CLOUDFLARE

WHITEPAPER

Un approccio strategico per mantenere la conformità PCI DSS 4.0

Contenuto

Panoramica

Tutte le organizzazioni che lavorano con carte di credito, debito o prepagate devono essere conformi allo standard PCI DSS (Payment Card Industry Data Security Standard). Ciò include piccoli commercianti, rivenditori al dettaglio, siti Web di e-commerce, banche e grandi imprese. Tuttavia, il passaggio al cloud e al lavoro ibrido, combinato con l'evoluzione degli standard con l'implementazione di PCI DSS 4.0, rendono difficile conformarsi in modo efficiente.

È necessario un nuovo approccio per questo mondo modernizzato digitalmente per semplificare il processo di conformità in modo scalabile, consentendo alle organizzazioni di stare al passo con il panorama normativo dinamico mentre sta al passo con la modernizzazione digitale aziendale.

Le difficoltà della conformità PCI DSS per le organizzazioni di oggi

La conformità PCI è fondamentale, poiché i trasgressori sono soggetti a multe, azioni legali e indagini governative. Tuttavia, la conformità presenta diverse sfide per gli istituti finanziari, le aziende di e-commerce e altri soggetti alle sue normative.

E poiché i team IT hanno perso il controllo dei propri ambienti digitali a causa della crescente dipendenza dal cloud computing e dal lavoro remoto, il processo di risoluzione di queste difficoltà è diventato più complesso.

Allocazione di tempo e risorse: il 53% delle organizzazioni afferma che i ruoli tecnici legati alla privacy sono a corto di personale, il che rende difficile la conformità.[1]

Sicurezza dei dati in ambienti diversi: con l'avvento del cloud computing e dei pagamenti mobili, garantire la conformità in ambienti diversi e spesso meno controllati è sempre più difficile.

Complessità con l'integrazione dello stack tecnologico: l'integrazione e la manutenzione delle tecnologie necessarie per soddisfare gli standard di conformità, come la crittografia e le configurazioni firewall, sono spesso complesse. Questa difficoltà è ancora maggiore nelle organizzazioni con sistemi legacy o in quelle in fase di trasformazione digitale.

Auditing: i team IT devono mantenere una traccia di controllo aggiornata su tutte le infrastrutture e i sistemi per garantire la conformità.

Conformità dei fornitori: garantire che i fornitori e i fornitori di servizi di terze parti rispettino gli standard PCI aggiunge un ulteriore livello di complessità.

Tieni il passo con le minacce informatiche sofisticate con PCI DSS 4.0

PCI DSS 4.0 è stato rilasciato il 31 marzo 2022 ed entrerà in vigore il 31 marzo 2024 con requisiti aggiuntivi che entreranno in vigore il 31 marzo 2025. Gli obiettivi di PCI DSS 4.0 sono:[2]

1. Continuare a soddisfare le esigenze di sicurezza del settore dei pagamenti

- **Requisiti di autenticazione avanzati:** viene posta una maggiore enfasi sull'autenticazione, in particolare sull'autenticazione a più fattori per tutti gli accessi al Cardholder Data Environment (CDE). Anche i requisiti per la password sono più rigorosi grazie all'aumento del numero di caratteri da un minimo di 8 a 12.
- **Requisiti di crittografia più rigorosi:** PCI DSS 4.0 impone l'uso di una crittografia "forte" per l'archiviazione e la trasmissione dei dati dei titolari di carta, come TLS che non è vulnerabile agli exploit noti.
- **Nuovi requisiti di e-commerce e phishing per affrontare le minacce continue:** PCI 4.0 prevede requisiti aggiuntivi per la sicurezza lato client e per la difesa da phishing e social engineering.

2. Promuovere la sicurezza come processo continuo

- **Maggiore attenzione all'analisi e alla gestione del rischio:** le organizzazioni sono incoraggiate a implementare processi continui di analisi e gestione del rischio per identificare e affrontare tempestivamente le vulnerabilità.
- **Maggiore enfasi sulla responsabilità e sulla governance:** la nuova versione pone una maggiore attenzione alla governance dei dati dei titolari di carta e alla responsabilità per il mantenimento dei controlli di sicurezza.
- **Maggiori indicazioni per l'implementazione e il rispetto dei requisiti di sicurezza:** PCI 4.0 chiarisce l'intento dello standard e i tempi utilizzati.

3. Aggiungere flessibilità per le diverse metodologie

- **Integrazione di nuove tecnologie:** PCI DSS 4.0 affronta la sicurezza delle tecnologie emergenti come il cloud e i sistemi di pagamento mobile.
- **Maggiore flessibilità nel modo in cui le organizzazioni possono raggiungere gli obiettivi di sicurezza:** le organizzazioni possono utilizzare un “approccio personalizzato”, ovvero una gamma più ampia di metodi per soddisfare i requisiti. E PCI 4.0 offre maggiore flessibilità per stabilire la frequenza con cui eseguire azioni basate su analisi di rischio mirate.

4. Migliorare i metodi di convalida

- **Monitoraggio e test continui:** Il nuovo standard incoraggia il passaggio dalla convalida annuale della conformità al monitoraggio continuo della sicurezza e della conformità.
- **Maggiore allineamento tra le valutazioni e gli attestati di conformità:** le informazioni contenute nei questionari di autovalutazione o nei rapporti di conformità sono più allineate a quanto riepilogato negli attestati di conformità.

Soluzione: Un nuovo approccio ai requisiti PCI tramite la connettività cloud di Cloudflare

I team IT e di sicurezza devono soddisfare i requisiti PCI in un modo semplice e programmabile che si integri facilmente con il loro attuale stack tecnologico e di sicurezza e continui a farlo man mano che la loro infrastruttura e PCI DSS si evolvono.

La risposta non è un approccio miscuglio con molte soluzioni di sicurezza legacy e puntuali. I team hanno invece bisogno di una piattaforma unificata di servizi di rete e sicurezza nativi del cloud progettati per aiutare le aziende a riprendere il controllo sui propri ambienti IT e a soddisfare vari requisiti di conformità, incluso PCI. Questa piattaforma unificata è detta connettività cloud.

La connettività cloud di Cloudflare offre:

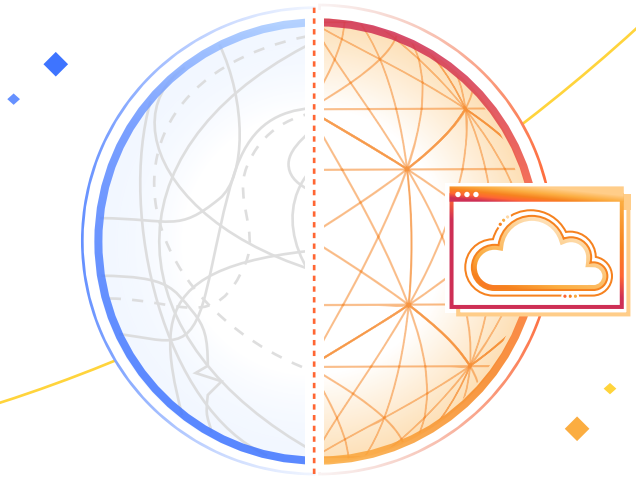
- Una piattaforma progettata per la conformità dei dati
- Un motore di criteri unificato
- Sovranità dei dati senza compromessi
- Reporting intelligente per soddisfare gli audit

Cloudflare consente ai team IT di applicare controlli coerenti in tutte le sedi, utilizzando un unico piano di controllo per attivarli ovunque.

I team possono inviare i log direttamente dal perimetro Cloudflare a una destinazione SIEM o cloud preferita per il controllo. Inoltre, la visibilità su larga scala di Cloudflare nel traffico Internet significa che Cloudflare può identificare e difendersi automaticamente dalle nuove minacce.

Cloudflare stesso è conforme PCI e supporta nativamente i requisiti PCI DSS 4.0. Ad esempio, Cloudflare consente ai team IT di applicare facilmente l'autenticazione a più fattori, una delle principali priorità di PCI DSS 4.0. Cloudflare supporta inoltre gli standard di crittografia più recenti e spesso contribuisce ad essi, aiutando i clienti a soddisfare i requisiti PCI DSS 4.0 per la crittografia delle informazioni sensibili.

Una mappatura riepilogativa dei requisiti PCI DSS per le funzionalità cloud di connettività Cloudflare è disponibile nella pagina successiva:



Aree chiave in cui Cloudflare può aiutare a soddisfare i requisiti PCI*

Requisito PCI	Funzionalità di Cloudflare
1. Installazione e gestione dei controlli di sicurezza della rete (in precedenza "installazione e gestione di un firewall").	Cloudflare protegge allo stesso modo reti, applicazioni e implementazioni cloud dal traffico di rete dannoso. Cloudflare utilizza l'intelligence delle minacce proveniente da centinaia di miliardi di minacce quotidiane per proteggere siti Web e applicazioni Web dalle minacce basate sul Web, inclusi gli attacchi top 10 e zero-day OWASP. La sua piattaforma di sicurezza è nativa del cloud, si implementa in pochi minuti e consente agli utenti di implementare modifiche alle policy globali in pochi secondi.
2. Applicazione di configurazioni sicure a tutti i componenti del sistema.	Gli utenti, i dispositivi e le applicazioni che utilizzano Cloudflare sono fortemente crittografati e mascherati da potenziali aggressori sul Web. Lo scudo API di Cloudflare consente agli utenti di creare protezioni contro le vulnerabilità nelle loro API identificando sequenze e applicando criteri relativi alle transazioni API.
3. Protezione dei dati archiviati tramite crittografia o altri metodi di protezione.	Cloudflare è in grado di identificare le informazioni di identificazione personale (PII) inattive e soddisfa i requisiti per il tempo di conservazione del registro dei titolari della carta.
4. Crittografia dei dati dei titolari di carta su reti pubbliche aperte.	Il traffico inviato attraverso la rete globale di Cloudflare soddisfa gli standard di crittografia specificati in questo requisito e Cloudflare può bloccare la trasmissione delle informazioni di identificazione personale (PII) che l'utente deve identificare.
5. Protezione di tutti i sistemi e le reti da software dannoso.	Cloudflare serve oltre 55 milioni di richieste HTTP al secondo, offrendoci una visione unica e ad ampio raggio degli ultimi attacchi in circolazione. Cloudflare fornisce agli utenti una suite di protezioni antimalware, tra cui antivirus, sicurezza della posta elettronica nel cloud e Browser Isolation remoto.
6. Sviluppo e gestione sicura di sistemi e software.	Cloudflare può classificare e ponderare le violazioni della sicurezza degli utenti, nonché le configurazioni errate rilevate all'interno delle applicazioni SaaS. I servizi di sicurezza di Cloudflare possono proteggere tutte le applicazioni pubbliche rivolte al Web da attacchi ed exploit noti.
7. Limitazione dell'accesso ai dati dei titolari di carta in base alla "necessità di sapere".	Cloudflare può applicare controlli di accesso granulari e con privilegi minimi, indipendentemente da dove si trovano gli utenti o dove vengono archiviati i dati.
8. Identificazione degli utenti e autenticazione degli accessi ai componenti del sistema.	Cloudflare può applicare politiche basate sull'identità e controlli sullo stato di sicurezza (ad esempio, se è stato utilizzato MFA) per qualsiasi traffico che attraversa la sua rete globale.
10. Registrazione e monitoraggio di tutti gli accessi ai componenti del sistema e ai dati dei titolari di carta.	Cloudflare fornisce log di audit granulari su tutti i prodotti nella sua piattaforma e si integra con la maggior parte dei principali SIEM.
11. Esecuzione regolare di test per la sicurezza dei sistemi e delle reti.	Cloudflare fornisce test delle politiche di accesso limitato e funzionalità del servizio di rilevamento delle intrusioni, oltre a fornire log approfonditi per tutti i suoi principali prodotti.

*Cloudflare non fornisce assistenza con i requisiti PCI DSS 4.0 9 e 12, che riguardano la sicurezza fisica e la struttura organizzativa.

Riepilogo: Affidati a Cloudflare per soddisfare i requisiti di conformità PCI

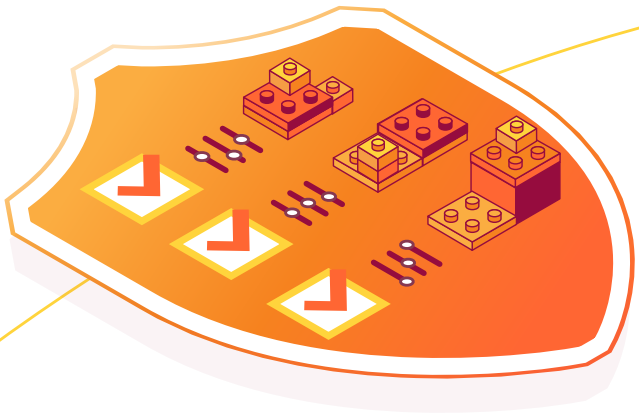
Cloudflare è conforme a PCI e dispone di funzionalità che aiutano i clienti a soddisfare autonomamente i requisiti di conformità, indipendentemente dall'aspetto della loro infrastruttura.

Infatti, l'uso di Cloudflare può comportare una riduzione del 65%[3] della probabilità di una violazione dei dati, una riduzione del 24%[4] sui premi annuali di assicurazione informatica e la riduzione del 59%[4] del tempo speso per gestire sistemi e processi.

I nostri clienti aziendali richiedono contrattualmente che Stax soddisfi standard di conformità molto specifici. Ciò ci ha portato a applicare controlli di sicurezza come Zero Trust in tutta la nostra infrastruttura... Cloudflare ha fatto esattamente ciò di cui avevamo bisogno. Ha protetto i nostri endpoint e ha bloccato la nostra sicurezza." [5]

Troy Ridgewell
Responsabile della sicurezza Stax

STAX



Scopri le soluzioni di conformità dei dati di Cloudflare oggi stesso. Parla con i nostri esperti per iniziare.

Riferimenti

1. https://www.isaca.org/about-us/newsroom/press-releases/2023/privacy-staff-shortages-continue-amid-increasing-demand-for-these-roles
2. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf
3. Report IBM Costi delle violazioni di dati, 2022
4. Sondaggio Cloudflare TechValidate 2023 sui clienti del servizio app Cloudflare
5. https://www.cloudflare.com/case-studies/stax

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

REV:BDES-5776.2024APR09