WHAT IS CIEM?

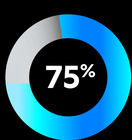
How can CIEM help to address the top risks associated with excessive entitlements?

Cloud environments are filled with human and machine identities, such as a developer, administrator, virtual machines, cloud functions, and service accounts. But as more users and services access sensitive data in the cloud, the risk of a breach increases. Most enterprises embracing the cloud do not have the level of visibility needed to identify who has access to their infrastructure, what operations they are authorized to execute, and what actions they have already performed.

of entitlements are granted to machines or non-human identities

of dormant privileges are open to misuse

of cloud security failures will be the customer's fault



of cloud security failures stem from identities, access, and privileges

Gartner Report: Innovation Insight for Cloud Security Posture Management
Gartner Report: Managing Privileged Access in Cloud Infrastructure
https://bit.ly/3A2O0Vo

Cloud Infrastructure Entitlement Management (CIEM) addresses the emerging risks of excessive entitlements that can expose data and increase the attack surface.

Key challenges of cloud infrastructure entitlement management

Impaired visibility and blind spots

Inability to track how cloud access entitlements are being used and who is able to access them.

Information silos

Unable to get accurate information on assets, identities, and associated entitlements across a multi-cloud environment with a single platform.

Greatly increased attack surface

With the massive increase in the number of human and machine identities accessing cloud infrastructure, attack surface is growing and changing at an extraordinary pace.

DevOps speed and agility

Managing thousands of permission changes per day and tens of millions overall.

Diverse IAM model

Each cloud provider offers a different set of IAM services and tools that are inadequate for detecting and remediating risk.

Gartner estimates that "by 2024, **organizations running cloud infrastructure services will suffer a minimum of 2,300 violations** of least privilege policies, per account, every year"

Reference: Innovation Insight for Cloud Infrastructure Entitlement Management
Published 15 June 2021 | ID G00740535

How can Zscaler CIEM help?

Discover

Understand cloud Identity, access, and entitlements through the access path across all clouds

Detect

Identify and understand top identity and access risk profile

Prioritize

Security actions using deep analysis with risk-based prioritization

Remediate

Remediate over-permissioned identities (user, role, group, resource) to create least-privileged roles and policies

Other Zscaler benefits

Advance access analytics

Leverage artificial intelligence to identify, prioritize the most important permissions-based risks and allow the security teams to maximize risk reduction with minimal effort.

Minimize attack surface

Detect over-privileged identities and risky access paths to sensitive resources.

DevSecOps

Integrate and enforce automated guardrails for identities, resources, and configuration at every development stage, empowering developers to innovate and deploy rapidly and securely.

Automate Compliance

Meet numerous IAM compliance requirements to improve overall cloud security posture.

Cloud Infrastructure Entitlement Management (CIEM)

Learn how CIEM mitigates the risk of data breaches in public clouds that result from excessive permissions. Schedule a free demo today.

Learn more about Zscaler CIEM