CLOUDFLARE

LIVRE BLANC

Une approche stratégique du respect de la conformité PCI DSS 4.0

Sommaire

Vue d'ensemble

Toutes les entreprises qui traitent des cartes de paiement (crédit, débit ou cartes prépayées) doivent respecter la Payment Card Industry Data Security Standard (PCI DSS, norme de sécurité des données du secteur des cartes de paiement). Les entités concernées regroupent les petits commerçants, les revendeurs, les sites web d'e-commerce, les banques et les grandes entreprises. Toutefois, le passage au cloud et au travail hybride, associé à l'évolution des normes (le déploiement de la norme PCI DSS 4.0, par exemple), complique la marche à suivre pour respecter la conformité de manière efficace.

Le monde moderne numérique a besoin d'une nouvelle approche pour rationaliser le processus de conformité d'une manière évolutive, afin de permettre aux entreprises de soutenir la cadence imposée par un paysage réglementaire dynamique, qui s'assure lui-même de rester en phase avec le processus de modernisation numérique des entreprises.

Les défis posés par la conformité PCI DSS pour les entreprises d'aujourd'hui

La conformité PCI est cruciale, et les contrevenants s'exposent à des amendes, des poursuites judiciaires et des enquêtes gouvernementales. Pourtant, le processus de conformité présente diverses difficultés pour les institutions financières, les e-commerçants et les autres entités soumises à ses règlements.

Répartition du temps et des ressources : 53 % des entreprises déclarent que les postes techniques chargés de la confidentialité manquent de personnel. Or, ce point vient encore compliquer le respect de la conformité.[1]

Complexité de l'intégration à la pile technologique : l'intégration et la maintenance des technologies nécessaires au respect des normes de conformité, comme le chiffrement et les configurations de pare-feu, se révèlent souvent complexes. Ce problème est encore aggravé dans les entreprises disposant de systèmes d'ancienne génération ou en cours de transformation numérique.

Conformité des fournisseurs : le fait de s'assurer que les fournisseurs et les prestataires de services tiers se conforment aux normes PCI ajoute une couche supplémentaire de complexité.

En outre, comme les équipes informatiques ont perdu le contrôle de leurs environnements numériques en raison du recours accru à l'informatique cloud et au travail à distance, la résolution de ces défis s'avère plus difficile.

Sécurité des données au sein d'environnements divers : avec l'essor de l'informatique cloud et des paiements par mobile, le respect de la conformité au sein d'environnements divers et souvent moins contrôlés s'avère de plus en plus difficile.

Auditing : pour assurer la conformité, les équipes informatiques doivent maintenir une piste d'audit à jour sur l'ensemble de l'infrastructure et des systèmes.

Suivre le rythme de l'évolution des cybermenaces sophistiquées grâce à la norme PCI DSS 4.0

La norme PCI DSS 4.0 a été publiée le 3 mars 2022 et est entrée en vigueur le 31 mars 2024, avec des conditions supplémentaires devant prendre effet le 31 mars 2025. Les objectifs de la norme PCI DSS 4.0 sont les suivants :[2]

1. **Continuer à répondre aux besoins en matière de sécurité du secteur des paiements**

- **Conditions d'authentification renforcées :** la norme insiste encore sur l'authentification, notamment l'authentification multi-facteurs (Multi-Factor Authentication, MFA), pour tous les accès à l'environnement CDE (Cardholder Data Environment, environnement de données des titulaires de cartes). Les conditions encadrant les mots de passe sont également plus strictes, ces derniers passant de 8 à 12 caractères minimum.
- **Exigences renforcées en matière de chiffrement :** la norme PCI DSS 4.0 impose l'utilisation d'un chiffrement « fort » pour le stockage et la transmission des données des titulaires de cartes (comme le protocole TLS, qui n'est pas vulnérable aux exploitations connues).
- **Nouvelles conditions relatives à l'e-commerce et au phishing pour répondre aux menaces actuelles :** la norme PCI 4.0 contient des conditions supplémentaires régissant la sécurité côté client, ainsi que la protection contre le phishing et l'ingénierie sociale.

2. **Promouvoir la sécurité en tant que processus continu**

- **Accent supplémentaire sur l'analyse et la gestion des risques :** les entreprises sont encouragées à mettre en œuvre des processus continus d'analyse et de gestion des risques afin d'identifier rapidement les vulnérabilités et d'y répondre.
- **Accent supplémentaire sur la responsabilité et la gouvernance :** la nouvelle version insiste encore sur la gouvernance des données des titulaires de cartes, ainsi que sur la responsabilité liée à la maintenance des mesures de sécurité.
- **Plus de conseils pour la mise en œuvre et le respect des exigences en matière de sécurité :** la version PCI 4.0 clarifie l'intention de la norme et les intervalles utilisés.

3. **Ajouter de la flexibilité pour des méthodologies différentes**

- **Intégration des nouvelles technologies :** la norme PCI DSS 4.0 répond à la sécurité des technologies émergentes, comme le cloud et les systèmes de paiement mobiles.
- **Plus de flexibilité dans la manière dont les entreprises peuvent réaliser leurs objectifs de sécurité :** les entreprises peuvent suivre une « approche personnalisée », c'est-à-dire une gamme plus étendue de méthodes, pour répondre aux exigences. De même, la norme PCI 4.0 propose davantage de flexibilité dans l'établissement de la fréquence à laquelle elles effectuent des actions en fonction d'analyses ciblées des risques.

4. **Renforcer les méthodes de validation**

- **Surveillance et tests en continu :** la nouvelle norme encourage le passage d'une validation annuelle de la conformité à un processus de surveillance continue de la sécurité et de la conformité.
- **Alignement accru entre les évaluations et les attestations de conformité :** les informations contenues au sein des questionnaires ou des rapports d'auto-évaluation de la conformité sont plus alignées avec le résumé fourni dans les attestations de conformité.

Solution : une nouvelle approche des exigences PCI via la connectivité cloud de Cloudflare

Les équipes chargées de l'informatique et de la sécurité doivent répondre aux exigences PCI d'une manière simple et programmable, qui s'intègre facilement à leur pile technologique et à leur pile de sécurité actuelles, tout en pouvant continuer à suivre l'évolution de leur infrastructure et des normes PCI DSS.

Une approche hétérogène, comportant de nombreuses solutions dédiées et des services d'ancienne génération, ne permettra pas de répondre à ce problème. À la place, les équipes ont besoin d'une plateforme unifiée de services de sécurité et de services réseau cloud-native, conçue pour aider les entreprises à reprendre le contrôle de leurs environnements informatiques et à répondre à diverses exigences de conformité, dont la norme PCI. Une telle plateforme unifiée existe. C'est ce que nous appelons la connectivité cloud.

La connectivité cloud de Cloudflare propose :

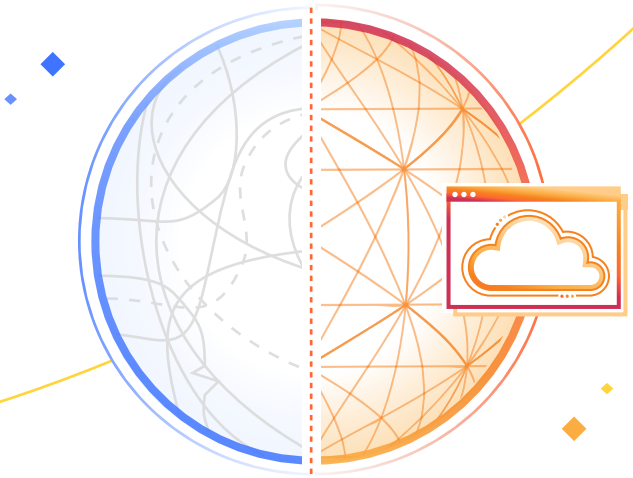
- une plateforme conçue pour la conformité des données ;
- un moteur de politiques unifié ;
- la souveraineté des données, sans compromis ;
- un service de reporting intelligent pour satisfaire les audits.

Cloudflare permet aux équipes informatiques d'appliquer des mesures de contrôle cohérentes sur l'ensemble des emplacements, activables partout grâce à un plan de contrôle unique.

Les équipes peuvent envoyer directement les journaux de la périphérie du réseau Cloudflare vers votre SIEM ou votre cloud de destination préféré à des fins d'audit. De même, la visibilité à grande échelle de Cloudflare sur le trafic Internet vous permet d'identifier automatiquement les nouvelles menaces et de vous défendre contre elles.

Le réseau Cloudflare lui-même est conforme PCI et prend en charge nativement les exigences de la norme PCI DSS 4.0. Cloudflare permet ainsi aux équipes informatiques de mettre facilement en œuvre l'authentification multi-facteurs, soit l'un des axes majeurs de la PCI DSS 4.0. Cloudflare prend également en charge les dernières normes de chiffrement et contribue souvent à leur élaboration, afin d'aider ses clients à répondre aux exigences de la norme PCI DSS 4.0 concernant le chiffrement et les informations sensibles.

Vous trouverez un récapitulatif des correspondances entre les exigences de la norme PCI DSS et les fonctionnalités de la connectivité cloud de Cloudflare en page suivante :



Les domaines essentiels dans lesquels Cloudflare peut vous aider à répondre aux exigences PCI*

Exigence PCI	Fonctionnalité Cloudflare
1. Installer et maintenir des mesures de contrôle de la sécurité réseau (anciennement, « Installer et maintenir un pare-feu »).	Cloudflare protège à la fois les réseaux, les applications et les déploiements cloud contre le trafic réseau malveillant. Nous nous appuyons sur un ensemble d'informations sur les menaces issu des centaines de milliards de menaces observées chaque jour pour protéger les sites et les applications web contre les menaces véhiculées par Internet, dont les attaques figurant au Top 10 de l'OWASP et les attaques zero-day. Notre plateforme cloud-native se déploie en quelques minutes et permet aux utilisateurs de déployer des modifications de politiques à l'échelle mondiale en quelques secondes.
2. Appliquer des configurations sécurisées à l'ensemble des composants d'un système.	Les utilisateurs, les applications et les appareils protégés par Cloudflare bénéficient d'un chiffrement fort et sont dissimulés aux yeux des potentiels acteurs malveillants sévissant sur Internet. La solution API Shield de Cloudflare permet aux utilisateurs de créer des mesures de protection contre les vulnérabilités de leurs API en identifiant des séquences et en appliquant des politiques encadrant les transactions d'API.
3. Protéger les données stockées par le biais du chiffrement ou d'autres méthodes de protection des données.	Cloudflare peut identifier les informations d'identification personnelle (PII, Personally Identifiable Information) au repos et son réseau répond aux exigences concernant le délai de conservation des journaux des titulaires de cartes.
4. Chiffrer les données des titulaires de cartes sur l'ensemble des réseaux ouverts et publics.	Le trafic envoyé par l'intermédiaire du réseau mondial de Cloudflare est conforme aux normes de chiffrement spécifiées dans cette exigence. De même, Cloudflare peut bloquer la transmission des PII dont l'utilisateur a besoin pour s'identifier.
5. Protéger l'ensemble des réseaux et des systèmes contre les logiciels malveillants.	Cloudflare diffuse plus de 55 millions de requêtes HTTP par seconde. Nous disposons ainsi d'une vision unique et particulièrement large sur les dernières attaques sévissant actuellement. Cloudflare propose une suite de protections anti-logiciels malveillants aux utilisateurs, notamment un antivirus, une solution de sécurité du courrier électronique cloud et l'isolement de navigateur à distance.
6. Développer et maintenir la sécurité des réseaux et des logiciels.	Cloudflare peut classer et évaluer les violations de sécurité des utilisateurs, ainsi que les erreurs de configuration, détectées au sein des applications SaaS. Les services de sécurité Cloudflare peuvent protéger l'ensemble des applications en contact avec Internet contre les attaques et les exploitations connues.
7. Limiter l'accès aux données des titulaires de cartes en fonction des besoins.	Cloudflare peut appliquer des mesures de contrôle des accès granulaires, basées sur le principe du moindre privilège, indépendamment de l'endroit où se situent les utilisateurs ou dans lequel les données sont stockées.
8. Identifier les utilisateurs et authentifier l'accès aux composants du système.	Cloudflare peut appliquer des politiques basées sur l'identité et des mesures de contrôle de la stratégie de sécurité (p. ex. lorsque la MFA est utilisée) à n'importe quel trafic circulant sur son réseau mondial.
10. Journaliser et surveiller tous les accès aux composants système et aux données des titulaires de cartes.	Cloudflare fournit des journaux d'audit détaillés pour l'ensemble des produits de sa plateforme et s'intègre à la plupart des grands SIEM.
11. Tester régulièrement la sécurité des systèmes et des réseaux.	Cloudflare propose un service de détection des intrusions et de test des politiques d'accès limité, en plus de fournir des journaux approfondis pour l'ensemble de ses principaux produits.

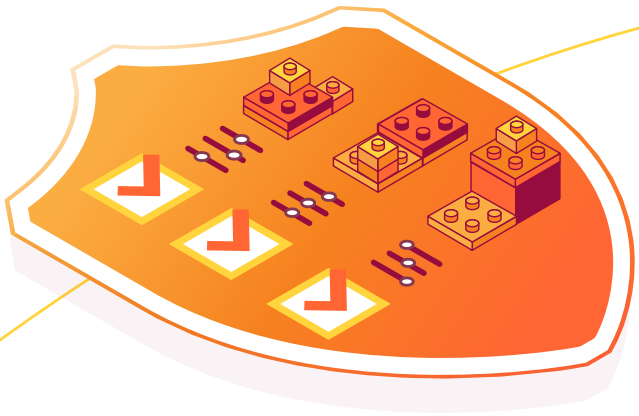
* Cloudflare n'offre aucune assistance concernant le respect des exigences 9 et 12 de la norme PCI DSS 4.0, qui traitent de la sécurité physique et de la structure organisationnelle.

Récapitulatif : faire confiance à Cloudflare peut vous aider à répondre aux exigences PCI

Conforme PCI, la plateforme Cloudflare peut aider ses clients à répondre eux-mêmes aux exigences de conformité, peu importe l'état de leur infrastructure.

En fait, l'utilisation de Cloudflare peut entraîner une réduction de 65 %[3] du risque de violation de données, de 24 %[4] du montant des primes de cyber-assurance et de 59 %[4] du temps consacré à la gestion des systèmes/processus.

> **Les clients de notre entreprise exigent contractuellement que Stax se conforme à des normes très spécifiques. Ce point nous a conduit à appliquer des mesures de contrôle de la sécurité, telles que le Zero Trust, sur l'ensemble de notre infrastructure... La plateforme Cloudflare a fonctionné exactement comme nous le souhaitions. Elle a protégé nos points de terminaison et verrouillé notre sécurité. »**[5]
>
> **Troy Ridgewell**
> Head of Security, Stax
>
> STAX



Découvrez les solutions de conformité des données de Cloudflare dès aujourd'hui. Discutez avec nos experts pour bien démarrer.

Références

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. IBM, Cost of a data breach 2022 (Coût d'une violation de données en 2022)
4. Étude Cloudflare TechValidate 2023 sur les clients des services Cloudflare pour applications
5. https://www.cloudflare.com/case-studies/stax/

CLOUDFLARE

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES-5776.2024APR09