PRÉSENTATION DE LA SOLUTION AKAMAI

Conformité à la norme PCI DSS v4.0 avec Akamai

La conformité PCI consiste à adhérer à un ensemble mondial d'exigences de sécurité visant à protéger et à sécuriser les environnements contenant des données de comptes de cartes de paiement. Toute entreprise qui traite, transmet ou stocke des données de titulaires de cartes en ligne est tenue de respecter la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS). Élaborée en 2004, cette norme est régulièrement mise à jour pour répondre aux changements du secteur et à l'évolution des menaces en matière de cybersécurité. La dernière norme, PCI DSS v4.0, a été publiée en mars 2022 avec des modifications importantes et contient 12 exigences fondamentales que les entreprises doivent respecter d'ici mars 2025.

Êtes-vous prêt pour la norme PCI DSS v4.0 ?

Bien que le non-respect des normes PCI ne soit pas punissable par la loi, les sociétés émettrices de cartes de crédit peuvent imposer des amendes aux entreprises qui ne respectent pas la norme. En outre, le fait de ne pas sécuriser les données des titulaires de cartes peut rendre les marques vulnérables aux cyberattaques, des cyberattaques qui entraînent des violations de données dévastatrices, des amendes élevées et une perte de confiance permanente de la part des clients.

Nous sommes là pour vous aider. Non seulement Akamai maintient la conformité PCI DSS de niveau 1, mais nous proposons également un large éventail de solutions de sécurité de pointe pour aider les entreprises à se conformer à la norme PCI DSS v4.0. Certaines solutions permettent même de réduire la portée d'un audit PCI, ce qui donne l'occasion d'économiser du temps et de l'argent pour répondre aux exigences de certification.

App & API Protector avec protection contre les logiciels malveillants

Maintenez la conformité des journaux et protégez-vous contre les fuites d'informations personnelles identifiables, les attaques Zero Day et les CVE, ainsi que d'autres attaques en bordure de l'Internet, afin de respecter les exigences 6.4.2, 6.5.3 et 11.5.

> « Chaque jour, 560 000 nouveaux logiciels malveillants sont détectés, s'ajoutant aux plus d'un milliard de programmes malveillants déjà en circulation. »
>
> Source : Getastra | 30+ Malware Statistics You Need to Know In 2023

Avantages

- **Rationalisation des flux de travail** pour les équipes chargées de la sécurité et de la conformité
- **Réduction de la charge d'audit** grâce à des fonctionnalités PCI dédiées et conçues à cet effet
- **Réception et enregistrement d'alertes PCI exploitables** pour les événements liés à la conformité
- **Consolidation des fournisseurs** pour répondre aux exigences PCI grâce au portefeuille complet de solutions de sécurité d'Akamai

| Publication : 04/24

API Security

Détectez et atténuez les comportements et logiques abusifs des API, consignez l'activité des API et mettez en œuvre une protection réactive et automatisée pour vos API afin de répondre aux exigences de conformité 6.2.3, 6.2.4, 6.3.2, 6.4.1, 6.4.2, 10.2.1,10.5.1 et 11.3.2.

> **« En 2024, les abus d'API et les violations de données associées devraient presque doubler. »**
>
> Source : Gartner: Top 10 Aspects Software Engineering Leaders Need to Know About APIs (disponible en anglais uniquement)

Client-Side Protection & Compliance

Répondez aux nouvelles exigences de sécurité JavaScript 6.4.3 et 11.6.1 en vous protégeant contre les attaques côté client, telles que le skimming Web ou les attaques de type Magecart, qui écrèment et exfiltrent des données de cartes de paiement à partir de pages de paiement en ligne par l'injection d'un code malveillant exécuté dans le navigateur.

> **« 81 % des grands détaillants en ligne déclarent que leur organisation a été la cible de comportements de script suspects en 2022. »**
>
> Source : From Bad Bots to Malicious Scripts: The Effectiveness of Specialized Defense | 2023 (disponible en anglais uniquement)

Akamai Guardicore Segmentation

Segmentez les actifs réglementés plus efficacement en tirant parti de plusieurs technologies intégrées au sein d'une même plateforme afin de répondre à de nombreuses exigences PCI. Bénéficiez d'une visibilité sur le réseau et les actifs, d'un pare-feu distribué, d'une application des règles jusqu'à la couche 7 et d'une détection et d'une réponse en cas de violation.

> **« La segmentation définie par logiciel nous a permis de créer et d'appliquer des règles de segmentation au niveau des processus, ce qui a considérablement amélioré notre posture de sécurité et notre capacité à répondre aux exigences techniques de la norme PCI-DSS. »**
>
> — Senior Infrastructure Engineer, The Honey Baked Ham Company

Pour en savoir plus sur la façon d'accélérer la mise en conformité avec la norme PCI DSS v4.0 avec Akamai, contactez notre équipe d'experts.

| Publication : 04/24