Symantec. Website Security.
We go beyond

FOLLETO

Symantec™ Complete Website Security

UN NUEVO CONCEPTO DE CONFIANZA

Proteja sus sitios web. Proteja su negocio.

Ninguna empresa está a salvo de los ciberataques. La delincuencia organizada acelera tanto la aparición como la evolución de amenazas avanzadas que ponen en peligro todo el ecosistema de los sitios web y, mientras los *hackers* sigan creando formas cada vez más sofisticadas y dañinas de beneficiarse de sus ataques, el poder destructivo de las amenazas no hará sino aumentar.

Por si fuera poco, pueden pasar de semanas a meses antes de percatarse de que su sitio web ha sido objeto de un ataque. A su vez, la naturaleza sigilosa de las amenazas regala tiempo a los ciberdelincuentes para robar y saquear a su antojo a lo largo y ancho del entorno de su sitio web.

Cuanto más tiempo pase entre su detección y su resolución, peor será el daño infligido. A esto se agregan las multas, pleitos, indemnizaciones, erosión a la reputación, descenso de las ventas, pérdida de clientes... Es todo un suma y sigue. Tampoco ayuda, desde luego, la falta de recursos o tiempo suficientes para invertir en mecanismos que aseguren una protección completa y velen por el cumplimiento de las políticas de ciberseguridad. La complejidad de la administración de la seguridad en Internet y la falta de visibilidad sobre todo su ecosistema web frustran aún más sus esfuerzos, pues es prácticamente imposible saber cómo y en qué invertir sus recursos.

Por eso necesita Symantec™ Complete Website Security. Symantec le permite armonizar y reforzar la seguridad de su sitio web mediante un catálogo integral de soluciones punteras para la protección de sitios web. Puede ayudarle a reforzar la seguridad general de su sitio web, prevenir o minimizar daños derivados de la escalada de amenazas sofisticadas, liberar recursos para iniciativas de carácter estratégico, simplificar las complejidades de la seguridad en Internet y desarrollar su actividad empresarial con confianza.

En 2016, en solo un mes aparecieron 96,1 millones de nuevos tipos de malware.[1]

El número de vulnerabilidades de día cero se ha duplicado de un año para otro.[2]

[1] https://www.Symantec.com/connect/blogs/latest-intelligence-october-2016

[2] Informe de Symantec sobre las amenazas para la seguridad en Internet (2016)

Proteja su negocio, su marca y a sus clientes

Symantec™ Complete Website Security le ofrece los niveles de visibilidad, agilidad y seguridad que necesita para proteger su negocio, su reputación y a sus clientes.

- La visibilidad en tiempo real sobre su ecosistema web le permite detectar problemas antes de que sea demasiado tarde, neutralizar ataques, arreglar errores y observar las políticas de seguridad.
- En el ámbito de la seguridad, hablamos de agilidad para referirnos a la capacidad para asegurar tanto la protección como el crecimiento controlados de su empresa en el menor tiempo posible.
- La protección de varios puntos y varias capas de su amplio catálogo de soluciones de primera línea ayuda a mantener su ecosistema web a salvo hasta de las amenazas más sofisticadas conforme aparecen.

La tecnología Symantec™ Complete Website Security, avalada por el líder mundial en ciberseguridad, garantiza los niveles de seguridad, servicio y soporte que necesita para blindar el entorno de su sitio web, sus clientes y su negocio.

Las amenazas en cifras

Symantec. Website Security.
We go beyond

Visibilidad en tiempo real sobre la seguridad en Internet 24/7

La complejidad de la administración de la seguridad y del cumplimiento normativo, unida a unos recursos finitos y a una visibilidad limitada, impone un difícil juego de asignaciones de recursos que no puede ganar por sí solo. Si a la falta de visibilidad se suma una comprensión deficiente del riesgo al que se expone y el desconocimiento del estado del cumplimiento de las normativas en materia de seguridad, tomar las decisiones adecuadas y diseñar un plan de acción que salvaguarde el entorno de su sitio web termina por ser poco menos que inviable.

Symantec™ Complete Website Security pone en sus manos una amplia variedad de tecnologías que armonizan la visibilidad y la obtención de información sobre el estado de salud general de su sitio web. Esto incluye visibilidad en tiempo real sobre los servidores, las aplicaciones y los datos de su sitio web. Todo, para que le resulte más fácil detectar vulnerabilidades, neutralizar ataques, mantener la integridad de sus aplicaciones y certificados, cumplir la normativa, descubrir agujeros de seguridad rápidamente y reaccionar con presteza.

- El descubrimiento automatizado le ofrece visibilidad sobre todos los certificados SSL/TLS asociados a su sitio web y le facilita información sobre el comprador de cada certificado, la fecha de emisión, las autoridades de certificación encargadas de emitirlo, la fecha de caducidad y si el certificado cumple todos los requisitos de seguridad.
- Los informes automatizados verifican la validez y la conformidad normativa de los certificados SSL/TLS, y determinan si los servidores están configurados correctamente.
- El monitoreo y el perfilado del tráfico del sitio web se combinan con herramientas de inteligencia y análisis de comportamientos para detectar, bloquear y responder a las amenazas antes incluso de que consigan penetrar en el perímetro de su empresa.
- El escaneado diario y las evaluaciones semanales de las páginas del sitio web y sus aplicaciones, del software del servidor y de los puertos de la red permiten detectar vulnerabilidades y código dañino.
- Los sistemas de rastreo, informes y control le ofrecen visibilidad e información detallada sobre todas sus actividades de firma de código, incluidos los métodos de protección y almacenamiento empleados para las claves de firma de código, quién tiene acceso a ellas, cuándo se firmaron las aplicaciones, qué claves se utilizaron para firmarlas y la fecha de caducidad de las claves de las aplicaciones firmadas.

Agilidad y control

La proliferación de amenazas cada vez más evolucionadas y sofisticadas exige agilidad y velocidad, así como un sistema de seguridad que no ponga freno al crecimiento de su negocio. Hay que tener cuidado con las soluciones de seguridad rígidas, que dejan su negocio a merced de los ciberdelincuentes y limitan su capacidad para expandirse.

Symantec™ Complete Website Security le permite adaptar su estrategia de seguridad al ritmo de crecimiento de su empresa. Agiliza la seguridad para ayudarlo a detectar y responder rápidamente a posibles amenazas mientras mejora sustancialmente su capacidad para proteger la propiedad intelectual, los datos privados, la fidelidad de sus clientes, la reputación de su empresa y la rentabilidad, limitando su repercusión en la cuenta de resultados.

Esta solución puede ayudarlo a:

- Aumentar la confiabilidad, prevenir caídas de servicio y liberar personal ayudándose de unas herramientas de administración de certificados SSL/TLS de gama empresarial que le permiten descubrir los problemas antes de que ocurran, así como a automatizar las tareas de sustitución rutinarias
- Incrementar la facilidad, la velocidad y el control de sus esfuerzos de firma de código en múltiples plataformas.
- Acelerar y simplificar la administración, la renovación y la revocación de las claves de firma de código de sus aplicaciones, una por una o a escala, con la posibilidad de revocarlas con efecto retroactivo para que sus clientes se vean lo menos afectados posible.

Seguridad de varias capas sin fisuras

Asegurar el ecosistema de su sitio web es un difícil ejercicio de equilibrio que requiere tiempo y recursos. Por mucho que intenta destinar sus recursos de protección y resolución de problemas a las áreas más arriesgadas y a los espacios de más valor para minimizar la exposición al riesgo de todo su entorno y fortalecer su situación general, enseguida se da cuenta de que sigue a merced de las amenazas, que evolucionan rápidamente en volumen y complejidad, y de sus métodos de ataque, que cada vez se lo hacen más difícil.

Muchas organizaciones han intentado poner fin a este problema con una amalgama de soluciones de distintos proveedores de seguridad que, al final, pueden crear discontinuidad y frustrar y complicar aún más cualquier intento de proteger la seguridad del sitio web. Además, la calidad y las características de los productos de seguridad varían de un proveedor a otro, lo que en ocasiones provoca vacíos y puntos de unión débiles en la estrategia de seguridad. Por no mencionar que el mero hecho de tener que lidiar con más de un proveedor de seguridad puede ahondar en la complejidad general de una tarea, de por sí difícil, de salvaguarda de los servidores, las aplicaciones y los datos del sitio web de una organización.

Symantec™ Complete Website Security reúne las mejores soluciones de seguridad de su proveedor de confianza con todo lo que necesita para proteger su sitio web. Armoniza y refuerza la seguridad de su sitio web con un mecanismo de protección de varios puntos y varias capas que mantiene a salvo los servidores, los datos y las aplicaciones de su sitio web frente a unas amenazas cada vez más sofisticadas y dirigidas. Symantec, uno de los líderes mundiales en ciberseguridad, cuenta con el catálogo de soluciones de seguridad más completo, junto con los conocimientos, la experiencia y el servicio de soporte técnico internacional que necesita, en el momento y lugar en que lo necesita.

Las siguientes secciones detallan algunas de las soluciones, servicios y tecnologías que, combinados, proporcionan la mejor seguridad de varias capas ofrecida con Symantec™ Complete Website Security.

Detección y automatización

Cuando su equipo trabaja en tareas manuales rutinarias, como puede ser la administración de certificados, no solo está desperdiciando unos recursos muy valiosos, sino que además corre el riesgo de introducir errores humanos. Por ejemplo, olvidar la renovación de ciertos certificados lo expone a que sus servicios queden interrumpidos de manera forzosa, así como a múltiples vulnerabilidades. Además de poner en peligro la seguridad y la continuidad de los servicios de su empresa, las investigaciones demuestran que más del 75 % de los internautas abandonarán una transacción por Internet al encontrarse con un certificado caducado.

Los certificados de origen dudoso pueden incrementar las vulnerabilidades y el riesgo al que se expone el sitio web. Una encuesta de Symantec indicaba que cuatro de cada cinco compañías que cuentan con más de 2000 certificados tenían certificados de origen dudoso en sus sistemas.

Las herramientas de descubrimiento y automatización de Symantec™ Complete Website Security simplifican y centralizan el proceso de gestión de certificados SSL/TLS e incluyen funciones de descubrimiento y visibilidad sobre todos los certificados de su empresa, con independencia de la autoridad de certificación que los haya emitido.

Antes de integrar las soluciones de descubrimiento y automatización de certificados de Symantec, las operaciones del grupo LocalTapiola se veían interrumpidas en promedio una vez cada tres meses debido a la caducidad inesperada de algún certificado.

«Los certificados se nos caducaban, y eso generaba horas de trabajo extra y caídas del servicio interno».

Leo Niemelä
Director de seguridad de la información del departamento de seguridad y administración del riesgo de los sistemas TIC del grupo LocalTapiola, un proveedor de servicios financieros finlandés que cuenta con más de 5000 certificados activos.

Secure App Service (firma de código)

Uno de los mayores riesgos que más perjudica a la lealtad de los clientes es el de descargar de forma inadvertida código dañino disfrazado de una de las aplicaciones de software legítimas de su empresa. La medida más eficaz a la hora de combatir esta amenaza es firmar el código de todas sus aplicaciones de software con una clave de confianza. Sin embargo, administrar los procesos de firma de código de una gran empresa de desarrollo de software presenta no pocos desafíos en términos de administración y seguridad.

Symantec Secure App Service le ofrece una completa solución en la nube para la administración de firmas de código. En lugar de firmar todas sus aplicaciones de forma local, las sube a nuestro servicio seguro de nube y las firmamos por usted. Esto le permite almacenar con seguridad tanto su certificado como las claves en la nube, en unos centros de datos que garantizan una seguridad comparable a la que se exige para usos militares.

Además, soportamos los modelos de firma de código más extendidos entre los usuarios y proveedores de sistemas operativos y aplicaciones de software, lo que le facilita la elección del modelo que mejor reúne los requisitos de su plataforma de destino y de las políticas de seguridad internas de su empresa, como puede ser el uso de claves únicas, claves de firma múltiples o bajo demanda, y grupos rotatorios de claves. La solución incluye, asimismo, funciones de verificación y autorización de distribuidores de código, revocación de certificados, generación de informes, controles administrativos y registros para auditoría.

«Uno de los motivos por los que elegimos Symantec Secure App Service es que la gente nunca tiene acceso a las claves propiamente dichas. Contamos con más de 4000 desarrolladores a lo largo y ancho de los cinco continentes e intentar proteger todas las claves que necesitan sería una auténtica locura. Con Symantec Secure App Service, las claves se quedan en la nube y los desarrolladores solamente acceden a ellas cuando necesitan firmar código, no pueden descargarlas. A nosotros, esto nos ha cambiado la vida».

David Nalley
Vicepresidente de infraestructuras de The Apache Software Foundation

EV

Certificados SSL/TLS con Extended Validation

Inyectar seguridad y confianza en su sitio web no es opcional, porque las personas que lo visitan necesitan sentir que es un lugar seguro para comprar. El método más seguro para proteger las sesiones web de sus clientes es el cifrado de claves públicas entre el navegador y el servidor web, y la forma más ampliamente aceptada para conseguirlo es el uso de certificados SSL (Secure Sockets Layer) y TLS (Transport Layer Security).

De los tres niveles de validación de certificados SSL/TLS que aparecen en la tabla, los certificados SSL/TLS con EV son los que emplean los estándares de autenticación más estrictos y ofrecen al consumidor la máxima confianza. Los sitios que utilizan EV muestran indicadores de confianza visuales bien reconocibles, como la barra de direcciones de color verde, para que el usuario se quede más tranquilo. Se ha comprobado que la tecnología EV es la solución más segura y que presenta un mejor desempeño a la hora de garantizar la seguridad en Internet, y es bien conocida por su capacidad para aumentar las conversiones y reducir la tasa de abandono en los sitios web.

Según un estudio de Econsultancy[4], el 50 % de los clientes que abandonan una compra en Internet lo hacen por falta de confianza. La buena noticia es que, según una encuesta reciente llevada a cabo por YouGov en el Reino Unido, Estados Unidos, Francia y Alemania, la mayoría de la gente sabe en qué tiene que fijarse para decidir si el sitio web merece su confianza o no. Mostrar indicadores visuales claros de que el sitio web cuenta con mecanismos de seguridad puede mejorar la confianza de los clientes en su empresa, lo que se traduce en un mayor número de clics y conversiones.

Cómo elegir el certificado SSL/TLS idóneo

Nivel 1: validación de dominio
El nivel de autenticación más bajo, suficiente en situaciones en las que la confianza y la credibilidad son menos importantes.

Nivel 2: validación de la empresa
El siguiente nivel de seguridad, pensado para sitios web públicos donde se realicen transacciones poco confidenciales.

Nivel 3: Extended Validation
Los certificados SSL/TLS más usados en sitios web de comercio electrónico o que manejen números de tarjetas de crédito y otros datos confidenciales.

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.

[4] https://econsultancy.com/blog/7730-why-do-consumers-abandon-online-purchases/

Análisis contra código dañino

Por desgracia, es muy habitual que las organizaciones acaben siendo víctimas del hacking y del código dañino por el mero hecho de no haber sometido sus sitios web a las comprobaciones de seguridad más elementales. En 2015, por ejemplo, el 78 % de los sitios web escaneados presentó vulnerabilidades, muy graves en una quinta parte de los casos. Estas infecciones pueden llegar a ser incapacitantes: sin ir más lejos, Google agrega a su lista negra 10 000 sitios web al día y el tiempo promedio para que esos dominios vuelvan a los resultados de búsqueda suele ser de seis semanas. La falta de comprobaciones de seguridad básicas también abre la puerta a agujeros de seguridad demoledores, como ataques de denegación de servicio distribuidos (DDoS) que pueden provocar desde un simple error 404 hasta la inutilización total del sitio.

Este es el motivo por el cual Symantec™ Complete Website Security somete todo el entorno de su sitio web (páginas, aplicaciones, software de servidor y puertos de red) tanto a evaluaciones de vulnerabilidades semanales como a análisis diarios contra código dañino. Las evaluaciones semanales pueden revelar vulnerabilidades que deben subsanarse urgentemente si no se quiere ser víctima de la ciberdelincuencia. Proporcionan informes exhaustivos donde se detallan todas las vulnerabilidades: tanto las críticas que requieren su intervención inmediata como los riesgos de menor importancia que pueden esperar a la siguiente actualización que tenga programada. Una vez instalados los parches pertinentes, tiene la opción de repetir el análisis y comprobar si se han eliminado las vulnerabilidades.

Los análisis diarios contra el código dañino lo ayudan a asegurarse de que sus sitios web están libres de malware. Además, una vez que tenga el sello Norton Secured instalado, y siempre que los resultados del análisis concluyan que no tiene código dañino, este se mostrará de forma automática en sus sitios.

El sello Norton Secured ofrece a los clientes otro signo evidente de que su empresa hace todo lo posible por proteger su privacidad y su seguridad en Internet. El sello Norton Secured es visto más de quinientos millones de veces al día en sitios web de más de 170 países, en los resultados de las búsquedas (en los navegadores compatibles) y en las tiendas de comercio electrónico y las páginas de análisis de productos de nuestros socios. El sello Norton Secured es una de las marcas de confianza más reconocibles por los consumidores.

El 90 %[5] de los encuestados manifestó que era más probable que continuaran con un proceso de compra electrónica si lo veían.

[5] Estudio internacional del consumidor en línea: Estados Unidos, Alemania, Reino Unido, Julio 2013

Criptografía de curva elíptica

Una alternativa más moderna al sistema estándar de cifrado RSA que se suele utilizar en los certificados SSL tradicionales es la criptografía de curva elíptica (ECC). El cifrado ECC de 256 bits no solo emplea un algoritmo de cifrado más avanzado 64 000 veces más difícil de romper que el del RSA de 2048 bits estándar, sino también su clave es mucho más pequeña (solo 256 bits de longitud) y requiere un número de ciclos de CPU inferior para cifrar los datos. Esto puede ayudarlo a reducir costos y mejorar el funcionamiento del sitio. Gracias a nuestros certificados SSL/TLS híbridos, tiene la posibilidad de combinar la ubicuidad de la raíz RSA con las ventajas de la criptografía de curva elíptica, que proporciona mayor seguridad y mejor rendimiento en el servidor.

Tras implementar la tecnología ECC en su empresa, Directorz Co. Ltd., un cliente de Symantec de Japón, constató que la carga de la CPU era un 46 % inferior y el tiempo de respuesta del sitio web, un 7 % más rápido.

Solución de autoridad de certificación privada

Symantec™ Complete Website Security ofrece la solución de autoridad de certificación privada con el objetivo de reducir los riesgos, errores y costos ocultos asociados a las autoridades de certificación autofirmadas. Esta solución mejora tanto la seguridad como la visibilidad gracias a la consolidación de la administración de los certificados públicos y privados en una sola consola. Además, puede seguir utilizando los nombres de los servidores internos sin preocuparse de las migraciones asociadas a las raíces públicas para crear una jerarquía personalizada basada en sus propias necesidades.

Protección frente a ataques DDoS*

Symantec™ Complete Website Security también incluye protección frente a ataques DDoS para que pueda neutralizar los ataques que suelen perpetrarse contra servicios electrónicos de todo tipo. Esta defensa protege de los ataques DDoS a nivel de aplicación actuando frente a las vulnerabilidades de los sistemas operativos o aplicaciones web que normalmente son inmunes a los filtros genéricos. Las funciones automáticas de detección y activación del modo «ataque en curso» garantizan nuestra respuesta lo más rápido posible y una recuperación con una interrupción mínima del servicio.
* Powered by Imperva Incapsula.

Firewall de aplicaciones web (WAF)

Symantec™ Complete Website Security ofrece un innovador firewall en la nube que protege los servidores de su sitio web de los ataques a la capa 7. El firewall WAF defiende contra todas las amenazas de la lista de OWASP Top 10, tales como la inyección de SQL, las secuencias de comandos entre sitios, el acceso ilegal a los recursos o la inclusión remota de archivos, y ofrece un método de defensa proactivo mediante vigilancia permanente y aplicación de medidas de seguridad específicas. Para activar el WAF solo se necesita hacer un simple cambio en el DNS.

Distribución optimizada de contenido a través de CDN

Además de la seguridad de varios niveles, ahora Symantec™ Complete Website Security también incluye una red de distribución de contenidos (CDN) global que tiene en cuenta las aplicaciones para acelerar el funcionamiento general del sitio. Este sistema global de servidores situados estratégicamente acerca el contenido de su sitio web a sus clientes ayudándolo a cargar y funcionar más rápido. Según estudios recientes, los sitios web que utilizan herramientas de optimización de la red y almacenamiento en caché de contenido estático y dinámico funcionan un 50 % más rápido en promedio y consumen un ancho de banda hasta un 70 % inferior.

Asistencia ininterrumpida

Con el servicio ininterrumpido de soporte técnico de Symantec, sabe que está en buenas manos porque recibirá la ayuda que necesita en el momento y el lugar en que la necesita.

Tendrá a su disposición siete días a la semana un gestor personal de asistencia técnica que se ocupará de:

- monitorear y priorizar sus incidencias;
- 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, y
- derivar las incidencias a quien corresponda.

Servicio por suscripción sencillo, flexible y previsible

Symantec™ Complete Website Security es un servicio de seguridad de sitios web flexible pensado para que pueda centrarse en su negocio sin tener que preocuparse por los costos y los problemas de administración a lo largo del año.

Dispone dos modelos de suscripción, uno anual y otro multianual, sin costos adicionales —se lo garantizamos— para que pueda prevenir el gasto total anual sin temor a equivocarse. Por un precio fijo y un plazo también fijo, su empresa disfruta de acceso flexible a todos los servicios que necesita, cuando y donde los necesita con una sola orden de compra.

Symantec™ Complete Website Security

Symantec Complete Website Security le ofrece los niveles de visibilidad, agilidad y seguridad que necesita para proteger su negocio, su reputación y sus clientes. Armoniza y refuerza la seguridad de su sitio web gracias a un completo catálogo de soluciones de primera línea. La protección de varios puntos y varias capas puede ayudarlo a mantener su ecosistema web a salvo hasta de las amenazas más sofisticadas conforme surgen. La visibilidad en tiempo real sobre su ecosistema web le permite detectar problemas antes de que sea demasiado tarde, neutralizar ataques, arreglar errores y observar las políticas de seguridad. Incluye las herramientas y servicios que necesita para salvaguardar la integridad y el rendimiento de los servidores, certificados y aplicaciones de sus sitios web. Su agilidad le asegura tanto la protección como el crecimiento controlados de su empresa en el menor tiempo posible. Esta tecnología, que está avalada por uno de los líderes en ciberseguridad, incorpora la marca de confianza más reconocible de la web y pertenece a una de las redes de ciberinteligencia mejor equipadas, puede confiar en que tendrá los niveles de seguridad, servicio y soporte que necesita para blindar el entorno de su sitio web, sus clientes y su negocio.

Symantec. Website Security.
We go beyond

Symantec™ Complete Website Security

Para recibir información sobre productos, llame al:
América Latina: +1 520 477 3111
España: 900 93 1298

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/complete-website-security

Symantec España
Parque Empresarial La Finca – Somosaguas,
Paseo del Club Deportivo,
Edificio 13, oficina D1, 28223,
Pozuelo de Alarcón, Madrid, España
900 93 1298
www.symantec.com/es/es/complete-website-security

Enero de 2017