FICHE PRODUIT AKAMAI

Client-Side Protection & Compliance

Protégez-vous contre les vulnérabilités JavaScript côté client et rationalisez la conformité réglementaire

JavaScript est un outil essentiel pour les applications Web actuelles. Qu'il s'agisse d'optimiser l'expérience utilisateur ou d'améliorer les fonctionnalités et les performances, l'utilisation de JavaScript, à la fois en interne et en externe, s'est développée considérablement au fil du temps. En dépit des nombreux avantages liés à son utilisation, une chaîne d'approvisionnement digitale JavaScript peut également rendre les sites Web vulnérables aux attaques côté client qui visent à dérober les informations sensibles de l'utilisateur final à partir du navigateur, y compris les données des cartes de paiement, grâce à l'injection d'un code malveillant.

Dans la mesure où ces attaques sont peu visibles côté serveur et contournent les mesures de sécurité traditionnelles, les entreprises peuvent facilement devenir des cibles, réduisant ainsi la confiance que leur accordent leurs clients et entraînant des amendes réglementaires et des pénalités de conformité dévastatrices, ainsi qu'une atteinte à la réputation de leur marque.

Client-Side Protection & Compliance d'Akamai

La solution Client-Side Protection & Compliance d'Akamai permet de protéger les utilisateurs finaux contre l'exfiltration de leurs données et de protéger les sites Web contre les menaces JavaScript. Cette solution est conçue pour détecter les scripts malveillants et alerter les équipes de sécurité afin qu'elles réduisent les activités nuisibles en temps réel.

Grâce à ses fonctionnalités de conformité à la norme PCI DSS v4.0, la solution Client-Side Protection & Compliance aide les entreprises à répondre aux nouvelles exigences en matière de sécurité des scripts et à protéger les données des cartes de paiement contre les attaques côté client. Gérez facilement l'inventaire des scripts de votre page de paiement, rationalisez le processus d'audit via un tableau de bord unique et complet, et recevez des alertes PCI dédiées pour répondre rapidement aux événements liés à la conformité.

Principales fonctionnalités

Protection contre l'exfiltration de données sensibles côté client

Les cybercriminels sont à la recherche des informations sensibles de vos utilisateurs finaux. Grâce à l'exploitation des vulnérabilités dans les chaînes d'approvisionnement JavaScript, les acteurs malveillants sont en mesure d'injecter du code dans les sites Web afin d'extraire des informations sensibles et de les exfiltrer pour les utiliser à des fins frauduleuses. La solution Client-Side Protection & Compliance allie l'apprentissage automatique et l'évaluation heuristique pour analyser le comportement des scripts en temps réel et détecter les activités malveillantes et les ressources vulnérables. Les équipes de sécurité disposent ainsi d'alertes immédiates et exploitables pour se défendre rapidement contre les attaques côté client, notamment les attaques de web skimming, les attaques de type Magecart et le détournement de formulaires.

AVANTAGES POUR VOTRE ENTREPRISE

Détection et protection
Surveillez le comportement des scripts dans les sessions d'utilisateurs réels afin de détecter toute activité suspecte

Flux de travail PCI DSS v4.0
Aidez à répondre aux exigences de sécurité JavaScript 6.4.3 et 11.6.1

Alertes prioritaires en temps réel
Atténuez immédiatement les événements à haut risque à l'aide d'alertes exploitables

Visibilité côté client
Bénéficiez d'une vue étendue de la surface d'attaque côté client

Gestion des politiques
Régulez le comportement des scripts et contrôlez la durée d'exécution de JavaScript au moment de l'exécution

Détection des vulnérabilités
Identifiez les vulnérabilités et failles courantes (CVE) grâce aux informations sur les menaces d'Akamai

Options de déploiement flexibles
Déployez facilement depuis Akamai Connected Cloud ou directement sur le serveur d'origine

Akamai

Support dédié à la conformité PCI DSS v4.0

Les exigences de sécurité des scripts PCI DSS v4.0 6.4.3 et 11.6.1 stipulent que les organisations doivent protéger les données des cartes de paiement contre les attaques côté client et assurer la gestion des scripts sur les pages de paiement. La solution Client-Side Protection & Compliance suit et inventorie tous les scripts sur les pages de paiement, garantissant leur intégrité et leur autorisation. Elle fournit des justifications prédéfinies et des règles automatisées pour expliquer facilement le bien-fondé de tous les scripts chargés. La solution assure également le suivi des modifications apportées aux en-têtes HTTP et à la protection des pages de paiement afin de se prémunir contre la falsification des pages. Un tableau de bord complet et des alertes PCI dédiées permettent aux organisations de réagir rapidement aux événements liés à la conformité et d'assurer la protection des données des cartes de paiement au sein du navigateur. Grâce à ces fonctionnalités, les équipes chargées de la sécurité et de la conformité peuvent réduire la charge du processus d'audit PCI et rationaliser rapidement les flux de travail.

Visibilité étendue sur les menaces JavaScript

Les protections traditionnelles des applications Web, telles que les pare-feu d'application Web, ne surveillent que le trafic côté serveur et ne peuvent pas fournir de visibilité sur les activités exécutées côté client. Les méthodes de protection standard contre ces menaces, telles que les politiques de sécurité du contenu, sont difficiles à gérer et ne fournissent qu'une protection limitée contre les charges utiles malveillantes introduites dans la chaîne d'approvisionnement des scripts en dehors du contrôle des opérateurs de pages Web. Cette situation crée un angle mort pour les organisations, ce qui permet au code malveillant de ne pas être détecté pendant des jours, des semaines, voire des mois, alors qu'il continue à voler des données sensibles. La solution Client-Side Protection & Compliance fournit une vue inégalée de la surface d'attaque côté client sur votre site Web, et notamment du comportement, des vulnérabilités, de la portée et de l'impact de chaque script, ainsi que des données consultées ou de la menace posée.

Fonctionnement

La solution Client-Side Protection & Compliance s'exécute dans le navigateur de l'utilisateur final pour surveiller les exécutions de scripts côté client sur une page Web protégée. Lorsque les scripts indiquent un changement de comportement, des techniques d'apprentissage automatique sont appliquées pour évaluer le risque d'actions non autorisées ou inappropriées. Les équipes de sécurité sont ainsi alertées des événements à haut risque, ce qui leur permet d'enquêter immédiatement sur les menaces potentielles et d'en atténuer les effets.

Configuration Des scripts simples sont injectés dans chaque page surveillée, sans impact significatif sur les performances.

Surveillance et évaluation Les données relatives à l'activité JavaScript sont collectées à partir du navigateur Web de l'utilisateur et surveillées. Des techniques d'apprentissage automatique sont utilisées pour évaluer le risque d'actions non autorisées ou inappropriées, le cas échéant.

Alerte Des alertes en temps réel contenant des informations détaillées pour atténuer les menaces sont envoyées si une menace ou une attaque active est détectée.

Atténuation Les fichiers JavaScript malveillants sont immédiatement limités dans l'accès et l'exfiltration des données sensibles sur les pages protégées, d'un simple clic.

Accélérer la conformité de la sécurité des scripts PCI DSS v4.0

Intégrité et autorisation des scripts (6.4.3)

Garantit l'intégrité et l'autorisation de tous les scripts chargés sur les pages de paiement protégées.

Inventaire et justification des scripts (6.4.3)

Suit et inventorie les scripts chargés sur les pages de paiement protégées. Permet de justifier rapidement tous les scripts, grâce à des justifications prédéfinies et à des règles automatisées.

Protection des pages de paiement (11.6.1)

Détecte et réagit immédiatement aux changements non autorisés sur les pages de paiement protégées.

Tableau de bord intuitif

Simplifie le processus de conformité et d'audit PCI DSS v4.0 grâce à un tableau de bord dédié contenant des informations détaillées sur les tâches et les alertes liées aux exigences de sécurité des scripts 6.4.3 et 11.6.1.

Alertes PCI exploitables

Les alertes détaillées concernant les événements liés à la conformité PCI, notamment les scripts non autorisés, l'exfiltration des données de paiement et la falsification des pages de paiement, sont reçues et consignées dans un journal.

Pour en savoir plus, rendez-vous sur notre page produit ou contactez l'équipe commerciale Akamai.