INFORME SOBRE LA SOLUCIÓN DE AKAMAI

Lograr la conformidad con el estándar PCI DSS v4.0 con Akamai

El cumplimiento de la norma PCI implica satisfacer una serie de requisitos globales para garantizar la protección y la seguridad de los entornos con datos de cuentas de tarjetas de pago. Cualquier empresa que procese, transmita o almacene datos de titulares de tarjetas online tiene la responsabilidad de cumplir la norma de seguridad de datos para el sector de las tarjetas de pago (PCI DSS). Desde su implantación en 2004, la norma se ha ido actualizando con regularidad para adaptarse a los cambios del sector y a las amenazas de ciberseguridad en constante evolución. La norma PCI DSS v4.0 ha sido la última en publicarse, en marzo de 2022, y plantea cambios significativos. Además, contiene 12 requisitos básicos que las organizaciones deben cumplir antes de marzo de 2025.

¿Está preparada su empresa para cumplir con la norma PCI DSS v4.0?

Aunque el incumplimiento de las normas PCI no es punible por ley, las compañías emisoras de tarjetas de crédito pueden imponer multas a las empresas que no se adhieran a las mismas. Además, si no se protegen debidamente los datos de los titulares de las tarjetas, las marcas pueden ser vulnerables a los ciberataques y sufrir filtraciones de datos devastadoras. Como consecuencia, tendrán que hacer frente a multas cuantiosas y perderán la confianza de los clientes para siempre.

Estamos aquí para ayudarle. Akamai no solo garantiza el cumplimiento de la norma PCI DSS de nivel 1, sino que también ofrece una amplia gama de soluciones de seguridad líderes en el sector para ayudar a las organizaciones a cumplir con la norma PCI DSS v4.0. Con algunas soluciones puede incluso reducir el alcance de una auditoría de PCI y, de esta forma, ahorrar el tiempo y el dinero que tendría que invertir en cumplir con los requisitos de la certificación.

App & API Protector con protección contra malware

Garantice la conformidad de los registros y protéjase de la filtración de datos de identificación personal, los ataques de día cero y las CVE, así como de otros ataques basados en el Edge, para cumplir con los requisitos 6.4.2, 6.5.3 y 11.5.

> "Cada día, se detectan 560 000 nuevos programas maliciosos, que se van sumando a los más de mil millones que ya están en circulación".
>
> Fuente: Getastra | 30+ Malware Statistics You Need to Know In 2023

Ventajas

- **Optimice los flujos de trabajo** de los equipos responsables de la seguridad y el cumplimiento
- **Reduzca el volumen de las auditorías** con capacidades diseñadas específicamente para PCI
- **Reciba y registre alertas de PCI útiles** para eventos relacionados con el cumplimiento normativo
- **Consolide a los proveedores** para satisfacer los requisitos de PCI gracias a la completa cartera de soluciones de seguridad de Akamai

©2024 Akamai Technologies | Asistencia |
| Publicado en abril de 2024

API Security

Detecte anomalías en el comportamiento y mitigue el abuso de la lógica de las API, registre su actividad, e implemente una protección automatizada y reactiva para sus API con el fin de cumplir los requisitos 6.2.3, 6.2.4, 6.3.2, 6.4.1, 6.4.2, 10.2.1,10.5.1 y 11.3.2.

> **"En 2024, los abusos de las API y las filtraciones de datos relacionadas casi se duplicarán".**
>
> Fuente: Gartner: Top 10 Aspects Software Engineering Leaders Need to Know About APIs (solo disponible en inglés)

Client-Side Protection & Compliance

Satisfaga los nuevos requisitos en materia de seguridad de JavaScript 6.4.3 y 11.6.1 y fortalezca la protección contra los ataques en el lado del cliente, como los de robo de información web y los de tipo Magecart, con los que acceden a los datos de las tarjetas en las páginas de pago en línea y los exfiltran mediante la inyección de código malicioso que se ejecuta en el navegador.

> **"El 81 % de los grandes retailers online afirma que en su organización se detectó un comportamiento sospechoso de los scripts en 2022".**
>
> Fuente: From Bad Bots to Malicious Scripts: The Effectiveness of Specialized Defense | 2023 (solo disponible en inglés)

Akamai Guardicore Segmentation

Para segmentar los activos regulados de forma más eficaz, integre diferentes tecnologías en una única plataforma para satisfacer, así, numerosos requisitos de PCI. Obtenga visibilidad de la red y de los activos, un firewall distribuido, detección y respuesta ante filtraciones, y, además, aplique las directivas hasta la capa 7.

> **"Con la segmentación definida por software pudimos crear y aplicar políticas de segmentación en los procesos, con lo que mejoramos significativamente nuestra estrategia de seguridad y pudimos cumplir los requisitos técnicos de PCI-DSS".**
>
> — Senior Infrastructure Engineer, The Honey Baked Ham Company

Para obtener más información sobre cómo acelerar la conformidad con la norma PCI DSS v4.0 con Akamai, póngase en contacto con nuestro equipo de expertos.

©2024 Akamai Technologies | Asistencia |
| Publicado en abril de 2024