

# Continuous Identity Discovery

Identifiez les risques cachés lors de votre déploiement PAM

Dans les environnements de cloud public dynamiques, de nouveaux comptes et identités ayant accès à des données et systèmes sensibles sont continuellement créés, étendus et modifiés. Les meilleures pratiques traditionnelles de gestion des identités et des accès, telles que l'authentification multi-facteurs et la sauvegarde des informations d'identification administratives, sont souvent ignorées au profit de l'agilité et de la rapidité. Les cybercriminels le savent, c'est pourquoi les comptes administratifs cloud sont des cibles privilégiées pour les attaques.

Continuous Identity Discovery vous aide à localiser et sécuriser les informations d'identification à privilèges dans des environnements hybrides complexes. Il analyse en permanence les fournisseurs de services cloud, tels que Google Cloud Platform (GCP), Amazon Web Services (AWS) et Microsoft Azure, ainsi que les fournisseurs d'identité (IdP), comme Okta, Ping, Entra et Active Directory (AD) sur site, pour découvrir de nouveaux comptes, des changements dans les privilèges administratifs existants et des administrateurs fictifs. Il analyse le paysage des identités décentralisées pour corréliser les données de compte à travers plusieurs fournisseurs d'identité et de services cloud, offrant ainsi une vue complète des comptes à privilèges au sein de votre organisation. Il suggère ensuite des options de correction automatisées qui incluent le stockage des informations d'identification avec Secret Server pour alléger la charge informatique et réduire le risque d'attaques basées sur les informations d'identification.

## COMMENT CELA FONCTIONNE

### ✓ Connecter

Connectez votre infrastructure de cloud public et vos IdP avec une API facile à utiliser et non des scripts, pour une intégration d'AD sur site à l'aide du moteur Delinea Platform.

### ✓ Découvrir

Analysez et découvrez en continu les comptes à privilèges dans plusieurs environnements cloud et sur site, surmontant ainsi un environnement complexe et en constante évolution.

### ✓ Analyser

Évaluez les comptes découverts en temps réel. Le filtrage avancé et l'analyse étendue des droits signalent les comptes à privilèges non protégés, vous permettant ainsi de remédier aux risques en matière de sécurité.

### ✓ Remédier

Sécurisez les informations d'identification des comptes à privilèges dans Secret Server, automatiquement ou à votre discrétion, à l'aide d'une interface utilisateur commune pour mieux protéger votre organisation et réduire le risque global.

## Avantages de Continuous Identity Discovery



### LIMITEZ LE RISQUE

Sécurisez et mettez vos informations d'identification en coffre-fort en toute tranquillité d'esprit, sachant que vous avez une visibilité complète sur vos comptes cloud à privilèges auprès de plusieurs fournisseurs de services cloud et fournisseurs d'identité.



### AMÉLIOREZ L'EFFICACITÉ OPÉRATIONNELLE

Analysez en continu vos CSP, vos IdP cloud et votre AD, découvrez les vecteurs d'attaque potentiels et corrigez-les avant qu'ils ne deviennent un problème, sans intervention lourde de votre équipe IT.



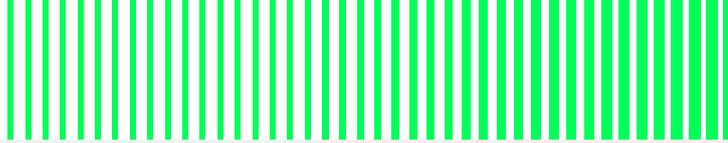
### TIREZ PARTI DE VOS INVESTISSEMENTS

Tirez le meilleur parti de votre investissement dans Secret Server en exploitant la même plateforme et la même interface utilisateur pour gérer tous les comptes à privilèges de votre organisation.



### HARMONISEZ L'ADMINISTRATION

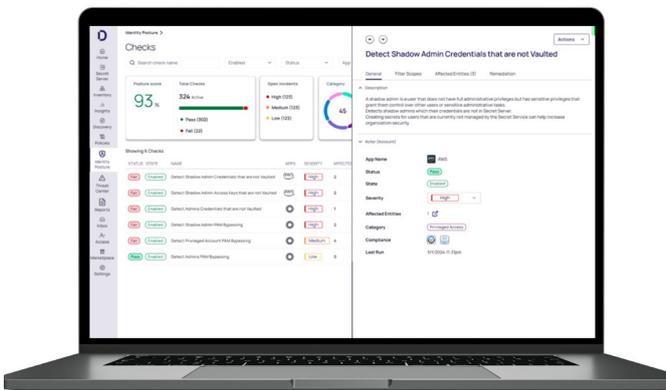
Assurez une rentabilité rapide et réduisez le coût total de possession grâce à une vue exhaustive des identités sur la plateforme cloud-native Delinea Platform.



# Continuous Identity Discovery offre une protection des informations d'identification de bout en bout

La gestion des accès à privilèges (PAM) sécurise les informations d'identification des utilisateurs cloud et sur site tout en leur permettant de rester agiles. Continuous Identity Discovery améliore la découverte de Secret Server avec une visibilité plus approfondie sur les clouds publics et les fournisseurs d'identité pour découvrir et corriger les comptes à risque. Cette fonctionnalité permet également de stocker les identifiants utilisateur dans un coffre-fort numérique, garantissant ainsi la cohérence des processus et des workflows PAM à l'échelle de l'organisation.

En utilisant Delinea Continuous Identity Discovery avec Secret Server, vous pouvez voir les contrôles de posture détaillés des comptes à privilèges et apporter les modifications nécessaires, le tout dans une seule interface.



## Accélérez l'adoption du PAM

Obtenez une visibilité détaillée sur vos comptes sensibles et leurs privilèges. Découvrez les voies d'accès potentielles utilisées pour naviguer dans votre environnement cloud, tout en détectant et en mettant en coffre-fort les utilisateurs à privilèges dans Secret Server.

## Centralisez le contrôle de votre solution PAM

Réduisez le risque que des attaques liées à l'identité menées sur vos ressources dans le cloud et sur site ne parviennent à s'implanter, à obtenir un accès plus élevé ou à persévérer. Détectez les utilisateurs à privilèges accédant aux applications cloud qui contournent votre coffre-fort. Bloquez automatiquement l'accès si nécessaire.

## Améliorer l'efficacité opérationnelle

En automatisant le processus de découverte et d'analyse, votre équipe informatique et de sécurité peut se concentrer sur des initiatives stratégiques de plus haut niveau plutôt que d'exécuter des audits de routine sur les accès à privilèges.

## Une plateforme adaptée à chaque type d'entreprise

### DELINEA PLATFORM Essentials



Commencez par identifier, gérer et mettre en coffre-fort les comptes à privilèges, avec la possibilité de définir des règles pour demander l'accès aux informations d'identification et pour surveiller et auditer les sessions d'accès à privilèges à distance.

### DELINEA PLATFORM Standard



Continuez votre parcours PAM en vous protégeant contre les menaces liées à l'identité, en attribuant juste-à-temps de privilèges juste-à-temps et en appliquant en profondeur l'authentification multi-facteurs.

### DELINEA PLATFORM Enterprise



Augmentez l'automatisation et l'intelligence de vos politiques d'autorisation pour réduire davantage les risques liés à l'identité et améliorer la productivité.

Pour en savoir plus sur Delinea Continuous Identity Discovery, visitez [Privilege Control for Cloud Entitlements](#) et Delinea Secret Server en visitant [Secret Server, solution PAM hautement performante sur site ou dans le cloud.](#)

## Delinea

Delinea est un pionnier dans la sécurisation des identités humaines et machines en proposant une autorisation intelligente et centralisée, permettant aux organisations de régir de manière intuitive leurs interactions au sein de l'entreprise moderne. S'appuyant sur l'intelligence alimentée par l'IA, Delinea Platform, la plateforme cloud-native de sécurité de l'identité de Delinea, applique le contexte tout au long du cycle de vie de l'identité sur l'infrastructure cloud et traditionnelle, les données, les applications SaaS et l'IA. C'est la seule plateforme qui vous permet de découvrir toutes les identités (y compris celles du personnel, de l'administrateur IT, des développeurs et des machines), d'attribuer des niveaux d'accès appropriés, de détecter les irrégularités et de répondre aux menaces en temps réel. Avec un déploiement en quelques semaines et non en quelques mois, 90 % de ressources en moins à gérer par rapport au concurrent le plus proche et une disponibilité de 99,995 %, Delinea Platform offre une sécurité robuste et une efficacité opérationnelle sans complexité. Pour en savoir plus sur Delinea, consultez nos pages [Delinea.com/fr](#), [LinkedIn](#), [X](#), et [YouTube](#).