FORTRA™

LIVRE BLANC

Conformité PCI DSS 4.0

Quelques conseils pour éviter les paniques de dernière minute

Préserver la conformité est une mission difficile, que ce soit pour définir son périmètre ou pour la mettre en œuvre. Les organisations doivent respecter un large éventail de réglementations en augmentation constante. Dans un monde régi par des règles de conformité toujours plus strictes, les entreprises et les institutions financières doivent se familiariser avec les exigences de la norme PCI DSS 4.0 (Payment Card Industry Data Security Standard), dont la date limite de mise en œuvre est prévue pour 2024.

Le respect d'une norme (nouvelle ou mise à jour) est parfois plus complexe qu'il n'y paraît. En réalité, les entreprises sont tellement occupées à gérer les demandes informatiques du quotidien qu'elles finissent souvent par reléguer la conformité au second plan… jusqu'à ce que celle-ci devienne un problème urgent à résoudre. Cela est particulièrement vrai dans les entreprises qui ne disposent pas des ressources, du temps, du personnel et de la stratégie globale nécessaires pour une sécurité et une conformité robustes.

La pénurie de talents et les sous-effectifs sont des problèmes qui touchent tous les secteurs. Le personnel et le temps devenant des ressources rares, les entreprises privilégient alors les projets urgents plutôt que les initiatives à long terme. Conséquence d'une telle approche : une panique peut alors s'emparer des équipes au moment d'aborder la question de la conformité.

La bonne nouvelle, c'est que les détaillants et les entités financières peuvent traiter leurs opérations et leurs exigences de sécurité quotidiennes tout en consolidant leur conformité vis-à-vis du PCI DSS 4.0. Pour ce faire, elles adoptent une stratégie dite TIO (touch it once) qui consiste à exécuter deux tâches par le biais d'une seule action, à satisfaire les priorités du quotidien et à assurer une transition efficace vers le PCI DSS 4.0.

Pour résumer, il s'agit d'effectuer les tâches de façon à ne pas devoir les réévaluer par la suite. Selon la stratégie TIO (qui s'apparente davantage à une éthique, un mécanisme de pensée ou un concept plutôt qu'à une règle précise), chaque fois que vous devez créer un processus métier, faites-le en vous demandant « Dans quelle mesure ce processus rend-il notre entreprise plus sûre et plus conforme au PCI DSS 4.0 ? »

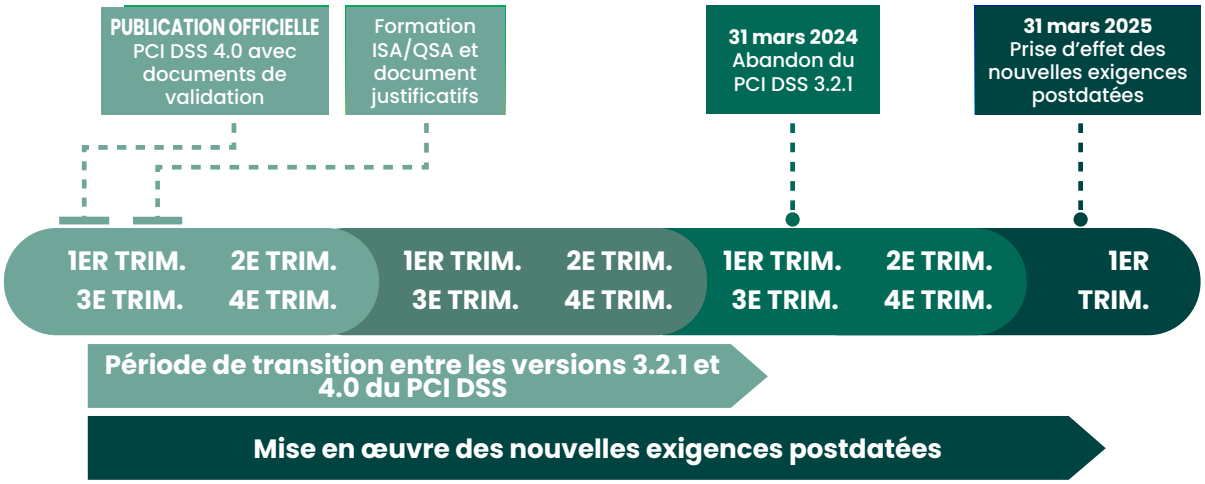
Ce guide vise à faciliter la compréhension des enjeux que sous-tend la conformité PCI DSS 4.0 et fournit un plan d'action priorisé afin de vous mettre en conformité, tout en protégeant votre entreprise des cyber-risques et autres menaces.

PCI DSS 4.0 : qu'est-ce qui change ?

La norme de sécurité de l'industrie des cartes de paiement (PCI DSS) a été créée en 2006 pour venir en aide aux entreprises traitant, stockant ou transmettant des données de cartes de paiement afin de prévenir le vol des données des titulaires de cartes. Spécifiquement conçu pour les environnements dans lesquels transitent les données des comptes des cartes de paiement, le PCI DSS peut également fournir une protection face aux menaces et sécuriser d'autres éléments de l'écosystème du paiement.

Les dates prévues pour l'adoption du PCI DSS 4.0 et l'arrêt du PCI DSS 3.2.1 se chevauchent afin d'assurer une transition sans heurts entre les deux versions. Ce chevauchement offre aux organisations suffisamment de temps pour se familiariser avec la nouvelle version ainsi que pour planifier et mettre en œuvre les changements nécessaires. Le diagramme ci-dessus (gracieusement fourni par le Conseil des normes de sécurité PCI) offre un aperçu de la chronologie de mise en œuvre du PCI DSS 4.0.

Chronologie de mise en œuvre du PCI DSS 4.0



Le PCI DSS 3.2.1 restera actif pendant deux ans après la publication de la version 4.0. Ce chevauchement offre aux organisations suffisamment de temps pour se familiariser avec la nouvelle version, ainsi que pour planifier et mettre en œuvre les changements nécessaires.

La mise en œuvre des modifications induites par la version 4.0 se justifie par quatre raisons clés :

- Veiller à ce que la norme respecte les exigences relatives aux paiements numériques sécurisés
- Promouvoir la sécurité en tant que processus dynamique continu
- Rendre les procédures de validation plus robustes
- Soutenir toute méthodologie supplémentaire qui tend vers les mêmes objectifs de sécurité

La nouvelle version introduit en outre le concept « d'approche personnalisée », qui repose sur l'idée que chaque approche de sécurité est différente et qu'un objectif de sécurité donné peut être atteint de plusieurs façons. Afin de faciliter une telle approche, la version 4.0 permettra la personnalisation des exigences et des procédures de test.

Bon nombre d'entreprises disposent de solutions de sécurité qui répondent à l'objectif de sécurité d'une exigence spécifique. Avec une approche personnalisée, les entreprises peuvent présenter la façon dont leur solution spécifique répond à l'objectif de sécurité et résout le risque, fournissant ainsi une méthode alternative de réponse à l'exigence.

La bonne nouvelle, c'est que les 12 exigences du PCI DSS restent fondamentalement inchangées avec le PCI DSS 4.0, car elles constituent le fondement critique de la sécurisation des données des cartes de paiement. Toutefois, les exigences sont désormais rédigées comme des énoncés axés sur les résultats et sur la mise en œuvre d'un contrôle de sécurité. Pour un grand nombre d'exigences, cela est possible par un simple changement de formulation – en remplaçant les exigences de mise en œuvre (ce qui « doit » être) par le résultat de la sécurité obtenu (ce qui « est »).

Les modifications les plus profondes portent sur l'authentification et le chiffrement des données. À l'heure où l'industrie du paiement a progressivement migré vers le cloud, le PCI DSS se focalise sur l'application de normes d'authentification plus robustes sur les connexions d'accès aux processus de paiement et de contrôle. Ces nouvelles exigences comprennent l'utilisation de l'authentification multi-factorielle pour tous les comptes accédant aux données des titulaires de cartes, et non pour les seuls administrateurs accédant à l'environnement des données des titulaires de cartes. Le PCI DSS 4.0 élargit en outre le champ d'application du chiffrement des données des titulaires de cartes, qui englobe désormais les réseaux de confiance. La liste complète des modifications est disponible dans le guide récapitulatif des modifications correspondant.

Une approche priorisée de la conformité PCI DSS 4.0

De par son caractère global, le PCI DSS fournit de nombreuses informations sur la sécurité – tellement d'informations, de fait, que certaines personnes responsables de la sécurité des données des comptes de paiement ne savent pas par où commencer. Le Conseil des normes de sécurité PCI a mis au point une approche priorisée de la conformité afin d'aider les organisations à savoir comment réduire le risque en amont de leur parcours de conformité PCI DSS.

Selon le guide, «*L'approche priorisée cartographie l'ensemble des exigences PCI DSS pour les diviser en six jalons de la sécurité basés sur le risque. Ces jalons visent à aider les organisations à progressivement mieux se prémunir face aux plus grands facteurs de risque et aux menaces croissantes, et ce, tout en progressant dans leur parcours de conformité PCI DSS.* »

L'approche priorisée du PCI DSS comporte six jalons :

1. **Ne stockez pas de données d'authentification sensibles non nécessaires, et limitez la rétention des données des titulaires de cartes.** Les entreprises peuvent limiter l'impact d'une fuite si les données d'authentification sensibles et les autres données de compte ne sont pas stockées.
2. **Protégez les points d'accès aux systèmes et réseaux, et soyez prêt à réagir en cas de fuite.**
3. **Applications de paiement sécurisé.** Les vulnérabilités de ces applications sont un vecteur courant d'accès illicite aux systèmes et d'obtention d'accès non autorisé aux données des titulaires de cartes.
4. **Surveillez et contrôlez l'accès à vos systèmes.** Ayez une visibilité claire sur l'accès aux environnements des données des titulaires de cartes (qui, quoi, quand et comment).
5. **Protégez les données stockées des titulaires de cartes.** Si le stockage des données des titulaires de cartes est une nécessité pour l'entreprise, implémentez des contrôles afin de protéger ces données.
6. **Exécutez les tâches de conformité restantes et veillez à ce que tous les contrôles soient en place.**

Ces jalons visent à aider les organisations à progressivement mieux se prémunir face aux plus grands facteurs de risque et aux menaces croissantes, et ce, tout en progressant dans leur parcours de conformité PCI DSS 4.0.

L'approche priorisée et ses jalons offrent les avantages suivants à toutes les entreprises :

- Une approche structurée pour traiter les risques par ordre de priorité
- Des « gains rapides » grâce à une approche réaliste en matière de cybersécurité et de conformité PCI DSS 4.0
- Une planification financière et opérationnelle
- Des indicateurs de progrès objectifs et mesurables

Meilleures pratiques quotidiennes pour renforcer votre conformité PCI DSS 4.0

S'il peut être difficile de se conformer au PCI DSS 4.0, cette version de la norme améliore la capacité d'atténuation des tactiques avancées employées par les individus mal intentionnés. Commencez par lire la norme PCI DSS 4.0 afin de vous familiariser avec les changements les plus notables susceptibles d'impacter votre processus de conformité. Ensuite, commencez à élaborer des plans d'implémentation des changements au sein de vos processus de cybersécurité afin de vous guider vers la conformité PCI DSS 4.0.

Les paragraphes ci-après vous permettront d'identifier les 12 exigences de la norme, tout en vous proposant de meilleures pratiques grâce auxquelles vous pourrez protéger votre organisation face aux menaces du quotidien, mais aussi consolider votre conformité vis-à-vis du PCI DSS 4.0. Pour obtenir une présentation plus détaillée, consultez les ressources PCI DSS.

Exigence 1 : installer et maintenir des contrôles de sécurité réseau

Les pare-feu réseaux sont essentiels à votre sécurité. Toutefois, vous ne pouvez pas vous contenter d'installer un pare-feu sur le périmètre réseau de votre organisation, en espérant que cela suffise pour vous protéger.

1. **Créez une ligne de base de configuration de pare-feu :** avant de mettre en œuvre les paramètres de pare-feu, documentez les paramètres et les procédures (p. ex. les paramètres de sécurité du matériel, les règles de port ou de service requises pour l'entreprise, la justification de ces règles, etc.) en tenant compte du trafic entrant et sortant.
2. **Testez tous les paramètres :** une fois les paramètres de configuration du pare-feu appliqués, testez ce dernier en externe et en interne pour vérifier que les paramètres sont corrects.
3. **Limitez le trafic sortant (et pas seulement le trafic entrant) :** trop souvent, nous nous préoccupons du blocage des ports entrants, sans penser à limiter au strict minimum le trafic sortant du réseau. Pourtant, une telle restriction permet de limiter les vecteurs d'exfiltration de données.
4. **Configurez des pare-feu sur les appareils mobiles personnels :** configurez des pare-feu personnels sur les plates-formes informatiques mobiles de façon à limiter la surface d'attaque ainsi que la propagation des logiciels malveillants en cas de connexion à des réseaux non sécurisés.
5. **Désactivez la gestion de pare-feu externe :** gérez uniquement le pare-feu depuis un emplacement au sein de votre réseau. Désactivez les services de gestion externe, sauf s'ils font partie d'une infrastructure de pare-feu gérée et sécurisée.

Exigence 2 : appliquer des configurations sécurisées à tous les composants du système

1. **Modifiez les paramètres par défaut afin de réduire les vulnérabilités inhérentes :** les appareils sont livrés dans leur configuration par défaut (p. ex. noms d'utilisateur et mots de passe). S'ils simplifient l'installation et l'assistance, les paramètres par défaut supposent également que chaque modèle comporte, à la base, un nom d'utilisateur et un mot de passe identiques. La non-modification de ces réglages par défaut constitue un vecteur d'attaque privilégié des pirates pour s'immiscer aisément dans votre écosystème. Aussi, il est indispensable de modifier les paramètres par défaut sur chaque système accédant aux données des titulaires de cartes.
2. **Durcissez l'environnement des données du titulaire de la carte (CDE) en suivant les meilleures pratiques du secteur :** tout système utilisé au sein de votre CDE doit être durci avant d'entrer en production. Cette consolidation vise à éliminer les éventuelles fonctionnalités inutiles et à configurer celles requises, en toute sécurité. Chaque application ou appareil connecté à un système introduit des vulnérabilités. Selon l'exigence 2.2 du PCI DSS, vous devez « *répondre à toutes les vulnérabilités de sécurité connues et vous mettre en conformité vis-à-vis des normes de durcissement des systèmes reconnues dans le secteur.* »
3. **Faites preuve de cohérence et gardez votre inventaire à jour :** une fois le durcissement du système mis en œuvre et documenté, les paramètres doivent être appliqués à l'ensemble des systèmes dans l'environnement, et ce, de manière cohérente. Une fois tous les systèmes et appareils situés dans le domaine correctement configurés, vous devez attribuer la responsabilité de garder l'inventaire à jour. Ainsi, les applications et les systèmes dont l'utilisation n'est pas approuvée peuvent être identifiés et supprimés.

Exigence 3 : protéger les données des comptes stockées

1. **Restez informé sur l'emplacement de vos données :** l'utilisation d'un outil de découverte des données permet d'identifier l'emplacement des données non chiffrées afin que vous puissiez les supprimer ou les chiffrer. Un tel outil facilite également l'identification des processus ou flux qui doivent être réparés. Les titulaires de cartes peuvent être facilement exposés suite à des processus inefficaces ou à des erreurs de configuration. Recherchez d'abord là où vous pensez que vos données résident, puis partout où ces données ne sont pas supposées se trouver.
2. **Chiffrez toutes vos données stockées :** les données des cartes stockées doivent être chiffrées à l'aide d'algorithmes reconnus dans le secteur. Bon nombre d'organisations détiennent, sans le savoir, des numéros de compte principal (PAN) non chiffrés. En plus de chiffrer les données des cartes, les entreprises doivent également protéger les clés de chiffrement. Ne pas sauvegarder l'emplacement d'une clé de chiffrement via un processus de gestion robuste, c'est comme laisser la clé de sa porte d'entrée sur la serrure !
3. **Réduisez la quantité de données que vous détenez :** ne conservez aucune donnée dont vous n'avez pas besoin. Réduisez le champ d'application du PCI DSS et demandez-vous si vous avez réellement besoin d'un dossier de données.

Exigence 4 : protéger les données des titulaires de cartes à l'aide d'un chiffrement fort pendant leur transmission sur des réseaux publics ouverts

1. **Sécurisez les données transmises sur les réseaux ouverts et publics :** identifiez les emplacements d'envoi des données des titulaires de cartes. Vous devez chiffrer vos données lorsqu'elles transitent sur des réseaux publics ouverts.
2. **Abandonnez les versions obsolètes des protocoles SSL/TLS :** les anciennes versions des protocoles SSL et TLS sont réputées pour leurs vulnérabilités en matière de sécurité. Vous devez cesser d'utiliser les versions obsolètes de ces protocoles de chiffrement, sauf si cela est nécessaire à des fins de rétrocompatibilité (p. ex. un équipement de point de vente qui ne prend pas en charge les versions ultérieures du protocole TLS sécurisé).

Exigence 5 : protéger les systèmes et réseaux face aux logiciels malveillants

1. **Mettez régulièrement à jour l'antivirus :** une gestion attentive des vulnérabilités est la façon la plus efficace de réduire proactivement la fenêtre de compromission et, ainsi, de réduire les opportunités offertes aux pirates de s'immiscer dans vos systèmes pour y subtiliser de précieuses données. Incluez la mise à jour du logiciel antivirus dans votre stratégie de gestion des vulnérabilités.

Exigence 6 : développer et maintenir des systèmes et logiciels sécurisés

1. **Mettez à jour et installez les correctifs de vos systèmes de façon régulière :** l'application en temps utile des mises à jour de sécurité est essentiel à votre niveau de sécurité. Installez les correctifs de tous les composants critiques de votre environnement, notamment les pare-feu, les applications, les bases de données, les terminaux de point de vente et les systèmes d'exploitation. Mettez à jour vos logiciels conformément à l'exigence 6.3.3 du PCI DSS qui stipule que les organisations doivent « installer les correctifs critiques dans le mois qui suit leur publication ». Pensez notamment aux installations de logiciels critiques, comme les applications de paiement par carte de crédit et les appareils mobiles. Le scan des vulnérabilités est un autre moyen d'atténuer les vulnérabilités : il s'agit en réalité de la meilleure méthode pour découvrir les lacunes de sécurité connues que les cybercriminels peuvent exploiter pour accéder à une organisation et la compromettre.
2. **Mettez en place des processus de développement logiciel sécurisés :** si vous développez des applications de paiement en interne, vous devez utiliser des processus rigoureux en matière de développement ainsi que des directives de codage sécurisées. Pensez à développer et à tester vos applications conformément aux normes reconnues dans le secteur, comme OWASP.
3. **Installez des pare-feu applicatifs (WAF) :** l'exigence 6.4 du PCI DSS impose la surveillance, la détection et la prévention régulières des attaques provenant du Web, et ce, en protégeant les applications Web destinées au public au moyen de pare-feu applicatifs, ou WAF (Web App Firewalls). Ces solutions sont spécialement conçues pour surveiller et bloquer le trafic Web malveillant.

Exigence 7 : restreindre l'accès aux composants système et aux données des titulaires de cartes

1. **Limitez l'accès aux données et aux systèmes :** vous devez disposer d'un système de contrôle d'accès basé sur les rôles (RBAC) doté d'une liste des rôles définie et à jour. Ce système octroie l'accès aux données des titulaires de cartes selon le principe du « besoin d'en connaître ». La restriction de l'accès contribue à éviter l'exposition des données sensibles à des individus non autorisés.

Exigence 8 : identifier les utilisateurs et authentifier l'accès

1. **Établissez des politiques de mots de passe forts et uniques, et déployez un gestionnaire des mots de passe :** lorsqu'un nom d'utilisateur ou mot de passe ne répond pas aux exigences de longueur, d'unicité et de complexité, il représente alors une

vulnérabilité. Pour répondre aux limites et aux risques inhérents à la nature humaine, pensez à déployer un logiciel de gestion des mots de passe d'entreprise, de façon à ce que la complexité des mots de passe ne vienne pas gâcher l'expérience utilisateur.

2. **Gestion robuste des comptes :** le PCI DSS impose de désactiver les comptes par défaut et de disposer de noms uniques pour les comptes utilisateur et administrateur. La multiplication des obstacles complique la tâche des pirates informatiques et, ainsi, renforce la sécurité de l'entreprise.

3. **Mettez en œuvre une authentification multi-factorielle :** aussi fort soit-il, un seul mot de passe ne peut pas constituer la seule mesure de sécurité mise en place. Nouvelle exigence du PCI DSS 4.0, l'authentification multi-factorielle (MFA) est la solution la plus efficace pour sécuriser l'accès à distance. Vos méthodes d'authentification doivent être hors bande et indépendantes les unes des autres. Une séparation physique doit exister entre les facteurs d'authentification, de sorte qu'un facteur donné ne puisse pas donner accès à un autre. Ainsi, en cas de compromission d'un facteur, l'intégrité et la confidentialité des autres facteurs sont préservées. Le PCI DSS vous impose en outre « *d'intégrer une authentification multi-factorielle pour tous les accès réseau à distance (utilisateur et administrateur, mais également l'accès des tiers à des fins d'assistance ou de maintenance) provenant d'une source extérieure au réseau de l'entité* ».

Exigence 9 : restreindre l'accès physique

1. **Contrôlez l'accès physique à vos sites :** pour atténuer les risques liés à la sécurité physique, mettez en œuvre des politiques de sécurité physique qui garantissent la sécurité sur site des actifs et données critiques. Vous pouvez, par exemple, protéger ces actifs critiques en les plaçant dans un site à la sécurité renforcée. Vous pouvez également limiter l'accès des personnes extérieures à une entrée surveillée unique, et imposer aux non-salariés le port de badges visiteur.

2. **Effectuer le suivi des terminaux de point de vente :** les entreprises utilisant des systèmes de point de vente ou des appareils de paiement mobiles doivent tenir à jour une liste de tous les appareils, inspecter régulièrement ces mêmes appareils et sensibiliser les membres du personnel qui utilisent au quotidien des appareils de paiement par carte.

Exigence 10 : consigner et surveiller tous les accès

1. **Passez en revue régulièrement les journaux et alertes système :** les systèmes chargés du suivi des journaux surveillent l'activité réseau, examinent les événements système, émettent des alertes en cas d'activité suspecte et enregistrent les actions des utilisateurs qui se produisent au sein de votre environnement. La collecte et la transmission des journaux vers un emplacement centralisé, un serveur de journalisation sur site ou un service Internet sont requises. Pour rechercher toute erreur, irrégularité ou activité suspecte inhabituelle, les entreprises doivent analyser leurs enregistrements tous les jours. Un suivi étroit des journaux offre de nombreux avantages, parmi lesquels un programme de sécurité plus efficace et une réponse plus rapide aux incidents de sécurité. En plus de témoigner de votre engagement en faveur des règles du PCI DSS, l'analyse et le suivi régulier des journaux contribuent également à déjouer les menaces internes et externes.

Exigence 11 : tester régulièrement la sécurité des systèmes et réseaux

1. **Identifiez votre environnement, mais aussi recherchez les vulnérabilités et effectuez des tests de pénétration sur une base régulière :** les cybercriminels peuvent accéder à un environnement en exploitant les failles d'un navigateur, d'un client de messagerie, d'un logiciel de point de vente, d'un système d'exploitation ou d'une interface de serveur. Un grand nombre des failles et vulnérabilités récemment découvertes peuvent être résolues avant que les pirates ne puissent les exploiter grâce à l'installation de mises à jour de sécurité et de correctifs système dans les environnements renfermant des informations de titulaires de cartes ou des données sensibles. Une méthode de scan des vulnérabilités peut s'avérer utile pour repérer et résoudre les vulnérabilités. Un « Code Testing » et un test de pénétration indépendant peuvent révéler de nombreuses failles courantes dans le code des applications (dans le cadre d'applications internes personnalisées). Les tests de pénétration et les scans de vulnérabilité sont des outils complémentaires qui favorisent la consolidation de la sécurité réseau. Ces méthodes de scan et de test constituent les meilleures lignes de défense afin d'identifier les vulnérabilités, que les entreprises pourront alors corriger avant le déploiement.

Exigence 12 : appuyer la sécurité de l'information par le biais de politiques et de programmes

1. **Documentez et mettez à jour régulièrement l'ensemble des pratiques de sécurité de l'entreprise :** tous les employés doivent pouvoir facilement accéder aux politiques écrites. En cas de fuite de données, la documentation peut contribuer à protéger votre entreprise face aux pertes éventuelles. Des politiques et procédures de sécurité, intégralement et précisément enregistrées, aident les enquêteurs de fraude à consulter les mesures de sécurité de votre entreprise et à démontrer dans quelle mesure votre entreprise s'engage proactivement sur le plan de la sécurité. Les entreprises doivent régulièrement mettre à jour leurs mesures de sécurité et la documentation répertoriant les actions à des fins de conformité PCI DSS 4.0.
2. **Établissez un processus d'évaluation des risques :** la norme PCI exige que chaque entité effectue une évaluation annuelle des risques afin d'identifier les principaux risques, vulnérabilités, menaces et ressources. Cette activité peut permettre aux organisations d'identifier, d'organiser et de gérer les menaces à la sécurité de l'information. Dans le cadre de l'évaluation des risques, l'attribution d'un classement ou d'une note aux menaces identifiées vous aidera à déterminer les vulnérabilités à traiter en premier, mais aussi à fixer les priorités. En classant, en évaluant et en atténuant méthodiquement les différents risques, vous pourrez réduire la fenêtre d'opportunité offerte aux cybercriminels (pour accéder à vos systèmes et y causer des dommages), puis arrêter l'attaque.
3. **Créez et testez le plan de réponse aux incidents :** vous devez vous préparer aux répercussions d'une fuite de données. Il vous incombe de garder le contrôle de l'événement, de réduire au maximum les dégâts infligés au client, de réduire les coûts liés à une fuite de données, de communiquer de façon adéquate avec les différentes autorités conformément aux spécifications des normes et des règles, et enfin de protéger votre entreprise. Une stratégie de réponse aux incidents efficace peut réduire l'impact des fuites, réduire le montant des amendes et la publicité négative, ou encore accélérer le retour à la normale.
4. **Sensibilisez tous vos employés :** la plupart des fuites peuvent être liées à une erreur humaine. La plupart des employés ne sont pas des individus malveillants, mais oublient souvent les meilleures pratiques de sécurité ou ne sont pas certains de savoir ce que l'on attend d'eux. Malheureusement, bon nombre de criminels exploitent l'erreur humaine dans le but d'obtenir des informations privées. Des directives précises et une formation continue doivent être prodiguées aux employés. L'importance de la sécurité sera rappelée aux employés par le biais d'un programme de sensibilisation (incluant notamment des formations fréquentes), notamment en les tenant informés sur les nouvelles politiques et procédures de sécurité.

Conclusions

Il vous reste encore beaucoup de temps avant l'échéance de mise en œuvre du PCI DSS 4.0 prévue en 2024. En commençant suffisamment tôt, vous serez sur la bonne voie pour assurer une transition sans heurts. N'attendez pas 2024 pour commencer la bascule vers le PCI DSS 4.0 : en étalant vos efforts sur la durée, vous vous conformerez à la nouvelle version au fur et à mesure.

Réfléchissez à vos besoins futurs et intégrez-les dans la stratégie et le programme de sécurité de votre organisation : vous utiliserez ainsi votre temps avec un maximum d'efficacité. Focalisez-vous sur les éléments généralement positifs sur le très long terme pour votre organisation.

Comment Fortra peut vous aider

Le portefeuille d'offres de cybersécurité et de conformité proposé par Fortra comprend un large éventail de solutions et de services destinés à aider les entreprises à se conformer au PCI DSS 4.0, mais aussi à répondre aux exigences quotidiennes qu'implique la protection de l'entreprise face aux risques et menaces. Le tableau suivant répertorie les différentes solutions Fortra adaptées à chaque exigence du PCI DSS 4.0.

Exigence du PCI DSS 4.0	Solution Fortra
Exigence 1 Installer et maintenir des contrôles de sécurité réseau	
Exigence 2 Appliquer des configurations sécurisées	La fonctionnalité de gestion des configurations de sécurité Tripwire Enterprise de Fortra permet aux entreprises de surveiller les configurations des réseaux, serveurs, pare-feu et autres composants.
Exigence 3 Protéger les données des comptes stockées	Avec le produit DLP Digital Guardian Enterprise de Fortra, les clients peuvent utiliser des politiques PCI pour surveiller et bloquer la sortie d'informations de crédit sur de nombreux points de sortie courants. Les appliances DLP Digital Guardian Network de Fortra inspectent l'intégralité du trafic réseau et appliquent des politiques préconfigurées pour le PCI et d'autres besoins de conformité, dans le but de protéger les données.
Exigence 4 Protéger les données des titulaires de cartes à l'aide d'un chiffrement fort pendant leur transmission sur des réseaux publics ouverts	La solution de transfert de fichiers sécurisé MFT GoAnywhere de Fortra aide les utilisateurs à maintenir la conformité de leurs transferts de fichiers vis-à-vis du PCI DSS. La solution Secure Collaboration de Fortra protège les fichiers contenant des données PII et PCI, quel que soit le lieu ou les modalités de leur partage. Les organisations peuvent chiffrer les données des titulaires de cartes et en contrôler l'accès, mais aussi suivre et auditer les données, ou encore révoquer l'accès à ces dernières.
Exigence 5 Protéger les systèmes et réseaux face aux logiciels malveillants	Powertech Antivirus de Fortra protège votre serveur face à un éventail complet de virus, de logiciels malveillants, de rançongiciels et bien plus encore.
Exigence 6 Développer et maintenir des systèmes et logiciels sécurisés	Beyond Security de Fortra contribue à détecter les vulnérabilités des applications en amont du processus de développement, grâce à des solutions de test dynamique de la sécurité des applications (DAST) et de test statique de la sécurité des applications (SAST). Les solutions de gestion des vulnérabilités de Fortra contribuent à identifier et à hiérarchiser les vulnérabilités dans votre environnement, afin de combler les failles de sécurité avant qu'elles ne puissent être détectées par les pirates. Les fonctionnalités de gestion des configurations de Tripwire Enterprise de Fortra facilitent la détection des modifications non planifiées dans votre environnement, contribuant ainsi à renforcer l'intégrité du système. Alert Logic MDR Essentials de Fortra comprend des outils de gestion et d'évaluation de l'exposition qui, grâce à un scan externe, de réseau et basé sur agent, offre une visibilité complète des expositions au sein des environnements informatiques – sur site et dans le cloud. Alert Logic de Fortra est un fournisseur approuvé (ASV) PCI. Alert Logic Managed WAF de Fortra protège les applications Web en fournissant des capacités de détection et de prévention continues pour les attaques basées sur le Web.
Exigence 7 Restreindre l'accès aux composants système et aux données des titulaires de cartes	La solution Access Assurance Suite du portefeuille Core Security de Fortra facilite l'identification et la gestion de l'accès partout dans votre organisation, via une interface unifiée. Core Privileged Access Manager (BoKS) vous aide à contrôler l'accès et les autorisations aux systèmes et aux informations critiques.
Exigence 8 Identifier les utilisateurs et authentifier l'accès	Core Password de Fortra est une solution leader du marché pour la gestion sécurisée et en libre-service des mots de passe. Elle propose de nombreuses options d'accès, une intégration robuste du centre d'assistance et la possibilité d'appliquer des politiques de mot de passe cohérentes sur n'importe quel système, application ou portail Web.
Exigence 9 Restreindre l'accès physique	

Exigence du PCI DSS 4.0	Solution Fortra
Exigence 10 Consigner et surveiller tous les accès	Tripwire LogCenter de Fortra est un moteur de corrélation qui assure la collecte, l'analyse et la fourniture centralisées des journaux. Le service Alert Logic MDR Professional de Fortra comprend la gestion et le stockage des journaux, ainsi que la recherche de toute activité suspecte/malveillante dans ces derniers au niveau du point d'ingestion, et ce, à l'aide d'une analytique avancée (p. ex. UBAD) ; ces activités sont ensuite triées par un analyste SOC le cas échéant. La console d'intégrité et la vue de l'intégrité réseau Alert Logic de Fortra surveillent et informent sur l'intégrité des appliances de sécurité Alert Logic.
Exigence 11 Tester régulièrement la sécurité des systèmes et réseaux	Les fonctionnalités de gestion de l'intégrité de Tripwire Enterprise de Fortra permettent de brosser un tableau précis de la situation, afin de mieux savoir où et quand des modifications ont été apportées. En tant que fournisseur approuvé (ASV) PCI, Fortra propose des solutions de gestion des vulnérabilités qui vous aident à effectuer des évaluations complètes de la sécurité grâce auxquelles vous pouvez classer les risques par ordre de priorité en fonction des besoins de votre organisation. Alert Logic MDR Essentials de Fortra comprend des outils de gestion et d'évaluation de l'exposition qui, grâce à un scan externe, de réseau et basé sur agent, offre une visibilité complète des expositions au sein des environnements informatiques – sur site et dans le cloud. Alert Logic de Fortra est un fournisseur approuvé (ASV) PCI. La solution Core Impact du portefeuille Core Security de Fortra facilite la mise en œuvre efficace de tests de pénétration avancés. Grâce à l'automatisation guidée et aux exploits certifiés, vous testez votre environnement en toute sécurité en recourant aux mêmes techniques que les pirates actuels.
Exigence 12 Appuyer la sécurité de l'information par le biais de politiques et de programmes	Terranova Security de Fortra propose une approche ciblée, intéressante, pratique et centrée sur l'individu pour sensibiliser les employés aux questions de sécurité. La solution comprend un module de formation spécialement conçu pour le PCI DSS.

Si vous n'êtes pas en mesure de prendre en charge toutes ces activités, nos équipes de services gérés Tripwire et Alert Logic peuvent assurer la liaison avec votre équipe afin de réduire les risques de sécurité et de simplifier la conformité PCI DSS 4.0.

Pour en savoir plus sur la façon dont Fortra peut vous aider à atteindre la conformité PCI DSS 4.0, consultez nos ressources PCI supplémentaires ou contactez-nous. Nous nous ferons un plaisir de vous écouter afin de vous proposer des solutions.

FORTRA™

Fortra.com

À propos de Fortra

Fortra est un fournisseur de logiciels de cybersécurité unique sur le marché. Nous créons un avenir plus simple et plus sûr pour nos clients. Nos experts fiables et notre portefeuille, riche en solutions évolutives et intégrées, offrent aux entreprises du monde entier maîtrise et équilibre. Nous sommes les artisans du changement positif et votre allié pour vous garantir la tranquillité d'esprit à chaque étape de votre parcours en matière de cybersécurité. Pour en savoir plus, rendez-vous sur fortra.com/fr.

(fta-corp-wp-0324-r2-hm)