Ermetic for Anomaly Detection and Response

Automate incident response by quickly finding the signal in the noise

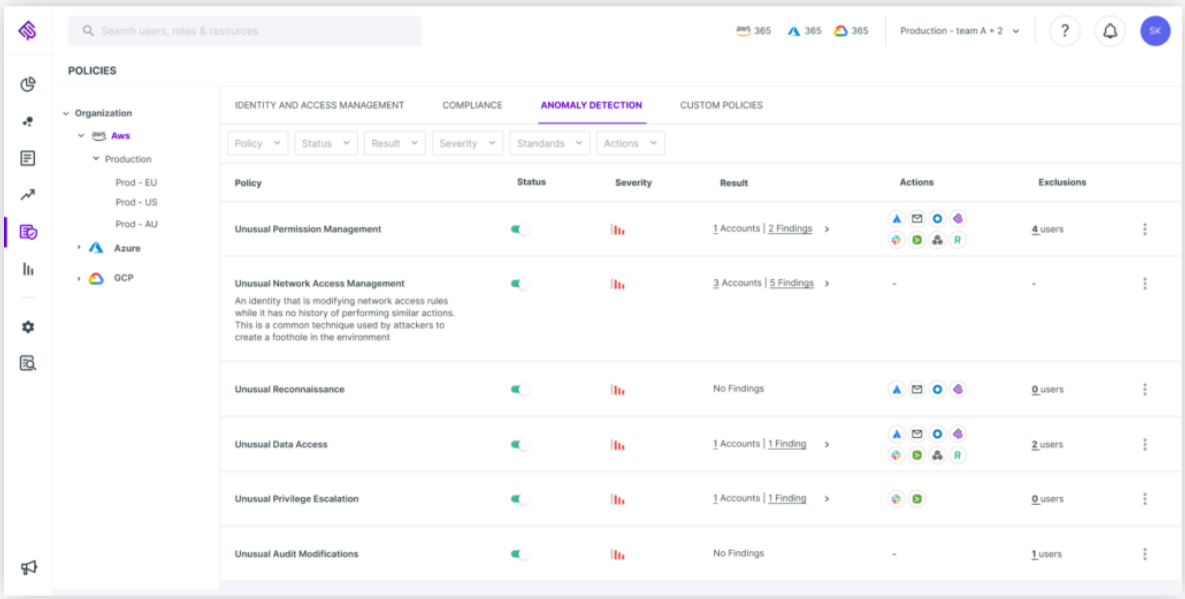
The dynamic, distributed nature of cloud environments often creates alerts that lack context at a volume that can overwhelm security teams. Manually sifting through log data and correlating it with multiple disparate feeds can quickly flood teams with false positives instead of actionable insights. To make matters worse, when suspicious or unusual activity such as misconfigurations or access-related risks are found, teams may quickly realize they lack the depth and context needed to get to the bottom of it. What if you could automate threat detection and remediation to eliminate noise enabling your teams to focus on what matters most?

Why Ermetic Anomaly Detection and Response?

- **Gain Deep Multicloud Visibility:** Get a deep, multi-dimensional, searchable view into all human and service identities, resources, entitlements and configurations in your multicloud environment.
- **Simplify Incident Response and Investigation:** Capture, analyze, and continuously monitor risk across access, entitlements and infrastructure configuration to alert and automate response on anomalous activity.
- **Uncover and Respond to Threats:** Context-rich alerts, visualizations and out-of-the-box integrations provide the information and the tools necessary to respond rapidly.

Detect Anomalies and Investigate Threats

Ermetic simplifies in-depth investigation by monitoring and reporting on suspicious or unusual activity across AWS, Azure and GCP. By creating a behavioral baseline for each identity captured across cloud provider log trails, the platform detects and turns anomalous findings into contextualized, risk-prioritized alerts.



Leveraging advanced analytics and granular visibility on access, entitlement and infrastructure configuration changes, Ermetic simplifies incident response and investigation. Upon identifying misconfigurations or risky privileges, Ermetic flags them, identifies the root cause and makes policy remediation recommendations based on actual use.

A centralized dashboard provides needed context to instantly assess and answer questions like:

- How is a specific resource actually accessed and/or used?
- What anomalies pose a possible threat?
  - Unexpected modifications such as disabling audit and logging
  - Network infrastructure changes like changing firewall rules
  - Configuration changes that affect public exposure of assets
  - Escalating privileges for users/roles/groups
- What unusual reconnaissance activity exists in my environment?
- Is there unauthorized use or theft of access keys?

Risk Factors- Misconfigurations / Vulnerabilities

Permissions Management

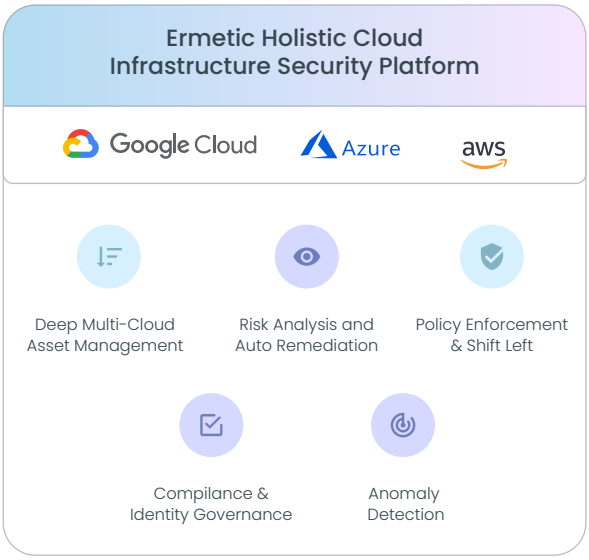
Behavior Detection

Armed with this actionable intelligence, Security teams can detect, investigate and remediate on the following use cases:

- Unusual data access
- Privilege escalation and other identity-related threats
- Changes in login settings
- Reconnaissance attempts
- Unauthorized changes to infrastructure configurations
- Unauthorized use or theft of access keys

The Ermetic Platform

Ermetic is a comprehensive cloud security platform for AWS, Azure and GCP that enables you to proactively reduce your attack surface, detect threats and reduce your blast radius in case of a breach. Ermetic's holistic cloud security solution enables comprehensive risk assessment across the entire security stack – from full asset discovery and deep risk visualization, prioritization and guided remediation to anomaly detection and compliance audit.



What Our Customers Are Saying

> "Ermetic has allowed us to focus on our business rather than concentrate only on cloud security"

Eugene Gorelik
VP Engineering at Airslate

Contact us!

Want to see our solution in action, and experience how easy it is to work with Ermetic?
Contact us at: **https://l.ermetic.com/get-a-demo**