Solution Guide

Symantec Web Security Service

Advanced Cloud-Delivered Network Security for the Cloud Generation.

Today's enterprise-security reality: Devices, data, and applications are outside of your physical control—and all of it must be managed and secured

Cloud apps   Mobile devices   Remote users

Symantec™

Solution Guide

Introduction
A perfect storm of security challenges

Section

00

The traditional approach to enterprise security has been rendered obsolete by a perfect storm of mobile users, remote offices, cloud apps, compliance obligations, and evolving security threats.

With employees wanting to access apps and data directly from the Internet, legacy security solutions—which require traffic to be routed back through the enterprise datacenter to enforce security and data compliance policies—are no longer effective.

Today, network operation and security teams need answers to these questions:

- How do we simplify our network security and reduce the amount of Internet traffic we are back-hauling?
- How can we improve the performance of our solution?
- How do we protect users from new/evolving threats from the web and the cloud?
- How do we secure data and maintain compliance with increasingly strict regulations?
- How do we effectively manage remote access, mobile users, and unsanctioned devices?

The new reality of enterprise network security calls for a comprehensive cloud-delivered security solution with advanced capabilities that enforces consistent threat protection and information security policies for all of your users wherever they are.

Solution Guide

Rethinking the role of the Secure Web Gateway in the security stack

Section

01

Many organizations rely on secure web gateways (SWGs) to perform the basics of URL filtering and to enforce permissible-use policies for the web and cloud. Due to their role in expediting the flow of data to web and cloud apps—and their unique ability to scan and orchestrate encrypted traffic—SWGs are uniquely becoming the core of your full network security stack. Beyond the core functions of traditional SWGs, a proxy-led solution can be expanded to secure all Internet traffic (not only web traffic), delivering data-loss prevention (DLP) scanning, advanced threat and malware protection, and powerful application controls for cloud apps.

When selecting a cloud-based SWG solution to address security and compliance challenges, it's essential to find an advanced solution that provides the flexibility to address a range of critical security and compliance challenges. Look for a secure web gateway that not only can effectively categorize/filter your web traffic and enforce your acceptable use police, but can also:

- Detect and prevent advanced threats while keeping false positives to a minimum
- Isolate web browsing sessions to prevent threats and phishing attacks
- Orchestrate encrypted traffic to DLP solutions, either on-premises or in the cloud
- Provide cloud app-security, known as CASB controls, that offers the ability to identify and manage the use of unsanctioned SaaS applications, known as shadow IT
- Block cloud email-based threats and eliminate leakage of sensitive data
- Offers a broad range of simple connectivity options as "on-ramps" to the service, including SD-WAN based approaches
- Extend threat protection all the way to the endpoint laptop and mobile devices
- Enforce consistent security policies across on-premises and cloud-enabled gateways

Solution Guide

Symantec Web Security Service: Built for the cloud generation

Section

02

Enterprise-grade security for wherever data resides or users roam

Symantec Web Security Service is a comprehensive cloud-delivered network security service based on an advanced proxy architecture that provides superior security for your data, apps and users – wherever they are. Protection from advanced threats, compliance for sensitive information, and controls enabling secure and compliant cloud application use – all delivered from a resilient, high performance globally distributed cloud network infrastructure.

Web Security Service Capabilities

Web URL filtering and categorization

The service accurately filters traffic into nine content-type categories to enable you to reduce the risk of web browsing without over-blocking access. You can set policies across 84 categories covering 60+ languages.

SSL inspection

SSL inspection has become an imperative for many enterprises. With nearly 75% of Internet traffic estimated to be encrypted, it's critical to decrypt and orchestrate traffic to security inspection engines such as DLP (which prevents data exfiltration and compliance violations) or content and malware analysis (which prevents attacks and blocks advanced threats).

The Symantec Web Security Service can be configured to intercept, decrypt, and hand off web and cloud traffic to DLP or Advanced Threat Prevention services for identification of policy violations and blocking of cyber threats. The service offers:

- Support for 40 cipher suites, allowing for broad website coverage to decrypt, inspect, and strongly re-encrypt SSL traffic after inspection. Symantec recently received an "A" rating in a third-party study that looked specifically at these capabilities.[1]
- The ability to set privacy rules to leave certain categories of traffic encrypted (e.g. you may choose to leave HR-related traffic encrypted).
- Streamline PKI management by allowing for customer-provided PKI and self-managed certificates.

Symantec's Global Intelligence Network
the world's largest civilian threat-intelligence system

80 Million
Web Proxy Users

180 Million
Endpoints

165 Million
Email Users

Threat/malware protection - content analysis & virus scanning

It's more important than ever to protect your users from the threats and impact of malware. Symantec combines real-time global web ecosystem analysis with inline malware detection to block malicious sites, malware-prone file types, and "phone-home" or botnet traffic. To prevent malware, the service uses multi-layered dual anti-virus and heuristic analysis, and file-reputation analysis. It also lets you scale up or down as your needs dictate to deliver real-time malware protection in the cloud.

In addition, you can set security policies based on Threat Risk Level and Geo IP Location intelligence, delivered by the Global Intelligence Network, to ensure extended web access without compromising security.

Threat/malware protection - cloud sandboxing

Malware analysis cloud-sandboxing service creates a multi-tiered line of defense to protect all enterprise endpoints, including mobile and remote users connecting directly to the Internet.

Symantec's solution supports a wide range of file types and, because the service scans upstream to your devices, it prevents malware and threats from reaching your network. The service detonates suspicious files, performs behavioral analysis to stop advanced threats, and provides:

- Powerful inspection capabilities that filter up to 99% of potential malware before delivery while minimizing false positives
- Visibility into (and blocking of) unknown and zero-day threats
- Dual detonation (virtual and/or emulation) with the ability to interact with malware
- Broad file type support
- Behavioral and static (YARA) analysis and risk-scoring

Threat/malware protection - web isolation

To avoid malware, some enterprises set web access policies to block access to sites with limited reputational history. These sites frequently do not have a category assignment (e.g. news, gambling, etc.) or a definitive risk analysis. But many times, employees have a legitimate business need to get to these web properties, causing some organizations to permit access in order not to impede their employees' ability to perform business activities.

Web isolation solves the challenge of providing secured access to the uncategorized and potentially risky websites. By creating a secure execution environment between users and the web—and sending only a safe visual stream to the users' browsers—web isolation helps eliminate web-borne threats from ever reaching their target machines.

Symantec's threat isolation solution:

- Allows protected access to uncategorized or potentially risky websites (using policies based on Risk-Levels)
- Increases business productivity by giving employees access to a broader set of websites
- Provides secure web browsing for executives and privileged users whose access to sensitive documents and systems makes them highly prized targets for cybercriminals
- Prevents users from disclosing corporate credentials to malicious websites.

Global Intelligence Network

Symantec's Global Intelligence Network—the world's largest civilian threat-intelligence system—is a powerful ally in your battle against malware and other cyber threats. Fed by threat data from 80 million web proxy users, 180 million endpoints, and 165 million end users, the network categorizes and analyzes threats posed by more than 1 billion previously unseen and uncategorized websites each day and more than 2 billion daily emails sent and received by our customers.

Protection extended to the endpoint

Symantec has integrated the Web Security Service with its award-winning Symantec Endpoint Protection (SEP) and Endpoint Protection Mobile (SEP Mobile) solutions, which delivers advanced endpoint security with prevention, detection, response, deception and adaptation in a single agent. So rather than deploying a dedicated agent on devices to route traffic to the Web Security Service, you can configure SEP and SEP Mobile send all Internet traffic from your devices to the Web Security Service. This solution makes it simple to add the service's advanced network protection to the industry's leading solution for protecting your users' laptops and mobile devices (including Apple iOS devices). Now, you can offer all of your users a full-time, layered endpoint and network defense system that protects them with consistent protection wherever they are located. The solution provides:

- Simple Web Security Service connectivity for network-connected or roaming SEP- and SEP Mobile-protected devices
- A comprehensive endpoint solution delivering prevention, EDR, deception, and hardening
- A single agent that combines layered endpoint and network defenses for your users

Unified policy management: cloud and on-premises

Symantec is uniquely positioned to help organizations move to the cloud. It offers the industry's broadest portfolio of secure web gateways, with options designed to meet any requirement—from private to public, physical, virtual, or cloud. Best of all, Symantec's Universal Policy Enforcement allows you to take existing on-premises policies and designate them to move to Symantec's cloud-delivered Web Security Service. If you need to create new policies, you can write them once and push them to all of your Symantec gateways for consistent enforcement, whether they are in the cloud or on-premises.

Our cloud and on-premises policy management solution enables you to:

- Simplify your organization's transition to cloud-based security
- Create and manage consistent policies across all your Symantec gateways
- Support your existing investment in policy creation
- Avoid the complexity of creating and managing policies in a mixed-vendor stack

Cloud Access Security Broker (CASB)

You likely have not been able to stop unsanctioned clouds—so-called "shadow IT"—from making their way into your enterprise. Fact is, they're already there. Our latest analysis shows that more than 900 unsanctioned applications exist in the typical enterprise.

Shadow IT adds to your security and compliance risks. Symantec's CASB Audit module includes discrete attribute data from more than 23,000 apps. Seamless integration between the Web Security Service and CASB Audit automates the process of analyzing your proxy logs to reveal risks of shadow IT, helping you to:

- Identify the clouds your users are accessing
- Evaluate the risks of these clouds by examining more than 90 attributes on each
- Set access and control policies based on cloud attribute data

Symantec's CASB solution, known as CloudSOC, has a rich set of capabilities beyond shadow IT control. It offers an additional set of access control and DLP capabilities that are integral to maintaining control and compliance in SaaS cloud apps. Additionally, CloudSOC's specialized threat-prevention utilizes user-behavior analytics to identify risks of compromised cloud credentials such as IDs and passwords.

Information protection (DLP)

Good news: If you're moving to the cloud for security to support mobile and remote users, you can stay in the cloud to enforce your data protection policies using Symantec's Cloud DLP. The integrated solution takes advantage of Web Security Service's capacity to decrypt SSL traffic and send it to the Symantec DLP Cloud for accurate and fast analysis. The solution also allows for offline scanning of accounts in applications such as Box and Dropbox in order to catch anything your employees may have put into corporate accounts (intentionally or inadvertently).

Want to use your existing DLP? With Symantec, you can. Leverage your investment —including all the time you have spent fine-tuning your policy rules—and extend its reach to the web, cloud, and mobile traffic. We've made it easy to configure Symantec Web Security Service to route specific types of traffic to your existing on-premises DLP for scanning.

The integrated service supports regulatory compliance and data protection by:

- Applying your privacy and data-protection policies to all your web traffic, including traffic for mobile and remote users
- Ensuring SSL encrypted traffic that needs to be inspected can be accurately analyzed
- Continuously monitoring and auditing uploaded files
- Automatically enforcing policy controls to sensitive data
- Alerting admin and data owners when information is put at risk

Cloud email security

Now, more than ever, you need protection from advanced phishing attacks and relief from spam. Because email comes over SMTP—which is a different channel from most Internet activity—it requires different threat-prevention and data protection capabilities. When emails contain file attachments or clickable URLs, your security program should scan them with advanced malware-detection engines and inspect them in sandboxes.

Symantec Email Security.cloud:

- Stops new and sophisticated email threats such as business email compromise and ransomware with multi-layered detection technologies including advanced heuristics, deep link evaluation, and cloud-based sandboxing
- Offers strong protection against spear phishing by using deep-link evaluation to stop malicious links before an email is delivered and when they are clicked on by users (to protect against email weaponized after delivery)
- Protects sensitive data and helps address legal and compliance requirements with granular DLP policies for your cloud-based email

Bandwidth and performance control

Some cloud applications, such as Office 365, create performance issues that can complicate adoption. For example, a typical user of MS Exchange Online will maintain six or more concurrent Internet connections, and an organization with 3,500 users on Exchange Online likely will require an additional 200MB of Internet bandwidth. This type of scenario can be addressed with bandwidth-control capabilities that reserve bandwidth for critical applications such as Office 365 and limiting disruptive recreational traffic to sites such as YouTube or Facebook. Powered by our Global Intelligence Network, Symantec Bandwidth Control accurately identifies cloud, business and mobile applications flows and allows you to prioritize business-relevant applications over recreational content.

Connectivity Options

With a vast network of distributed global data centers providing cloud access, you'll have the freedom to connect laptops, mobile devices, firewalls, proxies, and more to your local points of presence. Getting started is as easy as making a configuration change on your firewall or proxy, or a lightweight adjustment on your end-users' devices. Regardless of the method, all user access to the Web Security Service is encrypted.

Symantec connectivity options include:

- The ability to connect your branch offices to the cloud by simply forwarding traffic through IPSec tunnels
- Quick and simple connectivity of remote offices to the Symantec Web Security Service via SD-Cloud Connector, a simple to deploy, highly resilient connectivity option based on SD-WAN technology
- If you are using Symantec Endpoint Protection, a simple configuration update is all that is required to automatically route Internet traffic to the Web Security Service.
- Proxy chaining or proxy forwarding to send traffic from existing proxies
- The ability to connect your devices using Symantec Endpoint Protection through a lightweight agent, or by using a proxy auto-config (PAC) file
- Mobile-device configuring through profiles pushed with connections of a secure virtual private network (VPN) tunnel to the cloud service

Symantec Web Secuirty Service Global Cloud Network

- More than 55 global service points, with automatic closest data center selection
- Any customer can have access to any data center
- Network peering connections established with Microsoft, Amazon, Google, and more
- Standard 99.999% availability SLA
- Optimized TCP Window Scaling to boost performance
- Automatic IP-Address Alignment to facilitate security policy enforcement with Office 365
- Hosted at top tier infrastructure providers
- Redundant within and between locations
- World-class monitoring and reporting

Solution Guide

Web Security Service threat prevention in action: One file's journey

Section

03

Symantec™

When a file is scanned by Symantec's Web Security Service, it is analyzed using information in our Global Intelligence Network. As the largest civilian threat network in the world, Symantec's Global Intelligence Network collects, categorizes, and analyzes more than 1 billion previously unseen and uncategorized websites and 2 billion emails a day from hundreds of millions of Symantec's users. This information is fed into Symantec Web Security Service to keep our customers one step ahead of today's growing security threats.

How effective is the Symantec Global Intelligence Network? In 2017, we:

- Exposed 430 million new, unique pieces of malware
- Scanned 2 billion emails daily protecting 163 million users
- Blocked 100 million social engineering scams
- Denied 40 million web attacks
- Discovered and protected 23,000+ cloud applications

Let's look at the journey of a data file being downloaded from a website as it goes through Symantec's comprehensive security platform. When the file is detected, it faces a gauntlet of security tests before it can be determined safe. Here's what happens as it enters the proxy capabilities of Symantec Web Security Service:

1. If the customer's existing Web Security Service security policies define a file to be safe, it is allowed in the network (e.g. if the enterprise's policies identify it as a "known good," then the file is delivered and the employee requesting the file can continue with their business). If the policies uncover a potential risk, it is blocked.
2. Anything not immediately blocked proceeds to the Web Security Service's content analysis engine for inspection.
3. The file's hash reputation from multiple vendors is analyzed and determined. Custom whitelists and blacklists are used to pass known acceptable files to users.
4. If the file fails the hash-reputation stage, it is then analyzed by two antivirus engines, which are updated by the Symantec Global Threat Intelligence Network.
5. If the file's signatures evaluated in Content Analysis are identified as bad, then the file is blocked.
6. If the file's safety remains unknown, a static code analysis is run to determine if anything within the file code is flagged as malicious.
7. If the status of the file is still undetermined, further file behavioral analysis can occur via the optional Malware Analysis Scanning service (cloud sandbox).

Symantec Web Security Service Leadership

Symantec Web Security Service is a leading cloud-delivered Secure Web Gateway service. Symantec gateways have been listed as leaders for 10 consecutive years in the annual Gartner Magic Quadrant for Secure Web Gateways, the leader in Forrester's first Wave report on Cloud Security Gateways, and the leader in Radacati's Market Quadrant Report for Corporate Web Security. More than 70% of the Fortune Global 500 rely on Symantec SWGs to protect their businesses.[2] When you select Symantec, you are in good company.

Web Security Service Compared to a Leading Competitor

Capabilities	Competitor	Symantec
Cloud App Data & Controls (CASB)	200+	23K+
Data Loss Prevention (DLP)	No published reviews	Forrester Wave & Gartner MQ Leader Cloud and On-Premise DLP options
URL Threat Risk-Levels	No	Yes
Granular Policy Settings[2]	Limited	Detailed
Predictive File Analysis	No	Yes
SSL Inspection	No published reviews	"A" rating[1]
Web Isolation	No	Yes
Global Datacenters with Peering	Yes	Yes
Email Security	No	Yes
Integrated with Endpoint Security	No	Yes
Hybrid Deployment Support	Limited	Full, with ability to centrally manage policies for all gateways
Threat Protection for All-Port & Protocol Traffic	Yes	Yes
SD-WAN with QoS	Partnership Only	Yes - both Symantec & via Partnership

Key differentiators

- Symantec offers cloud-delivered solutions, as well as virtual and true physical appliances for those who need them; all can be centrally managed.
- Symantec offers Web Isolation services to secure web browsing of potentially risky sites; the closest competitive solution does not offer this critical capability.
- Symantec Web Security Service outperformed the competitive solution in a third-party threat protection comparative study while producing a 10x improvement in the rate of false positives.[3]
- Symantec's Threat Risk Level based policies allows for customization and fine-tuning of security policies according to business needs. Users get secure and expanded web access without over-blocking.
- Symantec's integrated CASB offering is a Leader in the recent Forrester Wave. The closest competitor was not evaluated due to lack of a legitimate CASB offering.
- Based on SD-WAN technology, the SD-Cloud Connector delivers Symantec Web Security Service to customer's headquarter and branch locations quickly and easily. The included QoS and Firewall capabilities provide additional benefits of performance management and security.

- Symantec's integration of Web Security Service with Endpoint Protection takes a defense-in-depth approach by delivering a multi-layered protection, both on the endpoint and from the network, against sophisticated security threats.
- Symantec's integrated DLP solution is a perennial leader in Forrester and Gartner reports. The closest competitor was not evaluated due to lack of a robust DLP offering.
- Symantec received the only "A" rating in an academic, third-party analysis of solutions for SSL visibility and inspection. All other vendors received a "C" rating or worse because of their inability to securely inspect traffic.[1]
- Symantec's Global Intelligence Network is the world's largest civilian threat intelligence network, scanning traffic from hundreds of millions of users and flagging threats to all users of the Web Security Service. The competitor's solution has threat intelligence from scanning the traffic of only 10 million users.
- Every Symantec data center is available to every subscriber, ensuring all can take full advantage of industry-standard global-security coverage wherever they are. Fewer than half of our competitors' data centers are accessible to all customers.

Symantec Web Security Service: The advanced security controls you need for the security challenges of the cloud generation

As enterprise data security and privacy threats grow, legacy solutions are proving to be ineffective in dealing with the challenge. Enterprises facing the security challenges of of the cloud generation need capabilities to:

- Govern access to all data, apps, and systems from all users and devices, regardless of where those users and devices are located.
- Secure all their information wherever it resides.
- Defend against advanced threats, internal and external.

Symantec Web Security Service was built to deliver advanced protection and security capabilities from the cloud. Backed by the strength, simplicity, and reach of our Global Intelligence Network, we're ready to protect your environment and all your sensitive data from the latest, most advanced threats every second of every day. That's the reason Symantec is the proven leader in cloud-generation solutions, ensuring that all use of the web and cloud is productive, compliant, and secure.

Learn more »

Contact us »

[1] "The Security Impact of HTTPS Interception" https://jhalderm.com/pub/papers/interception-ndss17.pdf

[2] "Corporate Web Security - Market Quadrant 2016," The Radicati Group, Inc. https://newberrygroup.com/wp-content/uploads/2017/10/report_radicati_2016_corporate_web_security_market_quadrant_en.pdf

[3] Third-party testing analysis study by the Tolly Group

Symantec™