LATCH

AWS Tech Partner Value Case Study

> 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.

Zack Stayman, Senior Site Reliability Engineer, Latch

Latch Uses Ermetic's Cloud Security Platform for AWS to Automate Least Privilege for New Services

Latch Overview
Latch makes spaces better places to live, work, and visit. Latch delivers a full-building operating system designed to help owners, residents, and third parties like guests, couriers, and service providers seamlessly experience the modern building. They've done this by digitizing building access and control platforms that combine software, devices and services with advanced technologies for smart building usage, control and connectivity to improve and heighten the occupant's experience, safety and convenience.

Founded in 2014, today, more than 1 in 10 new apartments in the U.S. are being built with Latch products, 7 out of 10 of the National Multifamily Housing Council (NMHC) largest developers are Latch customers, and 36 states feature Latch buildings. Latch is a global team of 200+ team members working to reimagine the modern buildings of today and drive the evolution of the cities of tomorrow. Visit: www.latch.com.

Latch Use Case

Latch is focused on monitoring, maintaining, and improving the security posture of the Latch cloud environment. This includes identifying and coordinating the remediation of vulnerabilities, reviewing and consulting on cloud architectures, and developing tooling and automations for common security tasks in concert with security analysts and site reliability engineers (SREs).

It was extremely important for Latch teams to gain full visibility into all their AWS identities and any risks related to access permissions to the many AWS services the organization was using. Among the risks Latch sought to understand was potential Internet exposure of any of their AWS resources.

Latch also aimed to integrate mitigation of such risks into their organizational workflows. Further, laser-focused on enforcing least-privilege principle across their cloud environment, servers, databases, and SaaS platforms, Latch sought to leverage technology to bring least privilege efficiencies and accuracy to their site reliability team.

Ermetic Overview and Value Delivered to Latch

Ermetic is an APN Advanced Technology Partner, ISV Accelerate, and ISV Validated SaaS security solution that provides an easy understanding of potential cloud security risks that can lead to the breach of a client's environment. Ermetic differentiates through granular visualizations and analysis of combined exploits like cloud misconfigurations and the over entitled access rights that machine or human identities have over IaaS or PaaS cloud infrastructures. In addition, Ermetic has the unique ability to remediate these risks via IAM rights policy enforcement, allowing clients to focus and leverage an Identity Defined Security strategy like the principle of Least Privilege or Zero Trust.

- Ermetic provided Latch with a method to implement the principle of least-privilege access to their cloud environments.
- Ermetic provided granular visualization and analysis around Latch's cloud infrastructure risks associated to entitled identity permissions on various AWS services.
- Latch is leveraging Ermetic to identify potential AWS role access risk and public exposure of their AWS resources, and to identify and coordinate the remediation of these vulnerabilities.
- Through Ermetic's integration with tech partner solutions like Atlassian Jira and HashiCorp Terraform, Latch has been able to streamline their security response workflow automation.
- Latch's SREs are using Ermetic auto-generated least privilege policies in their AWS CloudFormation and Terraform templates to build secure AWS roles and policies into their new services.
- Ermetic has enabled Latch to automate periodic audits on all AWS IAM permissions, avoiding the expense of a third party Privileged Access Management platform.

Latch, in using Ermetic's cloud security solution, has been able to achieve a better Identify Defined Security outcome for their cloud environment. Ermetic has enabled Latch's Security Analysts and SREs to continuously provide cloud security architecture reviews and easily automate the analysis of AWS IAM policies and permissions. Compared to the organization's legacy approach, this has saved Latch hours of time and the headcount equivalent of three to four additional analysts.

Latch's Next Steps with Ermetic

- Latch plans to expand use of Ermetic recommended policies in their CI/CD pipeline to further implement least privilege practice and remediate any excessive identity entitlements during their IaC deployments.
- Latch seeks to leverage Ermetic reporting to produce compliance evidence for audit requests pertaining to cloud infrastructure.
- Latch would like to consolidate their existing security tools and leverage Ermetic's anomaly detection feature to proactively spot and mitigate AWS cloud security risks early on.

About Ermetic

Ermetic provides identity-first security and compliance for cloud infrastructure. In one easy-to-use SaaS platform, Ermetic combines cloud identity governance and security posture management - for comprehensive risk mitigation across multi-cloud identities, network, data, and workloads. Designed to improve productivity for overstretched security teams, Ermetic does the heavy lifting, combining sophisticated risk analysis with intuitive visualization, accurate prioritization and automated remediation. Even in the most complex environments, Ermetic makes it possible to reduce the cloud attack surface, enforce least privilege and protect sensitive data at scale. The company is led by proven technology entrepreneurs and is backed by Accel, Glilot Capital Partners, Norwest Venture Partners and Target Global.