netskope

White Paper

Security Service Edge (SSE) Guide for Networking, Infrastructure & Operations:

The Six Essentials

TABLE OF CONTENTS

INTRODUCTION: THE CRITICAL ROLE OF SSE TO ADDRESS MODERN NETWORKING AND I&O CHALLENGES

Networking and Infrastructure & Operations (I&O) teams are vital in maintaining essential IT services as organizations increasingly adopt cloud services and support mobile workforces, facing complex environments that require agility and security.

In today's fast-paced digital landscape, organizations are constantly seeking ways to enhance their network infrastructure and improve operational efficiency. The integration of Secure Service Edge (SSE) has become essential in modern cybersecurity, replacing traditional perimeter-based approaches with a centralized, cloud-based integrated framework that combines multiple security functions at the network edge.

Why Does SSE Matter? - SSE is a crucial component of the broader Secure Access Service Edge (SASE) framework. It combines critical security capabilities such as secure web gateways (SWG), cloud access security brokers (CASB), and Zero Trust Network Access (ZTNA) into a unified cloud-delivered service. While it may appear to be a nominally "security stack" transformation, its implications extend far beyond traditional security boundaries, directly impacting and enhancing network performance and management.

The integration of security and networking through SSE is not just a transformation of the security stack; it is a strategic move that underpins the entire network infrastructure. By adopting SSE, organizations can address modern networking and I&O challenges more effectively, achieving a secure, agile, and high-performance network environment. This convergence is essential for meeting the demands of today's digital business landscape and positioning organizations for future success.

.

Essential #1

SSE DEMYSTIFIED - UNDERSTANDING THE COMPONENTS

Secure Service Edge (SSE) is a comprehensive approach to security that merges various protective services at the network edge, tailored to support the evolving needs of Infrastructure & Operations (I&O) teams.

SSE encompasses several key services that together form a robust defense mechanism for enterprise networks. It harmonizes policy administration and enforcement, simplifies administration and provides visibility across all traffic.

- **Secure Web Gateway (SWG):** Provides fine-grained control and security for internet access, and addresses cloud-enabled threats and data risks for personal instances of managed applications, thousands of shadow IT applications, and cloud services.
- **Cloud Access Security Broker (CASB):** Provides visibility and control over SaaS applications, enabling organizations to enforce security policies, recognize unauthorized access, and prevent cloud-based threats. It can also assess the security configurations of SaaS apps to ensure compliance with corporate policies.
- **Zero Trust Network Access (ZTNA):** Enforces the premise that no one is blindly trusted and implementation of least-privilege access, which selectively grants access only to resources that people or groups of people require, nothing more.
- **Remote browser isolation (RBI):** Separates worker devices from the act of web browsing by hosting and running all browsing activity in a remote, cloud-based container. Such isolation protects data, devices, and networks from all kinds of threats originating from malicious websites.
- **Firewall as a Service (FWaaS):** Provides consistent network security for all outbound ports and protocols for safe, direct-to-internet access via an agent on managed devices or via Generic Routing Encapsulation (GRE) and Internet Protocol Security (IPsec) for offices. Often integrated components include DNS Security and Intrusion Prevention Systems (IPS) to detect and prevent DNS initiated attacks, and identify threats in real time respectively.
- **Advanced Threat Protection (ATP):** Includes comprehensive security measures designed to protect enterprises from sophisticated cyber threats across cloud applications, web traffic, and private apps (e.g., multi-layered defense, real-time threat intelligence, cloud/web traffic analysis, and more).
- **Data Loss Prevention (DLP):** Ensures sensitive data is identified and protected in real-time, analyzes data movement within the network and blocks the transmission of sensitive information to unauthorized recipients, whether the data is at rest, in use, or in motion.
- **SaaS Security Posture Management (SSPM):** Automatically identifies and remediates misconfigurations in SaaS applications, reducing the risk of security breaches caused by configuration errors.

Essential #2

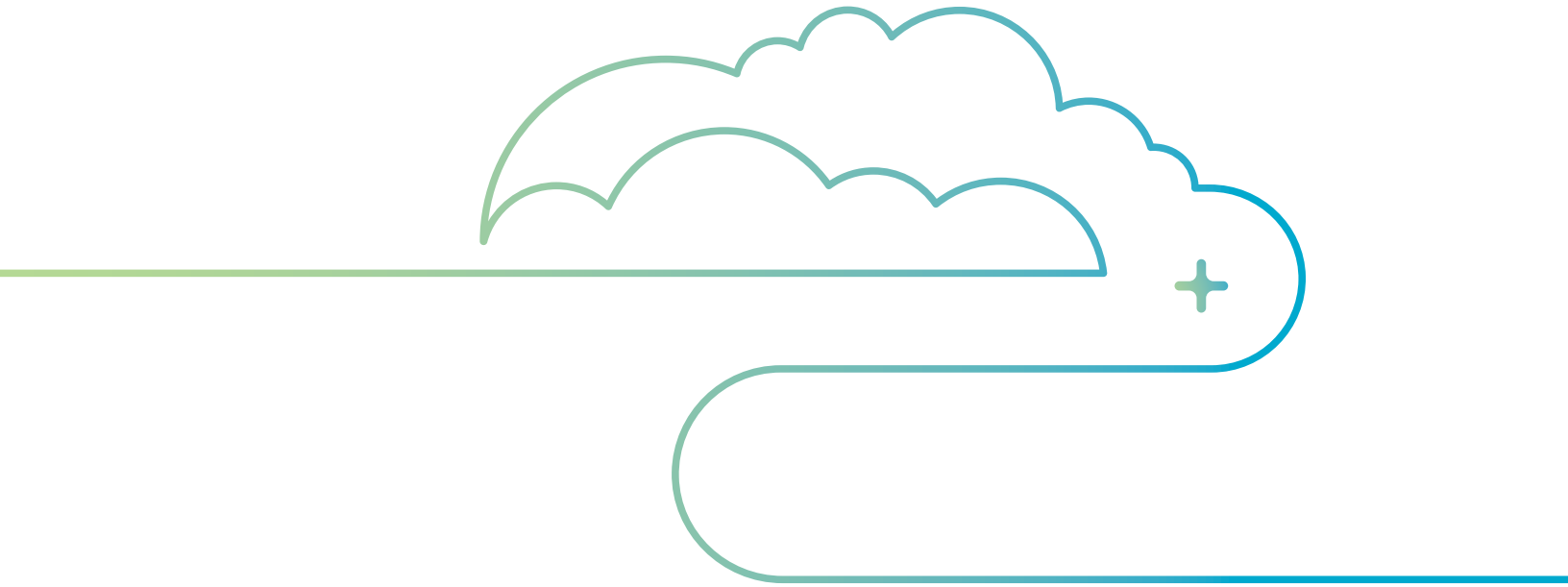
MAIN USE CASES: SSE IN ACTION

SSE provides robust, flexible security solutions tailored to the needs of modern enterprises. Here are some key use cases for SSE that illustrate its effectiveness in various operational scenarios:

USE CASE	SCENARIO	SSE SOLUTION
Vendor Consolidation	Organizations seek to streamline their security architectures, reduce complexity to enhance their overall security effectiveness, streamline operations, and potentially reduce costs, all while maintaining a flexible posture that adapts to evolving threats and business needs.	SSE enables organizations to migrate from disparate remote access, CASB, SWG, and RBI products to a single offering from a single vendor.
Connect and Secure Remote Workers	With the rise of remote work, organizations need to ensure that employees can access internal resources securely from any location (branch, HQ, home, coffee shop, etc.).	SSE employs Zero Trust Network Access (ZTNA) to verify and authenticate user identities and device security statuses before granting access to specific applications or data, without exposing the entire network.
Secure Access to Web and SaaS	Organizations need to ensure safe and efficient access to web resources and Software-as-a-Service (SaaS) applications that are critical for daily business operations. Essential for protecting organizational assets, ensuring compliance with legal and regulatory standards, and maintaining high productivity and performance in a secure and controlled IT environment.	SSE employs SWG to filter unwanted software/ malware from user-initiated web traffic and enforce company policies on the web, and CASB to monitor and secure access to cloud and SaaS applications.
Data Protection	A critical use case within the Security Service Edge (SSE) framework, focusing on securing sensitive information across an organization's networks and cloud environments and preventing sensitive information from leaking outside the company's digital walls to maintain privacy and compliance.	SSE strategies include: -Granular Zero Trust access through ZTNA to ensure that only authenticated and authorized users can access sensitive data. -DLP to ensure sensitive data is identified and protected in real time. -Encryption and tokenization capabilities to secure data at rest, in use, and in transit. -SWGs to prevent access to malicious websites and to detect attempts to exfiltrate data through web channels.
Threat Protection and Management	Organizations face a multitude of evolving threats that target users, access, and resources vulnerabilities.	SSE integrates advanced threat detection tools like sandboxes, antivirus, and intrusion prevention systems to identify and neutralize threats in real time. This includes analyzing patterns and behaviors to block advanced persistent threats (APTs) and zero-day attacks.

USE CASE	SCENARIO	SSE SOLUTION
Traffic Visibility and Control	IT departments need to oversee and manage the use of applications along traffic patterns within their networks to optimize performance and security.	SSE offers granular visibility and control over application usage through a single console, allowing IT to not only view but also control how applications are accessed and used. A Digital Experience Manager (DEM) provides detailed visibility into the network traffic, allowing IT teams to monitor, analyze, and manage access and activities at the edge of their network.
Enhanced Performance and Network Efficiency	Optimizing the performance of security measures without impacting user experience is essential.	SSE optimizes the delivery of security services by leveraging globally distributed points of presence (POPs), which minimizes latency and ensures that security processes do not hinder application performance.

Tip By deploying SSE, organizations can ensure secure, compliant, and efficient operations across increasingly complex IT environments.



Essential #3

PIVOTAL VALUE OF SSE FOR I&O TEAMS

In the rapidly evolving digital landscape, the integration of Security Service Edge (SSE) is a game-changer for modern enterprises. While the primary goal of SSE is to strengthen security, it simultaneously enhances overall infrastructure performance, leading to a more efficient, resilient, and agile network environment. This synergy between security and performance is crucial for businesses aiming to stay competitive and secure. By adopting SSE, organizations achieve robust security and superior network performance, positioning themselves for success in the digital age.

The Dual Benefits of a Better Security Posture:

Benefits	Impact
Operational Simplification with Centralized Security Management SSE consolidates multiple security functions into a single, cloud-delivered platform, which simplifies the management of security policies and procedures.	» Enhanced ease of management and reduced administrative overhead, allowing I&O teams to focus on strategic initiatives rather than routine security maintenance.
Consolidation for Enhanced Security Posture By integrating functionalities such as CASB, SWG, ZTNA, and DLP, within a Zero Trust framework, SSE provides comprehensive security measures that are inherently more cohesive and effective than piecemeal solutions.	» Stronger defense against a wide range of cyber threats, reduced risk of data breaches, and improved compliance with regulatory requirements.
Scalability and Flexibility for Business Agility SSE solutions are cloud-native, allowing them to scale seamlessly with the organization's needs without requiring significant hardware investments or manual reconfiguration.	» I&O teams can swiftly adapt to changes in the business environment, ensuring that security measures do not hinder growth or operational agility.

Benefits	Impact
Improved Network Performance and Efficiency By filtering out malicious activities and unauthorized access attempts, SSE keeps the network clean and efficient.	» A robust security posture ensures that only legitimate traffic flows through the network, reducing congestion and improving overall performance
Enhanced User Experience With SSE, users experience faster and more reliable access to applications and data. Direct-to-cloud access, handling security processing at global points of presence close to the user, minimizes latency and maximizes throughput, ensuring that users can work efficiently from any location.	» Better user experience with minimal performance trade-offs, supporting productivity across all levels of the organization.
Reduced Downtime and Disruptions Strong security measures protect the network from cyber threats that can cause significant downtime and operational disruptions.	» By preventing attacks and swiftly mitigating any incidents, SSE helps maintain business continuity and reduces the risk of costly interruptions.
Optimized Resource Utilization By leveraging cloud-native architecture, SSE optimizes resource allocation and utilization. It dynamically scales resources based on demand, ensuring that the network performs optimally even during peak usage times without compromising security.	» Reduced capital expenditures (CAPEX) and more efficient use of security budgets, enabling I&O departments to allocate resources more strategically.

Tip Integrating SSE into your network infrastructure is not just about enhancing security; it's about transforming the entire network for better performance and resilience.

Essential #4

DEPLOYING AND MANAGING YOUR SSE

Deploying and managing an SSE solution requires careful planning, execution, and ongoing management to ensure it effectively secures your organization's resources while aligning with operational goals and broader business objectives.

Key Steps	Best Practice
Initial Assessment and Planning Begin by assessing your current security posture and identifying gaps that SSE can address. Evaluate your network architecture, existing security solutions, and specific business needs to understand where SSE can be most beneficial.	» Develop a clear strategy for SSE deployment that includes defining objectives, expected outcomes, and key performance indicators (KPIs).
Choosing the Right SSE Provider Evaluate potential SSE vendors based on their ability to meet your specific requirements. Consider factors such as the comprehensiveness of their security services, ease of integration with existing systems, customer support, and cost-effectiveness.	» Conduct a pilot test with shortlisted vendors in your environment to see how the SSE solution can handle your specific security needs and network traffic patterns.
Deployment Work with your chosen vendor to configure the SSE solution to meet your specific security policies and compliance requirements. Customization may involve setting up security rules, configuring DLP settings, and defining access controls.	» Integrate the SSE solution with existing IT infrastructure, such as identity management systems, network infrastructure, and other security tools. Proper integration is vital for seamless operation and maximizing the value of your SSE solution.

Tip

Evaluating Success: Periodically review the performance of the SSE solution against the initial KPIs set during the planning phase. Adjust your strategy and the SSE configuration to meet your evolving security needs.

Key Steps

Training and Change Management

Ensure that your I&O team and end-users are adequately trained on how to use and manage the SSE solution. Training should cover operational procedures, best practices, and how to respond to security incidents.

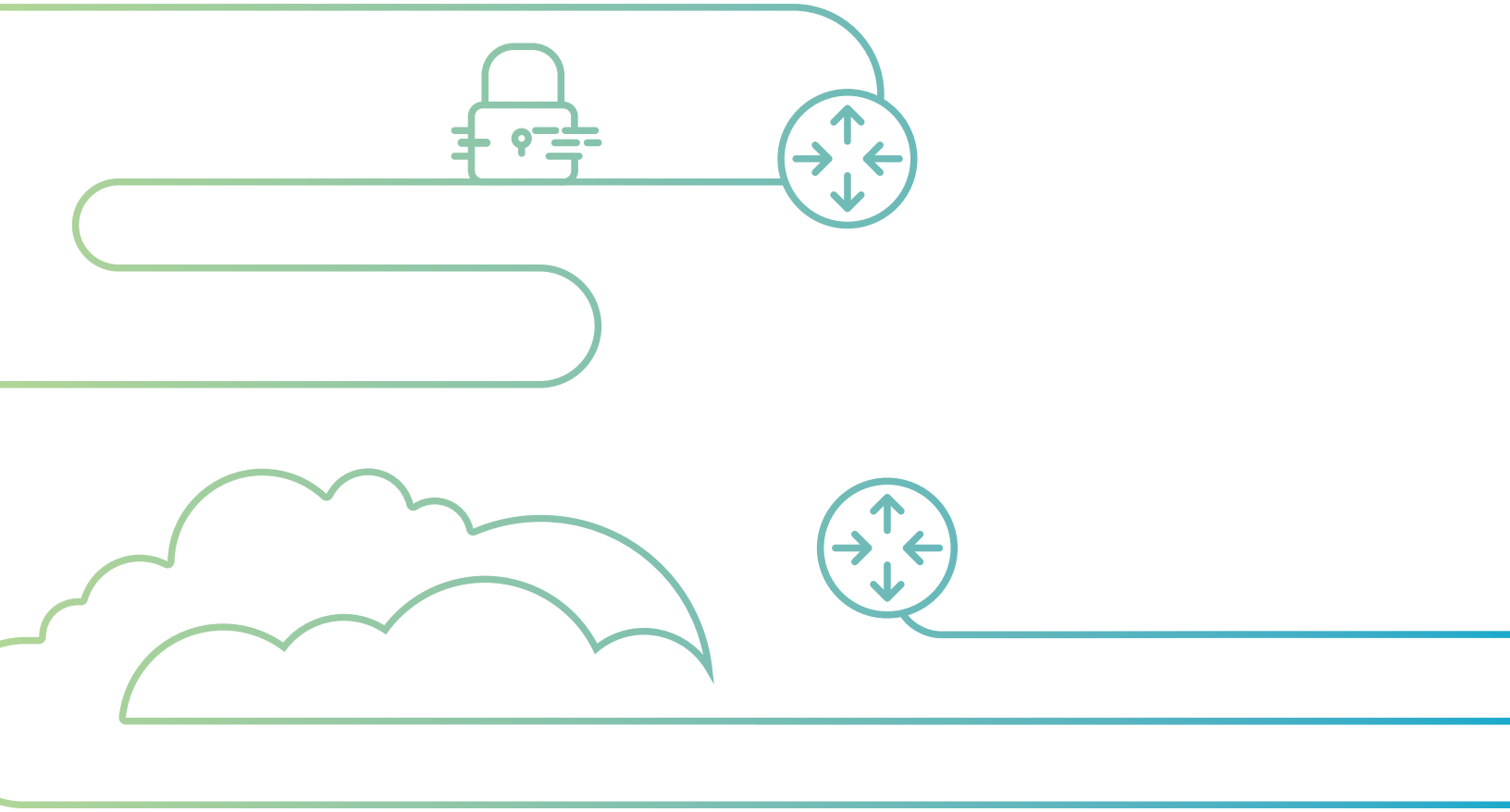
Ongoing Management and Optimization

Regularly monitor the performance and effectiveness of the SSE solution using the analytics and reporting tools provided. This will help identify any issues or areas for improvement.

Best Practice

» Implement a change management strategy to help staff adjust to the new system. This includes communicating the benefits of SSE, addressing any concerns, and providing ongoing support during the transition phase.

» Keep the SSE solution up to date with regular updates from the vendor and schedule regular maintenance checks to ensure the system continues to operate effectively and securely.



Essential #5

THE FUTURE LANDSCAPE OF SSE

As we look toward the future of Secure Service Edge (SSE), it's clear that the landscape is rapidly evolving, driven by advancements in AI, the expansion of Zero Trust architectures, and the growing importance of edge security.

Key Trends	Impact
Increased Integration with AI and Machine Learning SSE solutions will increasingly incorporate AI and ML technologies to automate threat detection, response processes, and network management tasks. This integration will enhance the intelligence of SSE platforms, enabling them to predict threats and automate responses more effectively.	» The use of AI and ML will streamline operations, reduce the burden on I&O teams, and improve the overall effectiveness of security measures.
Expansion of Zero Trust Architectures The Zero Trust model will continue to expand within SSE frameworks, becoming more deeply integrated into network architectures. This approach will extend beyond access controls to include more comprehensive security checks at every network interaction point.	» Significantly enhancing security across increasingly distributed environments, particularly important as remote work and cloud applications expand.
Greater Emphasis on Edge Security As the data generation points continue to move toward the edge with the proliferation of IoT devices and edge computing, SSE will need to adapt by providing more focused security measures at the edge for all devices.	» Crucial for protecting data in transit and at rest at the edge with no performance trade-offs, ensuring security measures are as close as possible to where data is generated and processed.
More Robust Multi-Cloud Support Organizations are increasingly relying on multi-cloud environments, prompting SSE solutions to offer more comprehensive multi-cloud support. This includes improved visibility and control over data and resources across different cloud platforms.	» Critical for organizations to navigate the regulatory landscape, avoid penalties, and protect customer data without impeding business expansion.

Key Trends	Impact
Interoperability, Standardization, and Less Complexity As the SSE market matures, there will be a greater push toward standardization and interoperability among security products and services.	» Facilitate more seamless integration of diverse security tools, along simplified user interfaces and management tools.
Adoption of SASE (Secure Access Service Edge) SSE will increasingly be discussed in conjunction with SASE, blending network and security functions into a unified, cloud-delivered service model.	» The convergence of SSE with SASE will provide streamlined, scalable, and flexible security solutions that support dynamic access control, improved network efficiency, and enhanced security.

Essential #6

SELECTING A SUPERIOR SSE SOLUTION

Selecting an SSE solution is a critical decision that requires careful consideration of your organization's unique needs. Consider not only your current security requirements but also your future growth and changes in the cybersecurity landscape.

Selection Guide

Assess Your Security Needs

Start by identifying the specific security challenges and requirements of your organization. Consider vendors with the ability to meet your security requirements, factoring the types of data to protect, the level of remote access required, and compliance obligations.

Key Questions

- Can you offer a complete SSE solution, including SWG, CASB, ZTNA, and FWaaS in one platform, policy engine, and client?
- Can your solution support real-time security and access policies that can block, alert, bypass, quarantine, and coach? Can they work with web and managed and unmanaged SaaS and IaaS services?
- Does your solution inspect traffic inline across web, SaaS applications, and cloud services,? Specifically, can it decode SaaS to differentiate instances (company vs. personal), assess activity, app risk, user risk, and data sensitivity?

Review Integration Capabilities

Evaluate how well potential SSE solutions can integrate with your existing infrastructure and support necessary APIs for further integration and seamless operations.

- Can I leverage my existing investments in next-gen firewalls, routers, or SD-WAN devices to efficiently and securely steer traffic to the cloud?
- Can I leverage APIs or ready-to-use plugins to facilitate deep integration with other security and network management tools including sharing IOCs, exporting logs, exchanging risk scores, or automating workflows and orchestration?

Selection Guide

Assess the Underlying SSE Architecture

Check if the solution is using the public cloud or a private cloud. Simple differences in approach, such as a vendor owning its own delivery network, rather than outsourcing—say via a public cloud service provider—(CSP) can have a huge impact on the quality of the SASE delivery, from basic performance to downtime issues and the inability to proactively manage that SASE network.

Key Questions

- Is the SASE solution private (owned and operated by the vendor) or operated by a public cloud? If operated by a public cloud, in how many regions are the services configured and are allowed to use the global network for ingress/egress?
- Where are their servers/service delivery points located and what do they actually consist of? How many regions are available to you? Are the POPs real or virtual?

Evaluate Scalability and Flexibility

Check if the solution can handle your data traffic and scale with your organization's growth and evolving IT strategies. Evaluate whether all SSE services are available at each SSE POP to truly embody a distributed service edge.

- Do I have access to all the advertised data centers? Or are some off-limits and designated only for select partners or customers, requiring additional fees or surcharges?
- How does the solution scale to handle increased volumes of traffic and threat data?

Tip

Choose an SSE solution that enhances your security posture, integrates well with your existing systems, and offers good value for your investment. According to 2024 Forrester Wave Zero Trust Edge: “Some SSE solution providers build and maintain their own network and have full control over the network roadmap. <...> In general, if you have significant requirements around performance or need these advanced features, you will find that vendors that run their own networks are a better fit.”

Selection Guide

Evaluate Performance and Reliability

Assess the performance impact of each SSE solution. High-performance solutions ensure that security measures do not impact user experience or business operations. It's important to understand SASE vendors' failover, redundancy, and recovery strategies.

Key Questions

- Do all POPs have compute resources for service delivery (and, for example, processing traffic to protect data, stop threats, inspect encrypted flows, etc.) or is there a need for service chaining traffic to another location? What happens when something breaks?
- If third parties are involved in the delivery network, what is the accountability of each provider in the event of a problem arising?

Consider User Experience and Management

Opt for a solution that balances robust security with best user experience and offers intuitive management tools.

- Do you have a single point for policy management across all components?
- Do you have an integrated digital experience management (DEM) with your solution to provide visibility across the entire traffic path with both synthetic probes and real user monitoring (RUM) including between data centers to SaaS and web destinations?
- Do you offer a single endpoint agent to unify remote user access to web, cloud, and private apps, alongside data protection and voice and video optimization at the endpoint by converging SWG, CASB, ZTNA, FWaaS, DLP, and SD-WAN?

Selection Guide	Key Questions
Analyze Threat Intelligence and Protection Features Look for vendors providing comprehensive, real-time zero-day protection, global threat intelligence and protection against various types of cyber threats, plus continuous and committed efforts to improve and maintain healthy threat efficacy scores.	» What types of threats can the solution detect (e.g., malware, phishing, zero-day attacks, advanced persistent threats)? Does the solution provide real-time threat analysis and automated response capabilities? What are the SSE threat efficacy scores for T+0 (real-time) and T+1-hour from a test lab like AV-TEST? » How does the solution handle encrypted traffic inspection without impacting performance, including the entire threat stack for threat protection, CFW, IPS, DNS security, RBI, and URL filtering? » Does it offer machine learning and artificial intelligence to enhance threat detection and response, including inline real-time protection from unknown zero-day executable files and phishing attacks?
Regulatory Compliance and Data Privacy Ensure the solution complies with relevant regulations and handles data privacy effectively.	» Can you list the certifications? Do I have control over where my traffic gets steered (e.g., keep all data in U.S. or EU region) to address data sovereignty or compliance requirements? » Does the SSE solution comply with relevant industry standards such as GDPR, HIPAA, CCPA, PCI DSS, and ISO/IEC 27001? Or other government regulations such as U.S. FedRAMP High certified and Canadian PBMM?
Support and Service Level Agreements (SLAs) Evaluate the quality of customer support and the specifics of SLAs to ensure they meet your operational needs.	» What are your published SLAs for the processing for both “encrypted” and “decrypted” cloud security traffic (full round-trip time)?

Selection Guide	Key Questions
Cost-Effectiveness Analyze total costs, including setup, licensing, and maintenance, against the benefits provided by the solution.	» How does the solution support future growth and technological advancements, potentially reducing future costs? Where is the SSE solution in Gartner's SSE Magic Quadrant and how does it rank for SSE critical capabilities? » How does the SSE solution improve network performance and operational efficiency? Can these improvements lead to cost savings in terms of reduced downtime, fewer security breaches, and more efficient use of IT resources?
Trial and Testing Conduct a trial or pilot to test the solution's compatibility and effectiveness within your infrastructure.	» Can you fully test the security features of the SSE solution during the trial, such as threat detection, data protection, and adaptive access controls? » What performance metrics are available during the trial? Can you monitor and assess key indicators such as latency, throughput, and uptime? » What unique benefits, features, or use cases does the SSE solution offer that others do not?

Tip

Future-proofing by Third-Party Analysts: Ensure that the SSE solution you choose is forward-thinking, with capabilities to adapt to future security challenges and technological advances.

Gartner has named Netskope a Leader in the 2024 Gartner® Magic Quadrant™ for Security Service Edge. Access the report.

Forrester has named Netskope a Leader in The Forrester Wave™: Security Service Edge (SSE) Solutions, Q1 2024. Access the report.

Interested in learning more?

Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.