

CASE STUDY: Reflectiz valida las capacidades de su plataforma PCI DSS con Integrity360

El cliente

Reflectiz ofrece una plataforma de gestión de exposición web sin agentes que ayuda a las organizaciones a identificar y gestionar scripts, componentes de terceros y cadenas de suministro digitales que operan en sus sitios web.

Su plataforma específica para PCI DSS ayuda a las organizaciones de comercio electrónico a cumplir con los requisitos de monitorización, autorización y recopilación de evidencias asociados a los requisitos 6.4.3 y 11.6.1 de PCI DSS v4.0.1.

La plataforma monitoriza de forma remota las páginas de pago sin necesidad de modificar código, instalar software o añadir etiquetas de monitorización.

Criterios de selección

Reflectiz necesitaba un evaluador capaz de:

- Aportar experiencia especializada en PCI DSS
- Evaluar capacidades técnicas y operativas de la plataforma
- Analizar el alineamiento con los requisitos 6.4.3 y 11.6.1
- Revisar los procesos de monitorización, aprobación e informes
- Ofrecer una evaluación independiente y creíble
- Comprender los requisitos de evidencias esperados en una evaluación QSA

Integrity360 Europe es una PCI Qualified Security Assessor Company y miembro de la Global Executive Assessor Roundtable del PCI Security Standards Council.

reflectiz



Sector

Cumplimiento
normativo en pagos



Reto

Reflectiz quería una evaluación independiente sobre cómo su plataforma PCI DSS se alineaba con los requisitos 6.4.3 y 11.6.1 de PCI DSS v4.0.1.

La evaluación debía determinar si la plataforma podía dar soporte eficaz a:

- Inventario y autorización de scripts en las páginas de pago
- Garantía de integridad de los scripts
- Justificaciones técnicas y de negocio documentadas
- Detección de manipulaciones en páginas de pago y cabeceras HTTP
- Monitorización continua y generación de alertas
- Recopilación de evidencias para auditorías PCI DSS

El proyecto consistió en una revisión de las capacidades de la plataforma y no en una certificación o evaluación de cumplimiento de un entorno concreto de cliente.

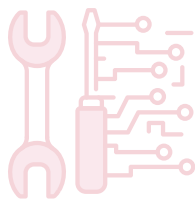
Solución

Integrity360 revisó la arquitectura, las capacidades de monitorización y los flujos de cumplimiento de la plataforma PCI DSS de Reflectiz.

La evaluación analizó cómo Reflectiz:

- Identifica scripts propios, de terceros y de cuartos proveedores
- Monitoriza el comportamiento de los scripts dentro del navegador
- Detecta cambios en las páginas de pago y en las cabeceras HTTP
- Mantiene inventarios de scripts y justificaciones documentadas
- Registra aprobaciones mediante trazas de auditoría con marca temporal
- Genera alertas y evidencias listas para auditorías

Integrity360 también revisó el modelo de despliegue sin agentes de la plataforma, la frecuencia de monitorización configurable, las capacidades Smart Approval y las integraciones con plataformas de seguridad y gestión de procesos.



Evaluación de Integrity360

Integrity360 concluyó que la plataforma PCI DSS de Reflectiz está bien posicionada para ayudar a las organizaciones a abordar los requisitos 6.4.3 y 11.6.1 de PCI DSS v4.0.1.

El inventario automatizado de scripts, el análisis de integridad basado en comportamiento, el flujo estructurado de aprobación, la monitorización continua de cabeceras HTTP y las capacidades de auditoría e informes respaldan directamente los objetivos de control relevantes. Además, su arquitectura sin agentes permite reforzar la monitorización de páginas de pago sin cambios importantes en el código ni una carga adicional para los equipos técnicos.



Los equipos de cumplimiento tienen motivos para ser escépticos ante las afirmaciones de los proveedores. Que Integrity360 Europe, una Qualified Security Assessor Company independiente, haya analizado cómo nuestra plataforma se alinea con los requisitos 6.4.3 y 11.6.1 de PCI DSS convierte nuestras promesas en algo que un comercio puede evaluar por sus propios méritos. Esa independencia es precisamente lo que hace que esta evaluación tenga tanto valor”

Idan Cohen
Cofundador y CEO de Reflectiz



Beneficios

- Validación independiente realizada por una PCI Qualified Security Assessor Company
- Clara alineación con los principales objetivos de control de PCI DSS
- Mayor confianza para clientes y auditores
- Soporte demostrado para el inventario y la autorización de scripts
- Monitorización basada en comportamiento más allá de los hashes estáticos
- Supervisión continua de páginas de pago y cabeceras HTTP
- Reducción del esfuerzo de preparación de evidencias para auditorías QSA
- Reconocimiento del valor añadido en la seguridad de la cadena de suministro

Si se configura correctamente y se integra en un programa más amplio de gobierno, riesgo y cumplimiento, Reflectiz puede ofrecer una alternativa más eficiente y sostenible que las revisiones manuales de scripts y los enfoques de monitorización estática.

Mirando al futuro

Esta evaluación independiente proporciona a Reflectiz una base sólida para demostrar cómo su plataforma puede ayudar a las organizaciones a cumplir los requisitos de seguridad de las páginas de pago de PCI DSS.

Además, la plataforma puede aportar valor adicional al mejorar la visibilidad de las cadenas de suministro digitales, identificar amenazas del lado cliente y apoyar programas más amplios de gobierno, privacidad y cumplimiento normativo.

Para los comercios elegibles para SAQ A, una implementación adecuada también puede ayudar a demostrar que las páginas de pago no son vulnerables a ataques basados en scripts. La elegibilidad y los resultados de cumplimiento seguirán dependiendo del entorno y los controles específicos de cada comercio.



Sobre Integrity360

Integrity360 es un destacado especialista independiente en ciberseguridad y PCI que opera en EMEA y Norteamérica, con oficinas en el Reino Unido e Irlanda, Bulgaria, Italia, Suecia, España, Alemania, Suiza, Francia, Bélgica, Lituania, Ucrania, África, el Caribe y Canadá. La compañía opera Centros de Operaciones de Seguridad (SOC) en Dublín, Madrid, Sofía, Estocolmo, Roma y Ciudad del Cabo, proporcionando supervisión y respuesta continuas en múltiples zonas horarias.

Con más de 700 empleados, incluidos más de 580 profesionales especializados en ciberseguridad, Integrity360 ofrece una cartera integral de servicios profesionales, soporte y servicios de seguridad gestionada que cubren todo el ciclo de vida del riesgo cibernético, desde la identificación y la prevención hasta la detección, la respuesta y la recuperación.



3000+

Clientes
empresariales

585+

Profesionales de
la ciberseguridad