LISTA DE COMPROBACIÓN DE AKAMAI

Lista de comprobación de seguridad de JavaScript conforme a PCI DSS v4.0 con Client-Side Protection & Compliance de Akamai

Las normas PCI DSS se han desarrollado para proteger la seguridad de los datos en los pagos con tarjeta online y para facilitar la adopción generalizada de unas medidas de seguridad estándar a escala global. Se trata de uno de los estándares de seguridad más importantes, y su cumplimiento se exige a cualquier organización que procese datos de tarjetas de pago online.

La última versión de PCI DSS (disponible solo en inglés), la 4.0, entra en vigor en 2025 e incluye 12 requisitos básicos de seguridad de datos, actualizados expresamente para hacer frente a las amenazas de ciberseguridad nuevas y en evolución. Se han añadido dos requisitos importantes a PCI DSS v4.0, 6.4.3 y 11.6.1, referentes a la seguridad de JavaScript y a la protección contra ataques de robo de información web del lado del cliente para hacerse con datos confidenciales de los usuarios finales desde el navegador. La popularidad de estos ataques ha aumentado a lo largo de los años, ya que con el uso de técnicas más sofisticadas se han vuelto más difíciles de detectar. Asimismo, pueden tener consecuencias devastadoras para las organizaciones afectadas, como cuantiosas multas, daños a la reputación de la marca, pérdida de ingresos y reducción de la confianza por parte de los clientes.

Veamos en una lista de comprobación lo que implican los nuevos requisitos de seguridad de scripts PCI DSS v4.0 y cómo Client-Side Protection & Compliance se sitúa por delante de la competencia.

Requisitos de PCI DSS v4.0	Cómo puede ayudar Client-Side Protection & Compliance
Requisito 6.4.3: Las aplicaciones web orientadas al público están protegidas contra ataques	**Autorizar con un solo clic**
☑ Se implementa un método para confirmar que cada script cargado y ejecutado en el navegador esté autorizado	☑ Gestione fácilmente qué scripts permite ejecutar en las páginas de pago de su sitio web directamente desde la herramienta
☑ Se implementa un método para garantizar la integridad de cada script cargado y ejecutado en el navegador	**Garantizar la integridad desde el principio**
☑ Se mantiene un inventario de todos los scripts cargados y ejecutados en el navegador con una justificación por escrito de por qué es necesario cada uno de ellos	☑ La tecnología conductual analiza cada script ejecutado en el navegador para detectar actividades maliciosas o exfiltraciones de datos y alertar sobre ellas
	Hacer seguimiento e inventario de todos los scripts automáticamente
	☑ Las justificaciones predefinidas y las reglas automatizadas facilitan la justificación del propósito de cada script cargado y ejecutado en el navegador

Akamai

Requisitos de PCI DSS v4.0	Cómo puede ayudar Client-Side Protection & Compliance
Requisito 11.6.1: Se detectan los cambios no autorizados en las páginas de pago y se responde a ellos **Un mecanismo de detección de cambios y manipulación se implementa de la siguiente manera:** ☑ Alertar al personal de modificaciones no autorizadas (incluidos indicadores de compromiso, cambios, adiciones y eliminaciones) en los encabezados HTTP y el contenido de las páginas de pago tal y como lo recibe el navegador del consumidor ☑ El mecanismo está configurado para evaluar el encabezado HTTP recibido y la página de pago **Las funciones del mecanismo se realizan** como mínimo una vez cada siete días o periódicamente (con la frecuencia definida en el análisis de riesgos específico de la entidad, de acuerdo con todos los elementos especificados en el requisito 12.3.1)	**Proteja sus páginas de pago** ☑ Supervise, analice y mitigue los intentos de manipulación malintencionada de las páginas de pago para garantizar la seguridad de los datos valiosos del usuario final **Investigue las modificaciones no autorizadas en tiempo real con alertas inmediatas y útiles** ☑ Gracias a la detección instantánea, los equipos de seguridad pueden responder rápidamente a cambios o modificaciones no autorizados de los encabezados HTTP de las páginas de pago **Proteja con la defensa siempre activa** ☑ La protección continua salvaguarda las interacciones de los usuarios en sus páginas de pago

Client-Side Protection & Compliance de Akamai proporciona una sólida protección contra las amenazas de JavaScript y ofrece visibilidad de la superficie de ataque de los clientes para proteger los datos confidenciales del navegador. Sus funciones, diseñadas específicamente para la versión 4.0 de PCI DSS, ayudan a los equipos de seguridad y de cumplimiento a optimizar el proceso de auditoría de PCI DSS v4.0 y a proporcionar flujos de trabajo dedicados que contribuyen al cumplimiento de los requisitos de seguridad de scripts 6.4.3 y 11.6.1.

Client-Side Protection & Compliance de Akamai cuenta con opciones de implementación flexibles y no requiere que Akamai Connected Cloud esté activado.

Obtenga más información sobre cómo estas funciones pueden ayudar a su organización a cumplir con la versión 4.0 del estándar PCI DSS.

 | Asistencia | Fecha de publicación: 09/23