Business white paper

3 steps to SSE success

A simple guide to securing the anywhere and everywhere workforce

Perhaps the most terrifying words to today's CISOs are the words "anywhere" and "everywhere".

Alone, they may sound harmless enough. But they're big red flags for ensuring corporate IT security. In fact, a recent survey found that 94% of organizations are now operating on a remote or hybrid model.[1]

Unlike the well-defined enterprise IT environment of just a few years ago that mainly had self-contained resources and distinct access points, today's CISOs must protect corporate assets that can live anywhere while enabling access from everywhere.

In an IT world where corporate resources are spread across multiple cloud providers and distributed internal systems — and users can connect from anywhere — traditional security approaches aren't as viable as they once were due to limited scalability, new security gaps, diminished performance, and other shortcomings.

In addition, increased corporate IT complexity has introduced new security risks, while changes stemming from the adoption of cloud services, increased distributed remote and mobile workers, and reliance on SaaS-based solutions have made IT security more difficult, more costly, and more time-consuming.

As a result, many organizations are moving to a Security Service Edge (SSE) approach. A subset of Secure Access Service Edge (SASE), SSE is a combination of cloud-based security services that enable organizations to deliver unfettered access to business resources and services to users distributed anywhere — securely, and safely. With an SSE approach, security teams can provide enhanced protection to enable today's mobile and cloud-oriented environments, with greater scalability and flexibility, reduced complexity, better performance, cost efficiency, and more.

As good as all that is, those benefits only start to accrue after companies take their first steps toward SSE. That's why we've pulled together this roadmap for organizations that want to confidently and incrementally start on their SSE journey. With the right approach, CISOs and organizations can transform traditional corporate security to address today's complex anywhere and everywhere IT challenges while providing a secure cost-effective foundation for future growth and agility.

This paper provides a guide to accelerated SSE deployment and a blueprint for long-term success.

[1] 2024 SSE Adoption Report, Cybersecurity Insiders

SSE overview

SSE solutions are typically composed of a combination of essential services, including Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and integrated Digital Experience Monitoring (DEM). The services work together but can be deployed separately for an incremental approach to SSE.

The starting point: why SSE?

The significant interest in SSE among CISOs and IT security leaders is driven by two main things: changes in the enterprise IT landscape and the benefits of SSE.

- **Enterprise IT changes.** For years, traditional, network-centric approaches to security, such as virtual private networks (VPNs), worked reasonably well within conventional enterprise IT environments where most applications, services, data, and even users resided physically inside corporate facilities.

  However, those approaches proved much less feasible as the enterprise landscape evolved over the past five years. The rapid move to cloud computing and multi-cloud resources requires organizations to provide integrated security inside and outside their physical locations. The drive to more mobile connections and increased remote work requires security from anywhere and increased security of corporate assets. As business environments have increased in complexity and security risks, finding ways to enforce consistent security policies across the entire organization has become more critical than ever. Several other overarching trends are also contributing to this change, including increased cybersecurity threats, the shift to zero trust security models, increased regulatory compliance, and the need for cost efficiency and better user experiences.

- **Benefits of SSE.** An SSE approach offers a range of significant benefits. SSE enhances overall security through zero trust access for all business applications, whether it's private, public, cloud-based, or data center deployed. SSE improves compliance and risk management through automatic and continual checking and enforcement of security policies. It makes secure remote work from anywhere feasible, manageable, and efficient. It simplifies security management and administration, making monitoring easier while centralizing visibility and control. SSE also enhances user experience by streamlining access and security processes, optimizing connections, and enabling user productivity.

While there are many potential applications of SSE, a few of the typical use cases that initially attract organizations to deploy it include:

- Securely enabling remote and mobile workers everywhere
- Protecting and securing data and services anywhere
- Securing all cloud and web access
- Increasing overall cybersecurity posture while reducing threat exposure

The elements of SSE

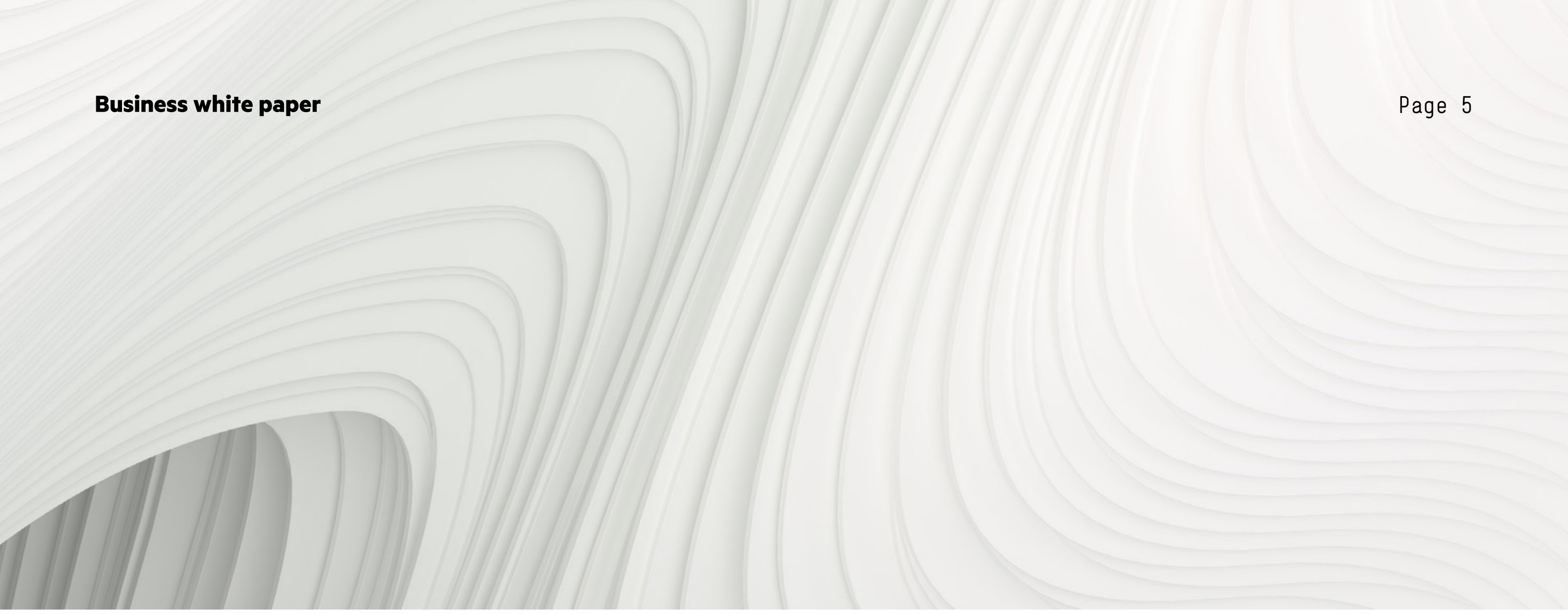
- **Zero Trust Network Access (ZTNA).** A vast improvement over traditional VPN access to private applications, ZTNA extends application access to remote users and allows access to only authorized resources after authentication. ZTNA essentially ensures that no user or device is trusted by default. Instead, all users and devices must pass robust identity verification processes to gain access to appropriate resources. Furthermore, least-privilege access is applied as users can access only the specified apps and data that admins permit.
- **Secure Web Gateway (SWG).** SWG is a core SSE service that manages internet access by applying company policies and preventing unwanted and unknown internet traffic from entering an organization's internal network. SWG protects users from accessing malicious websites, internet-spawned viruses, and malware, while still enabling users to access resources needed to get work done.
- **Cloud Access Security Broker (CASB).** A CASB provides an enhancement to the SSE security function. It enforces access and data loss prevention security policies as users and services access various corporate resources (whether cloud-based, private apps, etc.) and helps comply with company and industry security policies.
- **Digital Experience Monitoring (DEM).** DEM enables organizations to deliver a user experience that makes employees productive and safe. DEM monitors users' digital experience to ensure the system can handle spikes in CPU usage, network outages, and application performance challenges while giving IT visibility and metrics into each internet and network step.

Best practices for SSE Success

Regardless of your organization's size or industry, consider these best practices as you embark on your SSE journey:

- **Take an incremental approach.** While SSE can offer compelling benefits, what typically encourages CISOs and organizations to take their first SSE steps is the fact that they can move to SSE incrementally. An incremental approach to deploying SSE often makes the most sense for many organizations. That's why it's one of the best practices for SSE success.
- **Leverage small teams and focus on specific problems.** Organizations interested in SSE should leverage small teams and focus on critical issues in particular areas. This will create the environment for quick wins and allow the organization to build out from there.
- **Don't forget user experience.** A big part of any successful SSE deployment is ensuring it makes life easier for the users. The best approach for doing this is by considering security and experience in the same light and not neglecting one component for the other. SSE teams should use "employee eyes" when evaluating solution components and processes.
- **Focus on one SSE service first.** Another critical SSE best practice for quick success is not biting off more than you can chew. The first SSE project should likely use only some components of an SSE platform. The critical part is to start the move to SSE, and then add additional features or services as needed in the future, building on initial success.
- **Consider ZTNA as a first step.** Zero Trust Network Access (ZTNA) can be an ideal starting point for SSE success for many organizations. ZTNA replaces technology not initially designed for today's remote work and third-party access needs. It can be implemented independently and often provides an immediate upgrade from the traditional VPN user experience, while increasing performance and dramatically reducing security risks.

To implement these SSE best practices, it's best to take a three-step approach to your first SSE project: 1. plan, 2. execute, and 3. review.



While this paper uses a ZTNA service deployment as the initial SSE step for illustrative purposes, your organization can start with a different SSE component, such as their Secure Web Gateways (SWGs), if it better fits your business needs. The general steps for success will be similar.

Step 1: Planning

The first step to rapid SSE success is planning. While studying how a full SSE deployment might strategically impact your IT environment is a good idea, it's perfectly suitable to take a tactical approach to planning based on the initial deployed SSE service and the business problem you are trying to solve.

The basic steps for planning an initial SSE deployment include:

- **Assessment and planning.** Start by assessing your organization's security infrastructure and posture to identify possible shortcomings and potential needs. Then, select an initial project scope that maps to specific business or IT needs. A good place for many companies to start is with a ZTNA deployment for a particular group, application set, resources, or users. While this initial planning focuses on tactical objectives, it should include a longer-term view of security and business needs. That will help inform future steps and the choice of SSE provider.
- **Provider selection.** Selecting an SSE provider is an essential step in your SSE journey and will directly affect both initial and subsequent follow-on projects. After initial assessment and planning, your organization must evaluate potential SSE providers based on their specific capabilities and attributes and how they map to your specific IT and business needs. The choice of SSE provider should be informed by the assessment and planning done in the previous step. Factors to consider may include functional capabilities, reputation, cost, scalability, timing, integration capabilities, etc.
- **Deployment strategy definition.** As noted above, it's often ideal for an organization to start its SSE deployment with a single, core SSE component, such as ZTNA, SWG, or CASB. While defining a deployment strategy for the initial project, you should understand the project and define success through measurable security, productivity, and operational outcomes.

Step 2: Executing

After the step 1 components are done — assessment, selecting a provider, and defining a deployment strategy — it's time to focus on executing the deployment process.

ZTNA is an excellent choice for the first SSE service because it typically solves several pressing IT and business problems while also providing a strong foundation for added use cases in the future.

ZTNA is an excellent choice for the first SSE service because it typically solves several pressing IT and business problems while also providing a strong foundation for added use cases in the future.

ZTNA is designed to support the modern workforce with applications now outside the corporate network, and to support increasing remote access and even third-party access requirements, unlike traditional access technologies. A remote access VPN approach relied on an inflexible, hard to scale, "castle-and-moat" security strategy that often meant that once a user gained access to the VPN, they had lateral access to everything on the corporate network — a severe risk in today's world. In addition, VPNs often use just username and password authentication, making them an increasingly easy target for various security breaches and threats.

Additionally, a ZTNA approach keeps both security and its users "front-and-center" as it provides a much better user experience than existing solutions such as VPNs by eliminating "authentication fatigue" or the requirement for users to constantly pass through authentication hurdles across disparate IT resources and systems. ZTNA provides a genuinely frictionless experience for users.

ZTNA surpasses legacy VPN approaches, providing teams with a range of immediate and vital benefits, including:

- **Scalability, flexibility, and agility.** ZTNA excels in scalability and flexibility due to its cloud-delivered nature. As demand increases, so will the infrastructure's scale. The overarching SSE platform is designed to adapt to changing business requirements, making it easy to quickly support new applications, resources, users, or applications.
- **Granular access security.** While the user experience is critical, for CISOs, security is fundamental. ZTNA significantly improves remote and hybrid access security with fine granularity, ensuring remote users and devices are thoroughly authenticated before accessing resources, allowing users to gain application access without extending network access, and keeping the businesses environment invisible to threat actors.
- **Integration across cloud environments.** ZTNA easily integrates and supports cloud-based services and hybrid environments while maintaining advanced security. This allows organizations to use a single secure access solution to incorporate new additions to the business environment quickly, without compromising security, or adding complexity.
- **Greatly simplified user onboarding and offboarding.** A ZTNA-based security approach dramatically simplifies adding (or removing) users across distributed systems and resources. This zero trust approach ensures that users receive least-privileged access to authorized apps, while industry-standard System for Cross-domain Identity Management (SCIM) capabilities allow immediate termination of access, even mid-session.

While most organizations will choose a step-by-step approach to SSE, building on deployment success as they go, the long-term successful implementation of SSE requires an ongoing combination of strategic decisions, technical solutions, user involvement and education, and continuing management and refinement.

Implementing your first SSE service can be accomplished with in-house resources, although vendors and many consulting companies can also provide additional resources, guidance, and personnel.

Step 3: Reviewing

Long-term success with SSE doesn't stop once an SSE service is deployed. Instead, your organization must take the third and final step for SSE success — reviewing. This step also includes optimizing SSE service deployments as they and the IT environment evolves.

Because SSE deployments are often iterative and can have a significant impact on users as well as corporate and IT capabilities, CISOs and their organizations must take time to review all SSE projects to fine-tune them for the future and to identify improvement areas for future deployments. Among the areas that cybersecurity teams should review are:

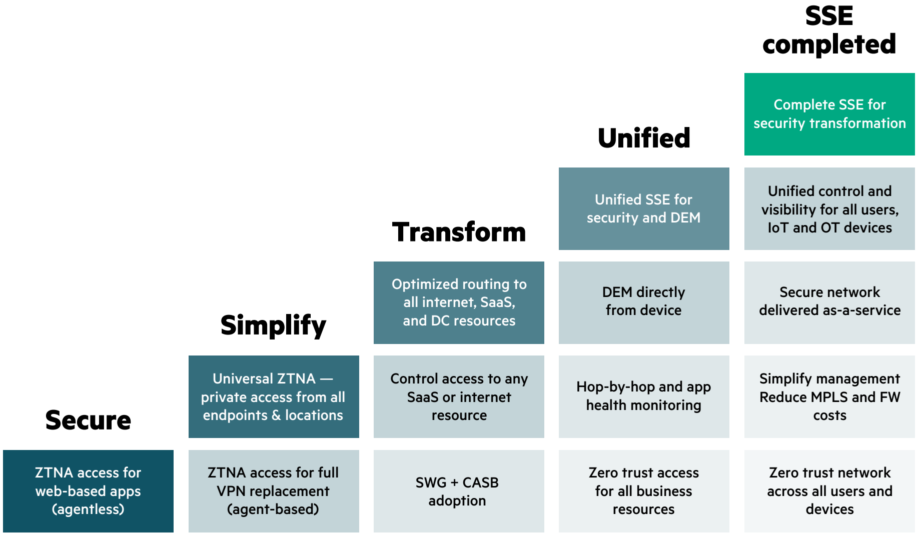
- User training
- Testing and optimization
- Review and feedback processes

Lastly, after reviews and updates to the initial SSE deployment are completed, organizations should start the process again by planning for the next SSE component deployment steps. An excellent place to begin considering SSE phase

69%

of teams plan to adopt SSE in the next 2 years[1]

two objectives is by identifying other SSE technologies and use cases that can be added, focusing on additional scalability for the initial deployment, or identifying ways to broaden the initial deployment. Here is an example of a common SSE journey.



Secure	Simplify	Transform	Unified	SSE completed
				Complete SSE for security transformation
			Unified SSE for security and DEM	Unified control and visibility for all users, IoT and OT devices
		Optimized routing to all internet, SaaS, and DC resources	DEM directly from device	Secure network delivered as-a-service
	Universal ZTNA — private access from all endpoints & locations	Control access to any SaaS or internet resource	Hop-by-hop and app health monitoring	Simplify management Reduce MPLS and FW costs
ZTNA access for web-based apps (agentless)	ZTNA access for full VPN replacement (agent-based)	SWG + CASB adoption	Zero trust access for all business resources	Zero trust network across all users and devices

Figure 1. Phased approach to SSE adoption

Building on SSE success

With SSE, CISOs and security teams no longer have to worry about the words “anywhere” and “everywhere”. SSE services like ZTNA, SWG, and CASB, allow organizations to gradually substitute outdated security technologies and processes with more efficient, contemporary ones. These modern methods not only promptly tackle urgent security and user requirements, but also offer a flexible platform to cater to future needs.

While most organizations will choose a step-by-step approach to SSE, building on deployment success as they go, the long-term successful implementation of SSE requires an ongoing combination of strategic decisions, technical solutions, user involvement and education, and continuing management and refinement.

In other words, SSE success is a process. One that can quickly start and finish depending on which SSE provider you choose to partner with. Consider HPE Aruba Networking SSE for your SSE project and we’ll walk with you every step of your deployment.

Learn more at

HPE Aruba Networking SSE

Take SSE for a free 24-hour test drive

Visit **ArubaNetworks.com**

[1] 2024 SSE Adoption Report, Cybersecurity Insiders

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Hewlett Packard
Enterprise