WHITE PAPER

# Security Service Edge

*A New Strategy To Secure Every Edge*

# Table of Contents

## Introduction

Organizations face significant challenges when securing their digital transformation initiatives, with traditional perimeter boundaries dissolving due to cloud, IoT, and hybrid work, leaving a network edge that is now everywhere- wherever data, users, and devices exist. Over time, piecemeal adaption of legacy security to this new reality has meant organic growth of point products in modern data center security stacks, leading to performance issues and making them complex to manage and challenging to integrate. Point products are daisy-chained together, resulting in latency and degrading the user experience. Administrators must cope with isolated policies for every user, device, and location. In turn, manually correlating fragmented and limited identity data across disparate systems generates volumes of false positive incidents, requiring additional specialized tools for response and remediation. This complexity creates gaps which can be exploited by advanced malware, phishing threats and ransomware attacks.

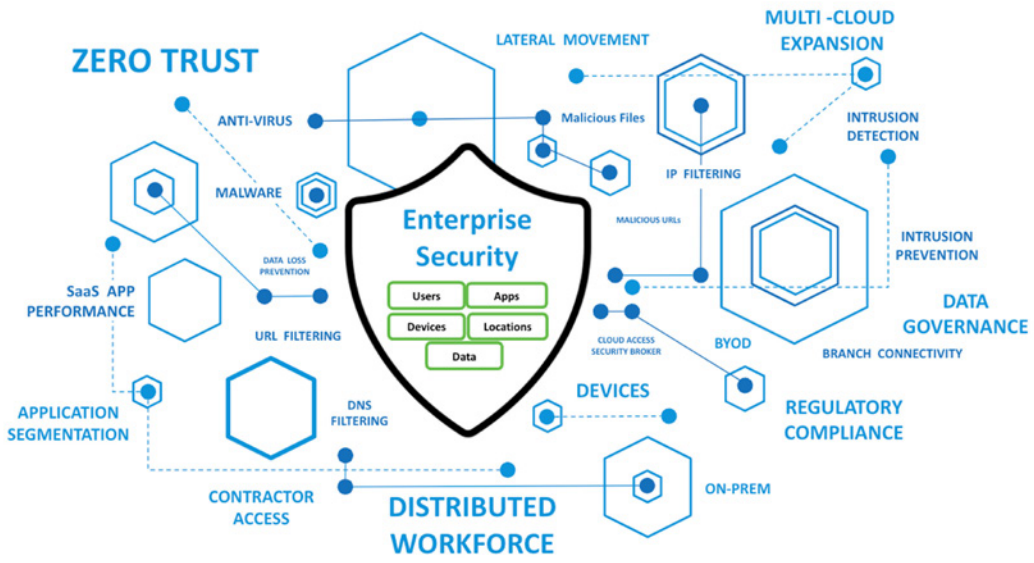



*Figure 1 - The evolving threat landscape for enterprise security -- risk has grown exponentially with cloud growth and hybrid work.*

Put simply, where people work has changed, and what people need access to – SaaS apps on the internet, private data center apps, private cloud apps, et al. – has expanded drastically. The attack surface has expanded correspondingly and the nature of threats has changed, so how we defend our users and data now has to change with it.

A promising new architectural response to growing complexity and continued security failures took form when two analysts at Gartner coined the term SASE – Secure Access Service Edge – to define a new approach evolved from the world of SD-WAN that combines networking and security in a single, scalable, cloud-native platform. Security Service Edge (SSE), a term also coined by Gartner, is then the security component of SASE.

## What is Security Service Edge?

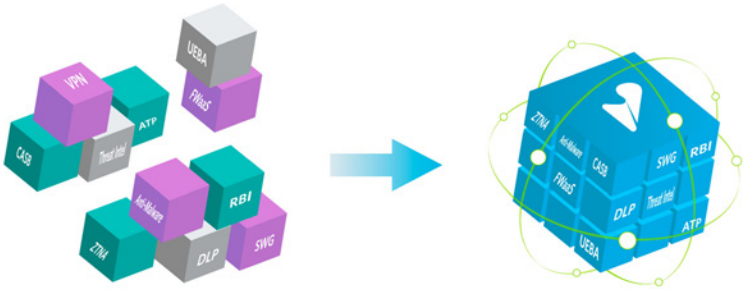
A Security Service Edge (SSE) solution is the convergence of security services delivered from a purpose-built cloud platform. By decoupling security from a centralized networking location and placing it at the edge, where it can be most efficient and useful, organizations can reduce their risk, increase their agility, and improve the user experience.

There are three classes of security services that SSE brings together:

- Secure access to the web, cloud services, and private applications
- Threat protection from web and network-delivered attacks
- Protection against data leaks and breaches

SSE combines access control, threat protection, data security, security monitoring, and acceptable-use controls. SSE can be considered an integral component of the secure access service edge (SASE) framework, with its architecture squarely focused on security services. SSE controls can be enforced across all hybrid environments to include edge, cloud, and on-premise.

SSE consists of four core services: a secure web gateway (SWG), a cloud access security broker (CASB), Data Loss Protection (DLP), and a zero trust network access (ZTNA) framework.




## How SSE Differs from Legacy Security

As a practical matter, SSE's integrated, cloud-based architecture represents a leap forward compared to traditional security approaches and differs in the following ways:

### Better Risk Reduction

- Central Management - SSE integrates and consolidates security functions, enabling centralized management and reducing the complexity of managing multiple security products. This approach enables organizations to enforce consistent security policies across all users and devices, regardless of location.
- Threat Detection and Response - SSE provides real-time threat detection and response capabilities using advanced analytics and machine learning algorithms. These capabilities enable SSE to identify and mitigate threats quickly, reducing the risk of data breaches and other security incidents.
- Identity Protection - SSE uses identity-based access control, which limits access to resources based on user identity and context. This approach reduces the risk of unauthorized access to sensitive data and applications.

- Network DLP - SSE utilizes Network Data Loss Prevention (DLP) solutions to prevent leakage of sensitive information via the network. An effective Network DLP solution monitors, detects, and potentially blocks sensitive data exfiltration while the data is in motion across the network using various protocols or when it is residing on popular cloud repositories. Network DLP is also used to enforce regulations required by certain industries to ensure that Enterprise organizations are able to demonstrate adequate care to avert the loss or theft of confidential and sensitive information.
- Continuous monitoring and analytics - SSE uses advanced analytics and machine learning algorithms to monitor users, device and network traffic in real-time. This enables SSE to detect and respond to threats quickly, reducing the risk of data breaches and other security incidents.

## Embraces Zero Trust

SSE is built fundamentally on the concept of zero trust as shown in Figure 4 below, specifically it is based on the following fundamental capabilities:

- Least privilege access - SSE provides users with the minimum level of access required to perform their job functions. This approach reduces the risk of unauthorized access to sensitive data and applications.
- Identity-based access control - SSE uses identity and context to control access to resources. Users are required to authenticate and provide additional context, such as their location, device, and behavior, before accessing resources.
- Dynamic policy enforcement - SSE dynamically adjusts security policies based on changing threats and business needs.
- Micro-segmentation - SSE uses micro-segmentation to divide the network into smaller segments, each with its own security policies that continuously monitor users, devices and network traffic in real-time. This approach limits the lateral movement of threats and reduces the attack surface.

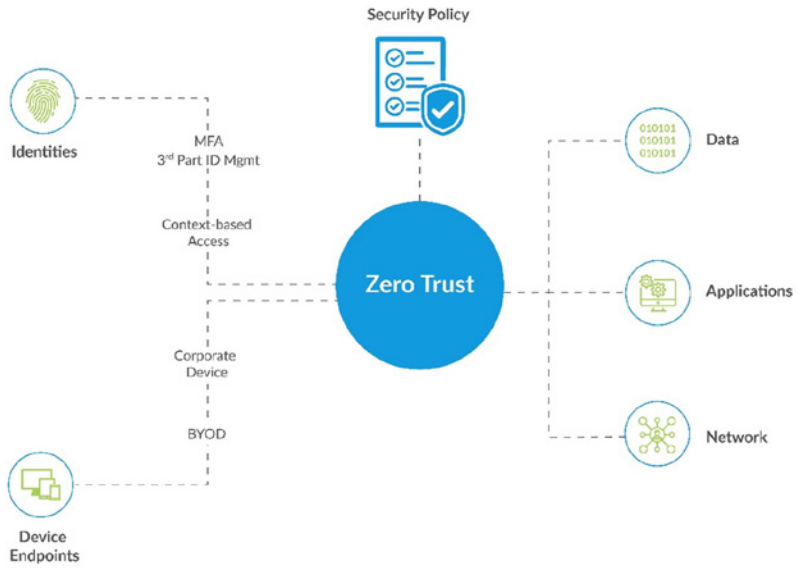



*Figure 2 - Note: Shift in Enterprise Security Landscape with Zero Trust. Users, Devices, Data, and Applications are Everywhere. Legacy security solution sprawl is obsolete.*

### Platform Security by Design

SSE brings the advantages of its cloud origins to the table, including:

- Security at the edge - SSE integrates security functions into the network edge, providing a comprehensive security solution for cloud-based applications and mobile users. SSE's security-by-design approach also reduces the risk of security vulnerabilities and makes it easier to maintain security over time.
- Simplicity - Having a unified platform with a unified management console and a single place to define and manage security policies reduces the complexity of managing multiple security products and enables organizations to enforce consistent security policies across all users and devices, regardless of their location.
- Scalability - A cloud-delivered platform also enables organizations to scale their security infrastructure more easily, reducing the cost and complexity of managing security at scale.

## The Core SSE Use Cases

Security Service Edge (SSE) integrates networking and security services at the edge of the internet to provide secure access and improved performance for cloud applications and remote users. Use cases include protecting remote workforces from cyber threats, streamlining cloud application access, and reducing latency for users distributed globally.

### Secure Cloud Access

SSE can provide secure to cloud-based applications and data. This is especially beneficial for organizations that leverage SaaS applications or store sensitive data in the cloud, as SSE can help maintain security compliance and data privacy.

### Secure Branch Office Connectivity

For organizations with multiple branches or remote offices, SSE can provide secure and direct connectivity to both cloud and on-premises resources. This is done while maintaining consistent security policies and managing all branches through a single pane of glass.

### Remote Workforce Security

With the increase in remote work, ensuring the security of remote connections is critical. SSE can provide secure and optimized connectivity for remote employees, ensuring they can access resources securely from any location.

### Data Security

SSE can help in the protection of sensitive data by enforcing security policies at the edge of the network. This includes data loss prevention, secure web gateways, and cloud access security brokers.

### Compliance Management

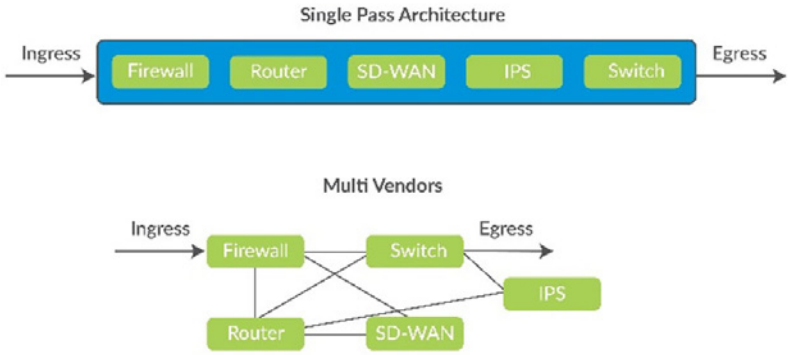
SSE can help organizations maintain compliance with various regulatory standards by providing detailed visibility and control over network traffic, user behavior, and data access. This can simplify the process of compliance reporting and auditing.

### Threat Detection and Response

By embedding security directly into the network infrastructure, SSE can help in identifying and neutralizing security threats in real-time. This capability can enhance an organization's overall cyber threat intelligence and response effectiveness.

## Considerations in Evaluating an SSE

### The importance of a single pass architecture.




A single vendor does not necessarily mean a single product, nor a single path for packets to follow. Many vendors have "bolted together" their SSE solutions from multiple point products that are loosely integrated and built on different approaches and architectures, perpetuating the legacy problem of systems complexity and essentially defeating the purpose of adopting SSE in the first place. This can result in a single packet being forwarded, decrypted, inspected, re-encrypted, and forwarded multiple times across these disparate products, significantly impacting performance.

This ensures increased visibility, significantly better performance, and enhanced security controls while maintaining control over operational costs.

### Security Shouldn't Degrade the User Experience

Latency in security products can be a significant issue, and its impact often varies depending on the specific security solution and the environment in which it's deployed. The importance of prioritizing the user experience can't be overstated, especially in the context of security.

Security solutions, especially those that inspect traffic or data in real-time (like intrusion prevention systems, web proxies, or antivirus software), can introduce latency. If this latency is perceptible to the end-users, it can reduce system or network performance, leading to user dissatisfaction.

These challenges are particularly pronounced with the increase in cloud adoption and remote working scenarios that are prone to hairpinning and collaboration apps where even minimal latency degrades the quality of the experience.

## All POPs Should Be Security Nodes

Every cloud POP (point of presence) should be a fully functional node running all security and networking functions, inspecting all traffic, and enforcing all policies. This approach is not shared by all SSE vendors, many of whom have cloud POPs that merely forward traffic to a limited set of security enforcement nodes, adding significant latency to their solutions.

## Centralized and Unified Management

Any SSE solution should enable centralized management of security policies across the entire network, reducing misconfigurations and speeding detection/response, and greatly reducing the Mean Time To Detection (MTTD) and Mean Time To Respond (MTTR) to security incidents.

## Dynamic Segmentation Across Hybrid Environments

Dynamic segmentation should be provided across hybrid environments and can reduce attack surfaces by dividing the network by class of traffic, by job responsibilities, by job functions across the entire enterprise network, and includes placement of devices and users into microsegments depending on device posture.

## Contextual Intelligence

A key aspect of SSE is the contextual intelligence and awareness of users, devices, sites, circuits, and clouds. This contextual intelligence enables robust and dynamic policies that support a multi-layered security posture.

## Distributed Policy Enforcement

Distributed policy enforcement at multiple data touchpoints enables defense-in-depth across multiple layers of the OSI model, with Layer 3 and 4 firewalls filtering traffic at the packet level and Layer 7 firewalls filtering content for granular protection.

## Advanced Analytics and Data Enrichment

Real-time analytics provide actionable insights into the advanced techniques of modern-day sophisticated threats. These can include real-time insights to network traffic and security threats, Detection of lateral movement, threat Intelligence and analytics.

## Flexibility and Scalability

The architectures should follow a centralized, multi-tenant “define once, deploy everywhere” approach for configuration and management. It should be able to support use cases across WAN, LAN, data center and cloud.

## Conclusion

As organizations accelerate their digital transformation journeys, it is crucial to implement a robust security strategy from the start that evolves as rapidly as the business. The traditional castle-and-moat approach is no longer sufficient as cloud adoption, mobility, and digital engagement expand the attack surface. Security Service Edge has emerged as a modern framework to effectively secure access and connectivity across today's dynamic and complex hybrid IT ecosystems. Rather than siloed point products, SSE provides an integrated suite of security services like SWG, CASB, DLP, NGFWaaS, and more on a unified software platform. This eliminates complexities, reduces costs, and improves security efficacy.

## About Versa Networks

Versa Networks is a leading innovator in SASE and SSE. Versa's solutions enable service providers and large enterprises to transform enterprise digital infrastructure to achieve unprecedented business advantages. Versa's carrier-grade cloud-native software platform provides unmatched agility, cost savings, and flexibility, transforming the business of networking. The company is backed by premier venture investors Sequoia, Mayfield, Artis Ventures, and Verizon Ventures.

For more information, visit https://www.versa-networks.com

Follow us on X (Twitter) @versanetworks.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com