Symantec™ Complete Website Security

Symantec™ Complete Website Security

Una solución completa para todo lo que necesita para que su sitio web sea seguro: sus funciones abarcan desde los certificados SSL/TLS con Extended Validation hasta el escaneado de malware, pasando por la neutralización de ataques DDoS y la optimización del rendimiento.

Symantec | Website Security

Nuevas defensas para nuevas amenazas

¿Un mundo feliz?
Cuando se trata de seguridad de sitios web, la única constante clara es que las amenazas nunca dejan de crecer, tanto en lo que se refiere a su alcance como a su complejidad. Esta situación se aprecia en la batalla que libran los que tratan de proteger la información online contra los que intentan acceder a ella de manera ilegal. Hemos aprendido mucho con la experiencia y hoy sabemos que no es posible construir una frontera segura para frenar a los intrusos, pues los delincuentes han demostrado ser capaces de colarse por túneles, abrirse paso a escondidas o, simplemente, disfrazarse y entrar por la puerta principal.

La importancia de conocer las amenazas
Hasta ahora, los sistemas de seguridad por lo general han actuado a posteriori, es decir, se han limitado a reaccionar con rapidez cada vez que aparecía una nueva amenaza, para construir defensas y mitigar las posibles consecuencias. Se necesita una solución que proteja el sitio web de forma eficaz y proactiva frente a los peligros que lo acechan, que no dejan de aumentar y ya no se trata de hackers solitarios encerrados en una habitación, sino de auténticas redes de delincuentes, «hacktivistas» y amenazas promovidas por gobiernos. Contar con los recursos adecuados en el lugar correcto y en el momento justo ya no es solo importante sino imprescindible.

La solución: los expertos en seguridad
Crear y conservar una infraestructura empresarial segura, al igual que ganarse la confianza de los clientes, es una actividad continua que se puede echar por tierra en cuestión de segundos. Ante las amenazas actuales, que se transforman a marchas forzadas, es imprescindible innovar constantemente con el fin de adaptar al mismo ritmo las soluciones de seguridad para sitios web. Aunque sabemos que sería absurdo quedarse de brazos cruzados, tampoco parece factible reaccionar a cada nueva amenaza que surge, pues el tiempo y dinero disponibles para ello son limitados. La solución es pedir ayuda a un experto en seguridad, que podrá enseñarle a detectar vulnerabilidades y a reducir los riesgos.
Adopte Symantec™ Complete Website Security.

Las amenazas, en cifras
(Datos del informe de Symantec de 2015 sobre las amenazas para la seguridad de los sitios web)

El 78 %
de los sitios web escaneados en 2015 tenían vulnerabilidades

431 millones
de nuevas variantes de malware surgieron en 2015

1,1 millones
de ataques web bloqueados diariamente

125 %
Aumento de las vulnerabilidades de día cero de 2014 a 2015

La importancia de la seguridad

El reto de adoptar los recursos adecuados para garantizar la seguridad

Como se sabe, en última instancia la seguridad de los sitios web permite ganarse la confianza de los internautas. Para ello, hay que analizar de forma realista los peligros que amenazan a la empresa y calcular con precisión los recursos necesarios para evitarlos. En realidad, podría decirse que la mayor amenaza es la habitual escasez de los recursos destinados a la protección de los sitios web, a lo que se suma el uso de procesos manuales. Todo ello, junto con las prisas, hace que incluso la tarea de seguridad más sencilla entrañe dificultades.

Certificados SSL/TLS con Extended Validation

Resulta vital que el sitio web inspire confianza: quien lo visite tiene que sentir que se encuentra en un lugar seguro para hacer transacciones con tranquilidad. Según un estudio de Econsultancy, el 50 % de los clientes que abandonan un proceso de compra online lo hacen porque no se fían. Recientemente YouGov ha realizado una encuesta online en el Reino Unido, Estados Unidos, Francia y Alemania que ha permitido llegar a conclusiones claras y alentadoras: la mayoría de la gente sabe qué tiene que buscar para saber si un sitio web es fiable o no. Si en su sitio web no aparecen indicios de seguridad claramente visibles, es probable que la confianza de los clientes en su empresa se vea perjudicada, lo que podría traducirse en una pérdida de ventas.

Cómo elegir el certificado SSL/TLS adecuado

Nivel 1: Validación de dominio (DV)

Se trata del nivel de autenticación más bajo, adecuado para situaciones en las que la confianza y la credibilidad no son muy importantes.

Nivel 2: Validación de empresa (OV)

Es una opción más segura, indicada para los sitios web públicos en los que se lleven a cabo transacciones que no sean demasiado delicadas.

Nivel 3: Extended Validation (EV)

Son los certificados SSL/TLS más seguros que existen, ideales para sitios web que manejen datos muy confidenciales, como los números de las tarjetas de crédito.

Tipo de certificado	¿Validación del dominio?	¿Cifrado «https»?	Validación de identidad	¿Validación de la dirección?	Símbolo del candado en la interfaz de usuario del navegador	Barra de direcciones verde*
DV	Sí	Sí	Ninguna	No	Sí	No
OV	Sí	Sí	Buena	Sí	Sí	No
EV	Sí	Sí	Muy buena	Sí	Sí	Sí

*O un candado verde o algún signo verde en la barra de direcciones.

Denegación de servicio

También se sabe que muchas empresas son víctima de los hackers o se infectan con malware porque no realizan unas comprobaciones básicas de su sitio web. Por ejemplo, en el año 2015, el 78 % de los sitios web escaneados presentaban vulnerabilidades, de las cuales una quinta parte eran graves. Estas infecciones pueden llegar a paralizar una empresa: Google bloquea 10 000 sitios web al día, y por término medio se tarda seis semanas en desbloquearlos. Por otro lado, también hay incidencias de seguridad más visibles, como los ataques de denegación de servicio (Distributed Denial of Service o DDoS), que generan desde meras páginas de error HTTP404 hasta el bloqueo total del sitio web, y que cada vez son más intensos. Ahora Symantec™ Complete Website Security, además de ofrecer nuestros instrumentos de eficacia comprobada para evitar daños en el sitio web, también incluye la protección frente a ataques DDoS, que neutraliza todo tipo de ataques DDoS contra cualquier servicio online.

Bots maliciosos en la capa de las aplicaciones

Además de los peligros mencionados anteriormente, también están los ataques DDoS en el nivel de las aplicaciones, que aprovechan vulnerabilidades del sistema operativo o de las aplicaciones web y son inmunes a los filtros genéricos. Estos ataques se llevan a cabo con bots maliciosos que se hacen pasar por visitantes humanos legítimos y secuestran los navegadores con el fin de inutilizar los servidores de una empresa. En el año 2014 detectamos un aumento del 240 % en el tráfico de bots, un dato que confirma lo que muchos expertos en seguridad ya saben: en la actualidad, los instrumentos de los hackers se diseñan de forma que actúen ante todo con sigilo. En consecuencia, para mejorar aún más el nivel de protección de nuestra solución, hemos añadido el firewall para aplicaciones web (WAF), un concepto nuevo de WAF que llega mucho más lejos que los tradicionales.

Symantec™ Complete Website Security

Principales funciones de seguridad

- Evaluación de vulnerabilidad
- Evaluación de vulnerabilidad
- Certificados SSL/TLS con Extended Validation
- Protección frente a ataques DDoS
- Firewall para aplicaciones web
- Secure App Service

En Symantec, trabajamos para ofrecerle soluciones que le protejan de las amenazas de hoy y de mañana.

La importancia de la gestión

Objetivo: simplificar

Cada vez es más evidente que gestionar la seguridad de los sitios web se ha convertido en algo mucho más complicado de lo que debería, sobre todo en lo que se refiere a las licencias de certificados SSL/TLS. De hecho, numerosos administradores de PKI y gestores de la seguridad de los sitios web se ven desbordados cuando tienen que buscar certificados ocultos para evitar que caduquen de forma imprevista.

Los certificados y su mantenimiento

En Symantec sabemos que no es fácil gestionar los certificados SSL/TLS, sobre todo si hay más de una persona autorizada para implantarlos de forma independiente. Además, si los certificados caducan, los efectos pueden ser devastadores: según nuestros estudios, más del 75 % de los consumidores abandonarían la transacción iniciada si se encontraran con un certificado SSL/TLS que ya no fuera válido. Por otro lado, el 45 % de las empresas encuestadas sufrieron incidentes de seguridad debido a problemas relacionados con los certificados SSL/TLS. Todo ello hace que sea imprescindible contar con instrumentos que simplifiquen y centralicen la gestión, y eso es precisamente lo que ofrece Symantec™ Complete Website Security.

La simplificación de la gestión de los certificados SSL/TLS

Por supuesto, comprar y renovar certificados no lo es todo, ni basta para garantizar la seguridad de los sitios web. También hay que buscar certificados de origen dudoso, estar al tanto de las fechas de caducidad y respetar ciertos estándares: todo ello puede resultar difícil en las empresas grandes con sedes en distintos lugares. Según una encuesta reciente de Symantec, cuatro de cada cinco empresas con más de 2000 certificados encontraron en sus sistemas certificados de origen dudoso. En cambio, las funciones de detección y automatización de Symantec permiten centralizar la gestión de los certificados SSL/TLS y encontrar todos los que tenga la empresa, independientemente de la autoridad de certificación que los haya emitido.

Symantec™ Complete Website Security

Principales funciones de gestión


Detección


Automatización


Private CA

Asistencia ininterrumpida

Complete Website Security va un paso más allá para simplificar la gestión de los certificados. Gracias a la licencia de suscripción, los gastos serán predecibles, el uso de su certificado flexible y su trabajo más sencillo. Podrá emitir certificados ilimitados en su empresa a un precio fijo durante la duración de su contrato.

La importancia del rendimiento

Gestión del sitio web
Es innegable que el parámetro principal a la hora de medir el rendimiento de un sitio web es el tráfico, lo cual abarca aspectos como los niveles de conversión, junto con cuestiones más técnicas como la latencia, la disponibilidad y el ancho de banda. La solución Symantec™ Complete Website Security resulta útil en todos estos ámbitos.

Distribución de contenidos optimizada
Según un estudio de Forrester, el 40 % de los compradores abandonan un sitio web de comercio electrónico si tarda más de tres segundos en cargarse.[1] Lo bueno es que hoy disponemos de una serie de herramientas avanzadas que aceleran la carga y el funcionamiento de los sitios web. Por ejemplo, una red de distribución de contenidos (o CDN, por sus siglas en inglés) es un sistema global de servidores ubicados estratégicamente que acerca el contenido web a los consumidores. Ahora Symantec™ Complete Website Security incluye CDN, que ofrece herramientas de almacenamiento en caché y optimización de la red y de contenidos: según los estudios realizados, los sitios web que han implantado esta solución son por término medio un 50 % más rápidos y consumen hasta un 70 % menos de ancho de banda.

Disfrute de la versatilidad de la nube en la aplicación de equilibrio de carga
Con el equilibrio de carga en la nube podrá maximizar el rendimiento y la fiabilidad de la aplicación, para así aprovechar mejor sus recursos. Además, con la flexibilidad que concede la nube, podrá ajustar la aplicación a sus necesidades puntuales para así reducir gastos. Nuestro servicio de equilibrio de carga es perfecto para un centro de datos con diversos servidores, tolerancia a fallos de centros de datos en casos de desastre y balanceo global de datos de servidores (GSLB).

La solidez y la velocidad del cifrado
Como sabemos, los certificados SSL/TLS permiten cifrar todos los datos que se transmiten entre el navegador de un usuario que consulta un sitio web protegido y el servidor empresarial en el que se aloja dicho sitio web. Por lo tanto, obviamente conviene que el cifrado sea lo más seguro posible. El algoritmo de criptografía de curva elíptica (ECC) de 256 bits es más avanzado y resulta 64 000 veces más seguro que el de los certificados RSA de 2048 bits. Además, ofrece una ventaja aún más importante: necesita mucha menos capacidad de servidor para cifrar la información, con lo que se reducen los costes y mejora el rendimiento del sitio web. Por ejemplo, al implantar el cifrado ECC, la empresa japonesa Directorz Co. Ltd. consiguió reducir el uso de recursos de CPU en un 46 % y mejorar los tiempos de respuesta en un 7 %. En la actualidad, gracias a nuestros certificados SSL/TLS híbridos, también es posible combinar la raíz RSA estándar con las ventajas del algoritmo ECC: una mayor seguridad y un mejor rendimiento en el servidor.

Cómo fomentar la confianza
Los consumidores necesitan sentirse seguros a la hora de proporcionar datos o comprar algo por Internet, y la mayoría sabe reconocer los distintivos de confianza que garantizan la seguridad del sitio web. Por ejemplo, el sello Norton Secured es uno de los que más confianza inspiran en Internet, y se visualiza más de mil millones de veces al día en 170 países. Su presencia marca una gran diferencia: en un estudio de consumo internacional, el 90 % de los encuestados han declarado que es más probable que continúen con un proceso de compra electrónica si ven el sello Norton Secured.[2] Asimismo, cuando el sello aparece junto al enlace a un sitio web en los resultados de los buscadores, también aumenta el número de visitas de forma considerable.

Symantec™ Complete Website Security

Principales funciones de rendimiento:

- CDN y optimización
- Criptografía de curva elíptica
- Seal in Search
- Sello Norton Secured
- Equilibrio de cargas y tolerancia a fallos

[1] Investigación sobre consumo en Internet realizada por los consultores de Forrester. Septiembre de 2009. [2] Investigación sobre consumo internacional en Internet: Estados Unidos, Alemania y Reino Unido. Julio de 2013.

Symantec™ Complete Website Security

Una solución mejorada frente a las amenazas avanzadas

Complete Website Security va mucho más allá del mero cifrado para proteger los sitios web, los datos y las aplicaciones de forma ininterrumpida. De este modo, se reducen los riesgos y se garantiza que los sitios web funcionen correctamente en todo momento. Gracias a sus numerosas capas de seguridad y control, nuestros procesos de autenticación y emisión de certificados están entre los más rigurosos del sector. El sistema de gestión automática señala los puntos débiles que pueda haber en el sitio web y en los certificados si estos caducan de forma imprevista, se instalan incorrectamente, dejan de ser válidos o presentan alguna vulnerabilidad grave en caso de ataque. Al mismo tiempo, la seguridad unificada de Symantec detecta problemas de seguridad en todo el mundo, ofrece análisis en tiempo real y ayuda a sus clientes a protegerse de forma ininterrumpida. Por eso somos la marca que inspira confianza.

Características y ventajas: Seguridad

EVALUACIÓN DE VULNERABILIDAD

- Los análisis semanales ayudan a detectar y solucionar las deficiencias de seguridad.
- Recibirá un práctico informe donde se detallan las vulnerabilidades críticas que se deben estudiar de inmediato y otros riesgos de menor importancia.
- Si lo desea, podrá repetir el análisis y comprobar si las vulnerabilidades se han eliminado.

ESCANEADO DE MALWARE

- La función de escaneado diario detecta el código dañino (malware) e informa al propietario del sitio web.
- Al indicarse claramente cuál es el código dañino, se tarda menos en resolver el problema.
- También se reduce el riesgo de acabar en las listas negras de los buscadores (Google bloquea 10 000 sitios web al día, un contratiempo que puede tardar hasta seis semanas en subsanarse).

CERTIFICADOS SSL/TLS CON EXTENDED VALIDATION

- Los certificados SSL/TLS con EV siguen procesos de autenticación sumamente rigurosos, lo que se traduce en el máximo nivel de confianza entre los consumidores.
- En los sitios web con EV aparecen distintivos de confianza visuales muy conocidos, con lo que los internautas se quedan más tranquilos.
- Se ha comprobado que con la tecnología EV, la solución más segura y de mayor rendimiento a la hora de garantizar la seguridad en Internet, aumentan las conversiones y disminuye la tasa de abandono en los sitios web.

PROTECCIÓN FRENTE A ATAQUES DDOS*

- El sistema de protección líder del mercado frente a uno de los ataques más habituales.
- Detección permanente de ataques y activación automática del modo «ataque en curso».
- Eliminación de inactividad empresarial gracias a una mitigación transparente con una cantidad mínima de falsos positivos.
- Protección integral frente a los ataques DDoS más grandes y sofisticados.

* Con tecnología de Imperva Incapsula

FIREWALL PARA APLICACIONES WEB*

- Innovador firewall en la nube para evitar los ataques de capa 7.
- Protección contra las amenazas de la lista de OWASP Top 10, como la inyección de SQL, las secuencias de comandos entre sitios, el acceso ilegal a los recursos y la inclusión remota de archivos.
- Método de defensa proactivo mediante vigilancia permanente y aplicación de medidas de seguridad específicas.
- Activación mediante un simple cambio de DNS.

SECURE APP SERVICE

- Permite a las empresas:
  - firmar aplicaciones y archivos en la nube;
  - proteger las claves de firma;
  - elaborar informes sobre la actividad de firma de código;
  - controlar la productividad del equipo por medio de un portal web integrado o de la API del servicio.

Características y ventajas - Gestión

DETECCIÓN

- Detecta todos los certificados SSL/TLS del entorno, sea cual sea la autoridad de certificación que los haya emitido.
- Evita que los certificados caduquen por descuido.

AUTOMATIZACIÓN

- Al automatizar la renovación de los certificados de Symantec, se ahorra tiempo y se reduce el riesgo de error humano.

PRIVATE CA

- Mejora la seguridad y permite gestionar certificados públicos y privados con una misma consola.
- Reduce los riesgos, errores y costes ocultos que supone recurrir a autoridades de certificación autofirmadas.
- Hace posible el uso prolongado de los nombres de servidores internos, sin preocuparse por las migraciones asociadas a las raíces públicas.
- Permite crear una jerarquía personalizada, según sus necesidades.

ASISTENCIA ININTERRUMPIDA

- Tendrá a su disposición siete días a la semana un gestor personal de asistencia técnica[1] que se ocupará de:
  - supervisar las incidencias que notifique y decidir cuáles conviene atender primero;
  - hacer un seguimiento de las solicitudes de mejora de productos (si las hubiera);
  - informarle cuando se lleven a cabo tareas de mantenimiento que afecten al servicio;
  - derivar las incidencias a quien corresponda.

* Con tecnología de Imperva Incapsula [1] No abarca los productos Imperva Incapsula.

Características y ventajas: Rendimiento

CDN Y OPTIMIZACIÓN*

- CDN global que tiene en cuenta las aplicaciones, para acelerar el funcionamiento de todo el sitio web.
- Contenidos y recursos optimizados para minimizar el tiempo de latencia.
- Almacenamiento en caché de contenido estático y dinámico para conseguir el máximo rendimiento posible en el sitio web.

CRIPTOGRAFÍA DE CURVA ELÍPTICA

- **Algoritmo de criptografía de curva elíptica (ECC)**
  - Es 64 000 veces más seguro que las claves RSA de 2048 bits de uso estándar en el sector.
  - Las claves ECC de 256 bits son 64 000 veces más difíciles de descifrar.
  - El sistema es entre un 7 y un 10 % más rápido y necesita menos potencia de procesamiento.

- **Algoritmo híbrido ECC/RSA**
  - Raíces compatibles con una mayor cantidad de navegadores.
  - Rendimiento más alto.
  - Mejor seguridad que con los certificados RSA «puros».

SELLO NORTON SECURED

- El sello Norton™ Secured es el distintivo de confianza más conocido de Internet. [1]
- El 77 % de los consumidores lo reconocen.[2]
- El 90 % de los encuestados declaran que es más probable que continúen con un proceso de compra electrónica si lo ven.[3]

SEAL IN SEARCH

- Los sitios web en los que aparece el sello Norton Secured inspiran más confianza a los internautas.
- Demuestre que su sitio web es legítimo y que permite realizar transacciones sin correr riesgos.
- Convierta a más visitantes en clientes.

EQUILIBRIO DE CARGAS Y TOLERANCIA A FALLOS*

- Equilibrio de tráfico en los distintos servidores de la base de datos directamente desde la nube.
- Optimización del reparto de tráfico para reducir la carga en los servidores y maximizar el rendimiento de las aplicaciones.
- Activación del dispositivo mediante un sencillo cambio de DNS, sin instalación, integración ni modificación de hardware ni software en el sitio web.
- Mejora de la disponibilidad mediante la supervisión y tolerancia a fallos en tiempo real.

* Con tecnología de Imperva Incapsula

[1] Investigación online internacional (Estados Unidos, Alemania, Reino Unido, Francia, Australia y Singapur). Octubre de 2015. [2] Investigación sobre consumo estadounidense en Internet. Noviembre de 2013. [3] Investigación sobre consumo internacional en Internet: Estados Unidos, Alemania y Reino Unido. Julio de 2013.

Seguridad mejorada, gestión más sencilla y rendimiento más alto

Si desea informarse sobre todo lo que ofrece Symantec™ Complete Website Security para responder de forma completa, eficaz y eficiente a todas las exigencias de su sitio web en materia de seguridad, póngase en contacto con nosotros:

Llame al 900 931 298 o escriba a ssl_info@symantec.com.