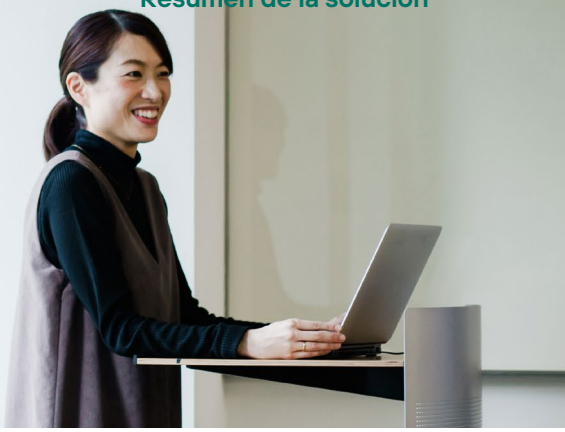
Forcepoint

Resumen de la solución

Desarme y reconstrucción de contenido (CDR) de Zero Trust de Forcepoint para la protección de portales

Cargue el archivo, ¡no la amenaza!



Desafíos

- Detener los ataques de día cero
- Reducir la latencia
- Evitar que el malware llegue a los dispositivos finales

Solución

- Alejarse de la detección: no intente diferenciar entre los datos buenos y malos. El CDR de Zero Trust supone que todos los datos son inseguros u hostiles, lo que se traduce en que solo los datos seguros hagan el recorrido de extremo a extremo.

Beneficios

- La protección para portales garantiza que el contenido que se carga a las aplicaciones de internet siempre esté libre de amenazas, sin que se deba detectar la amenaza o aislar a la empresa del contenido que necesita. Se eliminan las vulnerabilidades de día cero, ransomware, esteganografía, malware sin archivos y las amenazas inherentes en archivos polimórficos.
- Integración fluida con controladores de entrega de aplicaciones, equilibradores de carga/servidores proxy inversos y firewalls de aplicaciones web de los centros de datos existentes.

Las amenazas conocidas, desconocidas y de día cero se ocultan en documentos e imágenes empresariales y se utilizan cotidianamente para introducir malware en las organizaciones. Dentro del amplio rango de flujos de trabajo empresariales, entre los que se incluyen sitios de reclutamiento, portales para ciudadanos y sitios de servicios financieros, las organizaciones necesitan asegurarse de que cuando reciben documentos e imágenes de internet, no carguen a su vez amenazas ocultas en el contenido. Los intentos por invalidar estas amenazas utilizando tecnologías basadas en la detección convencionales y capacidades de sandbox y detonación añaden latencia innecesaria a la empresa, frustran a los usuarios y no eliminan el riesgo que presentan las amenazas desconocidas y de día cero.

Derrote a las amenazas desconocidas

Las tecnologías antimalware existentes brindan una primera línea de defensa, detectando amenazas conocidas al buscar firmas de vulnerabilidades anteriores o comportamientos inseguros. Pero muchas veces, las empresas se ven comprometidas por amenazas de día cero que penetran en la organización antes de que las defensas basadas en detección puedan encontrarlas o son atacadas por amenazas desconocidas que logran su cometido sin que sea posible identificarlas debidamente.

El desarme y reconstrucción de contenido (CDR) de Zero Trust para la protección de portales es la única alternativa para vencer no solo a las amenazas conocidas sino también a aquellas desconocidas y de día cero presentes en los documentos e imágenes empresariales que se cargan a los portales, ya que no confía en las capacidades de detección o sandbox y detonación. En su lugar, emplea un proceso único de transformación que brinda protección integral.

Transforme su seguridad

El CDR de Zero Trust para la protección de portales funciona extrayendo la información empresarial de los documentos e imágenes a medida que llegan al proxy inverso. Los datos que trasladan la información se descartan, junto con cualquier amenaza. Luego, se crean documentos e imágenes nuevos que se entregan a la aplicación de destino. Solo los datos seguros hacen el recorrido de extremo a extremo. Los atacantes no pueden penetrar y la organización obtiene lo que necesita.

Este proceso se conoce como transformación. Es la mejor opción: el equipo de seguridad queda satisfecho porque se eliminó la amenaza y los usuarios de la empresa también lo están porque obtienen la información que necesitan.

El CDR de Zero Trust es la única forma de garantizar que se eliminen las amenazas del contenido. Alejándose de los paradigmas fallidos de la detección y el aislamiento de amenazas, la tecnología única del CDR de Zero Trust de Forcepoint supone que todos los datos son inseguros u hostiles, y no intenta distinguir los buenos de los malos.

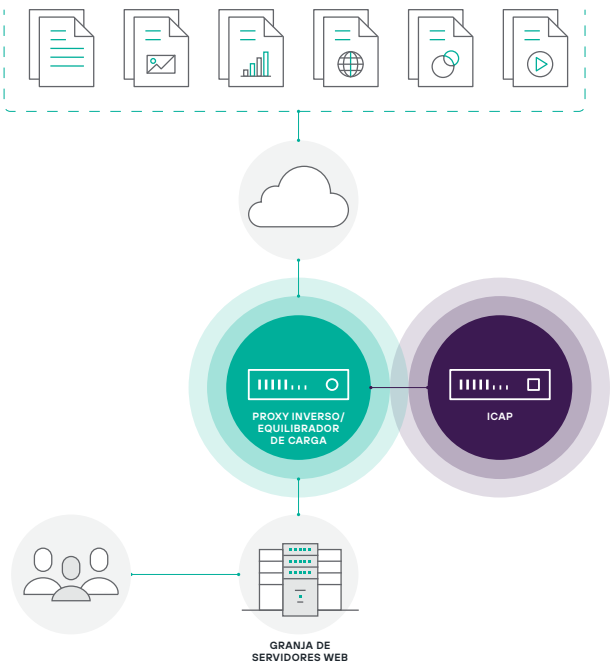
Acelere la transformación digital

Estamos en la era del portal de autoservicio. Tanto los clientes potenciales como los actuales deben cargar sus documentos para operaciones como préstamos personales, hipotecas o solicitudes de seguros automotrices. El problema es que si bien estos formatos de documentos son versátiles e increíblemente útiles, también son muy complejos, fáciles de sabotear y, con frecuencia, los delincuentes cibernéticos los utilizan para entregar cargas maliciosas.

Al utilizar el CDR de Zero Trust para la protección de portales, las organizaciones pueden acelerar sus proyectos de transformación digital, ofreciendo aplicaciones de internet y portales de autoservicio seguros, con la confianza de que los documentos que se cargan no se utilizarán para introducir amenazas o comprometer las redes de la empresa.

Garantice un contenido digitalmente puro

Todo portal incrementa potencialmente la "superficie de ataque" de una empresa. Los delincuentes saben esto e intentan aprovechar cualquier vulnerabilidad. Ahora, más que nunca, es vital garantizar que el contenido que se carga a una organización sea seguro, puro y esté libre de amenazas. Toda empresa que pueda establecer antecedentes de que garantiza el acceso a contenido empresarial limpio y puro logrará destacarse en lo que rápidamente se está transformando en un panorama cibernético anárquico.



El CDR de Zero Trust para la protección de portales permite a las empresas obtener los beneficios de sus proyectos de transformación digital, con la seguridad de que el contenido cargado que manejan se encuentra libre de amenazas.

Realice una integración fluida con las defensas existentes

La solución CDR de Zero Trust para la protección de portales abarca el producto de extensión de gateway (GX) de Forcepoint. La extensión de gateway (GX) se integra con un proxy inverso existente, como un equilibrador de carga o un firewall de aplicaciones web, a través de ICAP. El proxy inverso pasa el contenido a través de la GX, y posteriormente se transforma para eliminar las amenazas. La GX es fácil de integrar y requiere de una configuración mínima.

Probada con los principales servidores proxy inversos, la GX se integra fácilmente a proveedores de seguridad de terceros, como F5 BIG-IP, Citrix Netscaler, McAfee Web Gateway y Symantec Blue Coat. Detenga la infiltración de malware en el contenido

Los documentos de Office, el formato de archivos de documentos portátiles (PDF) de Adobe y las imágenes son las herramientas más utilizadas para entregar malware. La complejidad de estos formatos de archivos y de las aplicaciones para manejarlos hacen que sean un objetivo natural para los atacantes. Independientemente del tipo de malware, desde ransomware y troyanos bancarios hasta kits de acceso remoto y keyloggers, los delincuentes cibernéticos saben que el mejor lugar para ocultar las más recientes amenazas de día cero es dentro de documentos comerciales de uso diario. Las técnicas como el uso de malware sin archivos y el polimorfismo de archivos hacen que sea incluso más difícil abordar las amenazas mediante soluciones convencionales de seguridad cibernética basadas en detección.

El CDR de Zero Trust para protección de portales garantiza que los flujos de trabajo empresariales (como la importación de formularios de solicitudes de clientes, la carga de datos personales, etc.) continúen sin interrupciones gracias al exclusivo método utilizado para transformar los documentos que se cargan. Cada documento e imagen queda sujeto a transformación para eliminar totalmente las amenazas.

Elimine las amenazas ocultas en las imágenes mediante esteganografía

La esteganografía es el ocultamiento de datos en archivos aparentemente inocuos. Es una forma de codificar un mensaje secreto dentro de otro, conocido como el portador, de manera tal que solo el destinatario deseado pueda leerlo.

En la actualidad, el stegware, la utilización como arma de la esteganografía por parte de los atacantes cibernéticos, está en auge. Se ofrece de manera predeterminada en los kits de malware como servicio que circulan en la internet oscura. Se ha utilizado en campañas de malvertising (malware basado en avisos publicitarios) para exigir dinero a miles de usuarios y poner de rodillas a nuevos sitios respetables. Se implementa junto con sitios web de redes sociales para robar activos financieros valiosos ocultos en imágenes aparentemente inocuas. Estas no son buenas noticias para los profesionales de TI que utilizan herramientas para identificar los datos no seguros dado que la esteganografía es imposible de detectar.

El CDR de Zero Trust para la protección de portales garantiza que cada imagen incluida en un documento que se carga esté libre de contenido oculto mediante stegware. El proceso de transformación destruye el contenido oculto e inutiliza la imagen para el atacante. El CDR de Zero Trust para la protección de portales no solo resguarda a la organización de vulnerabilidades entrantes escondidas en imágenes mediante el uso de esteganografía, sino que incrementa la prevención contra la pérdida de datos existente y las iniciativas de gobernanza tales como el Reglamento General de Protección de Datos (RGPD) ya que detiene totalmente la pérdida de datos oculta en imágenes con esteganografía.

Desarrolle una solución ganadora

Junto con nuestros socios revendedores de Forcepoint, el equipo de Soluciones de Forcepoint ofrece diversos servicios profesionales que lo ayudarán a maximizar su inversión en la tecnología CDR de Zero Trust. Lo ayudaremos a determinar el alcance, planificar, instalar, configurar y gestionar su solución CDR de Zero Trust para la protección de portales.

Junto con el equipo de Soporte Técnico de Forcepoint, verificaremos que todo funcione adecuadamente durante el despliegue y luego de este. Nuestro equipo de Soluciones altamente capacitado cuenta con amplia experiencia e información a su disposición y, sin dudas, actuará como una extensión natural de su equipo interno.

Resumen: Disfrute de protección incomparable

Estamos a punto de vivir una revolución tecnológica. Ante la ola de ataques cibernéticos implacables y coordinados, las organizaciones se ven obligadas a reevaluar cada aspecto de sus actividades de compra, intercambio de información y transacciones en el ámbito digital.

Las defensas que se basan en la detección de amenazas conocidas son insuficientes. Aquellas basadas en el aislamiento y la detección mediante sandbox inhiben las actividades comerciales y dejan mucho librado al azar. Lo que se necesita es protección.

El CDR de Zero Trust para la protección de portales brinda protección sin igual para cualquier portal empresarial. Garantiza que los documentos e imágenes empresariales que se cargan se encuentren libres de amenazas.

Para obtener más información, consulte CDR de Zero Trust de Forcepoint

forcepoint.com/contact