

CLOUD ENTITLEMENT MANAGEMENT (CIEM).



Cloud IAM roles and service accounts are almost always granted far more access than they ever actually use. **That gap between granted and used permissions is exactly what defines a compromised identity's blast radius — and it's invisible to tools that only check resource configuration.**

- ENTITLEMENT GAP
- LEAST-PRIVILEGE RIGHT-SIZING
- TOXIC PERMISSION COMBINATIONS
- MULTI-CLOUD IAM

01 THE MECHANISM



Granted vs. Actually Used Permissions

Cloud IAM roles and service accounts are typically granted far broader permissions than they ever exercise, and **that gap between granted and used access is exactly what CIEM measures and closes.**



Effective Permissions Combine Every Policy Layer

A cloud identity's real access comes from combining identity-based, resource-based, permission-boundary, and organization-level policies together, **a calculation manual review routinely gets wrong at scale.**



Non-Human Identities Accumulate Access Fastest

Service accounts, CI/CD credentials, and workload identities are often granted broad access for development convenience and rarely revisited, **making them a disproportionate share of the entitlement gap.**

02 THE FLOW

The Right-Sized Entitlement Program

CONTAINED

- Every identity's granted permissions are continuously inventoried and **compared against what it has actually used** over a meaningful lookback period.
- Unused permissions are automatically flagged with a specific recommendation, **scoping each identity down to what its observed activity requires.**
- A compromised service account's blast radius is limited to a **narrow, actually-used permission set**, not the broad access it was originally granted.

The Unmanaged Entitlement Sprawl

EXPOSED

- Roles and service accounts accumulate broad permissions over time, **granted for convenience during development and never revisited** once the project moves on.
- A single compromised access key **inherits every permission ever granted** to that identity, far beyond anything it actually needed.
- The attacker discovers a toxic combination — the ability to both create roles and assume other roles — and **escalates into control over the broader environment.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Entitlement Discovery & Inventory	Continuously cataloging every human and non-human identity across every cloud account and exactly what permissions each has been granted.
Usage Analytics	Correlating granted permissions against actual activity from cloud provider audit logs to identify what's dormant versus actively used.
Right-Sizing Recommendations	Generating specific, actionable least-privilege policy recommendations that preserve an identity's actual observed functionality.
Toxic Combination & Escalation Detection	Flagging risky permission combinations, such as the ability to both create roles and assume other roles, that enable privilege escalation.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Granting Broad Permissions at Creation, Never Revisited	No	Permissions granted for initial convenience accumulate indefinitely, and the gap between granted and used access only grows.
Single Cloud-Native IAM Tooling in a Multi-Cloud Environment	No	AWS, Azure, and GCP each use different permission models, leaving no unified view of entitlement risk.
Manual Permission Review at Scale	No	Effective permissions require combining multiple policy layers per identity, a calculation manual review routinely gets wrong.
Treating CSPM Findings as Coverage for Identity Risk	No	CSPM evaluates resource configuration; it doesn't answer who or what can actually do what across the environment.
Continuous Discovery + Usage Analytics + Right-Sizing + Escalation Detection	Yes	Closes the gap between granted and used access before it becomes a compromised identity's blast radius.

CLOUD ENTITLEMENT MGMT (CIEM).

DISCOVER · RIGHT-SIZE · DETECT

05 PROGRAM OPERATIONS

The gap between what an identity is granted and what it actually uses is the **core problem CIEM measures**, and in most environments that gap is far larger than teams assume until they look.

Non-human identities are frequently the **fastest-growing, least-reviewed part of the entitlement gap**, since service accounts get broad access for convenience and are rarely revisited afterward.

A compromised identity's blast radius is defined by everything it was granted, not everything it actually does, which is why unused permissions are a real cost even before anything malicious happens.

Toxic permission combinations, like creating roles and assuming other roles, can let a single narrow compromise **escalate** into control over a much broader slice of the cloud environment.

06 CONTROL MAPPING

MIST SP 800-53 (AC-6)

The foundational **least-privilege access control principle** CIEM operationalizes at cloud scale, across every identity and every permission layer.

CLOUD-NATIVE ENTITLEMENT TOOLS

Provider-specific building blocks, such as AWS IAM Access Analyzer, that CIEM platforms build upon and extend across multi-cloud environments.

CIS CLOUD PROVIDER BENCHMARKS

Cloud-specific hardening benchmarks that include least-privilege IAM guidance relevant to entitlement right-sizing.

GARTNER CIEM CATEGORY

The **analyst-defined category** distinguishing entitlement management from CSPM and CWPP within the broader cloud security tooling landscape.

07 WHAT THIS DOES NOT SOLVE

Resource Configuration Risk

CIEM addresses who can do what; it **doesn't evaluate whether a resource itself**, like a storage bucket, is securely configured.

The Initial Credential Compromise

Right-sizing permissions limits blast radius; it **doesn't prevent the phishing or credential theft** that compromised the identity in the first place.

Legitimate Excessive Access Requests

A right-sizing recommendation can still be **overridden by a business justification** for broader access, which CIEM can flag but not unilaterally block.

Cross-Cloud Identity Federation Complexity

Entitlements granted through federated identity or cross-account trust add a layer of complexity that **basic per-account review can miss**.

08 MYTHS VS. REALITY

MYTH "Most granted cloud permissions eventually get used."	REALITY The significant majority of granted permissions in most cloud environments are never actually exercised, creating a persistent, measurable gap.
MYTH "CSPM and CIEM cover the same ground."	REALITY CSPM evaluates resource configuration; CIEM evaluates identity permissions, and an environment can pass every CSPM check while carrying massive unused entitlements.
MYTH "Service accounts are lower risk than human user accounts."	REALITY Non-human identities frequently accumulate broader, less-reviewed permissions than human accounts, making them a disproportionate share of real risk.
MYTH "A single cloud provider's IAM tools are enough in a multi-cloud environment."	REALITY AWS, Azure, and GCP each use different permission models, leaving no unified view of risk without dedicated multi-cloud tooling.
MYTH "Reviewing IAM policies manually is sufficient at scale."	REALITY Effective permissions require combining multiple policy layers per identity, a calculation that becomes infeasible to do accurately by hand at scale.

09 SPEAK THE PROGRAM — KEY TERMS

ENTITLEMENT GAP

The difference between the permissions an identity has been granted and the **permissions it actually uses**.

EFFECTIVE PERMISSIONS

An identity's real, actual access after **combining every applicable policy layer**, including identity-based and organization-level policies.

TOXIC COMBINATION

A set of permissions that individually seem reasonable but together **enable privilege escalation**, such as creating roles and assuming other roles.

RIGHT-SIZING

Generating a scoped-down permission policy that **preserves an identity's actual observed activity** while removing everything unused.

JUST-IN-TIME (JIT) ACCESS

Granting elevated permissions only for the specific duration they're needed, **then automatically revoking them** rather than leaving standing access.

CNAPP

Cloud-Native Application Protection Platform — the unified category **increasingly bundling CIEM, CSPM, and CWPP** into a single platform.