PRÉSENTATION DE LA SOLUTION AKAMAI

Préparation des institutions financières à la conformité PCI DSS avec Akamai

Alors que la norme PCI DSS v4.0 apporte les changements les plus drastiques aux normes de sécurité de l'industrie des cartes de paiement depuis 2004, les institutions financières doivent s'adapter rapidement pour rester conformes. Ce cadre exhaustif, établi par le PCI Security Standards Council, impose des mesures rigoureuses pour protéger les données des titulaires de carte. Les solutions d'Akamai permettent aux institutions financières de répondre à ces exigences en constante évolution grâce à des fonctionnalités de sécurité avancées, une surveillance continue et des tests de pénétration robustes. Nos outils sont conçus pour rationaliser la conformité, protéger les informations des clients et aider votre institution à se préparer avant la date limite de mars 2025 de PCI.

Conformité unifiée : simplifier la norme PCI DSS avec un fournisseur unique

Pour les institutions financières, la conformité PCI DSS implique non seulement la formation des collaborateurs et des stratégies d'entreprise, mais également des logiciels de sécurité sophistiqués pour répondre à la plupart des exigences. Compte tenu de la nature exhaustive de ces exigences, cela implique souvent de travailler avec plusieurs fournisseurs. Certaines exigences peuvent nécessiter un pare-feu, tandis que d'autres couvrent la gestion des identités. Les institutions financières qui sauront trouver un fournisseur unique disposant d'une technologie intégrée verront un processus d'audit simplifié et une sécurité améliorée des informations financières de leurs clients. L'adoption de solutions de cybersécurité robustes répondant à ces exigences dans le cadre d'une stratégie de sécurité plus vaste peut entraîner des économies de coûts et une réduction de la complexité à long terme. Le portefeuille de solutions d'Akamai répond de manière exhaustive aux exigences PCI DSS existantes et à venir, offrant une expérience fluide aux institutions financières.

Avantages

- **Rationalisez les flux de travail de sécurité et de conformité**
- **Réduisez les charges d'audit grâce à des fonctionnalités PCI dédiées**
- **Recevez et consignez des alertes de conformité PCI exploitables**
- **Protégez les données financières sensibles**
- **Améliorez l'efficacité opérationnelle et réduisez les coûts de conformité**

Gestion du champ d'application

La question du champ d'application constitue un défi de taille pour toute institution financière cherchant à répondre aux exigences de la norme PCI DSS. Les applications et les environnements réseau considérés comme étant « dans le champ d'application » de la norme PCI peuvent être complexes et couvrir différents types d'infrastructures, de technologies et de sites. À mesure que les institutions financières ont adopté le cloud pour l'infrastructure et pour les applications basées sur le SaaS, cet environnement hybride, entre le « sur site » et le « à la demande », ajoute une couche de complexité supplémentaire. Pour les institutions financières, y compris celles qui ont des entreprises de commerce électronique à ajustement automatique, comprendre l'emplacement d'une charge de travail donnée à tout moment peut être particulièrement difficile.

Les institutions financières se sont tournées vers les pare-feux internes, les VLAN et les listes de contrôle d'accès pour relever le défi de la portée. Cependant, ces applications héritées luttent souvent avec le rythme des environnements hybrides, ce qui génère de la complexité supplémentaire, des temps d'arrêt et des frais généraux d'exploitation tout en laissant des lacunes en matière de sécurité.

Akamai Guardicore Segmentation assure la visibilité sur l'environnement des données des titulaires de cartes (EDTC) et ses limites, une étape cruciale dans le processus de conformité. Cette visibilité aide les institutions financières à répondre aux multiples exigences de la norme PCI DSS et garantit une surveillance complète de leur réseau. Par exemple :

- L'exigence 1.2.3 nécessite que les organisations disposent d'un schéma de leur réseau. Le tableau de bord d'Akamai Guardicore Segmentation affiche tous les liens entre l'EDTC et les autres réseaux, aidant ainsi les institutions financières à répondre à cette exigence.
- L'exigence 1.2.4 implique que les organisations conservent un diagramme des flux de données montrant comment les données relatives aux comptes circulent entre les systèmes et les réseaux. Le tableau de bord d'Akamai Guardicore Segmentation aide les institutions financières à valider cette exigence en affichant les connexions nécessaires.

Gestion des contrôles

- L'exigence 1.2.5 précise la nécessité d'identifier, d'approuver et d'avoir une justification opérationnelle claire pour tous les services, protocoles et ports autorisés. Akamai Guardicore Segmentation aide les institutions financières à répondre à cette exigence en mettant en œuvre des règles appliquées de manière universelle, déterminant les protocoles ou services qui sont autorisés et ceux qui ne le sont pas.

Gestion de la protection côté client

Les institutions financières qui acceptent les données des cartes de paiement ne sont pas seulement responsables de leur propre environnement. L'utilisation de JavaScript dans le développement Web a apporté innovation et cohérence, mais elle a également créé des difficultés pour les organismes de traitement des cartes de paiement. L'exécution décentralisée côté client de JavaScript et les dépendances de tiers rendent la surveillance et la gestion des institutions financières extrêmement difficiles. Les pirates ont exploité cette difficulté pour injecter du code nuisible dans les sites Web côté client afin de voler des données sensibles. Ces types d'attaques (y compris le Web skimming, le détournement de formulaire et les attaques de type Magecart) ont gagné en popularité, ce qui a occasionné de nouvelles exigences concernant les protections côté client et la surveillance des scripts.

La norme PCI DSS v4.0 exigera des institutions financières qu'elles suivent, inventorient et justifient tous les scripts JavaScript exécutés sur les pages de paiement de leur site Web accessible au public. Conformément à l'exigence 6.4.3, elles devront garantir l'intégrité comportementale et l'autorisation de tous les scripts, et fournir un inventaire de ces scripts ainsi qu'une justification écrite de leur nécessité. En outre, conformément à l'exigence 11.6.1, les institutions financières doivent détecter toute modification non autorisée apportée à leurs pages de paiement, et y réagir. Le personnel autorisé doit être alerté de toutes les modifications, y compris des indicateurs de compromission, des changements, des ajouts ou des suppressions, apportées aux en-têtes HTTP et au contenu de la page de paiement par le navigateur de l'utilisateur.

Grâce à Akamai Guardicore Segmentation, nous avons considérablement réduit notre surface d'attaque sans les coûts et les retards associés à la mise à niveau des pare-feux existants.

– Dave Wigley,
CISO, Daiwa Capital Markets Europe

En résumé, la norme PCI DSS v4.0 oblige les institutions financières à :

- Conserver l'inventaire et la justification de chaque script exécuté sur les pages de paiement
- S'assurer que tous les scripts sont autorisés et qu'ils exécutent les actions pour lesquelles ils ont été conçus
- Mettre en place des mécanismes de détection, d'alerte et de réponse pour traiter les modifications non autorisées des scripts, la falsification de la protection et l'exfiltration de données sur les pages de paiement

Akamai Client-Side Protection & Compliance fournit un support étendu pour aider les institutions financières à répondre aux exigences 6.4.3 et 11.6.1 de la version 4.0 de la norme PCI DSS. Cette solution permet de suivre et d'inventorier automatiquement les scripts sur les pages de paiement, en accroissant leur intégrité et leur autorisation. Les équipes de sécurité peuvent facilement justifier l'objectif des scripts qui s'exécutent sur les pages de paiement, grâce à des critères prédéfinis et à des règles automatisées. La solution assure également le suivi des modifications apportées aux en-têtes HTTP et à la protection des pages de paiement afin d'empêcher la falsification des pages. Un tableau de bord complet et des alertes PCI dédiées permettent de répondre rapidement aux événements liés à la conformité et de fournir des preuves d'audit.

Protection contre les attaques

La protection des données des titulaires de carte est un principe fondamental de la norme PCI DSS, mais à mesure que les applications Web et les API se multiplient, elles peuvent également devenir des points d'entrée pour les pirates. Pour se conformer à la norme PCI DSS, les institutions financières ont besoin de protections solides contre les logiciels malveillants, les attaques Zero Day et d'autres attaques susceptibles d'entraîner des fuites de données.

Akamai App & API Protector avec le module de protection contre les logiciels malveillants peut aider les institutions financières à se protéger contre les fuites de données de cartes de paiement en analysant les fichiers en bordure de l'Internet avant qu'ils ne puissent pénétrer leurs systèmes et commencer à propager des logiciels malveillants. Les API peuvent introduire de nouvelles vulnérabilités que les attaquants à la recherche des données de cartes de paiement exploiteront. De nombreuses institutions financières ne peuvent même pas rendre compte de toutes les API, encore moins attester qu'elles sont sécurisées. Toute API qui reçoit ou transmet des données de titulaire de carte relève de la norme PCI DSS, ce qui signifie que les institutions financières doivent surveiller le développement et l'authentification des API et sécuriser ces API.

Akamai API Security automatise la découverte continue des API dans votre environnement. Cette solution attribue une note de risque à l'API et au point de terminaison, en comparant les API à la documentation existante et en informant les équipes de sécurité, de développement et d'API des configurations erronées et des vulnérabilités. Cette automatisation continue signifie que les vulnérabilités sont évaluées lorsque vous finalisez les mises à jour de votre parc d'API.

Conclusion

Bien que l'objectif ultime de la mise en œuvre des contrôles PCI DSS soit de protéger les données des titulaires de cartes préservant ainsi vos clients et votre entreprise, les institutions financières doivent néanmoins satisfaire les équipes d'audit. C'est là que le fait de disposer d'un fournisseur unique offre différents avantages. Grâce aux vues en temps réel et historiques de votre réseau, vous pouvez plus rapidement et plus facilement répondre à de nombreux aspects de vos audits. En outre, travailler avec un seul fournisseur dont le leadership est reconnu dans le secteur (et dont de nombreux clients ont répondu aux exigences de la norme PCI DSS) peut permettre des mises en œuvre plus fluides et des audits plus rapides, et fournir l'assistance nécessaire pour les besoins continus de conformité. La visibilité complète et les solutions intégrées d'Akamai aident les institutions financières à rationaliser leurs efforts de conformité et à renforcer leurs défenses contre des menaces en constante évolution.

Pour en savoir plus, rendez-vous sur akamai.com ou contactez votre équipe commerciale Akamai.