Guía de Soluciones

# Symantec Web Security Service

# Seguridad de Red Avanzada Entregada en la Nube para la Generación de la Nube.

La realidad actual de la seguridad empresarial: Los dispositivos, los datos y las aplicaciones están fuera de su control físico y todo debe ser administrado y protegido

Aplicaciones en la Nube  Dispositivos móviles  Usuarios remotos

Symantec

Guía de Soluciones

# Introducción
# Una tormenta perfecta de desafíos de seguridad

Sección

00

Symantec™

El enfoque tradicional para la seguridad empresarial se ha vuelto obsoleto debido a una tormenta perfecta de usuarios móviles, oficinas remotas, aplicaciones en la nube, obligaciones de cumplimiento y amenazas de seguridad en evolución.

Con los empleados que desean acceder a aplicaciones y datos directamente desde Internet, las soluciones de seguridad heredadas, que requieren que el tráfico pase a través del centro de datos empresarial para aplicar políticas de seguridad y cumplimiento de datos, ya no son efectivas.

Hoy, los equipos de operación y seguridad de la red necesitan respuestas a estas preguntas:

- ¿Cómo simplificamos la seguridad de nuestra red y reducimos la cantidad de tráfico de Internet que estamos regresando a la empresa?
- ¿Cómo podemos mejorar el rendimiento de nuestra solución?
- ¿Cómo protegemos a los usuarios de las nuevas amenazas en evolución de la Web y la nube?
- ¿Cómo aseguramos los datos y mantenemos el cumplimiento con reglamentos cada vez más estrictos?
- ¿Cómo administramos efectivamente el acceso remoto, los usuarios móviles y los dispositivos no autorizados?

La nueva realidad de la seguridad de la red empresarial requiere una solución de seguridad integral entregada en la nube con capacidades avanzadas que refuercen la protección contra amenazas y políticas de seguridad de la información para todos sus usuarios, en cualquier lugar.

Guía de Soluciones

# Repensando el papel de Secure Web Gateway en su sistema de seguridad

Sección

01

Symantec™

Muchas organizaciones confían en los gateways web seguros (SWG) para realizar las funciones básicas del filtrado de URL y para hacer cumplir las políticas de permiso de uso para la web y la nube. Debido a su papel en la agilización del flujo de datos a las aplicaciones web y en la nube y su capacidad única para escanear y orquestar el tráfico cifrado, los SWG se están convirtiendo en el núcleo de su sistema de seguridad de red completa. Más allá de las funciones básicas de SWG tradicionales, una solución dirigida por proxy puede expandirse para proteger todo el tráfico de Internet (no solo el tráfico web), ofrecer escaneo de prevención contra pérdida de datos (Data-Loss Prevention - DLP), protección avanzada contra amenazas y malware y poderosos controles para las aplicaciones en la nube.

Al seleccionar una solución SWG basada en la nube para abordar los desafíos de seguridad y cumplimiento, es esencial encontrar una solución avanzada que brinde la flexibilidad para resolver una gama de desafíos críticos de seguridad y cumplimiento.

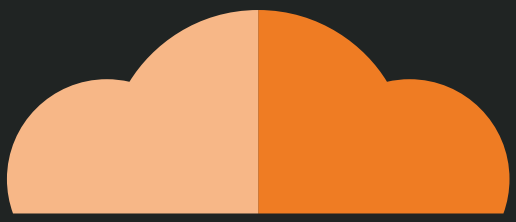
Busque un servicio de gateway seguro que no solo pueda categorizar y filtrar efectivamente su tráfico web y hacer cumplir su policía de uso aceptable, sino que también puede:

- Proteger el tráfico de la red en todos los puertos y todos los protocolos
- Detectar y prevenir amenazas avanzadas manteniendo falsos positivos a un nivel mínimo
- Aislar las sesiones de navegación web para prevenir las amenazas y los ataques de phishing
- Orquestar el tráfico cifrado a las soluciones DLP, ya sea en las instalaciones o en la nube
- Proporcionar seguridad a las aplicaciones en la nube, conocida como controles CASB, que ofrece la capacidad de identificar y administrar el uso de aplicaciones SaaS no autorizadas, conocida como Shadow IT
- Bloquear las amenazas basadas en el correo electrónico en la nube y eliminar la fuga de datos confidenciales
- Ofrecer una amplia variedad de opciones de conectividad simples, como accesos al servicio, incluidos los enfoques basados en SD-WAN
- Extienda la protección contra las amenazas hasta la computadora portátil y los dispositivos móviles
- Aplicar políticas de seguridad consistentes en gateways locales y habilitados para la nube

Guía de Soluciones

# Symantec Web Security Service: Creado para la generación de la nube

Sección



02

Symantec

**Seguridad de nivel empresarial para los datos y usuarios en cualquier lugar**

Symantec Web Security Service es un servicio integral de seguridad de red entregado en la nube basado en una arquitectura avanzada de proxy que brinda seguridad superior para sus datos, aplicaciones y usuarios, en cualquier lugar. Protección contra amenazas avanzadas, cumplimiento de la información confidencial y controles que permiten una aplicación en la nube segura y conforme el uso, todo entregado desde una infraestructura de red de nube distribuida globalmente de alto rendimiento y resistencia.

## Capacidades del Web Security Service

**Visibilidad y protección de todo el tráfico**

El tráfico actual de Internet está más relacionado a aplicaciones y va más allá del tráfico web. La función Cloud Firewall de Symantec Web Security Service agrega una capa adicional de protección para el tráfico en todos los puertos y protocolos, cerrando la brecha potencial en los tradicionales Secure Web Gateways. Puede estar seguro de que sus usuarios están bien protegidos, no solo por su tráfico web, sino por todo su tráfico de Internet.

**Filtrado y categorización de URL de Web**

El servicio filtra con precisión el tráfico en nueve categorías de tipo de contenido para permitirle reducir el riesgo de la navegación web sin un acceso excesivo. Puede establecer políticas en más de 70 categorías que abarcan más de 50 idiomas.

**Inspección SSL**

La inspección SSL se ha vuelto esencial para muchas empresas. Con casi el 75% del tráfico de Internet cifrado, es fundamental descifrar y orquestar el tráfico a los mecanismos de inspección de seguridad como DLP (que evita la filtración de datos y violaciones de cumplimiento) o análisis de contenido y malware (que previene los ataques y bloquea las amenazas avanzadas).

**Red de Inteligencia Global de Symantec**
**El sistema civil de inteligencia de amenazas más grande del mundo**

**80 Millones**
**Usuarios de Proxy Web**

**180 Millones**
**Endpoints**

**165 Millones**
**Usuarios de Correo Electrónico**

Symantec Web Security Service se puede configurar para interceptar, descifrar y transferir el tráfico web y en la nube a los servicios DLP o Advanced Threat Prevention para identificar violaciones de políticas y bloquear las amenazas cibernéticas. El servicio ofrece:

- Soporte para 40 suites de cifrado, lo que permite una amplia cobertura del sitio web para descifrar, inspeccionar y volver a cifrar el tráfico SSL después de la inspección. Recientemente Symantec recibió una calificación "A" en un estudio realizado por un tercero que analizó específicamente estas capacidades.[1]
- La capacidad de establecer reglas de privacidad para dejar cifradas ciertas categorías de tráfico (por ejemplo, puede optar por dejar cifrado el tráfico relacionado con Recursos Humanos).

**Protección contra amenazas/malware - Análisis de contenido y escaneo de virus**

Es más importante que nunca proteger a sus usuarios de las amenazas y el impacto de malware. Symantec combina el análisis del ecosistema web global en tiempo real con la detección de malware alineada para bloquear los sitios maliciosos, tipos de archivos propensos al malware y tráfico de "teléfono a domicilio" o de botnet. Para evitar el malware, el servicio utiliza un análisis heurístico y antivirus dual de múltiples capas, y análisis de reputación de archivos. También le permite que amplíe o reduzca su alcance según sus necesidades para ofrecer protección de malware en tiempo real en la nube.

**Protección contra amenazas/malware - Sandboxing en la nube**

El servicio de sandboxing en la nube de análisis de malware crea una línea de defensa de múltiples niveles para proteger todos los endpoints de la empresa, incluidos los usuarios móviles y remotos que se conectan directamente a Internet.

La solución de Symantec admite una amplia gama de tipos de archivos y, como el servicio escanea en sentido ascendente a sus dispositivos, evita que el malware y las amenazas lleguen a su red. El servicio detona los archivos sospechosos, realiza análisis de comportamiento para detener las amenazas avanzadas y proporciona:

- Capacidades de inspección potentes que filtran hasta el 99% de todo el potencial malware antes de la entrega, al tiempo que minimizan los falsos positivos
- Visibilidad dentro de (y bloqueo de) amenazas desconocidas y de día cero
- Detonación dual (virtual y/o emulación) con la capacidad de interactuar con el malware
- Soporte de tipo de archivo amplio
- Análisis de comportamiento y estático (YARA) y clasificación de riesgos

**Protección contra amenazas/malware - Aislamiento Web**

Para evitar el malware, algunas empresas establecen políticas de acceso web para bloquear el acceso a sitios con un historial de reputación limitado. Estos sitios con frecuencia no poseen una asignación de categoría (por ejemplo, noticias, apuestas, etc.) o un análisis de riesgo definitivo. Pero muchas veces, los empleados tienen una necesidad empresarial legítima para acceder a estas propiedades web, lo que hace que algunas organizaciones permitan el acceso para no impedir la capacidad de sus empleados de realizar estas actividades laborales.

El aislamiento web resuelve el desafío de proporcionar el acceso seguro a los sitios no categorizados y potencialmente de riesgo. Al crear un entorno de ejecución seguro entre los usuarios y la web, y al enviar solo una transmisión visual segura a los navegadores de los usuarios, el aislamiento web ayuda a evitar que las amenazas transmitidas por la web nunca lleguen a sus máquinas objetivo.

La solución de aislamiento de amenazas de Symantec:

- Permite el acceso protegido a sitios web potencialmente peligrosos
- Aumenta la productividad del negocio al brindar acceso a los empleados a un conjunto más amplio de sitios web
- Ofrece navegación web segura para ejecutivos y usuarios privilegiados cuyo acceso a documentos y sistemas sensibles los convierte en objetivos muy apreciados para los cibercriminales
- Impide que los usuarios divulguen credenciales corporativas a sitios web maliciosos.

**Red de Inteligencia Global de Symantec**

La Red Global de Inteligencia - el sistema civil de inteligencia de amenazas más grande del mundo - es un fuerte aliado en su batalla contra malware y otras amenazas virtuales. Alimentado por datos de amenazas de 80 millones de usuarios de proxy web, 180 millones de endpoints y 165 millones de usuarios finales, la red categoriza y analiza las amenazas planteadas por más de mil millones de sitios web nunca antes vistos y no categorizados y más de 2 mil millones de correos electrónicos enviados y recibidos a diario por nuestros clientes.

**Protección extendida al Endpoint**

Symantec ha integrado el Web Security Service con sus galardonadas soluciones de Symantec Endpoint Protection (SEP) y Endpoint Protection Mobile (SEP Mobile), que ofrecen seguridad avanzada para endpoints con prevención, detección, respuesta, inducción y adaptación en un único agente. Por lo tanto, en lugar de implementar un agente dedicado en dispositivos para enviar el tráfico al servicio de seguridad web, puede configurar SEP y SEP Mobile para enviar todo el tráfico del Internet desde sus dispositivos al Servicio de seguridad web. Esta solución lo hace simple para agregar la protección de red avanzada del servicio a la solución líder de la industria para proteger las computadoras portátiles y los dispositivos móviles de los usuarios (incluyendo los dispositivos Apple iOS). Ahora, puede ofrecerles a todos sus usuarios un sistema de defensa para endpoint y red en capas y de tiempo completo que los protege de modo consistente en cualquier lugar. La solución proporciona:

- Conectividad simple de Web Security Service para dispositivos conectados a la red o protegidos por SEP y SEP Mobile en roaming
- Una solución integral para endpoints que ofrece prevención, EDR, engaño y endurecimiento
- Un único agente que combina defensas en capas para redes y endpoints a sus usuarios

**Gestión unificada de políticas: en la nube y en las instalaciones**

Symantec está en una posición única para ayudar a las organizaciones a migrar a la nube. Ofrece el portafolio más amplio de la industria de Secure Web Gateways, con opciones diseñadas para satisfacer cualquier requisito - desde el privado al público, físico, virtual o en la nube. Lo mejor de todo es que Symantec Universal Policy Enforcement le permite migrar las políticas locales existentes al Web Security Service en la nube. Si necesita establecer nuevas políticas, puede escribirlas una vez y enviarlas a todos sus gateways de Symantec para una aplicación consistente, ya sea en la nube o en las instalaciones.

Nuestra solución de gestión de políticas en la nube y local le permite:

- Simplificar la transición de su organización a la seguridad basada en la nube
- Elaborar y administrar políticas consistentes en todos sus gateways de Symantec
- Optimizar su inversión existente en la creación de políticas
- Evitar la complejidad de elaborar y administrar políticas en múltiples herramientas de seguridad

**Cloud Access Security Broker (CASB)**

Es probable que no haya logrado evitar que los datos en la nube no autorizados, llamados Shadow IT, entre en su empresa. El hecho es que ya están allí. Nuestro último análisis muestra que existen más de 900 aplicaciones no autorizadas en una empresa típica.

Shadow IT se suma a sus riesgos de seguridad y cumplimiento. El módulo CASB Audit de Symantec incluye datos de atributos discretos de más de 23.000 aplicaciones. La integración perfecta entre o Web Security Service y CASB Audit automatiza el proceso de análisis de sus registros de proxy para revelar los riesgos de Shadow IT, ayudándoles a:

- Identificar las nubes a las que sus usuarios acceden
- Evaluar los riesgos de las nubes mediante la evaluación de 90 atributos en cada una
- Establecer políticas de acceso y control basadas en datos de atributos de la nube

La solución CASB de Symantec, conocida como CloudSOC, posee un amplio conjunto de capacidades más allá del control de Shadow IT. Ofrece un conjunto adicional de capacidades de control de acceso y DLP que son esenciales para mantener el control y cumplimiento en las aplicaciones de nube SaaS. Además, la prevención de amenazas especializada de CloudSOC utiliza análisis de comportamiento del usuario para identificar riesgos de credenciales de nube comprometidas, como ID y contraseñas.

**Protección de información (DLP)**

Buenas noticias: Si está migrando a la nube para que la seguridad pueda soportar usuarios móviles y remotos, puede permanecer en la nube para aplicar sus políticas de protección de datos utilizando Symantec DLP Cloud. La solución integrada aprovecha la capacidad de Web Security Service para descifrar el tráfico SSL y enviarlo a Symantec DLP Cloud para un análisis preciso y rápido.

La solución también permite el escaneo offline de cuentas en aplicaciones como Box y Dropbox con el objetivo de detectar cualquier cosa que sus empleados puedan haber ingresado en cuentas corporativas (intencionalmente o inadvertidamente).

¿Desea utilizar su solución DLP existente? Con Symantec, puede. Aproveche su inversión - incluyendo todo el tiempo que haya dedicado a ajustar sus reglas de políticas, y amplíe su alcance a la web, a la nube y al tráfico móvil. Hemos hecho que sea fácil configurar Symantec Web Security Service para enviar tipos específicos de tráfico a su DLP local existente para escanear.

El servicio integrado es compatible con el cumplimiento normativo y la protección de datos por medio de:

- Aplicar sus políticas de privacidad y protección de datos a todo su tráfico web, incluido el tráfico para usuarios móviles y remotos
- Garantizar que el tráfico cifrado SSL que debe inspeccionarse pueda analizarse con precisión
- Monitorear y auditar continuamente los archivos cargados
- Aplicar de forma automática controles de políticas a datos confidenciales
- Alertar a los administradores y a los propietarios de datos cuando la información se pone en riesgo

**Seguridad del correo electrónico en la nube**

Ahora, más que nunca, necesita protección contra los ataques avanzados de phishing y la reducción de spams. Debido a que el correo electrónico llega a través de SMTP, que es un canal diferente de la mayoría de las actividades de Internet, requiere diferentes capacidades de prevención de amenazas y protección de datos. Cuando los correos electrónicos contienen archivos adjuntos o URLs cliqueables, su programa de seguridad debe examinarlos con mecanismos avanzados de detección de malware e inspeccionarlos en entornos aislados.

Symantec Email Security.cloud:

- Detiene las amenazas de correo electrónico nuevas y sofisticadas, como el compromiso del correo electrónico corporativo y ransomware con tecnologías de detección de múltiples capas, que incluyen heurística avanzada, evaluación de enlaces profundos y sandboxing basado en la nube
- Ofrece una sólida protección contra spear phishing al utilizar la evaluación de enlaces profundos para detener enlaces maliciosos antes de que se entregue un correo electrónico y cuando los usuarios hacen clic en ellos (para protegerse contra el correo electrónico convertido en armas después de la entrega)
- Protege los datos confidenciales y ayuda a abordar los requisitos legales y de cumplimiento con las políticas granulares de DLP para su correo electrónico basado en la nube

**Ancho de banda y control de rendimiento**

Algunas aplicaciones en la nube, como Office 365, crean problemas de rendimiento que pueden complicar la adopción. Por ejemplo, un usuario típico de MS Exchange Online mantendrá seis o más conexiones simultáneas de Internet y una organización con 3.500 usuarios en Exchange Online probablemente requiera 200 MB adicionales de ancho de banda de Internet. Este tipo de escenario se puede abordar con capacidades de control de ancho de banda que reservan ancho de banda para aplicaciones críticas como Office 365 y que limitan el tráfico recreativo disruptivo a sitios como YouTube o Facebook.

Impulsado por nuestra red global de inteligencia, Symantec Bandwidth Control identifica con precisión los flujos de aplicaciones móviles, comerciales y en la nube, y le permite priorizar las aplicaciones relevantes para el negocio sobre el contenido recreativo.

**Opciones de Conectividad**

Con una amplia red de centros de datos globales distribuidos que brindan acceso a la nube, tendrá la libertad de conectar computadoras portátiles, dispositivos móviles, firewalls, servidores proxy y más a sus puntos de presencia locales. Comenzar es tan fácil como hacer un cambio de configuración en su firewall o proxy, o un ajuste simple en los dispositivos de sus usuarios. Más allá del método, todo el acceso del usuario al Web Security Service está cifrado.

Las opciones de conectividad de Symantec incluyen:

- La capacidad de conectar sus oficinas a la nube simplemente reenviando el tráfico a través de túneles IPSec
- Conectividad rápida y simple de oficinas remotas a Symantec Web Security Service a través de SD-Cloud Connector, una opción de conectividad fácil de implementar y muy resistente basada en tecnología SD-WAN
- Si está utilizando Symantec Endpoint Protection, una actualización de configuración simple es todo lo que se necesita para enviar automáticamente el tráfico de Internet al Web Security Service.
- Encadenamiento proxy o reenvío de proxy para enviar tráfico de proxies existentes
- La capacidad de conectar sus dispositivos usando Symantec Endpoint Protection a través de un agente liviano, o mediante el uso de un archivo proxy de autoconfiguración (PAC)
- Configuración de dispositivos móviles a través de perfiles insertados con conexiones de un túnel seguro de red privada virtual (VPN) al servicio en la nube

## Symantec Global Cloud Network de Web Security Service

- Más de 55 puntos de servicio globales, con la selección automática de centros de datos más próximos
- Cualquier cliente puede tener acceso a cualquier centro de datos
- Interconexiones de red establecidas con Microsoft, Amazon, y Google y más
- Estándar SLA de disponibilidad 99,999%
- Escalado de ventanas (Window Scaling) TCP optimizado para aumentar el rendimiento
- Alineación automática de direcciones IP para facilitar la aplicación de políticas de seguridad con Office 365
- Alojado en proveedores de infraestructura de nivel superior
- Redundante dentro y entre locales
- Monitoreo y envío de informes de alto nivel

Guía de Soluciones

# Prevención de amenazas del Web Security Service en acción: El viaje de un archivo

Sección

03

Symantec™

Cuando un archivo es escaneado por Symantec Web Security Service, su análisis utiliza información de nuestra Red de Inteligencia Global. Como la red de amenazas civiles más grande del mundo, la Red de Inteligencia Global de Symantec recopila, categoriza y analiza más de mil millones de sitios web nunca antes vistos o no categorizados y 2 mil millones de correos electrónicos al día de cientos de millones de usuarios de Symantec. Esta información es ingresada en Symantec Web Security Service para mantener a nuestros clientes un paso delante de las crecientes amenazas de seguridad en la actualidad.

¿Qué tan efectiva es la Red de Inteligencia Global de Symantec? En 2016, nosotros:

- Expusimos 430 millones de piezas nuevas y únicas de malware
- Se detuvieron mil millones de correos electrónicos maliciosos
- Se bloquearon 100 millones de escaneos de ingeniería social
- Se denegaron 182 millones de ataques web
- Se descubrieron y protegieron más de 21.000 aplicaciones en la nube

Vamos a observar el recorrido de un archivo de datos que se descarga desde un sitio web a medida que avanza a través de la plataforma de seguridad integral de Symantec. Cuando se detecta el archivo, se enfrenta a una serie de pruebas de seguridad antes de que se pueda determinar que es seguro. Esto es lo que ocurre cuando ingresa en las capacidades de proxy de Symantec Web Security Service:

1. Si las políticas de seguridad existentes de Web Security Service definen que un archivo es seguro, está permitido en la red (por ejemplo, si las políticas de la empresa lo identifican como “bien conocido”, el archivo se entrega y el empleado que ha solicitado el archivo puede continuar con sus actividades). Si las políticas descubren un riesgo potencial, está bloqueado.
2. Todo lo que no se bloquee de inmediato pasa al mecanismo de análisis de contenido de Web Security Service para su inspección.
3. Se analiza y determina la reputación de hash del archivo de múltiples proveedores. Whitelists y blacklists personalizadas se utilizan para transferir archivos conocidos aceptables a los usuarios.
4. Si el archivo no pasa la etapa de reputación de hash, es analizado por dos mecanismos antivirus, que son actualizados por Symantec Global Threat Intelligence Network.
5. Si las firmas del archivo evaluadas en análisis de contenido se identifican como inapropiadas, entonces el archivo es bloqueado.
6. Si la seguridad del archivo permanece desconocida, se ejecuta un análisis de código estático para determinar si algo dentro del código del archivo está marcado como malicioso.
7. Si el estado del archivo aún no está determinado, se puede realizar otro análisis de comportamiento del archivo a través del servicio opcional de análisis de malware (sandbox de la nube).

**Liderazgo de Symantec Web Security Service**

Symantec Web Security Service es un servicio líder de Secure Web Gateway entregado en la nube. Los gateways de Symantec han sido clasificados como líderes durante 10 años consecutivos en el Cuadrante Mágico de Gartner para Secure Web Gateways, líder en el primer informe Forrester Wave sobre Cloud Security Gateways y el líder en el Cuadrante de Mercado de Grupo Radacati para Seguridad Web Corporativa. Más del 70% de la lista Fortune Global 500 confía en los SWG de Symantec para proteger sus negocios.[2] Cuando opta por Symantec, está en buena compañía.

**Web Security Service Comparado con un Competidor Principal**

| Capacidades | Competidor | Symantec |
|---|---|---|
| Datos y controles de la aplicación en la nube (CASB) | 200+ | 23K+ |
| Data Loss Prevention (DLP) | Ninguna revisión publicada | Líder en el informe Forrester Wave y en el Cuadrante Mágico de Gartner en las opciones de DLP en las instalaciones y en la nube |
| Inteligencia en Amenazas | Por debajo del promedio | Por encima del promedio |
| Definición de pólizas granular[2] | Limitado | Detallado |
| Análisis predictivo de archivos | No | Sí |
| Inspección SSL | Ninguna revisión publicada | Clasificación "A"[1] |
| Aislamiento Web | No | Sí |
| Centro de Datos globales con interconexión | Sí | Sí |
| Seguridad del correo electrónico | No | Sí |
| Integrado con seguridad de endpoint | No | Sí |
| Soporte de despliegue híbrido | Limitado | Completo, con capacidad de administrar centralmente las políticas para todos los gateways |
| Protección contra amenazas para todos los puertos y tráfico de protocolo | Sí | Sí |
| SD-WAN con QoS | Apenas por medio de alianzas | Sí – Tanto por Symantec como por medio de alianzas |

## Principales Diferenciales

- Symantec ofrece soluciones entregadas en la nube, así como dispositivos físicos virtuales para quienes los necesitan; todos pueden ser administrados centralmente.
- Symantec Web Security Service superó a la solución de la competencia en un estudio comparativo de protección contra amenazas de terceros, al tiempo que produjo una mejora de 10 veces en la tasa de falsos positivos.[4]
- Symantec Web Security Service va más allá de la protección tradicional del tráfico web. Con Cloud Firewall, está protegido el tráfico en todos los puertos y protocolos. El tráfico web puede enviarse al mecanismo proxy para un análisis y filtrado profundo.
- Basado en la tecnología SD-WAN, SD-Cloud Connector ofrece Symantec Web Security
- Servicio a la sede del cliente y sucursales de manera rápida y fácil. Las capacidades incluidas de QoS y Firewall proporcionan beneficios adicionales de gestión del rendimiento y seguridad.
- Symantec ofrece servicios de aislamiento de la web para proteger la navegación web de sitios potencialmente peligrosos. La solución competitiva más cercana no ofrece esta capacidad crítica.

- La solución CASB integrada de Symantec es líder en el más reciente informe Forrester Wave. El competidor más cercano no fue evaluado debido a la falta de una solución legítima de CASB.
- La integración de Symantec de Web Security Service con Endpoint Protection toma un enfoque de defensa en profundidad entregando una protección de varias capas, tanto en el endpoint como desde la red, contra sofisticadas amenazas de seguridad.
- La solución DLP integrada de Symantec es un líder continuo en los informes de Forrester y Gartner. El competidor más cercano no fue evaluado debido a la falta de una solución legítima de DLP.
- Symantec recibió la única calificación “A” en un análisis académico y de terceros de soluciones para la visibilidad e inspección de SSL. Todos los demás proveedores recibieron una calificación “C” o peor debido a su incapacidad para inspeccionar el tráfico de manera segura.[1]
- La red de inteligencia global de Symantec es la red de inteligencia de amenazas civiles más grande del mundo, que escanea el tráfico de cientos de millones de usuarios y amenazas marcadas a todos los usuarios del Web Security Service. La solución del competidor tiene inteligencia de amenazas que escanea el tráfico de solo 10 millones de usuarios.
- Todos los centros de datos de Symantec están disponibles para todos los clientes, lo que garantiza que todos puedan aprovechar al máximo la cobertura de seguridad global estándar de la industria, en cualquier lugar. Menos de la mitad de los centros de datos de nuestros competidores son accesibles para todos los clientes.

# Symantec Web Security Service: Los controles avanzados de seguridad que necesita para los desafíos de la generación de la nube

**A medida que aumentan las amenazas a la privacidad y a la seguridad de los datos empresariales, las soluciones heredadas resultan ineficaces para hacer frente a los desafíos actuales. Las empresas que enfrentan los desafíos de seguridad de la generación de la nube necesitan capacidades para:**

- Administrar el acceso a todos los datos, aplicaciones y sistemas de todos los usuarios y dispositivos, independientemente de dónde se encuentren esos usuarios y dispositivos.
- Proteger toda su información, en cualquier lugar.
- Defenderse contra las amenazas avanzadas, tanto internas como externas.

Symantec Web Security Service fue creado para ofrecer capacidades avanzadas de protección y seguridad desde la nube. Respaldados por la fuerza, la simplicidad y el alcance de nuestra Red Global de Inteligencia, estamos preparados para proteger su entorno y todos sus datos confidenciales contra las amenazas más recientes y avanzadas, cada segundo todos los días. Por esa razón que Symantec es el líder comprobado en soluciones de generación de nube, asegurando que todo el uso de la web y de la nube sea productivo, seguro y atienda a los requisitos de cumplimiento.

**Más información »**

**Contacto »**

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 "Magic Quadrant for Secure Web Gateways," Gartner, 6 de junio de 2016

4 Estudio de análisis de test realizado por tercero por el Tolly Group



Symantec