Delinea

Cloud Infrastructure Entitlement Management (CIEM)

Buyer’s Guide

Cloud Infrastructure Entitlement Management (CIEM) Buyer's Guide

As a result of cloud transformation, sensitive data is now scattered throughout the enterprise. Cloud services are created rapidly, many times outside of central IT control. Moreover, virtually all enterprises have a mix of on-premise and cloud resources, often spread across data centers and multiple Cloud Service Providers (CSPs). Unfortunately, misconfigurations are common, leaving identities vulnerable to compromise or providing too much access, which could expose sensitive information.

Cyber criminals are taking advantage of the current situation to attack cloud resources. Most commonly they impersonate authenticated identities, leverage permissions to gain and elevate access, and achieve their malicious goals.

You can't protect your cloud resources from identity-based attacks like these using the same strategies you would in an on-premise world. It's incredibly difficult to track the potential or actual attack path of a single identity across such a distributed, dynamic, and inconsistent environment. The traditional tools — network firewalls, common corporate directory services, and static access controls — aren't effective in a cloud reality.

Therefore, in response to escalating identity-based attacks, organizations are embracing Cloud Identity Entitlement Management (CIEM) as a must-have security solution. CIEM connects the dots across the identity layer so you understand and control who has access to what, monitor their behavior, and respond rapidly to contain threats.

If you're responsible for cloud security, cloud architecture, or Identity and Access Management (IAM), and you're considering how CIEM solutions can fit into your security roadmap, this guide is for you.

The information inside will help you:

- ✓ Understand the use cases for CIEM
- ✓ Save you time preparing for conversations with CIEM providers by providing a checklist of questions to ask as you evaluate potential solutions
- ✓ Help you compare options and choose the best CIEM solution for your needs
- ✓ Consider CIEM within the context of your overall identity security strategy

Impact of the cloud on identity security

In a cloud environment, identity security becomes much more complex to manage, for several reasons:

Distributed control: Instead of a small admin group, numerous users and systems have access to data and resources and may even generate identities.

Role proliferation: The number of roles and permissions has exploded. This makes it hard to manage and understand them without specialized tools.

Misconfigurations: Misconfigured groups in identity management systems and/or cloud resources inadvertently expose risks.

Visibility gaps: A mix of different identity providers, federated apps/services, and local CSP users restrict identity monitoring and limit understanding of behavior across a cloud environment.

Complexity of cloud permissions: Modern cloud environments have intricate permission models with thousands of possible permissions across numerous services. It's easy to mistakenly grant excessive permissions, leading to excessive and risky permissions.

Privilege creep: Far too many identities have more privileges than needed, which is in violation of least privilege and zero trust best practices.

Constant change: Cloud environments experience rapid shifts with new identities (especially machine identities) created constantly, and entitlements provisioned and removed at breakneck speeds. The dynamic nature of cloud environments makes manual remediation of permission issues not scalable.

> CIEM connects the dots across the identity layer so you understand and control who has access to what, monitor their behavior, and respond rapidly to contain threats."

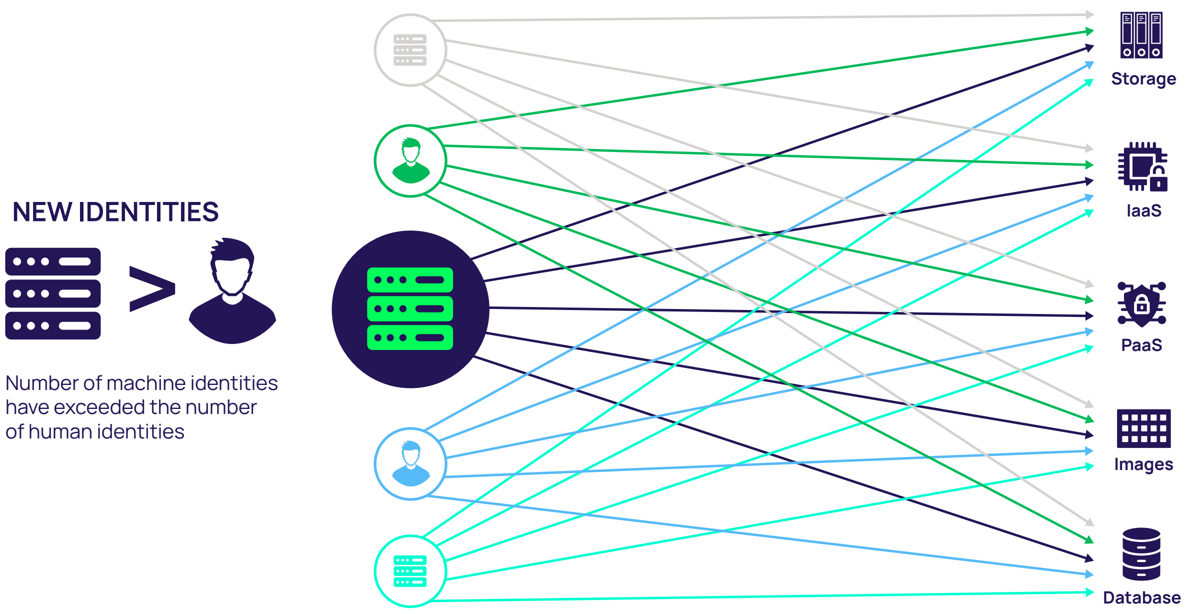
Cloud Infrastructure Entitlement Management (CIEM)

CIEM is the process of managing identities and their privileges in cloud environments. The purpose of CIEM is to understand which access entitlements exist across cloud and multi-cloud environments, and then identify and mitigate risks resulting from entitlements that grant a higher level of access than they should.

CIEM helps you reduce these risks of identity-based attacks by applying preventive controls for the governance of entitlements in hybrid and multi-cloud Identity-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). Utilizing analytics and Machine Learning (ML), CIEM continuously monitors identities, permissions, and activities. It detects anomalies in account entitlements, such as the accumulation of privileges, dormant permissions, and unused accounts or roles. By enforcing the Principle of Least Privilege, CIEM helps ensure identities have access only to what they need and minimizes your attack surface.

Unlike other cloud security solutions like Cloud-Native Application Protection Platforms (CNAPP), CIEM solutions are focused on identity risk. Ideally, CIEM solutions are an embedded part of your identity creation and lifecycle governance process.

FIGURE 1 | The number of identities in a cloud account multiplied by the number of entitlements each identity has makes for a massive attack surface.


NEW IDENTITIES
>
Number of machine identities have exceeded the number of human identities
Storage
IaaS
PaaS
Images
Database

Four core uses of CIEM solutions

1 Providing visibility of risky entitlements

CIEM provides granular visibility into human and non-human identities, sensitive assets, and entitlements. It shows you "effective access" for each identity through the discovery of potential access pathways they may use to navigate across your IT environment. Detecting dormant and excessive entitlements is a central function within CIEM solutions (also known as permissions management or permissions auditing).

2 Ensuring controls are working as expected

CIEM helps you ensure the right security controls for authentication and authorization are in place and being effective. With CIEM, you can reduce the potential for identity-related attacks to gain an initial foothold, elevate access, or achieve persistence.

3 Detecting behavioral anomalies

CIEM helps you recognize when a cybersecurity event is occurring. It collects meaningful data by continuously monitoring identities and their behavior and providing the essential context for understanding that information. Machine Learning enriches historical identity analytics with behavioral data, ensuring that granted entitlements align with genuine necessity and usage.

4 Remediating identity-related risks

Automatic risk remediation is an essential feature in a CIEM solution. When a risk is detected, CIEM will recommend a policy adjustment or trigger a workflow. For example, CIEM can address excessive entitlements by removing dormant privileges, it can fix policy drift by reducing privileges, and trigger actions to remediate misconfigurations.

In the next section, you'll find questions to ask any CIEM solution provider about each of these use cases as part of your vendor assessment.

Questions for CIEM Solution Providers

1. Providing visibility of risky entitlements

Your Identity Provider (IdP) cannot truly understand entitlements in your CSPs. Normal privilege sprawl, users created outside of your IdP (i.e., by local admins or external identities), privileges granted via unseen group membership, and other factors create blind spots. CIEM fills in missing information about the de facto state and usage of privileges.

These CIEM capabilities lay the groundwork for your cybersecurity actions by providing end-to-end visibility of your identity attack surface.

CIEM capability	Questions to ask a CIEM Provider
Discover human identities	Do you support multiple IdPs (Okta, Azure Active Directory, PingOne, etc.)? Can you connect to HR systems to track Joiner-Mover-Leaver (JML) changes and partial offboarding?
Discover machine identities	Can you discover machine identities such as APIs and workloads?
Discover federated identities	Can you discover federated identities that are generated externally and joined to your IdP via token exchange? Can you tie activity in AWS to federated users so that I can track them?
Discover all critical cloud services and apps and their current state	Does your coverage include IaaS and PaaS? Which CSPs do you support? Can you detect sensitive folders that are publicly accessible? How about our homegrown systems?
Discover permissions and privileges for all types of identities	Can you show what permissions are granted to whom and how in a centralized view? Can you provide granular, file-level visibility of access permissions? Can you detect over-privileged human and machine identities? How do you discover hidden privileges granted via groups, privilege escalation paths, and misconfigurations? Can you show me contractors who retain access to assets with their own identities?
Merge identities	Can you merge identities, including those not in our IdP but with access to our assets?
Continuous discovery	How does the system discover new identities and assets as they're created so they can quickly be brought under management?
Discover dormant identities and standing privileges	How do you determine when an identity or privileged access is no longer required? Can you show access privilege usage, detecting unused privileges over specified periods?

CIEM capability	Questions to ask a CIEM Provider
Discover effective access across environments	How do you trace access paths and entitlement permissions across systems and environments (on-premise, and multi-cloud)? Do you provide end-to-end visibility from the IdP to the asset? Can you show me privilege escalation paths like role chaining, the granting of temporary access to resources, in Amazon Web Services? How do you create visualizations of access paths so they're easy to understand immediately?
Risk scoring	Can you identify high-risk identities based on effective access? Can you provide risk scores for users based on the totality of access? Can you aggregate risk parameters and threat intelligence into a unified, dynamic identity risk score?

2. Ensuring controls are working as expected

Protecting your identity threat surface against attacks starts with reducing risks before they can be exploited by an adversary. Most likely, your organization already has some identity controls in place. However, are you confident they are working as expected and nothing has fallen through the cracks?

These CIEM capabilities help you ensure preventive security controls are working effectively to contain the potential blast radius of an identity-based attack. Primary areas of focus are enforcing least privilege and containing privilege escalation paths because they deny an attacker who has compromised an identity the privileges they need to reach their objectives.

CIEM capability	Questions to ask a CIEM Provider
Authentication support	Can you show me which privileged identities have multi-factor authentication (MFA) enabled and at what level? Can you uncover and fix IAM misconfigurations? Can you detect risky misconfigurations that would expose us to leaking clear text passwords or user impersonation?
Authorization support	Can you show me how users gain access to assets through group membership (ex. nested groups, public groups)? How do you limit privileged access? How do you eliminate privilege escalation paths to contain attacks?

3. Detecting behavioral anomalies

Detecting privilege escalation paths and events can be exceedingly tricky in the cloud due to complexity and lack of visibility. CIEM helps you uncover identity-based attacks in progress, including attempts to gain initial access with compromised credentials or escalate privileges if attackers are already inside.

CIEM capability	Questions to ask a CIEM Provider
Detecting Tactics, Techniques, and Procedures (TTPs)	Can you detect MFA bombing/fatigue attacks? Can you detect brute force attacks? Can you detect failed login attempts using credential stuffing across multiple applications that may indicate related attacks on an identity? Can you detect session hijacking?
Suspicious activity	Can you detect when new privileged identities are created? Can you detect dormant accounts that become active again? Can you detect unexpected/unwanted privilege elevation or escalation? Can you detect the connection of new upstream identity data sources like additional IdPs or HR applications? Can you detect newly created malicious misconfigurations at the IdP level? Can you detect changes users make to logs in our IdP that may indicate they're hiding their activity?
Usage monitoring	Can you provide a baseline of activity to determine a user's normal entitlement usage, so that we'll know when behavior outside of the norm occurs? Is monitoring continuous?
Flexibility	How will you help me to extend my existing detection capabilities for new IdPs and apps in my next M&A? Describe to me your flexibility in shifting scope or adding detection policies for the newly acquired company or its users.

4. Risk reduction and remediation

Because of the potential impact on the business that can occur from changes to access privileges, remediation can be a tricky task to undertake. CIEM provides actionable insights and recommendations on how to reduce risks with context, based on factors like effective access of an identity, privileged behavior, and potential blast radius of an attack.

CIEM capability	Questions to ask a CIEM Provider
Right-sizing	Can you provide recommendations for right-sizing identities and permissions? How do you provide context to understand how to right-size?
Risk scoring	Can you identify high-risk identities based on effective access? Can you provide risk scores for users based on the totality of access? Can you aggregate risk parameters and threat intelligence into a unified, dynamic identity risk score? Can I adjust the risk score formulas of alerts you provide?
Alerting	How do you integrate with my security tools for monitoring, analysis, and alerts, such as my SIEM? Can you send webhooks or open tickets in IT workflow systems like JIRA or ServiceNow?
Policy creation	Can you create new policies for permissions or roles?
Refactoring	Can you automatically refactor AWS/Azure/GCP permissions to be more secure based on actual usage?
Mitigating actions	Can you automate alerting users to change passwords when their credentials are compromised? Can you automatically log users out of current sessions to avoid hijacking attacks from stolen tokens? Can you challenge the user via additional MFA when they perform a suspicious or privileged activity? Or based on their changing identity risk level? Can you remove third-party access? Can you dynamically adjust conditional access based on risk level? Can you automate remediation workflows?

Partnership also matters

A key aspect of selecting the right vendor is feeling confident that you will have a relationship built for the long run. A true partner should understand your identity security strategy and help you achieve your goals, not just sell you a CIEM tool.

The fact is, CIEM by itself can only do so much to improve your identity security posture. Embedding CIEM in the end-to-end identity governance process means systems are talking to each other, and so are people. CIEM brings security, IAM, and IT operations teams together because they have a complete, accurate picture of identity and access in the cloud, a shared understanding of risk, and clear steps for remediation.

Look for a vendor who understands all your identity needs and can deliver the outcomes you expect in a timely way. To avoid unwelcome surprises, ask vendors these questions up front.

Vendor capability	Questions to ask a CIEM Provider
Time to value	How long does deployment take? Can I see functional results within 1-2 days? How will you help me decrease incident response time?
Usable security	What native connectors do you have? Do you have an open API? Is there any need to write scripts to operate your solution? What do you require from my side for deployment or integration? Can I adjust security policies to track and alert on risky accounts without the need for professional services or new feature development? Do you offer your solution through a SaaS platform, along with other privileged and identity services, that we can utilize as we develop our program?
Strategic support	How do you see CIEM fitting into my overall identity security strategy? How can you help me build alignment across teams?
Responsiveness	Are you going to pick up the phone when I have questions or feature requests? How easy is it to access your technical documentation? Will I have a dedicated success manager? Can I get insight into your roadmap?

About Delinea Privilege Control for Cloud Entitlements

Privilege Control for Cloud Entitlements provides cloud security leaders with deep context into cloud and identity usage to discover excess privilege and limit authorization across multi-cloud infrastructure to reduce risk.

Continuously discover and visualize all identities, accounts, and their access across Google, Amazon, and Microsoft clouds to identify anomalous behavior and refactor privileges. Delivered on the cloud-native Delinea Platform, you can integrate cloud entitlements as part of your single source of truth for authorization across all identities. Save time by automating the discovery and de-provisioning of stale local and federated accounts without impacting IT teams.

To learn more, visit our website https://delinea.com/products/privilege-control-for-cloud-entitlements. See an interactive demo of Delinea Privilege Control for Cloud Entitlements in action.

Delinea

Securing identities at every interaction

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across the modern enterprise. Delinea allows organizations to apply context and intelligence throughout the identity lifecycle across cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. With intelligent authorization, Delinea provides the only platform that enables you to discover all identities, assign appropriate access levels, detect irregularities, and immediately respond to identity threats in real-time. Delinea accelerates your teams' adoption by deploying in weeks, not months, and makes them more productive by requiring 90% fewer resources to manage than the nearest competitor. With a guaranteed 99.99% uptime, the Delinea Platform is the most reliable identity security solution available.
Learn more about Delinea on **LinkedIn**, **X**, and **YouTube**.