



# La gestion des mots de passe pour les comptes à privilèges élevés

Bernard Levasseur, ing. CISSP  
Spécialiste en solutions de sécurité

Séminaire Bell sur les solutions de sécurité  
Le 12 novembre 2009

# Les types d'identités

*Privilèges isolés*

Utilisateur

*individuel*

*Privilèges élevés*

Administrateur

*administrateur local*

*composantes réseau*

*syst. expl. de serveurs*

*dba*

*centrale*

*Privilèges élevés*

Applicative

*reporting*

*serveurs applicatifs*

*base de données*

*tâches en lot*

*ftp*

Le **3** à **5** fois plus de comptes utilisateurs  
privilèges élevés que de comptes utilisateurs!

# Leurs caractéristiques

*Privilèges isolés*

**Utilisateur**

*individuel*

*changements réguliers*

*autoréinitialisation*

*révocable*

*memorisé*

*Privilèges élevés*

**Administrateur**

*partagé*

*changements irréguliers*

*pas d'autoréinitialisation*

*irrévocable*

*chiffrier*

*Privilèges élevés*

**Intégré**

*Partagé*

*changements irréguliers*

*pas d'autoréinitialisation*

*irrévocable*

*figé dans le code*

# Que veut-on protéger?

---

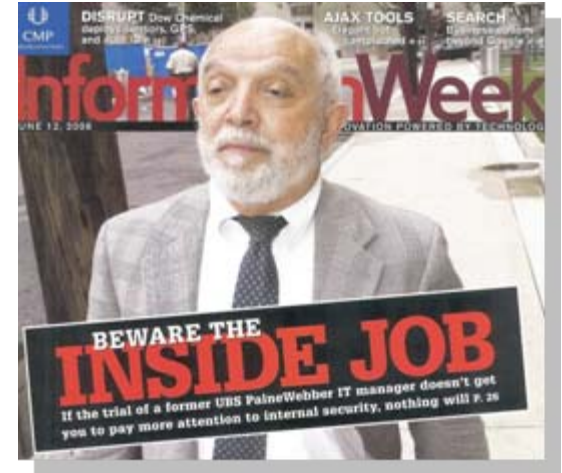
Selon Forrester, les priorités des entreprises sont :

1. Sécurité des données
2. Gestion des vulnérabilités et menaces
3. Continuité des affaires/reprise après sinistre
4. Sécurité des applications
5. Conformité
6. Alignement de la sécurité avec les besoins d'affaires
7. Appliquer les besoins en sécurité avec ceux des partenaires
8. Impartition de la sécurité

Gestion des accès privilégiés

# Protéger contre qui ? L'initié...

- Un initié déterminé :
  - connaît la valeur de vos systèmes
  - connaît l'étendu de vos défenses
  - a le temps de monter une attaque
  - n'est généralement pas considéré comme suspect
- Il/elle peut exécuter une attaque qui causera de sérieux dommages et sera détecté(e) trop tard



Ce n'est plus seulement une question d'ampleur des  
dommages  
C'est une question de survie de l'entreprise

# Qu'en disent les analystes?

---

Une composante négligée de la gestion des identités et des accès :

- **Gartner** : « *Shared-Account/Software-account Password Management (SAPM)* » ou « *Privilege Access Management (PAM)* »
- **Forrester** : « *Privileged User & Password Management (PUPM)* »
- **IDC** : « *Privileged Identity Management (PIM)* »

# Qu'en disent les analystes?

---

## Forrester

“Managing privileged users’ access to sensitive systems needs to be **centralized, policy-driven, and automated**: Manual paper- or spreadsheet-based solutions are insecure, expensive, don’t scale, and can’t be sufficiently audited.”

## IDC

“While identity and access management (**IAM**) solutions typically serve as the foundation for access control and audit, **insider threat remains a critical obstacle** within the IT enterprise. IDC believes that a significant portion of the insider threat problem can be alleviated by applying a specialized subset of IAM technologies, a privileged identity management (**PIM**) platform.”

“Most organizations have more privileged user passwords than personal passwords.”

# Qu'en disent les analystes?

---

## Burton Group

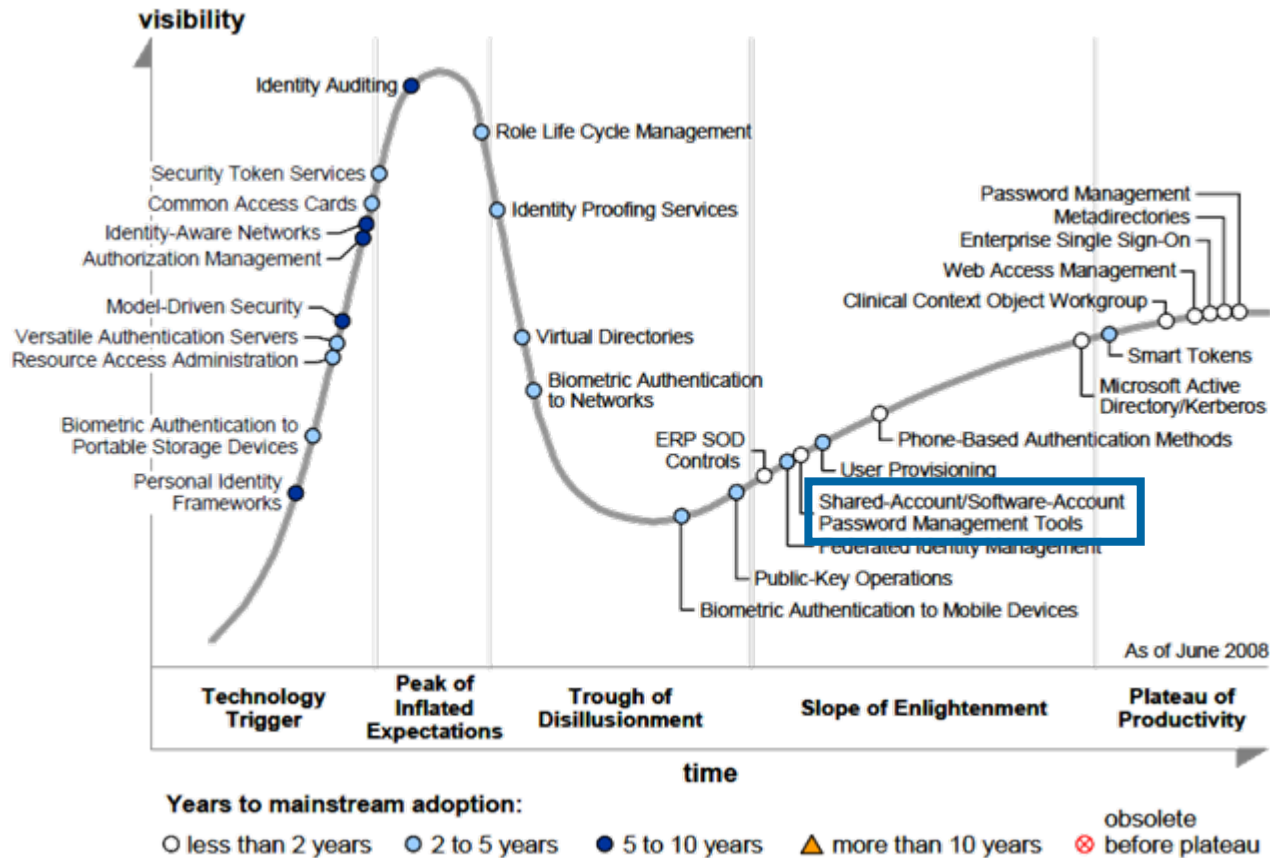
"**They're everywhere...** The problem is exponential..."

"Example: 300 hosts x 2 applications per host x 5 scripts per application = 3,000 stored passwords."

## 451 Group

"More and more organizations are recognizing the **serious potential for data breaches** and the likelihood of **compliance audit failures**, which arise from subpar access controls for sensitive resources. This recognition has in turn ***driven adoption of privileged identity management*** technologies.

# Où en sommes-nous?



# Où en sommes-nous?

benefit	years to mainstream adoption			
	less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational				
high	Metadirectories <b>Shared-Account/                      Software-Account                      Password Management                      Tools</b>	Role Life Cycle Management User Provisioning	Identity Auditing Model-Driven Security	
moderate	Clinical Context Object Workgroup Enterprise Single Sign-On ERP SOD Controls Microsoft Active Directory/Kerberos Password Management Phone-Based Authentication Methods Web Access Management	Biometric Authentication to Networks Biometric Authentication to Portable Storage Devices Common Access Cards Federated Identity Management Identity Proofing Services Public-Key Operations Resource Access Administration Security Token Services Smart Tokens Versatile Authentication Servers Virtual Directories	Authorization Management Identity-Aware Networks	
low		Biometric Authentication to Mobile Devices	Personal Identity Frameworks	

As of June 2008

# Où en sommes-nous?

---

D'après Gartner :

- L'adoption d'outils de gestion de mots de passe pour les comptes partagés et applicatifs en croissance annuelle de 50%
- En 2008 :
  - 1/2 des organisations > 5 000 utilisateurs
  - 2/3 en Amérique du nord
  - 1/5 sont des institutions financières et compagnie d'assurance

# Le défi A2A & A2DB

---

- 90% des contrôles d'accès aux bases de données dans les centres de données sont basés sur des identifiants et mots de passe
- Seulement 5% d'entre eux sont gérés (changés régulièrement)
- Raisons :
  - **Coûts** de développement pour changer les mots de passe dans les scripts et applications
  - **Indisponibilité** des systèmes dû aux changements de mots de passe et le redéploiement des scripts et applications
  - **Indisponibilité** des système dû aux erreurs dans les processus de changements de mots de passe

La gestion automatisée des mots de passe permet de restreindre l'accès aux BD et de diminuer les risques que les mots de passe soient divulgués en les changeants régulièrement

# Règles de sécurité en A2A/A2DB

---

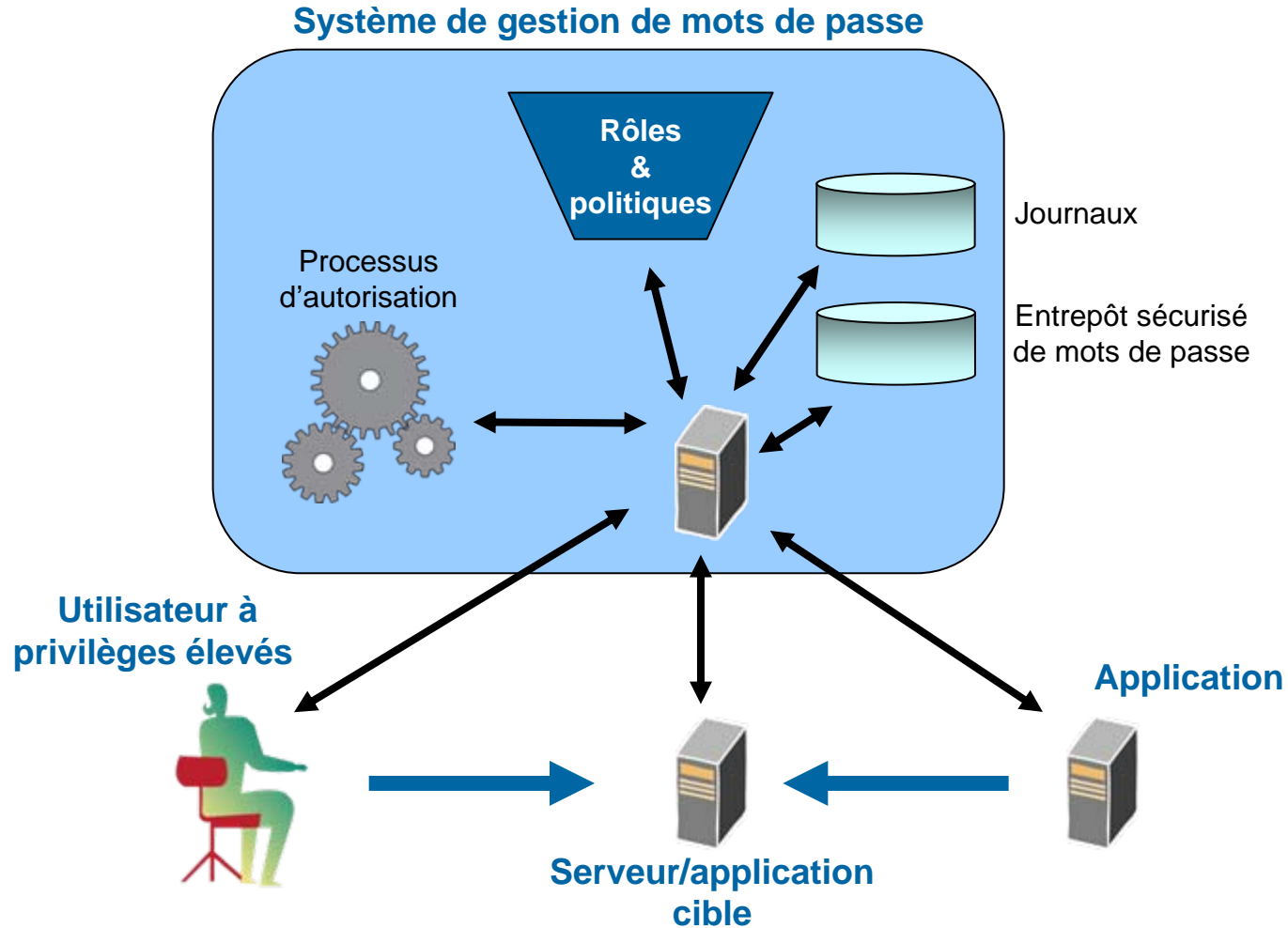
- **Changer de façon fréquente** les mots de passe des routeurs, commutateurs, systèmes d'exploitation, BD, serveurs et autres applications
- **Assurer l'intégrité du système** de changement de mots de passe, des scripts et applications qui utilisent les mots de passe
- **Se protéger contre les attaques** de réinsertion (replay attack) en utilisant des fonctions de hash et l'horodatation
- **Séparer** les mots de passe des environnements de développement et de production sans avoir à modifier les codes source

# Caractéristiques d'une solution

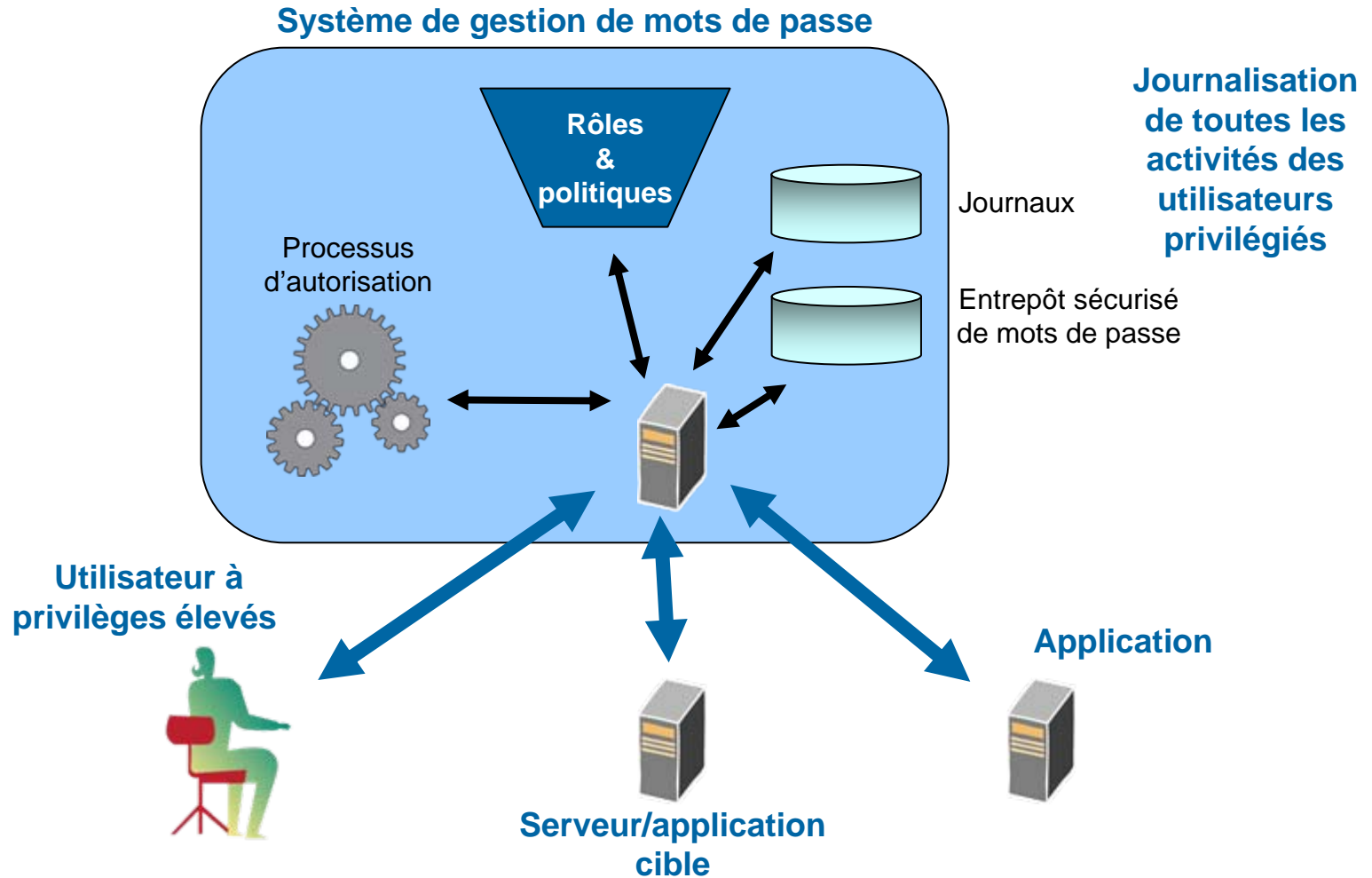
---

- **Dépôt** de mots de passe centralisé et protégé
- **Changements automatiques** des mots de passe des systèmes visés
- **Application de politiques** sur l'émission et la révocation des mots de passe (check in & check out)
- Utilisation de **processus d'approbation** pour l'émission de mots de passe
- Des **pistes d'audit** sont disponibles comme :
  - Qui a approuvé et reçu un mot de passe, quand et où?
  - Quand les mots de passe ont-ils été changés sur les applications

# Les composantes d'une solution



# Les composantes d'une solution



# Les bénéfices

---

- Amélioration de la sécurité :
  - transmission sécurisée des mots de passe à qui de droit
  - risques diminués de pertes ou divulgations non autorisées
  - mots de passe de meilleure qualité et changements fréquents
- Amélioration de l'efficacité des opérations :
  - Transmission rapide des mots de passe à tout moment (24/7, n'importe où)
  - Cohérence des accès entre administrateurs (horaires d'accès)
  - Élimination des erreurs dues aux changements manuels de mots de passe
- Réduction des coûts grâce à l'automatisation des processus
- Aide à la conformité aux lois et règlements grâce à une meilleure sécurité et protection de la vie privée, ce qui n'était pas atteignable à cause des coûts reliés aux changements de mots de passe.
- Historique sur les droits d'accès disponible en tout temps.

# Contribution à la conformité PCI

---

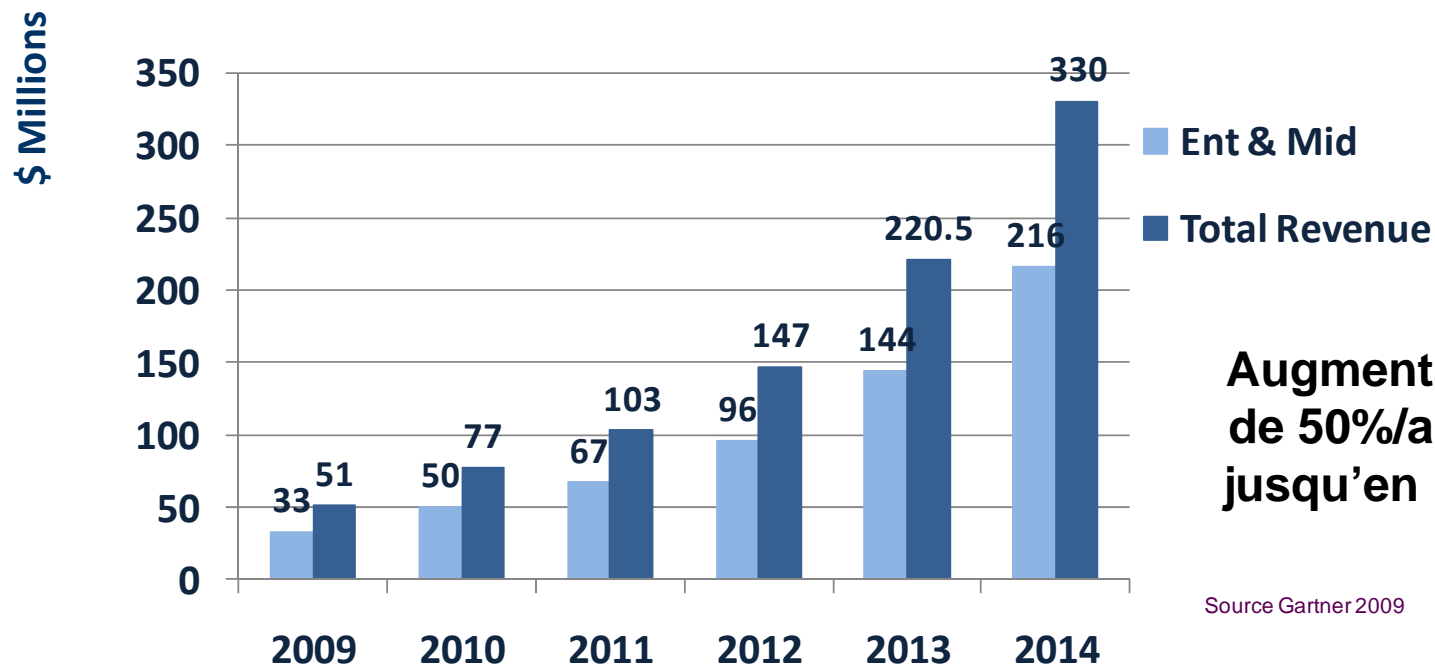
- 2 – N'utilisez pas les valeurs par défaut des fabricants pour les mots de passe et autres paramètres de sécurité
- 3 – Protégez les données des détenteurs de cartes
- 6 – Développez et maintenez des systèmes et applications sécuritaires
- 7 – Limitez l'accès aux données selon la ligne d'affaire et selon le principe de « besoin de connaître »
- 8 – Assignez un identifiant unique à chaque personne qui a accès à un système
- 10 – Surveillez tous les accès aux ressources du réseau et aux données des détenteurs de carte
- 12 – Maintenez une politique de sécurité de l'information

# Pas seulement une question de sécurité

---

- Sécurité et contrôle des risques
- Conformité
- Performance et évolutivité
- Haute disponibilité
- Facilité de gestion
- Support à l'intégration
- Audit et reporting

# Croissance de la demande pour 2009 - 2014



**Augmentation  
de 50%/année  
jusqu'en 2014**

Source Gartner 2009

# Conclusion

---

Selon Gartner, les organisations devraient :

- Limiter le nombres de comptes partagés
- Ne pas permettre le partage de mots de passe
- Établir des processus et contrôles en ligne avec leur politique de sécurité
- Ne pas se fier à des processus manuels pour de grands déploiements
- Mettre en place un système de gestion des mots de passe pour automatiser les processus, appliquer les contrôles et fournir une piste d'audit sur les activités individuelles
- Utiliser un système de gestion des événements de sécurité (SIEM) pour surveiller, corréler et analyser les activités sur les tous les comptes partagés
- Mettre en place un système de gestion des mots de passe pour le A2A et A2DB

**Merci!**