Développement et protection de l'entreprise ouverte

ca technologies

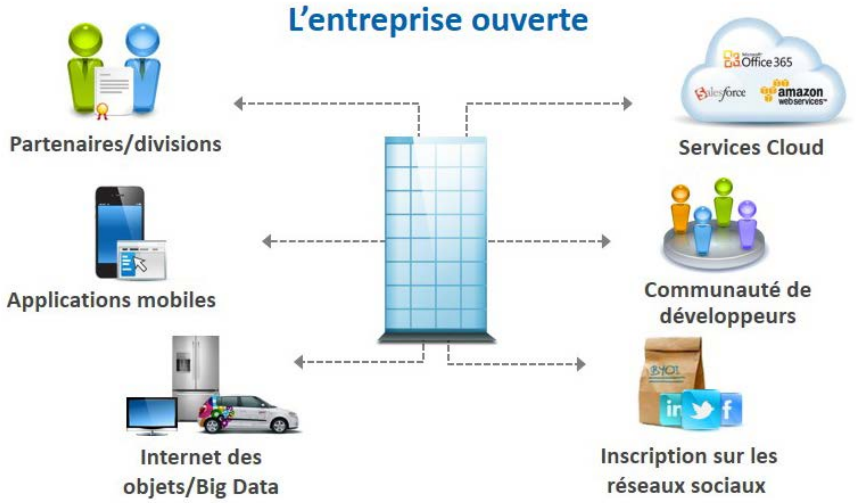
L’évolution du rôle de la sécurité

Il y a une dizaine d’années, la sécurité représentait un défi bien moindre que ce n’est le cas aujourd’hui. Les données, les applications et les utilisateurs étaient tous centralisés dans des data centers qui les maintenaient effectivement dans un périmètre réseau. Et toute personne ou tout périphérique se trouvant en dehors de ces limites pouvait être authentifié à l’aide d’un VPN (Virtual Private Network, réseau privé virtuel).

C’était le « bon vieux temps », l’époque où la sécurité était prévisible et plus facile à contrôler. Cette époque est toutefois à jamais révolue.

La consumérisation de l’informatique et l’avancée du Cloud, de la mobilité et des réseaux sociaux ont fondamentalement modifié la façon dont les organisations innovent et interagissent. Cela implique que les applications et données métier se trouvent désormais largement en dehors des frontières des pare-feu de l’entreprise. En effet, elles sont souvent distribuées hors site et sur de vastes zones géographiques. De plus, les utilisateurs peuvent accéder à ces données à l’aide de plusieurs identités et périphériques.

La notion traditionnelle de « périmètre réseau » a donc disparu. La nouvelle entreprise ouverte doit être capable de tirer parti des outils favorisant l’innovation et l’efficacité, tels que le Cloud et la mobilité. Cependant, la sécurisation de la multitude d’identités éparpillées à travers un nouvel environnement n’est pas simple.



John Hawley, Senior Director, CA Security Strategy, explique les implications de l’identité en tant que nouveau périmètre réseau.

Regardez la vidéo. Cliquez ici.

Les défis liés à la sécurisation de l'entreprise ouverte

Les « désagréments » croissants de la sécurité

La consumérisation de l'informatique. Le BYOD (« Bring Your Own Device »). L'explosion de la mobilité. Le rythme du marché. Face à toutes ces tendances, les processus de sécurité des utilisateurs finaux se sont révélés être un frein. Les processus lourds d'enregistrement et d'authentification, qui changent selon le canal utilisé (Web, mobile et API), peuvent rebuter les clients habitués à accéder rapidement aux informations. Ces derniers aspirent à des dispositifs de sécurité générant moins d'interruptions.

Les employés et les partenaires de l'entreprise attendent également un niveau semblable de convivialité. Ils souhaitent, eux aussi, des modèles de sécurité simples permettant l'application des règles à travers l'ensemble des canaux, afin de rationaliser les coûts et les délais de déploiement des applications et d'augmenter l'efficacité du processus d'accès aux données d'entreprise.

L'avènement de l'« informatique fantôme »

Bien qu'ayant amélioré l'efficacité, l'évolutivité et l'innovation des entreprises, le Cloud a également compliqué le rôle de la sécurité. Tout d'abord, des infrastructures informelles de serveurs, d'applications et de données ne cessent de faire leur apparition, dans la mesure où les employés peuvent facilement accéder à des services Cloud en ligne. Souvent, le département IT n'a même pas conscience de leur existence. La sécurisation de ces environnements d'« informatique fantôme », échappant au contrôle des équipes IT centralisées et ayant souvent leurs propres identités pour les applications basées sur le Cloud, est un défi considérable.

Le paysage des menaces constantes

Comme si les défis susmentionnés ne suffisaient pas encore à faire passer des nuits blanches aux responsables de la sécurité, de nombreux départements IT ont également beaucoup de fil à retordre afin de tenter de protéger leurs organisations face à une multitude de menaces, dont la divulgation ou la perte de données sensibles par les employés et les attaques extérieures motivées par des raisons financières. Après tout, le coût d'une violation externe réussie s'élève en moyenne à environ 5,4 millions de dollars[1], sans parler de l'impact métier persistant du préjudice à la réputation.

Une solution complète de gestion des identités et des accès (Identity and Access Management, IAM) peut vous aider à relever ces défis majeurs. Voyons comment.

[1]Ponemon Institute, 2013, « *Cost of Data Breach Study* », États-Unis.

Le nouveau rôle de la sécurité : le développement et la protection de l'entreprise ouverte

Par le passé, la sécurisation et le soutien des opérations et de la croissance de l'entreprise nécessitaient un équilibre délicat. En effet, une sécurité accrue s'accompagnait d'un ralentissement des activités. Plus vous renforciez la sécurité, plus les transactions avec vos clients étaient complexes. Inversement, une facilitation des activités reflétait une sécurité moindre. Aujourd'hui cependant, la sécurité ne doit plus être un exercice d'équilibre. L'IT *doit* favoriser la croissance des activités tout en protégeant ces dernières des risques et attaques. Cela est possible grâce aux mesures suivantes :

- Déploiement rapide de nouveaux services en ligne
- Protection des transactions des clients
- Sécurisation des accès aux ressources de l'entreprise sur l'ensemble des canaux
- Amélioration de l'expérience utilisateur

Parallèlement, le soutien de l'entreprise sera de peu d'utilité si elle reste exposée aux menaces de sécurité pouvant brutalement interrompre les activités et les revenus. L'équipe IT doit donc porter autant d'attention à la protection des systèmes et des données contre les menaces internes et les attaques extérieures.

Le développement en toute sécurité de l'entreprise ouverte : la voie à suivre

La feuille de route pour le développement et la protection de l'entreprise ouverte peut être considérée sous l'angle de trois impératifs critiques. Cliquez sur chaque impératif pour en savoir plus.

Fourniture de nouveaux services métier sécurisés >>

Sécurisation de l'entreprise mobile, connectée au Cloud >>

Protection contre les menaces internes et les attaques ciblées >>

Les meilleures solutions IAM du secteur peuvent aider les entreprises à atteindre les objectifs susmentionnés.

Le développement en toute sécurité de l'entreprise ouverte : la voie à suivre

La feuille de route pour le développement et la protection de l'entreprise ouverte peut être considérée sous l'angle de trois impératifs critiques. Cliquez sur chaque impératif pour en savoir plus.

Fourniture de nouveaux services métier sécurisés >>

Sécurisation de l'entreprise mobile, connectée au Cloud >>

Protection contre les menaces internes et les attaques ciblées >>

Fourniture de nouveaux services métier sécurisés

Afin de conserver leur avantage concurrentiel et de satisfaire aux exigences du marché, les organisations doivent adopter différentes technologies de soutien à l'innovation. Tout aussi importante est la nécessité de déployer des applications en toute sécurité, de manière transparente et au rythme du métier. Ce faisant, le département IT doit veiller à une expérience de sécurité conviviale ne requérant pas de modèles séparés sur les canaux Web et mobile.

Les meilleures solutions IAM du secteur peuvent aider les entreprises à atteindre les objectifs susmentionnés.

Le développement en toute sécurité de l'entreprise ouverte : la voie à suivre

La feuille de route pour le développement et la protection de l'entreprise ouverte peut être considérée sous l'angle de trois impératifs critiques. Cliquez sur chaque impératif pour en savoir plus.

Fourniture de nouveaux services métier sécurisés >>	**Sécurisation de l'entreprise mobile, connectée au Cloud >>**	Protection contre les menaces internes et les attaques ciblées >>

Sécurisation de l'accès à l'entreprise mobile, connectée au Cloud

L'IT doit veiller à ce que les employés, les partenaires et les clients du monde entier puissent avoir accès en toute sécurité aux ressources de l'organisation, qu'elles soient sur site ou dans le Cloud. De plus, des processus automatisés doivent être mis en place afin de garantir que chaque utilisateur dispose des droits d'accès appropriés en fonction de son type et de son rôle.

Les meilleures solutions IAM du secteur peuvent aider les entreprises à atteindre les objectifs susmentionnés.

Le développement en toute sécurité de l'entreprise ouverte : la voie à suivre

La feuille de route pour le développement et la protection de l'entreprise ouverte peut être considérée sous l'angle de trois impératifs critiques. Cliquez sur chaque impératif pour en savoir plus.

Fourniture de nouveaux services métier sécurisés >>

Sécurisation de l'entreprise mobile, connectée au Cloud >>

Protection contre les menaces internes et les attaques ciblées >>

Protection de l'entreprise contre les menaces internes et externes

Bien qu'il n'existe aucune solution miracle permettant de prévenir toutes les menaces, les organisations peuvent réduire considérablement leur exposition grâce à une compréhension de l'environnement global de menaces et à la prise de mesures proactives pour défendre l'entreprise contre les attaques. Il s'agit notamment de mettre en place des contrôles d'identité à chaque niveau de l'infrastructure afin de déployer une stratégie de « défense en profondeur ».

Les meilleures solutions IAM du secteur peuvent aider les entreprises à atteindre les objectifs susmentionnés.

Fourniture de nouveaux services métier sécurisés

Objectif : déployer rapidement et en toute sécurité des applications sur toute une gamme de modèles d'accès pour améliorer l'expérience client/utilisateur final globale tout en favorisant l'expansion et l'agilité des activités.

Initiatives IT (cliquez sur chacun des points pour en savoir plus) :

Renforcement de l'engagement des clients >>	Accélération de la fourniture de services >>	Externalisation de l'activité >>

Fourniture de nouveaux services métier sécurisés

Objectif : déployer rapidement et en toute sécurité des applications sur toute une gamme de modèles d'accès pour améliorer l'expérience client/utilisateur final globale tout en favorisant l'expansion et l'agilité des activités.

Initiatives IT (cliquez sur chacun des points pour en savoir plus) :

Renforcement de l'engagement des clients >>

Accélération de la fourniture de services >>

Externalisation de l'activité >>

Renforcement de l'engagement des clients

La fourniture d'une expérience utilisateur simple et pratique est loin de se limiter à la mise à disposition d'une interface graphique attrayante. Elle implique de pouvoir assurer une sécurité homogène sur l'ensemble des canaux d'applications, notamment Web, mobile et API, et d'éliminer le désagrément de conditions d'authentification différentes selon les applications et méthodes d'accès. Ces exigences peuvent être réalisées grâce aux éléments suivants :

- Solutions d'authentification unique (SSO) de pointe pour les applications Web et mobiles, permettant aux utilisateurs d'accéder à toutes les applications en s'identifiant une seule fois au lieu d'être invités à s'identifier séparément pour chaque application
- Fédération des identités reliant l'identité d'un utilisateur à travers plusieurs systèmes de gestion des identités
- Inscription avec les identités de réseaux sociaux, qui permet aux clients de tirer parti de leurs identités existantes provenant de sites tels que Facebook ou Google pour des interactions à faible risque (tel que la collecte d'informations)

Avantage : amélioration de l'expérience utilisateur final de sorte à contribuer à la création d'opportunités commerciales répétées et à la fidélisation des clients.

Fourniture de nouveaux services métier sécurisés

Objectif : déployer rapidement et en toute sécurité des applications sur toute une gamme de modèles d'accès pour améliorer l'expérience client/utilisateur final globale tout en favorisant l'expansion et l'agilité des activités.

Initiatives IT (cliquez sur chacun des points pour en savoir plus) :

Renforcement de l'engagement des clients >>

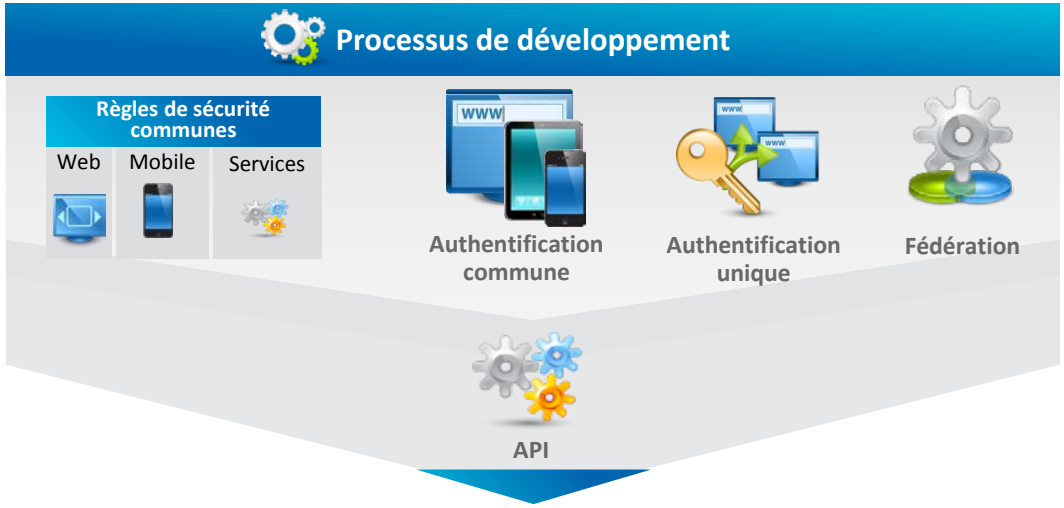
Accélération de la fourniture de services >>

Externalisation de l'activité >>

Accélération de la fourniture de services

De nos jours, la vitesse à laquelle une entreprise est en mesure de mettre à disposition des applications peut faire toute la différence en termes de réussite. Toutefois, il est tout aussi essentiel de distribuer les applications sur différents canaux et de prendre en charge de nombreuses méthodes d'accès. Une façon efficace de faciliter la réalisation de ces deux objectifs consiste à :

- centraliser les identités et les droits d'accès dans une source d'autorité unique externe aux applications elles-mêmes ;
- assurer la mise en œuvre des règles de sécurité en dehors des applications, ce qui permet d'accélérer à la fois le développement d'applications et de réduire les coûts et les risques de mise en œuvre incohérente de la sécurité ;
- implémenter une solution d'authentification forte basée sur les risques afin de fournir une authentification cohérente et adaptable sur l'ensemble des canaux.



Réduction du temps de développement

Avantage : accélération du développement d'applications tout en réduisant les coûts et en améliorant l'expérience utilisateur à l'aide de mécanismes de sécurité communs à l'ensemble des canaux.

Fourniture de nouveaux services métier sécurisés

Objectif : déployer rapidement et en toute sécurité des applications sur toute une gamme de modèles d'accès pour améliorer l'expérience client/utilisateur final globale tout en favorisant l'expansion et l'agilité des activités.

Initiatives IT (cliquez sur chacun des points pour en savoir plus) :

Renforcement de l'engagement des clients >>

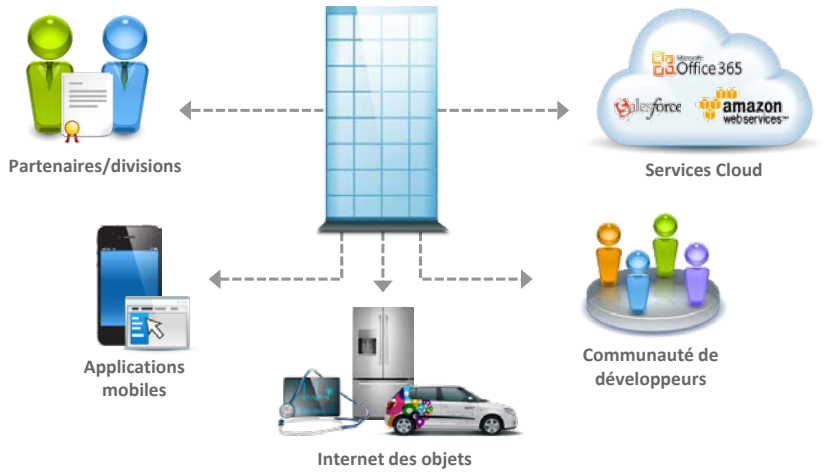
Accélération de la fourniture de services >>

Externalisation de l'activité >>

Externalisation de l'activité

L'idée est simple : rendre les données et applications accessibles à l'extérieur aux développeurs internes et tiers via des API afin de toucher davantage de canaux de distribution et de clients potentiels. Les partenaires d'une organisation peuvent ainsi développer des solutions complémentaires, afin d'accroître la richesse de l'environnement tout entier de solutions. Cela est possible à l'aide d'une solution complète de gestion et de sécurité des API qui ne se contente pas de contrôler l'accès aux API, mais permet également aux développeurs de les utiliser plus aisément afin d'accélérer le développement de ces solutions complémentaires.

Avantage : création de nouvelles opportunités commerciales par la génération en toute sécurité d'un écosystème partenaire permettant de développer des solutions complémentaires qui peuvent être distribuées via de nouveaux canaux.



Développement de nouveaux canaux par la gestion et la sécurité des API

Sécurisation de l’accès à l’entreprise mobile, connectée au Cloud

Objectif : sécuriser la collaboration métier et l’accès aux ressources IT distribuées dans toute l’entreprise pour les employés et les partenaires, tout en améliorant l’efficacité de processus clés de gestion des identités.

Initiatives IT (cliquez sur chacun des points pour en savoir plus) :

Sécurisation de l’accès aux applications >>	Rationalisation et gouvernance de l’accès utilisateur >>	Amélioration de la collaboration sûre >>

Sécurisation de l'accès à l'entreprise mobile, connectée au Cloud

Objectif : sécuriser la collaboration métier et l'accès aux ressources IT distribuées dans toute l'entreprise pour les employés et les partenaires, tout en améliorant l'efficacité de processus clés de gestion des identités.

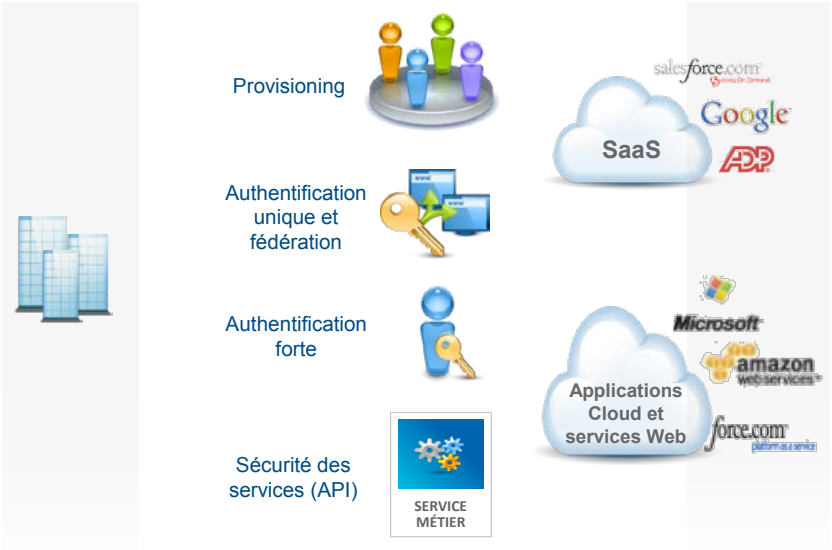
Initiatives IT (cliquez sur chacun des points pour en savoir plus) :

Sécurisation de l'accès aux applications >> | Rationalisation et gouvernance de l'accès utilisateur >> | Amélioration de la collaboration sûre >>

Sécurisation de l'accès aux applications

Que les applications soient dans le Cloud, sur site ou dans un environnement hybride, leur niveau de sécurité doit être identique. Les organisations doivent pouvoir fournir et gérer l'accès à toutes les applications et nombre d'entre elles déploient des services d'identités dans le Cloud en raison des avantages qu'ils peuvent apporter en termes d'efficacité. C'est pour cette raison qu'une solution IAM pouvant être déployée sur site ou dans le Cloud est importante. Cette flexibilité confère aux entreprises l'agilité métier accrue qu'elles requièrent pour l'adoption de services Cloud en fonction de leurs besoins.

Avantage : encouragement de l'innovation et de la collaboration métier en sécurisant les données d'entreprise.



Sécurisation de l'accès à l'entreprise mobile, connectée au Cloud

Objectif : sécuriser la collaboration métier et l'accès aux ressources IT distribuées dans toute l'entreprise pour les employés et les partenaires, tout en améliorant l'efficacité de processus clés de gestion des identités.

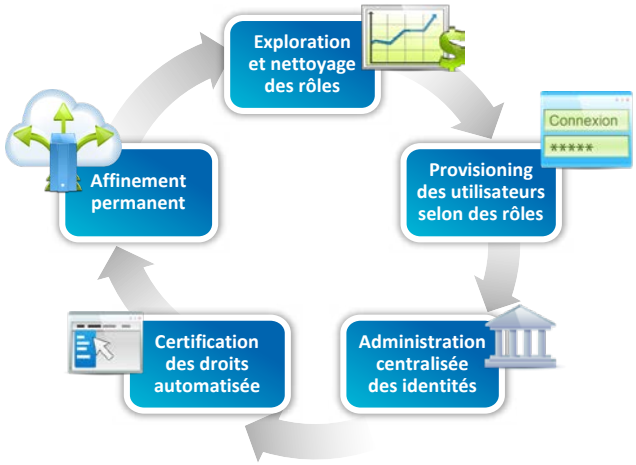
Initiatives IT (cliquez sur chacun des points pour en savoir plus) :

Sécurisation de l'accès aux applications >>	Rationalisation et gouvernance de l'accès utilisateur >>	Amélioration de la collaboration sûre >>

Rationalisation et gouvernance de l'accès utilisateur

De nombreuses entreprises recourent encore à des processus manuels pour la gestion des autorisations d'accès des utilisateurs. Une solution de gouvernance de la gestion des identités et des accès est capable d'automatiser, et donc de rationaliser, l'ensemble de ce processus. Les utilisateurs peuvent demander des droits d'accès aux applications au moyen de formulaires automatiquement soumis aux responsables. De plus, l'automatisation du processus de certification des accès peut améliorer la productivité de la gestion, réduire les coûts et simplifier les audits de conformité.

Avantage : rationalisation du processus de certification des accès des utilisateurs tout en renforçant la sécurité.



Gestion et gouvernance du cycle de vie des identités

Sécurisation de l'accès à l'entreprise mobile, connectée au Cloud

Objectif : sécuriser la collaboration métier et l'accès aux ressources IT distribuées dans toute l'entreprise pour les employés et les partenaires, tout en améliorant l'efficacité de processus clés de gestion des identités.

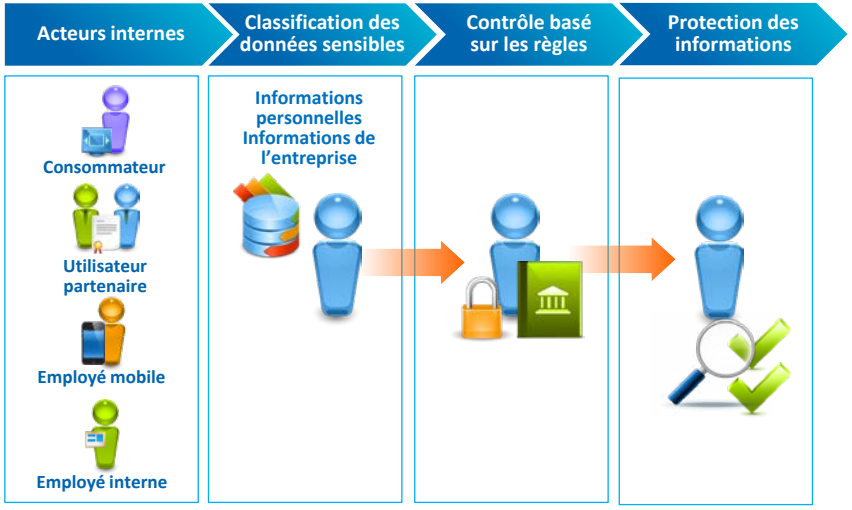
Initiatives IT (cliquez sur chacun des points pour en savoir plus) :

Sécurisation de l'accès aux applications >> | Rationalisation et gouvernance de l'accès utilisateur >> | Amélioration de la collaboration sûre >>

Amélioration de la collaboration sûre

Les employés et les partenaires doivent partager en toute sécurité des données métier de sorte à faciliter l'expansion efficace de l'activité. Ils ont dès lors besoin d'une méthode forte mais non invasive pour s'authentifier auprès des applications qu'ils partagent. De plus, il est important non seulement de contrôler l'accès aux données, mais également l'utilisation de ces dernières. Une utilisation inappropriée de données (telle que leur envoi par courriel à l'extérieur de l'entreprise) peut avoir des conséquences désastreuses. *La gestion des accès intégrant la reconnaissance du contenu* permet à une organisation de contrôler l'accès aux informations non seulement en fonction du rôle de l'utilisateur, mais également du contenu de celles-ci.

Avantage : amélioration du partage de données et de la protection contre l'utilisation abusive, le vol ou la divulgation des informations.



Protection de l'entreprise contre les menaces internes et externes

Objectif : prévenir les violations de données, même de la part d'administrateurs !

Initiatives IT :

Réduction de l'exposition aux menaces internes

Les acteurs internes responsables de vol ou de sabotage peuvent nuire considérablement à une entreprise par le biais de leur accès à des données sensibles et à l'infrastructure critique. Les administrateurs à forts privilèges représentent une menace particulièrement lourde puisqu'ils bénéficient souvent d'un accès illimité aux systèmes clés. Même des actes de pure négligence peuvent avoir des conséquences potentiellement désastreuses.

Lutte contre les attaques extérieures

Une menace persistante avancée (Advanced Persistent Threat, APT) est une offensive sophistiquée et à long terme lancée à l'encontre d'une entité spécifique. Elle cible notamment les systèmes et les données d'une multitude d'institutions. Les APT sont souvent parrainées par des États et leurs objectifs vont généralement bien au-delà du simple vol. Les auteurs sont fréquemment à la recherche de propriété intellectuelle, de renseignements stratégiques, de possibilités d'extorsion financière ou de sabotage technique ou économique.

Les organisations peuvent appliquer une approche proactive et globale de la sécurité pour prévenir tant les menaces internes que les attaques extérieures. Elles doivent pour cela faire appel à un modèle de sécurité autorisant ou non des actions en fonction de règles métier, de la sensibilité des données et de certains types de comportement. Les fonctionnalités correspondantes incluent :

- ☑ des contrôles pour la prévention de la perte de données ;
- ☑ la gestion des identités à forts privilèges.

Les affaires Edward Snowden et Bradley Manning illustrent ce qui peut arriver en cas de contrôles insuffisants des données et des utilisateurs à forts privilèges.

Avantage : prévention des violations de sécurité internes et externes par l'application de contrôles sur les utilisateurs à forts privilèges et les données.

Les solutions CA Technologies

Les solutions de sécurité informatique de CA Technologies peuvent aider les organisations à atteindre les objectifs suivants :

Fournir de nouveaux services métier sécurisés

- Déployer plus rapidement des services métier en ligne sécurisés pour une agilité accrue et la fidélisation des clients
- Renforcer l'engagement des clients en prenant en charge les identités de réseaux sociaux
- Développer de nouveaux canaux par l'externalisation des API métier

Sécuriser l'entreprise mobile, connectée au Cloud

- Adopter en toute sécurité des services Cloud
- Permettre une collaboration sûre entre employés et partenaires
- Rationaliser et gouverner l'accès utilisateur pour une efficacité accrue

Se protéger contre les menaces internes et les attaques extérieures

- Contrôler les actions des utilisateurs à forts privilèges et gérer les comptes partagés pour une réduction des risques
- Lutter contre les attaques extérieures
- Protéger les informations confidentielles relatives aux clients ou à l'entreprise contre une utilisation inappropriée, le vol et la divulgation

Suite >>

Les solutions de CA Technologies (suite)

Les solutions de sécurité informatique de CA Technologies représentent l'une des suites IAM les plus larges et les plus complètes du secteur. Nos solutions sont hautement intégrées à des fins de simplification et de réduction du coût total de la gestion de la sécurité IT. En outre, nous fournissons ces fonctionnalités sur l'ensemble des principaux environnements (Cloud/sur site, virtuels/physiques et distribués/mainframe) et modèles d'accès (Web, mobile et API) afin d'accroître de façon notable l'agilité métier.

Fonctionnalités de sécurité CA Technologies

- Gestion et gouvernance des identités
- Authentification unique sécurisée et gestion des accès
- Authentification avancée
- Gestion des identités à forts privilèges et sécurité de la virtualisation
- Gestion et sécurité des API
- Protection des données
- Services de gestion des identités dans le Cloud et sur site
- Gestion de la sécurité pour le mainframe

Avantages de sécurité CA Technologies

- Accélération de la livraison de toutes les applications, y compris celles pour les périphériques mobiles
- Sécurisation de la collaboration et du partage de données
- Protection des données contre les accès et les utilisations non autorisés
- Renforcement de la conformité grâce à un meilleur contrôle des droits d'accès des utilisateurs
- Croissance de l'activité à l'aide de nouveaux canaux pour la distribution et les partenaires
- Accroissement de l'efficacité par l'automatisation des processus de gestion des identités

Pour plus d'informations

Pour en savoir plus sur la façon dont les solutions CA Security peuvent aider les organisations à se développer et à s'épanouir en réduisant les risques, en améliorant l'efficacité opérationnelle et en renforçant l'agilité métier, visitez le site ca.com/fr/identity-and-access-management.aspx ou appelez le numéro 1-800-225-5224.

Pour des recommandations complémentaires sur le développement en toute sécurité de l'entreprise ouverte, consultez les ressources suivantes :

- Sécurité centrée sur l'identité (livre blanc)
- L'identité est le nouveau périmètre (eBook)
- Se défendre contre les menaces persistantes avancées (eBook)
- Promotion des activités en ligne en toute sécurité (livre blanc)
- The Forrester Wave: Identity and Access Management Suites (rapport d'analystes)
- Fidéliser vos clients mobiles tout en assurant la protection des données sensibles (livre blanc)

CA Technologies (NASDAQ : CA) est un éditeur de logiciels et de solutions intégrées de gestion des systèmes d'information, dont l'expertise couvre tous les environnements informatiques, du mainframe au Cloud Computing et des systèmes distribués aux infrastructures virtuelles. CA Technologies gère et sécurise les environnements informatiques et permet à ses clients de fournir des services informatiques plus flexibles. Grâce aux produits et aux services innovants de CA Technologies, les organisations informatiques disposent de la connaissance et des contrôles nécessaires pour renforcer l'agilité métier. La majorité des sociétés du classement « Fortune 500 » s'appuient sur CA Technologies pour gérer leurs écosystèmes IT en constante évolution.