

## Solutionner le défi de la conformité PCI DSS

Avec le logiciel de lutte contre la fraude Luminet

Le standard de sécurité des données de cartes de paiement PCI DSS impose aux entreprises des contraintes strictes et notamment l'obligation, au titre du paragraphe 10.2.1, de « mettre en œuvre, pour tous les composants système, des pistes d'audit automatisées permettant de reconstituer l'ensemble des accès des utilisateurs aux données des détenteurs de cartes ». Le paragraphe 10.2.2 exige également l'inclusion, dans la piste d'audit, de « toutes les opérations réalisées par des personnes disposant de privilèges centraux ou administratifs ».

### Pourquoi les pistes d'audit sont-elles si complexes à mettre en œuvre ?

La conformité aux exigences PCI DSS présente dans ce domaine quatre difficultés essentielles :

1. Qu'elles soient traditionnelles ou de dernière génération, les applications n'incluent généralement pas de mécanisme d'enregistrement (logs) offrant un historique complet des accès des utilisateurs aux données sur les cartes de paiement. La plupart du temps, les journaux de logs n'enregistrent que les mises à jour mais pas les requêtes et autres activités en « lecture seule » conduites par les utilisateurs – indispensables pour constituer une piste d'audit intégrale.
2. La simple agrégation des journaux répond à certaines exigences PCI DSS mais ne suffit pas à fournir la piste d'audit complète spécifiée au paragraphe 10.2. Si les journaux de logs contiennent des données insuffisantes ou limitées à certains types d'activités, leur agrégation ne permettra pas de répondre aux impératifs du paragraphe 10.2.
3. Le développement d'une solution interne spécifique représente un investissement majeur en temps, en efforts et en ressources financières, impliquant parfois des milliers de modifications, tests et redéploiements de programmes d'entreprise. De plus, la solution finalement obtenue n'offre généralement pas de moyen centralisé et administrable pour savoir « qui a fait quoi et quand » sur l'ensemble des applications et des systèmes.
4. En limitant l'enregistrement aux activités de base de données, les entreprises courent le risque de ne pas assurer leur conformité au standard car les applications utilisent la plupart du temps des identifiants génériques pour l'accès aux bases de données. Elles ne disposent alors d'aucun moyen de répondre à l'exigence d'audit de « tous les accès individuels ».

Il existe heureusement des technologies pour solutionner ces problématiques.

### Voir... Enregistrer... Analyser...

La solution Attachmate Luminet™ est spécifiquement conçue pour capturer une image complète des accès des utilisateurs aux informations sur les cartes de paiement et pour éviter le dépouillement de complexes fichiers de logs pour reconstituer un scénario plausible à des fins d'audit. Principes de fonctionnement de Luminet :

- **Visualisation des activités**

Les outils Luminet permettent de définir des règles paramétrables pour identifier tous les comportements suspects vis-à-vis de la stratégie de gestion du risque. Luminet génère des alertes en temps réel en cas d'activité suspecte pour concentrer immédiatement tous les efforts sur les anomalies.

- **Enregistrement des activités**

Luminet enregistre les activités utilisateur, en temps réel, écran par écran et touche par touche, en créant une piste d'audit directement à partir du réseau. Cette piste d'audit inclut tant les opérations de mise à jour que les actions en lecture seule, pour les utilisateurs « ordinaires » et ceux disposant de privilèges. Luminet enregistre ces informations dans un référentiel sécurisé permettant de lancer des recherches avancées en mode texte sur les activités enregistrées et en cours. Grâce à ces recherches, il est possible de reconstituer visuellement l'ensemble des écrans parcourus et saisies clavier dans le cadre de l'activité auditée. Des tableaux de bord, graphiques et rapports personnalisables permettent aux auditeurs internes d'accéder à une vue complète et de se focaliser sur les

#### À propos du standard PCI DSS

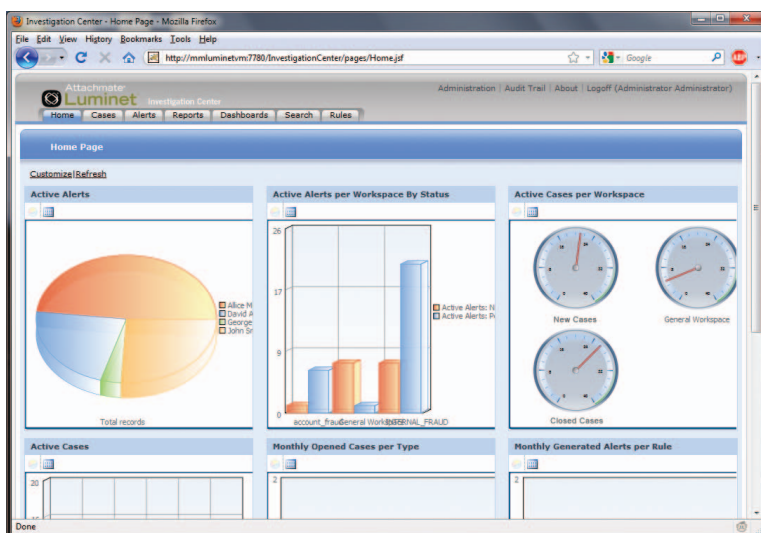
Le standard de sécurité des données de l'industrie des cartes de paiement (PCI DSS) a été développé par le PCI Security Standards Council (pcisecuritystandards.org) — un consortium mondial fondé par les principaux émetteurs de cartes de crédit pour définir des normes de traitement des données applicables aux entreprises. Le standard a pour objet de prévenir les fraudes aux cartes de paiement et d'établir des mesures de sécurité couvrant tous les types d'usage des informations des cartes de paiement. Il définit 12 mesures spécifiques que doit implémenter toute entreprise appelée à enregistrer, traiter ou transmettre des données sur les détenteurs de cartes.

activités susceptibles de compromettre la conformité PCI DSS de l'entreprise.

#### • Analyse des activités

Luminet permet de distinguer clairement les activités suspectes des tâches légitimes. Un outil interactif identifie les modes d'intervention multicanaux impliquant différents collaborateurs, départements ou applications et permet ainsi de prendre des mesures efficaces et immédiates en cas de comportement suspect.

En synthèse, Luminet voit, enregistre et analyse les activités des utilisateurs sur l'ensemble des applications d'entreprise pour fournir une piste d'audit complète des accès individuels aux informations sensibles telles que les données de cartes de paiement. Ainsi, et sans avoir à ajouter de nouveaux contrôles ni modifier le code de leurs applications existantes, les entreprises bénéficient d'un outil d'audit avancé simplifiant leur conformité aux exigences fixées par les paragraphes 10.2.1 et 10.2.2 du standard PCI DSS.



Suivi des métriques clés d'activités avec tableaux de bord personnalisables

### Luminet Voir... Enregistrer... Analyser...

Le logiciel antifraude Luminet voit, enregistre et analyse les activités des utilisateurs sur l'ensemble des applications d'entreprise et élimine ainsi toute subjectivité dans la supervision des applications ; Luminet vous offre une intelligence décisionnelle sans précédent grâce aux fonctionnalités et avantages suivants :

- Architecture sans agent
- Supervision multicanal
- Alertes en temps réel
- Répétition graphique des écrans applicatifs
- Fonctionnalités de recherche de type Google
- Analyse graphique des liens
- Support des applications existantes
- Suite de gestion des cas
- Tableaux de bord et rapports personnalisés

### À propos d'Attachmate

Attachmate commercialise des logiciels avancés d'émulation de terminal, de modernisation des sites centraux, d'administration des transferts de fichiers et de lutte contre la fraude. Grâce aux technologies Attachmate plus de 65 000 entreprises dans le monde maximisent la création de valeur de leurs systèmes d'information en mettant leurs ressources au service de l'innovation et de la performance. [www.attachmate.fr](http://www.attachmate.fr)



#### Siège Social

1500 Dexter Avenue North  
Seattle, Washington 98109  
États-Unis  
TEL +1 206 217 7500  
FAX +1 206 217 7515

#### Siège Social EMEA

Pays-Bas  
TEL +31 172 50 55 55  
FAX +31 172 50 55 51

#### Sales France

France  
TEL +33 1 46 04 10 10  
FAX +33 1 49 09 05 59

WEB [www.attachmate.fr](http://www.attachmate.fr)  
EMAIL [marketfr@attachmate.com](mailto:marketfr@attachmate.com)

Pour les informations relatives aux bureaux locaux, visitez le site [www.attachmate.fr](http://www.attachmate.fr)