

**Delinea**

# Delinea Platform : Étendre de manière intuitive la gestion des accès à privilèges

La plateforme cloud-native Delinea Platform fournit un accès à privilèges juste-à-temps aux utilisateurs autorisés avec des contrôles adaptatifs faciles à utiliser qui réduisent les risques tout en favorisant la croissance, l'efficacité et l'évolutivité.

Le nombre d'identités humaines et machines disposant d'un accès à privilèges est en augmentation. La plupart des responsables de l'informatique et de la sécurité utilisent une multitude d'outils disparates de sécurité avec peu ou pas de visibilité unifiée, ce qui complique la gestion de politiques fragmentées d'identité et d'accès à privilèges. Sans une méthode cohérente et centralisée de gestion des privilèges, les équipes informatiques et de sécurité perdent un temps précieux, commettent des erreurs et laissent des failles de sécurité qui ouvrent la porte aux cyberattaques.

Une vue complète de la sécurité des accès à privilèges dans un emplacement centralisé est essentielle pour gagner du temps, augmenter la productivité et réduire les risques.

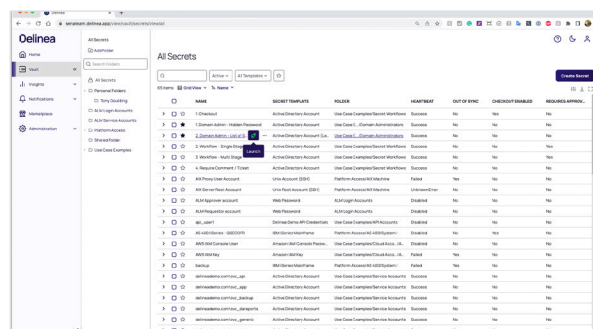
## Sécuriser rapidement les informations d'identification des comptes à privilèges

**Au cœur de Delinea Platform se trouve Secret Server, le coffre-fort de gestion des accès à privilèges (PAM) le plus performant du secteur, qui garantit une facilité d'utilisation avec une sécurité de niveau entreprise dans un environnement centralisé.**

Secret Server identifie, sécurise, gère, surveille et audite de manière intuitive les informations d'identification partagées pour les comptes de service, d'application, root et administrateur dans toute votre entreprise.

Sécurisez rapidement l'accès et surveillez l'activité sur les comptes à privilèges stratégiques tout en garantissant un équilibre parfait entre sécurité, efficacité et productivité au sein des équipes.

- **Améliorez la sécurité** Réduisez considérablement votre surface d'attaque grâce à des contrôles robustes et granulaires sur les informations d'identification partagées pour chaque compte à privilèges.



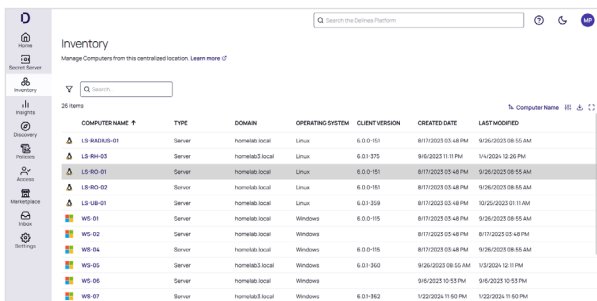
NAME	SECRET TEMPLATE	POLICY	HEARTBEAT	OUT OF SYNC	CHECKOUT ENABLED	REQUIRED APPROVALS
1 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
2 - Dnsadm	ActiveDirectoryAccount	Use Case - Global Administrators	Business	Yes	Yes	Yes
3 - Dnsadm	ActiveDirectoryAccount	Use Case - Global Administrators	Business	Yes	Yes	Yes
4 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
5 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
6 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
7 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
8 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
9 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
10 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
11 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
12 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
13 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
14 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
15 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
16 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
17 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
18 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
19 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes
20 - Dnsadm	ActiveDirectoryAccount	Use Case Computer/Service Accounts	Business	Yes	Yes	Yes

- **Gagnez en efficacité** - L'automatisation intelligente détecte automatiquement les privilèges orphelins ou oubliés et assure la rotation des mots de passe tout en les testant facilement à l'aide de contrôles « Heartbeat »
- **Rapide retour sur investissement** La facilité de déploiement, de mise en œuvre et de gestion permet de réduire le coût total de possession et de rentabiliser rapidement l'investissement.

## Centralisez les contrôles d'autorisation de manière cohérente entre les identités

La solution Privilege Control for Servers applique les principes du moindre privilège en centralisant les contrôles d'autorisation de manière cohérente sur toutes les identités pour aider les équipes informatiques et de sécurité à respecter la conformité, à améliorer la productivité et à limiter les risques.

Développez de manière intuitive votre coffre-fort d'informations d'identification en étendant la gestion des accès à privilèges et en superposant la sécurité directement sur vos serveurs à l'aide des identités d'entreprise.



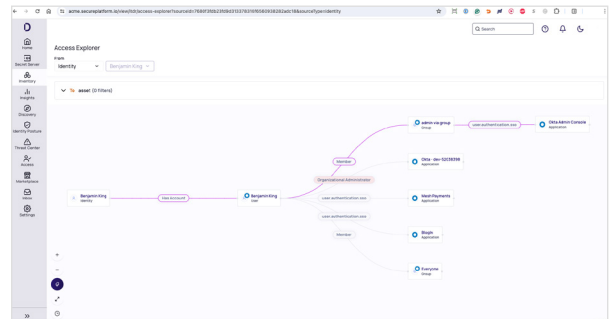
COMPUTER NAME #	TYPE	DOMAIN	OPERATING SYSTEM	CLIENT VERSION	CREATED DATE	LAST MODIFIED
LS-R426-01	Server	homelab.local	Linux	6.0.0-151	8/17/2023 03:48 PM	9/26/2023 08:55 AM
LS-R44-03	Server	homelab3.local	Linux	6.0.0-375	9/6/2023 11:31 PM	1/26/2024 12:26 PM
LS-R10-01	Server	homelab.local	Linux	6.0.0-151	8/17/2023 03:48 PM	9/26/2023 08:55 AM
LS-R10-02	Server	homelab.local	Linux	6.0.0-151	8/17/2023 03:48 PM	9/26/2023 08:55 AM
LS-UB-01	Server	homelab.local	Linux	6.0.0-359	8/17/2023 03:48 PM	10/26/2023 01:11 AM
WS-01	Server	homelab.local	Windows	6.0.0-115	8/17/2023 03:48 PM	9/26/2023 08:55 AM
WS-02	Server	homelab.local	Windows	6.0.0-115	8/17/2023 03:48 PM	9/26/2023 08:55 AM
WS-04	Server	homelab.local	Windows	6.0.0-115	8/17/2023 03:48 PM	9/26/2023 08:55 AM
WS-05	Server	homelab3.local	Windows	6.0.0-360	9/26/2023 08:55 AM	1/26/2024 12:11 PM
WS-06	Server	homelab3.local	Windows	6.0.0-360	9/26/2023 10:53 PM	9/26/2023 10:53 PM
WS-07	Server	homelab3.local	Windows	6.0.0-362	1/22/2024 11:50 PM	1/22/2024 11:50 PM

- **Privilège juste-assez et juste-à-temps** Accordez des droits et privilèges d'administration uniquement lorsqu'ils sont requis sous Windows, Linux et Unix dans des environnements multi-cloud hybrides.
- **Rationalisez l'accès à privilèges** Unifiez l'autorisation pour toutes les identités avec une piste d'audit complète directement depuis l'hôte.
- **Une sécurité en profondeur** Appliquez l'authentification multi-facteurs (MFA) lors de la connexion et de l'élévation des privilèges pour un contrôle supplémentaire des identités.

## Appliquez le principe du moindre privilège sur les cloud publics

La solution Privilege Control for Cloud Entitlements fournit aux responsables de la sécurité du cloud un contexte approfondi sur l'utilisation du cloud et des identités pour découvrir les privilèges excessifs et limiter les autorisations dans l'infrastructure multi-cloud afin de réduire les risques.

Intégrez les droits cloud dans le cadre de vos politiques d'autorisation centrales pour toutes les identités, en découvrant et en visualisant toutes les identités, tous les comptes et leur accès sur les cloud Google, Amazon et Microsoft afin d'identifier les comportements anormaux et de refactoriser les privilèges.



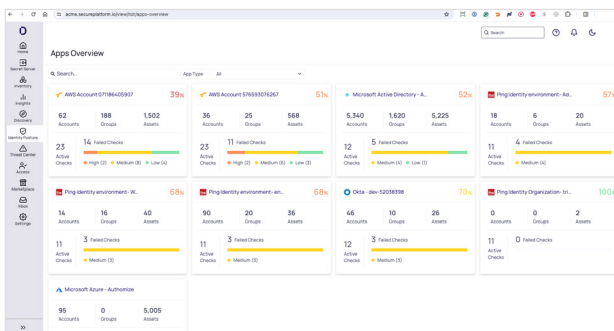
- **Découverte continue** Le lanceur à simple clic avec des contrôles robustes vous permet d'avancer rapidement.
- **Appliquez les principes du moindre privilège** Le déploiement sans agent élimine les logiciels supplémentaires et le temps de gestion.
- **Identifiez les identités à risques** L'enregistrement de session pour chaque session à distance vous permet d'avoir une vue d'ensemble.



## Détecter et traiter de manière proactive les menaces liées à l'identité

La solution Identity Threat Protection établit un contexte au niveau de la couche d'identité pour détecter et traiter les menaces en temps réel, en fournissant des informations de haute qualité qui aident les responsables des opérations de sécurité à limiter l'impact des menaces liées à l'identité.

Réduisez les risques de manière proactive en identifiant les comportements anormaux, en identifiant les identités les plus vulnérables, en déterminant l'impact potentiel en cas de compromission et en prenant les mesures qui s'imposent.

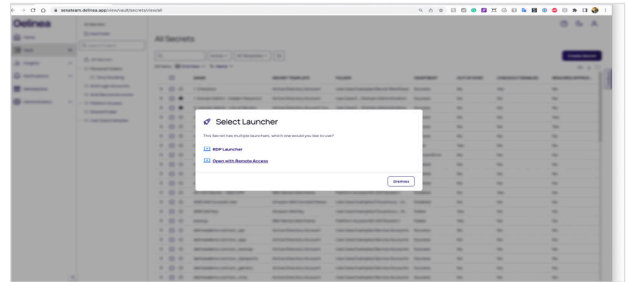


- **Détection continue** Découvrez les erreurs de configuration des identités et les comportements anormaux au sein des identités fédérées et locales.
- **Détection continue** Visualisez les chemins d'accès aux identités à travers les systèmes d'identité, les applications Software-as-a-Service (SaaS), le cloud et l'infrastructure traditionnelle.
- **Remédiez aux menaces** Suivez les actions recommandées ou automatisez les réponses pour réduire l'impact d'une attaque.

## Simplifiez l'accès sécurisé pour les utilisateurs à privilèges en dehors de votre réseau.

Privileged Remote Access, disponible sur Delinea Platform, fournit des sessions sans VPN basées sur un navigateur avec des contrôles du moindre privilège pour aider les responsables informatiques et de la sécurité à atténuer les risques et les manques d'efficacité liés à l'accès à distance.

Un accès à distance à privilèges peut être fourni à tout utilisateur extérieur au réseau. Intégrée à la plateforme cloud-native, Delinea Platform, la solution permet de centraliser l'autorisation pour les sessions à distance avec injection des identifiants afin de ne pas exposer les identifiants à privilèges sur le terminal tout en permettant aux utilisateurs de se connecter de manière intuitive aux ressources cibles.



- **Accès à distance à privilèges** Sécurisez l'accès à distance tout en appliquant des contrôles de privilèges.
- **Déploiement intuitif** Le déploiement sans agent élimine les logiciels supplémentaires et le temps de gestion.
- **Contrôles de conformité** Enregistrement de session et audit piloté par l'IA pour chaque session à distance.



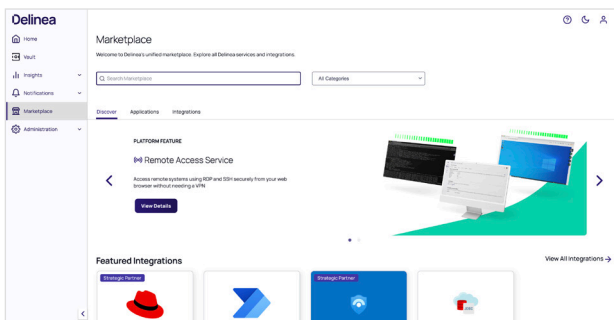
## PRÉSENTATION DE SOLUTION

Delinea Platform : Étendre facilement la gestion des accès à privilèges

### Un écosystème d'intégration extensible pour un accès centralisé aux fournisseurs et aux solutions

Avec la **marketplace** de Delinea Platform, vous pouvez **visualiser, tester et acheter** les intégrations tierces d'un seul coup d'œil, et y accéder.

Travailler avec des solutions de sécurité multiples et en silos augmente les coûts et prend du temps lorsque vous essayez de faire correspondre les données et les informations. Nous éliminons cette contrainte en permettant une vue consolidée de votre environnement de gestion des accès à privilèges dans une expérience unifiée.



- **Expérience unifiée** Connectez-vous à tous les pans de vos opérations et workflows informatiques, reporting de sécurité, réponse aux incidents et plus encore.
- **Améliorez l'efficacité** Augmentez l'adoption en intégrant le PAM, le CIEM et l'ITDR dans le workflow quotidien des équipes informatiques et de sécurité, des développeurs et des utilisateurs professionnels.
- **Augmentez la productivité** Accélérez la transformation numérique grâce à des solutions tierces faciles d'accès et téléchargeables.

Les entreprises évaluent la sécurité de leurs comptes à privilèges et découvrent que leurs attentes et leurs besoins ont évolué. Delinea Platform est conçue pour soutenir votre croissance tout en renforçant la sécurité des accès à privilèges et des identités. Elle offre une visibilité unifiée, améliore l'efficacité et la sécurité, rationalise la gestion et augmente la productivité. Delinea répond à vos besoins où que vous soyez, vous fournissant tout ce dont vous avez besoin, au moment où vous en avez besoin.

### En savoir plus sur [Delinea Platform](#).

## Delinea

Delinea est un pionnier de la sécurisation des identités en proposant une autorisation centralisée qui permet de rendre les organisations plus sûres et de régir de manière intuitive leurs interactions au sein de l'entreprise moderne. Delinea permet aux entreprises d'établir le contexte et l'intelligence tout au long du cycle de vie de l'identité à travers l'infrastructure cloud et traditionnelle, les données et les applications SaaS afin d'éliminer les menaces liées à l'identité. Avec l'autorisation intelligente, Delinea fournit la seule plateforme qui vous permet de découvrir toutes les identités, d'attribuer les niveaux d'accès appropriés, de détecter les irrégularités et de répondre immédiatement aux menaces liées à l'identité en temps réel. Delinea accélère l'adoption par vos équipes en déployant les solutions en quelques semaines, et non en quelques mois, et les rend plus productives en nécessitant 90% de ressources en moins à gérer que le concurrent le plus direct. Avec un temps de fonctionnement garanti de 99,99%, Delinea Platform est la solution de sécurité de l'identité la plus fiable du marché. Pour en savoir plus sur Delinea, consultez nos pages [LinkedIn](#), [X](#) et [YouTube](#).



### Simplifiez l'administration des accès à privilèges

Les capacités partagées sur Delinea Platform simplifient la gestion des accès à privilèges avec des fonctionnalités intégrées qui facilitent le déploiement et l'administration.

Les capacités cloisonnées de la gestion des accès à privilèges et le nombre croissant d'identités ayant accès aux actifs critiques de l'entreprise deviennent de plus en plus difficiles à gérer. Les fonctionnalités partagées éliminent les processus fastidieux d'administration des accès à privilèges.

- **Rationalisez l'administration** Les capacités partagées améliorent l'efficacité opérationnelle et la productivité à mesure que vous adoptez et perfectionnez vos contrôles PAM.
- **Réduisez la complexité** L'utilisation des services de découverte, d'audit, d'analyse, de surveillance et d'application de la MFA permet de réduire la complexité et de simplifier la gestion.
- **Vue unifiée** Une ligne de vue claire sur les activités à privilèges et les contrôles d'accès dans votre environnement permet d'atténuer les risques, de prouver la conformité et d'augmenter la productivité.