

websense®

TRITON® AP-ENDPOINT



websense
TRITON®
AP-ENDPOINT

Detenga las amenazas avanzadas y proteja la información confidencial de los usuarios remotos

La fuga de datos puede tener consecuencias devastadoras, desde una reputación dañada hasta multas y sanciones reguladoras. Proteger a los usuarios contra las amenazas y el robo de datos sigue siendo un desafío de TI sumamente significativo. TRITON AP-ENDPOINT protege a los usuarios remotos contra amenazas avanzadas y contra el robo de datos mientras están dentro y fuera de la red con una solución fácil de usar. Las tecnologías avanzadas le permiten identificar rápidamente la información confidencial y protegerla, brindándole información forense que puede utilizarse para actuar en respuesta a ataques a las terminales dentro y fuera de la red. TRITON AP-ENDPOINT de Websense protege sus datos y permite que sus trabajadores móviles realicen sus tareas donde sea que se encuentren y cuando lo necesiten.

Websense® potencia la seguridad de sus dispositivos finales

- Proteja la información confidencial en los dispositivos finales de Microsoft Windows y Mac OS X que se encuentren fuera de su red.
- Proteja las terminales que se encuentran fuera de su red contra las amenazas avanzadas.
- Protéjase contra las posibles amenazas entrantes o de los datos salientes ocultos en el tráfico de SSL procedente de todos sus dispositivos finales.
- Comparta los datos de forma segura con sus socios usando la encriptación de datos integrada basada en archivos.
- Adopte servicios en la nube como Microsoft Office 365 y Box con seguridad y confianza.
- Demuestre fácilmente los controles de seguridad a los auditores y ejecutivos para cumplir con los requisitos reglamentarios.

Capacidades de TRITON® AP-ENDPOINT

Habilite a usuarios remotos fuera de la red

A menudo los usuarios requieren acceso a información confidencial mientras operan de forma remota. TRITON AP ENDPOINT le brinda los controles necesarios para evitar el robo de datos en computadoras portátiles con MAC OS X y Microsoft Windows, con esto usted podrá habilitar a estos usuarios de forma segura. Detecta y protege los datos de importancia crítica que se alojan en los dispositivos finales, ya sea que el usuario se encuentre dentro o fuera de la red de su organización, también incluye potentes capacidades de impresión digital de datos que rara vez forman parte de las soluciones de DLP para las terminales.

El uso seguro de la web acompaña a sus usuarios remotos

Los riesgos de ataques basados en la web, incluidas las amenazas avanzadas, son incluso mayores para los usuarios que operan fuera del alcance de la red de su organización. TRITON AP-ENDPOINT extiende la seguridad en el uso de la web a los usuarios remotos, permitiéndoles un acceso seguro a recursos disponibles. Con un filtrado de URL sumamente simple, la actividad de ataque se puede identificar y bloquear a través de la cadena de ataque, aún cuando el usuario esté trabajando en un entorno libre de proxy. TRITON AP-ENDPOINT controla el tráfico de SSL protegiendo el canal de la web para sus usuarios remotos, incluso cuando éstos se encuentren usando el correo electrónico y las redes sociales en la nube u otros servicios que emplean conexiones seguras.

Adopte la innovación con seguridad y confianza

Para satisfacer las necesidades de sus clientes y seguir siendo competitivo, usted necesita innovar y permitir que sus empleados adopten nuevas soluciones y tecnologías. TRITON AP-ENDPOINT le permite adoptar de forma segura nuevos servicios en la nube como Microsoft Office 365 o Box, ya que le ofrece defensas contra ataques en la web y la capacidad de conservar el control de los datos confidenciales. Todos los usuarios de terminales con Microsoft Windows o Mac OS X, tanto dentro como fuera de la red que trabajen en cualquier momento y en cualquier lugar, reciben todos los beneficios de prevención de la pérdida de datos (DLP, Data Loss Prevention) y de las defensas contra amenazas avanzadas. Controle el uso de los medios extraíbles, como unidades de USB con opciones para bloquear o codificar los datos identificados por política. De igual manera controle el flujo de datos hacia los servicios en la nube y, al mismo tiempo, realice todas las innovaciones que sean necesarias para contribuir al crecimiento de su organización.

Gestione fácilmente con el personal de TI con que cuenta actualmente

Los desafíos más importantes en cuanto al personal dentro del área de TI, son el limitado número de recursos humanos y la dificultad para encontrar personal capacitado en materia de seguridad. La arquitectura de TRITON unifica la administración de la seguridad en el uso de la web, el correo electrónico, los datos y los dispositivos finales, además incluye políticas que se pueden definir e implementar fácilmente donde sea necesario. Responda rápidamente frente a las nuevas amenazas procedentes de múltiples canales y proteja también a los usuarios remotos. Proteja sus datos confidenciales de IP y PII y cumpla al mismo tiempo con sus requisitos reglamentarios mediante una extensa biblioteca de políticas predeterminadas.



Websense fue el único proveedor que pudo darnos los controles de política necesarios tanto para hacer un uso seguro de la web, como para evitar la pérdida de datos y así poder realizar nuestras operaciones de forma segura”.

- Larry Whiteside, CISO Visiting Nurse Service, New York

Características clave de TRITON AP-ENDPOINT

- Soporte para impresión digital (incluida la impresión digital parcial) para dispositivos finales dentro y fuera de la red.
- Compatible con Mac OS X y Microsoft Windows.
- Protege los datos confidenciales enviados a dispositivos USB, medios extraíbles, impresoras o servicios en la nube como Microsoft Office 365 y Box.
- Política basada en encriptación de archivos para proteger los datos confidenciales almacenados en medios extraíbles.
- Detecte los registros de IP y del cliente que se envían usando clientes de correo electrónico y correo web.
- Con su DLP “por goteo” (Drip DLP) evalúa la actividad de transmisión acumulativa de datos en el transcurso del tiempo para descubrir fugas de pequeñas cantidades de datos.
- Controla eficientemente el tráfico de HTTP y su flexibilidad le permite decidir qué tipo de tráfico de SSL inspeccionar.
- Identifica actividad en la web que implica una amenaza avanzada a través de toda la cadena de ataque en terminales que operan fuera del alcance de las defensas de la red.

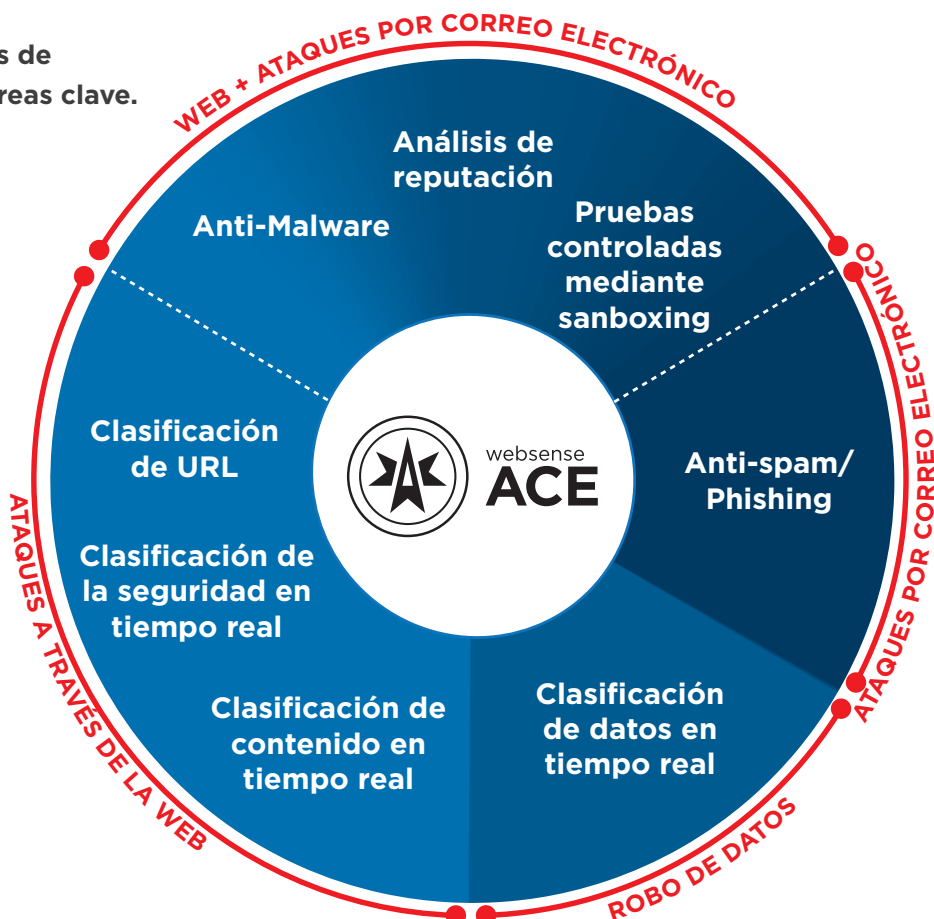
El poder que respalda las soluciones TRITON

Motor de clasificación avanzada ACE (Advanced Classification Engine)

Websense ACE proporciona defensas contextuales en línea, en tiempo real para la seguridad de la web, correo electrónico, de datos y seguridad móvil, utilizando la calificación de riesgos compuesta y el análisis predictivo, para así proporcionar seguridad más eficaz a la que se puede tener acceso actualmente. Brinda también contención a través del análisis del tráfico entrante y saliente con defensas atentas a los datos, proporcionando protección líder en la industria contra el robo de datos. Los clasificadores de seguridad en tiempo real y análisis de contenido y de datos, son el resultado de muchos años de investigación y desarrollo, los cuales permiten que ACE detecte todos los días más amenazas que los motores de antivirus tradicionales (la prueba se actualiza todos los días en <http://securitylabs.websense.com>). ACE es la principal defensa detrás de todas las soluciones Websense TRITON y cuenta con el respaldo de Websense ThreatSeeker Intelligence Cloud.

Set integrado de capacidades de evaluación de defensa en 8 áreas clave.

- 10,000 análisis disponibles para respaldar inspecciones profundas.
- Motores de seguridad predictivos que anticipan muchos movimientos.
- La operación en línea no solo monitorea, sino que además **bloquea** las amenazas.



ThreatSeeker® Intelligence Cloud

ThreatSeeker Intelligence Cloud, administrada por Websense Security Labs™, proporciona la inteligencia central de seguridad colectiva para todos los productos de seguridad Websense. Une más de 900 millones de dispositivos finales, incluyendo información de Facebook y; junto con las defensas de seguridad de Websense ACE, analiza más de 5 mil millones de solicitudes por día. Este extenso reconocimiento de amenazas de seguridad permite a ThreatSeeker Intelligence Cloud ofrecer actualizaciones de seguridad en tiempo real que bloquean amenazas avanzadas, malware, ataques de phishing, señuelos y estafas, además de proporcionar las últimas calificaciones web. No hay nada que pueda igualar a ThreatSeeker Intelligence Cloud en cuanto a su tamaño y al uso de las defensas en tiempo real de ACE para analizar ingresos colectivos de datos. Cuando se actualiza a Web Security, ThreatSeeker Intelligence Cloud lo ayuda a reducir el grado de exposición a las amenazas a través de la web y al robo de datos.

Arquitectura TRITON

Con la mejor seguridad en su clase, la arquitectura unificada de Websense TRITON ofrece protección a solo un clic de distancia, con defensas en línea en tiempo real de Websense ACE. Las inigualables defensas en tiempo real de ACE cuentan con el respaldo de Websense ThreatSeeker Intelligence Cloud y con la experiencia de los investigadores de Websense Security Labs. El poderoso resultado es una arquitectura unificada y simple, con una sola interfaz para el usuario e inteligencia de seguridad unificada.

TRITON APX

TRITON APX ofrece muchos beneficios clave a las organizaciones interesadas en implementar la mejor protección posible contra las amenazas avanzadas que se registran a lo largo de las 7 etapas de la cadena de ataque (Kill Chain). Éstas se pueden resumir en tres enunciados:

- **Implemente soluciones:** De seguridad adaptables para una tecnología en constante cambio y con panoramas amenazantes.
- **Proteja todos los frentes:** Los datos determinan el perímetro. Proteja la información crítica contra el robo, ya sea en las instalaciones, en la nube o en dispositivos móviles.
- **Eleve el coeficiente de seguridad:** Combata la escasez de habilidades de seguridad cibernética proporcionando inteligencia práctica predictiva durante todo el ciclo de vida de la amenaza.

DESAFÍE AL NUEVO MUNDO.

APX www.websense.com/APX

© 2015 Websense, Inc. Todos los derechos reservados. Websense, TRITON, el logotipo de Websense y ThreatSeeker son marcas comerciales registradas de Websense, Inc. en los Estados Unidos y varios países. Todas las demás marcas son propiedad de sus respectivos dueños. [TRITON® AP-ENDPOINT-BROCHURE-A4ESLA-18NOV14]