holistic Approach to Universal ZTNA

June 2025

Written by: Frank Dickson, Group Vice President, Security and Trust, and Christopher Rodriguez, Research Director, Security and Trust

Introduction

The traditional approach to cybersecurity — relying on increasing numbers of single-function appliances and specialized services — has proven to be incompatible with the rigors of a modern enterprise IT environment that is complex and expansive. Legacy, point-product security strategies introduced 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 was a critical first step toward aligning network security architecture to meet the dynamic needs of modern digital businesses. Security service edge (SSE) promised to deliver a solution to address this reality, offering a framework that aimed to consolidate key network security technologies, such as zero trust network access (ZTNA), cloud access security broker (CASB), and secure web gateway (SWG). Secure access service edge (SASE) is an even broader combination of both SSE and software-defined wide area network (SD-WAN) functionality to efficiently connect and protect all users as they access both private and public resources.

AT A GLANCE

WHAT'S IMPORTANT

Today's SSE offers a single, consistent, and powerful solution for access control and network protection to all applications, including private applications, legacy applications, SaaS, and the internet. What's missing in many cases is:

- Intelligent use of deep identity context and dynamic user trust scoring
- Integration with networking and network security devices to ensure optimum performance and enable flexible enforcement options
- Zero trust access for IoT/OT devices
- End-to-end traffic visibility and troubleshooting

However, new technologies continue to emerge and introduce new security requirements. For example, generative AI (GenAI) is a high-visibility innovation that introduces additional security risks and considerations. ZTNA is one key aspect of SSE that must evolve beyond initial definitions to meet modern enterprise needs for secure access. Vendors are racing to deliver new ZTNA capabilities to address emerging threat vectors and extend the benefits of SSE across the entire IT environment and its use cases.

Modern solutions extend key zero trust practices to provide holistic protection through capabilities such as:

- Enhanced identity context insights and monitoring
- Networking and security integrations to balance optimized performance and flexible enforcement

- Zero trust access for IoT/OT devices
- End-to-end traffic visibility and troubleshooting

These extended requirements go beyond the traditional SSE platform, but they are essential to creating a truly universal zero trust environment across all applications, users, things, and locations. Including this set of functions can elevate the benefits of SSE to a higher level with tighter security while making the job of security professionals easier and delighting end users.

The Benefits of a Universal Zero Trust Access Transformation

Convergence Enhances Security Posture and Usability

While there is no "magic pill" for cybersecurity, the SSE approach addresses key security and business concerns. SSE consolidates several critical network security technologies into a single security solution, leveraging a common cloud architecture to perform necessary security functions at the edge.

As organizations adopted SSE, platforms largely delivered on the initial promises and security postures drastically evolved after the rollout of the core SSE components. According to IDC's March 2025 *SSE/SASE Buyer Adoption Survey,* 64% of respondents felt that their security posture remained consistent during migration (partial adoption). 27% felt that their security posture improved during the migration phase, 51% reported posture improvement once their adoption was complete, and 28% felt that their security posture drastically improved by the complete adoption phase.

The key takeaway is that security posture dramatically improves with the adoption of a solution that integrates ZTNA, SWG, and CASB. Adoption of SSE led to overall improvements in security posture, threats detected, false positives reduced, threats blocked, and network performance.

However, there is an opportunity to magnify the efficiencies and further reduce risk with additional convergence. For example, the number of attacks leveraging compromised identities is still much too high. There is a need for more rigorous posture checking at the onset and visibility into questionable behavior during sessions to more quickly detect a problem and restrict or even curtail access if appropriate. This additional identity-based security needs to apply to IoT/OT devices and users.

Advancing to Universal ZTNA for Holistic Protection

SSE includes ZTNA capabilities that allow organizations to create and enforce granular access policies that limit user access to only the resources required for a specific role or group. ZTNA enhances security posture by enforcing 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. ZTNA enhances the remote user experience, allowing users to work as if they were in the office, with secure, frictionless access to all applications (not just some). For security professionals that manage ZTNA policies, ease of management, implementation, and usage are necessary considerations.

Some hybrid worker scenarios still present challenges for both the security team and end users. Administrators have a broad mix of private applications to support. While they are happy to route the majority through a cloud inspection point, they usually have some application traffic that they want to go directly to a local inspection point for privacy or compliance reasons. End users want the best experience possible, so if they are in the same location as a private app, it

doesn't make sense to hairpin them through a cloud POP. Both situations require the ability to have easily configurable enforcement options. While cloud-based ZTNA covering user access to private apps is core, the aforementioned use cases and the growing number of connected devices (IoT/OT) need to be incorporated in an efficient, least privilege approach.

Today, delivering secure access to just private enterprise applications is not enough. Software as a service (SaaS) has become foundational to modern business. End users now have more flexibility and administrator sway over data sharing settings within traditional SaaS applications such as documents, spreadsheets, slides, email groups, chat messages, no-code/low-code integrations, and open authorization connections. New categories of SaaS, such as customer databases, corporate IP, and production access, are part of this concern. Whether a customer list is stolen out of a production database or from a rogue SaaS marketing app, the same reporting obligations and brand damage apply.

In addition to the growth of SaaS, the rise of AI, specifically GenAI, has elevated the risk to the organization. The use of AI applications and APIs requires data loss prevention (DLP) control of both prompts and responses, as well as guardrails to protect against prompt injections, toxic content, and inappropriate use of code. DLP has historically been tightly integrated with CASB as a means of protecting data, which is increasingly transferred to and from cloud resources. While this has been a convenient relationship for these two technologies, the newfound role of CASB as a core integrated component of SSE has deepened its ties to other technologies (i.e., ZTNA and SWG). The tight integration of DLP with CASB has made it one of the most commonly adopted extended security capabilities typically offered with an SSE/SASE. Only 21% of SSE/SASE buyers feel that DLP should remain separated from the SSE/SASE solution, and a small minority (3%) is simply not interested in DLP at this time, according to IDC research. Thus 76% of all SSE/SASE buyers either have already adopted integrated DLP capabilities with their platform or are interested in doing so. Recent interviews with DLP buyers have indicated that extending to DLP with their SSE/SASE platform offers significant cost benefits, as well as a more cohesive user experience.

The reality is that device coverage is about more than just user devices and also includes devices related to IoT and OT. As a part of IDC's 2025 *SSE/SASE Buyer Adoption Survey,* most respondents confirmed that they are securing an IT ecosystem. However, many had additional resources to secure outside of IT, with IoT/smart building ecosystems requiring attention from 59% of SSE/SASE buyers. This trend showed up again in a follow-up question regarding SSE/SASE adoption challenges, where 30% of respondents indicated that OT/IoT devices are a significant challenge when adopting/deploying an SSE/SASE solution. In addition, while IoMT and OT have a smaller presence than IoT and IT ecosystems, they are essential within specific vertical markets, such as the medical, manufacturing, and oil and gas industries. These more specialized vendors are actively looking to modernize and harden the security of their non-IT ecosystems and manage security within the same interface as their IT ecosystem.

Today's SSE offers a single, consistent, and powerful solution for access control and network protection to all applications, including enterprise applications, legacy applications, SaaS, and the internet. Importantly, a single SSE agent can support ZTNA, device protection, compliance, and DLP, reducing the high resource usage necessary to support multiple security agents. The convergence strategy also offers centralized control and reporting through a single pane of glass.

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 three foundational capabilities: SWG, CASB, and ZTNA. These core capabilities, augmented with additional SSE features such as

DLP, DNS security, and digital experience monitoring (DEM), address the following key use cases, which are frequently cited as top-of-mind concerns for securing users and their access and devices:

- Safeguarding web users from malware, phishing, other data theft, and risky or unapproved activities
- Ensuring the security and privacy of users accessing all applications, regardless of delivery, user location, or device
- Ensuring the security and privacy of data accessed and generated in cloud applications
- Addressing emerging GenAI risks
- Upgrading the end-user experience
- Protecting IoT and OT as well as users
- Extending visibility into off-network devices and traffic
- Enhancing protection against identity-based attacks

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. Firewall as a service (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. SSE also includes optional add-on services to further boost security posture, such as sandboxing, remote browser isolation (RBI), DLP, web application firewall, DEM, and deception. These additional capabilities are available as add-on subscriptions or built-in features, and they assist organizations in addressing specific use cases.

On a strategic level, SSE vendors strive not only to deliver consolidation and bundled pricing but also to provide customers with greater value as competitive differentiators. True integration of key technologies such as SWG, CASB, ZTNA, DEM, and DLP is driving improved security posture, user experience, business productivity, and security outcomes.

However, even during convergence cycles, enterprise IT organizations face a practical need to focus on specific security use cases. They 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 enables vendors to eventually displace their competition with a full SSE platform and an even more extensive universal ZTNA approach.

Considering Cisco's Universal ZTNA Approach

Cisco is a long-standing network infrastructure and cybersecurity vendor that first launched its converged SSE solution in 2019. The company now has a security portfolio with increasing levels of integration among its components for SSE and beyond. This includes all core SSE components as well as DNS, DLP, DEM, and RBI. Cisco has integrated a set of identity intelligence features to better secure the initial access and adapt to threatening behaviors during a user session. In addition, Cisco's road map includes multiple new capabilities that go beyond SSE and into related security and network infrastructure technologies.

Cisco Secure Access Overview

Cisco Secure Access intelligently automates user access decisions based on the most secure route, resulting in a seamless user experience for all private and public applications and resources. The solution leverages capabilities from Cisco's security and networking portfolio, including embedded internet and cloud network visibility from Cisco ThousandEyes.

The solution contains the following product features:

- Secure web gateway
- Cloud access security broker
- ZTNA (client based and clientless)
- Firewall as a service
- VPN as a service (VPNaaS)
- Digital experience monitoring
- Cisco AI Access with discovery and control for over 1,200 AI applications currently
- DNS security
- Remote browser isolation
- Data loss protection
- Advanced malware protection
- Sandboxing
- Talos threat intelligence
- User trust scoring
- End-to-end visibility and troubleshooting recommendations

The converged solution enables improved efficiency through a single agent, management console, identity and posture assessment, and policy management system. It is also part of Cisco Security Cloud Control, which provides a comprehensive cloud-based management platform — complete with identity, posture, unified policy, design system, and service-level agreement — designed to enable better threat protection and easier realization of benefits across the Cisco security portfolio. Essentially, there is a single location that allows for viewing traffic, setting policies, and analyzing risks. Consolidated licensing enables lower costs, requires fewer people for management, and reduces or eliminates the need for hardware.

Delivering SSE with Flexible ZTNA Options

Prior to Secure Access, Cisco had many existing security technologies, such as Duo-based identity controls and its Cisco Umbrella cloud service. Cisco Secure Access leverages these technologies to provide secure, identity-based private access for all users, for all applications in the cloud or on premises, and with client-based or clientless controls.

The Cisco Secure Client is a unified agent that supports VPN, VPNaaS, and ZTNA and protects over 180 million endpoints. It enables device posture–based controls and provides least privilege access to both private and internet/SaaS destinations to reduce risk and improve efficiency.

Importantly, Cisco offers implementation flexibility, such as support for ZTNA Resource Connectors or backhaul VPN, lowering adoption barriers for organizations with complex environments. The solution allows organizations to leverage

existing network security investments, such as firewalls, as enforcement points, providing flexibility to choose cloud security or on-premises security to ensure an optimal user experience and a consistent level of protection. Support for integration with third-party, software-defined wide area network solutions or Cisco SD-WAN also helps achieve deployment flexibility. Cisco offers flexible, tiered packaging to aid organizations on their zero trust journey. This kind of flexibility is important because end customers are at various stages of their evolution and have a range of security gaps to fill.

Capabilities

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

- **Performant protection:** The solution uses 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 a target server.
- **Device-level zero trust control:** An OS vendor can leverage MASQUE to enable zero trust access directly from the device, eliminating the need for a vendor-specific ZTNA or VPN software implementation. Cisco, for example, has collaborated with Apple to enable the iOS Secure Access feature. The ability to bring micro-segmentation all the way to the application running on the device is an advantage of these new OS-native zero trust access implementations.
- **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 hooks at the DNS resolver layer, allowing Cisco Secure Access to effectively identify and block malicious traffic at a high level while coexisting with other solutions. Cisco Talos threat intelligence powers this service, processing over 600 billion DNS requests and 2 million malware samples per day, according to the company.
- **Automated troubleshooting:** Embedded DEM with Cisco ThousandEyes powering it significantly reduces the time to resolve help desk trouble tickets. According to Cisco, proactively alerting the user of connection issues and possible quick fixes has resulted in the ability to achieve a 95% reduction in deflectable calls, which can cost between $80 and $250 each. For example, most deflected calls involve a simple user-initiated remediation task, such as a reboot.

Challenges

If an organization is passionate about buying point products and integrating, Cisco's platform approach will be challenging. Cisco integrates SASE (SSE and SD-WAN) and identity functionality into its overall universal ZTNA approach to create synergistic outcomes. Both vendors and customers favor this approach. Respondents from IDC's 2025 *SASE Buyer Insights Survey* are more adamant that their SASE purchase comes from a single vendor than they were in 2024. 74% of survey respondents in 2025 indicated that it is either important or very important that their SSE/SASE solution comes from a single vendor for all components, which is 11% higher than in 2024. This indicates two trends:

- Organizations do not want any of their core SSE/SASE functionality compromised because it comes from multiple vendors (as there could be less integration).

» Organizations are more likely to consider adopting optional features/capabilities and components from their SASE vendor as a means to extend that tight integration between components as they expand.

In addition, many SSE/SASE products are now highly consolidated at the SKU level, meaning that purchasing à la carte products is becoming less common. If an SSE/SASE buyer purchases an SSE/SASE with a single SKU for all core capabilities (SWG, CASB, ZTNA, and SD-WAN), they are likely to adopt all these components as a means of maximizing their ROI from the investment. For 2025, under 1% of SSE/SASE buyers indicated to IDC that their solution coming from a single vendor was of no importance. Thus nearly all buyers at least somewhat embrace the idea that a single vendor can offer them either stronger security efficacy or better value than multiple vendors. However, this survey data does not include any companies or organizations that have no intention of purchasing an SSE/SASE.

Conclusion

Updated security tools and integrated platforms are necessary in the modern era of remote and hybrid work, distributed networks, and smart devices. As a result, the need for enhanced security that respects the importance of the user experience and is also business-friendly is driving the rapid expansion of the market for integrated platforms. IDC believes that Cisco is positioned to be among the next set of network security leaders driving the market — not only for SSE but also for the broader definition of universal ZTNA — and to the extent that Cisco can continue to execute and address the challenges this paper describes, the company has a significant opportunity for success.

About the Analysts

Christopher Rodriguez, *Research Director, Security and Trust*

Christopher Rodriguez is a research director in 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 and active application security and fraud.

Frank Dickson, *Group Vice President, Security and Trust*

Frank Dickson is the group vice president for IDC's Security and Trust research practice. In this role, he leads the team that delivers compelling research in the areas of security services; information and data security; endpoint security; trust; governance, risk, and compliance; identity and digital trust; IoT security; network security; privacy and legal tech; security analytics; video surveillance; and application security and fraud. Topically, he provides thought leadership and guidance for clients on a wide range of security topics including ransomware and emerging products designed to protect transforming architectures and business models.

MESSAGE FROM THE SPONSOR

Security convergence and the adoption of zero trust architectures are driving many organizations to rethink their security and networking architecture. They need to simplify operations, block threats, and provide zero trust–based access to all public and private applications and resources, regardless of where users and applications are located.

Cisco's Universal ZTNA approach includes an innovative SSE solution along with identity intelligence, flexible enforcement options, zero trust IoT/OT security, and end-to-end visibility with AI assisted troubleshooting. The Cisco Secure Access SSE solution alone consolidates twelve security technologies into one unified, cloud-delivered platform. Risk is mitigated by applying zero trust network access (ZTNA) principles and enforcing granular security policies across private and internet traffic. IT operations are simplified and automated through a single, cloud-managed console and client, centralized policy creation, and aggregated reporting.

Learn more about Cisco's Universal ZTNA approach and Secure Access SSE solution.

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
blogs.idc.com
www.idc.com