Symantec Web Security Service

At A Glance

Web Security and Threat Protection

- Protect internet traffic, users, and devices via cloud-delivered security service using the market's leading Secure Web Gateway
- Set granular policies to manage web internet usage by app, device, user or location
- Use powerful web threat intelligence data combined with advanced malware scanning
- Leverage state-of-the-art sandboxing to address zero day threats

Data Protection & Cloud Control

- Use cloud-based or on-premise DLP options
- Inspect SSL encrypted traffic to ensure compliance and security
- Set Cloud Access Security Broker (CASB) policies to control Shadow IT, Shadow Data and manage cloud compliance

Management, Visibility & Reporting

- Define consistent policies once and distribute to cloud and on-premise gateways for enforcement
- Access centralized visibility and reporting across cloud and on-premise gateways
- Monitor internet usage, threats, incidents, etc. by user, location, and application in real-time

Secure Web Gateway as a Service

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

- How do we protect our users from an evolving threat landscape?
- How can we make sure our data is secured and maintains compliance with legal regulations?
- How do we effectively manage new types of devices and our mobile/remote users?
- How can we transition our own infrastructure to cloud without sacrificing functionality or flexibility?

The Symantec Web Security Service is designed to answer these questions. It provides the same proactive web protection capabilities delivered by the market's leading on-premises Secure Web Gateway, the Blue Coat ProxySG, but delivered as a resilient and performant cloud security service. Sitting between your employees, wherever they are located, and the Internet, the service protects your enterprise from cyber threats, controls and protects corporate use of the cloud and the web, prevents data leaks, and ensures compliance with all of your company's information and web/cloud access policies.

Web Security Service delivers web and cloud security from a diversified network of certified global datacenters. Since the Universal Policy Enforcement (UPE) capability allows 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 and flexible subscription pricing model, have made Web Security Service the smart choice for companies looking for enterprise-class security capabilities in a cloud-delivered service.

Symantec

Core Capabilities

The Symantec Web Security Service enforces granular access and security policies that manage web internet usage by app, device, user or location. Enterprise-class functionality includes:

URL Filtering and Categorization

- Leverage 9 security categories to block 90% of all threats
- Unique URL Threat Risk Score to increase security without over-blocking
- Classify URLs in one of 70 categories covering over 50 languages
- Dynamic, real time ratings for the latest information

User Authentication

- ID users with multiple authentication methods
- Integrate across multiple auth systems used by your enterprise

Advanced Threat Protection

- Multi-layered dual anti-virus and heuristic analysis combines to block malware
- Utilize customized White-List/Black-List capabilities and file reputation analysis

Universal Connectivity

- Distributed global datacenters provide local cloud access
- Easily connect laptops, mobile devices, firewalls, proxies and more

Optional Capabilities

Symantec has integrated the Web Security Service with other products in its broad security portfolio. These additional solutions include:

Malware Analysis Service

- Add powerful inspection capabilities to filter up to 99% of potential malware before delivery while minimizing false positives
- Leverage advanced analysis (static code, YARA rules, behavioral) as well as inline, real-time file blocking to combat threats
- Utilize sandboxing to detonate suspicious samples; coordinate with Web Security Service to delay file delivery until analysis is complete

Cloud Access Security Broker (CASB)

- Identify Shadow IT – identify the clouds your users are accessing; evaluate the risks of these clouds (over 18,000) by examining up to 90 attributes on each
- Set access and control policies based on cloud attribute data in order to manage risk, address threats and protect information

Data Loss Prevention (DLP)

- Monitor and protect sensitive data on mobile devices, on-premise, and in the cloud using the most advanced DLP matching and recognition engines on the market
- Extend your DLP coverage and get direct visibility and control of content in over 60 cloud apps - including Office 365, Box, Dropbox, Google Apps or Salesforce
- Already have on-premise DLP? Extend the value & ROI of your DLP investment. Use the Symantec Cloud to Premises Connection technology to use your existing DLP infrastructure and policies to protect your data

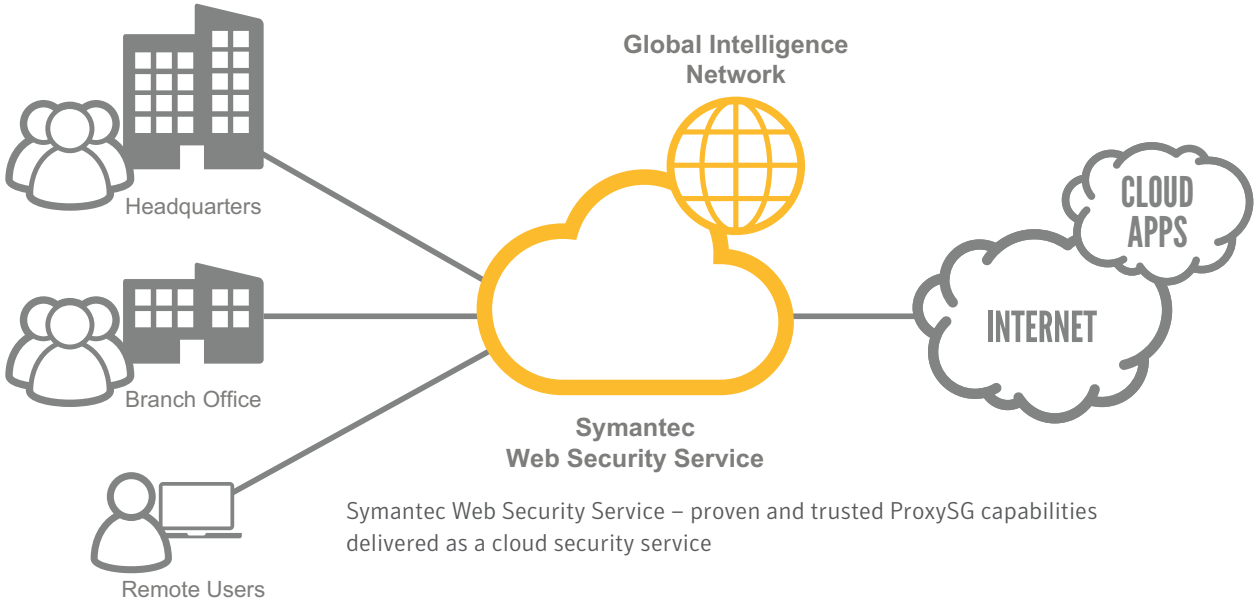
Strength in Numbers – Symantec Global Intelligence Network

The Symantec Web Security Service taps into the Symantec Global Intelligence Network, one of the world's premier civilian cyber defense threat intelligence services. Fed by threat information from 15,000 enterprises, 175 million consumer and enterprise endpoints, and 3,000 threat researchers and engineers, the solution categorizes and analyzes the threats posed by over a billion previously unseen and uncategorized websites each day and over 2 billion daily emails sent/received by our customers. Symantec's unique expertise minimizes false positives and you benefit from the network effect of joining over 90% of the Fortune 500 as a Symantec customer, giving you access to the world's most powerful analytical threat engine that will keep you a step ahead of fast-changing security threats.

Web Security Service for 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's Web Security Service gives you the enterprise-class capabilities to address these realities and ensure your web and cloud use remains efficient, effective, secure and compliant.

Its proven proxy technology leverages the Symantec Global Intelligence Network to ensure real-time protection against known and unknown web-borne threats. With extensive web and cloud application controls, malware scanning, data loss prevention, CASB services and detailed reporting features, the Web Security Service enables administrators to create and enforce granular policies that are instantly applied to all covered users, including fixed locations and roaming users.



Symantec Web Security Service – proven and trusted ProxySG capabilities delivered as a cloud security service

Symantec Web Security Service Capabilities

Threat Protection
- Largest Civilian Global Intelligence Network feeding threat information (15K enterprises, 175M users, 3K researchers)
- Default best-practices policies
- Dual AV engines
- Sandboxing for real-time file analysis
- Background deep analysis with IoC results*

Acceptable Use Controls
- URL filtering via granular policies (by user, group, location, etc.)
- Web application blocking
- Cloud Access Security Broker (CASB) discovery and controls*

Data Loss Prevention
- Integration with Symantec DLP Cloud*
- Integration with 3rd party DLP, including on-premise DLP software*

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

Controls on SWG Logging
- Control data removal by restrictions on Authorization Level or location
- Configurable data retention period (2-365 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/TLS encrypted traffic interception, decryption and inspection
- Employs Secure CA, with Symantec PKI hosted Root and Intermediate CAs
- Server Certificate Authority validation with revocation checking

Connection Methods
- Secure connection method
- Unsecured proxy access
- IPsec connection (PSK and Certificate methods)
- Hardened Agent (Windows and MacOS)*

Cloud Infrastructure
- All global datacenters available to enterprise users
- Regional datacenter available for reporting
- ISO27001 and SSAE-16 SOC3 certifications

License dependent options to configuration

Connection Methods		
IPSec VPN (Site to Site) – most IPSec-capable Juniper, Cisco, Palo Alto, Fortinet and Checkpoint firewalls*		
Proxy Chaining – from ProxySG and other proxy devices		
Explicit Proxy		
Desktop Connector	**Unified-Agent Connector Operating Systems (optional)** • Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8 (32-bit and 64-bit) • Microsoft Windows 10 • Apple Macintosh › OS X 10.7+	**Unified Agent Minimum Hardware Requirements** • Must meet minimum hardware requirements for Windows 7 and later or Macintosh OS X 10.7 and later • X86 or x86-64 compatible processor • 100MB of available hard disk space for software installation and logging • High speed internet connection

*Refer to the Deployment Guide for details

Supported Authentication Services		
Active Directory	**Operating Systems** • 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 • 100MB of available hard disk space for software installation and logging • High speed internet connection

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Copyright © 2017 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners. # DS-SYM-Web-Security-Service-0217-v2f