HAFS
Distributeur à valeur ajoutée

VOTRE PARTENAIRE TECHNOLOGIQUE

POUR DES INFRASTRUCTURES IT SÉCURISÉES ET PERFORMANTES

EXPERTISE
Des solutions adaptées à chaque environnement

CONFIANCE
Un partenaire fiable à vos côtés

PERFORMANCE
Des infrastructures sécurisées et évolutives

SUPPORT
Un accompagnement technique de qualité

HAFS
Distributeur à valeur ajoutée

Des solutions IT innovantes pour un monde connecté et sécurisé

WIRELESS RADIO
Connectivité sans fil haute performance

RÉSEAUX & SÉCURITÉ IT
Des réseaux fiables et sécurisés

VIRTUALISATION CLOUD
Des solutions Cloud flexibles et évolutives

CYBERSECURITY
Protéger vos données et vos systèmes

VIDÉO PROTECTION
Solutions de vidéosurveillance intelligentes

HCI STOCKAGE SAUVEGARDE
Stockage, sauvegarde et haute disponibilité

SOLUTIONS IT | CYBERSÉCURITÉ | CLOUD | INFRASTRUCTURE RÉSEAU | STOCKAGE | PROTECTION

Axidian

Faites du PAM une preuve de conformité

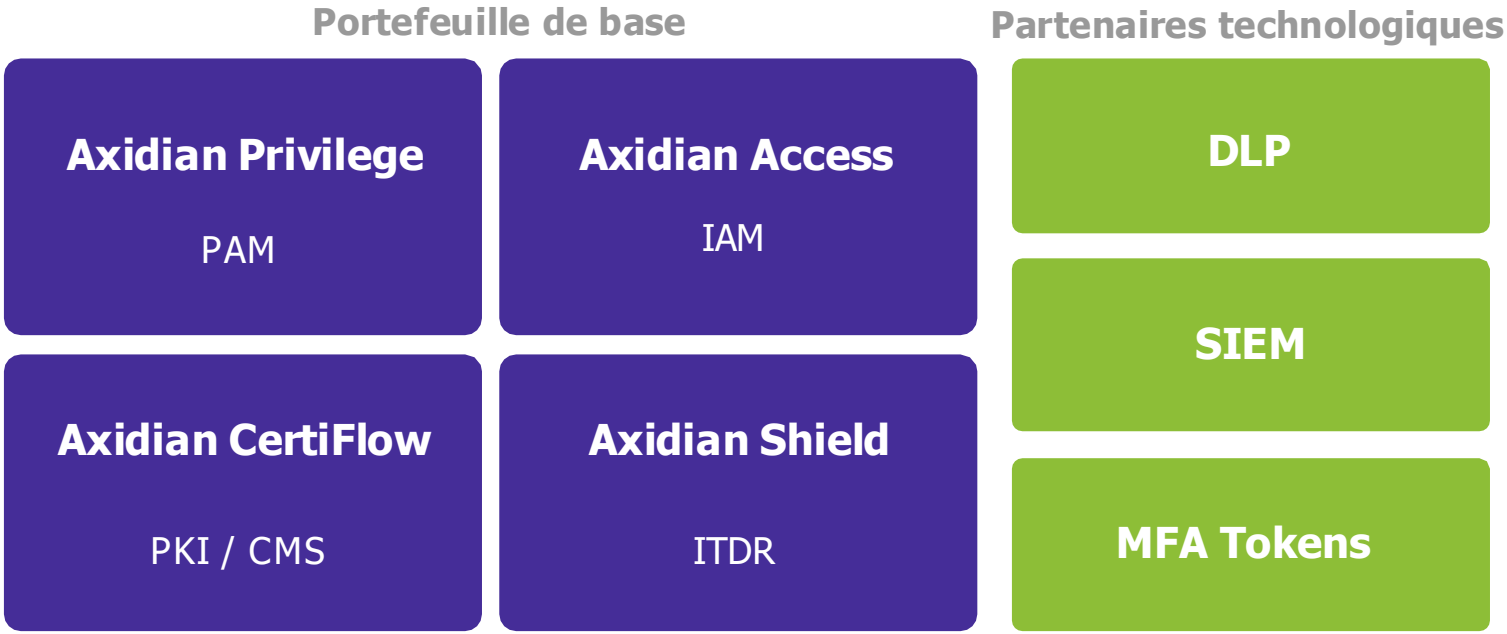
ISO 27001 / PCI DSS

Mouadh CHAÂBANI

Senior Pre-sale Engineer
at Axidian

Axidian

Couverture complète en matière de sécurité de l'identité



Axidian

Pourquoi Axidian

Portefeuille complète de sécurité d'identité

PoCs pour les clients, Formation pour les partenaires

Accessible à tous, des PME aux grandes entreprises

Facile à vendre – licences et tarifs flexibles

Soutien commercial et marketing axé sur la région

Assistance 24h/7, sans distinction de niveaux

La conformité prend trop de temps

Réglementations locales

DNSSI Maroc RGSI

Côte d'ivoire RNSI

Algérie

BCEAO : Banque Centrale des Etats de l'Afrique de l'Ouest

Normes internationales

PCI DSS

ISO/IEC 27001:2022

NIST SP 800-53

RGPD

HIPAA

Axidian

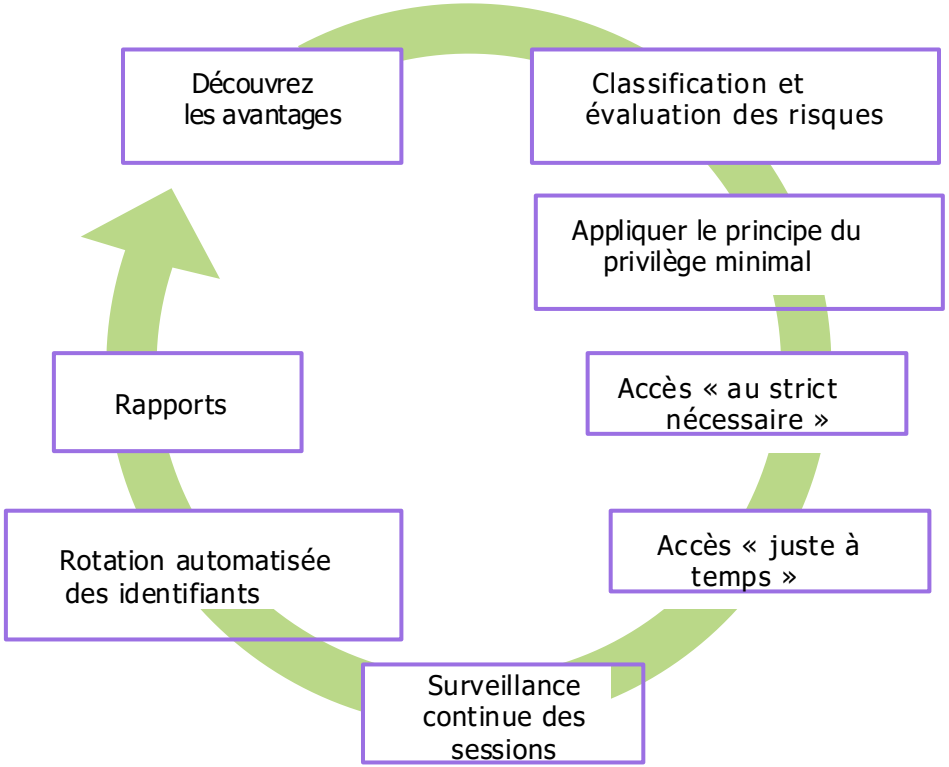
Axidian Privilege

Gestion des accès privilégiés

La gestion des accès privilégiés (PAM) protège les ressources critiques en contrôlant les accès privilégiés, en surveillant l'activité des utilisateurs et en prévenant les risques de sécurité.

Axidian

Simplifiez les audits



Contrôle > Enregistrement > Vérification

- Mettez en place les contrôles nécessaires
- Conservez un historique unique et consultable des activités
- Générez des rapports pour les auditeurs
- Démontrez rapidement qui a accédé à quoi, quand et pourquoi

Transformez les contrôles manuels fragmentés en un accès privilégié traçable pour les rapports.

Norme PCI DSS 4.0

s'applique à toute organisation qui stocke, traite ou transmet des données de cartes de paiement

6 objectifs

1. Construire et maintenir un réseau et des systèmes sécurisés
2. Protéger les données de comptes
3. Maintenir un programme de gestion des vulnérabilités
4. **Mettre en œuvre des mesures de contrôle d'accès strictes** ✓
5 Surveiller et tester régulièrement les réseaux
6. Maintenir une politique de sécurité de l'information

12 exigences majeurs

300 exigences detailées

À partir de 2025

Obligatoire en Afrique d'Ouest pour:

- Banques émettrices et acquéreuses
- Fintechs et établissements de monnaie électronique
- Établissements de paiement et processeurs
- Prestataires de services ayant accès aux données de cartes

Axidian

Conséquences de la non-conformité aux normes PCI DSS

- Atteinte à la réputation et perte de confiance
- Restrictions sur les paiements
- License revocation or refusal to renew
- Sanctions financières
- Cessation d'activité de l'entreprise

Axidian

Soyez en conformité avec PCI DSS avec Axidian

Objective 4 - Mettre en œuvre des mesures de contrôle d'accès strictes

Axidian PAM

Requirement 7: Restrict Access To Cardholder Data By Business Need To Know

1. Processes and mechanisms for restricting access are defined and understood.
2. Access is appropriately defined and assigned.
3. Access is managed via an access control systems.

Requirement 10:
Logging and monitoring

Axidian PAM + Axidian Access MFA/SSO

Requirement 8: Identify Users and Authenticate Access to System Components

1. User identification and authentication processes are defined.
2. User and admin accounts are managed throughout their lifecycle.
3. Strong authentication is enforced for users and admins.
4. MFA is required for CDE access.
5. MFA is configured to prevent misuse.
6. Application and system accounts and authentication factors are managed.

Coverage of controls

Axidian

Exigence 7: Restrict Access To Cardholder Data By Business Need To Know

7.2.2
Access is assigned to privileged users, based on
- *Job function.*
- *Least privileges for job responsibilities.*

7.2.3
Required privileges are approved by authorized personnel.

Axidian Privilege (PAM)

- N’accordez aux utilisateurs que les accès privilégiés nécessaires à leur rôle et à leurs responsabilités.

- Mettez en place un processus d’approbation exigeant une justification de connexion pour chaque ressource critique.

Axidian

Exigence 7.2.5.1: Review of Privileged Accounts

7.2.5.1
All access by application and system accounts and related access privileges are reviewed:
- *Periodically,*
- *The application/system access is appropriate for the function*
- *Inappropriate access is addressed.*

Axidian Privilege (PAM)

Axidian Privilege intègre **la découverte de comptes** : des recherches régulières de nouveaux comptes sont effectuées sur l'ensemble des ressources et domaines connectés.

Personnalisez la fréquence de recherche et spécifiez-la pour des groupes de ressources spécifiques.

Axidian

Exigence 8: Identify Users and Authenticate Access to System Components

> ***8.4*** *MFA is required for CDE access.*
>
> ***8.5*** *MFA is configured to prevent misuse.*

Axidian Privilege (PAM)

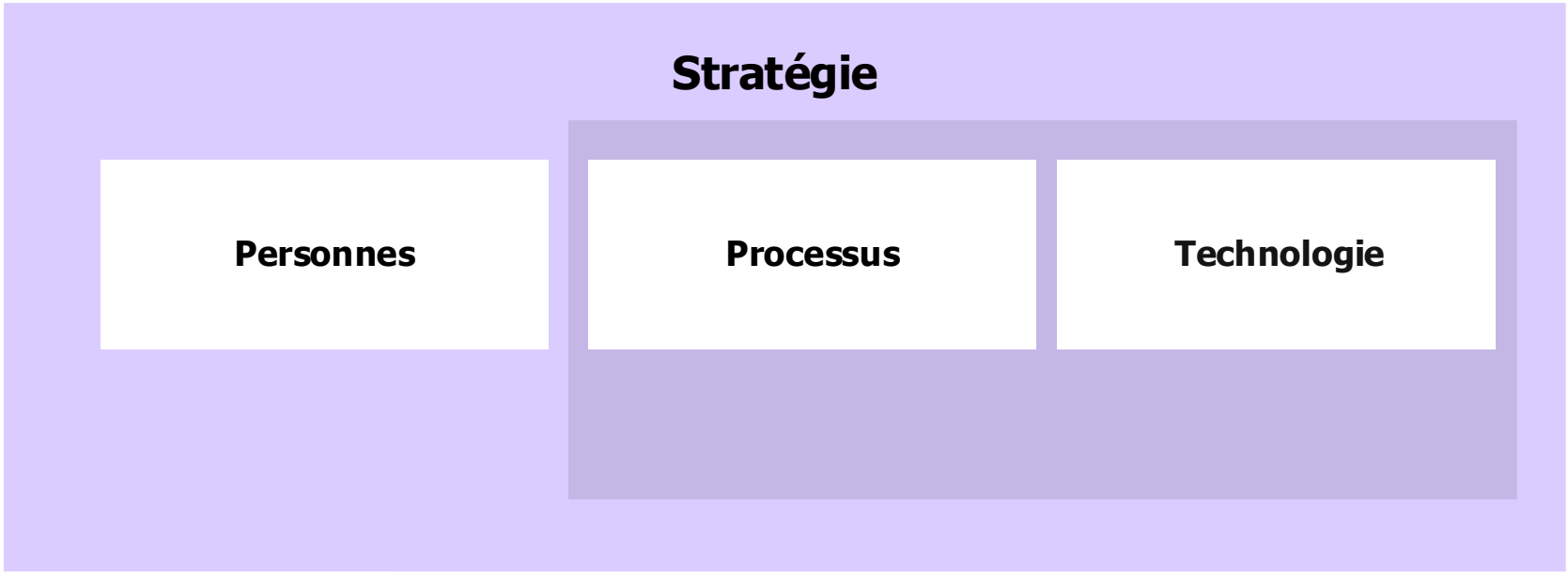
- MFA/SSO intégrée pour l'accès local et distant des utilisateurs privilégiés.

Axidian Access (IAM)

- Mettez en œuvre l'authentification multifacteur (MFA) pour l'accès local et distant à tous les environnements de données partagés (CDE) des SI
- Sécurisez l'accès en ligne et hors ligne.

Axidian

Comment aborder ISO 27001:



Axidian

ISO 27001: 4 domaines et 93 controls

PAM n'est plus un “nice-to-have”, mais un “must-have”.

- Axidian PAM couvre intégralement 4 contrôles et prend partiellement en charge 44 contrôles.
- PAM et MFA font partie des exigences réglementaires obligatoires dans certains secteurs.

A5. Organizational controls **37**	**A6. People controls** **8**
A7. Physical controls **14**	**A8. Technological controls** **34**

Comment Axidian PAM aide à être en conformité avec ISO 27001:

Full coverage of controls

A.8.2 Privileged access rights
A.8.3 Information access restriction
A.8.15 Logging
A.8.18 Use of privileged utility programs

Partial coverage of controls**

A5.2 IS roles and responsibilities
14. Information transfer
15. Access control
16. Identity management
17. Authentication information
18. Access rights

A.6.8 Information security event reporting
A.8.5 Secure authentication
A.8.16 Monitoring activities

To have is fully covered by Axidian
+it's necessary to have additional solutions

Axidian

ISO 27001 Privileged Access Management Controls

A.8.2 Privileged access rights

A.8.18 Use of privileged utility programs

A 5.19 Information security in supplier relations

Axidian Privilege (PAM)

- Appliquez le principe du moindre privilège : accordez l'accès selon les principes du « besoin d'en connaître » et du « besoin d'utiliser ».
- Accordez un accès juste-à-temps (JAT) uniquement aux ressources nécessaires.
- Contrôlez les sessions et surveillez les transferts de fichiers afin de protéger les informations critiques lors de leur accès par les adminis et les sous-traitants externes.

Axidian

ISO 27001 Identify and Access Management Controls

A5.2 IS roles and responsibilities
A.5.3 Segregation of duties

A.5.3 Access control
A.5.16 Identity management

A 5.18 Access rights

Axidian Privilege (PAM)

- Mettez en œuvre le modèle RBAC avec des rôles personnalisés (ex. : Administrateur, Superviseur, Sous-traitant) et atténuez les conflits de tâches.
- Définissez les autorisations nécessaires uniquement à l'exécution des tâches requises.

Axidian

ISO 27001 Logging and Monitoring controls

A.8.15 - Logging

A.8.16 Monitoring activities

A6.8 Reporting information security events

A5.28 Collecting evidence

Axidian Privilege (PAM)

- Surveillez et enregistrez toutes les activités d'accès privilégié, avec une visibilité complète (qui, quoi, quand, pourquoi).
- Contrôlez les activités privilégiées et enregistrez les sessions (vidéo, captures d'écran, journaux text).
- Générez et téléchargez des rapports personnalisables.

Axidian

Axidian

Obtenez des réponses rapidement…

Qui a accédé à quoi et quand ?
Sur quels systèmes ?
Quelles commandes ont été exécutées ?

…en utilisant…

- Enregistrement vidéo de la session
- (Visionnage en temps réel ou en replay)
- Captures d'écran
- Journaux d'événements
- Copies fantômes des fichiers transférés
- Métadonnées utilisateur

… et répondez

(PAM +SIEM +SOAR)

- Détectez les connexions anormales
- Fermez la session si nécessaire
- Renouvelez automatiquement les identifiants
- Verrouillez le compte

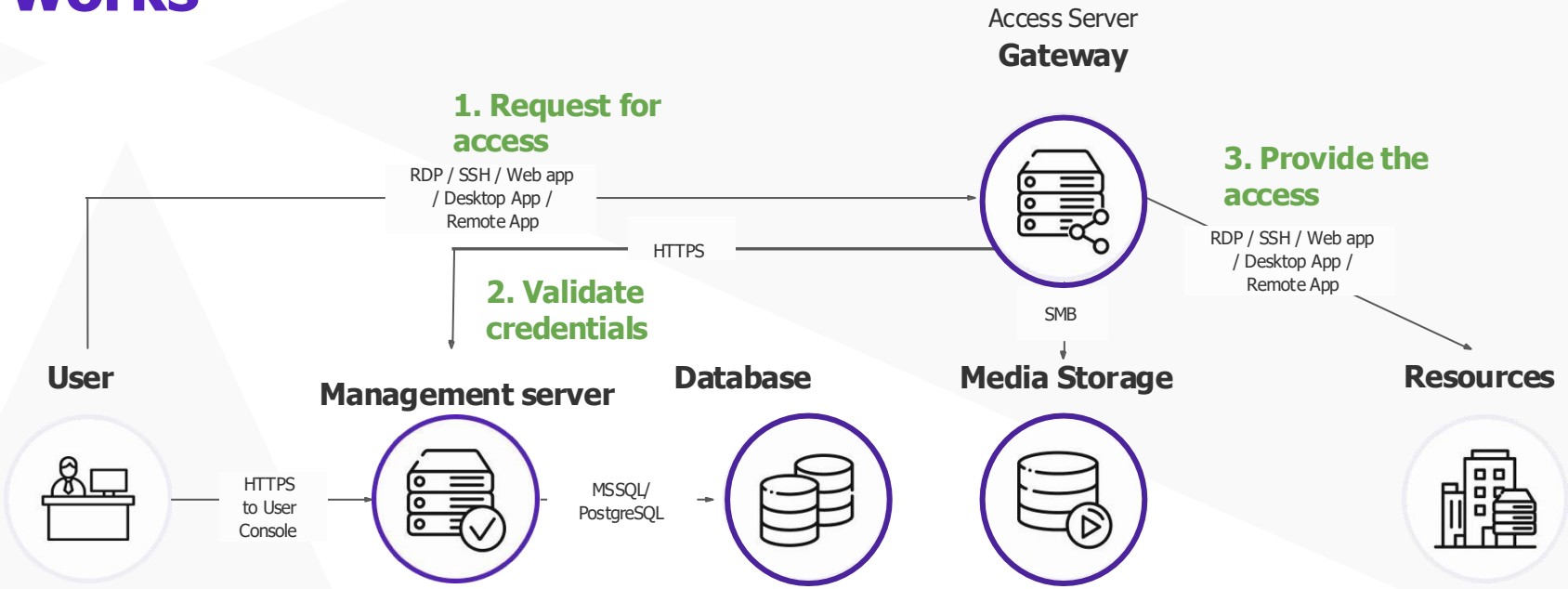
Sachez précisément QUI était derrière ces agissements privilégiés et tenez-les responsables.

Fonctionnalités

Axidian

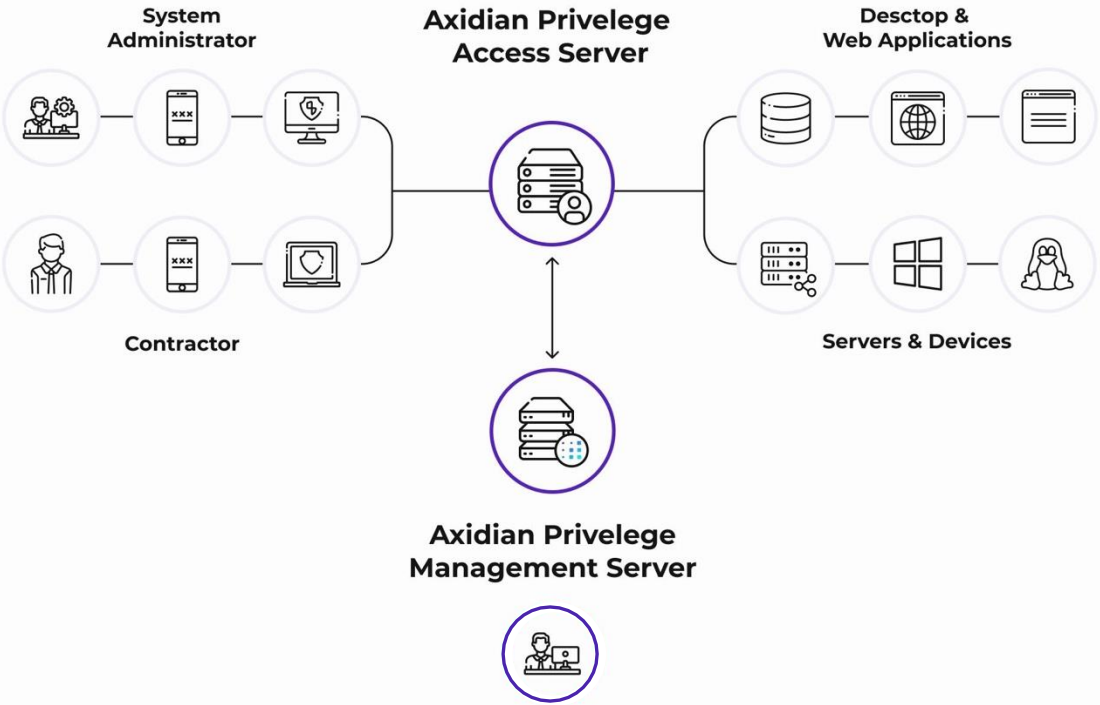
Axidian

How PAM works



Axidian

Principes de fonctionnement



Protocols:

- RDP
- SSH, Telnet
- HTTP(S)
- Proprietary protocols by Application publication via RemoteApp

Ressources cibles pour la gestion des mots de passe :

- MS Active Directory
- MS Windows
- Linux/Unix
- DBMS (PostgreSQL, MS SQL, MySQL, Oracle DB)
- Web-Application
- Desktop Application

Enregistrement et contrôle des activités :

- Enregistrement vidéo
- Enregistrement texte
- Captures d'écran
- Copie fantôme des fichiers transférés
- Filtrage des commandes
- Interruption de session à distance

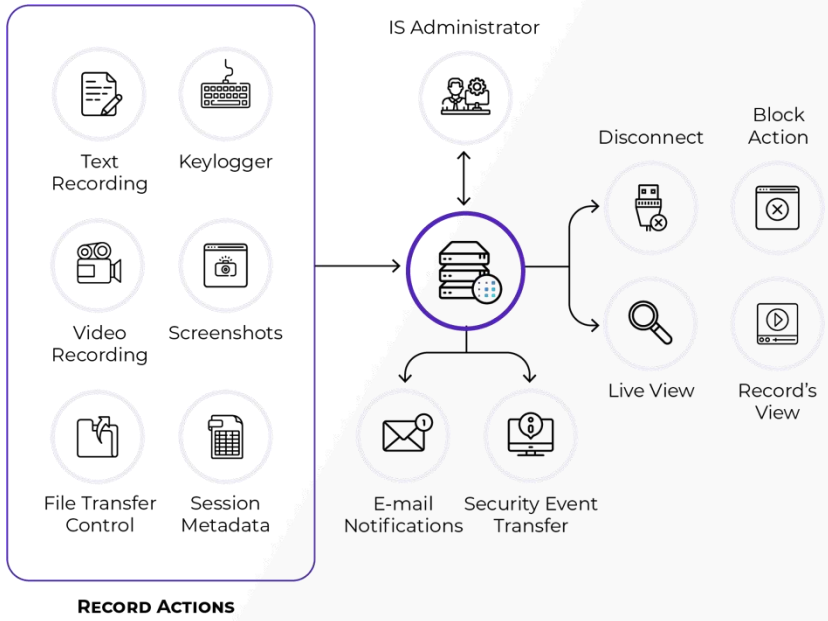
Integration:

- SIEM (syslog)
- Mail (SMTP)
- IdM
- API

Axidian

Enregistrement et contrôle des activités

- Différentes méthodes d'enregistrement des activités
- Filtrage des commandes et interruption de connexion
- Surveillance des sessions privilégiées en temps réel
- Disponibilité de la vue et de la recherche dans tous les enregistrements
- Copiage instantané des fichiers transférés (RDP, SFTP, SCP)*
- Notifications en cas de comportement suspecte

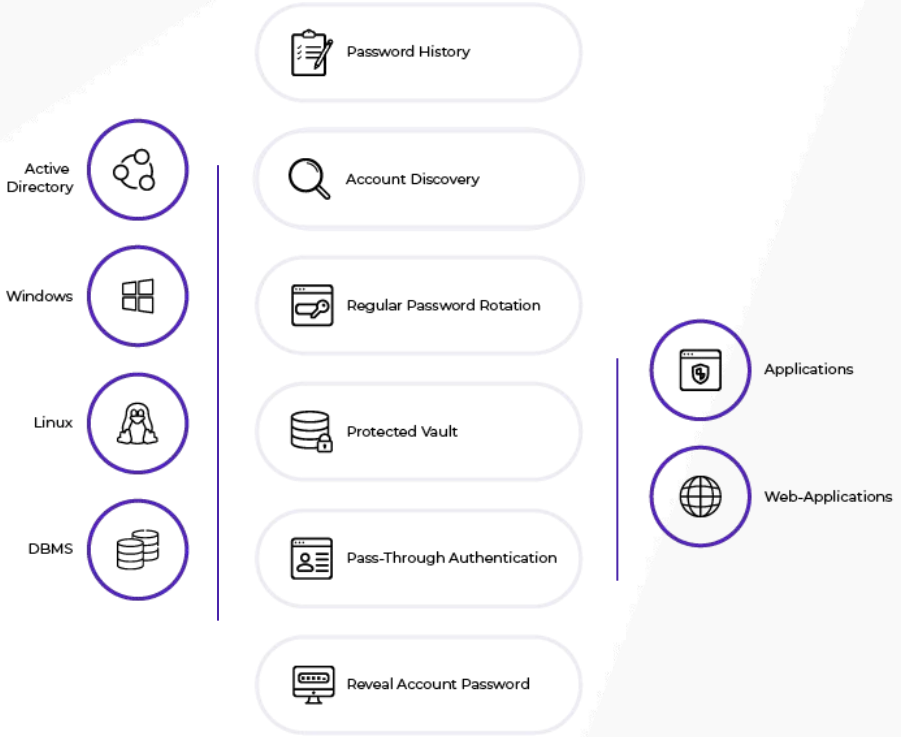


Axidian

Gestion des comptes privilégiés

Fonctionnalités principales :

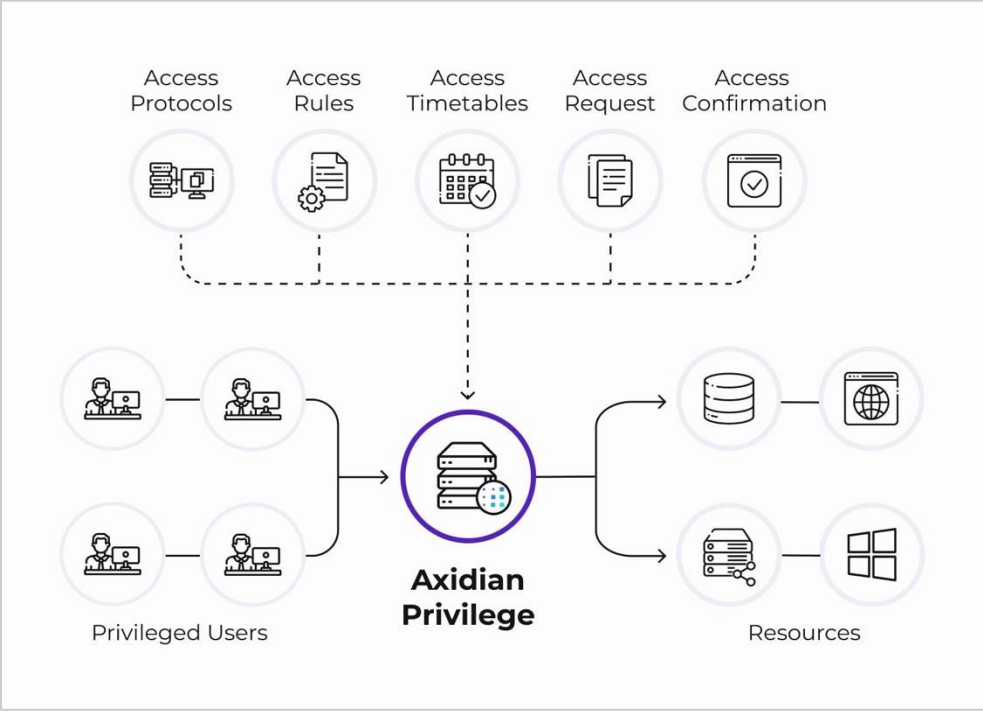
- Coffres-forts pour clés SSH et mots de passe
- Découverte des comptes et des ressources
- Gestion des mots de passe (rotation selon le calendrier et après connexion, révélation, etc.)
- Single Sign-On pour les applications et les applications Web
- Authentification forte - MFA intégrée



Axidian

Gestion des sessions privilégiées

- Intégration avec Active Directory
- Annuaire interne
- Prise en charge des protocoles : RDP, SSH, Telnet, HTTP(S), SQL
- Prise en charge des applications publiées (RemoteApp)



Axidian

Ajoutez une autre couche de contrôle avec MFA/SSO

Axidian Privilege garantit que seul le personnel autorisé bénéficie d'un accès privilégié.

- Technologies d'authentification : mot de passe + TOTP
- L'accès privilégié ne sera pas accordé sans authentification réussie.

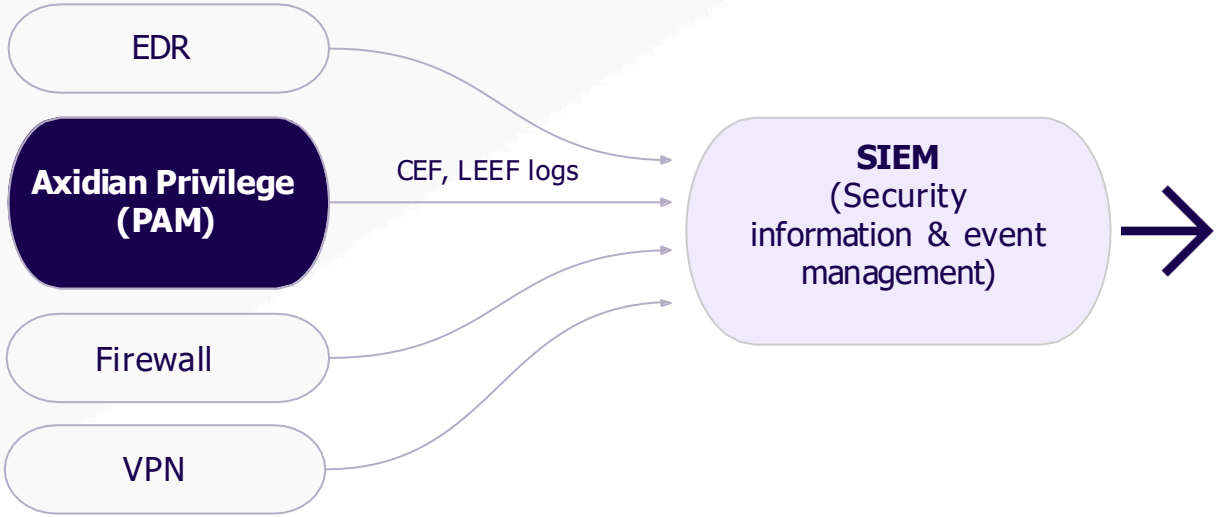
Axidian

Gerez des sessions WEB et SQL sans “ infrastructure hidden costs”

L’accès privilégié et traçabilité directement dans le navigateur.

Sessions **Web et SQL** — sans agent, sans extension et **sans licences RDS**

PAM +SIEM →ISO A. 6.8: *Information security event reporting*



Détection de :

- horaires d'accès inhabituels
- multiples échecs de connexion
- demandes d'accès rapides et consécutives
- tentatives d'accès à plusieurs systèmes critiques
- extractions excessives de mots de passe

Axidian

AAPM Module

Protegez avec le PAM:

- le code source
- les fichiers de configuration
- les scripts de déploiement

Avec l'AAPM (Application-to-Application Password Management), les identifiants sont :

- stockés dans un coffre-fort chiffré AES-256
- non visibles dans le code
- automatiquement renouvelés
- injectés de manière sécurisée lorsque nécessaire

Modèles de licence du PAM Axidian Privilege

Licences par **abonnement** ou **perpétuelles :**

Privileged Users

Calculez uniquement le nombre d'utilisateurs

Privileged Sessions

Calculez uniquement le nombre de connexions simultanées

Resources

Calculez uniquement le nombre de hôtes, applications,serveurs, etc.

*Axidian propose **3 modèles de licences** pour rendre la gestion des accès privilégiés accessible et rentable pour tout type d'entreprise.*

Département Commercial

WCA

HAFS

Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

sales-ci@hafs-networks.com
Envoyez-nous un e-mail

(+225) 07 69 32 13 55
Contact commercial 1

(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY Vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx Wavell. Smart. Seamless | SEARCHINFORM RISK AND COMPLIANCE MANAGEMENT | MOBOTIX | EXTRAVIS Analyse Automatisée Réponse XDR | HAFS MediVision