Préparé pour

KEEPER

Au-delà du coffre-fort : renforcer la gestion des accès privilégiés dans les entreprises modernes

Livre blanc EMA de juillet 2025 par **Ken Buckler, CASP** ; directeur de recherche,
sécurité de l'information, gestion des risques et de la conformité

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table des matières

Introduction

Dans une ère marquée par des cybermenaces incessantes et une transformation numérique rapide, la gestion des accès privilégiés (PAM) est devenue une discipline fondamentale dans le domaine de la sécurité. Les entreprises d'aujourd'hui exigent davantage que le stockage sécurisé des identifiants. Elles ont besoin d'un cadre complet qui protège leurs actifs critiques, applique le principe du moindre privilège et s'intègre parfaitement dans les environnements cloud et sur site.

Une solution PAM efficace commence par une vérification rigoureuse des identités et une authentification multifacteur combinant jetons matériels, approbations mobiles et contrôles biométriques, le tout soutenu par un chiffrement de bout en bout et une sécurité zero-knowledge. Des contrôles granulaires basés sur les rôles et un provisionnement juste-à-temps au sein d'une architecture zero-trust garantissent que les utilisateurs reçoivent les privilèges minimaux nécessaires, ce qui réduit considérablement les conséquences en cas de violation. Simultanément, les journaux d'audit capturent chaque session privilégiée, des commandes exécutées au enregistrements visuels, en passant par la durée des sessions. Ils alimentent ensuite des moteurs de conformité automatisés qui harmonisent les pratiques avec les normes HIPAA, SOX et PCI DSS, tandis que des campagnes de recertification éliminent les comptes orphelins ou excessifs.

Une intégration parfaite avec les services cloud et les outils existants est essentielle. L'injection d'identifiants dans les scripts, les pipelines et les passerelles d'accès à distance maintient la productivité des utilisateurs sans sacrifier la supervision. L'analyse comportementale avancée et l'IA agentique élèvent ensuite la PAM au rang de défense active. Des alertes et des actions en temps réel permettent de neutraliser les menaces et de révoquer instantanément les privilèges. L'extension de ces contrôles aux tiers grâce au partage limité dans le temps et aux appareils, à la rotation automatique des mots de passe et à des flux d'approbation stricts atténue encore davantage les risques liés aux sous-traitants et à la chaîne d'approvisionnement.

Dans ce livre blanc, nous examinerons les défis auxquels sont confrontées les entreprises dans la mise en œuvre de ces priorités en matière de PAM et verrons comment la plateforme KeeperPAM de Keeper Security se positionne par rapport au reste du secteur.

Zero Trust par conception

Zero-trust et zero-knowledge

Notre solution intègre le zero trust dès sa conception

Intégrer les principes zero-trust dès le départ n'est plus une option pour la gestion des accès privilégiés, c'est une nécessité. Un cadre « zero-trust dès la conception » considère chaque demande d'accès privilégié comme intrinsèquement non fiable, ce qui nécessite une vérification continue, une segmentation stricte et l'application du principe du moindre privilège. En passant d'identifiants statiques et omnipotents à des jetons d'accès éphémères et contextuels, les entreprises peuvent réduire considérablement leur surface d'attaque et limiter les mouvements latéraux en cas de violation. Avec le zero trust dès la conception, chaque décision d'accès tient compte de l'identité de l'utilisateur, de la posture de l'appareil, de l'emplacement, de l'heure et du contexte comportemental. Le provisionnement juste-à-temps garantit que les droits privilégiés sont accordés uniquement pour la durée exacte nécessaire, puis automatiquement révoqués par la suite. Des contrôles d'accès granulaires basés sur les rôles minimisent les autorisations excessives, tandis que l'authentification multifacteur et la surveillance continue des sessions protègent contre la compromission des identifiants et les menaces internes.

« [En ce qui concerne la gestion des accès privilégiés, nos priorités sont] l'intégration avec une architecture zero-trust et un cadre de validation continue. »
- Directeur informatique, 500 à 749 employés, utilisant KeeperPAM

L'approche zero-knowledge de Keeper en matière de conception de produits renforce encore davantage ce concept, qui garantit que l'intégralité du chiffrement et du déchiffrement s'effectue localement sur votre appareil. Seul le texte chiffré est transmis au cloud de Keeper. Le mot de passe principal et toutes les clés dérivées ne quittent jamais l'appareil choisi, ce qui signifie que les serveurs de Keeper ne peuvent pas accéder aux données non chiffrées ou aux clés qui les protègent, ni les stocker. Même en cas de violation de l'infrastructure, les attaquants obtiendraient uniquement une chaîne de caractères illisible, garantissant une véritable confidentialité de bout en bout.

Les données d'enquête soulignent l'impact de cette approche : 60 % des utilisateurs de Keeper Security considèrent que leur implémentation PAM est « zero-knowledge » et « zero-trust dès la conception », contre seulement 34,9 % des utilisateurs de tous les autres fournisseurs. Cet écart reflète une posture de sécurité proactive (les clients de Keeper mettent l'accent sur la validation continue, l'élimination des comptes partagés et la gestion automatisée du cycle de vie des privilèges) par opposition à une mentalité plus réactive et axée sur la conformité observée ailleurs.

La PAM zero-trust facilite également la conformité et la préparation aux audits. Chaque session privilégiée est enregistrée de bout en bout (commandes exécutées, enregistrements visuels et indicateurs de durée) et alimente des moteurs de conformité automatisés conformes aux exigences HIPAA, SOX et PCI DSS. Dans la pratique, les entreprises qui intègrent le zero trust dans leur architecture PAM renforcent non seulement leurs défenses, mais rationalisent également leurs opérations, réduisent les coûts associés aux comptes orphelins et démontrent des améliorations mesurables en matière de limitation des violations.

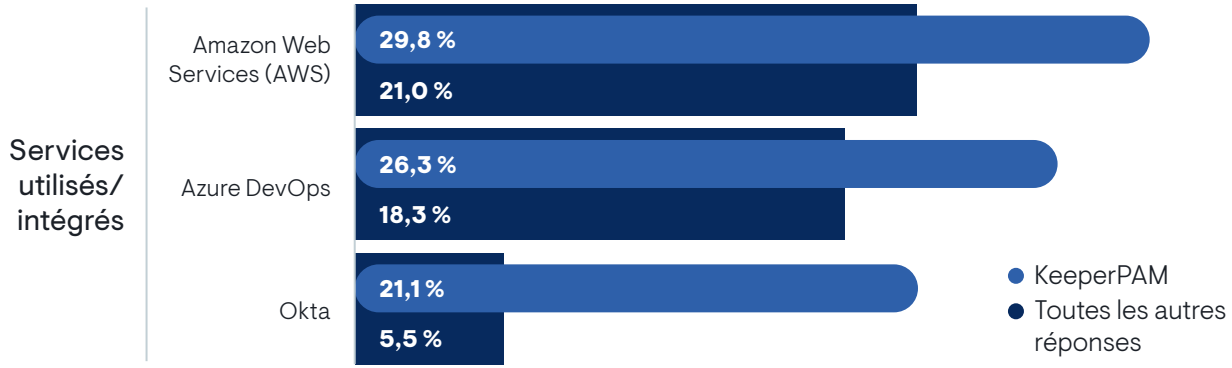
En fin de compte, l'approche zero-knowledge et la conception zero-trust de Keeper font passer l'accès privilégié de risque potentiel à processus contrôlé et vérifiable, qui s'adapte en temps réel à l'évolution des risques et garantit la sécurité, la conformité et la résilience des systèmes critiques.

Facilité de déploiement, de configuration et d'intégration

Il n'existe pas de solution miracle, mais Keeper s'en rapproche

La facilité de déploiement, de configuration et d'intégration peut garantir ou compromettre la rentabilité d'un projet PAM. Selon l'enquête d'EMA, 60 % des clients de Keeper Security ont jugé le déploiement initial « très facile », contre seulement 22,1 % des utilisateurs d'autres plateformes PAM. Par ailleurs, 10 % des clients de l'ensemble des autres solutions ont qualifié le déploiement de « assez difficile » ou « très difficile », une source d'irritation totalement absente chez les utilisateurs de KeeperPAM. La migration des outils PAM hérités et sur site vers le cloud pose encore des difficultés à 39 % des entreprises, une complexité que l'architecture cloud-native de Keeper permet d'éviter. Les problèmes d'intégration affectent 11 % des déploiements hors Keeper, qui nécessitent souvent des connecteurs propriétaires et des scripts manuels pour se connecter aux systèmes SIEM, de gestion des tickets ou aux pipelines DevOps. Les API modulaires, les connecteurs prêts à l'emploi et l'orchestration cloud transparente de KeeperPAM accélèrent le délai de réalisation de la valeur et minimisent les frictions opérationnelles.

Joue bien avec les autres



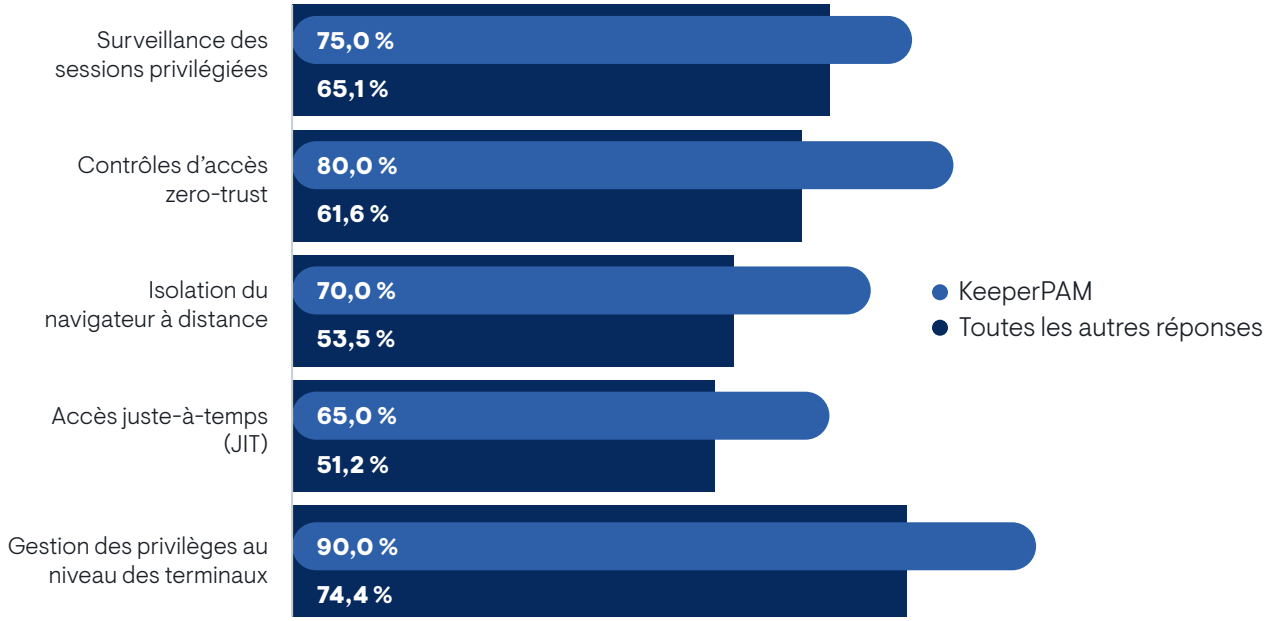
La fluidité d'intégration est la pierre angulaire de toute stratégie PAM moderne, et Keeper est également en tête dans ce domaine. Des connecteurs et des API prêts à l'emploi permettent une intégration rapide et bidirectionnelle avec les plateformes principales, qu'il s'agisse d'exécuter des instances EC2 dans Amazon Web Services, d'automatiser des pipelines dans Azure DevOps ou de centraliser l'authentification par l'intermédiaire d'Okta. Les utilisateurs de KeeperPAM signalent une adoption beaucoup plus élevée de ces intégrations par rapport à d'autres solutions PAM, ce qui élimine le besoin de personnalisation fastidieuse des scripts ou de maintenance manuelle des connecteurs. En intégrant l'injection d'identifiants privilégiés directement dans vos flux de travail CI/CD, vos consoles cloud et vos fournisseurs d'identité, KeeperPAM minimise les frictions, stimule la productivité des développeurs et garantit la protection des secrets à tous les niveaux.

Faire Plus avec Moins de Personnel

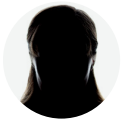
Les besoins en personnel pour la mise en œuvre de solutions PAM varient considérablement d'une plateforme à l'autre. Seuls 15 % des clients de Keeper Security déclarent avoir besoin de personnel dédié pour gérer le déploiement, la configuration et l'intégration, grâce à l'interface utilisateur intuitive de Keeper, à ses assistants de configuration guidés et à sa documentation complète. En revanche, 39,5 % des entreprises qui utilisent d'autres solutions PAM ont besoin d'un ou plusieurs administrateurs à temps plein pour assurer le bon fonctionnement de leurs environnements. Ces équipes doivent souvent jongler entre la maintenance complexe des appareils sur site, la création de scripts sur mesure et les mises à jour manuelles des connecteurs, ce qui augmente les effectifs et sollicite les ressources informatiques existantes. La conception cloud-native et les outils en libre-service de Keeper minimisent le recours à des compétences spécialisées. Les administrateurs peuvent mettre en place de nouveaux systèmes, ajuster les politiques relatives aux privilèges et les intégrer à des pipelines SIEM ou DevOps sans personnalisation importante. Au final, la réduction des frais généraux liés au personnel se traduit par des déploiements plus rapides et des opérations à long terme plus durables et plus abordables.

Au-delà de la gestion des mots de passe et des secrets

Fonctionnalités PAM avancées



Les solutions PAM modernes exigent bien plus que le simple stockage sécurisé des identifiants : elles doivent offrir un ensemble complet de fonctionnalités qui protègent contre les menaces, les surveillent et s'adaptent à leur évolution. KeeperPAM se distingue en proposant des fonctionnalités avancées que de nombreux fournisseurs traditionnels ne proposent tout simplement pas ou ne peuvent pas mettre en œuvre à grande échelle. La surveillance des sessions privilégiées, par exemple, est essentielle pour capturer chaque aspect des activités à haut risque (frappes, commandes, affichage de l'écran). Les clients de Keeper utilisent cette fonctionnalité plus fréquemment que leurs concurrents, ce qui leur permet de détecter les menaces en temps réel et d'effectuer des analyses approfondies.



« L'utilisation de PAM renforce l'intégrité de nos données et notre réputation. »
- VP du développement/de l'ingénierie, 1 000 à 2 499 employés, utilisant KeeperPAM

L'accès réseau zero-trust étend les principes du moindre privilège au-delà des mots de passe à chaque demande d'accès. Keeper intègre des contrôles contextuels des politiques (état de l'appareil, emplacement, heure et références comportementales) garantissant que même les sessions authentifiées restent sous surveillance continue. Ce contrôle granulaire des opérations privilégiées réduit considérablement la fenêtre d'exposition potentielle par rapport aux modèles statiques de type « tout ou rien ».

L'isolation du navigateur à distance (RBI) est un autre domaine dans lequel Keeper surpasse ses concurrents. En mettant en proxy les consoles d'administration via des navigateurs isolés et sécurisés, les entreprises éliminent tout accès direct aux terminaux pour les tiers et les sous-traitants, ce qui permet de mettre efficacement en quarantaine les logiciels malveillants potentiels ou d'empêcher le vol d'identifiants. Peu d'autres solutions PAM intègrent la RBI de manière aussi parfaite. Le reste impose à la place des solutions manuelles qui nuisent à la sécurité et à l'expérience utilisateur.

Le provisionnement juste-à-temps et la gestion automatisée du cycle de vie des privilèges complètent la boîte à outils avancée de Keeper. L'élévation temporaire et limitée dans le temps des privilèges empêche l'accumulation de comptes à privilèges élevés, tandis que les campagnes automatiques de suppression des privilèges et de recertification garantissent le respect des obligations de conformité sans effort manuel supplémentaire. Enfin, la gestion des privilèges au niveau des terminaux, qui supprime les droits d'administrateur local tout en accordant des privilèges limités à la demande, protège à la fois contre les attaques externes et les abus internes.

En allant au-delà des mots de passe et des secrets, Keeper fait de la PAM une plateforme de défense active : elle anticipe les attaques, applique le principe du zero trust à tous les niveaux et offre les contrôles avancés exigés par les environnements complexes d'aujourd'hui.

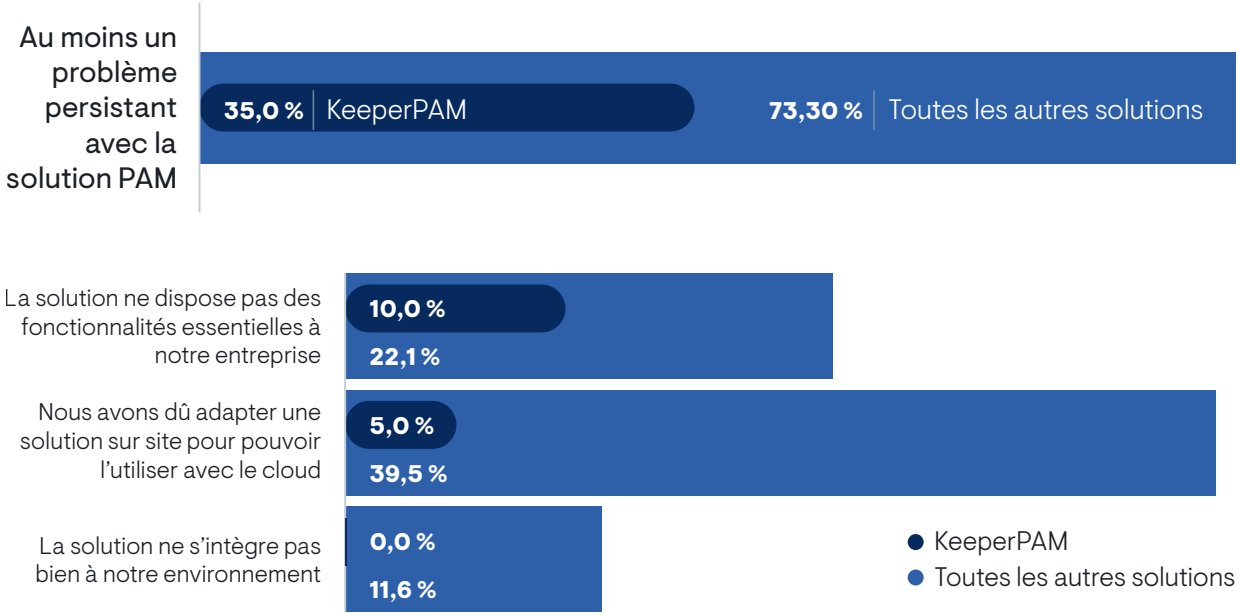
Satisfaction générale

Votre solution PAM résiste-t-elle à la tempête ?

La satisfaction client est le baromètre ultime de la valeur et de la longévité de toute solution PAM. Lorsque 5 % des entreprises utilisant d'autres plateformes recherchent activement une solution de remplacement, cela indique des lacunes critiques en matière de fiabilité, d'utilisabilité et/ou d'assistance. En revanche, aucun utilisateur de Keeper Security n'a déclaré avoir l'intention d'abandonner son outil PAM, ce qui souligne la capacité de Keeper à répondre à l'évolution des besoins en matière de sécurité et d'exploitation.

De plus, 75 % des clients de Keeper se déclarent « très satisfaits » dans l'ensemble, ce qui dépasse largement les 53,5 % d'utilisateurs « très satisfaits » parmi les clients des fournisseurs concurrents. Un niveau de satisfaction élevé est corrélé à une adoption plus rapide, à une réduction plus efficace des risques et à un coût total de possession plus faible, car les équipes satisfaites investissent dans des intégrations plus approfondies et des fonctionnalités plus avancées. Dans un contexte où les accès privilégiés sont constamment ciblés, choisir une plateforme qui satisfait ses utilisateurs n'est pas seulement un plus, c'est une nécessité absolue.

Les fonctionnalités et les intégrations sont d'importantes sources d'irritation



Malgré leur rôle essentiel, de nombreux déploiements PAM se heurtent à des obstacles persistants. Près de trois quarts (73 %) des entreprises qui utilisent des solutions autres que Keeper signalent au moins une difficulté majeure, contre seulement 35 % des clients Keeper. Parmi les sources d'irritation courantes, citons l'absence de fonctionnalités essentielles, qui oblige les équipes à recourir à des outils tiers, la mauvaise intégration dans l'infrastructure existante et la complexité liée à la modernisation des plateformes sur site pour prendre en charge les environnements cloud. Les utilisateurs KeeperPAM rencontrent beaucoup moins souvent ces problèmes grâce à l'ensemble complet de fonctionnalités, à l'architecture cloud-native et à la vaste bibliothèque de connecteurs de Keeper. En réduisant au minimum les lacunes fonctionnelles et en simplifiant les déploiements hybrides, Keeper accélère non seulement le délai de réalisation de la valeur, mais réduit également la charge liée au dépannage et aux solutions de rechange, ce qui permet aux équipes de sécurité de s'attacher davantage à réduire proactivement les risques plutôt qu'à remédier aux limitations des systèmes existants.

Meilleure solution, meilleures priorités

Les autres solutions PAM ne sont pas à la hauteur de leur potentiel

Zone prioritaire	Clients Keeper	Autres solutions PAM
Authentification	Continue, zero-trust	Basé sur les rôles, MFA
Gestion des identifiants	Suppression des identifiants statiques/ partagés	Contrôle et surveillance des accès de base
Formation	Priorité explicite	N'est pas une priorité
Automatisation	Concentration sur l'atténuation des risques (parce que le	Process efficiency focus
Conformité	Accent mis sur l'utilisation abusive des identifiants et l'audit	Conformité réglementaire minimale

Keeper Security permet aux entreprises de passer d'une approche axée sur la maintenance et la conformité à une posture proactive qui privilégie la sécurité. KeeperPAM élimine les identifiants statiques et partagés de manière non sécurisée grâce à un moteur de coffre-fort zero-knowledge qui génère des secrets éphémères et à moindre privilège, réduisant ainsi considérablement les vecteurs d'attaque externes et les abus internes par rapport aux approches traditionnelles basées uniquement sur des coffres-forts. L'authentification continue et les contrôles d'accès zero-trust, notamment les vérifications de l'état des appareils, la géolocalisation et l'analyse comportementale, garantissent que toute session reste sous surveillance longtemps après une invite MFA unique, rendant pratiquement impossible pour les attaquants d'exploiter des identifiants volés sans être repérés. L'automatisation centrée sur les risques de Keeper couvre l'ensemble du cycle de vie des privilèges, de la découverte et de l'intégration à la rotation automatique et à la suppression, empêchant ainsi la prolifération des identifiants et la création de comptes orphelins, alors que de nombreuses autres solutions se contentent d'automatiser les flux d'approbation ou les rapports de conformité. Il est important de noter que les clients de Keeper intègrent explicitement la formation et la sensibilisation du personnel dans leurs contrôles de sécurité fondamentaux,

reconnaissant que les facteurs humains sont aussi importants que la technologie pour favoriser l'adoption et empêcher la mise en place de palliatifs risqués.

« Je crois que la surveillance constante des comptes privilégiés m'aide à mieux dormir la nuit. »
– VP du développement/de l'ingénierie, 2 500 à 4 999 employés, utilisant KeeperPAM

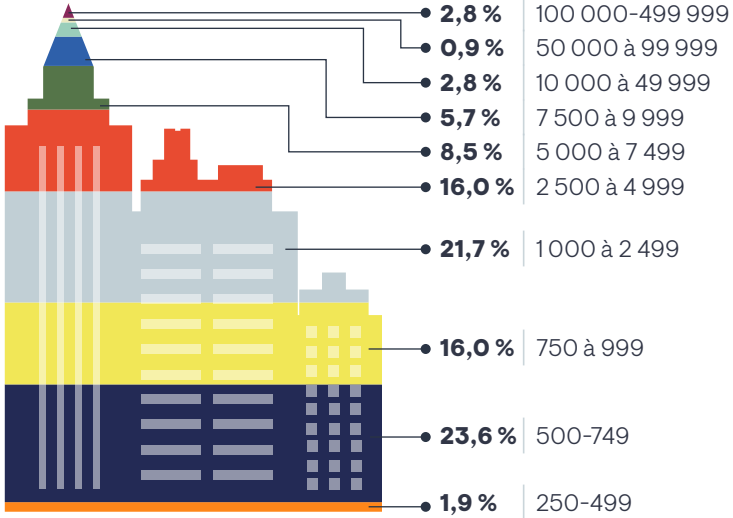
En revanche, les utilisateurs d'autres outils PAM mettent souvent l'accent sur les contrôles traditionnels, tels que l'accès basé sur les rôles, l'audit post-accès et l'efficacité opérationnelle, reflétant une mentalité réactive qui se heurte à des lacunes fonctionnelles, à des intégrations fragiles et à la complexité de la modernisation des solutions sur site vers le cloud. L'architecture cloud-native de Keeper et sa vaste bibliothèque de connecteurs prêts à l'emploi éliminent ces difficultés, permettant une intégration rapide avec les plateformes SIEM, les fournisseurs d'identité tels qu'Okta et les pipelines CI/CD dans AWS ou Azure DevOps. Les fonctionnalités avancées, notamment la surveillance des sessions privilégiées, l'isolation du navigateur à distance, le provisionnement juste-à-temps et la gestion des privilèges au niveau des terminaux, sont toutes intégrées nativement à Keeper, ce qui réduit les frictions liées aux déploiements et les besoins en personnel.

En combinant ces fonctionnalités nouvelle génération avec une expérience utilisateur fluide, Keeper permet aux équipes de sécurité d'anticiper les menaces, d'assurer une protection continue et de renforcer véritablement leur environnement en matière d'accès privilégié.

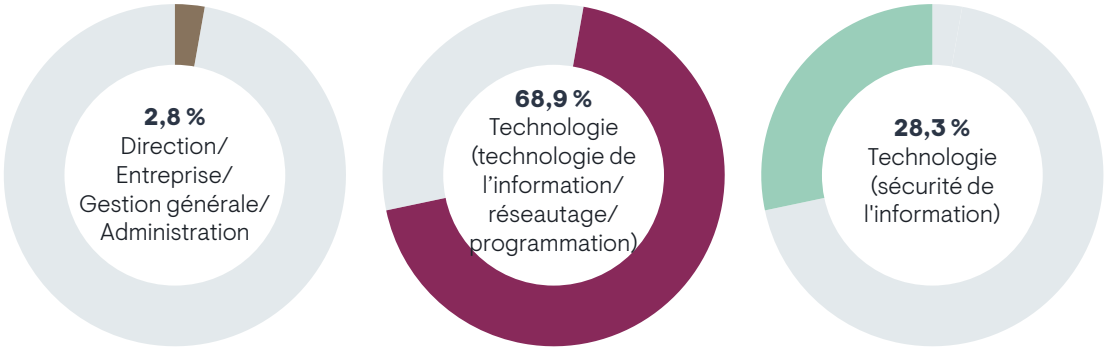
Méthodologie

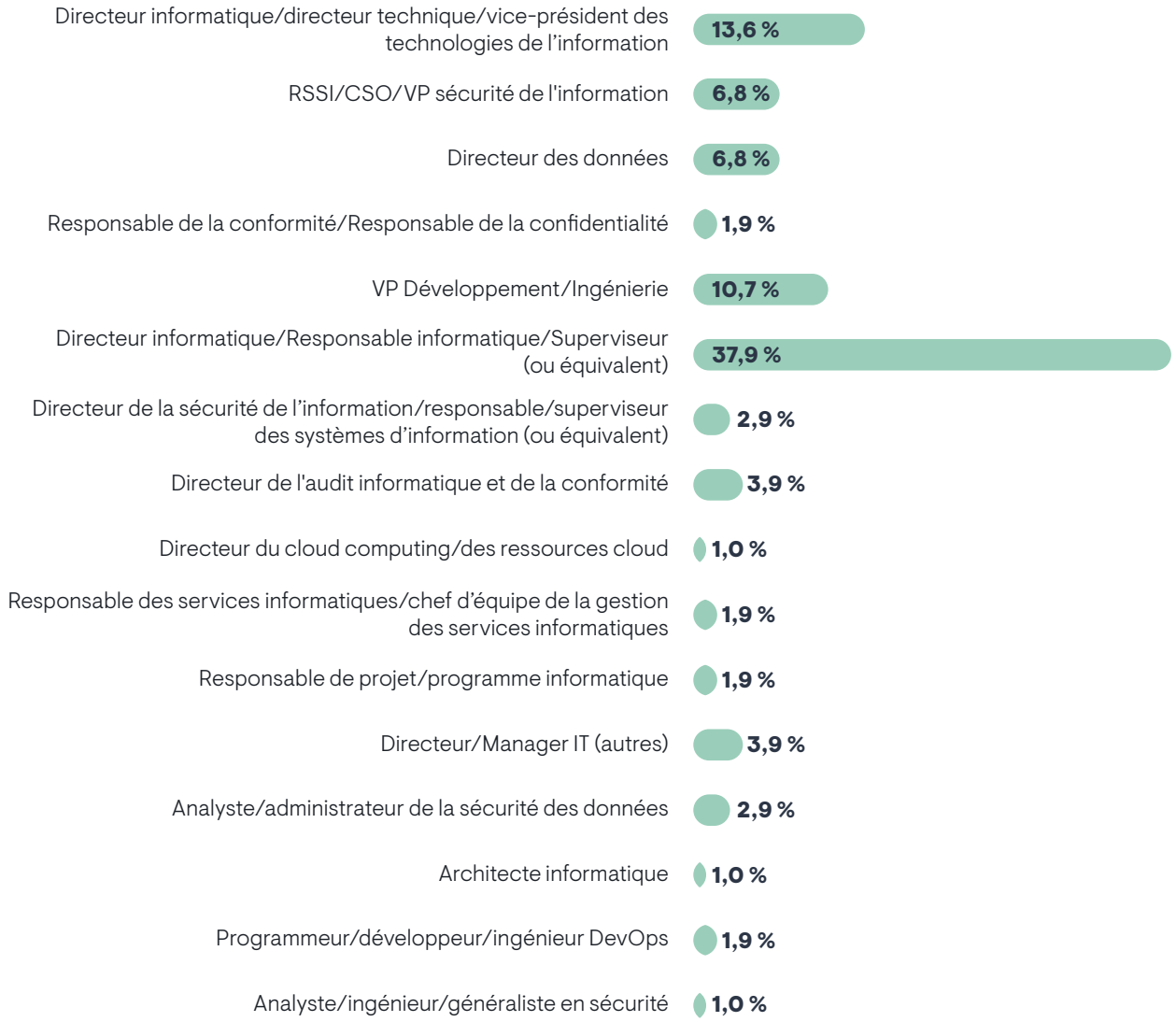
Total de 106 professionnels utilisant BeyondTrust, CyberArk, Delinea, Devolutions, Keeper Security, ManageEngine, One Identity ou StrongDM en juin 2025. Toutes les données contenues dans ce livre blanc sont basées sur les réponses à l'enquête et les réponses ouvertes concernant les priorités et les défis en matière de gestion des accès privilégiés dans l'entreprise.

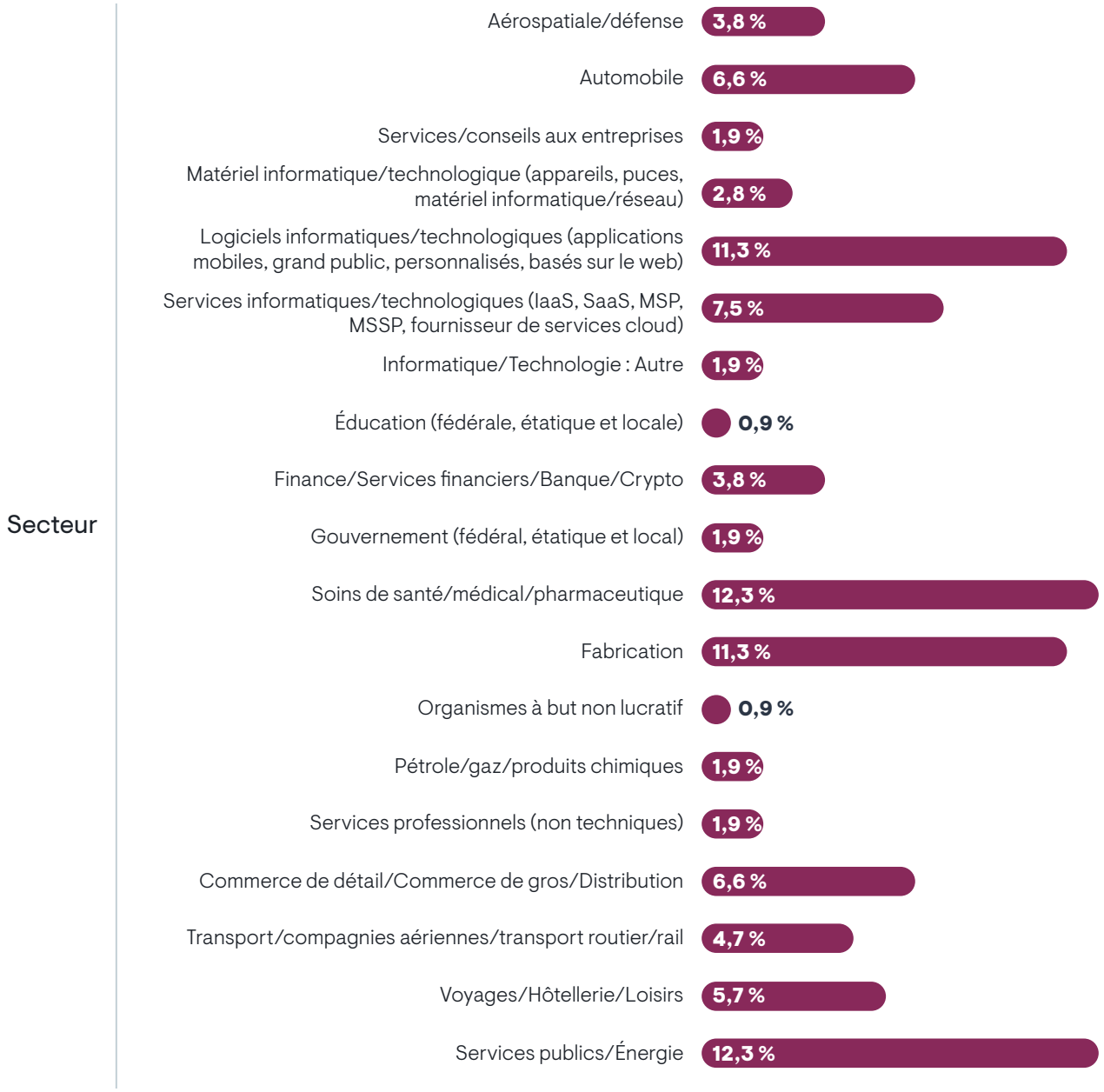
Taille de l'organisation



Rôle du Répondant




Directeur informatique/directeur technique/vice-président des technologies de l'information
13,6 %
RSSI/CSO/VP sécurité de l'information
6,8 %
Directeur des données
6,8 %
Responsable de la conformité/Responsable de la confidentialité
1,9 %
VP Développement/Ingénierie
10,7 %
Directeur informatique/Responsable informatique/Superviseur (ou équivalent)
37,9 %
Directeur de la sécurité de l'information/responsable/superviseur des systèmes d'information (ou équivalent)
2,9 %
Directeur de l'audit informatique et de la conformité
3,9 %
Directeur du cloud computing/des ressources cloud
1,0 %
Responsable des services informatiques/chef d'équipe de la gestion des services informatiques
1,9 %
Responsable de projet/programme informatique
1,9 %
Directeur/Manager IT (autres)
3,9 %
Analyste/administrateur de la sécurité des données
2,9 %
Architecte informatique
1,0 %
Programmeur/développeur/ingénieur DevOps
1,9 %
Analyste/ingénieur/généraliste en sécurité
1,0 %


Secteur
Aérospatiale/défense
3,8 %
Automobile
6,6 %
Services/conseils aux entreprises
1,9 %
Matériel informatique/technologique (appareils, puces, matériel informatique/réseau)
2,8 %
Logiciels informatiques/technologiques (applications mobiles, grand public, personnalisés, basés sur le web)
11,3 %
Services informatiques/technologiques (IaaS, SaaS, MSP, MSSP, fournisseur de services cloud)
7,5 %
Informatique/Technologie : Autre
1,9 %
Éducation (fédérale, étatique et locale)
0,9 %
Finance/Services financiers/Banque/Crypto
3,8 %
Gouvernement (fédéral, étatique et local)
1,9 %
Soins de santé/médical/pharmaceutique
12,3 %
Fabrication
11,3 %
Organismes à but non lucratif
0,9 %
Pétrole/gaz/produits chimiques
1,9 %
Services professionnels (non techniques)
1,9 %
Commerce de détail/Commerce de gros/Distribution
6,6 %
Transport/compagnies aériennes/transport routier/rail
4,7 %
Voyages/Hôtellerie/Loisirs
5,7 %
Services publics/Énergie
12,3 %

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4577.081325-FR