PRODUCT BRIEF

Symantec® Cloud Secure Web Gateway

(Formerly Web Security Service)

AT A GLANCE

Web Access and Threat Protection

- Protect web and cloud app traffic, users, and devices through cloud-delivered security service based on an advanced proxy architecture
- Use innovative web isolation to block threats targeting web browsers
- Use advanced threat intelligence data with risk-level ratings combined with AV scanning and sandboxing to block malware hidden in encrypted traffic
- Prevent non-web threats with Cloud Firewall Service

Data Protection and Cloud Control

- Use Symantec DLP with cloud-based or on-premises management
- Inspect content in SSL encrypted traffic to identify information security violations and ensure data compliance
- Set Cloud Access Security Broker (CASB) policies to control Shadow IT, Shadow Data, and ensure compliant use of cloud applications

Security and Performance for Office 365

- Enforce information protection and threat prevention policies when using Office 365 applications
- Automatic policy updates to align with changes in IP addresses associated with Office 365 infrastructure changes
- Accelerate performance using cloud infrastructure peering with Microsoft

Cloud-delivered Secure Web Gateway

Enterprise's rapid adoption of cloud applications and increasing use of the web is putting pressure on existing network security architectures. Roaming users and new endpoint device types add additional complexity and challenges. Enterprise security teams must grapple with a series of questions against this new backdrop, such as:

- How to protect users, regardless where they are located, from an evolving threat landscape?
- How to ensure data is secure and in compliance with legal regulations?
- How to effectively manage new types of devices and mobile or remote users?
- How to migrate current infrastructure to the cloud without sacrificing functionality or flexibility?

Symantec® Cloud Secure Web Gateway (SWG), a key feature capability for all Symantec Web Protection licensees, answers these questions. It provides the same proactive web protection capabilities delivered by the market's leading Edge Secure Web Gateway (included with the same license) but delivered as a resilient and high-performing cloud security service. Sitting between employees, wherever they are located, and the Internet, the service protects the enterprise from advanced threats, controls and protects corporate use of cloud applications and the web, prevents data leaks, and ensures compliance with all company information and web or cloud access policies.

Symantec Cloud SWG is a multi-tentant cloud capability that delivers web and cloud application security from a diversified network of certified global data centers. Universal Policy Enforcement (UPE) capabilities allow administrators to define protection policies once and distribute them to all of their gateways. Whether they are in the cloud or on-premises, enterprises can ensure consistent protection is in place. Its best-in-class feature set, combined with powerful integrated solution options, enterprise-class network security capabilities, and flexible subscription pricing model, has made our *secure web gateway* the smart choice for companies looking for enterprise-class security capabilities in a cloud-delivered service.

Features and Capabilities

The Symantec Cloud SWG within Symantec Web Protection enforces granular access and security policies that manage web Internet usage by app, device, user, or location. Enterprise-class functionality includes the technology described on the following page.

Features and Capabilities (cont.)

URL Filtering and Categorization

- Process over 6 billion web requests and block millions of web attacks and social engineering scams daily
- Use dynamic, real-time URL risk ratings using real-time global threat intelligence
- Classify URLs into one or more of 72 content categories, 12 security categories (6 blocked by default policy) covering over 60 languages

Advanced Threat Protection

- Multi-layered dual anti-virus and heuristic analysis combines to block malware
- Customized Allow/Deny-List capabilities and file reputation analysis
- Policy customization with Threat Risk Level and Geo IP Location intelligence

Universal Connectivity

- Hyperscale Google Cloud backbone
- Easily connect laptops, mobile devices, firewalls, proxies, and more

Deep File Inspection

- Advanced analysis (static code, YARA rules, behavioral) as well as in-line, real-time file blocking to combat threat
- Sandboxing to detonate suspicious samples; coordinate with our Symantec Cloud SWG to delay file delivery until analysis is complete

Encrypted Traffic Management

- Intercept and decrypt SSL and TLS traffic to uncover threats and potentially malicious content hidden in encrypted traffic.
- Streamline customer PKI management with Self-Managed Certificate

Cloud Firewall Service

- Configure policy to block traffic based any TCP/UDP port
- Set policy (allow/deny) based on authenticated User/Groups, as well as Source or Destination criteria

Web Isolation Service

- Boost employee productivity by allowing protected access to uncategorized or potentially risky sites
- Fine-tune employee access control with customized isolation policies based on Risk Levels
- Secure web browsing for executives and privileged users with access to sensitive information and critical systems

Cloud Access Security Broker (CASB)

- Identify Shadow IT by identifying applications and services in use, evaluating the risk of tens of thousands (30,000+) of unique cloud applications in use by examining hundreds of attributes
- In-line visibility, data security, and threat protection over the use of any cloud application from managed or unmanaged endpoints

Data Loss Prevention (DLP)

- Monitor and protect sensitive data on mobile devices, on-premises, and in the cloud using the most advanced DLP matching and recognition engines on the market
- Extend DLP coverage and get direct visibility and control of content in over 60 cloud apps—including Office 365, Box, Dropbox, Google Apps, and Salesforce

Easy On-Ramp for Branch Office and Mobile Users

- Enable comprehensive multi-layered network-to-endpoint protection with Symantec Endpoint Security, simplifying mobile device app management
- Integrate with leading SD-WAN solutions

Comprehensive Security to Meet Today's Enterprise Realities

Mobile users, remote offices, cloud application adoption, increasing compliance obligations, and an evolving and sophisticated threat environment—the new reality for enterprise IT and Security teams. Symantec Cloud SWG enables enterprise-class capabilities to address these realities and ensure web and cloud use remains efficient, effective, secure, and compliant.

Proven proxy technology is fed by the Symantec Global Intelligence Network, the world's largest civilian threat intelligence network, to ensure real-time protection against known and unknown web-borne threats. With extensive web and cloud application controls, web isolation, malware scanning, data loss prevention, CASB services, and detailed reporting features, the Symantec Cloud SWG capability enables administrators to create and enforce granular policies that are instantly applied to all covered users, regardless where they are located, including fixed locations and roaming users.

Symantec Cloud SWG: A critical, cloud-delivered capability of Symantec Web Protection.

Cloud Secure Web Gateway
SSL Inspection
Edge Secure Web Gateway
Cloud Firewall Service

Web Isolation
Content Analysis and Sandboxing
CASB Controls
Management and Reporting

Symantec Cloud SWG Capabilities

Threat Protection

- Largest Civilian Global Intelligence Network feeding threat information (15K enterprises, 175M users, 3K researchers)
- Default best-practices policies
- Advanced controls based on threat risk levels
- Web Isolation for secure web browsing of uncategorized or risky websites
- Cloud Firewall Service for non-web traffic
- Content analysis using AV scanning and sandboxing (with IoC results)*

Acceptable Use Controls

- URL filtering through granular policies (by user, group, location, and more)
- Web application blocking
- Cloud Access Security Broker (CASB) discovery and reporting*

Data Loss Prevention

- Integration with Symantec DLP Cloud*
- Integration with on-premises configured Symantec DLP policies for native scanning in the cloud.*

Reporting and Visualization

- Customizable dashboards with drill-down information
- Preconfigured and custom reporting
- Scheduled reporting and triggered alerts with e-mail delivery

SECURITY AND PERFORMANCE FOR OFFICE 365 USERS

Traditional network architecture has been drastically altered as enterprises move to cloud applications like Office 365. Traditionally, traffic from remote sites and mobile users connects through corporate data centers to access applications and utilizes security infrastructure to access the web. This security architecture can add latency and increase costs as organizations move to Office 365.

Enterprises can rely on the Symantec Cloud SWG capabilities within Symantec Web Protection to move their entire network security stack to the cloud—enabling direct, secure connectivity to cloud and SaaS applications like Office 365, benefiting from faster security and network architectures at a lower cost. The service can enforce a full set of controls when accessing Office 365, including scanning for malware and threats within Office 365 traffic as well as inspecting encrypted traffic for data leaks and information security compliance violations.

The Symantec Global Intelligence Network feeds Symantec Cloud SWG to ensure that any updates made to the infrastructure for Office 365 applications—such as changes to IP Addresses—get automatically aligned in an enterprise's Office 365 security policies, resulting in consistent policy enforcement for our customers. Additionally, advanced content peering and Transmission Control Protocol (TCP) connection acceleration reduce data hops and boosts throughputs, offering customers increased performance and enhanced user experience.

Symantec Cloud SWG Capabilities (cont.)

Controls on SWG Logging

- Control data removal by restrictions on Authorization Level or location
- Configurable data retention period (2 to 365 days)*

Authentication

- Leverage Windows Active Directory (AD) without requiring changes
- Support for SAML v2 (Post and Redirect bindings)

Encrypted Traffic Inspection

- Compliant practices for SSL and TLS encrypted traffic interception, decryption and inspection
- Employs Secure CA, with Symantec PKI hosted Root and Intermediate CAs, or customer-provided PKI
- Server Certificate Authority validation with revocation checking

Connection Methods

- Secure traffic redirection through Symantec Endpoint
- Unsecured proxy access
- IPSec connection (PSK and Certificate methods)
- Hardened Agent (Windows and Mac OS)*

Cloud Infrastructure

- All global data centers available to enterprise users
- Regional data center available for reporting
- ISO27001 and SSAE-16 SOC3 certifications

Connection Methods		
IPSec VPN (Site to Site): Most IPSec-capable Juniper, Cisco, Palo Alto, Fortinet, and Checkpoint firewalls*		
Proxy Chaining from Symantec Edge SWG and other proxy devices		
Explicit Proxy		
Symantec Endpoint Protection (SEP): SEP 14 (14.1 RU1 MP1) or later		
Symantec Endpoint Protection Mobile (SEP Mobile): iOS mobile devices		
SD-WAN Technology Partnership: Certified inter-operable partnerships with third-party SD-WAN solution providers		
Desktop Connector	WSS Agent Operating Systems: • 64-bit Windows 10 Professional, Enterprise or Education version 1703 or later • macOS 10.15 High Sierra or later	Minimum Hardware Requirements: • Must meet minimum hardware requirements for specific operating system • X86 or x86-64 compatible processor • 100 MB of available hard disk space for software installation and logging • High-speed Internet connection
Supported Authentication Services		
Active Directory	Operating Systems: • Windows 2003 SP2 or later • Windows 2008 SP2 or later	Minimum Hardware Requirements: • Must meet minimum hardware requirements for Windows 2003 SP2 and later • X86 or x86-64 compatible processor • 100 MB of available hard disk space for software installation and logging • High-speed Internet connection

*License-dependent options to configuration.
**Refer to the Deployment Guide for details.

Symantec™ by Broadcom Software

About Broadcom® Software

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software is building a comprehensive portfolio of industry-leading infrastructure and security software, including AIOps, Cyber Security, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

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

SED-WSS-PB103 January 19, 2023