

SOLUTION BRIEF

KEY FEATURES

- The most comprehensive threat protection with a full network security stack
- High-performance, fully redundant cloud infrastructure
- Advanced Secure Web Gateway (SWG) technology
- Integrated next-generation firewall (NGFW) technology
- Integrated with endpoint protection technologies
- Validated security effectiveness
- Protects business-critical applications
- Continuous risk assessment and threat intelligence via Global Intelligence Network and Symantec STAR Labs
- Workflow automation for activities such as compliance audits and reporting
- Enterprise-class security management

Symantec® Cloud Firewall Service

Extend network protection beyond the web

Overview

Symantec® Cloud Secure Web Gateway (SWG) is the foundation of Symantec Security Service Edge (SSE). Built on industry-leading proxy and content analysis technology and powered by comprehensive threat intelligence, it is a cloud-delivered network security service that offers protection against advanced threats, provides access control, and safeguards critical business information for secure and compliant use of cloud applications and the web.

An Expanding Attack Surface Puts Data and Network Access at Risk

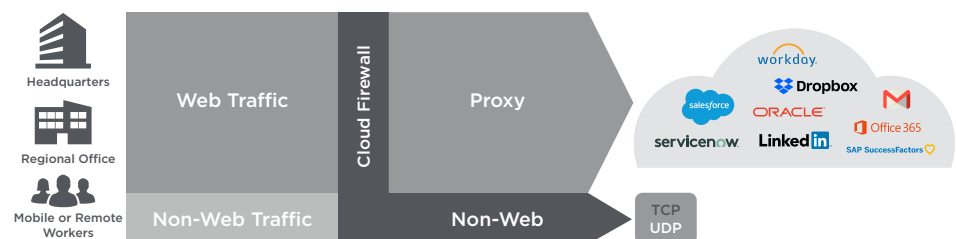
Greater exposure to threats through an ever-expanding attack surface is a key contributor to extended intrusion response times. Enterprises are embracing cloud services and direct-to-net access from branch offices, remote locations, and users on the go. Consequently, the attack surface continues to grow with many new connection points, all of which must be secured.

To meet this challenge, security architects need solutions that increase infrastructure visibility, enable immediate threat intelligence sharing, and unlock automated threat protection at all network edges, ensuring greater user protection from modern-day security threats. Solutions must be scalable, maintain high performance standards, and go beyond the web, securing all ports and protocols of traffic.

Symantec SSE Fortifies Network Security with SWG and NGFW Technologies

The integration of next-generation firewall (NGFW) technology into Symantec SSE expands the most comprehensive set of cloud-delivered threat prevention capabilities available today. This integrated solution provides real-time, intelligent protection against malware and emerging threats with control of network traffic over all ports and protocols, regardless of where enterprise users are.

Figure 1: Symantec SSE with Integrated NGFW Technology



The Symantec network security solution delivers a broad set of powerful capabilities—including SWG, Cloud Firewall Service (CFS), antivirus scanning, sandboxing, web isolation, Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and email security. Symantec SSE offers secure SSL/TLS inspection and high-performance threat protection. The integrated CFS capabilities include users/groups, source and destination IP, TCP/UDP, custom-defined locations, well-known services (registered ports) and applications, allowing customers to build adaptive trust models based on business intent, permissions, and network locations that reduce risk exposure.

CFS Application Monitoring discovers and reports on applications traversing the network, making it simpler to build accept/deny policies more rapidly.

Secure Traffic Across Distributed Locations

Symantec Cloud SWG offers a global footprint built on Google Cloud infrastructure that will scale to any organization's needs. The Universal Policy Enforcement (UPE) capability allows administrators to define protection policies once and distribute them to all of their gateways, whether in the cloud or on-premises. This ensures unified protection and consistent security policies for all users.

Protecting users wherever they are located, whether it's at the company headquarters, a branch office, or remote, the service safeguards the enterprise from cyber threats, controls and secures corporate use of the cloud and the web, prevents data leaks, and ensures compliance with all of the company's information, as well as web and cloud access policies. It offers NGFW capabilities and supports customer-specific firewall policies for both fixed locations and roaming users. It also includes simple security management via the Symantec Enterprise Cloud Portal, as well as centralized reporting.

CFS also extends capabilities that enable organizations to segment security policy and dynamically adjust enforcement as users move in and out of the organization's network. Additionally, CFS can control access based on user and group, via tight integration with the user identity and authentication systems of Symantec SSE.

Symantec SSE delivers the broadest possible range of advanced security services, allowing organizations to consolidate traditional-point products onto a single cloud service. This delivers a lower total cost of ownership while enhancing security effectiveness for all users.

Figure 2: Symantec Secure Access Service Edge (SASE) Framework

