DATA SHEET

Web Security Service

At A Glance

Web Security and Threat Protection

- Protect web and cloud app traffic, users, and devices via 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
- Simplified connection options including SEP agent and SD-Cloud Connector (SD-WAN)

Data Protection & Cloud Control

- Use cloud-based or on-premise DLP options
- 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 and ensure compliant use of cloud applications

Security & Performance for O365

- Enforce information protection and threat prevention policies when using O365 applications
- Automatic policy updates to align with changes in IP addresses associated with O365 infrastructure changes
- Accelerate performance using cloud infrastructure peering with Microsoft

Network Security as a Service

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 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, regardless where they are located, from an evolving threat landscape?
- How can we make sure our data is secure and maintains compliance with legal regulations?
- How do we effectively manage new types of devices and our mobile/remote users?
- How can we migrate our current infrastructure to the cloud without sacrificing functionality or flexibility?

Symantec Web Security Service, being a key component in Symantec's Integrated Cyber Defense, answers these questions. It provides the same proactive web protection capabilities delivered by the market's leading on-premises Secure Web Gateway, the Symantec 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 cloud applications 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) 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, have made Web Security Service the smart choice for companies looking for enterprise-class security capabilities in a cloud-delivered service.

Features and 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

- Processes over 6 billion web requests and blocks 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
- Utilize customized White-List/Black-List capabilities and file reputation analysis
- Customize policies with Threat Risk Level and Geo IP Location intelligence

Universal Connectivity

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

Malware Analysis Service

- Leverage advanced analysis (static code, YARA rules, behavioral) as well as inline, real-time file blocking to combat threat
- Utilize sandboxing to detonate suspicious samples; coordinate with Web Security Service to delay file delivery until analysis is complete

Encrypted Traffic Management

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

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; or leverage your existing on-premises DLP for your web/cloud traffic
- 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

Easy On-Ramp for Branch Office & Mobile Users

- Connect remote/branch office to Web Security Service with SD-Cloud Connector leveraging the performance and flexibility of Software Defined WAN (SD-WAN) technology
- Enable comprehensive multi-layered network-to-endpoint protection with Symantec Endpoint Protection (SEP) and SEP Mobile integration, simplifying mobile device app management

Security and Performance for Office 365 Users

The traditional network architecture has been drastically altered as enterprises move to cloud applications like Office 365. Traditionally, traffic from remote sites and mobile users connected 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 leverage Symantec's Web Security Service 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.

Symantec's Global Intelligence Network feeds the Web Security Service 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.

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'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, 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 Web Security Service 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 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
- Advanced controls based on threat risk levels
- Web Isolation for secure web browsing of uncategorized or risky websites
- Content analysis using AV scanning and sandboxing (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 reporting*

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, or customer-provided PKI
- Server Certificate Authority validation with revocation checking

Connection Methods
- Secure traffic redirection via SEP, SEP Mobile or Unified Agent for remote/mobile users
- Secure SD-WAN based branch office connection via SD-Cloud Connector
- Unsecured proxy access
- IPsec connection (PSK and Certificate methods)
- Hardened Agent (Windows® and Mac® OS)*

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

Connection Methods
SD-Cloud Connector - Based on SD-WAN technology, the Symantec SD-Cloud Connector provides connectivity from HQ, branch and remote offices to the Web Security Service
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
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 (please visit **https://www.symantec.com/integration** and click on the SD-WAN box for more partner integration details)

Desktop Connector	Unified-Agent Connector Operating Systems (optional)	Unified Agent Minimum Hardware Requirements
	• Microsoft® Windows® 7 (32-bit and 64-bit) • Microsoft Windows 8 (32-bit and 64-bit) • Mac® OS X 10.7+	• 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

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 • 100MB 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

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

Copyright © 2018 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

20A246851_ds_Web_Security_Service_EN