INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Client-Side Protection & Compliance

Protéjase contra las vulnerabilidades de JavaScript en el lado del cliente y optimice el cumplimiento normativo

JavaScript es una herramienta esencial para las aplicaciones web de hoy en día. Desde la optimización de la experiencia del usuario hasta la mejora de la funcionalidad y el rendimiento, el uso de JavaScript tanto propio como de terceros ha crecido exponencialmente con el tiempo. Aunque su uso presenta numerosas ventajas, una cadena de suministro digital de JavaScript también puede dejar los sitios web vulnerables ante ataques del lado del cliente cuyo objetivo sea robar información confidencial del usuario final desde dentro del navegador, como datos de tarjetas de pago, mediante la inyección de código malicioso.

Dado que estos ataques no son visibles del lado del servidor y eluden las medidas de seguridad tradicionales, las organizaciones pueden convertirse fácilmente en el objetivo, y esto se traduce en una pérdida de confianza por parte del cliente, imposición de multas devastadoras, sanciones por incumplimiento y daños a la reputación de la marca.

Client-Side Protection & Compliance de Akamai

Client-Side Protection & Compliance de Akamai ayuda a proteger contra la exfiltración de los datos del usuario final y defiende los sitios web frente a amenazas JavaScript. La solución se ha diseñado para detectar comportamientos de scripts maliciosos y activar alertas útiles, de manera que los equipos de seguridad puedan mitigar las actividades dañinas en tiempo real.

Con funcionalidades de conformidad con PCI DSS v4.0 diseñadas específicamente, Client-Side Protection & Compliance ayuda a las organizaciones a cumplir los nuevos requisitos de seguridad de scripts y protege los datos de las tarjetas de pago contra los ataques del lado del cliente. Gestione fácilmente el inventario de scripts de su página de pagos, optimice el proceso de auditoría mediante un único y completo panel, y reciba alertas específicas del sector de las tarjetas de pago (PCI) para responder rápidamente a los eventos relacionados con el cumplimiento.

Funciones clave

Protección contra la exfiltración de datos confidenciales en el lado del cliente

Los ciberdelincuentes buscan la información confidencial de los usuarios finales. Al explotar las vulnerabilidades de las cadenas de suministro de JavaScript, los agentes maliciosos pueden inyectar código en los sitios web para acceder a información confidencial y exfiltrarla para usos fraudulentos. Client-Side Protection & Compliance combina el aprendizaje automático con evaluación heurística para analizar el comportamiento de los scripts en tiempo real y detectar así actividades maliciosas y recursos vulnerables. Proporciona a los equipos de seguridad útiles alertas inmediatas para defenderse rápidamente ante los ataques del lado del cliente, como el robo de información web, los ataques de Magecart y formjacking.

VENTAJAS PARA SU EMPRESA

Detección y protección
Monitorice el comportamiento de los scripts en sesiones en tiempo real para detectar actividades sospechosas

Flujos de trabajo de PCI DSS v4.0
Ayudan a cumplir los requisitos de seguridad 6.4.3 y 11.6.1 relativos a JavaScript

Alertas priorizadas en tiempo real Mitigue de manera inmediata los eventos de alto riesgo con alertas útiles

Visibilidad en el lado del cliente
Disfrute de vistas completas de la superficie de ataque en el lado del cliente

Gestión de políticas
Regule el comportamiento de los scripts y controle el funcionamiento de JavaScript en tiempo de ejecución

Detección de vulnerabilidades
Identifique vulnerabilidades y exposiciones comunes (CVE) con el respaldo de la inteligencia contra amenazas de Akamai

Opciones de implementación flexibles
Implementación sencilla mediante Akamai Connected Cloud o directamente en el servidor de origen

Akamai

Ayuda específica para el cumplimiento de PCI DSS v4.0

Los requisitos de seguridad de scripts de PCI DSS v4.0 6.4.3 y 11.6.1 exigen que las organizaciones protejan los datos de las tarjetas de pago contra los ataques del lado del cliente y, asimismo, garanticen la gestión de los scripts en las páginas de pagos. Client-Side Protection & Compliance hace seguimiento e inventario de todos los scripts de las páginas de pagos, garantizando su integridad y autorización. Asimismo, proporciona justificaciones predefinidas y reglas automatizadas para probar fácilmente todos los scripts cargados. La solución también monitoriza los cambios en los encabezados HTTP y en la protección de las páginas de pagos para evitar la posible manipulación. Un completo panel y alertas específicas de PCI permiten a las organizaciones responder rápidamente ante los eventos relacionados con el cumplimiento y garantizar la protección de los datos de las tarjetas de pago dentro del navegador. Al contar con estas funcionalidades, los equipos de seguridad y cumplimiento pueden reducir la carga del proceso de auditoría de PCI y optimizar rápidamente los flujos de trabajo.

Amplia visibilidad de las amenazas JavaScript

Las protecciones tradicionales para aplicaciones web, como los firewalls, solo monitorizan el tráfico del lado del servidor y no ofrecen visibilidad de las actividades que se ejecutan en el lado del cliente. Los enfoques basados en estándares para protegerse de estas amenazas, como las políticas de seguridad del contenido, son difíciles de gestionar y ofrecen una protección limitada contra cargas maliciosas introducidas en la cadena de suministro de los scripts fuera del control del operador de la página web. Por esto, las organizaciones tienen un punto ciego, que permite que el código dañino no se detecte durante días, semanas o incluso meses, mientras sigue robando datos confidenciales. Client-Side Protection & Compliance ofrece una vista incomparable de la superficie de ataque del lado del cliente de su sitio web, e incluye el comportamiento, las vulnerabilidades, el alcance y el impacto de cada script, así como los datos a los que se ha accedido o las amenazas que suponen.

Cómo funciona

Client-Side Protection & Compliance se ejecuta en el explorador del usuario final y monitoriza los scripts del lado del cliente en una página web protegida. Cuando estos scripts muestran cambios de comportamiento, se aplican técnicas de aprendizaje automático para evaluar el riesgo de acciones no autorizadas o inapropiadas. A continuación, alerta a los equipos de seguridad sobre los eventos de alto riesgo y permite la investigación y mitigación inmediatas de las posibles amenazas.

Configuración Se inyectan scripts simples en cada página monitorizada sin que afecte al rendimiento significativamente.

Monitorización y evaluación Se recopilan los datos de la actividad de JavaScript del navegador web del usuario y se supervisan. Se aplican técnicas de aprendizaje automático para evaluar el riesgo de acciones no autorizadas o inapropiadas, si lo hubiera.

Alertas Se envían alertas en tiempo real con información detallada para mitigar las amenazas si se detecta un ataque o una amenaza activa.

Mitigación Se restringe inmediatamente el acceso de JavaScript malicioso a los datos confidenciales, así como su exfiltración, en páginas protegidas con tan solo un clic.

Acelere el cumplimiento de los requisitos de seguridad de scripts de PCI DSS v4.0

Integridad y autorización de scripts (6.4.3)

Garantice la integridad y la autorización de todos los scripts cargados en las páginas de pagos protegidas.

Inventario y justificación de scripts (6.4.3)

Haga seguimiento e inventario de los scripts cargados en las páginas de pagos protegidas. Justifique rápidamente todos los scripts, aprovechando las justificaciones predefinidas y las reglas automatizadas.

Protección de páginas de pagos (11.6.1)

Detecte los cambios no autorizados en las páginas de pagos protegidas y responda ante ellos de forma inmediata.

Panel intuitivo

Simplifique el proceso de auditoría de cumplimiento de PCI DSS v4.0 con un panel específico con información detallada sobre tareas y alertas relacionadas con los requisitos de seguridad 6.4.3 y 11.6.1.

Alertas de PCI útiles

Reciba y registre alertas sobre eventos relacionados con el cumplimiento de PCI, como scripts no autorizados, exfiltración de datos de pagos y manipulación de páginas de pagos.

Para más información, visite nuestra página de producto o póngase en contacto con el equipo de ventas de Akamai.

 | Asistencia | Publicado en 09/23