VERSA

Choose Your Own SSE Adoption Pathway

Table of Contents

There's a common misconception that Security Service Edge (SSE) solutions must be adopted all at once, but that's most certainly not the case. While some organizations may choose to implement SSE comprehensively from the start, it can also be adopted gradually to better align with specific needs and resources. By evaluating your unique security requirements, risk profiles, and existing contracts with point security product providers, you can prioritize which SSE components to implement first, and then complete the implementation of the remaining capabilities in your preferred sequence.

Such a phased approach allows your organization to address the most pressing security gaps immediately, plan the integration of SSE solutions to minimize disrupting existing workflows or incurring unnecessary costs, and ensure that each step is aligned with the organization's overall security strategy and operational goals.

Core SSE capabilities

SSE is a transformative approach that seamlessly integrates security with networking. It provides organizations with a unified framework to protect data and users across various environments, enhancing both security and performance. A comprehensive SSE offering is generally understood by the market to include the following components:

1. Secure Web Gateway (SWG)

Description

- SWG acts as a barrier between users and the internet, providing advanced web filtering and protection against malware. It inspects web traffic to ensure safe browsing and prevents access to malicious sites.

Key Features

- URL filtering
- Malware detection and prevention
- SSL inspection

2. Cloud Access Security Broker (CASB)

Description

- CASB provides visibility and control over data and users in cloud applications. It acts as a gatekeeper, ensuring that cloud usage complies with security policies.

Key Features

- Data encryption
- Access control
- Threat protection

3. Zero Trust Network Access (ZTNA)

Description

- ZTNA is a security framework that grants access based on identity and context, rather than location. It enforces strict identity verification and limits access to applications and data.

Key Features

- Identity-based access
- Contextual access control
- Micro-segmentation

4. Firewall as a Service (FWaaS)

Description

- FWaaS delivers firewall capabilities through the cloud, providing scalable and centralized security for networks. It eliminates the need for physical firewall appliances.

Key Features

- Centralized policy management
- Intrusion prevention
- Traffic monitoring

5. Data Loss Prevention (DLP)

Description

- DLP technologies identify, monitor, and protect sensitive data across networks and endpoints. They prevent unauthorized access and data leaks.

Key Features

- Data classification
- Policy enforcement
- Incident response

Choosing your pathway

Selecting the right implementation sequence for SSE capabilities in a phased approach requires a thoughtful evaluation of several critical factors to ensure alignment with your organization's unique needs and objectives.

First, consider your business priorities. Determine how each SSE approach can support your strategic goals, whether that's enhancing security, improving scalability, or optimizing operational efficiency. Understanding these priorities will lead you to a path that delivers the most value.

Next, assess your regulatory environment. Compliance requirements often dictate specific security measures that must be implemented. Choosing a path that aligns with these regulations ensures that your organization remains compliant while protecting sensitive data.

Workforce distribution is another crucial factor. Whether your teams are remote, hybrid, or primarily on-site will influence the technologies you need to secure access and communication. Ensuring seamless and secure connectivity for all employees is vital.

Additionally, consider timing your SSE adoption with your renewal cycles for existing contracts. This alignment can facilitate smoother transitions and potentially reduce costs.

Evaluate your cybersecurity and risk priorities, along with your organization's tolerance for risk. Consider the specific threats you face and how each path addresses these risks. Understanding your risk tolerance will help in choosing an approach that provides adequate protection without compromising agility or innovation.

Finally, you could consider the maturation level of the different technologies. Over time, technologies like SWG and DLP have achieved high maturity and significant adoption, reflecting their established roles in security strategies. In contrast, emerging technologies such as Zero Trust Network Access (ZTNA) and Remote Browser Isolation (RBI) are gaining traction as organizations adapt to modern challenges. High-maturity technologies offer proven effectiveness with ample resources for implementation, while emerging ones provide opportunities for first-time integration without system replacement. This makes them attractive for organizations looking to modernize their security posture. Ultimately, understanding these maturity differences helps prioritize investments, balancing stability with the agility needed to address evolving threats effectively.

Adoption Rate %	Maturity Level	Age (Years)
SWG (Secure Web Gateway)	High	15
CASB (Cloud Access Security Broker)	Moderate	10
ZTNA (Zero Trust Network Access)	Emerging	05
FWaaS (Firewall as a Service)	Moderate	10
DLP (Data Loss Prevention)	High	15

By carefully considering the above factors, you can select an SSE adoption path that not only addresses immediate security challenges, but also positions your organization for future growth and resilience.

Six pathways to SSE adoption

With multiple routes available, each offering distinct advantages and considerations, businesses can start their journey with what's most important to them—comprehensive security, scalability, compliance, or remote access. This section explores these diverse pathways, enabling you to choose the strategy that aligns with your organizational priorities for a successful and, eventually, full SSE deployment. The goal is to provide a tailored approach, ensuring that each organization can effectively integrate SSE technologies in a way that meets its unique needs and resources, ultimately achieving a robust security framework.

Pathway options to full SSE adoption

- **Comprehensive Pathway:** Focuses on comprehensive adoption covering all technologies.
- **Scalability Pathway:** Prioritizes ZTNA and FWaaS for scalable and flexible security.
- **Compliance Pathway:** Starts with CASB and DLP to meet compliance requirements.
- **Web and SaaS Pathway:** Emphasizes SWG and CASB for securing web and SaaS applications.
- **Remote & Hybrid Workers Pathway:** Begins with ZTNA and FWaaS for remote access.
- **Data Protection Pathway:** Centers on DLP and CASB for data protection.

Comprehensive Pathway

The Traditional Pathway to SSE adoption is ideal for organizations seeking comprehensive coverage from the outset. It is well-suited for large enterprises due to its established processes and ability to deliver extensive security coverage. However, this path presents challenges, including high complexity, lengthy implementation times, and the need for significant resources. Focusing on full integration from the start ensures a robust security framework. Organizations choosing this path are typically organizations with the capacity to manage intricate deployments and a clear vision for comprehensive security integration.

Pros:

- **Comprehensive coverage:** Provides extensive security across all areas from the start.
- **Established processes:** Utilizes proven frameworks and methodologies.
- **Suitable for large enterprises:** Designed to meet the needs of complex, large-scale organizations.

Cons:

- **High complexity:** Involves intricate setups and configurations.
- **Lengthy implementation:** Requires a significant amount of time to fully deploy.
- **Requires significant resources:** Demands substantial investment in terms of time, money, and personnel.

Why: Focuses on broader full integration from the start.

- **Order**: SWG → CASB → ZTNA → FWaaS → DLP

Scalability Pathway

This pathway prioritizes implementing agile and adaptable security first. It offers scalable solutions that support dynamic environments, providing quick wins, especially with ZTNA. However, this path may initially present security gaps, such as unaddressed vulnerabilities or incomplete protection in certain areas, requiring ongoing adjustments and potential integration efforts to ensure comprehensive coverage. By emphasizing scalability, organizations can adapt swiftly to changing needs. Organizations choosing this path are those seeking agile security solutions that can evolve with their business demands.

Pros:

- **Scalable solutions:** Easily adapts to changing business needs.
- **Supports dynamic environments:** Offers flexibility for evolving operational landscapes.
- **Quick wins with ZTNA:** Provides immediate security improvements with Zero Trust Network Access.

Cons:

- **Initial security gaps:** May leave some vulnerabilities early on.
- **Requires ongoing adjustments:** Needs continuous updates and modifications.
- **Potential integration issues:** Can face challenges in combining with existing systems.

Why: Prioritizes agile and scalable security.

- **Order**: ZTNA → FWaaS → CASB → SWG → DLP

Compliance Pathway

The compliance-driven approach is tailored to organizations prioritizing regulatory requirements and data protection. This path starts with CASB and DLP, followed by SWG, ZTNA, and FWaaS. It focuses on meeting compliance standards such as GDPR, HIPAA, and PCI-DSS, and safeguarding sensitive information. While this approach ensures strong compliance from the outset, it may overlook broader security needs and involve high initial costs. Additionally, it can be slower to adapt to new threats. Organizations choosing this path are those driven by the need to align with strict regulatory environments and protect critical data assets.

Pros:

- **Meets regulatory requirements:** Ensures alignment with legal and industry standards.
- **Protects sensitive data:** Focuses on safeguarding critical information.
- **Strong compliance focus:** Prioritizes adherence to compliance from the outset.

Cons:

- **May overlook broader security needs:** Can miss other important security areas.
- **High initial costs:** Involves significant upfront investment.
- **Slower to adapt to new threats:** Might lag in responding to emerging vulnerabilities.

Why: Ensures compliance from the outset.

- **Order**: CASB → DLP → SWG → ZTNA → FWaaS

Web and SaaS Pathway

The secure web and SaaS usage pathway focuses on enhancing security for web applications and SaaS environments. It begins with SWG and CASB, followed by DLP, ZTNA, and FWaaS. This approach quickly addresses web and SaaS-related risks, offering rapid implementation. However, it may have a limited initial scope and could require further integration to avoid siloed solutions. Organizations choosing this path are those aiming to swiftly secure web applications and SaaS, ensuring immediate protection while planning for future integration needs.

Pros:

- **Enhances web app security:** Strengthens protection for web-based applications.
- **Reduces SaaS-related risks:** Minimizes vulnerabilities in Software as a Service environments.
- **Quick implementation:** Allows for rapid deployment of security measures.

Cons:

- **Limited initial scope:** May not cover all security needs initially.
- **May need further integration:** Requires additional efforts to unify solutions.
- **Potential for siloed solutions:** Risks creating isolated security systems.

Why: Focuses on immediate web and SaaS security.

- **Order**: SWG → CASB → DLP → ZTNA → FWaaS

Remote Workers Pathway

The Connect and Secure Remote Workers path is designed to enhance security for remote access. It begins with ZTNA and FWaaS, followed by SWG, CASB, and DLP. This approach supports remote work by providing secure and reliable access, ensuring quick deployment for remote teams. While it effectively enhances access security, the initial focus might overlook broader threats and require a robust infrastructure. Organizations choosing this path are organizations prioritizing remote workforce security and seeking efficient solutions for connecting distributed teams.

Pros:

- **Scalable solutions:** Easily adapts to changing business needs.
- **Supports dynamic environments:** Offers flexibility for evolving operational landscapes.
- **Quick wins with ZTNA:** Provides immediate security improvements with Zero Trust Network Access.

Cons:

- **Initial security gaps:** May leave some vulnerabilities early on.
- **Requires ongoing adjustments:** Needs continuous updates and modifications.
- **Potential integration issues:** Can face challenges in combining with existing systems.

Why: Prioritizes agile and scalable security.

- **Order**: ZTNA → FWaaS → SWG → CASB → DLP

Data Protection Pathway

This pathway is centered on beginning the SSE journey by safeguarding sensitive information from the outset, emphasizing strong data protection and compliance. It differs from the compliance-driven pathway discussed above only in that it starts with DLP and then moves to CASB, followed by SWG, FWaaS, and ZTNA. While it offers robust data security, it initially provides limited network security and requires extensive policy setup.

Pros:

- **Strong data protection:** Offers robust measures to secure sensitive information.
- **Focused on sensitive information:** Prioritizes the safeguarding of critical data.
- **Supports compliance:** Aligns with regulatory standards for data protection.

Cons:

- **Limited initial network security:** May not fully secure network environments at first.
- **May require extensive policy setup:** Involves detailed configuration of security policies.
- **Can be resource-intensive:** Demands significant resources for implementation and maintenance.

Why: Centers on safeguarding data from the start.

- **Order**: DLP → CASB → SWG → FWaaS → ZTNA

Within each pathway it's important to recognize that, in addition to the prioritizing of the deployment of the various capabilities, within a given capability there will likely be opportunities for staged deployment following a Crawl-Walk-Run model along the lines suggested in the table immediately below. For example, secure web gateway deployment can be done by first turning on basic web filtering and protection (crawl), followed by activation of advanced threat protection and SSL inspection (walk), then finally implementing comprehensive DLP and user behavior analytics.

Crawl-Walk-Run capabilities deployment

Technology	Crawl	Walk	Run
SWG	Basic web filtering and protection	Advanced threat protection and SSL inspection	Comprehensive DLP and user behaviour analytics
CASB	Visibility in to cloud app usgae	Enforce data protection and compliance policies	Advanced threat protection and real-time access control
ZTNA	Replace/supplement VPNs for specific apps	Expand to more apps/users with contextual access	Full Zero-trust architecture across the network
FWaaS	Basic firewall capabilities in the cloud	Integrate with network security policies	Advanced threat detection and unified policy management
DLP	Monitoring and reporting	Enforce policies to prevent data exfiltration	Integrate with other security solutions for comprehensive coverage

Conclusion: Your journey awaits

Choosing the right path for SSE adoption depends on your organization's specific needs and priorities. Whether you aim for comprehensive integration, prioritize flexibility and scalability, focus on compliance, enhance web and SaaS security, secure remote workers, or protect data, each approach offers distinct advantages and challenges. By considering factors such as business objectives, regulatory requirements, and security priorities, you can tailor your SSE strategy effectively.

Many possible paths to one outcome - Full SSE adoption

Path	SWG	CASB	ZTNA	FWaaS	DLP
Traditional Path	1	2	3	4	5
Flexibility and Scalability	4	3	1	2	5
Compliance-Driven Approach	3	1	4	5	2
Secure Web and SaaS Usage	1	2	4	5	3
Connect and Secure Remote Workers	3	4	1	2	5
Protect Data	3	2	5	4	1

Looking for more?

Check out Versa Network's SSE Buyer's Guide

SSE BUYER'S GUIDE ↗

As organizations navigate today's evolving digital landscape, securing their networks and data has become an increasingly complex undertaking. Traditional security approaches are proving themselves outdated in a new era of expanding cloud services, IoT devices, flexible work, and sophisticated threats.

About Versa Networks

Versa Networks, the leader in single-vendor Unified SASE platforms, delivers AI/ML-powered SASE, SSE, and SD-WAN solutions. The platform provides networking and security with true multitenancy and sophisticated analytics via the cloud, on-premises, or as a blended combination of both to meet SASE requirements for small to extremely large enterprises and service providers.

For more information, visit www.versa-networks.com