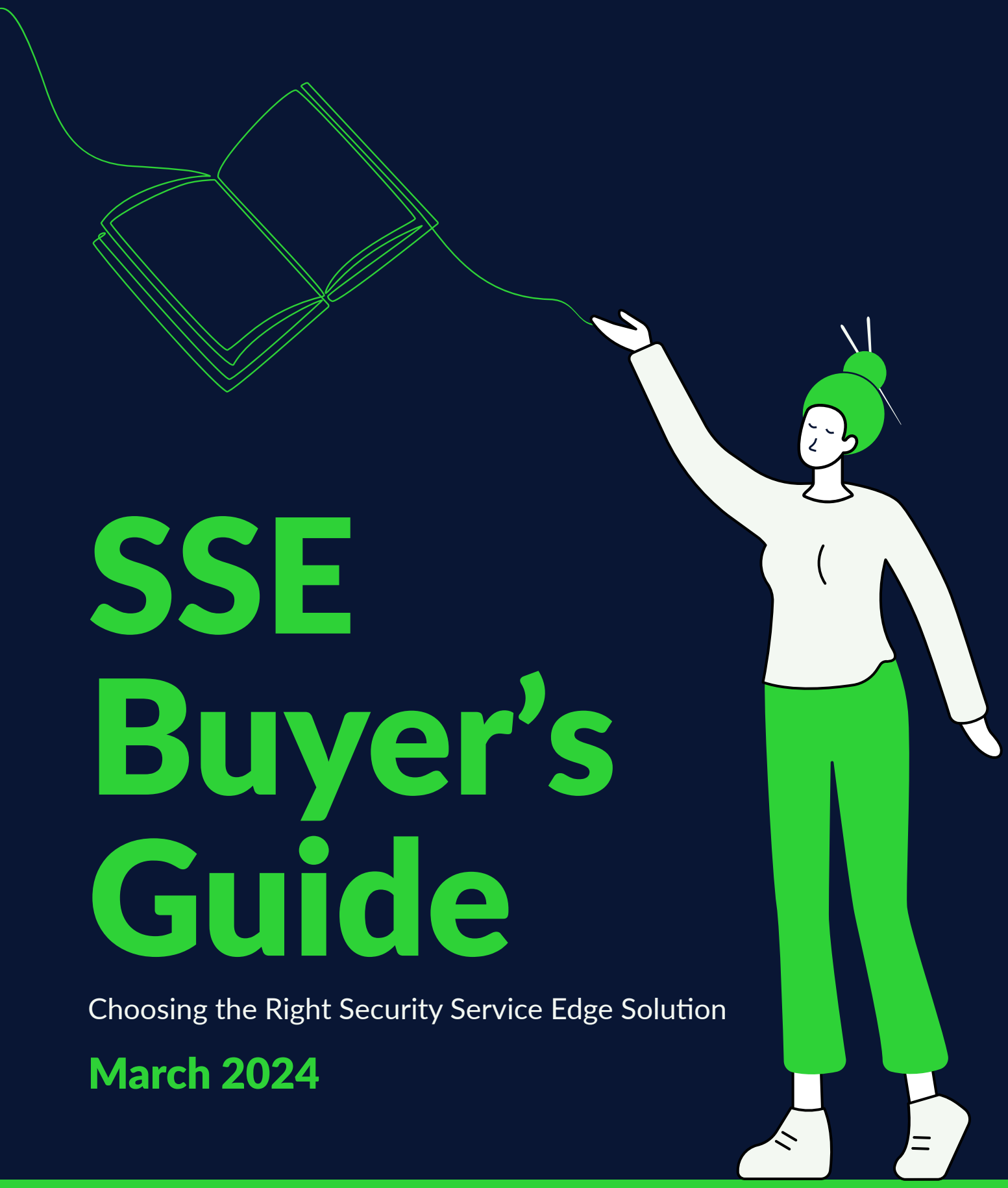
VERSA NETWORKS



SSE Buyer's Guide

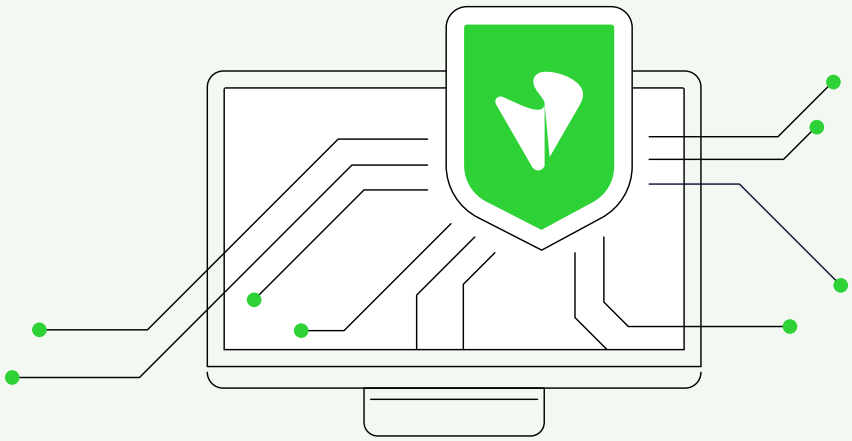
Choosing the Right Security Service Edge Solution

March 2024

Table of Contents

Introduction

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 Traditional security approaches are proving themselves outdated in a new era of expanding cloud services, IoT devices, flexible work, and sophisticated threats. To adapt enterprise security to this new reality and address these challenges more robustly, a new approach called Security Service Edge (SSE) has emerged that is a logical outgrowth of recent advances in cloud and networking technologies. This buyer's guide aims to help you choose the right SSE solution for your organization's security needs. A well-chosen SSE solution, grounded in Zero Trust principles, can serve as the cornerstone of your organization's security architecture.



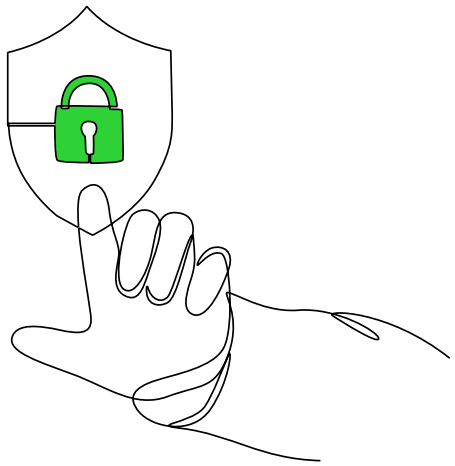
Understanding Security Service Edge (SSE)

SSE is a cloud-based solution that delivers an integrated set of security capabilities at the network edge, shifting security closer to users and devices while eliminating poorly integrated products, slow user experiences, and the management complexity of the past. SSE provides secure access to web, cloud, and private applications, threat protection against web and network attacks, and data leak prevention. It combines multiple point solutions into a single converged security service delivering Secure Web Gateway (SWG), Next-Gen Firewall (NGFW), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and Zero Trust Network Access (ZTNA).

For more background, see the white paper
SSE: A New Strategy to Secure Every Edge

Key Considerations for an SSE Solution

To help you evaluate different SSE solutions, we begin immediately below with a discussion of several "first principles" as general guidance on what you should be looking for, followed by discussion of specific requirements in the ensuing SSE Feature Evaluation Criteria section. We have organized these requirements into three categories – web and cloud security requirements, zero trust access requirements, and platform requirements. You will also find a one-page "at-a-glance" checklist of these requirements at the end in Appendix I.



The following are general expectations you should have for any SSE solution:

SSE should improve your security posture

Cyber threats today are faster and more sophisticated than ever. An SSE solution plays a critical role in enhancing your organization's security posture by providing a comprehensive and adaptive security framework that protects against a wide range of cyber threats. By integrating various security functions such as data protection, threat prevention, and secure access within a unified cloud-based platform, an SSE solution ensures that security policies are consistently enforced across all users, devices, and locations. This is particularly crucial in an era of increased remote work and cloud adoption, where traditional perimeter-based security models are no longer adequate. An SSE solution also facilitates the implementation of a Zero Trust security model, which assumes that threats can exist both inside and outside traditional network boundaries, thereby requiring continuous verification of all access requests regardless of their origin. This approach significantly reduces the attack surface and minimizes the risk of data breaches, making it an essential requirement for organizations aiming to strengthen their security posture in a dynamic threat environment.

SSE should give you x-ray vision

If you don't have visibility, you don't have security. Visibility into network and user activities through detailed reporting and analytics is vital for informed decision-making and compliance management, and the premise of an integrated solution should both simplify AND enrich your ability to understand what is happening throughout your network.

SSE should be comprehensive

In evaluating an SSE solution, an essential consideration is the comprehensiveness of its security framework. It should include robust data protection measures like encryption and malware detection, advanced threat prevention tools such as sandboxing and intrusion prevention systems, and granular access control policies anchored in Zero Trust principles. The solution should offer seamless secure access to a wide range of cloud services and applications, while ensuring an efficient and consistent user access experience regardless of the user's location at any given time. Security measures should not compromise the user experience, maintaining high performance and low latency connectivity for remote users and branch offices.

SSE should work with what you have

Integration capabilities and scalability stand out as critical considerations. The chosen SSE solution should easily integrate with existing security infrastructure, support identity provider systems for authentication, and be capable of scaling to accommodate future growth in user numbers, devices, and data traffic. The solution should align with the organization's compliance requirements and data sovereignty concerns, especially for operations across multiple jurisdictions.

SSE should deliver on TCO

Evaluating the solution's total cost of ownership, alongside the vendor's reputation, support offerings, and the richness of their ecosystem, is fundamental. Opting for a vendor known for innovation, reliability, and comprehensive support can significantly enhance the value of the SSE investment. Organizations should engage in thorough market research, including proof-of-concept tests and consultations with industry peers, to ensure the chosen SSE solution aligns with their security needs, operational demands, and business objectives, setting a solid foundation for secure and efficient cloud-based operations.

SSE Feature Evaluation Criteria

Secure Web and Cloud Usage Requirements

Securing cloud and web usage is a critical component of an SSE solution, focusing on protecting users, data, resources, and IoT devices across the infrastructure. An SSE offering should integrate various security functions to provide comprehensive security for cloud-based services and internet access. This includes SWG, NGFW, CASB, and DLP capabilities.

Anti-malware and anti-virus defenses

The solution should scan all incoming web and cloud application traffic for malware, ransomware, and other advanced threats. By analyzing files and executable downloads in real time, the solution can identify and block threats before they reach the user's device.

Advanced threat protection

Effective threat detection and response are crucial to protect against advanced cyber threats and maintain the integrity and availability of services. Key requirements for advanced threat detection within an SSE framework include the deployment of multiple defensive layers utilizing a combination of signature-based, heuristic, and behavior-based detection methods to identify known and unknown threats, coupled with AI/ML-enhanced sandboxing to detonate and analyze suspicious files and URLs in a secure and isolated environment to identify patterns, anomalies, and emerging threats based on large data sets and predictive analysis.

Automated threat response

Once threats are detected, automated threat response should be enacted such as isolating infected devices, blocking malicious traffic, and/or revoking user access in real time to prevent the spread of a potential incident or threat.

SSL/TLS decryption and inspection

With the majority of web traffic being encrypted, SSE solutions must decrypt SSL/TLS traffic to inspect the content for malicious activity, potential data exfiltration, and policy violations. This ensures that encrypted traffic does not serve as a blind spot for security controls. The solution needs to deliver these decryption and inspection services while limiting or eliminating user experience issues like connectivity performance — note that this decryption and inspection can be a processing bottleneck for many cloud-based SSE solutions due to the static nature of their environments, having an elastic environment allows the solution to adapt to the customer's needs without noticeable issues.

IoT security

Internet of Things (IoT) devices are becoming increasingly pervasive in enterprise, medical, and industrial networks. Securing their communications is critical due to their sensitive data and the potential point of entry into the overall network they are connected to. Key capabilities to look for from an SSE solution include: device fingerprinting and identification for OT, IoT, IIoT, and IoMT devices; the ability to apply Zero Trust policies and appropriate segmentation; AI/ML-based threat detection for these devices based on anomalous behavior; and the ability to dynamically adjust these devices network access based on threat detection.

Web usage policy control

The solution should enforce organizational policies on internet use, ensuring security, corporate compliance, and efficient use of resources. This includes policy definition and management, user and group-based policies, category and reputation-based filtering of URLs and IP addresses (e.g., adult content, social media, entertainment, gambling), and keyword and content filtering.

Cloud app discovery (Shadow IT)

This capability provides comprehensive visibility into all cloud services being used within an organization, including sanctioned, tolerated, and unsanctioned applications. This visibility is crucial for understanding the organization's cloud footprint and for identifying potential security and compliance risks.

Cloud app identification and risk scoring

Once cloud applications are identified, the SSE solution should assess each app for potential security, compliance, and governance risks. This involves evaluating the security features and practices of the cloud service providers, such as data encryption standards, authentication mechanisms, and compliance with relevant regulations (e.g., GDPR, HIPAA). The solution should be able to identify all major cloud applications on the internet.

Cloud app usage management

The solution should allow organizations to enforce granular access control policies for cloud applications. These policies can restrict access to cloud applications and specific controls and functions within cloud applications based on user roles, locations, device types, and time of access, ensuring that only authorized users can access sensitive applications under specified conditions.

Data protection

Data Loss Prevention policies are central to a cloud data protection strategy. These policies prevent unauthorized sharing, transfer, or storage of sensitive data based on predefined rules and detection techniques. The solution should enforce DLP policies across cloud applications, taking actions that violate these policies such as information redaction or by preventing the upload of sensitive documents.

Zero Trust Network Access Requirements

ZTNA is a critical component of SSE solutions, embracing the principle of "never trust, always verify" to provide secure access by users and devices to private applications and resources.

The key requirements for ZTNA as part of an SSE solution include:

Identity-based access control

Robust Identity and Access Management (IAM) are used to verify and authenticate users before granting access to resources. This requires integrating with existing identity providers (IdPs) and supporting multi-factor authentication (MFA) to ensure that access is securely controlled and based on verified user identities.

Device assessment and enrollment

Devices attempting to access the network need to be assessed for compliance with the organization's security policies. This process involves checking the security posture of the device, using multiple contextual controls like the operating system version, the presence of required security software (antivirus, anti-malware), and the absence of known vulnerabilities or compromised states. Devices meeting these and additional criteria are only then allowed to connect.

Least privilege access

Least privilege access is applied to ensure that each user or device is only able to access the specific applications, resources, or data they need to fulfill their job responsibilities. This minimizes the potential for lateral movement within the environment by creating micro-segmentation for SSE users/devices and network resources.

Continuous posture assessment

Client posture monitoring provides real-time assessments of risk and compliance by performing regular host checks to ensure that the device, while connected without forcing any disconnects, still complies with the assessment performed during initial enrollment.

Dynamic policy enforcement

ZTNA solutions must enforce access policies based on the user privilege and context of each access request based upon the criteria set during the initial enrollment of the user/device. If a device falls out of compliance for any reason, the system should automatically restrict access to sensitive resources or disconnect/quarantine the device from the network altogether until the issues are resolved.

Encryption

All communications between users/devices, enterprise-owned resources either on-premises or in a hybrid environment, and the SSE platform should be encrypted, ensuring data privacy and the application of consistent security policies and access controls across a company's entire digital estate. This applies to data in transit and often extends to data at rest, providing comprehensive protection against interception and eavesdropping.

Platform Requirements

Characteristics of the solution from a platform design and operations perspective that bear special attention include:

Cloud-native architecture

The solution should be built as a cloud-native platform to ensure scalability, flexibility, and the ability to seamlessly integrate with cloud services and adapt to evolving security needs. This architecture supports rapid deployment, easy management, and automatic updates.

Hybrid environment support

Look for an SSE solution that supports dynamic segmentation across hybrid environments, including multi-cloud and on-premises setups.

Integration with your existing ecosystem

The solution should integrate seamlessly with an organization's existing tools such as an endpoint protection suite, identity provider, network monitoring solution, security analytics platform, automation platform, and mobile device management suite.

Global cloud backbone

An SSE solution should have a globally distributed network of points of presence (PoPs) interconnected with each other so that traffic engineered data can be passed from PoP to PoP to ensure low-latency access for users anywhere in the world. The solution must also know to select and use the security policy enforcement point that is closest to the user/device, considering not just geographic location, but also interconnection latency values for the specific application access being made. This is critical for maintaining high performance and a positive user experience, especially for remote and mobile workers.

Scalability and reliability

The platform must be elastic to support peak demand bursts and the overall growth of an organization's users, devices, and data, demonstrating the ability to activate additional global PoPs and processing resources as needed and on demand. It should offer high availability and reliability to ensure continuous access to applications and services.

Visibility, analytics, and real-time reporting

The solution should provide deep visibility into threats and vulnerabilities and collect a wide range of data types from various sources, including network traffic, user activities, application usage, security events, and threat events, and process data in real time as a foundation for comprehensive analytics and reporting. Employing AI/ML to enhance analytics can help in identifying patterns, anomalies, and trends in the data. An effective real-time reporting system must include an alerting mechanism that notifies relevant personnel of critical events or indicators of compromise (IoCs).

Unified management and operations

A unified approach to SSE should mean a single management console. This simplification reduces the complexity of managing disparate security tools, enabling more efficient policy configuration, enforcement and updating across the entire security infrastructure. Note that some vendors have acquired and "bolted together" disparate security tools to try to create this unified approach – make sure to evaluate the ease of administration, policy management, analytics, and troubleshooting across all SSE functional capabilities.

Advanced AI and ML capabilities

Artificial intelligence (AI) and machine learning (ML) can contribute advanced capabilities for threat detection, response, and predictive analytics. Using AI/ML to enhance the analysis of network traffic and user behavior can uncover Indicators of Compromise (IoC) and establish security baselines. The solution should perform predictive analysis for potential threats before they materialize, allowing automated preventive measures to be taken through dynamic controls based on the risk profile of a user or device.

Cost efficiency

Consolidating security services into a unified platform will result in significant cost savings. Organizations can reduce the overhead associated with licensing, integrating, and managing multiple standalone security products. Additionally, operational efficiencies gained through centralized management can further reduce total cost of ownership.

User experience

A unified SSE platform should deliver a seamless and consistent user experience, regardless of where users are located or what resources they are accessing. Security measures should not impede performance or usability, which is particularly important for supporting flexible workforces – who may be working from home, an office, and on the road in a given week or even day – using cloud-based applications.

Compliance

The SSE solution should meet major compliance standards (SOC type 2, ISO 27001, GDPR, HIPPA, PCI, etc.), taking into account that your data is being transported by and residing in hosted infrastructure. By centralizing the oversight of data protection and access controls, organizations can easily generate reports to streamline and validate compliance during yearly audits.

Conclusion

Selecting the most suitable SSE solution is a pivotal step for organizations aiming to bolster their cybersecurity in an era marked by complex digital threats and distributed work environments. It will enable you to maintain the strongest possible security posture across all cloud services, web access, and private applications, irrespective of where your users are located or what devices they are using, and without compromising their productivity.

A comprehensive SSE solution should not only address immediate security challenges, but also be capable of adapting to the evolving landscape and scaling with the organization's growth. It must deliver robust threat protection, vigilant data protection, granular access control, and continuous monitoring while ensuring a seamless user experience.

As you embark on the journey to secure your digital perimeters, consider not just the technical capabilities, but also the vendor's reputation, the solution's integration ease, and the overall value it brings to your organization. A trusted vendor with a proven track record, robust support structure, and a clear vision for the future of cybersecurity will be a valuable partner in safeguarding your enterprise's assets. Remember, the right SSE solution is more than just a tool — it is an investment in the resilience and sustainability of your business operations in an interconnected digital world.

Appendix I

SSE Feature Evaluation Checklist

Platform Requirements

- ☐ Cloud-native architecture
- ☐ Hybrid environment support
- ☐ Integration with your existing ecosystem
- ☐ Global cloud backbone
- ☐ Scalability and reliability
- ☐ Visibility, analytics and real-time reporting
- ☐ Unified management and operations
- ☐ Advanced AI and ML capabilities
- ☐ Cost efficiency
- ☐ Seamless user experience
- ☐ Simplified compliance management

Zero Trust Network Access Requirements

- ☐ Identity-based access control
- ☐ Device assessment and enrollment
- ☐ Least privilege access and microsegmentation
- ☐ Continuous posture monitoring
- ☐ Dynamic policy enforcement
- ☐ Encryption

Secure Cloud and Web Usage Requirements

- ☐ Anti-malware and anti-virus defenses
- ☐ Advanced Threat Protection
- ☐ Automated threat response
- ☐ SSL/TLS description and inspection
- ☐ IoT security
- ☐ Web usage policy control
- ☐ Cloud app discovery (Shadow IT)
- ☐ Cloud app identification and risk scoring
- ☐ Cloud app usage management
- ☐ Data protection

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.

Thousands of customer's globally with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security. Versa Networks is privately held and funded by Sequoia Capital, Mayfield, Artis Ventures, Verizon Ventures, Comcast Ventures, BlackRock Inc., Liberty Global Ventures, Princeville Capital, RPS Ventures and Triangle Peak Partners.

Versa Unified SASE Platform

Securely connect any user, device or location to any workload or app

VERSA NETWORKS

SSE Buyer's Guide

Choosing the Right Security Service Edge Solution

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

Follow us on @versanetworks