IDENTITY GOVERNANCE AND ENTITLEMENTS MANAGEMENT FOR CLOUD INFRASTRUCTURE

IAM MISCONFIGURATION IS THE BIGGEST RISK TO DATA IN THE PUBLIC CLOUD

According to Gartner, by 2023, 75% of security failures will result from inadequate management of identities, access, and privileges.*

In IaaS/PaaS environments, managing access entitlements is your responsibility alone. But complex infrastructure and DevOps velocity make it difficult to enforce granular, least-privilege access policies where it counts the most.

- Thousands of identities, roles and policies to analyze.
- No contextual usage data to reveal risks and excessive privileges.
- Conflicting policies leave crown jewel data exposed.
- Dev and Ops teams make frequent changes to code and configuration.

Today more than ever, it is essential to govern identities and access in the public cloud. Our mission is to create a new cloud security solution that gives enterprises full visibility and control over access to critical data and infrastructure, along with policy enforcement, risk assessment, and automated remediation.

GET ACCESS ENTITLEMENTS UNDER CONTROL

Ermetic reveals the effective access entitlements in your cloud and enables you to automatically remediate risks to sensitive data and resources.

With Ermetic, you can:

- Achieve full visibility into all access entitlements (humans and machines).
- Automatically identify third party access.
- Prevent identity and access-based threats.
- Allow developers, IT, security, and DevOps to securely access the cloud.
- Govern access policies to ensure standards compliance.

THE ERMETIC SOLUTION

Ermetic addresses the most urgent challenge in IaaS/PaaS - detecting and mitigating identity and access related risk and governing identities, at scale.

Through continuous analysis of entitlements and activity, Ermetic powers least-privilege access policy definition and enforcement at scale for both human and machine identities. It provides full-stack insight into the effective access entitlements granted by configuration of identities, compute resources, data stores and the network.

CONTINUOUSLY ENFORCE LEAST-PRIVILEGE ACCESS TO CROWN JEWEL DATA

IDENTITY & ACCESS GOVERNANCE
• Enforcement of custom enterprise policies
• Provisioning of just-in-time access
• Auditing of access entitlements, reporting and SIEM

ACCESS THREAT PREVENTION
• Visualization of effective access entitlements
• Access risk assessment
• Enforcement of granular, least-privilege policies

AUTOMATION & ANALYTICS
• Continuous discovery
• Full-stack entitlement analysis
• Automated remediation via direct-to-cloud policy wizards and Terraform and Cloudformation templates

ANOMALY DETECTION
• Continuous monitoring of access activity
• Detection of suspicious behavior
• Threat prioritization and configurable alerts