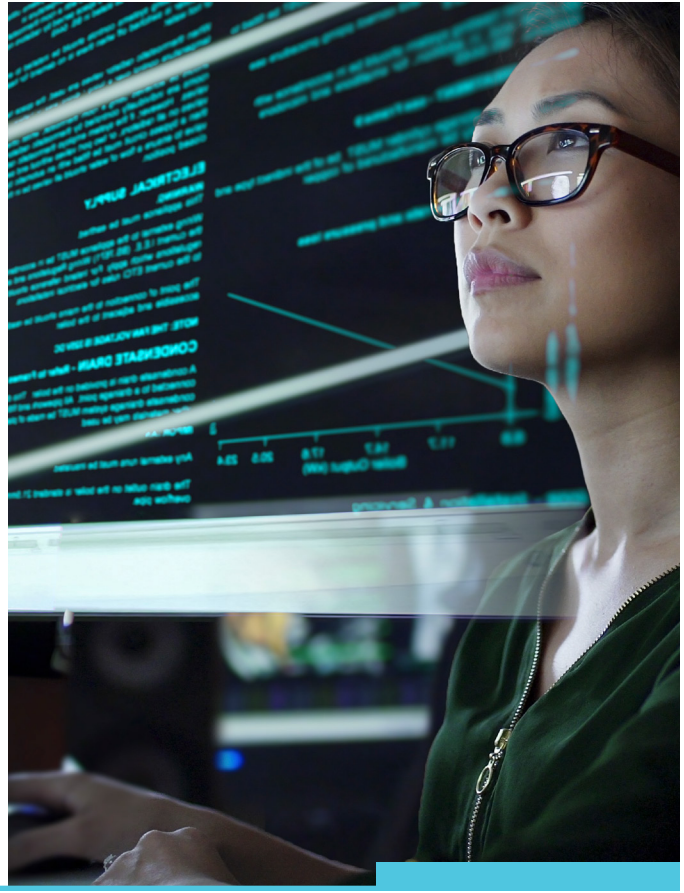
The 5-Minute Guide to Understanding Cloud Infrastructure Entitlement Management

CIEM: Everything You Need to Know



paloalto NETWORKS

Table of Contents

Introduction

At first glance, managing cloud entitlements—the access and authorization controls that define who can do what within cloud environments—may seem simple enough. You define roles, you assign permissions to them, and you call it a day, right?

Well, not exactly. Although cloud entitlement management may have been straightforward in the days when most organizations used just one cloud and one identity and access management (IAM) framework to manage entitlements within it, those days are gone. Today, teams face a dizzying conflagration of different entitlement management tools and concepts across the various cloud platforms, services, and workloads they deploy. Defining roles and permissions in a secure manner, let alone keeping track of them across sprawling environments, is anything but simple.

Indeed, Gartner recently reported that among 95% of cloud accounts, fewer than 3% of active entitlements were actually used.[1] That means that the vast majority of entitlements create excess privileges—exactly the opposite of what organizations should be striving for as they aim to implement Zero Trust cloud security strategies.

Fortunately, a solution to these challenges has emerged in the form of a new strategy for entitlement management: Cloud Infrastructure Entitlement Management (CIEM). By automatically assessing entitlements in any type of cloud environment and basing them on any access control configuration framework, CIEM enables a more granular, scalable, and comprehensive approach to entitlement management.

This guide explains how to leverage CIEM to improve the security posture of modern cloud-centric environments. It begins by defining CIEM and discussing why CIEM has become so critically difficult in modern environments. It then describes the tools and techniques that enable effective CIEM. It explains, too, how CIEM relates to other core aspects of cloud security management, including Cloud Security Posture Management (CSPM), Privileged Access Management (PAM), and Identity Governance and Administration (IGA).

Defining roles and permissions in a secure manner, let alone keeping track of them across sprawling environments, is anything but simple.

With these insights, you'll gain the clarity you need to define a CIEM strategy that effectively addresses the complexity of entitlement management in the modern cloud as one pillar of a comprehensive cloud security strategy.

1. Abhyuday Data, Michael Kelley, and Henrique Teixeira, *Innovation Insight for Cloud Infrastructure Entitlement Management*, Gartner, June 15, 2021, https://www.gartner.com/en/documents/4002548/innovation-insight-for-cloud-infrastructure-entitlement-.

What Is Cloud Infrastructure Entitlement Management?

Cloud Infrastructure Entitlement Management is the process of managing identities and privileges in cloud environments. The purpose of CIEM is to understand which access entitlements exist in cloud environments, then identify and mitigate risks that result from entitlements that grant a higher level of access than they should.

Importantly, although the term "Cloud Infrastructure Entitlement Management" can be interpreted to imply that CIEM only addresses access rights associated with cloud infrastructure (such as storage and compute resources), this is a bit misleading. CIEM applies to access entitlements of all kinds, including resources like application services and APIs that fall beyond the scope of infrastructure as it is traditionally defined.

CIEM also applies both to human users of cloud environments and to "machine" identities running in them. In other words, CIEM can be used to manage entitlements for developers, IT engineers, and other users and groups who deploy workloads to the cloud. At the same time, it can address access privileges for applications and services hosted in cloud environments.

Across these various contexts, CIEM addresses three specific categories of entitlements:

- **Resource-level entitlements:** These entitlements define functional work. They grant privileges such as the ability to read and/or write data or set up virtual machine instances.
- **Service-level entitlements:** At the service level, entitlements define operational privileges, such as starting and stopping virtual machine instances or cloning databases.
- **Management-level entitlements:** Management entitlements are used to define administrative privileges that apply to the cloud environment as a whole. Examples include privileges for configuring environment-level security settings or creating new cloud accounts.

What Do CIEM Tools Do?

CIEM allows teams to manage entitlements at all of these levels via several key areas of functionality.

Entitlement Visibility

The first step in managing entitlements and mitigating entitlement risks is to understand which entitlements exist within your environment. CIEM tools do this by automatically scanning access control policies, rules, and configurations of all types in order to determine:

- Which entitlements exist.
- What each human or machine user can do based on those entitlements.
- Which human and machine users can access each cloud resource based on those entitlements.

In this way, CIEM gives teams visibility into the state of their entitlements across all layers and segments of their cloud environment—even if that environment includes multiple clouds or multiple types of access control frameworks and configurations.

Rightsizing Permissions

After identifying an entitlement, CIEM tools assess it to determine whether the access privileges it grants are the least necessary for achieving a workload's intended purpose. If the entitlement provides too much access, CIEM tools can alert administrators so they can address the problem manually. The tools can also be configured to adjust entitlements automatically, which allows teams to work efficiently in large-scale environments that might include hundreds of thousands or even millions of individual entitlements.

Because CIEM tools monitor entitlement configurations and workload requirements on a continuous basis, they not only identify entitlements that are risky when they are first created but can also detect instances where entitlements are outdated or have become overly permissive.

Advanced Analytics

The entitlement assessment that CIEM tools perform is based not simply on generic rules and conditions but on advanced analytics powered by machine learning and User and Entity Behavior Analytics (UEBA).

Using these techniques, CIEM tools can dynamically determine whether an entitlement provides the right level of access based on current workload needs and update them in a dynamic fashion. For example, if a user identity ceases to exist because a user leaves the organization, CIEM tools can detect entitlements associated with that identity and remove them.

Compliance

While compliance is not the sole focus of CIEM, CIEM tools can align entitlements with compliance requirements by automatically assessing whether entitlements conform with compliance needs. They can also detect instances of "drift," in which entitlements that were once compliant come out of compliance as a result of configuration changes.

Why CIEM, and Why Now?

Managing access rights in the cloud is nothing new. Since the origins of modern cloud computing platforms more than 15 years ago, cloud service providers (CSPs) have provided tools for configuring entitlements within their environments. Along with security vendors, CSPs have also developed tools to help assess and manage entitlement-based risks in the cloud.

However, as cloud environments have grown increasingly complex in recent years, traditional approaches to entitlement management have begun falling short of guaranteeing complete visibility. There are several reasons why.

Massive Scale of Entitlement

As cloud environments have grown in scale, many businesses simply have too many entitlements to manage effectively. Even in a single-cloud architecture—to say nothing of architectures that include multiple clouds or that combine public cloud resources and private infrastructure via a hybrid model—a single business may have hundreds of accounts, thousands of workloads, and thousands of human and machine identities associated with them. Such a configuration can easily result in millions of individual entitlements.

Tracking entitlements on this massive scale is a task that conventional cloud access management tools were not designed to address.

Entitlement Complexity

Organizations that use multiple clouds at once, or even simply deploy multiple types of cloud services within a single cloud, often struggle to understand the full implications of the entitlements they grant.

For example, consider an identity that is granted access privileges via "get," a so-called verb that can often be assigned within access control policies. However, the exact implications of "get" can vary from one type of cloud service to another. A human or machine user who has "get" rights for a cloud storage bucket will be able to perform different actions than one with "get" privileges in Kubernetes®, for instance.

A single business may have hundreds of accounts, thousands of workloads, and thousands of human and machine identities associated with them. Tracking entitlements on this massive scale is a task that conventional cloud access management tools were not designed to address.

In contexts like this, it's only by interpreting entitlements in a granular, nuanced fashion that tools can identify whether access configurations pose security risks.

Inconsistent Access Control Frameworks

Along similar lines, the fact that access control settings and configurations tend to vary widely between clouds and cloud services poses a major challenge for modern entitlement management, especially for organizations that use multicloud or hybrid cloud architectures.

Although all CSPs offer IAM frameworks, the configuration languages, tools, and concepts they use are not very consistent. For instance, Microsoft Azure® uses an IAM framework oriented around Microsoft Active Directory (although Azure also supports other ways of defining access rights), whereas the other clouds use native IAM frameworks. Likewise, the meaning of concepts like "service," "permissions," "actions," and "roles" can vary from one cloud to another.

Given this complexity, access control management tools that were designed for just one cloud or one type of service no longer suffice. Modern businesses must be able to identify and assess all identities across all of their clouds using a single solution.

Ephemeral Cloud Services

A final key challenge in entitlement management is that many cloud workloads are ephemeral. Resources like virtual machine instances and containers may exist for only a few minutes before they are spun down or destroyed.

What this means from the perspective of entitlement management is that it is critical to track entitlements in real time. Periodic audits of entitlement configurations don't suffice for identifying and remediating all potential risks across highly dynamic cloud environments.

Modern businesses must be able to identify and assess all identities across all of their clouds using a single solution.

CIEM vs. Other Entitlement Management Tools

Over the years, various solutions have emerged to help manage access controls and entitlements in the cloud. These solutions address some of the challenges described above, but they are typically not sufficient on their own for complete entitlement management within modern cloud environments.

To explain why, let's compare CIEM to three other popular categories of cloud security tools: Identity Governance and Administration (IGA), Privileged Access Management (PAM), and Cloud Security Posture Management (CSPM).

CIEM vs. IGA

IGA tools are designed primarily to help businesses define and apply entitlements across cloud environments. They help translate governance and compliance rules into access policies that can be deployed into the cloud.

While IGA is a useful starting point for establishing secure entitlements, its major shortcoming is that IGA tools don't typically audit entitlements once they are in place. Thus, they cannot identify entitlement configuration oversights or situations where entitlement requirements have changed due to a change in the nature of an identity. Only CIEM provides this type of continuous, granular assessment of entitlement policies.

CIEM vs. PAM

In the cloud, PAM tools help to configure access rights for human and machine users that require special access to cloud resources. They are helpful for granting proper permissions to administrative accounts, for example. Like IGA tools, however, PAM tools don't provide continuous assessment of entitlement policies. They also don't apply to entitlements of all types; instead, they focus on privileged access controls.

In contrast, CIEM manages entitlements of all types—privileged or not—for all identities. It also provides continuous auditing of entitlement configurations, as noted above.

CIEM manages entitlements of all types—privileged or not—for all identities.

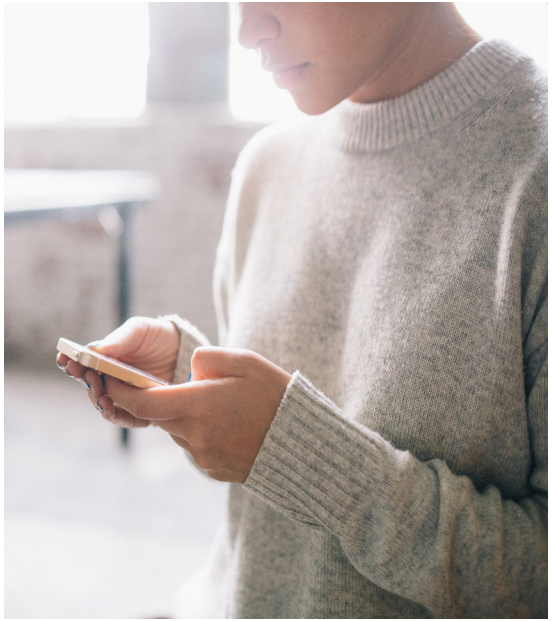
CIEM vs. CSPM

The category of tool that comes closest to CIEM is CSPM. Like CIEM, CSPM automatically assesses cloud access control configurations to identify risks. CSPM tools can typically perform these assessments on a continuous basis.

However, the main difference between CIEM and CSPM is that CSPM focuses mostly on identifying generic cloud configuration mistakes that could have security consequences, such as the failure to collect and analyze important logs or the existence of IAM rules that grant public access to cloud storage buckets.

In contrast, CIEM identifies and assesses access configurations at a highly granular level. Its goal is to ensure that each individual human or machine identity in the cloud has the proper entitlements. To do this, CIEM tools must be able to understand which entitlements a given cloud resource should have, then compare them to the entitlements actually assigned. CSPM tools don't do this; instead, they identify risks by recognizing types of configurations that are known to be insecure in a generic sense, rather than assessing each resource's individual entitlement requirements.

Thus, whereas CSPM is useful for detecting major configuration issues that apply to broad categories of workloads, CIEM catches access management errors that are too nuanced or obscure to be detected by CSPM tools.



The Prisma Cloud Approach to CIEM

The entitlement management challenges described above are the reasons why Prisma® Cloud has pioneered the integration of CSPM with CIEM in a single cloud security platform. The combined functionality empowers users to extend their cloud vulnerability management strategies to include any cloud, as well as more granular detection of risks, even if they have millions of entitlements to manage.

With Prisma Cloud, your team gains:

- **Visibility:** Understand the state of entitlements on any cloud and any IAM framework by quantifying overall entitlement risk, run queries to determine the entitlements of specific users or resources, and monitor entitlements across multiple cloud accounts.
- **Governance:** Identify excess and unused privileges based on governance policies that Prisma Cloud generates automatically via machine learning and UEBA. Demonstrate compliance via built-in reporting.
- **Response and remediation:** Remediate entitlement risks based on least-privileged configurations that Prisma Cloud recommends. Where desired, enable fully automated remediation so that entitlement risks are mitigated automatically by Prisma Cloud.

To learn more, request a demo of Prisma Cloud.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com