



The Security Division of EMC

Brief Solution RSAf

## Protection des données de cartes de crédit

Se conformer au standard de sécurité des données de cartes de crédit ( PCI DSS 1.1)

# Épidémie de fuites de données clients: Plus de 200 millions d'enregistrements perdus

Au cours des dernières années, des centaines de dirigeants d'entreprises se sont retrouvés dans la position peu enviable d'avoir à annoncer la perte ou le vol d'informations personnelles clients – telles que des numéros de cartes de crédit ou de sécurité sociale. Ce problème est planétaire et touche tous les secteurs d'activités : des commerces de détail à l'hôtellerie, en passant par les administrations, la santé, les universités et les institutions financières, tous ont été contraints d'avouer des pertes de données clients.

En raison de ce problème, une attention particulière est portée à la protection de certaines données: l'information des cartes de crédit consommateurs. En réponse, American Express, Discover Financial Services, JCB, MasterCard et Visa se sont associés pour créer un framework qui précise aux entreprises manipulant des données de cartes de crédit (banques, marchands, établissements de traitement, etc.) comment protéger ces informations. Le résultat est le standard PCI DSS (Payment Card Industry Data Security Standard), un ensemble d'exigences pour protéger les données de carte tout au long de leur cycle de vie.

Le standard PCI s'articule autour de six objectifs de contrôle — essentiellement destinés à optimiser la sécurité des données de cartes de crédit. Douze exigences extensives de sécurité sous-tendent ces objectifs et sont subdivisées en 200 exigences secondaires définissant les technologies, politiques et procédures requises pour protéger les données sur les détenteurs de cartes. Diffusée en septembre 2006, la version 1.1 est la première mise à jour du standard PCI DSS. Développé par le « PCI Security Standards Council », PCI DSS 1.1 étend la version précédente en plaçant un nouvel accent sur la sécurité applicative.

Les banques, commerçants et instituts de traitement des paiements approchent la conformité PCI DSS comme un effort continu. En effet, la conformité doit être validée chaque année et les entreprises doivent être prêtes à intégrer de nouvelles spécifications du standard. En synthèse, elles doivent rester vigilantes pour non seulement se conformer ponctuellement aux exigences PCI DSS — mais également pérenniser cette conformité.

---

## Implications de PCI pour aujourd'hui et pour demain...

---

Les responsables de la sécurité et de la conformité sont aujourd'hui soumis à des niveaux extrêmement élevés de responsabilité vis-à-vis des exigences de sécurisation des données de cartes de crédit. Le standard PCI a en effet mis en lumière des challenges significatifs : les entreprises doivent identifier l'emplacement exact de l'ensemble des données sur les cartes – et ce, dans un environnement souvent distribué – et garantir la sécurité de ces données et des accès à l'information associée. Elles doivent également prouver que les précautions stipulées par la norme ont été prises et que des mesures proactives ont été mises en place pour surveiller tout accès non-authorized aussi bien aux données de cartes qu'aux systèmes associés sur les porteurs.

Ces challenges ont conduit à des investissements considérables sur la mise en conformité aux spécifications PCI DSS. Ce qui soulève la question suivante : « Les investissements consentis pour PCI permettent-ils de réaliser des progrès de conformité dans d'autres domaines ? »

---

## Solutions PCI RSA : Addresser le standard de sécurité des données PCI

---

PCI identifie plusieurs technologies fondamentales de sécurité et différents processus et procédures requis pour protéger les données sur les détenteurs de carte. Pour faire face à ces exigences, RSA, la Division Sécurité d'EMC, propose la solution RSA PCI qui englobe une large gamme de technologies et services.

L'approche centrée sur l'information prônée par RSA étend la protection au-delà du strict périmètre physique pour garantir que les données sont sécurisées quel que soit leur emplacement. En outre, les solutions RSA pour PCI permettent de répondre à ces questions critiques :

- 1) Où les données sur les cartes sont-elles stockées ?
- 2) Comment s'assurer qu'elles sont sécurisées ?
- 3) Comment déployer des contrôles appropriés permettant une réactivité immédiate en cas de risques potentiels et pouvoir que l'investissement PCI DSS peut aider le business au-delà de l'audit?

### Comprendre PCI DSS

#### OBJECTIFS DE CONTROLE

6 objectifs de haut niveau de sécurisation des données de carte

#### EXEMPLE

Restreindre l'accès aux données sur les détenteurs de carte en fonction des besoins métier

#### EXIGENCES

12 catégories d'actions nécessaires pour sécuriser les données sur les détenteurs de carte

#### EXEMPLE

Affecter un identifiant unique à chaque personne bénéficiant d'un accès informatique

#### SOUS-EXIGENCES

Plus de 200 actions spécifiques requises pour sécuriser les données de carte

#### EXEMPLE

Implémenter une authentification à deux facteurs pour les accès réseau distants des collaborateurs, administrateurs et tiers

Pour relever tous ces défis, RSA dispose d'une combinaison sans équivalent de fonctionnalités, produits et services: découverte des données de cartes de crédit ; sécurisation ; protection de l'accès aux informations et systèmes associés ; réactivité accélérée en cas de violation potentielle ; production de preuves pour les auditeurs et les banques.

RSA peut aussi assister les clients à étendre la portée de ces investissements pour protéger toutes les informations vitales de l'entreprise (informations clients , partenaires, métier, etc.) et garantir que l'investissement PCI DSS serve à améliorer la protection et la croissance du business à long terme.

### Opportunités au delà de la conformité PCI DSS

En envisageant les prochaines étapes pour la mise en conformité ou la re-certification de votre entreprise, il faudra prendre en considération le fait que :

- PCI DSS ne se limite pas à la sécurisation des informations mais requiert une combinaison réfléchie de ressources humaines, processus et ajustements technologiques pour faciliter la conformité et pour améliorer la sécurité et les processus métier de l'entreprise dans son ensemble.
- L'adoption d'une approche stratégique et planifiée de la conformité PCI DSS dès le départ, permet non seulement d'éviter les coûts significatifs liés à toute brèche sur les données, mais surtout, de libérer des ressources pour les consacrer à des activités créatrices de valeur.
- Quelles que soient les exigences applicables (Niveau 1, 2, 3 ou 4), considérer PCI DSS comme un « framework » permettant de minimiser les risques pesant sur les données stratégiques et ainsi de recentrer les efforts sur les objectifs métiers .

## Comprendre PCI DSS

OBJECTIFS DE CONTROLE	EXIGENCES
Construire et maintenir un réseau sécurisé	<ol style="list-style-type: none"><li>1. Installer et maintenir une config. pare-feu pour protéger les données des détenteurs de cartes</li><li>2. Ne pas utiliser les mots de passe et autres paramètres de sécurité système fournis par défaut</li></ol>
Protéger les données sur les détenteurs de cartes	<ol style="list-style-type: none"><li>3. Protéger les données enregistrées sur les détenteurs de cartes</li><li>4. Crypter la transmission des données de détenteurs de cartes sur des réseaux ouverts et publics</li></ol>
Maintenir un programme de gestion de la vulnérabilité	<ol style="list-style-type: none"><li>5. Utiliser et mettre à jour régulièrement les logiciels antivirus</li><li>6. Développer et maintenir des systèmes et applications sécurisés</li></ol>
Implémenter des mesures renforcées de contrôle des accès	<ol style="list-style-type: none"><li>7. Restreindre l'accès aux données des détenteurs de cartes aux cas métiers "need-to-know"</li><li>8. Affecter un identifiant unique à chaque personne bénéficiant d'un accès informatique</li><li>9. Restreindre l'accès physique aux données sur les détenteurs de cartes</li></ol>
Superviser et tester régulièrement les réseaux	<ol style="list-style-type: none"><li>10. Suivre et surveiller tous les accès aux ressources réseau et données des détenteurs de cartes</li><li>11. Tester régulièrement les systèmes et processus de sécurité</li></ol>
Maintenir une politique de sécurité de l'information	<ol style="list-style-type: none"><li>12. Maintenir une politique couvrant la sécurité informationnelle</li></ol>

## Pré-Evaluation de conformité PCI

Au début du processus de conformité PCI DSS, il est essentiel de déceler les éventuelles failles afin d'identifier les besoins d'actions correctives. À travers une pré-évaluation PCI DSS, les Services Professionnels RSA aident les clients à diagnostiquer leur posture PCI actuelle et développer une stratégie corrective avant de mener un audit PCI formel. Cette prestation n'a pas pour vocation de remplacer l'audit PCI, mais aide les entreprises à identifier et corriger leurs faiblesses avant un audit formel.

Le livrable majeur de cette prestation est une recommandation d'« architecture de référence » garantissant un traitement approprié des données de cartes. Les consultants RSA établissent cette proposition d'architecturale selon le processus suivant:

1. Évaluation des niveaux de conformité au standard PCI DSS à travers une revue de l'architecture actuelle et de ses composants (réseaux, applications, serveurs, appareils de stockage, etc.) et à l'aide de technologies avancées de classification et de découverte utilisées pour la manipulation et le traitement des données de cartes de crédit

### Avantages clients:

#### Solutions RSA pour la conformité PCI DSS

Les puissantes fonctionnalités du portefeuille technologique RSA/EMC – alliées à des Services Professionnels et des prestations de consulting renommés – permettent de:

- Identifier où résident toutes les données sur les cartes afin de prendre les mesures requises pour les sécuriser.
- Protéger les données de cartes, quel que soit leur emplacement ; authentifier l'identité des personnes y accédant et s'assurer que seuls ceux ayant un réel besoin métier disposent des droits pour accéder ces données.
- Surveiller et suivre l'accès aux données de porteurs de cartes, de sorte qu'en cas de violation d'une politique ou d'une sécurité, vous êtes informé et capable d'y répondre.
- Comprendre comment les investissements réalisés en vue de la conformité PCI DSS peuvent être utilisés au-delà de l'audit pour améliorer la sécurité des données et des opérations métier de l'entreprise.

# Sécuriser les données avant de les localiser est impossible

2. Revue des politiques et processus existants de traitement des données sur les détenteurs de cartes et leur comparaison aux spécifications PCI DSS et aux bonnes pratiques recensées par les équipes consulting de RSA.
3. Production d'un rapport documentant les écarts entre l'état actuel de l'infrastructure, des politiques et des procédures et celui à atteindre pour assurer la conformité PCI DSS.
4. Développement d'une stratégie corrective incluant un calendrier détaillé des changements recommandés à apporter à l'infrastructure et aux processus pour assurer la conformité PCI DSS – prenant en considération les contraintes budgétaires, de ressources humaines et de gestion de l'information.

Par ailleurs, un service d'évaluation dédié à la sécurité du stockage propose une analyse détaillée des pratiques et procédures de sécurité liées aux infrastructures de stockage réseau EMC.

---

## Découverte et classification des données de carte de crédit

---

Les Services Professionnels RSA permettent de comprendre où résident les données de cartes dans l'infrastructure afin d'assurer une gestion cohérente pendant tout leur cycle de vie. Pour cela, ils utilisent une large gamme d'outils de classification et de découverte au niveau postes utilisateurs, applications, réseaux et datacenter afin d'analyser les emplacements et les flux transactionnels des données de porteurs de cartes.

Ces services vérifient que les données sur les détenteurs de cartes sont correctement utilisées, que leurs modalités de traitement sont documentées et que seules les informations appropriées et nécessaires sont stockées. Les flux transactionnels relatifs à ces données sont analysés pour s'assurer que les informations dans les applications dépendantes et les lignes d'activités associées sont inventoriées et cataloguées.

### Suite RSA DLP: Découvrir les données de cartes de crédit pour supporter la Conformité

Au-delà de la localisation des données cartes dans les applications, fichiers, dossiers, bases de données et systèmes de stockage, les entreprises doivent découvrir leur présence éventuelle en tout autre point de l'infrastructure (par exemple, si des utilisateurs en créent des enregistrements PDF, Excel ou de simples fichiers texte dans des systèmes partagés).

Il n'est en effet pas rare que des centaines de documents contenant des données client sensibles (comme des numéros de cartes de crédit) soient enregistrés dans de multiples serveurs de fichiers. Ce problème est naturellement amplifié par la mobilité ; les utilisateurs pouvant transmettre ces fichiers par e-mail/copie/transfert vers des destinations non-autorisées. Il est donc essentiel pour les entreprises d'identifier ces fichiers et de les sécuriser dans le cadre d'une politique cohérente, afin de respecter les spécifications PCI DSS.

RSA DLP Suite adresse ce challenge en examinant les systèmes de fichiers, les réseaux et les postes utilisateurs pour découvrir les données de porteurs de cartes. Lorsque des fichiers avec des données sensibles sont identifiés et classés, ils peuvent être copiés, déplacés, archivés, supprimés ou sécurisés selon la politique prévue.

De plus, la suite RSA DLP examine les systèmes de fichiers, réseaux et postes utilisateurs pour localiser et supprimer les données sensibles d'authentification – information dont le stockage est interdit par PCI.

---

### Exigence 3: Protéger les données enregistrées de cartes — La solution RSA

---

RSA propose une large gamme de solutions permettant aux clients de répondre à la 3<sup>ème</sup> spécification PCI en protégeant les données stockées des porteurs de cartes – quel que soit leur emplacement et supprimant les données d'authentification. Les solutions de sécurisation des données RSA permettent de protéger les données de porteurs de cartes sur tous les points terminaux de cryptage – qu'elles résident dans une application, une base de données, des fichiers ou dossiers ou sur disque/bande. En outre, la plateforme de gestion des clés d'entreprise RSA Key Manager garantit l'extensibilité des solutions de protection et leur adaptabilité aux évolutions métier et assure que les données restent disponibles tout en étant correctement protégées – à tous les stades de leur cycle de vie.

Les sous-exigences couvertes par les technologies RSA incluent :

- Exigence 3.2: ne pas enregistrer les données d'authentification après l'autorisation (même si elles sont cryptées).

La suite RSA DLP scrute les systèmes de fichiers, réseaux et postes utilisateurs pour identifier des instances de données sensibles d'authentification. Une fois trouvées, la suite DLP peut alors supprimer ces données.

- Exigences 3.4: Rendre au minimum illisible le numéro PAN (Primary Account Number) quel que soit son lieu de stockage

RSA Key Manager propose des bibliothèques applicatives supportant de multiples langages de développement et permettant aux développeurs d'intégrer facilement du cryptage aux multiples applications métiers créant ou manipulant des informations sensibles (ex: point de vente, paiement, CRM, ERP, etc.). RSA Key Manager peut également être utilisé pour crypter les données lorsqu'elles se déplacent vers les disques ou bandes.

## Aider les entreprises à garantir la protection des données de cartes au niveau de toutes les localisations

- Exigence 3.5: Protéger les clés de cryptage utilisées pour coder les données de carte contre toute divulgation ou utilisation illicite

RSA Key Manager est une technologie de gestion centralisée des clés de cryptage permettant d'appliquer de façon centralisée des politiques à toute l'entreprise. Elle offre en outre des possibilités de restriction d'accès et de stockage sécurisé des clés.

RSA Key Manager assure également la conformité à la spécification n°3.5 en offrant des possibilités de restriction de l'accès aux clés de cryptage (par authentification et habilitation) – autant de contrôles examinés attentivement par les auditeurs PCI DSS. Enfin, RSA Key Manager enregistre les clés de cryptage dans une base de données à protection renforcée où les clés sont elles-mêmes cryptées à l'aide d'une clé maîtresse KEK (Key Encryption Key). Les clients peuvent stocker cette clé KEK dans un module de sécurité matérielle renforcée de type HSM (pour « hardware security module ») – c'est-à-dire un périphérique dédié et sécurisé offrant une protection optimale de toutes les clés de cryptage de l'entreprise.

- Exigence 3.6: Documenter et implémenter tous les processus et procédures de gestion des clés utilisés pour crypter les données de carte

RSA Key Manager offre de puissantes fonctionnalités pour gérer tout le cycle de vie des clés de cryptage, en assurant la génération de clés renforcées, en sécurisant leur stockage et leur distribution et en rendant les clés quasiment inaccessibles.

---

## Exigence 4: Crypter les transmissions de données de cartes sur les réseaux ouverts et publics — la solution RSA

---

Les solutions RSA de sécurité des données permettent de protéger les données en transit sur le réseau – y compris dans des emails – et de gérer efficacement le cycle de vie des clés de cryptage associées. Les fonctionnalités spécifiques incluent :

- Exigence 4.1: Utiliser des protocoles renforcés de cryptographie et sécurité pour protéger les données sensibles de détenteurs de cartes pendant les transmissions.

RSA Key Manager s'intègre avec une variété d'applications et peut être utilisé pour crypter des données sur des terminaux de points de vente. Ainsi, les données de cartes de crédit sont sécurisées lorsqu'elles voyagent sur des réseaux ouverts ou publics. Grâce à un partenariat avec CipherOptics, RSA propose une sécurité transparente pour les données en transit sur les réseaux IP – en protégeant les liens inter-systèmes pour empêcher que les données ne soient vulnérables lorsqu'elles passent d'un système à l'autre. Le service de conception et d'implémentation de stockage crypté de RSA intègre des appliances CipherOptics aux environnements clients en appliquant les meilleures pratiques de déploiement de l'industrie.

- Exigence 4.2: Ne jamais envoyer par e-mail des "Primary Account Numbers" non cryptés.

RSA DLP Network peut automatiquement router des e-mails contenant des données de cartes vers un système de cryptage pour sécuriser le message et les fichiers attachés avant leur envoi. Si souhaité, DLP Network peut simplement bloquer ou mettre en quarantaine ces e-mails.

---

## Exigence 6: Développer et maintenir des systèmes et applications sécurisés — la solution RSA

---

Les Services Professionnels RSA procèdent à une revue de la conception et de l'implémentation de la

sécurité des applications pour s'assurer qu'elles sont conformes aux meilleures pratiques, spécifiquement :

- Exigence 6.5: Développer toutes les applications Web sur la base de politiques de codage sécurisé telles que l'« Open Web Application Security Project guidelines»

Le service RSA d'évaluation de conception de sécurité des applications est une offre intégrée fournissant un diagnostic rapide et précis de l'état de sécurité actuel des applications. Les consultants des Services Professionnels RSA analysent le modèle conceptuel et opérationnel des applications cibles et leur environnement ; revoient la conception actuelle des applications et la documentation technique associée ; examinent l'architecture des applications et les flux d'informations et produisent un rapport mettant en lumière les forces et faiblesses des systèmes et opérations relativement aux bonnes pratiques recensées par RSA.

---

## Exigence 7: Restreindre l'accès aux données des détenteurs de cartes aux cas métier "Need-to-Know" —solution RSA

---

Les solutions d'autorisation d'accès RSA permettent de répondre à la 7ième exigence PCI en s'assurant que seuls les utilisateurs autorisés peuvent accéder aux données de cartes dans les systèmes Web et de fichiers. ces fonctionnalités comprennent notamment:

- Exigence 7.1: Restreindre l'accès aux ressources informatiques et informations sur les détenteurs de cartes aux seules personnes ayant besoin d'y accéder pour accomplir leur mission professionnelle.

RSA Access Manager permet également de limiter l'accès aux données de porteurs de cartes dans les applications Web aux seules personnes autorisées et d'affecter ces privilèges sur la base des responsabilités spécifiques d'un collaborateur ou d'un groupe de collaborateurs. Les habilitations RSA Access Manager peuvent être définies selon des attributs sélectifs tels que le rôle (par exemple, service de comptabilité) – ce qui assure la résiliation automatique de l'accès si, par exemple, un collaborateur du service autorisé est transféré à un

autre département. De plus, RSA Access Manager permet de centraliser l'accès aux données de carte ce qui optimise la sécurité en garantissant l'implémentation de contrôles efficaces sur les points d'accès Web.

– Exigence 7.2: Établir, pour les systèmes multiutilisateurs, un mécanisme limitant l'accès en fonction du besoin utilisateur "need-to-know", paramétré pour refuser toute demande d'accès, sauf autorisation spécifique.

RSA Access Manager apporte la capacité de restreindre l'accès aux données en fonction de règles métiers prédéfinies et/ou rôle utilisateur dans l'entreprise. Le logiciel propose des fonctionnalités de "refuser tout" prêtes à l'emploi.

---

### **Exigence 8: Affecter un identifiant unique à chaque personne ayant un accès informatique — la solution RSA**

---

Les solutions d'authentification RSA permettent de s'assurer que les utilisateurs accédant aux informations sur les cartes sont bien ceux qu'ils prétendent être. Les fonctionnalités spécifiques incluent :

– Exigence 8.2: Outre l'affectation d'un identifiant unique, employer au moins une des méthodes suivantes pour authentifier les utilisateurs : 1) Mot de passe 2) Token ou clé de sécurité (SecurID, certificats ou clé publique) 3) Biométrie

RSA SecurID répond à cette exigence grâce à une large gamme de tokens ou authentificateurs matériels et logiciels exécutant l'authentification à deux facteurs. De plus, les solutions RSA de certificats numériques offrent aux clients la liberté de sélectionner le mécanisme d'authentification correspondant le mieux à leurs besoins.

– Exigence 8.3: Implémenter une authentification à deux facteurs pour les accès réseau distants des collaborateurs, administrateurs et tiers.

RSA SecurID permet d'implémenter un système d'authentification à deux facteurs grâce à de multiples options de tokens matériels et logiciels. De

#### **Accès habilité à l'infrastructure PCI**

Grâce au programme de partenariat RSA Secured, RSA SecurID propose des intégrations prêtes à l'emploi avec des centaines de systèmes pouvant appartenir à l'infrastructure PCI (VPN, pare-feux, serveurs d'applications, etc.) permettant ainsi aux clients de s'assurer que les utilisateurs accédant aux systèmes à distance ou de l'intérieur du pare-feu y sont bien habilités. Même si le programme RSA Secured facilite la conformité PCI DSS, l'authentification forte sur l'ensemble du système d'information permet d'améliorer la sécurité bien au-delà de l'audit PCI DSS.

plus, les partenaires certifiés "RSA Secured" proposent des solutions d'accès distant présentant une intégration RSA SecurID prête à l'emploi, ce qui facilite pour les entreprises l'authentification forte de leurs utilisateurs accédant aux ressources via des connexions VPN.

– Exigence 8.4: Crypter tous les mots de passe pendant leur transmission et stockage sur les composants système.

RSA SecurID (en particulier l'authentificateur PINpad RSA SID200 et l'authentificateur logiciel) assure le cryptage du code PIN de l'utilisateur final avant toute transmission physique. Toutes les communications entre les agents RSA SecurID et le serveur sont cryptées, de même que l'ensemble des informations relatives au code PIN de l'utilisateur final pendant leur stockage sur le serveur.

– Exigence 8.5: Assurer l'authentification des utilisateurs et la gestion des mots de passe pour les utilisateurs (autres que consommateurs) et les administrateurs sur tous les composants système

La technologie RSA SecurID aide les clients à aller au delà de cette exigence en leur fournissant les moyens d'une authentification forte des utilisateurs avant tout accès.

---

## Exigence 9: Restreindre l'accès physique aux données de cartes — la solution RSA

---

RSA et EMC fournissent des solutions pour superviser, analyser et gérer la sécurité physique des installations et systèmes sur lesquels sont hébergées et traitées les données de carte de crédit. Les fonctionnalités spécifiques répondant à cette sous-spécification incluent:

- Exigence 9.1: Utiliser des contrôles appropriés sur les points d'entrée pour limiter et superviser l'accès physique aux systèmes hébergeant, traitant ou transmettant des données de carte

La solution de sécurité physique d'EMC permet la gestion, l'analyse, l'archivage et l'extension des informations de sécurité physique et de vidéosurveillance pendant tout leur cycle de vie. EMC Surveillance Manager fournit de puissantes fonctionnalités d'analyse et de gestion automatisée basée sur des règles. Par ailleurs, les systèmes de stockage d'entreprise EMC rendent la solution extensible pour s'adapter à l'évolution des besoins de sécurité physique. Les plates-formes de stockage EMC Centera et la solution de gestion de contenu Documentum permettent de stocker les preuves à des fins d'analyse et de lutte contre les attaques – et d'archiver à long terme les informations de vidéo surveillance et autres données de sécurité physique. EMC Global Services prend en charge la conception et l'intégration de la solution de sécurité physique d'EMC dans les environnements clients les plus divers.

- Exigence 9.7: Établir des contrôles rigoureux sur la distribution interne et externe de tout type de support contenant des données de carte (avec classification des supports afin de permettre leur identification en tant que contenu confidentiel)

L'offre de Services Professionnels RSA de classification des informations à des fins de sécurité est destinée à accompagner les clients dans leurs activités de classification des supports contenant des données de carte de crédit. Les clients peuvent recevoir des instructions de manipulation et d'étiquetage pour les médias contenant des données de cartes.

## Une solution complète pour adresser PCI DSS 10

- Exigence 9.10: Détruire les supports contenant des données de carte dès qu'ils ne sont plus nécessaires au business ou la réglementation

Les Services d'effacement certifié d'EMC mettent en œuvre des techniques propriétaires et des outils standards pour effacer les supports de stockage selon des niveaux spécifiques d'écrasement (3x, 5x, 7x ou personnalisé) et remplacer les données par une séquence de « patterns à bit variable » rendant les données irrécupérables. Les experts d'EMC peuvent fournir ce service sur le site client ou hors-site, sur une gamme entière d'appareils de stockage ou sur des supports spécifiques après un remplacement proactif. Ces services sont disponibles pour les gammes de stockage EMC et pour les systèmes Hitachi, IBM, Sun, Network Appliance et HP. À l'issue du processus, EMC génère un rapport complet et un certificat de destruction pour les drives effacés en indiquant le niveau d'écrasement atteint.

---

## Exigence 10: Contrôler et superviser tous les accès aux ressources réseau et aux données de cartes—la solution RSA

---

La solution RSA de gestion de la conformité et des informations de sécurité, permet aux clients d'établir un point central pour le suivi et le monitoring des accès aux données de cartes dans tout l'environnement PCI. RSA enVision répond intégralement aux contraintes de reporting de la 10<sup>ième</sup> exigence:

- Exigence 10.1: Établir un processus corrélant à chaque utilisateur tous les accès aux composants système (en particulier les accès utilisant des privilèges administratifs de type root).

RSA enVision permet le suivi des activités des utilisateurs administrateurs et fournit une vision qui aide à vérifier qu'un utilisateur agit selon la politique établie. Le système peut également adresser une alerte au supérieur hiérarchique d'un utilisateur en cas de comportement non-conforme.

- **Exigence 10.2: Implémenter pistes d'audit automatiques pour tous les composants système afin de reconstruire les événements clé**

L'appli RSA enVision aide les entreprises à implémenter des pistes d'audit automatisées fournissant des informations détaillées sur les accès aux données de carte ; les actions effectuées par les utilisateurs disposant de privilèges administratifs ; l'accès aux pistes d'audit ; les tentatives invalides d'accès logique ; l'utilisation des mécanismes d'identification/authentification ; l'initialisation des logs d'audit et la création /suppression d'objets système.

- **Exigence 10.3: Enregistrer les données de pistes d'audit**

RSA enVision enregistre les événements fournis par les périphériques et enregistre les métadonnées événementielles qui peuvent être analysées pour déterminer le type d'événement.

- **Exigence 10.5: Sécuriser les pistes d'audit pour éviter leur altération**

RSA enVision adresse des données miroir non-filtrées à sa base de données IP afin qu'elles soient conservées sous leur format original. De plus, ses fonctions exclusives d'écriture unique et de lectures multiples (WORM pour « write once, read many ») empêchent l'altération de la copie miroir – même en cas de corruption des données originales. Les logs d'événements capturés par RSA enVision sont stockés sur un système d'exploitation à protection renforcée, sous une forme compressée et protégés par un cryptage léger.

- **Exigence 10.7: : Conserver l'historique des pistes d'audit pendant une durée minimum d'un an, avec disponibilité en ligne d'au moins trois mois**

RSA enVision NAS3500 offre une plate-forme EMC Celerra préconfigurée pour permettre un stockage de 3,5 à 7 To – particulièrement adapté à la conservation en ligne des données de log. Offrant une intégration immédiate aux plates-formes de stockage réseau EMC® Centera™ et EMC Celerra®, RSA enVision simplifie le stockage des informations critiques pour répondre aux exigences de conformité.

Les systèmes NAS (Network Attached Storage) EMC Celerra offrent le rapport prix/performance leader de l'industrie sans compromis de disponibilité – ceci signifiant que les applications continuent à fonctionner avec le même niveau de performance et de qualité de service même en cas de panne. Celerra accomplit ceci grâce à une architecture de cluster actif/ passif N+1 et à l'élimination de tous les points de défaillance uniques. De plus, les systèmes NAS EMC Celerra implémentent la rétention FLR (« File Level Retention ») offrant une protection de type WORM sur disque – afin de protéger les fichiers et répertoires contre toute tentative de suppression, altération, renommage ou écrasements pendant une période prédéfinie de rétention. Ceci permet notamment de protéger l'intégrité des journaux d'audit en ligne pendant une période spécifique (3 mois, par exemple).

Au delà de sa capacité à aider les clients à répondre à l'exigence 10 PCI DSS, la technologie RSA enVision fournit une robuste plate-forme pour collecter, corrélater et auditer l'accès à une variété de systèmes PCI – des firewalls aux réseaux sans fil en passant par les mécanismes d'authentification et autres. Cette technologie facilite considérablement la démonstration de la conformité à l'exigence 12 PCI.

---

## **Exigence 12: Maintenir une politique de sécurité des informations— la solution RSA**

---

RSA Professional Services aident les clients à créer des politiques et processus pour développer ou améliorer leurs programmes de sécurité. Les consultants revoient notamment les politiques existantes et développent de nouvelles pour garantir que les données de carte sont manipulées correctement. Ils revoient aussi les processus de partage, stockage, étiquetage des média contenant des données de cartes afin de s'assurer qu'ils respectent les pratiques du standard PCI DSS. Ces politiques doivent définir les usages appropriés et nécessaires des données de carte ainsi que les procédures de traitement.

pour plus d'informations, visiter [www.rsa.com/pci](http://www.rsa.com/pci)

## Composant de la solution RSA PCI: Produits et Solutions

- > **RSA® Access Manager** Logiciel de contrôle d'accès aux ressources Web et d'implémentation de politiques centralisées pour les utilisateurs à travers toute l'entreprise.
- > **RSA Data Loss Prevention (DLP) Suite** découverte des données de cartes sur les postes utilisateurs, les réseaux et fichiers de partage. DLP suite aide les entreprises à protéger les fichiers et emails contenant des données de détenteurs de carte et peut être utilisé pour purger les données sensibles d'authentification.
- > **RSA enVision®** Plate-forme complète d'entreprise pour collecter, corréler et analyser les informations de sécurité et de conformité de toute l'entreprise, et prendre en charge le suivi et la supervision des accès aux ressources réseau et données des détenteurs de cartes.
- > **RSA® File Security Manager** offre aux clients la capacité de protéger les données de cartes contenues dans les fichiers sur postes de travail, portables et serveurs contre les attaques internes et externes.
- > **RSA® Key Manager** Logiciel de gestion des clés de cryptage générées par des applications d'entreprise disparates, permettant aux développeurs d'intégrer simplement des fonctionnalités de sécurité à leurs applications – conformément aux politiques de sécurité établies.
- > **RSA SecurID®** Technologie d'authentification à deux facteurs éprouvée garantissant l'identité des utilisateurs accédant aux ressources critiques – notamment à celles contenant des données sur les titulaires de cartes.
- > **EMC Storage Systems y compris EMC Symmetrix®, CLARiiON®, Centera® et Celerra™** Plates-formes de stockage réseau intégrées à RSA enVision, fournissant la capacité de stocker les informations critiques et répondre aux spécifications PCI DSS.
- > **EMC Physical Security Solution** Solution de gestion, d'analyse, d'archivage et d'extension des informations de sécurité physique et de vidéosurveillance pendant tout leur cycle de vie.
- > **Partenaires sélectionnés EMC—CipherOptics—** A travers un partenariat CipherOptics et RSA offrent une sécurité transparente aux données transitant sur les réseaux IP internes.

## Services

- > **Service d'évaluation de conception de sécurité des applications** Diagnostic rapide et précis de l'état actuel de sécurité des applications.
- > **Service de découverte et de classification des données de carte de crédit** Aider les clients à découvrir où sont localisées les données de porteurs de cartes dans l'entreprise et de la gérer efficacement sur son cycle de vie.
- > **Service certifié d'effacement de données EMC** Mise en œuvre de techniques propriétaires et d'outils standards pour effacer les supports de stockage avec des niveaux spécifiques d'écrasement.
- > **Service de politique de sécurité des informations** Création de politiques et processus pour développer et améliorer les programmes de sécurité des informations.
- > **Service d'évaluation de pré-conformité PCI DSS** Diagnostic de la posture PCI actuelle et développement d'une stratégie corrective avant de mener un audit PCI formel.

## RSA Votre partenaire de confiance

RSA, la Division Sécurité d'EMC, est le premier fournisseur de solutions de sécurité pour l'accélération métier et le partenaire privilégié des plus grandes entreprises mondiales pour résoudre leurs challenges de sécurité les plus pressants, complexes et sensibles. L'approche de la sécurité centrée sur l'information prônée par RSA garantit l'intégrité et la confidentialité de l'information tout au long de son cycle de vie - quels que soient ses cheminements, ses consommateurs ou ses modalités d'utilisation.

RSA propose des solutions leaders de certification des identités et de contrôle d'accès; de prévention des pertes de données; de cryptage et gestion de clés; de gestion de la conformité et informations de sécurité et de lutte contre la fraude. Cette large gamme de solutions certifie l'identité de millions d'utilisateurs dans le monde et des données qu'ils génèrent lors de leurs transactions quotidiennes. Pour plus d'informations, veuillez consulter [www.RSA.com](http://www.RSA.com) et [www.EMC.com](http://www.EMC.com).



The Security Division of EMC

RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

©2008 RSA Security Inc. Tous droits réservés  
RSA, RSA Security, enVision, SecurID et le logo RSA sont des marques ou marques déposées de RSA Security Inc. aux États-Unis et/ou dans d'autres pays. EMC est une marque déposée d'EMC Corporation. Tous les autres produits et services mentionnés sont des marques de leurs propriétaires respectifs.

FR PCI SB 0208