

# Solutions Imperva pour PCI

Assurer la conformité à la norme de sécurité des données PCI 1.1



## Pare-feu d'application Web

- Répond aux exigences PCI de pare-feu de couche applicative
- Bloque les attaques
- Empêche les accès non autorisés
- Protège contre le Top 10 OWASP
- Consigne toutes les requêtes illégales et suspectes

## Passerelle de base de données

- Répond aux exigences PCI de contrôle d'accès aux données des titulaires de cartes
- Contrôle l'accès de l'utilisateur à la base de données
- Bloque les attaques de base de données
- Enregistre l'activité en temps réel
- Audite toutes les transactions de bases de données
- Piste les utilisateurs finals réels

## Avantages de SecureSphere

- La protection la plus complète et la plus précise pour PCI
- Faible coût total d'acquisition
- Zéro changement d'infrastructure
- Configuration de politique automatisée
- Administration pour de grandes entreprises

## Répondre aux exigences PCI les plus difficiles

Les dispositifs de sécurité Web et de bases de données SecureSphere permettent aux intermédiaires et fournisseurs de services de répondre aux exigences PCI les plus strictes rapidement, sans effort, et de manière rentable.

### Exigence de sécurité applicative

La section 6.6 du PCI 1.1 demande aux sociétés de se plier à l'une des exigences suivantes :

- Installer un pare-feu de couche applicative en face des applications Web
- Faire examiner tous les codes applicatifs pour rechercher les vulnérabilités par un organisme extérieur spécialisé dans la sécurité des applications.

### Solution SecureSphere

Le pare-feu d'application SecureSphere répond à toutes les exigences de sécurité de la section 6.6.

#### SecureSphere :

- Il détecte automatiquement les changements dans les applications et garantit que les applications Web sont toujours protégées contre les attaques les plus récentes.
- Il est beaucoup plus rapide, plus simple et moins cher qu'une révision du code source des applications.

### Exigence de contrôle des bases de données

La section 10 demande aux sociétés de surveiller et contrôler tout accès aux données des titulaires de cartes. Les sous-sections de ces exigences comprennent :

- Le contrôle de tout accès aux données des titulaires de cartes
- L'enregistrement de la création et la suppression des objets du système
- L'audit des accès non autorisés
- La protection des logs contre la modification

### Solution SecureSphere

La passerelle SecureSphere répond à toutes les exigences d'audit et de contrôle des bases de données de la section 10.

#### SecureSphere :

- Contrôle tout accès aux données des titulaires de cartes
- Enregistre tout changement dans la base de données
- Audite les tentatives d'accès non autorisées
- A titre optionnel crypte les logs ou appose une signature numérique
- Piste l'activité de l'utilisateur avec la Surveillance Universelle de l'Utilisateur (UUT)

### Protection avancée des données

L'annexe B de PCI 1.1 liste les contrôles correctifs pour rendre les données de titulaires de cartes illisibles. Les sociétés avec des contraintes commerciales ou technologiques spécifiques peuvent considérer l'utilisation des contrôles correctifs, qui comprennent :

- Un accès restreint aux données de titulaires de cartes
- Un accès logique restreint à la base de données
- La prévention des attaques de bases de données
- Une segmentation de réseau additionnelle

### Solution SecureSphere

La passerelle SecureSphere répond à l'ensemble des exigences pour les contrôles correctifs.

#### SecureSphere :

- Restreint l'accès par l'adresse IP, l'application, le nom utilisateur ou le type de données.
- Un accès logique restreint à la base de données
- Bloque les attaques de base de données
- Fournit une segmentation de réseau

## Le challenge PCI

Le standard PCI (Payment Card Industry : Industrie de la carte de paiement) de sécurité des données comprend douze exigences de haut niveau définissant les politiques, les outils, et les contrôles nécessaires pour protéger les données des titulaires de cartes. Alors que certaines de ces exigences sont relativement faciles à résoudre et à mettre en œuvre, celles liées à la sécurité des bases de données et des applications Web comportent des défis métiers et techniques importants. Le chemin vers la conformité PCI peut entraîner des missions coûteuses de consultation et des modifications structurelles considérables.

## La solution

Les dispositifs de sécurité Web et de bases de données SecureSphere permettent aux sociétés de répondre aux exigences PCI les plus strictes rapidement, sans effort, et de manière rentable. Le pare-feu pour application Web SecureSphere remplit les exigences de pare-feu de couche applicative de PCI version 1.1. En plus de répondre aux réglementations de conformité, SecureSphere empêche une large gamme d'attaques avec une extrême précision et sans aucun réglage ou configuration manuels.

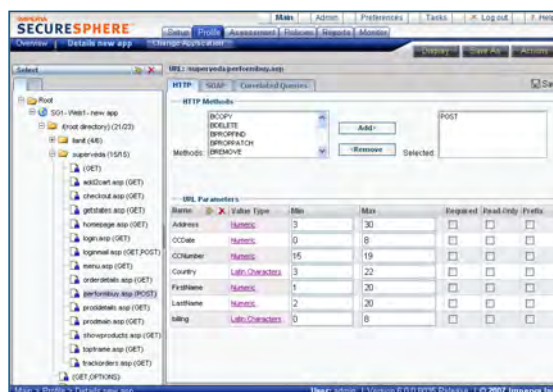
La passerelle SecureSphere répond aux exigences PCI de la section 10 pour le contrôle et la surveillance des bases de données. Elle remplit également les contrôles compensatoires listés en annexe B du standard PCI 1.1. SecureSphere renforce la sécurité des données en évaluant la vulnérabilité des bases de données, en identifiant les mauvaises pratiques et en empêchant les fuites de données des titulaires de cartes. SecureSphere contrôle et protège les applications de bases de données sans impacter la performance des bases.

## L'avantage SecureSphere

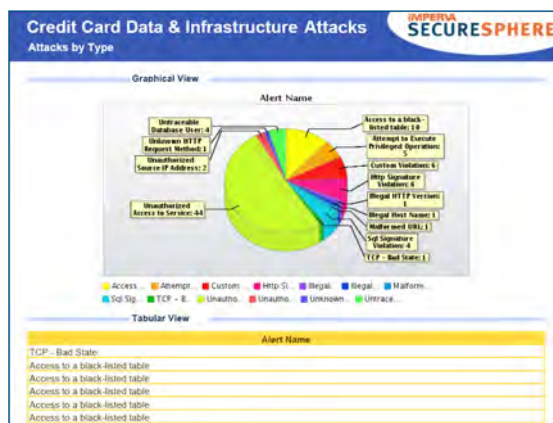
La famille SecureSphere des dispositifs de sécurité intègre des technologies en attente de brevet qui accélèrent le déploiement, réduisent les coûts d'exploitation et renforcent la sécurité.

- Le **Profilage Dynamique** établit automatiquement le profil de l'usage légitime des données et met à jour ce profil au fil des modifications de l'usage au cours du temps. L'activité de l'utilisateur est constamment comparée à l'information stockée sur ce profil, permettant à SecureSphere d'autoriser ou de bloquer immédiatement des tentatives d'accès non autorisées.
- La **surveillance universelle** de l'utilisateur donne le droit aux organisations d'auditer les accès des utilisateurs aux données en pistant les transactions des bases de données sur les utilisateurs individuels.
- L'**inspection transparente** analyse la logique de l'application et l'usage des données avec zéro modification des applications, bases de données, et autres infrastructures de réseau, en maintenant une production de transactions multi-gigabits et une latence inférieure à la milliseconde.
- La **validation corrélée** des attaques met en corrélation les sources multiples de l'information au cours du temps et au-travers des couches pour identifier avec précision l'activité malicieuse.
- L'**administration unifiée** permet aux entreprises de configurer, mettre à jour, et contrôler les déploiements mixtes Web et de bases de données à travers d'une interface unique, accessible via un navigateur.
- **PCI Insights**, un des services Imperva ADC, offre une identification des données sensibles, des rapports préétablis de conformité PCI, et les bonnes pratiques en matière de sécurité des données bancaires.

Surtout, les intermédiaires et ceux qui traitent les données de cartes bancaires peuvent être assurés qu'avec SecureSphere, leurs données bancaires sont sécurisées.



Le Profilage Dynamique modélise automatiquement tous les aspects de l'application y compris les URL, champs, cookies, méthodes, et valeurs.



Les services ADC Insight fournissent des rapports de conformité PCI prédéfinis comprenant les attaques aux données de cartes bancaires et à l'infrastructure.



Un tableau de bord en temps réel des événements liés à la sécurité.

### Imperva, Inc.

Siège social aux États-Unis  
950 Tower Lane  
Suite 1550  
Foster City, CA 94404  
Tél : +1-650-345-9000  
Fax : +1-650-345-9004

Siège social international  
125 Menachem Begin Street  
Tel-Aviv 67010  
Israël  
Tél : +972-3-6840100  
Fax : +972-3-6840200

Numéro vert (États-Unis seulement) +1-866-926-4678  
www.imperva.com

