DESCRIZIONE DELLA SOLUZIONE AKAMAI

Conformità al PCI DSS v4.0 con Akamai

La conformità al PCI implica l'adesione ad una serie globale di requisiti di sicurezza per proteggere e mettere al sicuro gli ambienti che contengono dati relativi ai conti delle carte di pagamento. Qualsiasi azienda che elabora, trasmette o archivia i dati dei titolari di carte online ha la responsabilità di aderire allo standard PCI DSS (Payment Card Industry Data Security Standard). Sviluppato nel 2004, questo standard viene regolarmente aggiornato in base ai cambiamenti del settore e alle minacce per la cybersicurezza in continua evoluzione. La versione più recente dello standard, la PCI DSS v4.0, rilasciata a marzo 2022, contiene notevoli cambiamenti e 12 requisiti fondamentali a cui le organizzazioni dovranno conformarsi entro marzo 2025.

Siete pronti per soddisfare i requisiti del PCI DSS v4.0?

Sebbene il mancato rispetto degli standard PCI non sia perseguibile legalmente, le società che emettono carte di credito possono imporre sanzioni alle aziende che non soddisfano i relativi requisiti. Inoltre, la mancata protezione dei dati dei titolari di carte di credito può rendere i brand vulnerabili agli attacchi informatici che provocano devastanti violazioni dei dati con multe salate e perdita permanente della fiducia dei clienti.

Noi siamo qui per aiutarvi. Non solo Akamai mantiene la conformità al PCI DSS di livello 1, ma offre anche una vasta gamma di soluzioni per la sicurezza leader del settore per aiutare le organizzazioni a soddisfare i requisiti di conformità al PCI DSS v4.0. Alcune soluzioni aiutano addirittura a ridurre l'ambito di un controllo di conformità al PCI, risparmiando il tempo e il denaro necessari per soddisfare i requisiti di certificazione.

App & API Protector con protezione dai malware

Mantiene la conformità del registro e la protezione da fughe di informazioni di identificazione personale, attacchi zero-day e vulnerabilità CVE, nonché da attacchi basati sull'edge per conformarsi ai requisiti 6.4.2, 6.5.3 e 11.5.

> "Ogni giorno vengono rilevati 560.000 nuovi malware, che si aggiungono all'oltre 1 miliardo di programmi malware già in circolazione".
>
> Fonte: Getastra | 30+ Malware Statistics You Need to Know In 2023

Vantaggi

- **Workflow semplificati** per i team addetti alla sicurezza e alla conformità
- **Riduzione dell'onere dei controlli** con funzionalità PCI appositamente concepite e dedicate
- **Ricezione e registrazione di avvisi PCI utili** per eventi relativi alla conformità
- **Vendor consolidati** per soddisfare i requisiti del PCI con la gamma completa delle soluzioni per la sicurezza di Akamai

API Security

Rileva e mitiga il comportamento delle API e l'abuso della logica aziendale, registra le attività delle API e implementa una protezione reattiva e automatizzata per le API al fine di contribuire a soddisfare i requisiti di conformità 6.2.3, 6.2.4, 6.3.2, 6.4.1, 6.4.2, 10.2.1, 10.5.1 e 11.3.2.

> **"Entro il 2024, gli abusi di API e le relative violazioni di dati aumenteranno quasi del doppio".**
>
> Fonte: Gartner: Top 10 Aspects Software Engineering Leaders Need to Know About APIs (disponibile solo in inglese)

Client-Side Protection & Compliance

Soddisfa i nuovi requisiti di sicurezza JavaScript 6.4.3 e 11.6.1 aiutando a proteggersi dagli attacchi lato client, come web skimming o Magecart, che riescono a sottrarre ed esfiltrare i dati delle carte di credito dalle pagine di pagamento online iniettando codice dannoso nel browser.

> **"L'81% dei grandi retailer online segnala che le loro organizzazioni sono state prese di mira da comportamenti di script sospetti nel 2022".**
>
> Fonte: From Bad Bots to Malicious Scripts: The Effectiveness of Specialized Defense | 2023 (disponibile solo in inglese)

Akamai Guardicore Segmentation

Segmenta le risorse regolamentate in modo più efficiente sfruttando diverse tecnologie integrate in un'unica piattaforma per aiutare a soddisfare molti requisiti del PCI. Consente di ottenere la visibilità sulla rete e sulle risorse, un firewall distribuito, l'applicazione delle policy fino al livello 7 e un sistema di rilevamento e risposta alle violazioni.

> **"La segmentazione definita dal software ci ha consentito di creare e applicare policy di segmentazione a livello di processi, migliorando notevolmente la nostra strategia di sicurezza e la nostra capacità di soddisfare i requisiti tecnici dello standard PCI-DSS".**
>
> - Senior Infrastructure Engineer, The Honey Baked Ham Company

Per saperne di più su come accelerare la conformità al PCI DSS v4.0 con Akamai, contattate il nostro team di esperti.