LIVRE BLANC
CA PRIVILEGED ACCESS MANAGEMENT

Quand transformation digitale rime avec cybercriminalité.

Co-rédigé par Marc CIERPISZ
Cyber Security offer Director
et CA Technologies

cyber security | econocom

ca technologies

Les identifiants à forts privilèges servent de principal vecteur d'attaque à de nombreux incidents de violation. La protection des accès à forts privilèges est donc un impératif pour préserver une organisation d'une violation et est un élément indispensable au respect de nombreux programmes de conformité. CA Privileged Access Management aide à promouvoir la sécurité IT et la réduction des risques liés à la conformité tout en améliorant l'efficacité opérationnelle par le biais d'un plan de défense approfondi des accès à forts privilèges et d'une protection globale et cohérente des identifiants d'administrateur sensibles, d'une gestion des accès et identités à forts privilèges et d'un contrôle des activités des administrateurs.

Résumé

Défi

Nombreuses sont les divulgations de données qui résultent d'une violation de comptes utilisateur à forts privilèges. Les risques se propagent à toute vitesse dans les environnements traditionnels, Cloud et virtualisés dynamiques qui sont aujourd'hui la norme dans les entreprises. Un seul compte utilisateur à forts privilèges doté d'autorisations inappropriées peut causer des dommages conséquents et irréversibles à l'infrastructure d'une organisation, à sa propriété intellectuelle et à son image de marque, entraînant une chute brutale de sa valeur boursière et des perturbations organisationnelles de grande ampleur, ainsi que de lourdes pénalités pour manque de conformité. Une gestion efficace de ces accès dans votre entreprise hybride est indispensable pour réduire les risques liés à la sécurité et à la conformité.

Solution

CA Technologies aide les organisations à implémenter une stratégie de défense approfondie englobant tous les éléments indispensables pour pouvoir relever le défi de la gestion des accès à forts privilèges. La solution CA Privileged Access Management fournit un éventail complet de fonctionnalités de gestion des accès à forts privilèges pour l'ensemble de l'entreprise «hybride», y compris les ressources des data centers physiques traditionnels, des data centers logiciels, des réseaux et du Cloud.

Avantages

En termes financiers et de réputation, les avantages d'une gestion efficace des risques liés à la sécurité et à la conformité, de la protection contre une utilisation inappropriée des comptes à forts privilèges et de la mise en sécurité des ressources critiques peuvent être significatifs pour l'organisation. CA Privileged Access Management offre plusieurs couches de protection des identités et identifiants à forts privilèges à travers l'entreprise hybride. Ces fonctionnalités aident les organisations à mener une prévention active contre les violations, à faciliter les audits et la conformité, et à améliorer la productivité du personnel ainsi que l'efficacité opérationnelle globale.

Section 1

Protéger son entreprise contre les violations

Qu'ils soient administrateurs, auditeurs, managers, RH, DSI, RSSI, membres du COMEX ou simplement employés, ils ont un point commun : posséder au moins un compte avec des accès privilégiés.
Leur métier : permettre à l'entreprise d'être agile, de prospérer et d'être au service des utilisateurs et des clients de l'entreprise. Ils sont là pour protéger et faire prospérer l'entreprise...
En Février 2015, 78 millions de dossiers de patients ont été exposés dans une violation de données majeure à Anthem, et déjà certains professionnels vont fustiger ces propos et dire que ce n'est pas vrai.
Pourtant, la plupart des affaires qui ont fait la une des médias l'ont démontré : du post-it collé sur l'écran, au fichier Excel contenant les mots de passes, une majorité des entreprises est fortement exposée et ce n'est pas une image d'Epinal.
La preuve en est :
La France a été classée au 9ème Rank par le Global Cybersecurity Index & Cyberwellness Profiles Avril 2015 qui vise à mesurer l'engagement et la préparation en termes de cybersécurité d'un pays.

De plus, la France vient de rentrer dans le Top 10 des pays les plus exposés à la Cybercriminalité dans une autre étude publiée par les chercheurs de Symantec sur les cybermenaces portant sur l'année 2015.

Fort de ce constat, nous ne pouvons que dire que « La cybercriminalité, est un secteur en pleine croissance » et que nous nous devons de changer notre vision de la sécurité.
500 millions d'informations personnelles ont été volées ou perdues en 2015.
On comprend mieux pourquoi la Cybersécurité reste toujours autant sous-estimée en France par rapport au reste du monde.
Comme pour le nuage de Tchernobyl nous avons nos frontières !
Et pourtant, la liste des victimes Entreprises, PME, Startup, FinTech, etc... ne cesse de s'allonger.
La mauvaise nouvelle pour ces dernières est que les demandes évoluent avec les nouvelles générations «Digital Native» et les nouvelles orientations technologiques comme le Cloud, la Mobilité et l'IOT. Se protéger contre de telles menaces est devenu aujourd'hui un véritable casse-tête chinois.

Entre 2015 et 2016, le budget moyen annuel relatif aux investissements de cyber-sécurité est passé de 3,7 à 4,8 milliards de dollars, soit une augmentation de 29%, selon l'enquête 2016 de PwC.
Le nombre quotidien des cyber-attaques s'est établi en 2015 à environ 160.000 actes de cybercriminalité, en hausse de 38%, expliquant que le coût global de ces attaques pour les entreprises s'est élevé à 400 milliards de dollars. - Lire aussi : http://lematin.ma/journal/2016/l--inquietante--progression-de-menaces/245488.html#sthash.twNIZJWw.dpuf

Mais alors, de nouvelles vulnérabilités dans l'économie ou plus simplement un manque de temps dans la révolution numérique nous bousculent.

Il y a une dizaine d'année, nous parlions du Cloud et de l'impact de la sécurité de nos données, du Patriot-Act et bien d'autres choses encore…
Et pourtant, le Cloud reste avant tout une évolution économique « Time is money ».
En effet, il est demandé aux services IT des entreprises une optimisation des coûts et une amélioration de la qualité de service qu'elles peuvent proposer à leurs utilisateurs.
Mais l'évolution Trans-générationnel et technologique nous conduit vers une autre révolution « Time is The Market ».
Il faut toujours plus d'Agilité, de destruction créative, de création de valeurs. Dans quel but ? « Gagner du temps !»
Cependant, cette révolution qui arrive fait perdre pied à beaucoup d'entreprises et aussi à leur S.I.
Combien de DSI, de RSSI ne maîtrisent plus la totalité de leur système d'information et pensent toujours continuer de maîtriser les vulnérabilités qui les entourent au quotidien ?
Quelle entreprise a eu un réel plan de gestion de l'obsolescence ou de transformation de son S.I ?
A chaque fois, les mêmes réponses : « Trop cher ! » « On verra plus tard ! »
Sauf que maintenant nous y sommes !

Cette attitude, couplée à cette lame fond qu'est la transformation du digital, ont généré toute une panoplie de nouvelles zones d'exposition aux attaques, à protéger en plus des infrastructures existantes que vous protégez déjà depuis des années.

Ces nouveaux points faibles sont notamment les suivants :

Les environnements hybrides : à mesure que votre environnement IT évoluait pour inclure des réseaux et des data centers logiciels, et s'étendait au-delà de vos quatre murs physiques pour intégrer des ressources de Cloud public et des applications SaaS (Software-as-a-Service), les approches traditionnelles en matière d'administration et de gestion se sont vite avérées insuffisantes, principalement parce qu'elles ne permettaient pas de protéger les nouvelles zones d'exposition aux attaques telles que les consoles de gestion et les API.

Les droits d'administration : les administrateurs disposent en outre d'un pouvoir exceptionnel dans ces environnements en évolution, car ils possèdent les droits nécessaires pour définir, ou redéfinir, l'ensemble de l'infrastructure IT de l'organisation, d'un simple clic.

Les outils d'automatisation : dans les organisations IT les plus sophistiquées, certains de ces processus sont totalement dépourvus d'intervention humaine. Les tâches telles que le provisioning, l'administration et la gestion sont automatisées avec des scripts ou des outils, comme Chef et Puppet, souvent par le biais de droits d'administration codés en dur qui sont une véritable porte ouverte pour le vol et l'utilisation abusive.

Les risques associés liés à la génération Digital Native et à la révolution du numérique doivent nous permettre de mieux comprendre ce phénomène et ses implications pour éviter l'incapacité des entreprises à définir et contenir les menaces internes et les vols de données qui représentent déjà plus de 40% aujourd'hui.

« D'ici à 2017, des réglementations plus strictes en matière de contrôle des accès à forts privilèges entraîneront une hausse de 40 % des amendes et pénalités imposées par les organismes de réglementation pour les organisations dont les contrôles de gestion des accès à forts privilèges laissent à désirer. »

Étude de Gartner, « Market Guide for Privileged Access Management », 2015

Saviez-vous que le vol et l'exploitation des comptes à forts privilèges est un facteur de succès critique pour les pirates dans 100 % des attaques de haut niveau, quelle que soit l'origine de l'attaque ?

Une révélation ? Une mauvaise nouvelle ?
Non ! Plutôt une nouvelle fenêtre de réflexion pour revenir sur les fondamentaux.
Si les comptes à forts privilèges sont le fil rouge de ces innombrables attaques et vulnérabilités, c'est exactement sur ces comptes et sur les données d'identification associées, que vous devez concentrer vos efforts de protection.

Pourquoi a-t-on autant de difficulté pour gérer les « utilisateurs à forts privilèges » en tant que groupe, car cette population est parfois très diversifiée.
Et bien toujours la recherche de l'optimisation du temps.

Par exemple, elle peut inclure des utilisateurs internes qui travaillent pour vous, des utilisateurs extérieurs tels que des fournisseurs ou des prestataires, et même des utilisateurs à forts privilèges inconnus qui sécurisent des ressources IT « fantômes » sans que vous en ayez connaissance.

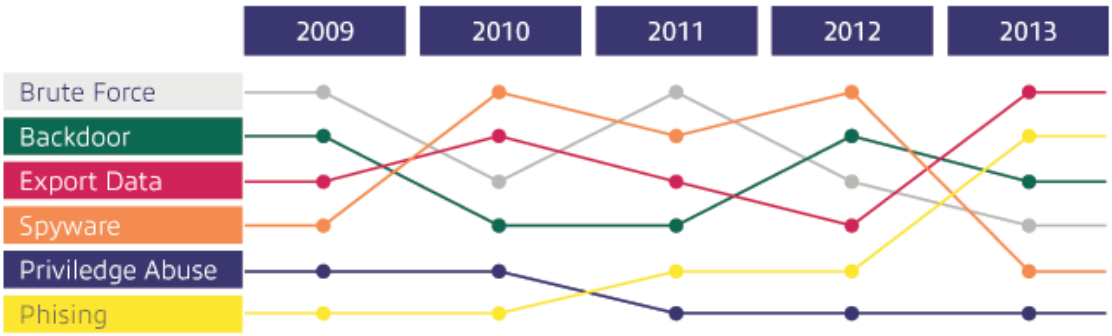
Si vous ne parvenez même pas à tenir un décompte précis de vos utilisateurs à forts privilèges, la question se pose de savoir comment vous espérez protéger ces comptes.

En sécurisant les données d'identification à chaque étape de la chaîne de frappe des violations de données.

Avant de revenir sur la chaine de frappe

Si l'on reprend les différentes analyses sur les typologies d'attaques et leurs cyclicités comme si dessous :

Valeur cyclique des cyberattaques



Source : Verizon « 2013 Data Breach Investigations Report »

2009
- Cloud computing et informatique déportée
- Open source

2010
- Smartphone
- Virtualisation
- Réseaux sociaux en entreprise

2011
- Tablettes
- Applications mobiles
- Big data
- Bases de données en mémoire

2012
- Conformité
- Consumérisation
- BYOD

2013
- Mobilité au service des métiers
- Open data
- Applications en entreprises

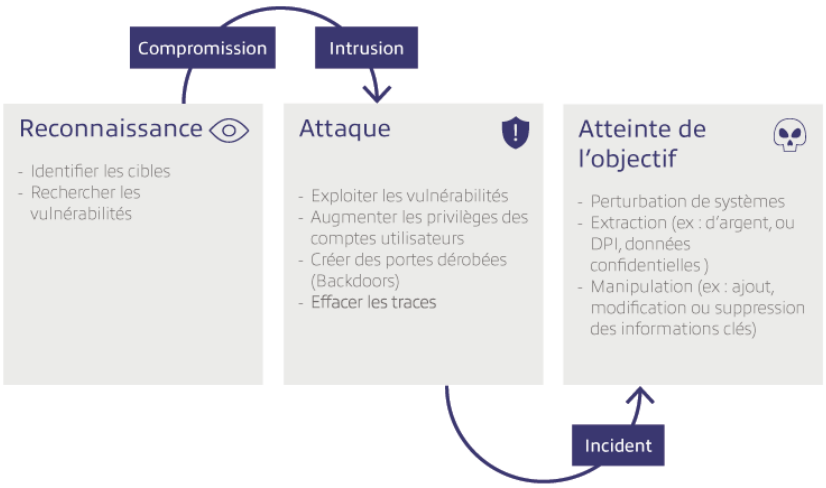
On constate que la perte de données ou d'informations sensibles est l'un des plus grands risques auxquels les entreprises doivent faire face plus qu'hier et moins que demain en fonction des évolutions technologiques. La fréquence accrue des incidents de sécurité liés à une cyberattaque et l'augmentation des coûts liés aux réparations ainsi que l'allongement du temps de la réponse sont autant de vulnérabilités supplémentaires. De plus, les entreprises ne disposent que d'une visibilité restreinte et limitée pour identifier les cibles des attaques, et déterminer où et comment les données ont pu être dérobées, ce qui ne fait qu'ajouter de la complexité au problème.

Il devient de plus en plus difficile de répondre aux incidents de manière appropriée. Il suffit de quelques minutes aux personnes malveillantes pour entrer et sortir de votre système, et laisser derrière elles des mois de travail aux équipes en charge de la sécurité pour rassembler et analyser les données.

Mais alors qu'est-ce que les cybercriminels ont de plus ? Du temps !

Maintenant revenons sur les fondamentaux : Connaître la Kill Chain (la chaine de frappe)

La chaîne de frappe (Kill Chain) est une série d'étapes qu'un pirate informatique exécute lors d'une violation de données. Bien qu'une chaîne de frappe puisse comporter de nombreuses étapes différentes, il existe trois étapes critiques pour lesquelles les données d'identification constituent la pierre angulaire de l'attaque. Les voici :



Effectuer la reconnaissance :
Pour accéder au réseau, les cybercriminels internes doivent exploiter les données d'identification qu'ils possèdent déjà, tandis que les cybercriminels extérieurs doivent exploiter une vulnérabilité du système (par ex., via une attaque par hameçonnage) afin de dérober les données d'identification nécessaires. Durant cette étape, ils ont tout le temps nécessaire pour cartographier leur cible et analyser les risques de l'entreprise.

Préparer l'attaque :
Une fois qu'une brèche du système a été identifiée et que les cybercriminels se sont introduit dans le S.I, ils tentent généralement d'augmenter leurs privilèges afin de pouvoir émettre des commandes et accéder aux ressources qui les intéressent compromettant ainsi l'entreprise sans être repérés. Ils en profitent pour effectuer une reconnaissance et se déplacer au sein du réseau afin de se rapprocher de leur objectif final et ainsi avoir une cartographie complète que les entreprises n'ont plus le temps de tenir à jour du fait du manque de temps dans le programme de transformation constant du S.I.

Atteindre l'objectif :
Une fois qu'ils ont en leur possession les données d'identification dont ils ont besoin et qu'ils ont trouvé ce qu'ils cherchaient, les cybercriminels sont libres de semer le chaos (vol, perturbation du fonctionnement de l'entreprise, etc.).

Face à ce manque de temps, Découvrez ce que vous pouvez faire à chacune de ces étapes pour gérer vos identités à forts privilèges et sécuriser votre organisation dans cette période où le temps nous est compté.

Empêcher les accès non autorisés

Pour mettre en place une authentification solide, vous devez vous assurer que les conditions suivantes sont réunies :

- Toutes les données d'identification sont intégrées à un même système de gestion des identités à forts privilèges, *ceci permettant d'avoir une politique de sécurité cohérente et centralisée.*
- Le système de gestion des identités à forts privilèges est intégré aux référentiels d'identités existants, tels que les annuaires Active Directory ou LDAP.
- Une authentification multifacteur est utilisée d'une manière ou d'une autre (par ex., jetons logiciels pour smartphone, cartes de clé physiques, etc.).
- Des restrictions de connexion sont utilisées en fonction du moment et de l'endroit où les utilisateurs requièrent un accès (par ex., adresse IP ou heure de la journée).
- Les données d'identification sont protégées dans des référentiels cryptés et renouvelées régulièrement.

Limiter l'escalade des privilèges, la reconnaissance et le mouvement latéral

Pour éviter les accès non autorisés, vous devez vous garantir les points suivants :

- Une règle « confiance zéro » oblige les utilisateurs à s'authentifier pour pouvoir accéder aux systèmes, et uniquement à ceux dont ils ont besoin pour faire leur travail.
- Des contrôles d'accès basés sur les rôles et une authentification unique (SSO) sont appliqués conjointement pour définir et présenter les autorisations aux utilisateurs au moment de leur connexion.
- Des règles sont mises en œuvre via des filtres de commande, ainsi que des listes noires et blanches, pour permettre un contrôle précis des actions que les utilisateurs sont autorisés ou non à exécuter sur un système donné.
- Toute tentative de mouvement latéral par un utilisateur, entre des systèmes non autorisés, est stoppée de manière proactive.

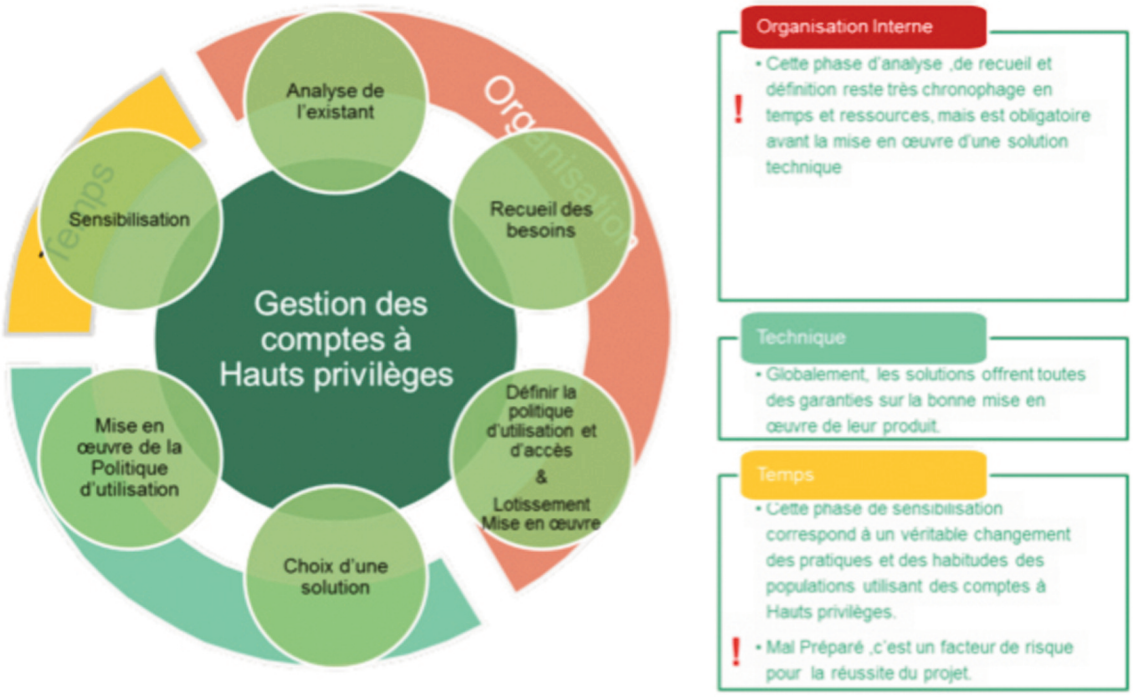
Superviser, enregistrer et auditer l'activité

Pour prévenir les violations lors de cette étape avancée de la chaîne de frappe, vous devez garantir les points suivants :

- Les sessions utilisateur sont en permanence supervisées, enregistrées et consignées, afin de pouvoir les revoir ultérieurement, comme avec un DVD.
- Toutes les données d'activité (données graphiques et texte), ainsi que les métadonnées, sont enregistrées, notamment le moment où la session a démarré et toute tentative de violation des règles en place.
- Toute activité des comptes à forts privilèges est attribuée à un utilisateur spécifique, afin d'éviter la confusion qui peut régner en cas de comptes partagés.
- Les fonctions d'analyse en place incluent la capacité à détecter de manière proactive tout comportement inapproprié, en intégrant l'activité des utilisateurs à forts privilèges aux données SIEM existantes.

Le rôle central de l'entreprise face à la révolution du Digital et aux risques de cyberattaques

Les impacts liés à une cyberattaque peuvent être considérables pour toute entreprise. Il n'existe malheureusement aucune solution miracle pour empêcher quelqu'un de vouloir s'introduire dans le système d'information et ce, en dépit des efforts de préparation et de protection qu'une entreprise peut y consacrer.
Les entreprises doivent donc modifier leur positionnement en matière d'appréciation de la sécurité, abandonner la posture défensive pour adopter une approche à la fois stratégique, proactive et pragmatique et maîtriser le temps de leur transformation.



Section 2

CA Privileged Access Management

Les violations de données constituent aujourd'hui un problème majeur, qui ne cesse de prendre de l'ampleur. Les enjeux se multiplient et nos adversaires sont de plus en plus redoutables. Les exigences de conformité réglementaire sont de plus en plus nombreuses et les organisations éprouvent de plus en plus de difficultés à y faire face et à les respecter sans mettre leurs ressources sous pression. Les procédures de sécurité et de conformité liées à la gestion et au contrôle des accès à forts privilèges se complexifient et il devient de plus en plus difficile de les gérer de façon rentable. Que faire pour relever des défis d'une telle ampleur ?

La bonne nouvelle est qu'il existe un point commun qui les unit : les utilisateurs à forts privilèges et, plus spécifiquement, les identifiants et les comptes à forts privilèges que ces utilisateurs utilisent pour la configuration, la maintenance et l'exploitation de l'infrastructure IT. Les utilisateurs à forts privilèges ne sont pas uniquement des personnes internes à l'organisation ayant une responsabilité concrète et directe dans l'administration du système et du réseau. En réalité, nombre d'utilisateurs à forts privilèges ne sont pas internes à l'organisation ; il s'agit de fournisseurs, de sous-traitants, de partenaires commerciaux ou de toute autre personne à qui des droits d'accès à forts privilégiés ont été octroyés au sein de l'organisation. Qui plus est, les utilisateurs à forts privilèges ne sont pas toujours de « vraies » personnes. Il peut également s'agir d'identifiants d'administration habituellement codés de manière irréversible dans les applications ou les fichiers de configuration.

Les organisations capables d'acquérir les fonctionnalités leur permettant d'éviter le vol et l'exploitation de leurs identifiants, de prouver l'efficacité de l'implémentation des contrôles de gestion et de supervision des accès à forts privilèges, et d'offrir un accès privilégié efficace à une infrastructure IT, sont en bonne voie pour protéger leur entreprise hybride des violations et pour respecter le nombre croissant d'exigences de conformité, mais aussi pour améliorer leur efficacité opérationnelle.

Exigences clés de la solution

Une solution efficace des accès à forts privilèges répond aux exigences suivantes :

- **Gestion des identifiants de comptes partagés :** gestion des mots de passe, garantie de l'accès et du stockage sécurisés des mots de passe des utilisateurs à forts privilèges et contrôle des accès aux comptes partagés
- **Gestion des sessions des utilisateurs à forts privilèges :** établissement de sessions à forts privilèges (au moyen d'une authentification unique), supervision et enregistrement de l'activité au cours des sessions des utilisateurs à forts privilèges
- **Gestion des mots de passe application par application :** élimination des mots de passe codés de manière irréversible utilisés par les applications, automatisation de la gestion des mots de passe des applications, et fonctionnalités d'audit de mots de passe et reporting sur les activités
- **Gestion des utilisateurs à forts privilèges :** autorisation d'un filtrage très fin des commandes et des actions exécutées par les administrateurs, les membres de confiance, les tiers et les autres utilisateurs à forts privilèges

Par ailleurs, une exigence clé que nous avons fait passer à l'avant-plan est la capacité de **sécuriser l'entreprise hybride** dans la mesure où de plus en plus d'organisations adoptent une infrastructure combinant informatique traditionnelle, virtualisation et Cloud public pour fournir rapidement et efficacement des applications métier, et ce de manière rentable. La migration des systèmes sur le Cloud ou l'exploitation de l'évolutivité et de la flexibilité du Cloud Computing pour fournir de toutes nouvelles applications peut être source de nouveaux défis. Ce Cloud hybride modifie les déploiements et les exigences en matière de gestion des accès à forts privilèges. Un plan de gestion étendu, allant au-delà des défenses traditionnelles du périmètre, nécessite une protection spécifique. Le recours accru à une responsabilité partagée en matière de sécurité exige une meilleure compréhension et utilisation de ces modèles. Les nouvelles technologies et les nouveaux modèles qui caractérisent les environnements Cloud ultraflexibles impliquent un contrôle et une protection dynamiques. Bien évidemment, la sécurisation de l'entreprise hybride passe par la protection des organisations contre les risques de sécurité et les problèmes de conformité associés aux comptes d'administration des utilisateurs à forts privilèges dans les environnements IT traditionnels, virtualisés et Cloud.

Défense approfondie de la solution de gestion des accès à forts privilèges

CA Technologies garantit une défense approfondie des comptes à forts privilèges, en proposant un large éventail de possibilités aux clients cherchant à réduire au maximum les risques liés à la sécurité et à la conformité par le biais d'une gestion des accès aux identités à forts privilèges et d'un contrôle des activités des administrateurs pour l'entreprise hybride. CA Technologies offre à cet égard :

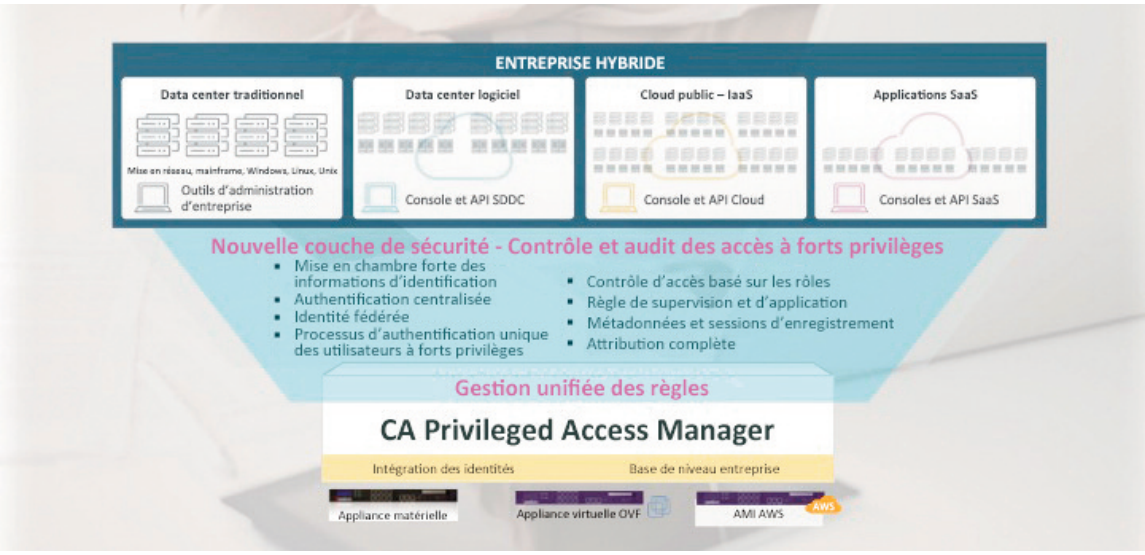
- Une gestion centralisée des accès à forts privilèges simple à déployer au moyen d'une architecture réseau, permettant une gestion des identifiants, un filtrage des commandes, ainsi qu'une supervision et un enregistrement des sessions
- Un contrôle des accès très fin et localisé au niveau de l'hôte pour renforcer la protection des ressources les plus critiques

CA IDENTITY GOVERNANCE ▪ Demandes d'accès ▪ Certification ▪ Analyses des risques	CA Privileged Access Manager	CA Privileged Access Manager Server Control
	▪ Authentification forte, y compris multifacteur ▪ Gestion des informations d'identification ▪ Contrôle d'accès basé sur des règles pour *l'attribution des privilèges les plus faibles* ▪ Filtrage des commandes ▪ Enregistrement, audit et attribution des sessions ▪ Gestion des mots de passe des applications ▪ Protection complète et hybride à l'echelle de l'entreprise ▪ Appliance indépendante renforcée	▪ Protection étendue des serveurs critiques ▪ Contrôle très précis des accès ▪ Séparation des tâches de superutilisateurs ▪ Contrôle des accès aux ressources système (fichiers, dossiers, processus et registres) ▪ Sécurisation de la délégation des tâches (sudo) ▪ Application d'une base de calcul approuvée

Composants de la solution

CA Privileged Access Manager

CA Privileged Access Manager est une solution éprouvée, automatisée et facile à déployer, qui permet une gestion des accès à forts privilèges dans les environnements physiques, virtuels et Cloud de l'organisation. Disponible sous forme d'appliance matérielle renforcée montée sur rack, d'appliance virtuelle OVF (Open Virtualization Format) ou d'instance AMI (Amazon Machine Instance), CA Privileged Access Manager renforce la sécurité en assurant la protection des identifiants administratifs sensibles, notamment les mots de passe des utilisateurs root et des administrateurs, en contrôlant l'accès des utilisateurs à forts privilèges, en appliquant les règles de sécurité de manière proactive et en supervisant et enregistrant l'activité des utilisateurs à forts privilèges sur l'ensemble des ressources IT.



Authentification des utilisateurs à forts privilèges : CA Privileged Access Manager tire pleinement parti de votre infrastructure existante de gestion des identités et des accès grâce à une intégration avec Active Directory et les annuaires compatibles LDAP et les systèmes d'authentification tels que Radius. Intégré avec des outils d'authentification avancés tels que CA Advanced Authentication et d'autres, la solution facilite une authentification renforcée ou multifacteur des utilisateurs à forts privilèges. Par ailleurs, CA Privileged Access Manager prend pleinement en charge des technologies telles que les jetons de sécurité et certificats PKI/X.509. Sa capacité à fournir un support pour les cartes PIV/CAC (Personal Identity Verification/Common Access Cards) garantit le respect des obligations HSPD-12 et OMB M-11-11 imposées par le gouvernement fédéral américain.

Gestion des identifiants : CA Privileged Access Manager protège et gère les identifiants administratifs sensibles. Stockés dans un coffre fort, les identifiants sont codés lors de leur stockage, transfert ou utilisation, limitant ainsi le risque de vol ou de divulgation. Tous les types d'identifiants, y compris les clés SSH, sont stockés dans un coffre fort et gérés, et pas uniquement les mots de passe traditionnels. CA Privileged Access Manager limite les risques associés aux mots de passe codés de manière irréversible dans des scripts et applications, offrant sa propre solution de chiffrement compatible avec la norme FIPS 140-2 de niveau 1 et intégrant les solutions FIPS de niveaux 2 et 3.

Contrôle d'accès basé sur les règles : CA Privileged Access Manager fournit un contrôle d'accès réseau basé sur les rôles très précis pour le Cloud hybride. La solution contrôle l'accès des administrateurs réseau, des membres de confiance, des tiers et d'autres utilisateurs à forts privilèges. Le contrôle commence lors de l'authentification initiale des utilisateurs à forts privilèges auprès du système, lorsque CA Privileged Access Manager implémente une approche d'exception de refus de tout accès ou d'autorisation d'un utilisateur pour les accès appliqués selon le principe du moindre privilège. Les utilisateurs sont uniquement autorisés à afficher les systèmes et méthodes d'accès pour lesquels ils ont reçu une autorisation expresse.

Filtrage des commandes : CA Privileged Access Manager fournit un contrôle d'accès réseau basé sur les rôles très précis pour le Cloud hybride. La solution contrôle l'accès des administrateurs réseau, des membres de confiance, des tiers et d'autres utilisateurs à forts privilèges. Le contrôle commence lors de l'authentification initiale des utilisateurs à forts privilèges auprès du système, lorsque CA Privileged Access Manager implémente une approche d'exception de refus de tout accès ou d'autorisation d'un utilisateur à moindres privilèges. Les utilisateurs sont uniquement autorisés à afficher les systèmes et méthodes d'accès pour lesquels ils ont reçu une autorisation expresse.

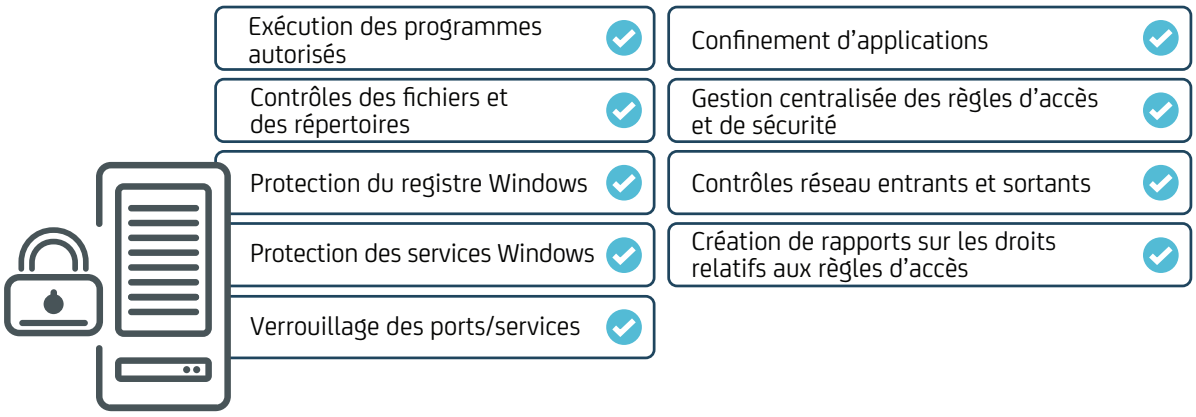
Enregistrement des sessions : CA Privileged Access Manager fournit une capture pleine résolution des sessions des utilisateurs à forts privilèges. Les contrôles de lecture de type DVD permettent aux auditeurs et investigateurs de passer en revue les événements d'une session avec la possibilité de passer directement aux tentatives de violations des règles. Les fonctionnalités d'enregistrement et de lecture sont offertes pour des sessions RDP graphiques, des liens SSH (y compris l'utilisation de clients SSH natifs), des applications Web et des consoles de gestion Cloud.

Gestion des mots de passe des applications : CA Privileged Access Manager élimine des applications et des scripts, les mots de passe codés de manière irréversible, difficiles à modifier, offrant une gestion et une protection efficaces de ces « portes du royaume ». Les mots de passe de chaque application et les autres identifiants sont stockés, dans un format codé, au sein d'une chambre forte, authentifiant les applications qui en font la demande avant que la chambre forte émette les mots de passe. Parmi les autres fonctionnalités, citons l'automatisation de la gestion des mots de passe des applications, leur chiffrement (pendant leur stockage, transfert et utilisation), le déploiement et l'intégration rapides avec l'infrastructure système et les applications, ainsi que des audits détaillés concernant les mots de passe et des rapports d'activité.

Protection de l'entreprise hybride : CA Privileged Access Manager fournit des fonctionnalités étroitement intégrées de gestion des identités à forts privilèges pour les grandes plates-formes informatiques hybrides/Cloud et les systèmes traditionnels, notamment : Amazon Web Services (AWS), VMware vSphere et NSX, les services en ligne Microsoft® et les systèmes de data center traditionnels (mainframes, serveurs, bases de données, périphériques réseau et toute autre type d'infrastructure).

CA Privileged Access Manager Server Control

Pour les organisations ayant des exigences de sécurité supplémentaires pour les serveurs hébergeant des ressources métier critiques, CA Privileged Access Manager Server Control offre une protection et un contrôle des accès très fin et localisé tant au niveau du système d'exploitation que des applications. Par ailleurs, la solution offre une protection basée sur les agents au niveau du kernel pour des fichiers, dossiers et commandes spécifiques basées sur une règle et/ou des contrôles très fins sur certains hôtes.



Protection d'un serveur critique : CA Privileged Access Manager Server Control fournit des contrôles très fins pour des serveurs critiques contenant des ressources sensibles en offrant une protection des fichiers, des répertoires et des ressources du processus système, des contrôles au niveau du kernel, une protection du registre et d'autres contrôles très fins et localisés au niveau du serveur, afin de garantir la protection des ressources précieuses hébergées sur des serveurs critiques contre les dommages causés par des actions malveillantes ou accidentelles de la part d'utilisateurs internes.

Un contrôle d'accès basé sur les hôtes : le système d'exploitation (OS) n'a souvent pas la possibilité de restreindre et de réglementer l'accès à des serveurs et applications critiques. CA Privileged Access Manager Server Control offre des contrôles d'accès très fins allant au-delà de la sécurité du système d'exploitation. La solution contrôle et supervise la façon dont les utilisateurs à forts privilèges accèdent et utilisent les données de l'entreprise et les ressources sensibles.

Séparation des fonctions pour les utilisateurs à forts privilèges : CA Privileged Access Manager Server Control aide les organisations à implémenter des principes de sécurité des accès à moindres privilèges et de séparation des fonctions en appliquant une gestion centralisée des règles de séparation des fonctions, mais aussi en supervisant les activités des utilisateurs à forts privilèges. De cette façon, la conformité avec les règlements est prise en compte et facilitée, en particulier concernant les obligations de séparation des fonctions.

Délégation sécurisée des tâches (sudo) : CA Privileged Access Manager Server Control offre de solides fonctionnalités de délégation centralisée des tâches (sudo) aidant à éliminer les risques de sécurité et les inefficacités opérationnelles associées à l'administration des fichiers des utilisateurs sudo, à fournir un audit de niveau entreprise ainsi qu'un suivi des activités des utilisateurs et à éviter l'élévation des privilèges lorsque les restrictions sudo sont inefficaces.

Section 3

Avantages de la solution

CA Privileged Access Management offre de nombreux contrôles et fonctionnalités qui agissent pour empêcher les pirates de mener à bien des étapes clés de leurs attaques et offrent une aide supplémentaire pour réduire les risques et améliorer l'efficacité opérationnelle. Ainsi, CA Privileged Access Management offre les avantages suivants :

- **Réduction des risques :** empêchez les accès non autorisés et limitez l'accès aux ressources une fois la connexion au réseau établie. Protégez les mots de passe et autres identifiants contre toute utilisation non autorisée et malveillante. Limitez les actions que les utilisateurs sont autorisés à réaliser sur les systèmes, prévenez l'exécution des commandes non autorisées et empêchez le mouvement latéral au sein du réseau.
- **Amélioration de la responsabilisation :** retracez avec précision l'activité de chaque utilisateur, même en cas de compte partagé. Capturez l'activité et mettez en place des mesures dissuasives contre les comportements indésirables par le biais de fonctions complètes de journalisation, d'enregistrement de session et d'avertissements utilisateur.
- **Amélioration des audits et facilitation de la mise en conformité :** simplifiez la mise en conformité en supportant les exigences émergentes en matière d'authentification et de contrôle d'accès. Limitez la portée des exigences de conformité par le biais d'une segmentation logique du réseau.
- **Réduction de la complexité et amélioration de la productivité des opérateurs :** l'authentification unique pour les utilisateurs à forts privilèges limite les risques, mais améliore aussi la productivité individuelle des administrateurs en leur permettant d'accéder plus rapidement et plus facilement aux systèmes et aux ressources qu'ils doivent gérer. La création et la mise en oeuvre des contrôles de sécurité sont simplifiées par la définition et l'application centralisées des règles de sécurité.

Section 5

Conclusion

Les identifiants, les comptes et les accès à forts privilèges sont des ressources critiques pour les entreprises, qui doivent être protégées à tout prix par une stratégie de défense approfondie combinant technologies et processus au moyen d'une gestion des accès à forts privilèges. Capable d'offrir plusieurs niveaux de défense autour des identifiants, des comptes et des utilisateurs à forts privilèges, aussi bien au niveau des couches réseau que des hôtes, CA Privileged Access Management vous aide à atteindre les objectifs suivants :

- Préserver la réputation d'une organisation, en évitant de nombreuses violations et en réduisant l'impact de celles qui se produisent malgré tout.
- Respecter les nombreuses exigences réglementaires d'une organisation tout en réduisant le coût de mise en conformité avec une solution globale qui s'intègre de manière transparente aux solutions existantes.
- Améliorer l'efficacité opérationnelle globale d'une organisation en offrant une automatisation et une gestion centralisée des règles ainsi que des fonctionnalités d'application de contrôles.