



Implantación de Websense TruHybrid

ThreatSeeker Network es una red global que analiza amenazas de seguridad potenciales mediante el empleo de avanzadas técnicas de análisis de comportamiento y de reputación en tiempo real. Envía los últimos descubrimientos en materia de seguridad al motor de clasificación avanzada, que forma parte de las soluciones de seguridad web, del correo electrónico y de prevención de fuga de información de Websense.

Al emplear un modelo de análisis de contenidos unificado, Websense ofrece protección en tiempo real contra amenazas emergentes y combinadas, sin importar dónde residan. Los clientes se evitan el coste y la complejidad que representan las soluciones de seguridad puntuales, obtienen mejores funcionalidades de cumplimiento de las normativas y disfrutan de la capacidad de habilitar nuevas tecnologías de colaboración y comunicación basadas en la web.

Plataforma unificada

Una infraestructura moderna de redes empresariales se extiende mucho más allá de un único emplazamiento: también debe abarcar las oficinas de las sucursales y a los trabajadores móviles. Websense se enfrenta a este reto con una solución híbrida que integra plataformas de provisión basadas en la nube y de implantación en los sistemas de la empresa. Las empresas pueden optar libremente por una única plataforma o por implantar la combinación que mejor se adapte a sus necesidades. Así, una plataforma unificada permite a los administradores reducir la complejidad, aprovechar al máximo la infraestructura existente y eliminar los gastos generales de administración; y todo ello mientras reducen el coste total de propiedad.

Appliance Websense V-Series™: extensible, sencilla y potente

El appliance V-Series ofrece una mezcla única de flexibilidad, rendimiento y sencillez. Los appliances V-Series reducen de forma significativa el tiempo de implantación y el coste operativo para los clientes de Websense, pero al mismo tiempo son lo suficientemente escalables como para adaptarse incluso a los mayores entornos empresariales. El appliance V-Series se integra perfectamente en la plataforma de seguridad como servicio (SaaS) de Websense y, de ese modo, ofrece a los clientes más opciones para implantar y gestionar sus soluciones de seguridad de contenidos.

Seguridad como servicio: rápida, sencilla y eficaz

SaaS de Websense ofrece una ruta de implantación rápida para productos Websense. SaaS traslada los procesos de inspección, aplicación y administración de seguridad del emplazamiento del cliente a 10 centros de datos en la nube disponibles a escala global. Los clientes obtienen todas las ventajas de la solución de seguridad de contenidos líder en el sector e incluso se libran del engorro que representa implantar y actualizar hardware en los sistemas de la empresa.



Habilitar su empresa de forma segura

Puesto que más empresas buscan ganar margen competitivo con las actuales tecnologías Web 2.0 dinámicas, sus soluciones de seguridad también deben mejorar para poder hacer frente a nuevos desafíos. Websense tiene la respuesta y ofrece la primera y única solución de seguridad de contenidos unificada del sector.

Con Websense, las organizaciones pueden construir una infraestructura de seguridad exhaustiva que ofrezca protección integral contra amenazas de seguridad web, del correo electrónico y de la información. Las organizaciones son capaces de minimizar su exposición a riesgos de seguridad, maximizar la productividad y hacer posible la innovación; y todo ello sin introducir nuevas fuentes de gastos, complejidad y gastos generales de administración. Una solución de seguridad de contenidos unificada permite a las empresas derribar las barreras para permitir la entrada a la innovación y a la habilitación de nuevas tecnologías de vital importancia.

Sedes Corporativas:

Websense, Inc.
San Diego, CA USA
tel 800 723 1166
fax 858 458 2950
www.websense.com

Websense UK Ltd.
Reading, Berkshire UK
tel 0118 938 8600
fax 0118 938 8698
www.websense.co.uk

Websense Ireland
Dublin Ireland
tel 01 6319360
fax 01 6319001
www.websense.com

Websense Singapore
Singapore
tel 6736 7467
fax 6248 4531
www.websense.com/apac

Websense Spain
Madrid, Spain
tel +34 91 28 44 750
fax +34 91 28 44 751
www.websense.es

Resto de sitios

www.websense.com/international

Delegaciones:

Australia websense.com.au	Italia websense.it
Brasil websense.com/brasil	Japón websense.jp
Colombia websense.com/latam	Malasia websense.com
Francia websense.fr	México websense.com/latam
Alemania websense.de	PRC prc.websense.com
Hong Kong websense.cn	Singapur websense.com
India websense.com	España websense.com.es
Irlanda websense.co.uk	Taiwán websense.cn
Israel websense.co.uk	UAE websense.com

Solución unificada

TRITON combina en una única interfaz las funcionalidades de administración y de generación de informes para tecnologías web, del correo electrónico y de prevención de fuga de información de Websense, ofreciendo así mayor flexibilidad, control y mejores funcionalidades de administración. La consola Websense TRITON permite a los usuarios establecer políticas, gestionar incidentes, ejecutar informes y realizar tareas administrativas desde un administrador central basado en la web.

Seguridad Web

Websense Web Security Gateway inspecciona el contenido entrante y saliente, y protege a las empresas contra malware web dinámico, previene la fuga de información confidencial y mejora la productividad de los empleados. La implantación de TruHybrid™ es compatible con appliances de implantación en los sistemas de la empresa y con SaaS al tiempo que administra todo el entorno desde una sola infraestructura de políticas y de generación de informes. A diferencia de otros enfoques, los clientes de Websense pueden optar libremente por una implantación que se adapte a sus requisitos operativos específicos sin verse obligados a gestionar múltiples sistemas o a tratar con múltiples proveedores.

Websense Web Security Gateway se puede implantar como software en los sistemas de la empresa, como el appliance Websense V-Series, como SaaS o como una oferta híbrida.

Seguridad del correo electrónico

Con las soluciones de seguridad del correo electrónico de Websense, los clientes pueden implantar seguridad de vital importancia y desarrollar una estrategia de seguridad consolidada con el líder de confianza en Essential Information Protection™.

La solución de seguridad del correo electrónico de Websense protege contra amenazas que combinan la web y el correo electrónico, como, por ejemplo, la fuga de información y el incumplimiento de las normativas. Sólo la solución de seguridad del correo electrónico de Websense ofrece cumplimiento de las normativas y seguridad del correo electrónico con apoyo de la inteligencia de Websense ThreatSeeker Network.

La solución de seguridad del correo electrónico de Websense está disponible como software de implantación en los sistemas de las empresas, como plataforma basada en la nube o de seguridad como servicio (SaaS), o como opción de implantación híbrida.

Prevención de fuga de información de Websense

Websense ofrece la tecnología de prevención de fuga de información líder en el sector diseñada para identificar, controlar y proteger información confidencial. Las soluciones de prevención de fuga de información de Websense, que aprovechan el análisis de contenidos unificado que ofrecen las tecnologías de seguridad web y de prevención de fuga de información de Websense, previenen de forma precisa la fuga de información, protegen los procesos empresariales y administran el riesgo y el cumplimiento de las normativas.

Websense adopta un enfoque modular para hacer frente a las amenazas de fuga de información. Su solución ofrece un grado de visibilidad sin rival con respecto a quién está enviando información confidencial, qué tipo de información se está enviando y adónde se dirige dicha información. Las soluciones de prevención de fuga de información de Websense capacitan a las organizaciones para que puedan hacer frente a problemas de fuga de información a un bajo coste y de una forma más fácil que las soluciones de la competencia.

Websense es la primera y única empresa en ofrecer una plataforma de seguridad de contenidos completa que une todos estos elementos en una única solución totalmente integrada. Una solución unificada garantiza una definición y aplicación coherentes de políticas, permite que un administrador adopte una postura en materia de seguridad que satisfaga las necesidades específicas de una organización, reduce la complejidad y los gastos generales de administración, y permite un ahorro inmediato comparado con un enfoque que se base en herramientas de administración redundantes y de múltiples proveedores.

Para obtener una versión de evaluación gratuita de cualquier producto Websense o para ver nuestras demostraciones en línea, vaya a www.websense.com/evaluations.

websense®
ESSENTIAL INFORMATION PROTECTION™



Proteger a la empresa sin fronteras

Solución Websense TRITON™

El lugar de trabajo Web 2.0: Nuevas oportunidades y nuevos riesgos

Las tecnologías habilitadas para la web están transformando la empresa moderna. Potentes herramientas para los negocios basadas en la nube como SalesForce.com y Workday ofrecen nuevas formas de crear, compartir y gestionar información. Aplicaciones Web 2.0 como Google Docs y Zoho han transformado el escritorio de la empresa mientras que blogs, wikis y sitios de redes sociales ofrecen nuevas y revolucionarias funcionalidades de colaboración.

Estas innovaciones hacen posible un nuevo tipo de empresa sin fronteras: más rápida, ágil y receptiva que nunca. Pero también introduce nuevos riesgos de seguridad peligrosos.

Los sitios basados en contenido Web 2.0 –como, por ejemplo, los principales destinos en línea actuales– son excepcionalmente vulnerables a amenazas de seguridad agresivas y que se mueven con rapidez. Un personal de ventas que trabaje con sitios de redes sociales como LinkedIn y Facebook puede estar expuesto a explotaciones basadas en secuencia de comandos diseñadas para transmitir infecciones por malware. Los artistas del fraude suelen apuntar a ejecutivos con sofisticados ataques de “spear-phishing” (phishing con arpón) y ataques transmitidos a través del spam. Los empleados pueden visualizar contenido inapropiado o publicar datos confidenciales del negocio y generar así importantes riesgos relacionados con la responsabilidad y el cumplimiento de las normativas.

Las soluciones de seguridad tradicionales no se diseñaron para hacer frente a estas amenazas. Los ataques que combinan la web y el correo electrónico eluden fácilmente las herramientas antimimalware autónomas. Las herramientas de filtrado de URL y las basadas en la reputación pueden detener las amenazas de ayer, pero no tienen la velocidad y agilidad necesarias para identificar amenazas relacionadas con contenido en línea dinámico o ataques contra sitios Web 2.0 legales. Las soluciones de seguridad puntuales de todo tipo dejan huecos que aprovechan los agresores.

Las empresas también deben considerar los gastos relacionados con las soluciones de seguridad puntuales heredadas. La superposición de productos, los múltiples proveedores y los sistemas redundantes de administración y de generación de informes aumentan los costes de propiedad al tiempo que reducen el rendimiento de la inversión. Las amenazas de seguridad cambiantes y que evolucionan rápidamente requieren más software, hardware e inversiones en infraestructura, lo cual va incrementando el coste y la complejidad. El batiburrillo de soluciones de seguridad resultante impone desafíos adicionales de administración e integración, sin que por ello la postura global en materia de seguridad de una empresa mejore de forma significativa.

La única respuesta a este dilema es una solución de seguridad unificada y completamente integrada. Una solución de estas características hará frente a las amenazas de seguridad web y del correo electrónico relacionadas con las nuevas herramientas de comunicación y colaboración. Reducirá el riesgo de perder valiosos datos del negocio por ataques externos y filtraciones internas. Eliminará la complejidad que supone implantar, gestionar y mantener múltiples productos de seguridad heredados.

Pero, por encima de todo, una solución de seguridad de contenidos unificada ofrecerá un mayor grado de protección contra las amenazas modernas a un coste total de propiedad inferior. Posibilita la innovación sin renunciar a la seguridad.



TRITON™

Es una solución de seguridad moderna gracias a la inteligencia de Websense TruContent™, el primer y único sistema que unifica la visibilidad y el análisis de contenidos hasta el nivel de la información a medida que esta entra y sale de una organización. Las organizaciones pueden prevenir las amenazas de Internet entrantes y dinámicas, controlar el contenido no autorizado, asegurar la productividad y detener de forma efectiva la fuga de información saliente por canales clave de intercambio de información como son la web y el correo electrónico.

Reduce los costes de seguridad porque ofrece el primer modelo de administración entrante y saliente unificada, de generación de informes y de implantación del sector para tecnologías de seguridad de contenidos con funcionalidades de implantación adheridas a la red, de seguridad como servicio y de Websense TruHybrid™. Ello permite a las organizaciones aumentar la flexibilidad de implantación y cobertura, y al mismo tiempo reducir la complejidad, los gastos generales y el coste que supone gestionar distintos sistemas y enfoques de implantación.

TRITON ofrece la mejor protección contra amenazas modernas al coste total de propiedad más bajo.

La solución es la seguridad de contenidos unificada

La primera solución de seguridad de contenidos unificada del sector Websense® TRITON™ es la primera y única solución de seguridad de contenidos unificada del sector porque es la mejor solución de seguridad moderna para amenazas entrantes y riesgos salientes, y todo ello combinado con el coste total de propiedad más bajo. Websense protege a la empresa moderna incluso si su infraestructura se disuelve y los usuarios, la información y las aplicaciones se trasladan a la web.

Con Websense TRITON, las organizaciones:

Obtienen la mejor solución de seguridad moderna para

- Aprovechar la potencia de las nuevas herramientas web sociales, de comunicación y colaboración como Facebook, LinkedIn, Twitter y otros servicios basados en la nube, sin amenazas de malware, nuevos ataques basados en la web que eluden el software antivirus y sin contenido inapropiado ni fuga de información confidencial.
- Proteger el uso de aplicaciones en línea y de seguridad como servicio (SaaS) sin perder visibilidad y control sobre la información.
- Detener ataques combinados que aprovechan la web y el correo electrónico para comprometer a usuarios, infectar sistemas y robar información.

Consiguen el coste total de propiedad más bajo

- Fusionando la administración de la web, del correo electrónico, del control de aplicaciones y de la prevención de fuga de información en una consola unificada para la seguridad en toda la organización.
- Fusionando la infraestructura de appliances de seguridad y utilizando SaaS para reducir el coste y la complejidad y, al mismo tiempo, ampliar el grado de cobertura y visibilidad.
- Cubriendo a trabajadores móviles, sitios distribuidos y sitios centrales con controles continuos a través de una consola de administración y de generación de informes.

Websense TRITON es la primera y única solución que ofrece seguridad de contenidos realmente unificada, diseñada para reducir drásticamente los costes administrativos y de implantación y, al mismo tiempo, ofrecer un nivel de protección líder en el sector. Esta solución de Websense incluye la administración de políticas unificada para implementaciones en los sistemas de la empresa y basadas en la nube que abarcan la seguridad web y del correo electrónico, así como la prevención de fuga de información. Su arquitectura de implantación híbrida abarca toda la empresa global porque combina appliances de alto rendimiento en la sede central corporativa con SaaS en las oficinas remotas y de las sucursales.

Websense TRITON ofrece una serie de funcionalidades únicas:

Una arquitectura de implantación híbrida, rápida y flexible que permite a las empresas proteger las oficinas remotas y a los trabajadores móviles de forma tan efectiva como una sede central corporativa. Con una implantación híbrida:

- Los administradores de seguridad establecen políticas utilizando una única interfaz unificada.
- Los administradores de red utilizan una infraestructura de red rentable basada en la nube.
- Los ejecutivos de TI administran el riesgo y consiguen una mayor cobertura de seguridad a un coste total de propiedad inferior.

Una solución de prevención de fuga de información integrada y totalmente escalable que combina la inspección de inspección de contenidos salientes de primera clase con las soluciones de seguridad web y del correo electrónico entrante líderes en el sector. Este enfoque ofrece las funcionalidades de control de contenidos granular y en profundidad relacionadas con completas herramientas de prevención de fuga de información integradas en una única solución de seguridad web, del correo electrónico o combinada. Con la prevención de fuga de información integrada:

- Los administradores de seguridad implementan una sola arquitectura de seguridad de contenidos unificada.
- Los administradores de red eliminan la necesidad de actualizaciones de infraestructura costosas.
- Los ejecutivos de TI evitan el coste y la complejidad relacionados con soluciones de múltiples proveedores.

Administración de políticas y generación de informes unificadas que permiten alcanzar el máximo nivel de control y flexibilidad comparado con soluciones puntuales de múltiples proveedores. Una única interfaz de administración controla las políticas de seguridad web, del correo electrónico y de la información de la empresa, y avanzadas herramientas de generación de informes totalmente personalizables ofrecen visibilidad con respecto a las operaciones de seguridad de una organización. Con la administración de políticas y la generación de informes unificadas:

- Los administradores de red obtienen visibilidad con respecto al uso de la infraestructura de una empresa.
- Los administradores de seguridad racionalizan el proceso de definición y administración de políticas.
- Los ejecutivos de TI obtienen herramientas en tiempo real para controlar métricas de seguridad clave, identificar tendencias y aplicar directivas de cumplimiento de las normativas.

La arquitectura de TRITON es rápida, flexible y potente

TRITON lanza las tecnologías de seguridad web, del correo electrónico y de prevención de fuga de información líderes en el sector como una única solución de seguridad de contenidos que combina una arquitectura integrada con una potencia y flexibilidad excepcionales. La combinación resultante de tecnologías de Websense ofrece un potente y exclusivo conjunto de funcionalidades de seguridad interrelacionadas.

Análisis de contenido unificado

El motor de clasificación avanzada Websense TRITON ofrece una infraestructura de análisis de amenazas en tiempo real para la solución TRITON. El motor de clasificación avanzada, que utiliza Websense ThreatSeeker® Network, combina múltiples métodos de análisis, como, por ejemplo, el filtrado de URL, antivirus, servicios de reputación, tatuaje numérico de la información, entre otros, para clasificar de forma dinámica el contenido entrante y saliente.

Más que basarse en métodos de detección heredados orientados a los archivos y a las bases de datos, el motor de clasificación avanzada hace un análisis multipunto que evalúa las intenciones de los usuarios, los sitios web, las secuencias de comandos y el código ejecutable. Por ejemplo: si el sitio de un banco utiliza Javascript de forma que parezca un ataque basado en secuencia de comandos, el motor de clasificación avanzada identifica en el acto esta actividad potencialmente peligrosa y la puede prevenir.



“Websense es líder absoluto en el mercado de suites de seguridad de contenidos por su actual funcionalidad y estrategia de producto orientada a suites.”

Informe independiente: “The Forrester Wave™: Content Security Suites, Q2 2009” [Forrester Wave™: suites de seguridad de contenidos, T2 de 2009],

Forrester Research, Inc.,
abril de 2009