Delinea

# Gestion des droits d'accès à l'infrastructure cloud (CIEM)

## Guide de l'acheteur

# Gestion des droits d'accès à l'infrastructure cloud (CIEM)

Suite à la transformation du cloud, les données sensibles sont désormais dispersées dans toute l'entreprise. Les services cloud sont créés rapidement, bien souvent hors du contrôle informatique central. En outre, pratiquement toutes les entreprises combinent des ressources sur site et dans le cloud, souvent réparties entre plusieurs centres de données et fournisseurs de services cloud (CSP). Malheureusement, les erreurs de configuration sont courantes, ce qui génère des vulnérabilités pour les identités ou des niveaux d'accès trop élevés, avec le risque d'exposer les informations sensibles.

Les cybercriminels profitent de la situation actuelle pour attaquer les ressources cloud. Le plus souvent, ils usurpent des identités authentifiées, exploitent les autorisations pour obtenir et élever l'accès, et atteignent leurs objectifs malveillants.

Vous ne pouvez pas protéger vos ressources cloud contre de telles attaques basées sur l'identité en utilisant les mêmes stratégies que vous le feriez dans un environnement sur site. Il est incroyablement difficile de suivre le chemin d'attaque potentiel ou réel d'une identité unique dans un environnement aussi distribué, dynamique et incohérent. Les outils traditionnels (pare-feu de réseau, services d'annuaire d'entreprise communs et contrôles d'accès statiques) ne sont pas efficaces dans la réalité du cloud.

C'est pourquoi, face à la prolifération des attaques basées sur les identités, la gestion des droits d'accès à l'infrastructure cloud (CIEM) s'est imposée comme une solution incontournable pour les organisations. La CIEM relie les points de la couche des identités afin que vous puissiez comprendre et contrôler qui a accès à quoi, surveiller les comportements et réagir rapidement pour contenir les menaces.

Si vous êtes responsable de la sécurité du cloud, de l'architecture du cloud ou de la gestion des identités et des accès (IAM) et que vous vous demandez comment les solutions CIEM peuvent s'intégrer dans votre feuille de route en matière de sécurité, ce guide est fait pour vous.

Les informations qu'il contient vous aideront à :

- Comprendre les cas d'utilisation de la CIEM
- Gagner du temps en préparant les conversations avec les fournisseurs CIEM en fournissant une liste de questions à poser lors de l'évaluation des solutions potentielles.
- Comparer les options et choisir la solution CIEM la mieux adaptée à vos besoins
- Évaluer la CIEM dans le contexte de votre stratégie globale de sécurité des identités

# Impact du cloud sur la sécurité des identités

Dans un environnement cloud, la sécurité des identités s'avère beaucoup plus complexe à gérer, pour plusieurs raisons :

**Contrôle distribué :** Au lieu d'un petit groupe d'administrateurs, de nombreux utilisateurs et systèmes ont accès aux données et aux ressources et peuvent même générer des identités.

**Prolifération des rôles :** Le nombre de rôles et d'autorisations a explosé. Il est donc difficile de les gérer et de les comprendre sans outils spécialisés.

**Erreurs de configuration :** Les groupes mal configurés dans les systèmes de gestion des identités et/ou les ressources cloud peuvent entraîner des risques.

**Lacunes en matière de visibilité :** La combinaison de différents fournisseurs d'identité, applications/services fédérés et utilisateurs CSP locaux a pour effet de restreindre la surveillance des identités et de limiter la compréhension des comportements dans les environnements cloud.

**Complexité des autorisations dans le cloud :** Les environnements cloud modernes comportent des modèles d'autorisations complexes avec des milliers d'autorisations possibles sur de nombreux services. Il est facile d'accorder par erreur des autorisations trop élevées, ce qui conduit à des autorisations excessives et risquées.

**Dérive des privilèges :** Beaucoup trop d'identités ont plus de privilèges que nécessaire, ce qui va à l'encontre des meilleures pratiques du moindre privilège et du Zero Trust.

**Changement constant :** Les environnements cloud connaissent des évolutions rapides avec de nouvelles identités (en particulier les identités machines) créées en permanence et des droits provisionnés et supprimés à une vitesse vertigineuse. En raison de la nature dynamique des environnements cloud, la remédiation manuelle des problèmes d'autorisation n'est pas modulable.

> La CIEM relie les points de la couche des identités afin que vous puissiez comprendre et contrôler qui a accès à quoi, surveiller les comportements et réagir rapidement pour contenir les menaces. »

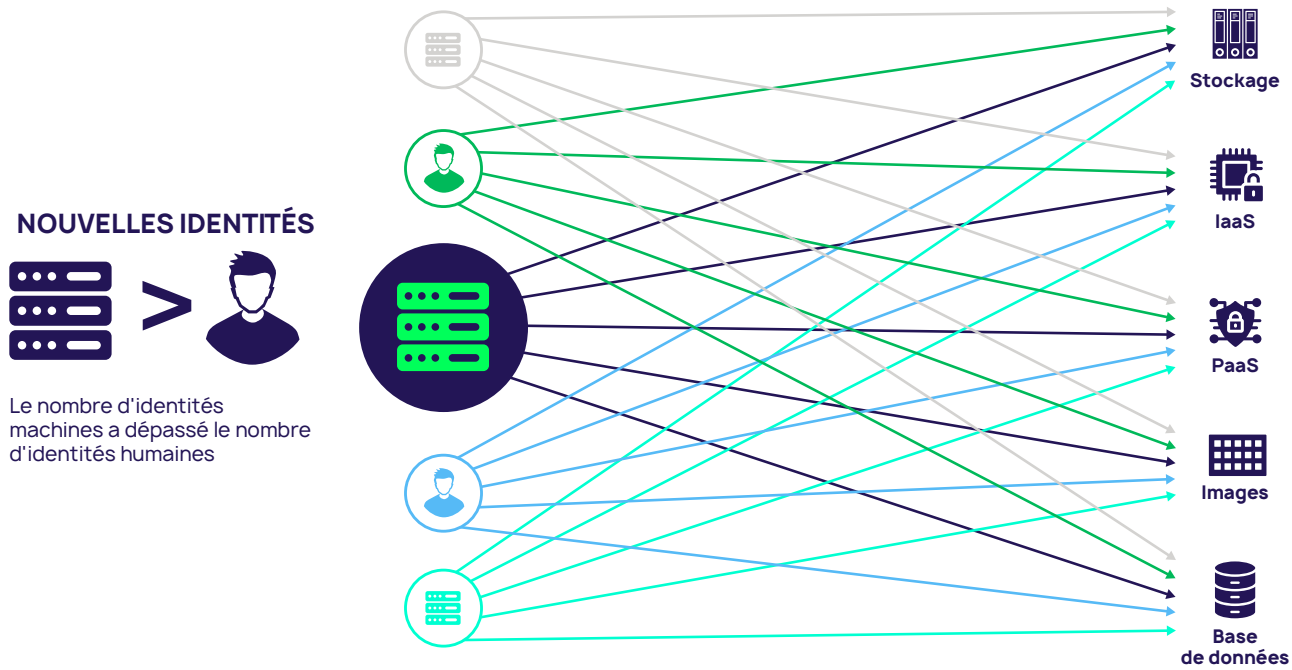
# Gestion des droits d'accès à l'infrastructure cloud (CIEM)

La CIEM est le processus de gestion des identités et de leurs privilèges dans les environnements cloud. L'objectif de la CIEM est de comprendre quels droits d'accès existent dans les environnements cloud et multi-cloud, puis d'identifier et d'atténuer les risques résultant des droits qui accordent un niveau d'accès plus élevé qu'ils ne le devraient.

La CIEM vous aide à réduire ces risques d'attaques basées sur l'identité en appliquant des contrôles préventifs pour la gouvernance des droits dans les environnements hybrides et multi-cloud IaaS (Identity-as-a-Service, identité en tant que service) et PaaS (Platform-as-a-Service, plateforme en tant que service). Grâce à l'analyse et à l'apprentissage automatique (ML), la CIEM surveille en permanence les identités, les autorisations et les activités. Elle détecte les anomalies dans les droits des comptes, telles que l'accumulation de privilèges, les autorisations dormantes et les comptes ou rôles inutilisés. En appliquant le principe du moindre privilège, la CIEM contribue à garantir que les identités ont accès uniquement à ce dont elles ont besoin et à réduire au minimum votre surface d'attaque.

Contrairement à d'autres solutions de sécurité cloud telles que les plateformes de protection des applications cloud-native (CNAPP), les solutions CIEM se concentrent sur les risques liés aux identités. Idéalement, les solutions CIEM font partie intégrante de votre processus de création d'identité et de gouvernance du cycle de vie.

FIGURE 1 | Le nombre d'identités dans un compte cloud multiplié par le nombre de droits de chaque identité constitue une surface d'attaque massive.



# Quatre utilisations principales des solutions CIEM

## 1 Offrir une visibilité sur les droits à risque

La CIEM offre une visibilité granulaire sur les identités humaines et non humaines, les actifs sensibles et les droits. Elle indique « l'accès effectif » de chaque identité en découvrant les voies d'accès potentielles qu'elle peut utiliser pour naviguer dans votre environnement informatique. La détection des droits dormants et excessifs est une fonction centrale des solutions CIEM (également connue sous le nom de gestion des autorisations ou d'audit des autorisations).

## 2 S'assurer que les contrôles fonctionnent comme prévu

CIEM vous aide à garantir que les contrôles de sécurité appropriés des authentifications et des autorisations sont en place et efficaces. Grâce à la CIEM, vous pouvez réduire les possibilités d'attaques liées aux identités pour obtenir un point d'ancrage, un accès plus élevé ou une persistance.

## 3 Détection des anomalies comportementales

La CIEM vous aide à détecter les événements de cybersécurité. Elle recueille des données significatives en surveillant en permanence les identités et leur comportement, et en fournissant le contexte essentiel à la compréhension de ces informations. L'apprentissage automatique enrichit l'analyse historique des identités avec des données comportementales, garantissant que les droits accordés répondent à un besoin réel et nécessaire.

## 4 Remédier aux risques liés aux identités

La remédiation automatique des risques est une fonction essentielle des solutions CIEM. Lorsqu'un risque est détecté, la CIEM recommande un ajustement de la politique ou déclenche un workflow. Par exemple, la CIEM peut traiter les droits excessifs en supprimant les privilèges dormants, elle peut corriger la dérive de la politique en réduisant les privilèges et déclencher des actions pour corriger les erreurs de configuration.

Dans la section suivante, vous trouverez des questions à poser à tout fournisseur de solution CIEM sur chacun de ces cas d'utilisation dans le cadre de votre évaluation des fournisseurs.

# Questions à poser aux fournisseurs de solutions CIEM

## 1. Offrir une visibilité sur les droits à risque

Votre fournisseur d'identité (IdP) ne peut pas vraiment comprendre les droits de vos CSP. Des angles morts se forment en raison de la prolifération normale des privilèges, des utilisateurs créés en dehors de votre IdP (c'est-à-dire par des administrateurs locaux ou des identités externes), des privilèges accordés via une appartenance à un groupe invisible, entre autres. La CIEM comble ces lacunes en fournissant les informations manquantes sur l'état et l'utilisation de facto des privilèges.

Ces capacités CIEM jettent les bases de vos mesures de cybersécurité en offrant une visibilité complète de votre surface d'attaque au niveau des identités.

| Capacités de la CIEM | Questions à poser à un fournisseur de CIEM |
|---|---|
| **Découvrir les identités humaines** | Prenez-vous en charge plusieurs IdP (Okta, Azure Active Directory, PingOne, etc.) ?<br>Pouvez-vous vous connecter aux systèmes des ressources humaines pour suivre les changements JML (Joiner-Mover-Leaver, Nouvelles recrues - Changements de poste - Départs) et les départs partiels ? |
| **Découvrir les identités machines** | Pouvez-vous découvrir les identités machines telles que les API et les charges de travail ? |
| **Découvrir les identités fédérées** | Pouvez-vous découvrir les identités fédérées générées en externe et reliées à votre IdP via un échange de jetons ?<br>Pouvez-vous lier l'activité dans AWS aux utilisateurs fédérés afin que je puisse les suivre ? |
| **Découvrir tous les services et applications cloud critiques et leur état actuel** | Votre offre inclut-elle IaaS et PaaS ?<br>Quels fournisseurs de services cloud prenez-vous en charge ?<br>Pouvez-vous détecter les dossiers sensibles qui sont accessibles au public ?<br>Qu'en est-il de nos systèmes hérités ? |
| **Découvrir les autorisations et les privilèges pour tous les types d'identités** | Pouvez-vous montrer quelles autorisations sont accordées à qui et comment dans une vue centralisée ?<br>Pouvez-vous fournir une visibilité granulaire, au niveau des fichiers, des autorisations d'accès ?<br>Pouvez-vous détecter les identités humaines et machines dont les privilèges sont trop élevés ?<br>Comment découvrir les privilèges cachés accordés par des groupes, les voies d'élévation des privilèges et les erreurs de configuration ?<br>Pouvez-vous me montrer les sous-traitants qui conservent l'accès à des actifs avec leurs propres identités ? |
| **Fusionner les identités** | Pouvez-vous fusionner les identités, y compris celles qui ne figurent pas dans notre IdP mais qui ont accès à nos actifs ? |
| **Découverte continue** | Comment le système découvre-t-il les nouvelles identités et les nouveaux actifs au fur et à mesure qu'ils sont créés, afin qu'ils puissent être rapidement pris en charge ? |
| **Découvrir les identités dormantes et les privilèges permanents** | Comment déterminez-vous si une identité ou un accès à privilèges n'est plus nécessaire ?<br>Pouvez-vous montrer l'utilisation des privilèges d'accès, en détectant les privilèges inutilisés sur des périodes données ? |

| Capacités de la CIEM | Questions à poser à un fournisseur de CIEM |
|---|---|
| **Découvrir l'efficacité des accès dans les différents environnements** | Comment tracez-vous les chemins et autorisations d'accès dans les différents systèmes et environnements (sur site et multi-cloud) ?<br>Offrez-vous une visibilité de bout en bout, de l'IdP à l'actif ?<br>Pouvez-vous me montrer des voies d'élévation des privilèges tels que le chaînage de rôles, l'octroi d'un accès temporaire aux ressources, dans Amazon Web Services ?<br>Comment créez-vous des visualisations des chemins d'accès pour qu'ils soient faciles à comprendre instantanément ? |
| **Évaluation des risques** | Pouvez-vous identifier les identités à haut risque sur la base de l'accès effectif ?<br>Pouvez-vous fournir des scores de risque pour les utilisateurs en fonction de l'ensemble des accès ?<br>Pouvez-vous regrouper les paramètres de risque et la threat intelligence sur les menaces dans un score de risque d'identité unifié et dynamique ? |

## 2. S'assurer que les contrôles fonctionnent comme prévu

La protection de votre surface de menace des identités contre les attaques commence par la réduction des risques avant qu'ils ne puissent être exploités par un attaquant. Il est fort probable que votre organisation ait déjà mis en place des contrôles des identités. Cependant, êtes-vous sûr qu'ils fonctionnent comme prévu et que rien n'est passé entre les mailles du filet ?

Ces capacités CIEM vous aident à vous assurer que les contrôles de sécurité préventifs fonctionnent efficacement pour contenir l'impact potentiel des attaques basées sur les identités. Les principaux domaines d'intérêt sont l'application du principe du moindre privilège et la limitation des voies d'élévation des privilèges, car ils empêchent les attaquants ayant compromis une identité d'obtenir les privilèges dont ils ont besoin pour atteindre leurs objectifs.

| Capacités de la CIEM | Questions à poser à un fournisseur de CIEM |
|---|---|
| **Prise en charge de l'authentification** | Pouvez-vous me montrer quelles identités privilégiées ont une authentification multi-facteurs (MFA) activée, et à quel niveau ?<br>Pouvez-vous découvrir et corriger les erreurs de configuration de l'IAM ?<br>Pouvez-vous détecter les erreurs de configuration à risque qui nous exposeraient à des fuites de mots de passe en texte clair ou à des usurpations d'identité ? |
| **Prise en charge des autorisations** | Pouvez-vous me montrer comment les utilisateurs accèdent aux actifs via l'appartenance à un groupe (par exemple : groupes imbriqués, groupes publics) ?<br>Comment limitez-vous les accès à privilèges ?<br>Comment éliminez-vous les voies d'élévation des privilèges pour contenir les attaques ? |

## 3. Détection des anomalies comportementales

En raison la complexité et du manque de visibilité du cloud, la détection des voies et événements d'élévation des privilèges peut s'avérer extrêmement délicate. La CIEM vous aide à découvrir les attaques basées sur les identités en cours, notamment les tentatives d'accès initial avec des informations d'identification compromises ou d'élévation des privilèges si les attaquants sont déjà à l'intérieur.

| Capacités de la CIEM | Questions à poser à un fournisseur de CIEM |
|---|---|
| **Détection des tactiques, techniques et procédures (TTP)** | Pouvez-vous détecter les attaques par MFA bombing ?<br>Pouvez-vous détecter les attaques par force brute ?<br>Pouvez-vous détecter les échecs de tentatives de connexion par bourrage d'informations d'identification dans plusieurs applications, ce qui pourrait indiquer des attaques connexes sur une identité ?<br>Pouvez-vous détecter le détournement de session ? |
| **Activité suspecte** | Pouvez-vous détecter la création de nouvelles identités privilégiées ?<br>Pouvez-vous détecter les comptes dormants qui redeviennent actifs ?<br>Pouvez-vous détecter les élévations inattendues/non souhaitées des privilèges ?<br>Pouvez-vous détecter la connexion de nouvelles sources de données d'identité en amont, telles que des IdP supplémentaires ou des applications RH ?<br>Pouvez-vous détecter les erreurs de configuration malveillantes nouvellement créées au niveau de l'IdP ?<br>Pouvez-vous détecter les modifications apportées par les utilisateurs aux journaux de notre IdP qui peuvent indiquer qu'ils cachent leur activité ? |
| **Surveillance de l'utilisation** | Pouvez-vous fournir une base d'activité pour déterminer l'utilisation normale des droits d'un utilisateur, afin que nous sachions quand un comportement hors norme se produit ?<br>La surveillance est-elle continue ? |
| **Flexibilité** | Comment allez-vous m'aider à étendre mes capacités de détection existantes à de nouveaux IdP et à de nouvelles applications lors de ma prochaine fusion-acquisition ? Décrivez-moi votre flexibilité pour modifier le champ d'application ou ajouter des politiques de détection pour l'entreprise nouvellement acquise ou ses utilisateurs. |

# 4. Réduction des risques et remédiation

En raison de l'impact potentiel sur l'entreprise des changements de privilèges d'accès, la remédiation peut être une tâche délicate à entreprendre. La CIEM fournit des informations et des recommandations exploitables sur la façon de réduire les risques en fonction du contexte et de facteurs tels que l'accès effectif d'une identité, le comportement privilégié et le rayon d'action potentiel d'une attaque.

| Capacités de la CIEM | Questions à poser à un fournisseur de CIEM |
|---|---|
| **Dimensionnement** | Pouvez-vous fournir des recommandations sur le dimensionnement des identités et des autorisations ?<br>Comment fournissez-vous le contexte permettant de comprendre comment procéder au dimensionnement adéquat ? |
| **Évaluation des risques** | Pouvez-vous identifier les identités à haut risque sur la base de l'accès effectif ?<br>Pouvez-vous fournir des scores de risque pour les utilisateurs en fonction de l'ensemble des accès ?<br>Pouvez-vous regrouper les paramètres de risque et la threat intelligence sur les menaces dans un score de risque d'identité unifié et dynamique ?<br>Puis-je ajuster les formules de score de risque des alertes que vous fournissez ? |
| **Alertes** | Comment vous intégrez-vous à mes outils de sécurité, tels que mon SIEM, pour la surveillance, l'analyse et les alertes ?<br>Pouvez-vous envoyer des webhooks ou ouvrir des tickets dans des systèmes de workflow informatique tels que JIRA ou ServiceNow ? |
| **Création de politiques** | Pouvez-vous créer de nouvelles politiques pour les autorisations ou les rôles ? |
| **Refactorisation** | Pouvez-vous refactoriser automatiquement les autorisations AWS/Azure/GCP pour qu'elles soient plus sécurisées en fonction de l'utilisation réelle ? |
| **Mesures d'atténuation** | Pouvez-vous automatiser les alertes aux utilisateurs pour qu'ils changent de mot de passe lorsque leurs informations d'identification sont compromises ?<br>Pouvez-vous déconnecter automatiquement les utilisateurs des sessions en cours pour éviter les attaques par détournement de jetons volés ?<br>Pouvez-vous imposer une MFA supplémentaire à l'utilisateur lorsqu'il effectue une activité suspecte ou privilégiée ? Ou en fonction de l'évolution de son niveau de risque d'identité ?<br>Pouvez-vous supprimer les accès tiers ?<br>Pouvez-vous ajuster dynamiquement l'accès conditionnel en fonction du niveau de risque ?<br>Pouvez-vous automatiser les workflows de remédiation ? |

# Le partenariat est également important

Pour choisir le bon fournisseur, il est essentiel d'avoir la certitude que votre relation sera établie sur le long terme. Un véritable partenaire doit comprendre votre stratégie de sécurité des identités et vous aider à atteindre vos objectifs, et pas seulement vous vendre un outil CIEM.

Le fait est que la CIEM à elle seule ne peut pas faire grand-chose pour améliorer la sécurité de vos identités. L'intégration de la CIEM dans le processus de gouvernance des identités de bout en bout permet aux systèmes de communiquer entre eux, tout comme les individus. La CIEM rassemble les équipes de sécurité, d'IAM et des opérations informatiques car elles disposent d'une image complète et précise des identités et des accès dans le cloud, d'une compréhension commune des risques et d'étapes claires pour y remédier.

Recherchez un fournisseur qui comprend tous vos besoins en matière d'identité, et qui peut vous fournir les résultats que vous attendez dans les meilleurs délais. Pour éviter les mauvaises surprises, posez d'emblée les questions suivantes aux fournisseurs.

| Capacités du fournisseur | Questions à poser à un fournisseur de CIEM |
|---|---|
| **Temps de valorisation** | Combien de temps prend le déploiement ?<br>Puis-je voir des résultats fonctionnels dans un délai de 1 à 2 jours ?<br>Comment allez-vous m'aider à réduire le temps de réponse aux incidents ? |
| **Sécurité opérationnelle** | De quels connecteurs natifs disposez-vous ?<br>Avez-vous une API ouverte ?<br>Est-il nécessaire d'écrire des scripts pour faire fonctionner votre solution ?<br>Qu'attendez-vous de ma part pour le déploiement ou l'intégration ?<br>Puis-je ajuster les politiques de sécurité pour suivre et alerter sur les comptes à risque sans avoir besoin de services professionnels ou de développer de nouvelles fonctionnalités ?<br>Proposez-vous votre solution via une plateforme SaaS, ainsi que d'autres services de gestion des privilèges et des identités, que nous pouvons utiliser pour développer notre programme ? |
| **Soutien stratégique** | Comment voyez-vous la CIEM s'intégrer dans ma stratégie globale de sécurité des identités ?<br>Comment pouvez-vous m'aider à aligner les équipes ? |
| **Réactivité** | Allez-vous décrocher le téléphone lorsque j'ai des questions ou des demandes relatives aux fonctionnalités ?<br>Votre documentation technique est-elle facilement accessible ?<br>Un success manager me sera-t-il dédié ?<br>Puis-je avoir un aperçu de votre feuille de route ? |

# À propos de Privilege Control for Cloud Entitlements de Delinea

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.

Découvrez et visualisez en permanence toutes les identités, tous les comptes et leurs accès dans les cloud Google, Amazon et Microsoft pour identifier les comportements anormaux et refactoriser les privilèges. Cloud-native, la plateforme Delinea Platform vous permet d'intégrer les droits d'accès au cloud dans votre source unique de vérité pour les autorisations de toutes les identités. Gagnez du temps en automatisant la découverte et le déprovisionnement des comptes locaux et fédérés obsolètes sans impact sur les équipes informatiques.

Pour en savoir plus, rendez-vous sur notre site Web https://delinea.com/fr/products/privilege-control-for-cloud-entitlements . Découvrez une démonstration interactive de Delinea Privilege Control for Cloud Entitlements en action.

Delinea

Securing identities at every interaction

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**, **Twitter** et **YouTube**.