AYI NEDJIMI Consultants

PAM : guide complet de gestion des accès à privilèges

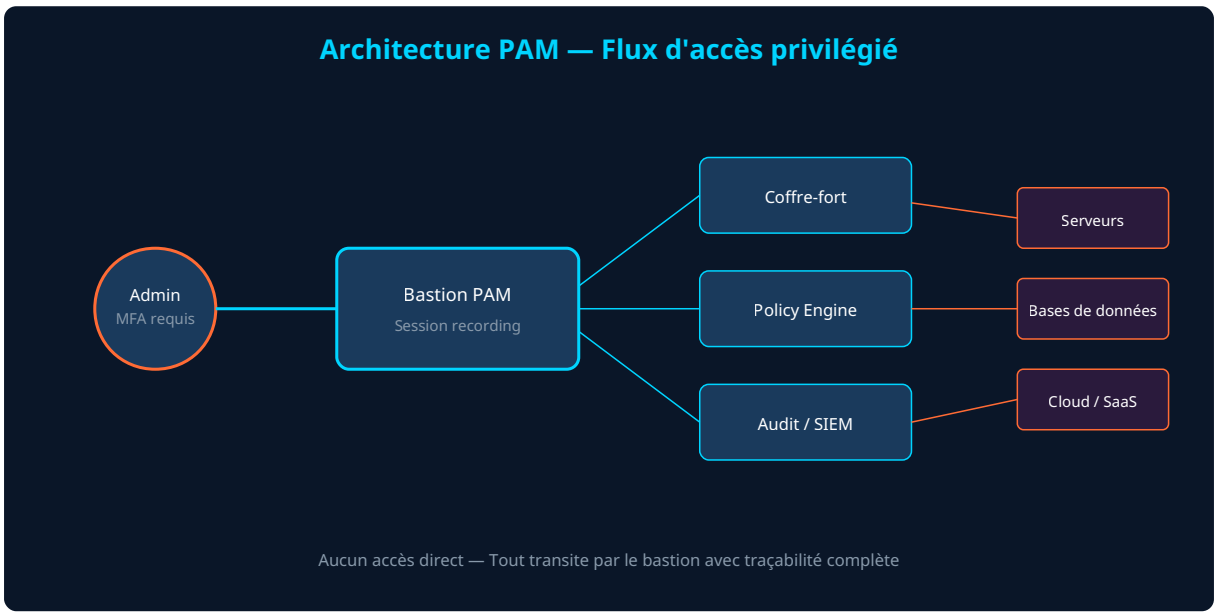
Catégorie : IAM et Gestion des Identités Lecture : 6 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide complet PAM : architecture, déploiement et bonnes pratiques pour sécuriser les accès à privilèges en entreprise avec CyberArk, Delinea et.

Les comptes à privilèges représentent la cible numéro un des attaquants. Un seul compte administrateur compromis peut donner accès à l'intégralité du système d'information en quelques heures. Le Privileged Access Management, ou PAM, désigne l'ensemble des processus et technologies permettant de contrôler, surveiller et auditer ces accès critiques. Que vous soyez RSSI, architecte sécurité ou ingénieur IAM, ce guide vous fournit une méthodologie complète pour déployer une solution PAM adaptée à votre contexte. Nous couvrirons l'inventaire des comptes privilégiés, le choix de la solution technique, l'architecture de déploiement, les cas d'usage métier et les pièges à éviter. Parce que trop de projets PAM échouent non pas par manque de technologie, mais par manque de méthode. L'approche présentée ici repose sur des retours d'expérience concrets, issus de déploiements dans des organisations de 500 à 50 000 utilisateurs, tous secteurs confondus. Vous y trouverez des recommandations directement applicables à votre environnement.

Points clés à retenir

- 80% des brèches impliquent des **comptes à privilèges** compromis (source : Verizon DBIR 2025)
- Un projet PAM réussi commence par un inventaire exhaustif des comptes privilégiés
- Les trois fonctions PAM fondamentales : **coffre-fort de mots de passe**, **enregistrement de sessions** et **élévation de privilèges**
- Le déploiement se fait par cercles concentriques : comptes domaine, puis serveurs, puis applications
- Le ROI moyen d'un projet PAM se situe entre 150% et 300% sur 3 ans



Inventaire des comptes à privilèges : le point de départ

Avant de déployer quoi que ce soit, vous devez savoir ce que vous protégez. L'inventaire des comptes privilégiés est la première étape de tout projet PAM. Et c'est souvent là que les surprises arrivent. Dans une organisation type de 2000 employés, on découvre généralement entre 3 et 5 fois plus de comptes privilégiés qu'estimé initialement. Les comptes d'administration Active Directory ne sont que la partie visible de l'iceberg.

Catégorisez vos comptes en quatre familles : les comptes d'administration système (Domain Admins, root, administrateurs locaux), les comptes de service applicatifs, les comptes d'accès aux bases de données et les comptes d'administration cloud (AWS IAM, Azure RBAC, GCP IAM). Pour chaque catégorie, documentez le propriétaire, la fréquence d'utilisation, le niveau de criticité et les dépendances applicatives. Des outils comme **BloodHound** pour l'AD ou **Prowler** pour AWS accélèrent considérablement cette phase.

Les trois piliers fonctionnels du PAM

Une solution PAM complète repose sur trois fonctions complémentaires. Le *coffre-fort de mots de passe* (password vault) stocke, gère et fait tourner automatiquement les credentials des comptes privilégiés. Plus personne ne connaît le mot de passe root du serveur de production — c'est le coffre qui l'injecte à la demande. La *gestion des sessions privilégiées* (session management) enregistre et surveille en temps réel toutes les sessions administratives. Chaque commande tapée, chaque écran affiché est capturé pour l'audit et la détection d'anomalies.

Le troisième pilier, l'*élévation de privilèges contrôlée* (privilege elevation), permet aux utilisateurs d'exécuter des tâches spécifiques avec des droits élevés sans disposer d'un compte admin permanent. C'est le principe du moindre privilège appliqué dans sa forme la plus concrète. Pensez-y comme un sudo intelligent avec approbation workflow et traçabilité.

Comparatif des solutions PAM du marché

Le marché PAM est dominé par trois acteurs majeurs, chacun avec ses forces et ses zones d'ombre. **CyberArk** reste le leader historique avec la couverture fonctionnelle la plus large, mais son coût et sa complexité de déploiement le destinent aux grandes organisations (budget : 150 à 500 k€/an). **BeyondTrust** offre un excellent rapport fonctionnalités/ergonomie avec une approche modulaire qui permet de démarrer petit et de monter en puissance. **Delinea** (ex-Thycotic + Centrify) se distingue par sa facilité d'intégration cloud-native et ses prix compétitifs pour le mid-market.

Critère	CyberArk	BeyondTrust	Delinea
Password Vault	Excellent	Très bon	Très bon
Session Recording	Excellent	Très bon	Bon
Privilege Elevation	Très bon	Excellent (EPM)	Bon
Cloud-native	En progression	Bon	Excellent
Complexité déploiement	Élevée	Moyenne	Faible
Budget annuel (1000 users)	200-500 k€	100-300 k€	80-200 k€

Architecture de déploiement recommandée

L'architecture de référence PAM suit un modèle en couches. La couche frontale expose le portail web et les connecteurs de session (RDP, SSH, HTTPS). La couche applicative héberge le moteur de politiques, le workflow d'approbation et l'API. La couche données stocke le coffre-fort chiffré (AES-256) et les enregistrements de session. En environnement hybride, un composant de gestion des secrets cloud s'ajoute pour couvrir les credentials AWS, Azure et GCP.

La haute disponibilité exige a minima deux nœuds actifs avec réplication synchrone du coffre-fort. Le disaster recovery repose sur des sauvegardes chiffrées hors site avec un RPO de 4 heures maximum. Prévoyez une zone réseau dédiée (VLAN d'administration) avec des règles de pare-feu strictes : seul le bastion PAM communique avec les cibles, jamais les postes de travail directement.

Déploiement par cercles concentriques

Le déploiement PAM suit une logique de cercles concentriques, du plus critique au plus large. Le premier cercle couvre les comptes **Domain Admins** et les accès root aux serveurs de production. C'est le quick win à plus fort impact sécuritaire. Le deuxième cercle étend la couverture aux comptes de service applicatifs et aux chemins d'attaque identifiés par BloodHound. Le troisième cercle intègre les accès aux bases de données, aux équipements réseau et aux consoles cloud.

Chaque cercle suit un cycle de quatre semaines : onboarding des comptes (semaine 1-2), configuration des politiques de rotation et d'approbation (semaine 3), activation du monitoring et ajustement (semaine 4). La clé du succès : ne jamais passer au cercle suivant tant que le précédent n'est pas stabilisé. Un retour d'expérience CyberArk montre que 70% des projets PAM qui échouent ont tenté de couvrir trop de périmètre trop vite.

Cas d'usage métier et ROI mesurable

Le PAM n'est pas qu'un projet technique — c'est un enabler business. Premier cas d'usage : la conformité réglementaire. Les recommandations ANSSI pour l'administration sécurisée des SI imposent la traçabilité des accès privilégiés. Le PAM automatise cette conformité et réduit le temps d'audit de 60%. Deuxième cas : la réduction du risque opérationnel. La rotation automatique des mots de passe élimine le risque de credentials statiques partagés entre équipes. Troisième cas : l'accélération du DevOps sécurisé en intégrant le coffre-fort PAM dans les pipelines CI/CD via API.

Le ROI se calcule sur trois axes : réduction des incidents (un incident PAM évité vaut entre 50 et 200 k€), gain de productivité des équipes IT (30 minutes/jour/admin en gestion de credentials) et conformité (évitement de pénalités réglementaires). Sur un périmètre de 1000 utilisateurs, le business case pour le COMEX démontre un retour sur investissement entre 150 et 300% sur 3 ans.

Questions fréquentes sur le PAM en entreprise

Quelle différence entre PAM et IAM ?

L'IAM (Identity and Access Management) gère l'ensemble des identités et des accès de l'organisation : provisioning, SSO, MFA, gouvernance des accès. Le PAM est un sous-ensemble de l'IAM spécialisé dans la gestion des comptes à privilèges élevés. Pensez à l'IAM comme le cadre global et au PAM comme la sécurité renforcée pour les accès les plus critiques. Les deux sont complémentaires et s'intègrent via des connecteurs natifs.

Comment gérer la résistance des équipes techniques au PAM ?

La résistance au PAM est le premier facteur d'échec des projets. Trois leviers fonctionnent : impliquer les admins dans le choix de la solution (ils préfèrent tester eux-mêmes), garantir que le PAM ne ralentit pas leur workflow quotidien (SSO vers le bastion, copier-coller activé pour les cas légitimes), et démontrer la valeur ajoutée (plus besoin de mémoriser 47 mots de passe différents). La communication doit être transparente sur le monitoring sans tomber dans la surveillance punitive.

Faut-il déployer le PAM on-premise ou en SaaS ?

Le choix dépend de votre architecture et de vos contraintes réglementaires. Le SaaS (Delinea Secret Server Cloud, CyberArk Privilege Cloud) offre un déploiement rapide et une maintenance réduite. L'on-premise garde le contrôle total sur les données et convient aux environnements réglementés (défense, santé, finance). L'approche hybride, avec un vault on-premise synchronisé avec un connecteur cloud, est le compromis le plus fréquent en 2026.

Sources et références : ANSSI · MITRE ATT&CK

Synthèse et prochaines étapes

Le PAM est un projet structurant qui transforme la posture de sécurité de votre organisation. Commencez par l'inventaire, choisissez une solution adaptée à votre maturité et votre budget, déployez par cercles concentriques et mesurez le ROI à chaque étape. Les organisations qui réussissent leur projet PAM partagent un point commun : elles traitent le PAM comme un programme continu, pas comme un projet ponctuel. La gestion des accès privilégiés évolue avec votre SI — votre solution PAM doit suivre le rythme.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr