websense®

APX MÓDULO DE SANDBOXING

TRITON AP-WEB | TRITON AP-EMAIL | TRITON AP-DATA | TRITON AP-ENDPOINT

PREPÁRESE PARA LAS AMENAZAS PERSISTENTES Y LAS AMENAZAS DEL DÍA CERO MÁS AVANZADAS

Las amenazas masivas que existen en el mercado han dado lugar a ataques diseccionados más personalizados. El Módulo Sandboxing de Websense brinda defensas adicionales contra las amenazas persistentes y las amenazas del día cero más avanzadas y direccionadas que atacan a través de los canales de la web o del correo electrónico. La generación de informes forenses y el feedback de la capacitación en materia de phishing fortalecen las medidas proactivas de defensa.

¿POR QUÉ IMPLEMENTAR EL MÓDULO DE SANDBOXING DE WEBSENSE®?

El Módulo de Sandboxing de Websense ofrece mejoras de protección inigualables para las defensas de seguridad en el uso de la web y el correo electrónico de Websense. Los resultados del entorno seguro de comportamiento integrado se evalúan junto con otros análisis del motor de clasificación avanzado ACE (Advanced Classification Engine) de Websense para hacer frente a las técnicas de evasión innovadoras que se presentan, lo que asegura la precisa identificación de las amenazas. Los usuarios móviles interconectados en la red se benefician con un feedback en tiempo real con respecto a las comunicaciones sospechosas por correo electrónico, aún cuando se encuentren trabajando en forma remota. Y los detallados informes forenses y de phishing del entorno seguro les permiten a las organizaciones asumir una postura más proactiva en materia de seguridad para protegerse contra futuros ataques.

> **"El malware hoy es diseccionado, polimórfico y dinámico. Se le puede hacer llegar al destinatario a través de una página web, de ataques de phishing dirigidos por correo electrónico o mediante muchas otras vías de acceso".**
>
> —IDC, Worldwide Specialized Threat Analysis and Protection 2013-2017 Forecast (Pronóstico mundial 2013-2017 de protección y análisis especializado de amenazas) y 2012 Vendor Shares (Acciones del proveedor en 2012), Agosto de 2013Shares, August 2013

EL MÓDULO DE SANDBOXING DE WEBSENSE MEJORA LA DEFENSA EN CINCO ÁREAS:

1. **Sandboxing de archivos para la web**
   Monitoree el tráfico en la web para un análisis de código en tiempo real en un entorno seguro de comportamiento para identificación de amenazas avanzadas.
2. **Sandboxing de archivos para correo electrónico**
   Intercepte adjuntos en tiempo real para realizar un análisis adicional de amenazas en un entorno seguro de comportamiento.
3. **Sandboxing de URL de correo electrónico**
   Evalúe nuevamente los vínculos sospechosos que aparecen en el correo electrónico cuando accede a ellos, no únicamente cuando se recibe el correo electrónico.
4. **Generación de informes forenses detallados**
   Utilice los resultados del sandboxing para orientar las respuestas que resulten necesarias o las medidas proactivas pertinentes para prevenir futuros ataques.
5. **Generación de informes y capacitación en materia de phishing**
   Incremente el nivel de sensibilidad frente al phishing tanto en el usuario como en la red para generar un cambio efectivo.

INFORMES FORENSES DE LAS PRUEBAS CONTROLADAS MEDIANTE SANDBOXING

El Módulo de Sandboxing de Websense ofrece un entorno en línea para evaluar el malware potencial de manera segura. Utilizando los análisis de ACE, toda la actividad es monitoreada y documentada en un informe detallado que incluye:

- El proceso de la infección y la actividad posterior
- Los eventos a nivel del sistema y las modificaciones en los archivos, procesos, registros, etc.
- Las comunicaciones en la red, incluidas las conexiones/métodos utilizados y su destino

El comportamiento observado se pone en relación con las amenazas conocidas para proporcionar conclusiones valiosas que permitan tomar decisiones y actuar.

PODEROSOS ANÁLISIS FORENSES

- Permiten la ejecución segura de códigos sospechosos ajenos a los recursos de la red.
- Sandboxing de investigación utilizado y administrado por los investigadores de Websense.
- La generación de informes forenses detallados brinda valiosa información que permite actuar y tomar decisiones.

websense TRITON® APX ADVANCED PROTECTION

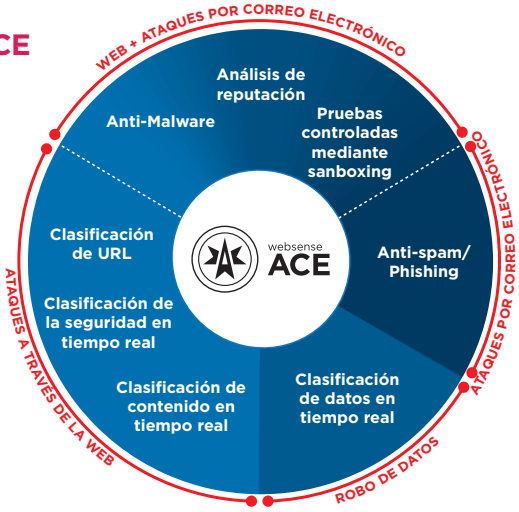
websense

APX MÓDULO DE SANDBOXING

TRITON AP-WEB | TRITON AP-EMAIL | TRITON AP-DATA | TRITON AP-ENDPOINT

LA DIFERENCIA DE WEBSENSE: MOTOR DE CLASIFICACIÓN AVANZADA ACE (ADVANCED CLASSIFICATION ENGINE)

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



SUS NECESIDADES - SOLUCIONES WEBSENSE

INTEGRE LAS SOLUCIONES LÍDERES TRITON® DE WEBSENSE

El Análisis de imágenes de Websense se encuentra disponible como un módulo opcional que se puede agregar a las soluciones TRITON AP-EMAIL y AP-DATA.

PROTEJA LA WEB Y EL CORREO ELECTRÓNICO CONTRA EL MALWARE AVANZADO

Cuando trabaja con TRITON AP-WEB y AP-EMAIL, se activa un código sospechoso en un entorno seguro de comportamiento aislado, lo que permite que se ejecute de forma segura, y que revele cualquier tipo de intención maliciosa. Una vez interceptado el ataque en línea, se alerta a los responsables de IT en tiempo real acerca de las amenazas que se acaban de revelar, y se les proporcionan informes forenses detallados al respecto.

INFORMACIÓN QUE PERMITE ACTUAR A PARTIR DE LA GENERACIÓN DE INFORMES FORENSES

El informe forense del Módulo de Sandboxing brinda detalles tanto acerca de la actividad que se produce durante la infección como de la actividad posterior a esta. Dicha información se puede usar para intensificar las defensas contra los ataques y para identificar y posiblemente recuperar los sistemas infectados.

DEFENSAS INTEGRADAS PARA LOGRAR UNA MÁXIMA EFECTIVIDAD

Los puntos claves que resultan suficientes para lograr un ataque realmente avanzado y con un objetivo específico pueden no residir únicamente en un código malicioso cuidadosamente diseñado. En consecuencia, los resultados del Módulo de Sandboxing de Websense también se evalúan en contexto con un análisis de ACE del vehículo con el que se hizo llegar la infección al destinatario (la web o el correo electrónico).

DEFENSAS AVANZADAS PARA VÍNCULOS EN EL CORREO ELECTRÓNICO

Se modifican las URL sospechosas de manera tal que cuando un usuario hace clic en un vínculo en un mensaje en cualquier dispositivo (por ejemplo, una computadora portátil, un teléfono inteligente, una tableta), la URL se analiza en tiempo real antes de permitir el acceso. A pesar de los otros beneficios, esta ventaja en particular tiene un valor incalculable cuando una página web se encuentra comprometida una vez que el vínculo es originalmente enviado por correo electrónico.

PERSONALICE LAS SITUACIONES DE PHISHING

Tanto los usuarios como el personal de TI reciben información personalizada. La capacitación del usuario y el feedback mantienen a los usuarios alertas a los riesgos, y los informes de TI permiten identificar tendencias que pueden indicar la necesidad de implementar una política, un proceso, u otro tipo de cambios.

DESAFÍE AL NUEVO MUNDO.

MÁS INFORMACIÓN: www.websense.com/APX

websense TRITON® APX ADVANCED PROTECTION