Web Security Service

Cloud-Delivered Advanced Network Security Service

Increasing web use, rapid cloud adoption, greater mobility, and a growing number of remote users expose your network to risk. Symantec Web Security Service is a leading cloud-delivered security service that controls web access, protects users from threats, and secures their data.

This document summarizes key areas of competitive differentiation for the service. Please contact your Symantec Sales Representative to explore each of these areas, and more, in detail.

Analyst Recognitions by Gartner & Radicati

Symantec’s Web Security Service (WSS) and ProxySG Secure Web Gateway technology has been recognized and ranked highly by both Gartner and Radicati. Gartner has nominated Symantec’s Secure Web Gateway in its Magic Quadrant’s “Leader Quadrant” for 11 times in a row, while Radicati continues to place Symantec as the leader in the Top Players quadrant of its Market Quadrant report. These achievements are due to Symantec’s continuous effort in improving and expanding the capabilities of its SWG technology. For example, Symantec is continuously improving our SWG technology by enhancing its Global Intelligence Network, integration with Content Analysis, Malware Analysis, SSL Visibility, and DLP technologies. Additional enhancements with new technologies such as CASB, Web Isolation and Secure Access Cloud with application level controls are providing more layers of protection to our users.

Our competitor while offers effective cloud-based security technologies, it lacks some advanced new security technologies such as CASB and Web Isolation; and is also experiencing scalability and performance challenges in demanding enterprise environment.

Superior threat prevention including innovative web isolation capabilities

A core capability of the Symantec service is enforcing security policies based on detailed data and predictive threat intelligence. Symantec offers the market’s best enterprise-grade threat prevention security service, which includes a granular URL classification engine, an accurate detection engine, data feeds from the world’s largest civilian threat intelligence network, and dual antivirus scanning. The proof is in the results: A third-party testing organization found that compared to using the service of our primary cloud-delivered competitor, a typical enterprise using the Web Security Service would experience a dramatic reduction in false-positives while benefiting from superior protection (e.g. more malware attacks being blocked). Additional threat prevention options include threat prevention based on Risk Levels & Geo IP, cloud-based sandboxing and web isolation with Risk Levels, an innovative technology that blocks sophisticated malware, phishing, and ransomware targeting user web browsing activity. Our primary competitor does not offer this critical advanced threat prevention technology.

Superior SSL/TLS inspection functionality

Analyst firm Gartner, Inc. estimates that 80 percent of a typical enterprise’s traffic will be encrypted by 2019, and over half of cyber attacks will target ‘blind spots’ created by encryption. This means the ability to securely inspect encrypted traffic is essential to protecting an organization. Symantec supports 40 cipher suites, broad support that enabled Symantec to receive the only ‘A’ grade in a recent third-party analysis that assessed the ability of various SSL
Inspection solutions to securely inspect encrypted traffic. In contrast, our primary cloud competitor offers support for only 17 cipher suites. Although this competitor supports for the popular ECDHE_RSA cipher, analysis shows their service is configured to deprecate (downgrade) the cipher used to access web sites requesting the use of ECDHE_RSA to secure the web session. Enterprises need to understand this process, since it can expose their business to security vulnerabilities.

In addition, Symantec offers more flexibility and streamlined PKI management which customers can choose either Symantec-provided encryption certificates or customer-provided, Self-Managed Certificates that are generated by customer’s own HSM system hosted by AWS.

Market-leading CASB capabilities

Analyst firms Gartner and Forrester Research both recognize the Symantec Cloud Access Security Broker (CASB) offering, CloudSOC, as an industry leader. Web Security Service uses CloudSOC—with its database of over 23,000 cloud applications—to identify cloud use (including ‘shadow IT’) and set policies to control employees’ use of cloud applications. Our primary cloud competitor does not have its own CASB offering and instead offers limited integrations with McAfee and Microsoft.

Market-leading data loss prevention (DLP) service

Gartner and Forrester also recognize Symantec Data Loss Prevention as the market’s leading DLP solution. Web Security Service can deliver this complete DLP solution via the cloud or on-premises through our innovative Web Security Service and Data Loss Prevention integration. Our primary competitor, in contrast, offers a limited DLP solution based on simple regex rules. Most enterprises need much more than simple ‘credit card detection-type’ rules to accurately detect and enforce information security policies. Our competitor’s website offers no independent third-party comparative analysis of their DLP capabilities.

Simple Application-Level Zero Trust Access Security with Secure Access Cloud

Symantec’s recent acquisition and planned integration of Secure Access Cloud technology from Luminate plays an important role in our offering of a secure access technology for a Zero Trust environment. This Zero Trust and Software-Defined Perimeter (SDP) technology, combined with the values of the of the Symantec Integrated Cyber Defense platform, secures access at the application layer through a simple, agent-less deployment enabling Symantec to offer a more comprehensive coverage for the enterprise. The Secure Access Cloud technology provides a highly efficient, scalable, and flexible solution that offers authentication, control, and security for the data paths to all destinations. This is great news for Symantec’s customers, as they now have a one-stop-shop for an Integrated Cyber Defense Platform that is built for today’s more advanced and dynamic network environment.

In comparison, our competitor’s private access offering stays at the network-level, lacking the simplicity and the level of granular controls of Symantec’s Secure Access Control solution.
Security for Office 365

Many cloud security vendors, including our primary competitor, do not provide deep security policy enforcement on Office 365 traffic because they cannot maintain performance while securing traffic. Symantec is different. We have partnered with Microsoft to optimize our cloud security network to secure Office 365 traffic. Web Security Service protects Office 365 in everything from simply authenticating and logging Office 365 access for compliance and audit requirements to inspecting encrypted traffic (such as files going back and forth from OneDrive) for malware/ransomware or data loss prevention policy violations. Additionally, we have built our globally distributed cloud network with performance optimization technologies—such as content peering with Microsoft and TCP window scaling—that ensure optimal customer experience.

Symantec Endpoint Protection (SEP) and Endpoint Protection Mobile (SEP Mobile) Integration

SEP, positioned by Gartner, Inc. in the Leaders quadrant of their “Magic Quadrant for Endpoint Protection Platforms” since its inception in 2002, and SEP Mobile can be configured to send web traffic directly to the Web Security Service for enforcement of network-based security policies. As a result of this integration, enterprises can use a single endpoint agent to implement a comprehensive defense-in-depth security strategy, with complete protection deployed across the endpoint and the network. Enterprises using SEP and SEP Mobile do not need to deploy and manage a separate Web Security Service agent on their endpoints, reducing IT cost and complexity.

SD-WAN connectivity for branch and remote offices

Secure remote and branch office with WSS is quick and simple using the SD-Cloud Connector. Implementing the optional Symantec SD-Cloud Connector in branch or remote locations provides fast and reliable connectivity to the Symantec Web Security Service cloud, as well as local firewall and network bandwidth control capabilities.

Strong SD-WAN Partnership Ecosystem

Symantec not only offers a more comprehensive Integrated Cyber Defense Platform, we have also built a large security protection ecosystem with our key partners and industry leaders. Symantec established a Software-Defined-Wide-Area-Network (SD-WAN) ecosystem program offering a broad coverage in partnership with the industry’s leading SD-WAN technology providers for its Web Security Service.

SD-WAN technology provides the flexibility and performance required for today’s demanding new business environment. The SD-WAN solutions offered by members of this partnership ecosystem are fully certified with the Symantec Web Security Service. These fully tested and fully certified solutions eliminate the potential complexity and complications of product integration, providing a simple turn-key solution for redirecting web traffic to Web Security Service for enforcing consistent security policies and corporate policy compliance. Members of the SD-WAN Partnership Program includes well recognized industry names such as VMware (VeloCloud), CloudGenix, Cisco (Viptela), Silver Peak, Cradlepoint, Versa Networks, Meta Networks, Citrix, Aryaka, InfoVista, and TALARI Networks.

To get the latest update on partners in the Symantec SD-WAN Partnership Ecosystem Program, please visit the Symantec TIP Program Certified Partner Solutions website.
Cloud adoption at your own pace with hybrid deployment options

The full Symantec portfolio of Secure Web Gateway solutions range from physical/virtual appliances to a complete cloud-based SaaS service (Web Security Service). Whether an enterprise runs its applications purely in the cloud or on a hybrid mix of cloud and on-premises, it can centrally manage security and threat prevention policies using the Symantec Universal Policy Enforcement capability. Our primary competitor is cloud-only, it does not offer a high-performance on-premises option and cannot support an enterprise-class hybrid model.

Integrated Cyber Defense

Symantec not only provides protection for Web and Endpoint, our Integrated Cyber Defense (ICD) platform unifies products, services, and partners to reduce cost and complexity of cyber security, while increase the effectiveness of protecting enterprises against sophisticated threats. ICD combines information protection, threat protection, identity management, compliance, and other advanced services, powered by shared intelligence and automation across endpoints, networks, applications, and clouds.

<table>
<thead>
<tr>
<th>Capabilities</th>
<th>Competitor</th>
<th>Symantec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud App Data &amp; Controls (CASB)</td>
<td>Partnerships</td>
<td>23K</td>
</tr>
<tr>
<td>Data Loss Prevention (DLP)</td>
<td>No published reviews</td>
<td>Forrester Wave and Gartner MQ Leader</td>
</tr>
<tr>
<td>Threat Intelligence with Risk Level &amp; Geo IP</td>
<td>Below average</td>
<td>Above average</td>
</tr>
<tr>
<td>Granular Policy Settings</td>
<td>Limited</td>
<td>Detailed</td>
</tr>
<tr>
<td>Predictive File Analysis</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Web Isolation with Risk Level</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allowing Customer-Provided PKI</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Global Datacenters with Peering</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrated with Endpoint Security</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SD-WAN</td>
<td>Partners</td>
<td>Symantec &amp; Partners</td>
</tr>
<tr>
<td>Hybrid Deployment Support</td>
<td>Limited</td>
<td>Full, with ability to centrally manage policies for all gateways</td>
</tr>
</tbody>
</table>