LIVRE BLANC | DÉCEMBRE 2015

Garantir la conformité PCI

grâce à la gestion des accès à forts privilèges

ca technologies

Résumé

Défi

Les organisations qui traitent des transactions impliquant des cartes de crédit doivent répondre à des exigences toujours plus fortes pour garantir leur conformité avec les réglementations. L'une de ces réglementations est la norme PCI DSS : mise au point par le secteur des services de paiement par carte, cette norme, dont la version 3 est applicable depuis janvier 2015[1], définit un certain nombre d'exigences (conditions) visant à protéger les systèmes et réseaux de l'organisation, en particulier l'environnement de données des détenteurs de carte (Cardholder Data Environment, CDE). Dans un contexte réglementaire exigeant une authentification et un contrôle stricts des accès au CDE, implémenter une authentification multifacteur, un contrôle des accès et des outils ou pratiques de reporting sur les activités, en particulier celles des comptes administrateur ou à forts privilèges, relève du défi pour les organisations.

Solution

Les conditions de la norme PCI DSS relatives à la gestion des accès à forts privilèges identifient les risques associés à une utilisation abusive de comptes à forts privilèges et de l'accès que ces comptes offrent à des ressources critiques de l'entreprise. Si nous examinons les incidents de sécurité informatique les plus récents, nous constatons que dans la plupart des cas, des utilisateurs ou identifiants à forts privilèges ont servi de vecteurs d'attaque. Une approche de gestion des accès à forts privilèges efficace doit permettre à l'organisation de restreindre, journaliser et superviser toutes les activités de ses comptes à forts privilèges, tels que les administrateurs réseau, système et de bases de données, pour lui offrir une visibilité et un contrôle renforcés sur ses utilisateurs à forts privilèges et leur accès « superutilisateur » à ses ressources les plus précieuses. Sans cela, l'organisation éprouvera des difficultés non seulement pour assurer sa conformité avec les conditions d'identification, d'authentification et de contrôle des accès de la norme PCI DSS v3, mais aussi pour réduire son exposition aux risques de violations de sécurité et d'attaques.

Avantages

Une approche de gestion avancée des accès à forts privilèges, intégrée dans une solution facile à déployer telle que CA Privileged Access Manager, peut aider l'organisation à répondre aux exigences de la norme PCI DSS v3 pour mieux protéger non seulement son CDE, mais également l'ensemble de son environnement informatique hybride (réseau, serveur, virtuel et Cloud). C'est le moyen pour elle de gagner en sécurité et de réduire son exposition aux violations de sécurité et attaques, tout en garantissant sa conformité avec la norme PCI DSS.

Section 1

Gestion des accès à forts privilèges : un impératif

Il n'a jamais été aussi important de mettre en œuvre une gestion des accès à forts privilèges. Étude après étude, les défaillances des systèmes de défense traditionnels apparaissent au grand jour. Il semblerait même que pratiquement chaque organisation ait au moins une fois dans son existence été la victime d'une attaque avérée.[2] Les médias se font régulièrement l'écho de divulgations de données majeures : toutes ces affaires (Target à la fin de l'année 2013, Home Depot en 2014 et Office of Personnel Management en 2015, pour n'en citer que trois) ont impliqué le vol d'identifiants par des tiers. En fait, le rapport 2014 de Verizon sur les violations de sécurité cite l'utilisation d'identifiants volés au premier rang des menaces auxquelles les organisations sont confrontées.[3]

Or, ces dernières ne sont souvent pas conscientes des dangers que posent leurs comptes à forts privilèges, tant par leur nature que par leur nombre. Les collaborateurs de l'organisation ne sont pas les seuls utilisateurs de comptes à forts privilèges : une organisation peut également en attribuer à des tiers, notamment des fournisseurs, des sous-traitants ou encore à des personnes assurant un service d'assistance technique sur des systèmes, des périphériques réseau et des applications. Une seule organisation peut ainsi se retrouver avec des milliers, voire des dizaines de milliers de comptes à forts privilèges, chacun posant un risque de sécurité particulier à l'échelle de l'organisation.

Le véritable objectif d'une gestion des accès à forts privilèges est de renforcer la responsabilisation et la visibilité sur les activités des administrateurs, pour sortir d'un modèle de fonctionnement traditionnel dans lequel l'entreprise accordait une confiance totale à l'ensemble de ses administrateurs. Une confiance naïve qui occultait deux risque majeurs : le risque de voir un administrateur mécontent devenir une menace interne et le risque lié à la compromission d'un compte administrateur par un attaquant externe, un risque d'autant plus présent si l'administrateur en question est un fournisseur ou un autre tiers.

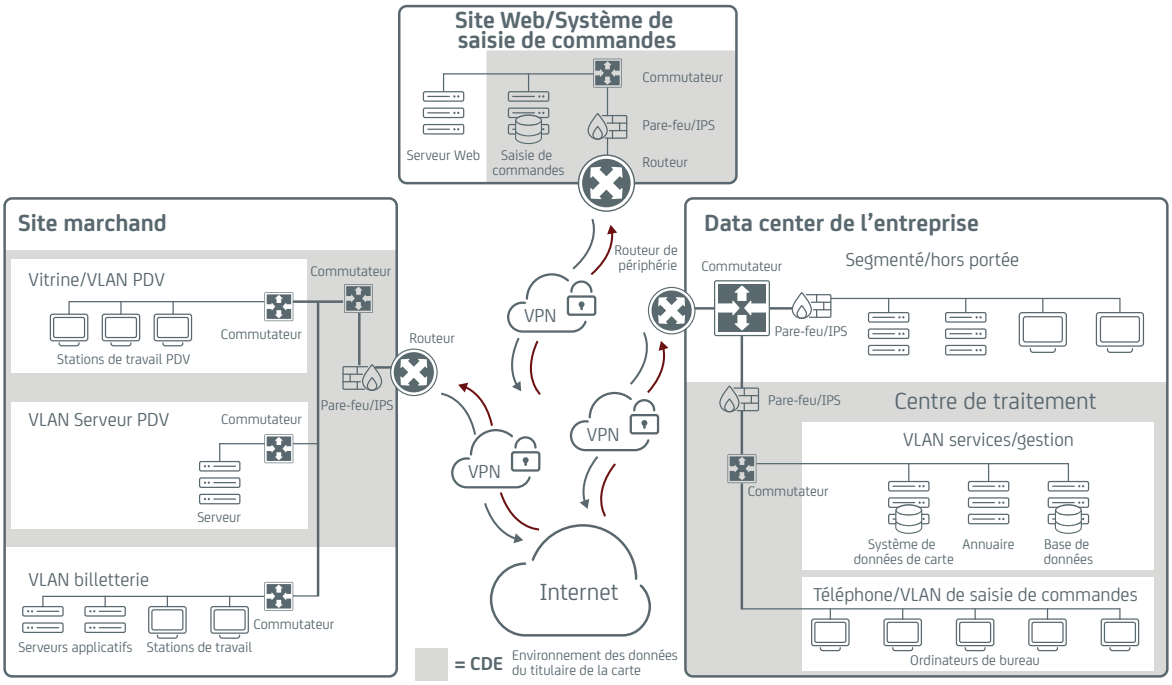
Pour protéger l'organisation face à ces risques, il convient d'adopter un modèle « zéro confiance » dans lequel les administrateurs ne disposent pas d'une confiance totale : cette approche est celle appliquée par CA Privileged Access Manager (anciennement Xceedium Xsuite), un composant clé des solutions de gestion des accès à forts privilèges de CA Technologies. Ce modèle de fonctionnement permet de limiter le nombre de divulgations, mais aussi leur gravité. Plusieurs exigences de la norme PCI DSS reflètent ce modèle zéro confiance : ainsi, la condition 7.1.2 préconise de restreindre l'accès des ID utilisateurs privilégiés aux privilèges les plus faibles nécessaires pour la réalisation du travail.

Cependant, bien que la norme PCI offre des bases solides pour sécuriser les CDE, il ne suffit pas de cocher des cases et de se conformer aux exigences minimales définies pour se défendre dans l'environnement de menace actuel. Pour préserver son CDE de manière optimale, une organisation doit dépasser ces exigences dans sa gestion des accès à forts privilèges.

Au-delà de la conformité PCI, la mise en place d'une gestion des accès à forts privilèges est importante pour aider l'organisation à rompre la chaîne de frappe, limiter les menaces en interne, journaliser et superviser les commandes et éliminer les mots de passe codés de manière irréversible.

Illustration A : la portée des exigences de la norme PCI DSS

La norme PCI DSS v3 édicte des mesures pour préserver l'environnement de données des détenteurs de cartes.



Rompre la chaîne de frappe

Le concept de chaîne de frappe fait référence au fait qu'un attaquant suit un schéma répétitif afin de gagner (ou d'étendre) l'accès à un système, avant de rehausser ses privilèges. Il utilise ensuite ces privilèges pour accéder à un autre système ou étendre davantage son accès existant, avant de rehausser à nouveau ses privilèges pour continuer d'exploiter la chaîne de frappe… jusqu'au moment où il atteint sa cible finale. L'enjeu est de parvenir à rompre cette chaîne de frappe, afin d'arrêter l'attaque avant qu'elle atteigne la cible finale.

CA Privileged Access Manager propose des fonctionnalités pour aider les organisations à rompre les chaînes de frappe : elle prend notamment en charge l'authentification multifacteur pour les comptes à forts privilèges, ce qui rend ces derniers bien plus difficiles à compromettre, car l'attaquant doit usurper plusieurs identifiants pour atteindre un seul de ces comptes. Par ailleurs, comme chaque compte à forts privilèges dispose des privilèges les plus faibles de manière à ne pouvoir effectuer que certaines commandes sur des composants spécifiques du CDE de l'organisation, l'accès aux informations sensibles, et donc les risques d'accès non autorisés, sont limités.

La prise en charge de la segmentation du réseau est une autre fonctionnalité qui contribue à rompre les chaînes de frappe : elle permet de restreindre le nombre de sous-réseaux auxquels un compte à forts privilèges particulier peut accéder, ainsi que les systèmes pouvant être administrés sur chaque sous-réseau. La segmentation réseau contribue à limiter la propagation des attaques d'un système à un autre, ainsi que la visibilité que les attaquants peuvent avoir sur le réseau de l'organisation. CA Privileged Access Manager propose également un agent de filtre de sockets (SFA) qui empêche un administrateur d'ouvrir une connexion réseau non autorisée avec un autre système (une session SSH ou Telnet vers un hôte non autorisé par une règle CA Privileged Access Manager, par exemple).

Toutes ces fonctionnalités de CA Privileged Access Manager sont recommandées par des sources telles que Mandiant pour réduire les fraudes aux cartes de crédit.[4]

Limiter les menaces internes

Bien que les exigences PCI se concentrent sur les attaquants externes, elles reconnaissent également l'importance des menaces internes, de plus en plus présentes aujourd'hui. D'après une étude, plus de 10 % des collaborateurs ont déjà volé des informations de leur employeur pour leur propre profit ou connaissent une personne qui l'a fait.[5]

CA Privileged Access Manager contribue à réduire les menaces internes de plusieurs façons. Premièrement, en attribuant à chaque utilisateur les privilèges les plus faibles dont il a besoin pour exécuter son travail, la solution limite les commandes qu'il est en mesure d'émettre ainsi que le nombre de composants du CDE pouvant être affectés par ces commandes. Cela permet dans les faits de minimiser les dommages que risquerait de provoquer une attaque initiée par un membre de l'organisation. Par ailleurs, la solution journalise et supervise l'ensemble des activités des comptes à forts privilèges, de sorte que l'organisation dispose d'un journal complet et détaillé dans lequel chaque commande est associée à une personne spécifique plutôt qu'à un ID générique (partagé).

Journaliser et superviser les commandes

Quelle que soit la force des contrôles de sécurité en place, les failles sont toujours possibles, et par conséquent, des violations sont inévitables dans tous les environnements. En journalisant et en supervisant toutes les activités impliquant des comptes à forts privilèges, la solution CA Privileged Access Manager simplifie considérablement les processus d'investigation permettant de retracer le parcours d'attaquants ayant utilisé ces comptes de manière abusive.

Éliminer les mots de passe codés de manière irréversible

Nombreux sont les développeurs logiciels, administrateurs et autres professionnels qui utilisent des mots de passe codés de manière irréversible dans leurs scripts, les codes source et ailleurs. C'est une source de vulnérabilité importante, dans la mesure où ces mots de passe sont accessibles aux développeurs, testeurs et autres utilisateurs spécialisés, et que les attaquants savent où les rechercher lorsqu'ils s'infiltrent dans un système, pour les exploiter afin de gagner l'accès à d'autres systèmes (des bases de données de détenteurs de cartes, par exemple). CA Privileged Access Manager propose des fonctionnalités d'authentification d'application à application qui permettent d'éviter de recourir à des mots de passe codés de manière irréversible.

Section 2

En quoi une gestion des accès à forts privilèges aide l'organisation à atteindre la conformité PCI

Comme nous l'avons mentionné précédemment, une gestion des accès à forts privilèges est essentielle pour atteindre la conformité avec la norme PCI DSS. Dans les environnements d'entreprise classiques, une multitude d'exigences PCI ne peuvent pas être respectées si vous ne faites pas appel à une solution de gestion des accès à forts privilèges. Prenons l'exemple de ce grand distributeur, qui risquait une amende mensuelle de 100 000 dollars du fait de sa non-conformité aux exigences d'identification, d'authentification et de contrôle des accès de la norme PCI. En intégrant CA Privileged Access Manager dans son portefeuille de solutions de sécurité, il est parvenu à répondre à ces exigences et à éviter d'autres amendes.

CA Privileged Access Manager permet aux organisations de satisfaire à l'ensemble des exigences PCI décrites ci-après.[6]

Condition 2 : ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur.

CA Privileged Access Manager satisfait à cette exigence de deux façons : au moment du déploiement du système, en prenant le contrôle des comptes à forts privilèges par défaut et en assurant la réinitialisation des mots de passe par défaut de ces comptes. Ensuite, en limitant le nombre de protocoles pouvant être utilisés pour les accès administrateur à distance (SSH ou SSL/TLS, par exemple). La solution permet ainsi d'empêcher l'exécution de tâches d'administration système sur des réseaux utilisant des protocoles non sécurisés.

Condition 6 : développer et gérer des systèmes et des applications sécurisés.

Cette exigence implique une gestion appropriée des identifiants et la séparation des fonctions dans les environnements de développement, test et production. CA Privileged Access Manager applique un contrôle des accès basé sur les rôles pour les comptes à forts privilèges dans l'ensemble de ces environnements, prenant en charge la séparation des fonctions tout en facilitant la suppression des comptes (développement, test et autres) qui ne sont plus nécessaires à la suite du déploiement d'un système ou d'une application.

Condition 7 : restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître.

CA Privileged Access Manager permet à l'organisation d'attribuer à chaque utilisateur les privilèges les plus faibles dont il a besoin pour l'exécution de ses tâches. Son modèle de fonctionnement « zéro confiance » assure un contrôle avancé des accès pour les utilisateurs ou groupes d'utilisateurs à forts privilèges (administrateurs de bases de données par ex.), afin de restreindre le nombre de composants système (serveurs, périphériques réseau et applications notamment) auxquels chacun peut accéder, ainsi que les commandes qu'il peut exécuter sur ces composants. En outre, CA Privileged Access Manager peut s'intégrer avec des annuaires Active Directory, LDAP et autres annuaires d'entreprises, pour réutiliser leurs définitions de groupes et de rôles.

Condition 8 : identifier et authentifier l'accès aux composants du système.

La quasi-totalité des critères de la condition 8 sont pris en charge explicitement par CA Privileged Access Manager. Cette solution exige l'attribution d'un ID unique à chaque utilisateur à forts privilèges, fournit l'ensemble des fonctionnalités de gestion des mots de passe standard et prend en charge un large éventail de technologies d'authentification à un ou plusieurs facteurs. CA Privileged Access Manager satisfait à la condition 8 de la norme PCI comme suit :

- **8.1 :** CA Privileged Access Manager identifie chaque utilisateur à forts privilèges de manière unique, même lorsque l'organisation utilise des « comptes partagés » pour des composants d'infrastructure spécifiques (routeurs, par exemple). La solution permet d'appliquer la séparation des fonctions entre les utilisateurs à forts privilèges et fournit des fonctionnalités standard permettant d'annuler immédiatement des privilèges d'accès révoqués, de désactiver des comptes à forts privilèges inactifs et d'appliquer des règles de verrouillage pour les tentatives d'authentification échouées ou de réauthentification dans le cas de sessions restées inactives trop longtemps).
- **8.2 :** la solution intègre un grand nombre de méthodes d'authentification et oblige tous les utilisateurs à forts privilèges à s'authentifier. Elle stocke les mots de passe et autres identifiants (notamment les clés cryptographiques privées) dans une chambre forte avec chiffrement avancé, et les transmet uniquement via des canaux chiffrés. Elle applique des règles de longueur, de force, de durée de vie et de réutilisation des mots de passe standard.
- **8.3 :** la solution prend en charge plusieurs méthodes d'authentification multifacteur, ainsi que les certificats RADIUS, X.509 et les cartes à puce.
- **8.5, 8.6 :** la solution permet à l'organisation d'utiliser des « comptes partagés » en arrière-plan tout en exigeant une identification et une authentification uniques de chaque utilisateur à forts privilèges, y compris tiers. Cette identification unique peut être réalisée à l'aide d'une carte à puce, d'un certificat numérique, d'un jeton cryptographique ou d'une autre forme d'identification sans mot de passe.
- **8.7 :** la solution restreint l'accès direct à la base de données des détenteurs de carte aux seuls administrateurs autorisés. La prise en charge d'application à application permet de garantir que les individus ne puissent pas accéder aux identifiants d'application ni les réutiliser.

Condition 10 : effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes.

Comme pour la condition 8, CA Privileged Access Manager prend en charge quasiment tous les critères de la condition 10 de la norme PCI DSS. La solution journalise et enregistre toutes les activités exécutées au moyen de chaque compte à forts privilèges, y compris les enregistrements d'audit au format Syslog et les enregistrements des sessions administrateur (format lecteur DVD), et permet d'insérer des balises indiquant des violations potentielles de règles dans les enregistrements afin

d'accélérer leur examen. CA Privileged Access Manager prend en charge la condition 10 de la norme avec les fonctionnalités suivantes :

- **10.1 :** CA Privileged Access Manager permet de relier chaque instance d'accès à forts privilèges à une personne spécifique. Elle fournit des pistes d'audit pour chaque personne utilisant un compte à forts privilèges pour accéder à des composants du système.
- **10.2 :** CA Privileged Access Manager utilise une journalisation en mode natif et au format Syslog pour générer des pistes d'audit automatisées qui enregistrent toutes les actions de chaque utilisateur à forts privilèges sur les serveurs, périphériques réseau, bases de données et autres applications. Elle prend en compte toutes les activités d'identification et d'authentification des comptes à forts privilèges. Elle restreint l'accès aux pistes d'audit, afin que seuls les utilisateurs autorisés puissent les consulter, et journalise l'ensemble de ces consultations.
- **10.3 :** la solution enregistre toutes les informations de conformité PCI de chaque événement, notamment l'identification de l'utilisateur, le type d'événement, la date et l'heure, l'état d'échec ou de réussite, l'origine de l'événement et l'identité de la ressource concernée (nom d'hôte, etc.).
- **10.4 :** elle utilise une technologie de synchronisation (protocole NTP) pour réaliser la synchronisation des horloges.
- **10.5 :** elle utilise des techniques de hachage pour identifier toute altération des enregistrements et journaux d'audit. Elle intègre une fonctionnalité de transfert syslog qui permet de sauvegarder les enregistrements d'audit dans un emplacement de stockage centralisé.
- **10.7 :** elle utilise syslog et prend en charge le transfert syslog, pour garantir la conservation des enregistrements d'audit pendant la durée souhaitée.

Condition 12 : entretenir une règle qui répond aux exigences de sécurité et l'appliquer à l'ensemble du personnel.

CA Privileged Access Manager permet la capture et l'application de règles applicables aux utilisateurs à forts privilèges. Par ailleurs, la solution journalise toutes les tentatives de violation des règles, dans le cadre du processus d'évaluation des risques.

Protection du CDE : perspective de contrôle des serveurs

CA Technologies propose une gestion des accès à forts privilèges qui répond également aux exigences liées à un contrôle avancé des accès au niveau de l'hôte, pour renforcer la protection des ressources les plus critiques de l'organisation, parmi lesquelles son CDE. CA Privileged Access Manager Server Control fournit une couche supplémentaire critique de protection pour les plates-formes serveur, qui prend en charge un contrôle fin des accès, une gestion basée sur des règles et un audit sécurisé, trois composants essentiels à la sauvegarde des ressources électroniques de l'organisation. Ce produit permet de créer des règles d'accès définissant les conditions d'accès aux ressources serveur, programmes, fichiers et processus sur la base d'un large éventail de critères.

Section 3

Modifications apportées dans la version 3 de la norme PCI DSS

La version 3 de la norme PCI DSS intègre un certain nombre de critères de protection importants pour le CDE :

- Mise en œuvre d'une segmentation réseau, pour mieux isoler les différentes portions du CDE. Cela implique également de garantir la documentation de l'ensemble des flux de données entre les composants du système et l'audit des activités des utilisateurs à forts privilèges.
- Réalisation de tests de pénétration sur le périmètre du CDE.
- Gestion des identifiants et implémentation d'un contrôle des accès basé sur l'attribution des privilèges les plus faibles nécessaires et l'audit de tous les accès au CDE.
- Renforcement des contrôles de sécurité pour les prestataires de services.[7]

Ces protections soulignent le besoin d'une solution de gestion des accès à forts privilèges telle que CA Privileged Access Manager pour protéger le CDE et satisfaire aux exigences PCI. Dans la plupart des environnements, la gestion des accès à forts privilèges est le seul instrument permettant une implémentation efficace du principe d'attribution des privilèges les plus faibles nécessaires et une journalisation détaillée des activités administrateur. Sa valeur peut être inestimable dans l'implémentation d'une segmentation réseau et d'une supervision de toutes les activités impliquant des flux de données entre les différents segments du réseau.

La mise à jour de la norme PCI DSS contient d'autres modifications liées à la gestion des accès à forts privilèges. La condition 8 sur l'identification et l'authentification a été fortement restructurée, si bien qu'elle semble très différente à première vue.

La principale modification apportée est l'ajout de la condition 8.6 qui stipule que lorsque des mécanismes d'authentification autres que les mots de passe sont utilisés (par exemple, des jetons cryptographiques, des cartes électroniques, etc.), les mécanismes d'authentification doivent être affectés à un utilisateur unique et non pas partagés par de multiples personnes. CA Privileged Access Manager satisfait à cette exigence, comme expliqué dans la section précédente.

Section 4

Avantages

Une organisation qui implémente une solution de gestion des accès à forts privilèges gagne un meilleur niveau de sécurité, réduit son exposition aux menaces internes et externes et améliore sa conformité avec les normes (PCI DSS et autres).

Ainsi, CA Privileged Access Manager peut aider une organisation à se mettre en conformité avec la norme PCI DSS, mais aussi à améliorer de façon économique sa sécurité globale :

- **Réduction des coûts :** CA Privileged Access Manager permet de réduire de manière considérable le coût des audits PCI DSS, notamment en fournissant une méthode simple et très économique pour segmenter logiquement le réseau de l'organisation. La solution fonctionne à la manière d'un périphérique de type proxy, au niveau de la couche applicative du réseau, contrôlant quels utilisateurs à forts privilèges peuvent accéder aux systèmes. La segmentation logique du plan de gestion permet à l'organisation de conserver sa topologie réseau physique existante, tout en divisant les systèmes comportant des données de détenteurs de cartes en plusieurs îlots dont l'accès est étroitement contrôlé. Grâce à cette approche, CA Privileged Access Manager est en mesure d'isoler de manière logique les systèmes comportant les données de détenteurs de cartes, et ainsi de limiter la portée des audits PCI sans engager le coût qu'une segmentation physique des réseaux.
- **Sécurité renforcée :** l'approche de défense en profondeur de CA Privileged Access Manager aide l'organisation à implémenter un ensemble complet de contrôles, pour réduire les risques liés aux utilisateurs à forts privilèges et mieux se protéger contre les menaces externes, en prévenant les brèches de sécurité ou en minimisant leur impact.
- **Déploiement plus rapide des fonctionnalités de protection et de gestion :** la facilité de déploiement et la gestion depuis une plate-forme unique permettent un contrôle amélioré et accéléré des accès à forts privilèges et la protection des identifiants d'accès aux systèmes sur l'ensemble de l'environnement de l'organisation (data centers, environnements virtualisés, Clouds publics ou hybrides) sans engendrer les coûts généralement associés aux autres approches.

Section 5 :

Conclusions

Si une gestion des accès à forts privilèges est un impératif pour la mise en conformité de l'organisation avec les exigences PCI, son importance va bien au-delà, car elle permet d'améliorer la sécurité globale de l'organisation, dans un contexte actuel où les menaces viennent autant de l'extérieur que de l'intérieur. CA Privileged Access Manager fournit une méthode de gestion des accès à forts privilèges efficace et prenant en charge la conformité PCI et d'autres exigences de sécurité.

Grâce à CA Privileged Access Manager, les organisations peuvent mieux réaliser les objectifs suivants :

- Réduire leurs coûts de mise en conformité PCI, au moyen d'une solution unique et prête à l'emploi qui s'intègre de manière transparente avec leurs solutions existantes.
- Économiser sur leurs dépenses liées aux incidents de sécurité et préserver leur réputation, en évitant de nombreuses violations et en réduisant l'impact de celles qui se produisent.

1. PCI DSS v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids
2. Cisco 2014 Annual Security Report, http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
3. Verizon 2014 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2014/?utm_source=earlyaccess&utm_medium=redirect&utm_campaign=DBIR
4. M-Trends 2014: Beyond the Breach, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf
5. Data Leakage Worldwide: The High Cost of Insider Threats, http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.pdf
6. PCI DSS v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids
7. PCI DSS Summary of Changes v2.0 to v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

CS200-163851_1215