Shift Left on Cloud Infrastructure Security

Secure identities, resources and network configuration, from dev to production

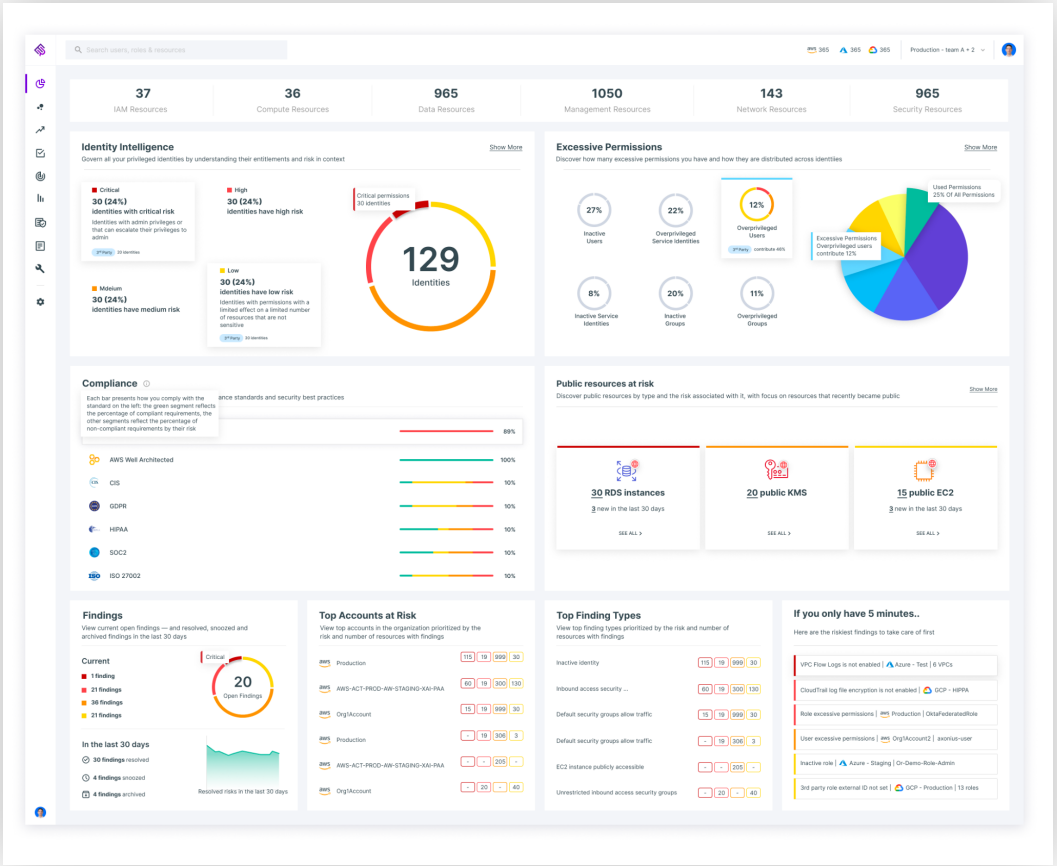
While the cloud has revolutionized how companies operate and develop new products and services, cloud security is very often an afterthought. With cloud-native technologies now enabling developers to move swiftly, testing and QAing applications before they can be deployed significantly slows down the process. So how can organizations ensure development speed while shifting left on essential security and compliance requirements? How do you enforce automated guardrails throughout the CI/CD development process and ensure no gaps exist?

Shift-left and Improve Security From Development to Runtime

- **Gain Deep Multicloud Visibility:** Discover all identities, permissions, configurations and resources in your environment to provide a contextual inventory for managing cloud assets and policy analysis that displays all access paths to specific resources.
- **Focus on the Risks that Matter:** Rich, risk-prioritized findings across the entire security stack helps you uncover toxic combinations while eliminating the manual labor of sifting through siloed alerts.
- **Just-in-Time (JIT) Access:** Enforce zero trust and least privilege by proactively managing and monitoring developer access to cloud environments. Provide full audit trails of all privileged activity.

Contextualized Multicloud Visibility

Ermetic enables teams to easily visualize and assess effective exposure, misconfigurations, excessive and risky privileges, leaked secrets and vulnerabilities. It also detects unusual data access, privilege escalation and other identity-related threats, as well as changes in login settings, unusual reconnaissance, and unauthorized use or theft of access keys. Ermetic analyzes cloud provider logs to reveal the identity behind each activity and affected accounts, resources and services.

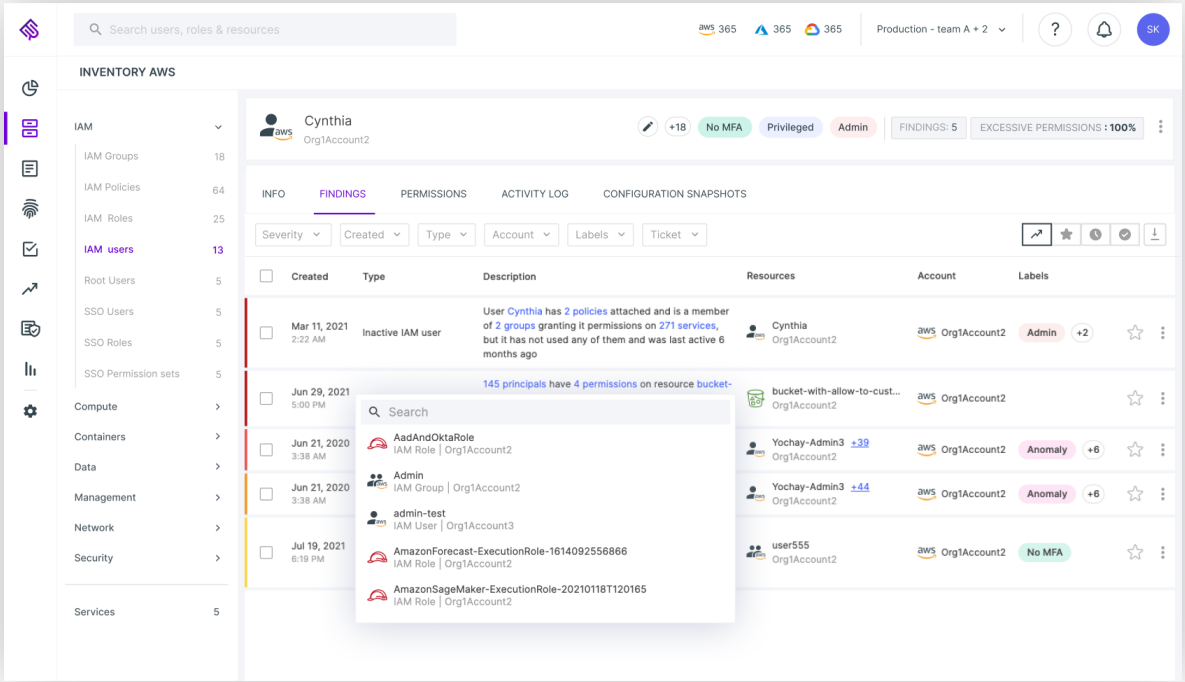


A centralized dashboard provides the needed context to instantly assess and answer questions like:

- How many entitlements are excessive?
- Where do I need to improve compliance?
- What are my top risks?
- What cloud misconfigurations exist in my environment?
- Is unencrypted data exposed or are secrets stored in vulnerable locations?

Prioritize and Focus Security Efforts

Ermetic empowers DevOps teams through customized prioritization and automatic remediation of risky privileges, excessive permissions and faulty configurations. When anomalies are detected, automated remediation kicks in - routing and assigning risk-prioritized findings to appropriate teams. Upon identifying misconfigurations, Ermetic flags them, identifies the root cause and makes policy recommendations for remediation. When risky privileges are detected, Ermetic generates least privilege policy recommendations based on actual use.

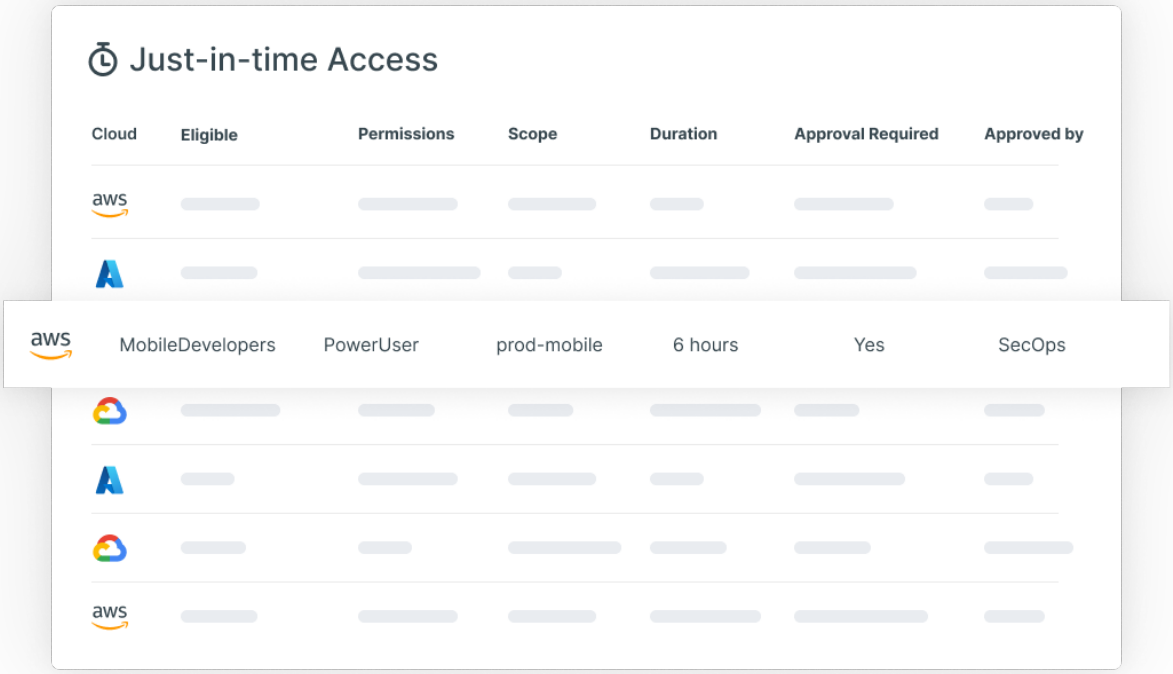


Ermetic expedites remediation and improves efficiency by addressing the following questions:

- How are stakeholders notified of a misconfiguration or at-risk identities?
- How are misconfigurations tracked until resolved?
- How do I define the best remediation method for each issue found?

Proactively Enforce Least Privilege with Just-in-Time Access

Leverage Ermetic's industry unique JIT access to grant developers and DevOps access to cloud asset accounts and proactively enforce the principle of least privilege. Ermetic ensures privileged activities are conducted in accordance with an organization's IAM and entitlements policies, IT Service Management (ITSM) requirements and compliance leveraging full user access behavior and audit trails.

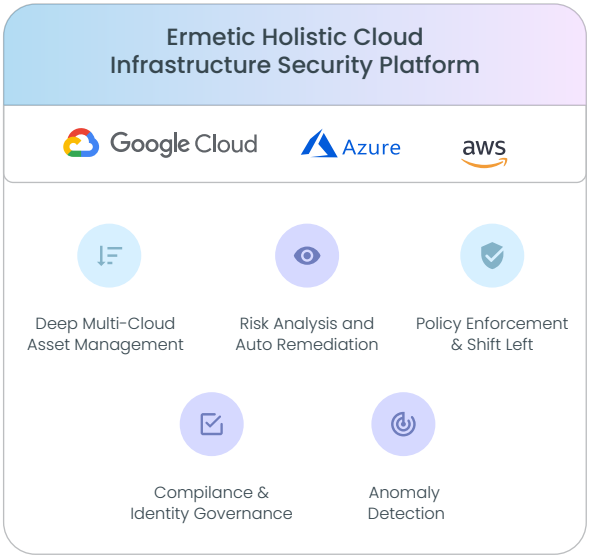


Enforce least privilege and zero trust with a dedicated dashboard that allows administrators to:

- Minimize risk of potential attackers exploiting excessive privileges
- Grant access for the smallest period of time needed for users to complete a task
- Streamline the process of both requesting and reviewing/approving access
- Automate the approval process for common requests to reduce friction

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

"We're using Ermetic to strategically push least privilege best practice as far left as we can. Ermetic automation is helping us reduce errors and inter team dependencies -- it's win-win for our SRE and security teams, and is fortifying our cloud infrastructure against risk."

Dominic Zanardi
Senior Site Reliability Engineer, Latch

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**