LISTE DE CONTRÔLE D'AKAMAI

Liste de contrôle de sécurité JavaScript PCI DSS v4.0 avec Akamai Client-Side Protection & Compliance

La norme de sécurité de l'industrie des cartes de paiement (PCI DSS) est une norme de sécurité internationale élaborée pour protéger la sécurité des données des cartes de paiement en ligne et pour faciliter l'adoption généralisée de mesures cohérentes de sécurité des données à l'échelle mondiale. Il s'agit de l'une des normes de sécurité les plus importantes, à laquelle toute organisation qui traite les données des cartes de paiement en ligne exige de se conformer.

La dernière version de la norme PCI DSS (disponible en anglais uniquement), version 4.0, entrera en vigueur en 2025. Elle comprend 12 exigences essentielles en matière de sécurité des données, mises à jour avec des conseils pour faire face aux menaces nouvelles et en évolution de la cybersécurité. Deux exigences majeures ajoutées à la norme PCI DSS version 4.0, 6.4.3 et 11.6.1 concernent la sécurité JavaScript et la protection contre les attaques de web skimming côté client qui volent des informations sensibles de l'utilisateur final à partir du navigateur. Ces attaques ont gagné en popularité au fil des ans et des techniques sophistiquées les rendent de plus en plus difficiles à détecter. Elles peuvent avoir des conséquences dévastatrices pour les entreprises qui en sont victimes, notamment de lourdes amendes, une atteinte à la réputation de la marque, une perte de revenus et une diminution de la confiance des clients.

Passons en revue une liste de contrôle pour comprendre ce qu'impliquent les nouvelles exigences en matière de sécurité des scripts de la norme PCI DSS v4.0 et ce que peut apporter Client-Side Protection & Compliance.

Exigences de la norme PCI DSS v4.0	Rôles de Client-Side Protection & Compliance
Exigence 6.4.3 : les applications Web destinées au public sont protégées contre les attaques	**Octroi d'autorisations en un clic**
☑ Une méthode est mise en œuvre pour confirmer que chaque script chargé et exécuté dans le navigateur est autorisé	☑ Gérez facilement les scripts que vous autorisez à exécuter sur les pages de paiement de votre site Web directement dans l'outil
☑ Une méthode est mise en œuvre pour assurer l'intégrité de chaque script chargé et exécuté dans le navigateur	**Intégrité garantie dès le départ**
☑ Un inventaire de tous les scripts chargés et exécutés dans le navigateur est tenu à jour avec une justification écrite de leur nécessité	☑ La technologie comportementale analyse chaque script exécuté dans le navigateur pour détecter et donner l'alerte en cas d'activité malveillante ou d'exfiltration de données
	Suivi et inventaire automatiques de l'ensemble des scripts
	☑ Les justifications prédéfinies et les règles automatisées permettent de justifier facilement le rôle de chaque script chargé et exécuté dans le navigateur

Akamai

Exigences de la norme PCI DSS v4.0	Rôles de Client-Side Protection & Compliance
Exigence 11.6.1 : les modifications non autorisées sur les pages de paiement sont détectées et traitées en conséquence **Un mécanisme de détection des modifications et des falsifications est déployé comme suit :** ☑ Il permet d'alerter le personnel en cas de modification non autorisée (y compris des indicateurs d'infection, de changements, d'ajouts et de suppressions) des en-têtes HTTP et du contenu des pages de paiement tel que reçu par le navigateur de l'internaute ☑ Le mécanisme est configuré pour évaluer l'en-tête HTTP et la page de paiement reçus **Les fonctions du mécanisme sont exécutées** au moins une fois tous les sept jours ou périodiquement (à la fréquence définie dans l'analyse des risques ciblés de l'entité, qui est effectuée conformément à tous les éléments spécifiés à l'exigence 12.3.1).	**Protection des pages de paiement** ☑ Surveillez, analysez et atténuez la falsification malveillante des pages de paiement pour garantir la sécurité des données précieuses de votre utilisateur final **Analyse des modifications non autorisées en temps réel avec alertes immédiates et exploitables** ☑ Grâce à la détection instantanée, les équipes de sécurité peuvent réagir rapidement aux changements non autorisés ou aux modifications apportées aux en-têtes HTTP sur les pages de paiement **Défense en continu** ☑ Une protection 24 h/24 protège les interactions des utilisateurs sur vos pages de paiement

La solution Client-Side Protection & Compliance d'Akamai offre une protection robuste contre les menaces JavaScript et assure une visibilité de la surface d'attaque côté client afin de protéger les données sensibles dans le navigateur. Ses fonctionnalités PCI DSS v4.0 spécialement conçues aident les équipes de sécurité et de conformité à rationaliser le processus d'audit PCI DSS v4.0 et fournissent des workflows dédiés pour aider à répondre aux exigences de sécurité des scripts 6.4.3 et 11.6.1.

La solution Client-Side Protection & Compliance d'Akamai offre des options de déploiement flexibles et ne nécessite pas l'activation d'Akamai Connected Cloud.

Découvrez comment ces fonctionnalités peuvent aider votre entreprise à se conformer à la norme PCI DSS v4.0.