HPE aruba networking

Business white paper

CHOOSING THE RIGHT SSE PLATFORM

HPE

In today's dynamic and interconnected business environment, organizations are adopting hybrid cloud architectures, blending on-premises infrastructure with cloud-based applications and services. This strategic move allows businesses to leverage a wealth of benefits, including access to data and resources, enhanced agility, and scalability to meet evolving business demands.

However, this transition to a hybrid cloud landscape has also introduced a new set of security challenges, presenting organizations with the daunting task of safeguarding networks and sensitive data from increasingly sophisticated cyber threats.

This new decentralized nature of hybrid cloud environments poses unique challenges to the traditional, familiar security measures. With users, devices, data, and applications spread across multiple environments, organizations face the arduous task of maintaining consistent security policies and configurations across on-premises and cloud-based resources. This complexity hinders visibility into the overall IT infrastructure, making it difficult to identify and respond to potential security breaches promptly.

To effectively address these security challenges, organizations must adopt a holistic approach that encompasses both on-premises and cloud-based security measures. This integrated approach requires a unified security strategy that aligns with the overall IT architecture, ensuring consistent security policies and configurations across all environments.

Organizations must also prioritize visibility and control across their hybrid cloud infrastructure. Implementing comprehensive monitoring tools and visibility solutions can enable organizations to gain a complete understanding of their IT environment, enabling them to detect anomalies and potential threats early on.

The challenges faced in our new hybrid world

This transition to hybrid cloud environments has exposed organizations to a broader attack surface, with endpoints extending far beyond the traditional perimeter of corporate networks. This distributed nature makes it challenging to enforce consistent security policies and effectively protect against threats that can enter through any entry point, including cloud applications, remote workers, and personal devices.

Additionally, the increasing sophistication of cyberattackers is making it even more difficult to detect and mitigate attacks using traditional perimeter-based security solutions. These traditional approaches often rely on signature-based detection, which can be bypassed by attackers using new and unknown malware.

What is SSE and why now?

Security service edge (SSE) is a relatively new term that encompasses security solutions that have been around for quite some time. In 2021, Gartner introduced the SSE framework as a way to bring these disparate security solutions together under a single umbrella. This consolidation has made it easier for organizations to adopt and manage these solutions, while also driving innovation in the market.

The core concept of SSE is to deliver security services closer to users and applications, regardless of their location. The cloud-based architecture eliminates the need for multiple security appliances deployed at various locations, simplifying network management and reducing operational costs. Gone are the days of constant patching, downtime, and hardware renewal cycles.

SSE's unified approach to security provides a comprehensive suite of capabilities that address the evolving threat landscape:

— **Zero trust network access (ZTNA):** Enforces strong authentication and authorization policies, preventing unauthorized access to sensitive data and resources. ZTNA eliminates reliance on traditional perimeter-based security, replacing it with identity-based access that verifies users and devices before granting access to specific applications and data. This approach enhances security by granting access only when necessary and for specific tasks.

— **Secure web gateway (SWG):** Protects users from malicious websites and content, preventing data breaches and malware infections. SWGs filter and inspect web traffic, ensuring only legitimate and trusted websites are accessible to users, shielding them from phishing attacks, malware downloads, and other online threats.

— **Cloud access security broker (CASB):** Controls access to cloud applications, ensuring that users access authorized and secure environments only. CASBs enforce granular access policies, granting or denying access based on user identity, device posture, and application risk. This helps organizations mitigate data breaches and compliance violations associated with unauthorized cloud access.

— **Digital experience monitoring (DEM):** Measures and analyzes user experience across all applications, devices, and networks, providing insights into performance issues and identifying potential security threats. DEM tools gather data on network traffic, user behavior, and application performance, enabling organizations to pinpoint performance bottlenecks, diagnose network disruptions, and detect anomalous activity that could indicate security breaches or malware infections.

SSE has emerged as a compelling solution to address the challenges of hybrid cloud security, particularly for organizations with distributed workforces and a growing reliance on cloud-based applications. By consolidating security services into a unified cloud-based architecture, SSE simplifies security management, reduces operational costs, and enhances overall security posture.

As organizations continue to embrace hybrid and cloud architectures, SSE is expected to play an even more crucial role in protecting their data, applications, and users from evolving cyber threats. By adopting SSE solutions, organizations can effectively safeguard their digital assets and maintain resilience in the face of evolving security challenges.

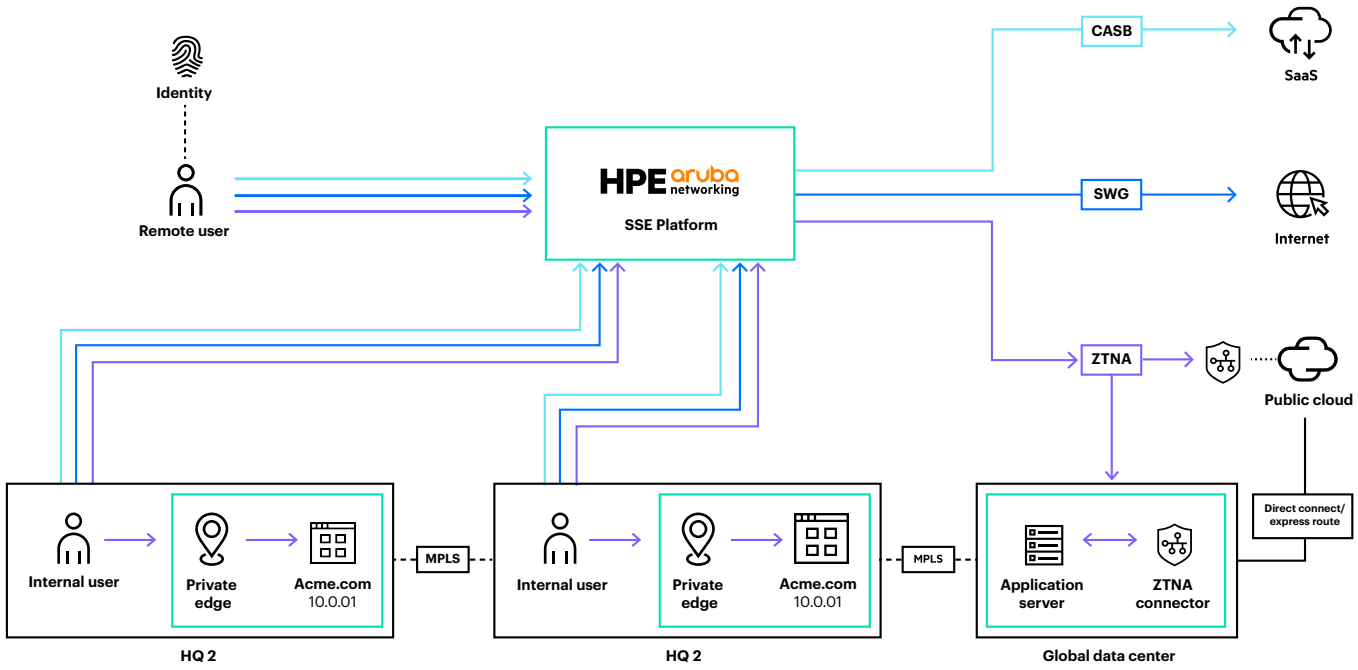

Figure 1. HPE Aruba Networking SSE architecture

Not all SSE platforms are the same

While SSE offers a unified security solution, it's also crucial to recognize that not all SSE platforms are created equal. Each platform has its unique strengths and limitations, making it essential for organizations to carefully evaluate their specific requirements before making a decision. There are several things that you should consider when purchasing an SSE solution.

Architecture

The architectural approach of SSE platforms significantly influences their performance, scalability, redundancy, resilience, and ease of management. Physical data center-based SSE platforms are constrained by the need for dedicated hardware, limiting their flexibility to accommodate evolving requirements or expand capacity when needed. They also often encounter redundancy and resilience challenges in the event of hardware failures.

In contrast, cloud-based SSE platforms fully harness the power of cloud infrastructure, providing elasticity and flexibility. These platforms tap into hyperscalers' robust backbones to enhance performance and minimize latency for users, optimizing the overall user experience. Cloud architecture allows for edge and PoP locations to be easily scaled out without requiring new hardware or new data center contracts. With cloud-based SSE platforms, scalability becomes the provider's responsibility and not the customers. The best SSE solutions are cloud-agnostic and built on top of multiple cloud vendors, and the best-practicing SSE platforms have built-in redundancy measures to ensure zero outages or downtime.

Organizations should meticulously evaluate the architectural design of their prospective providers' SSE platforms to ensure resilience, redundancy, flexibility, and a favorable user experience.

Simplicity

Ease of use is paramount when selecting an SSE platform. Platforms built from the ground up for simplicity feature intuitive interfaces and administrator-friendly configuration tools, streamlining both deployment and management. This leads to reduced training time for IT and security teams as well as fewer configuration errors.

In contrast, SSE platforms that are cobbled together from multiple disparate products often pose a significantly steeper learning curve for IT and security teams, demanding higher technical proficiency for configuration which can often lead to human error and overall, a poor security design. Simplicity leads to lower management costs and an improved security design.

Organizations should carefully assess the complexity of each SSE platform to ensure optimal user experience and efficient management practices.

User experience

A seamless and responsive user experience is crucial for any security platform, including SSE. A good SSE platform should provide users with a simple and easy-to-use portal, minimal latency and uninterrupted access to applications and data, regardless of location or device. Simple interfaces minimize training time and ensure easy adoption for all users. Fewer logins and streamlined workflows boost user productivity and satisfaction, and simplified authentication minimizes human error and potential security vulnerabilities by reducing login requirements.

In contrast, SSE platforms that necessitate users to navigate multiple, different user interfaces and repeatedly log in or authenticate hinder productivity, increase response times, and compromise overall security.

Organizations should choose a platform that prioritizes user experience and minimizes unnecessary friction. This will lead to a positive user experience, foster happier and more productive employees, streamline workflows, and reduce troubleshooting — saving time and resources.

Capabilities

A comprehensive SSE platform should seamlessly integrate the core SSE features of SWG for web protection, CASB for cloud access control, ZTNA for secure application access, and DEM for user experience monitoring into a single unified platform to safeguard organizational data, applications, and users. This unified approach eliminates the need for multiple disparate platforms, providing a centralized management interface for enhanced security posture and reduced operational complexity.

In contrast, fragmented SSE solutions from multiple vendors require individual, piecemeal products to replicate the same level of functionality, leading to inefficiency, potential security gaps, and management challenges. Juggling multiple platforms creates unnecessary complexity and overhead and disparate solutions often lead to vulnerabilities between functionalities. Managing multiple vendors and interfaces increases the difficulty.

Organizations should prioritize unified platforms that consolidate these core functions, streamlining operations, strengthening security posture, and minimizing the risk of threats and breaches.

Integrations

Seamless integration with existing security infrastructure is critical for unified threat detection and incident response. SSE platforms should integrate with Security Information and Event Management (SIEM) and Security Orchestration Automation and Response (SOAR) systems to enable organizations to effectively respond to security threats across their entire security stack. Tight integration with SIEM and SOAR systems enables comprehensive threat visibility and swift incident response throughout your organization's attack surface. Additionally, integration with Identity Access Management (IAM) solutions is a must, as these are typically already deployed in most enterprises. The user, app, and device access policies should seamlessly tie into these installed IAM systems.

In contrast, SSE platforms that lack tight integration with existing infrastructure make it challenging to manage security threats effectively. Disparate systems hinder visibility and slow down incident response. Lack of data correlation limits your ability to understand and address complex threats. Security gaps between tools create vulnerabilities for attackers to exploit.

Visibility

Granular insights into user behavior, network patterns, and traffic flow are essential for effective security operations. SSE platforms should provide deep visibility to identify anomalies, detect potential threats early, and take immediate action to protect networks and data. Proactive threat hunting and mitigation becomes possible with comprehensive visibility into network activities, and you gain a detailed understanding of data movement within your network for better control and optimization. This means you can quickly identify and isolate potential threats before they can cause damage.

In contrast, SSE platforms that provide limited insights or require separate platforms for this functionality hinder visibility and make it difficult to identify and address security risks. Lack of insight can leave your network vulnerable to undetected attacks, and the inability to identify threats early puts your organization at risk.

Selecting the right SSE platform: A strategic decision

The selection of an SSE platform is not merely an IT decision; it is a strategic one that has profound implications for an organization's security posture, overall resilience, and ability to thrive in the digital era. Organizations must carefully consider their unique security needs, risk tolerance, and growth objectives to identify the SSE platform that aligns seamlessly with their evolving security landscape.

The architectural foundation of the SSE platform plays a crucial role in determining its ability to adapt to changing security requirements and scale with the organization's growth. Cloud-based SSE platforms, with their inherent scalability and elasticity, offer organizations unparalleled flexibility and cost-efficiency. These platforms can provision and decommission resources on-demand, ensuring optimal performance and always-available security to meet the organization's needs.

Simplicity is not a luxury; it is a necessity in today's complex cybersecurity environment. A user-friendly SSE platform simplifies deployment, configuration, and management, reducing the burden on IT and security teams. Organizations should prioritize platforms that offer intuitive interfaces and configuration wizards to streamline operations and minimize human error.

Effective SSE platforms encompass a comprehensive suite of security capabilities, seamlessly integrating the core functionalities of ZTNA, SWG, CASB, and DEM. This unified approach eliminates the need for multiple disparate platforms, providing a centralized management interface and reducing operational complexity.

To effectively combat the ever-evolving threat landscape, SSE platforms must seamlessly integrate with existing security infrastructure, particularly SIEM platforms. This integration enables organizations to correlate events, prioritize threats, and automate incident response processes, ensuring that security teams can respond swiftly to emerging threats.

Granular visibility into user behavior, application usage, and network traffic is the cornerstone of effective security operations. SSE platforms should provide deep insights into these critical data points, enabling organizations to identify anomalies, detect potential threats early, and take immediate action to protect their assets. This visibility also facilitates compliance audits and helps organizations understand user behavior patterns, preventing misuse of resources and identifying potential security risks.

Next steps

Selecting the right SSE platform is a critical decision that requires careful consideration of architectural foundation, simplicity, capabilities, integrations, and visibility. Organizations that prioritize these factors will establish a unified, scalable, and adaptable security strategy that empowers them to navigate the ever-evolving cybersecurity landscape, protect their valuable assets, and drive business success in the digital era.

HPE Aruba Networking SSE is a connectivity-as-a-service platform that elegantly integrates ZTNA, SWG, CASB and DEM into a single, easy to use interface. Our solution helps protect organizations of all shapes and sizes worldwide and enables safe, compliant productivity. Consider how HPE Aruba Networking can assist you in your pursuit of a comprehensive SSE platform to best protect your corporate assets.

Visit HPE.com

Learn more at

Meet with an SSE expert

Free ZTNA test drive for 24 hours

Chat now

a00143070ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com