PRODUCT BRIEF

Symantec® Security Service Edge (SSE)

Symantec Enterprise Cloud Security

AT A GLANCE

Flexible, Comprehensive, and Transparent:

- Comprehensive access protection
- Full-feature SSE capabilities
- Fast, flexible cloud deployment

Core Cloud Access Security Broker (CASB) Capabilities:

- Application visibility and control
- Shadow IT control

Core Secure Web Gateway (SWG) Capabilities:

- Cloud-delivered SWG as a service
- Reverse proxy
- Content analysis
- Cloud firewall service
- SSL inspection
- Centralized management
- Application visibility and control
- Advanced threat intelligence

Advanced Security Capabilities:

- Zero Trust Network Access (ZTNA)
- Full web isolation
- Advanced cloud sandboxing
- Hosted reporting

Comprehensive Follow-the-User SSE Capabilities

As enterprises embrace a digital transformation, they quickly realize that the only way to secure users, content, and resources in the cloud is to have their security in the cloud as well. Moving to the cloud is an enormous undertaking, especially for large, complex organizations. These organizations wrestle with the following challenges:

- How do get a complete SSE solution from a single vendor?
- How do I move security to the cloud without breaking anything?
- How can I replace my VPN technology to connect my users?
- How do I ensure a strong security posture when moving to the cloud?

To address the security challenges of digital transformation, the industry has coalesced around the framework of a Secure Access Service Edge (SASE) architecture. When data protection is a cornerstone of the framework, data-centric SASE becomes a means to achieving Zero Trust security in the cloud. But before data-centric SASE is possible, a SSE foundation must be in place.

However, SSE is only a blueprint for what organizations need to deploy. It is a vision of an end state, not a definitive guide for how to deploy it. There is no singular path that is right for everyone. What is next on a customer's SASE journey is determined by what they have, what is missing, budget, headcount, contractual obligations, regulations, business needs, and other factors. The journey to data-centric security is often a long one, and yet the most difficult step has long been the first: determining where to start…until now!

Symantec SSE – A Comprehensive Solution

Symantec® SSE removes the uncertainty of how to begin a SASE journey because it includes a comprehensive set of critical capabilities that customers can deploy how, when, and where they see fit. Symantec SSE is a complete solution for securing all network, web, and cloud applications with an industry-leading set of services deployed in a world-class edge network. Built upon a cloud-native architecture with an advanced secure web gateway, CASB controls, ZTNA, and Web Isolation, rich security capabilities are extended to web, public, and private cloud applications.

The rich, cloud-delivered SSE solution is supported with simplified management that allows customers to maintain consolidated policy across cloud and edge security environments. This enables digital transformation at any speed as users are seamlessly protected, whether they are working from headquarters, remote offices, or any location. Symantec SSE is easily matched with Symantec DLP Cloud, a uniquely capable information protection solution from Broadcom, to form the industry's most comprehensive, single-vendor, data-centric security solution.

KEY FEATURES

- SSE protection at a fixed, predictable, and annual per-user cost
- Includes advanced security options and integrations at no additional cost
- Supports flexible movement between cloud and on-premises
- Features critical network security access capabilities within the SSE framework

Incredible Value, Advanced Security

Core Capabilities

Symantec SSE features core cloud-delivered SWG capabilities and integration with the leading on-premises SWG—both of which can operate seamlessly together with a unified management, reporting, and policy control interface. Core CASB functionality gives customers greater insight and management of cloud applications. Organizations are secure with follow-the-user protection across both cloud and edge deployments.

Advanced Security

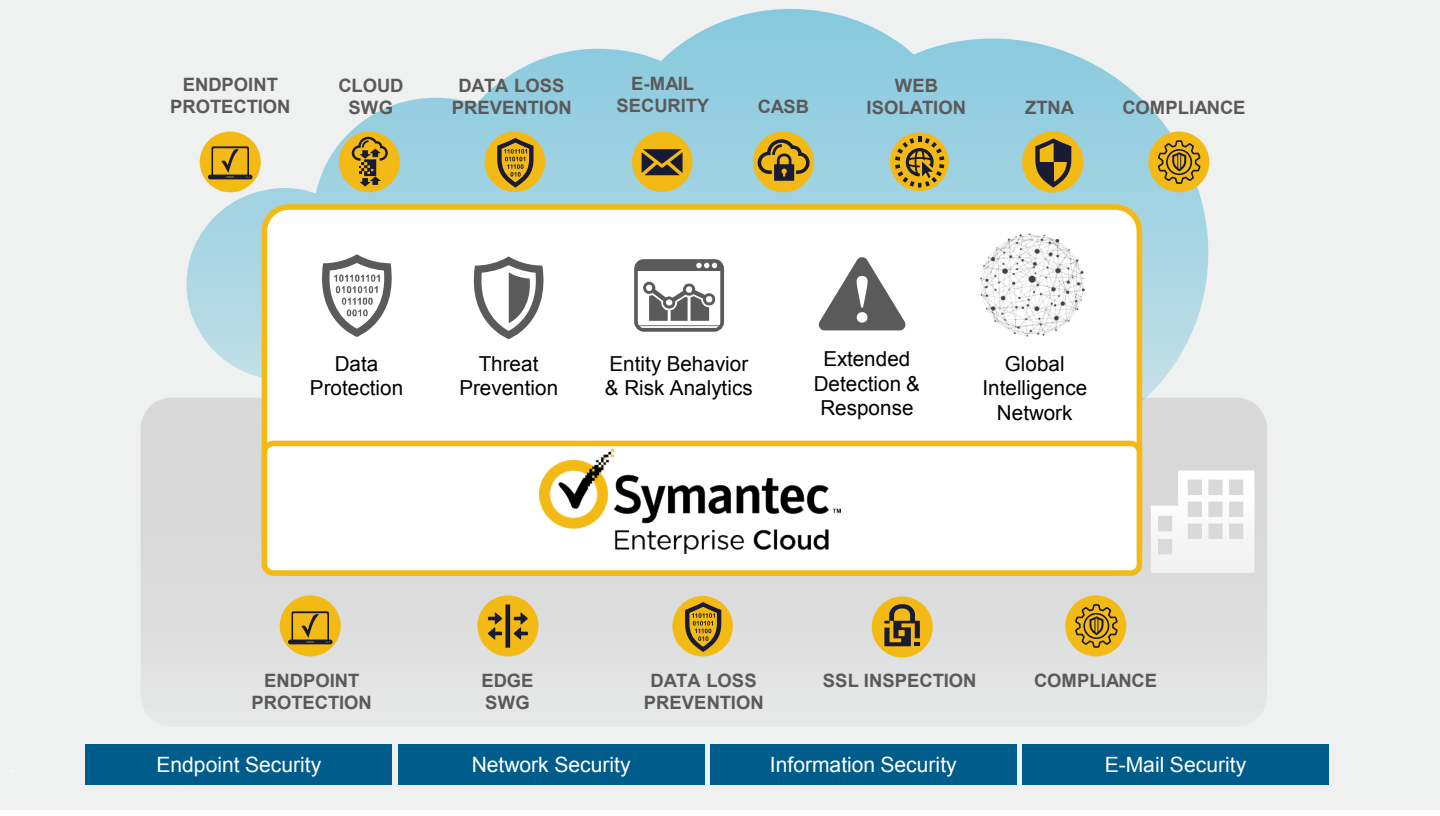
Broadcom takes network security to the next level with several advanced SSE capabilities. Innovative ZTNA technology enables secure access to private applications from any managed or unmanaged device, eliminating the need for a VPN.

Users are also protected from threats with Full Browser Isolation, Advanced Cloud Sandboxing, and Deep Content Inspection.

Symantec SSE capabilities are delivered on an advanced, edge-optimized network architecture that uses Google's public cloud infrastructure. It is closely peered with nearby ISPs, CDNs, and application providers, delivering hyperscale, reliability, and high performance.

Symantec SSE is a key network security component of Symantec Enterprise Cloud, integrating Broadcom® cybersecurity solutions—delivered from the cloud—for cloud, edge, and hybrid deployments.

Figure 1: The Symantec Enterprise Cloud



Components and Capabilities

With cloud-delivered protection available for every user, Symantec SSE supports comprehensive security environments where on-premises, hybrid, or all-cloud deployments are needed.

Table 1: Core SWG Capabilities

Components	What It Is	What It Offers
Cloud SWG	*Cloud SWG protection for every user, delivered as-a-service.*	*Fast, direct-to-net access delivers a better user experience while avoiding costly backhauling.*
Reverse Proxy	*Proxy architecture with integrated caching to accelerate delivery of web applications.*	*Protect web infrastructure by isolating origin servers from direct Internet access and safeguard with real-time anti-malware scanning of all uploaded content.*
Content Analysis and Symantec File Inspection	*Multi-layered inspection and threat detection engines with Symantec antivirus included.*	*Blocks known threats, sources, and signatures and centrally analyzes unknown content.*
Cloud Firewall Service	*Further protects remote users by extending firewall protections without backhauling traffic.*	*Identify and inspect all traffic on non-standard ports and define rules based on source, destination IP, destination service, and application.*
Centralized Management	*Centralized management and reporting for Symantec network infrastructure.*	*End-to-end visibility and control to improve web security, and cut operational costs.*
Advanced Intelligence Services and CASB Controls	*Real-time protection, categorization, and application control of web content. Includes CASB visibility into over 45,000 cloud applications.*	*Filters billions of URLs into easily managed categories for precision policy enforcement at the gateway. Control the use of Shadow IT.*
Zero Trust Network Access	*Zero Trust access to corporate resources hosted in cloud environments or on-premises data centers. This eliminates inbound connections to customer networks and creates a software-defined perimeter between users and corporate applications.*	*A VPN-replacement technology that allows only authorized users to connect to specific applications, without the need of an agent, while making applications invisible to attackers.*
Full Web Isolation	*Execution of all web sessions away from endpoints, sending only a safe rendering of information to users' browsers. This prevents any website-delivered, zero-day malware from reaching user devices.*	*Eliminates web-based malware and phishing threats and solves the challenge of providing secure access to uncategorized and potentially risky websites.*
Advanced Malware Analysis and Cloud Sandboxing	*Multi-layered inspection and sandboxing prevents threats that elude traditional analysis.*	*The most effective way to detect and neutralize file-based malware.*
Hosted Reporting	*Scalable log collection and storage for Edge and Cloud SWG deployments.*	*Intuitive reports for security specialists, department managers, HR managers, and network administrators who need visibility into web-related user activity.*

Stakeholder Advantages

Consistent high performance cloud security and support for edge deployments make Symantec SSE a great solution for all enterprise stakeholders.

Users

- Fast, frictionless access to content and applications
- Identical user experience whether working on premises or remotely
- Support for bring-your-own-device (BYOD) policies that favor end-user choice
- Up-to-date threat intelligence and web isolation eliminate the need for over-blocking websites to ensure security

Network Operations

- High-performance solution built on Google Cloud
- Hyperscale: add new locations or services in hours
- One set of tools and reports simplifies management
- Easy to use: provision thousands of users per day
- Universal policy enforcement provides single-policy management to cover on-premises and the cloud
- Cloud migrations can be tested, rolled out, or rolled back as needed
- True cloud solution that requires no on-premises gear

IT Security

- A wide range of advanced SSE capabilities ready to be switched on, including: SSL inspection, anti-malware, Content Analysis, Cloud Firewall Service, ZTNA, Web Isolation, log streaming, and more
- A single, familiar architecture simplifies policy enforcement and compliance, reducing risk
- Future-prepared for the SSE framework with integrations for DLP and full CASB
- Cloud-delivered agents can be provisioned instantly with no additional contracts or purchase orders

Finance and Executive Management

- Reduction in remote traffic backhaul charges
- Cost savings compared to separate security stacks
- Simplified per-user, per-year pricing
- Full life-cycle utility from legacy SWG investments—no need to rip and replace

One Solution for Any Cloud Strategy

Deployment flexibility and management simplicity establish Symanec SSE as the best choice for the broadest set of cloud security capabilities to secure an organization and align with the SSE framework. Unparalleled deployment ease and market leadership make the decision easy.

Table 2: Symanec SSE Flexibility

Strategy	Goals	Pathway
On-Premises	*Protect key on-premises data and applications, but expect growth in remote work and cloud applications.*	*Refresh on-premises proxies with virtual appliances as licenses expire; manage as a single environment.*
Cloud-First	*Prioritize cloud for economy and rapid scalability.*	*Protect data and applications with the full suite of included cloud-native security components.*
Hybrid	*Anticipate gradual move to the cloud or continued side-by-side architecture.*	*Adopt a hybrid approach and seamlessly shift users from edge to cloud as needed.*
Future-Focused	*Committed to the SSE framework long term but need to manage migration.*	*Move traffic to the cloud, maximize scalability, deliver advanced SSE features now and easily integrate with DLP Cloud when ready for full data-centric security solution.*
Risk-Averse	*Volatile or uncertain business environment demands a flexibility-first posture and quick response.*	*Protect users and data through cloud security, with no hardware or appliances to deploy.*
Cost-Averse	*Prioritize the cloud as a low-cost alternative.*	*Consolidate security and management under a single solution; maximizing use of advanced security capabilities.*

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SYM-Network-Protection-PB104 April 17, 2025