CHECK POINT THREAT EXTRACTION

CHECK POINT THREAT EXTRACTION

Cero Malware en Cero Segundos

Ventajas del producto

- Protección preventiva frente a amenazas conocidas y desconocidas contenidas en documentos enviados por correo electrónico o descargados de la Web
- Entrega instantánea de documentos libres de malware
- Esta flexible protección aborda las necesidades propias de cualquier organización

Características del producto

- Protege documentos PDF y de Microsoft Office
- Elimina contenido “activo” u otros que puedan aprovechar vulnerabilidades de los documentos
- Convierte, para mayor seguridad, archivos reconstruidos a formato PDF, o los mantiene en el formato original dependiendo de la política
- Reconstruye los archivos en aproximadamente un segundo
- Opciones de protección configurables
- Acceso sencillo a los archivos originales según sea necesario

[1] Informe de Seguridad de Check Point 2014

PERSPECTIVAS

Los documentos todavía suponen uno de los riesgos más grandes para las organizaciones hoy en día. El pasado año un 84% de las empresas descargaron un documento malicioso.[1] Sin embargo, en departamentos empresariales típicos como recursos humanos, compras u otros, los empleados deben abrir de forma rutinaria documentos de solicitantes de empleo, clientes o proveedores como parte de sus responsabilidades laborales. Mientras se investigan los mercados, la competencia, y nuevas tecnologías, los empleados normalmente abren documentos descargados de la Web. La mayoría de los empleados abren estos documentos sin considerar las implicaciones, y el riesgo al exponer a sus empresas a posibles amenazas, troyanos y otro malware embebido en su interior.

Las organizaciones necesitan implementar protecciones frente a los riesgos que supone el contenido malicioso de los documentos. El enfoque tradicional de protegerse frente a los documentos infectados buscando el malware y bloqueándolo no proporciona una protección completa. El software antivirus es rápido, pero solo puede capturar malware conocido o "antiguo", y no previene frente a las infecciones dedía cero. Las soluciones de día cero identifican malware "nuevo" desconocido y Amenazas Persistentes Avanzadas (Advanced Persistent Threats - APTs). Sin embargo, este enfoque lleva tiempo y tiene el riesgo de una exposición potencial de la red frente a infecciones antes de que se produzca la detección y el bloqueo correspondiente. Se necesita un nuevo enfoque para abordar estas amenazas y eliminar todo el malware, antes de que tenga la menor oportunidad de llegar a los empleados.

SOLUCIÓN

Check Point Threat Extraction proporciona una nueva aproximación a la hora de eliminar el malware contenido en los documentos descargados de la Web y enviados mediante correo electrónico. Al proporcionar una protección completa frente amenazas eliminando el contenido que, potencialmente, puedan aprovechar las vulnerabilidades, Threat Extraction entrega los documentos libres de malware a sus empleados con una latencia despreciable.

Threat Extraction elimina las amenazas de documentos PDF y de Microsoft Office eliminando el contenido que puede aprovechar una vulnerabilidad, como las macros, objetos y archivos incrustados, y enlaces externos. Los empleados reciben los documentos reconstruidos con elementos que se sabe que son seguros. Con Threat Extraction, las organizaciones pueden proporcionar documentos sin malware alguno en cero segundos.

DOCUMENTOS SIN MALWARE

Los documentos usados en el trabajo diario pueden incluir contenido peligroso, incluyendo macros o enlaces incrustados que pueden aprovecharse para infectar sus equipos y redes. Con Check Point Threat Extraction, las amenazas son eliminadas extrayendo ese contenido y reconstruyéndolo usando elementos que se sabe son seguros, entregando así documentos libres de malware a los destinatarios previstos.

ENTREGA EN CERO SEGUNDOS

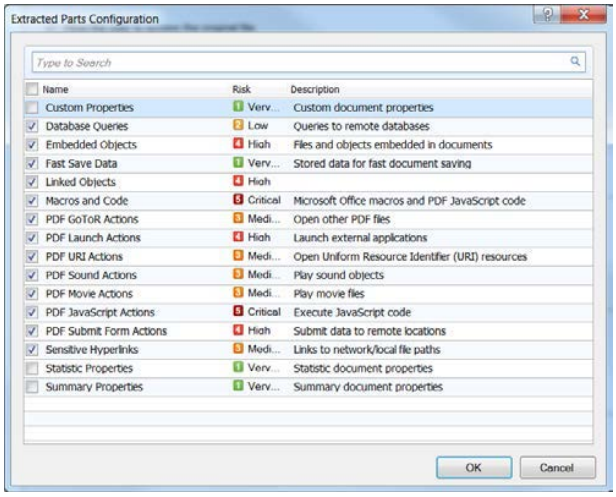
Al contrario que las tecnologías de detección que requieren tiempo para buscar e identificar amenazas antes de bloquearlas, Threat Extraction elimina el riesgo de forma preventiva, asegurando la entrega de documentos seguros en cero segundos.

PROTEGE LOS TIPOS DE ARCHIVOS MÁS COMUNES

Check Point Threat Extraction soporta los tipos de archivo más comunes usados en las organizaciones hoy en día, incluyendo documentos Word, Excel, y Power Point de Microsoft Office, y PDFs de Adobe. Los administradores pueden seleccionar cuáles de estos tipos serán sometidos a Threat Extraction cuando entren en la red a través de correo o de descargas Web.

OPCIONES DE PROTECCIÓN FLEXIBLES

Threat Extraction proporciona flexibilidad a las organizaciones para seleccionar las opciones de protección del documento que mejor se adapten a sus necesidades operativas. Para la mejor protección, nosotros recomendamos reconstruir y convertir los documentos a un formato PDF. De modo alternativo, las organizaciones pueden elegir mantener el formato del documento original, y eliminar el contenido que pueda suponer una amenaza. Esta opción permite a los administradores determinar los tipos de contenido a eliminar, desde macros de alto riesgo a archivos incrustados y enlaces externos.



FÁCIL DE IMPLEMENTAR

Se instala como un Software Blade adicional en el gateway, Threat Extraction se integra en modo Mail Transfer Agent en la red de correo electrónico. Aplique Threat Extraction en toda la organización, o impleméntelo solo para determinadas personas, dominios o departamentos. Los administradores pueden configurar los usuarios y grupos incluidos basándose en sus propias necesidades, facilitando de una forma sencilla su implementación gradual en la organización.

SINCRONIZADO CON THREAT EMULATION

Threat Extraction y Threat Emulation funcionan de forma conjunta para ofrecerle una protección aún más avanzada. Threat Extraction entrega los documentos con cero malware en cero segundos. Threat Emulation analiza el documento original en un sandbox aislado para identificar amenazas desconocidas. Ejecuta este análisis y proporciona visibilidad de los ataques a la organización.

Configure Threat Extraction de una de las dos formas posibles. Proporcionar rápidamente un documento reconstruido al usuario, o configurar Threat Extraction para que espere la respuesta de Threat Emulation antes de determinar si reconstruir o no el documento. Además, el acceso a los archivos originales solo se permite cuando el documento es declarado como no peligroso por Threat Emulation.

EMPAQUETADO PARA LA MEJOR PROTECCIÓN

Con nuestro NGTX, las organizaciones son capaces de aprovechar las protecciones proporcionadas por Threat Extraction, y obtener protección adicional de IPS, Control de Aplicaciones, Filtrado URL, Antivirus, Anti-Bot, Anti-Spam, y Threat Emulation. Esta protección completa guarda a los usuarios de descargar archivos peligrosos, acceder a sitios Web malicioso y detiene las comunicaciones de bots antes de que ocurra el daño.

ESPECIFICACIONES

Característica	Descripción
Tipos de archivos soportados	Microsoft Office 2003-2013, Adobe PDF
Opciones de implementación	• MTA – el gateway recibe todo el correo electrónico entrante, y lo reenvía al siguiente salto tras la inspección • WebAPI - envía los archivos a la máquina para su reconstrucción • Web Browser Extension (extensión para el navegador Web) - soporta la reconstrucción para los archivos descargados
Rendimiento	~1% de descenso en el rendimiento con 8000 usuarios
Versión y SO	Desde R77.30 usando SecurePlatform o GAiA