Delinea

# Cloud Infrastructure Entitlement Management (CIEM)

## Guida all'acquisto

GUIDA ALL'ACQUISTO

# Guida all'acquisto delle soluzioni Cloud Infrastructure Entitlement Management (CIEM)

Come risultato della trasformazione del cloud, ora i dati sensibili sono dispersi in tutta l'azienda. I servizi cloud vengono creati rapidamente, molte volte al di fuori del controllo dell'ufficio IT centrale. Inoltre, praticamente tutte le aziende dispongono di un mix di risorse on-premise e cloud, spesso distribuite tra data center e più fornitori di servizi cloud (CSP). Purtroppo, le configurazioni errate sono un problema diffuso: esse rendono le identità vulnerabili alla compromissione o forniscono un accesso eccessivo, con il rischio di esporre dati sensibili.

I criminali informatici approfittano di questa situazione per attaccare le risorse cloud. Nella maggior parte dei casi, impersonano identità autenticate e sfruttano le autorizzazioni per ottenere ed aumentare i privilegi d'accesso e raggiungere così i loro obiettivi dannosi.

Non è possibile proteggere le risorse cloud da attacchi basati sull'identità come questi, utilizzando le stesse strategie che si adotterebbero in una realtà on-premise.
È incredibilmente difficile tracciare il percorso di attacco potenziale o effettivo di una singola identità in un ambiente così distribuito, dinamico e non omogeneo. Gli strumenti tradizionali (firewall di rete, servizi di directory aziendali comuni e controlli di accesso statici) non sono efficaci nella realtà del cloud.

Pertanto, in risposta all'escalation di attacchi basati sull'identità, le aziende hanno identificato la gestione dei diritti dell'infrastruttura cloud (Cloud Infrastructure Entitlement Management o CIEM) come soluzione di sicurezza indispensabile. Le soluzioni CIEM collegano i punti a livello di identità in modo da comprendere e controllare chi ha accesso a cosa, monitorare i comportamenti e reagire rapidamente per contenere le minacce.

Se siete responsabili della sicurezza cloud, dell'architettura cloud o della gestione delle identità e degli accessi (IAM) e state valutando in che modo le soluzioni CIEM possono adattarsi alla vostra roadmap di sicurezza, questa guida fa al caso vostro.

Le informazioni contenute in questa guida vi aiuteranno a:

- Comprendere i casi d'uso delle soluzioni CIEM
- Risparmiare tempo nella preparazione delle conversazioni con i fornitori CIEM grazie a un elenco di domande da porre quando si valutano le potenziali soluzioni
- Confrontare le opzioni e scegliere la soluzione CIEM più adatta alle vostre esigenze
- Valutare le soluzioni CIEM nel contesto della vostra strategia complessiva di sicurezza delle identità

# Impatto del cloud sulla sicurezza delle identità

In un ambiente cloud, la sicurezza delle identità diventa molto più complessa da gestire, per diversi motivi:

**Controllo distribuito:** Invece di un piccolo gruppo di amministratori, numerosi utenti e sistemi hanno accesso a dati e risorse e possono persino generare identità.

**Proliferazione dei ruoli:** Il numero di ruoli e autorizzazioni è aumentato in modo esponenziale. Ciò rende difficile gestirli e comprenderli senza strumenti specializzati.

**Errori di configurazione:** I gruppi configurati in modo errato nei sistemi di gestione delle identità e/o nelle risorse cloud espongono involontariamente a rischi.

**Lacune nella visibilità:** Un mix di diversi provider di identità, app/servizi federati e utenti CSP locali limitano il monitoraggio delle identità e la comprensione del comportamento in un ambiente cloud.

**Complessità delle autorizzazioni cloud:** I moderni ambienti cloud dispongono di modelli di autorizzazione complessi con migliaia di possibili autorizzazioni su numerosi servizi. È facile concedere erroneamente autorizzazioni eccessive, aumentando i fattori di rischio.

**Accumulo di privilegi:** Troppe identità hanno più privilegi del necessario e questo viola i principi del privilegio minimo e delle migliori prassi zero trust.

**Cambiamento costante:** Gli ambienti cloud subiscono rapidi cambiamenti con la costante creazione di nuove identità (in particolare identità a utenti artificiali) e l'assegnazione e la revoca diritti a velocità vertiginosa. La natura dinamica degli ambienti cloud rende non scalabile la riparazione manuale dei problemi di autorizzazione.

> Le soluzioni CIEM collegano i punti a livello di identità in modo da comprendere e controllare chi ha accesso a cosa, monitorare i comportamenti e reagire rapidamente per contenere le minacce."

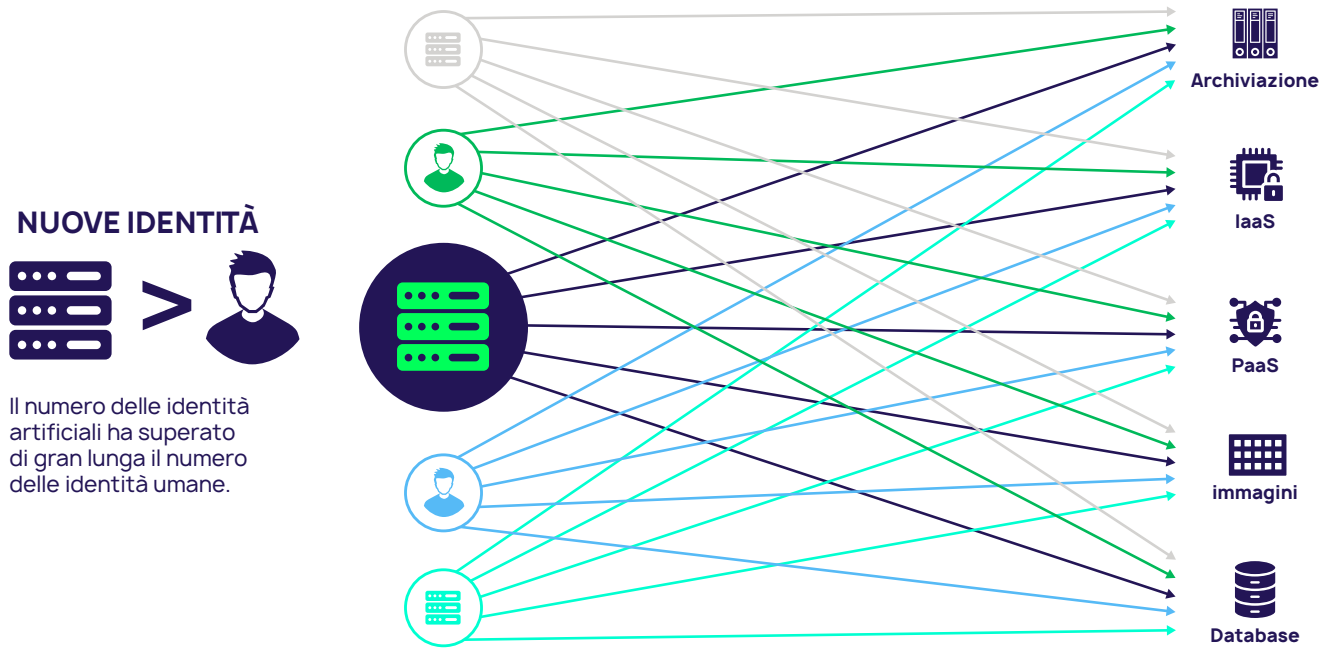
# Cloud Infrastructure Entitlement Management (CIEM)

Con CIEM si intende il processo di gestione delle identità e dei relativi privilegi negli ambienti cloud. Lo scopo del CIEM è comprendere quali diritti di accesso esistono negli ambienti cloud e multi-cloud, quindi identificare e mitigare i rischi derivanti da diritti che garantiscono un livello di accesso più elevato di quanto dovrebbero.

Le soluzioni CIEM vi aiutano a ridurre questi rischi di attacchi basati sulle identità applicando controlli preventivi per la governance dei diritti in ambienti Identity-as-a-Service (IaaS) e Platform-as-a-Service (PaaS) ibridi e multi-cloud. Utilizzando analisi e machine learning (ML), le soluzioni CIEM monitorano continuamente identità, autorizzazioni e attività. Rilevano anomalie nei diritti degli account, come l'accumulo di privilegi, autorizzazioni dormienti e account o ruoli inutilizzati. Applicando il principio del privilegio minimo, una soluzione CIEM aiuta a garantire che le identità abbiano accesso solo a ciò di cui hanno bisogno e riduce al minimo la superficie di attacco.

A differenza di altre soluzioni di sicurezza cloud come le piattaforme di protezione delle applicazioni cloud-native (CNAPP), le soluzioni CIEM si concentrano sul rischio delle identità. Idealmente, sono un componente integrato nel processo di creazione dell'identità e di governance del ciclo di vita.

FIGURA 1 | Il numero di identità in un account cloud moltiplicato per il numero di diritti di cui ciascuna identità dispone costituisce una superficie di attacco enorme.



# Quattro usi principali delle soluzioni CIEM

## 1 Fornire visibilità sui diritti rischiosi

Le soluzioni CIEM forniscono visibilità granulare su identità umane e non umane, risorse sensibili e diritti. Mostrano l'accesso effettivo per ciascuna identità attraverso la scoperta di potenziali percorsi di accesso che un'identità potrebbe utilizzare per navigare nel vostro ambiente IT. Il rilevamento dei diritti dormienti ed eccessivi è una funzione centrale nelle soluzioni CIEM (nota anche come gestione delle autorizzazioni o auditing delle autorizzazioni).

## 2 Garantire che i controlli funzionino come previsto

Le soluzioni CIEM contribuiscono a garantire che i giusti controlli di sicurezza per l'autenticazione e l'autorizzazione siano presenti ed efficaci. Consentono di ridurre la possibilità che gli attacchi legati all'identità ottengano un punto d'appoggio iniziale, acquisiscano diritti d'accesso di livello superiore o la persistenza.

## 3 Rilevamento di anomalie comportamentali

Le soluzioni CIEM aiutano a individuare la presenza di un evento di sicurezza informatica. Raccolgono dati significativi monitorando continuamente le identità e il loro comportamento e fornendo il contesto essenziale per comprendere tali informazioni.
Il machine learning arricchisce l'analisi dell'identità storica con dati comportamentali, garantendo che i diritti concessi siano in linea con la necessità e l'utilizzo reali.

## 4 Risolvere le minacce relative alle identità

La riparazione automatica dei rischi è una funzionalità essenziale in una soluzione CIEM. Quando viene rilevato un rischio, la soluzione CIEM consiglierà un aggiustamento delle policy o attiverà un workflow. Ad esempio, può gestire i diritti eccessivi rimuovendo i privilegi dormienti, può correggere la deviazione dalle policy riducendo i privilegi e attivare azioni per risolvere configurazioni errate.

Nella prossima sezione troverete domande da porre a qualsiasi fornitore di soluzioni CIEM su ciascuno di questi casi d'uso come parte della valutazione del fornitore stesso.

# Domande per i fornitori di soluzioni CIEM

## 1. Fornire visibilità sui diritti rischiosi

Il vostro provider di identità (IdP) non è in grado di comprendere a fondo i diritti all'interno dei vostri CSP. La normale espansione dei privilegi, gli utenti creati al di fuori del vostro IdP (ad esempio, da amministratori locali o identità esterne), i privilegi concessi tramite l'appartenenza a gruppi invisibili e altri fattori creano punti ciechi. Una soluzione CIEM inserisce le informazioni mancanti sullo stato di fatto e sull'utilizzo dei privilegi.

Queste funzionalità CIEM gettano le basi per i vostri interventi di sicurezza informatica fornendo visibilità end-to-end della superficie di attacco delle vostre identità.

| Funzionalità CIEM | Domande da porre a un fornitore CIEM |
|---|---|
| **Scoprire le identità umane** | Supportate più IdP (Okta, Azure Active Directory, PingOne, ecc.)?<br>Offrite la possibilità di connettersi ai sistemi HR per monitorare le modifiche JML (Joiner-Mover-Leaver) e l'offboarding parziale? |
| **Scoprire le identità artificiali** | Siete in grado di individuare le identità artificiali come API e workload? |
| **Scoprire le identità federate** | Siete in grado di scoprire identità federate generate esternamente e collegate al vostro IdP tramite scambio di token?<br>È possibile collegare l'attività in AWS agli utenti federati in modo da poterli monitorare? |
| **Scoprire tutti i servizi e le app cloud critici e il loro stato attuale** | La vostra copertura include IaaS e PaaS?<br>Quali CSP supportate?<br>Siete in grado rilevare le cartelle sensibili accessibili pubblicamente?<br>Come gestite i nostri sistemi sviluppati internamente? |
| **Scoprire autorizzazioni e privilegi per tutti i tipi di identità** | Siete in grado di rappresentare in una vista centralizzata quali autorizzazioni vengono concesse a chi e come?<br>Potete fornire una visibilità granulare a livello di file delle autorizzazioni di accesso?<br>Siete in grado di individuare le identità relative a utenti umani e artificiali con privilegi eccessivi?<br>In che modo individuate i privilegi nascosti concessi tramite gruppi, percorsi di escalation dei privilegi e configurazioni errate?<br>Siete in grado mostrarci gli appaltatori che mantengono l'accesso alle risorse con le proprie identità? |
| **Unione delle identità** | È possibile unire le identità, comprese quelle non presenti nel nostro IdP ma con accesso alle nostre risorse? |
| **Individuazione continua** | In che modo il sistema scopre nuove identità e risorse man mano che vengono create per consentire di gestirle rapidamente? |
| **Scoprire identità dormienti e privilegi permanenti** | Come fate a stabilire quando un'identità o un accesso privilegiato non è più necessario?<br>Siete in grado di mostrare l'utilizzo dei privilegi di accesso, rilevando quelli non utilizzati in periodi specifici? |

| Funzionalità CIEM | Domande da porre a un fornitore CIEM |
|---|---|
| **Scoprire gli accessi effettivi a tutti gli ambienti** | Come tracciate i percorsi di accesso e le autorizzazioni ai diritti tra sistemi e ambienti (on-premise e multi-cloud)?<br>Fornite visibilità end-to-end dall'IdP alla risorsa?<br>Potete mostrarci percorsi di escalation dei privilegi come il concatenamento dei ruoli o la concessione di un accesso temporaneo alle risorse in Amazon Web Services?<br>Come vengono create visualizzazioni dei percorsi di accesso in modo che siano di facile e immediata comprensione? |
| **Valutazione del rischio** | Siete in grado di identificare le identità ad alto rischio sulla base di un accesso effettivo?<br>Siete in grado di fornire una valutazione del rischio per gli utenti in base alla totalità degli accessi?<br>È possibile aggregare i parametri di rischio e l'intelligence sulle minacce in una valutazione del rischio delle identità unificate e dinamiche? |

## 2. Garantire che i controlli funzionino come previsto

La protezione della superficie vulnerabile delle vostre identità dagli attacchi inizia con la riduzione dei rischi prima che possano essere sfruttati da un avversario. Molto probabilmente, la vostra azienda ha già implementato alcuni controlli delle identità. Tuttavia, avete la certezza che funzionino come previsto e che nulla sia passato inosservato?

Queste funzionalità CIEM vi aiutano a garantire che i controlli di sicurezza preventivi funzionino in modo efficace per contenere il potenziale raggio d'azione di un attacco basato sull'identità. Le aree di interesse principali sono l'applicazione dei privilegi minimi e il contenimento dei percorsi di escalation dei privilegi, perché negano a un hacker che ha compromesso un'identità i privilegi di cui ha bisogno per raggiungere i propri obiettivi.

| Funzionalità CIEM | Domande da porre a un fornitore CIEM |
|---|---|
| **Supporto per l'autenticazione** | Potete mostrarci quali identità privilegiate dispongono dell'autenticazione a più fattori (MFA) e a quale livello?<br>Siete in grado di identificare e correggere le configurazioni IAM errate?<br>Siete in grado di rilevare configurazioni errate rischiose che ci esporrebbero alla fuga di password in chiaro o all'impersonificazione di un utente? |
| **Supporto per l'autorizzazione** | Potete mostrarci in che modo gli utenti ottengono l'accesso alle risorse tramite l'appartenenza a gruppi (ad esempio gruppi nidificati, gruppi pubblici)?<br>Come limitate l'accesso privilegiato?<br>Come eliminate i percorsi di escalation dei privilegi per contenere gli attacchi? |

## 3. Rilevamento di anomalie comportamentali

Rilevare percorsi ed eventi di escalation dei privilegi può essere estremamente complicato nel cloud a causa della complessità e della mancanza di visibilità. Le soluzioni CIEM vi aiutano a scoprire gli attacchi basati sull'identità in corso, inclusi i tentativi di ottenere l'accesso iniziale con credenziali compromesse o di aumentare i privilegi se gli hacker sono già all'interno.

| Funzionalità CIEM | Domande da porre a un fornitore CIEM |
|---|---|
| **Tattiche, tecniche e procedure (TTP) di rilevamento** | Siete in grado di rilevare gli attacchi di MFA bombing/fatigue?<br>Siete in grado di rilevare gli attacchi di forza bruta?<br>Siete in grado di rilevare tentativi di accesso non riusciti utilizzando il credential stuffing su più applicazioni che potrebbero indicare attacchi correlati a un'identità?<br>Siete in grado di rilevare dirottamenti di sessione? |
| **Attività sospette** | Siete in grado di rilevare quando vengono create nuove identità privilegiate?<br>Siete in grado di rilevare account dormienti che diventano nuovamente attivi?<br>Siete in grado di rilevare un'elevazione o un'escalation di privilegi imprevista/indesiderata?<br>Siete in grado di rilevare la connessione di nuove origini dati di identità upstream come IdP aggiuntivi o applicazioni HR?<br>Siete in grado di rilevare configurazioni errate dannose appena create a livello di IdP?<br>Siete in grado di rilevare le modifiche apportate dagli utenti ai log nel nostro IdP che potrebbero indicare che stanno nascondendo la loro attività? |
| **Monitoraggio dell'uso** | Potete fornire attività di riferimento per determinare il normale utilizzo dei diritti da parte di un utente, in modo da sapere quando si verifica un comportamento anomalo?<br>Il monitoraggio è continuo? |
| **Flessibilità** | In che modo ci aiuterete ad estendere le nostre funzionalità di rilevamento esistenti per nuovi IdP e app in caso di una futura fusione o acquisizione? Descriveteci la vostra flessibilità nel modificare l'ambito di applicazione o nell'aggiungere policy di rilevamento per una società appena acquisita o i suoi utenti. |

# 4. Riduzione e riparazione del rischio

A causa del potenziale impatto sull'azienda che può derivare dalle modifiche ai privilegi di accesso, la riparazione può essere un compito complicato da intraprendere. Le soluzioni CIEM forniscono informazioni utili e raccomandazioni su come ridurre i rischi in base al contesto, valutando fattori quali l'accesso effettivo a un'identità, i comportamenti privilegiati e il potenziale raggio d'azione di un attacco.

| Funzionalità CIEM | Domande da porre a un fornitore CIEM |
|---|---|
| **Dimensionamento corretto** | Potete fornire consigli per il corretto dimensionamento delle identità e delle autorizzazioni?<br>In che modo fornite il contesto per capire come dimensionare correttamente? |
| **Valutazione del rischio** | Siete in grado di identificare le identità ad alto rischio sulla base di un accesso effettivo?<br>Siete in grado di fornire una valutazione del rischio per gli utenti in base alla totalità degli accessi?<br>È possibile aggregare i parametri di rischio e l'intelligence sulle minacce in una valutazione del rischio delle identità unificate e dinamiche?<br>Possiamo modificare le formule della valutazione del rischio degli avvisi forniti? |
| **Avvisi** | In che modo la vostra soluzione si integra con i nostri strumenti di sicurezza per il monitoraggio, l'analisi e gli avvisi, come il nostro SIEM?<br>Siete in grado di inviare webhook o aprire ticket in sistemi di workflow IT come JIRA o ServiceNow? |
| **Creazione di policy** | Siete in grado di creare nuove policy per autorizzazioni o ruoli? |
| **Refactoring** | È possibile effettuare il refactoring automatico delle autorizzazioni AWS/Azure/GCP per renderle più sicure in base all'utilizzo effettivo? |
| **Azioni di mitigazione dei rischi** | È possibile automatizzare gli avvisi agli utenti affinché modifichino le password quando le loro credenziali vengono compromesse?<br>È possibile disconnettere automaticamente gli utenti dalle sessioni in corso per evitare attacchi di dirottamento da token rubati?<br>Siete in grado di monitorare gli utenti tramite MFA aggiuntiva quando eseguono un'attività sospetta o privilegiata? E in base al cambiamento del livello di rischio della loro identità?<br>Siete in grado di eliminare l'accesso di terze parti?<br>Siete in grado di regolare dinamicamente l'accesso condizionato in base al livello di rischio?<br>È possibile automatizzare i workflow di riparazione? |

## Anche la collaborazione è importante

Un aspetto chiave nella scelta del fornitore giusto è sentirsi sicuri di instaurare un rapporto destinato a durare a lungo. Un vero partner dovrebbe comprendere la vostra strategia di sicurezza delle identità e aiutarvi a raggiungere i vostri obiettivi, non limitarsi a vendervi uno strumento CIEM.

Il fatto è che una soluzione CIEM da sola può fare molto solo per migliorare il vostro livello di sicurezza delle identità. Integrare le soluzioni CIEM nel processo di governance delle identità end-to-end significa che i sistemi comunicano tra loro, così come le persone. Il processo CIEM riunisce i team di sicurezza, IAM e attività IT perché fornisce un quadro completo e accurato delle identità e dell'accesso nel cloud, una comprensione condivisa del rischio e passaggi chiari per la riparazione.

Cercate un fornitore che comprenda tutte le vostre esigenze in termini di identità e possa fornire i risultati che vi aspettate in modo tempestivo. Per evitare sorprese sgradite, ponete ai fornitori queste domande prima di effettuare la vostra scelta.

| Competenze del fornitore | Domande da porre a un fornitore CIEM |
|---|---|
| **Time to value** | Quanto tempo richiede la distribuzione?<br>Vedremo risultati funzionali entro 1-2 giorni?<br>Come ci aiuterete a ridurre i tempi di risposta agli incidenti? |
| **Sicurezza utilizzabile** | Di quali connettori nativi disponete?<br>Avete un'API aperta?<br>È necessario scrivere script per far funzionare la vostra soluzione?<br>Che cosa vi serve da parte nostra per l'implementazione o l'integrazione?<br>Possiamo modificare le policy di sicurezza in modo da monitorare gli account rischiosi e ricevere avvisi senza la necessità di servizi professionali o di sviluppo di nuove funzionalità?<br>Offrite la vostra soluzione attraverso una piattaforma SaaS, insieme ad altri servizi privilegiati e di identità, che possiamo utilizzare mentre sviluppiamo il nostro programma? |
| **Supporto strategico** | In che modo secondo voi una soluzione CIEM si inserisce nella nostra strategia complessiva di sicurezza delle identità?<br>Come potete aiutarci a creare allineamento tra i team? |
| **Reattività** | Quando avremo domande o richieste di funzionalità sarete disponibili al telefono?<br>È facile accedere alla documentazione tecnica?<br>Avremo un referente specifico per garantire che tutto funzioni come deve?<br>Possiamo avere informazioni dettagliate sulla vostra roadmap? |

# Informazioni su Privilege Control for Cloud Entitlements di Delinea:

Privilege Control for Cloud Entitlements offre ai leader della sicurezza sul cloud un contesto approfondito sull'utilizzo del cloud e delle identità per scoprire privilegi in eccesso e limitare le autorizzazioni nell'infrastruttura multi-cloud per ridurre i rischi.

Scoprite e visualizzate costantemente tutte le identità, gli account e il relativo accesso sui cloud Google, Amazon e Microsoft per identificare comportamenti anomali e riconsiderare i privilegi. Fornito sulla Delinea Platform cloud-native, vi consente di inserite i diritti cloud nella vostra unica fonte di verità per l'autorizzazione su tutte le identità. Risparmiate tempo automatizzando il rilevamento e il deprovisioning di account locali e federati obsoleti senza alcun impatto sui team IT.

Per saperne di più, visitate il nostro sito web https://delinea.com/products/privilege-control-for-cloud-entitlements Guardate una demo interattiva di Delinea Privilege Control for Cloud Entitlements in azione.

Delinea

Securing identities at every interaction

Delinea, azienda pioniere nella protezione delle identità attraverso l'autorizzazione centralizzata, rende le organizzazioni più sicure governando senza soluzione di continuità le loro interazioni in tutta l'azienda moderna. Delinea consente alle organizzazioni di applicare il contesto e l'intelligenza in tutto il ciclo di vita dell'identità attraverso l'infrastruttura cloud e tradizionale, i dati e le applicazioni SaaS per eliminare le minacce legate all'identità. Grazie all'autorizzazione intelligente, Delinea è l'unica piattaforma che consente di scoprire tutte le identità, assegnare i livelli di accesso appropriati, rilevare le irregolarità e rispondere immediatamente alle minacce all'identità in tempo reale. Delinea accelera l'adozione da parte dei vostri team, con un'implementazione in settimane, non in mesi, e li rende inoltre più produttivi, richiedendo il 90% in meno delle risorse da gestire rispetto al concorrente più prossimo. Con un tempo di attività garantito del 99,99%, la Delinea Platform è la soluzione di sicurezza delle identità più affidabile sul mercato. Per saperne di più su Delinea, visitate **LinkedIn**, **Twitter** e **YouTube**.