EASYSOLUTIONS®
A CYXTERA BUSINESS

> Resumen de la Solución

Detect Safe Browsing Framework

Transacciones Seguras en Todos los Dispositivos

La identificación y eliminación de archivos maliciosos no es suficiente para detener el malware financiero. La gran mayoría de dispositivos ya se encuentran infectados de alguna forma, y nuevas variantes de malware que explotan vulnerabilidades de día cero aparecen diariamente. Detect Safe Browsing Framework toma un enfoque de seguridad diferente. Al bloquear el robo de credenciales de acceso y los canales de comunicación que el malware emplea para apropiarse de cuentas y monetizar ataques, la solución garantiza que incluso dispositivos infectados puedan seguir realizando transacciones seguras.

Prevención de Fraude Multinivel y Protección contra Amenazas

Detect Safe Browsing Client

Cliente descargable que protege PCs y Macs contra ataques de phishing y malware.

- Liviano software para PCs con back-end en la nube
- API de arquitectura abierta
- Sin exclusividad de navegadores
- Protege incluso después de actualizaciones del navegador
- Enfoque en el comportamiento del malware, no en las firmas

Detect Safe Browsing Mobile SDK

Protege la aplicación bancaria y la navegación móvil al detectar malware y otras amenazas.

- Visibilidad total
- Sencillo despliegue
- Protección contra MitM, superposición, pharming, y reempaque de apps
- Evaluación del riesgo en dispositivos y autenticación basada en riesgo

Detect Safe Browsing Clientless

Detección transparente sin software que identifica los tipos de malware que tratan de modificar portales y sesiones online.

- Detección de malware, MitB, amenazas día cero, MitM, y phishing
- Identificación de inyecciones HTML en páginas
- Malware Snapshot® registra evidencia de ataques
- Detección de credenciales comprometidas

EASYSOLUTIONS®
A CYXTERA BUSINESS

> Resumen de la Solución

Detect Safe Browsing Framework – Funciones y Beneficios

Detecta y Detiene Infecciones de Malware

La solución analiza todos los procesos del dispositivo y ayuda a proteger contra ataques de malware mediante el bloqueo de las conexiones a los servidores de control. En caso de detectar infecciones de malware, las correspondientes alertas son enviadas a los equipos de seguridad.

Protege los Sensitivos Datos de los Usuarios

Identifica el envenenamiento del DNS, lo cual puede ser indicio de que un ataque de pharming se está llevando a cabo, y bloquea el redireccionamiento a sitios fraudulentos. La solución cifra los golpes de tecla para que no puedan ser interceptados.

Descubre y Frena Ataques de Phishing

Nuestra avanzada solución de monitoreo de amenazas penetra la zona de la Internet conocida como Dark Web en busca de datos de tarjetas comprometidas de crédito/débito con el fin de mitigar proactivamente el impacto de brechas e incidentes ocurridos.

Previene la Causa del Fraude al Identificar Amenazas Activas en Tiempo Real

Detiene ataques en las primeras etapas del ciclo de vida del fraude e identifica con precisión factores de riesgo en los dispositivos de los usuarios. De esta forma, las organizaciones pueden tomar acción contra las amenazas más peligrosas antes de que se vean afectadas.

Mejora la Experiencia de Uso al Eliminar Fricción Innecesaria

Reduce procesos de autenticación y verificación redundantes, y otras interrupciones que pueden impactar negativamente la experiencia de sus usuarios. Así obtendrá una solución de remediación proactiva para sesiones y dispositivos en riesgo.

Reduce el Impacto Operacional de las Investigaciones de Fraude

Detect Safe Browsing Framework les permite a las organizaciones calibrar la tolerancia de riesgo, y reducir el volumen de alertas y falsos positivos con el fin de poder enfocar los esfuerzos en las áreas que más lo requieran.

Aprovecha Inteligencia de Amenazas en Tiempo Real

Nuestro Centro de Operaciones de Seguridad 24-7 analiza la inteligencia recolectada por Detect Safe Browsing Framework en más de 270 millones de puntos finales y cientos de organizaciones para adaptar la protección a cada interacción realizada por los usuarios.