The Risk of Excessive Cloud Access Permissions

An IDC infographic sponsored by Ermetic

An IDC survey found that given the scale and complexity of IaaS and PaaS environments, organizations struggle to define and enforce least-privilege access policies for identities and data.

A primary cause of cloud data breaches is access-related misconfigurations resulting from human error and excessive permissions. While least privilege is considered a best practice to mitigate excessive cloud access, the survey indicated a lack of solutions to effectively implement this model.

Cloud Data Breaches on the Rise

79% of the companies that participated in the survey reported that they had a cloud data breach in the last 18 months.

and

43% of respondents reported that they had experienced 10 breaches or more in the last 18 months.

Top IaaS/PaaS Concerns

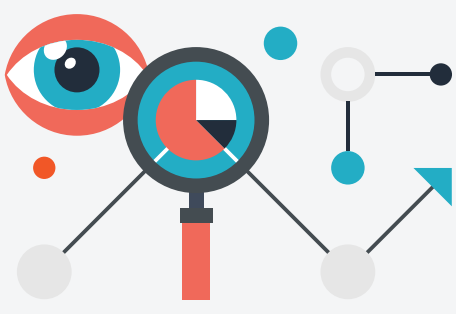
In a survey of 300 companies in the United States, we asked senior decision makers responsible for cloud security about their concerns regarding their cloud production environments. Below are the top responses.

67% Security Misconfiguration

64% Lack of Visibility

61% Improper IAM Configuration

Excessive Access Permissions Hard to Detect and Mitigate



80% of respondents did not identify cases of excessive access to sensitive data. Many organizations also reported that they were unable to mitigate the risk before data was exposed, which may point to a lack of adequate solutions for effectively reducing excessive permissions.

Least Privilege is Equally Important for Human and Machine Identities

Top choices Ranked as Very Important

63% Ensuring **employees** have the right level of access to execute their jobs effectively

69% Ensuring **workloads** have minimum permissions required to operate

The Top Priorities: Managing Permissions and Security Configuration

75% Authorization and permission management in the cloud

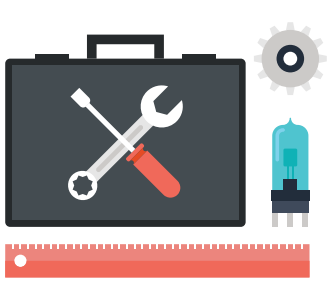
73% Cloud production environment security configuration

Essential Guidance

The survey findings indicate the need for a different approach to protecting access to cloud production environments and minimizing exposure to excessive access permissions. Given the scale and flexibility of IaaS and PaaS environments, demand is rising for a new model of security based on several key principles:

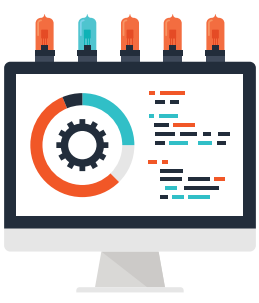
Least Privilege

A typical environment includes thousands of human and machine identities and hundreds of policies. Permissions must be managed to ensure that identities can only access the resources they need for legitimate purposes.



Automation

Given the large number of identities, resources and permissions, the process of creating and enforcing least privilege policies must be automatic and scalable for DevOps and security teams.



Continuous Lifecycle

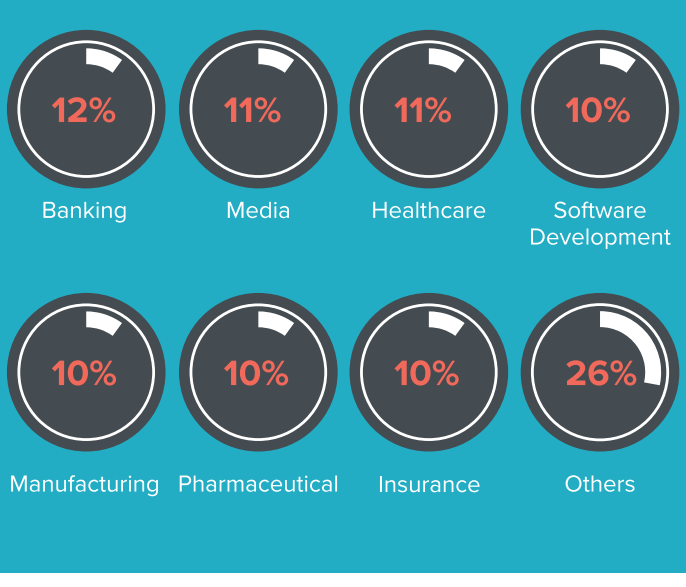
Eliminating excessive access is a continuous process of designing least-privilege policies, analyzing usage, reducing the attack surface and flagging risks.

Survey Methodology

n=300 in the United States

Industry Segmentation

(% share of interviews)



Business Segmentation: Number of Employees

(% share of interviews)