ermetic | Case Study

KiKa

> Ermetic is addressing a use case that none of our other cloud security solutions does: giving visibility, and letting security gain trust and build collaboration with devops and other teams to mitigate identity risk.
>
> Etienne Smith, CTO, Kikapay

Kikapay is a cloud native company offering KiKa, an online payment service launched in 2020 to make the world of online banking fairer for everyone. KiKa delivers to organizations a cost effective payment service while giving customers more visibility and control over their payments.

The Challenge

Kikapay partnered with MOHARA, a UK based digital product design and development solutions provider, to build Kika, their revolutionary online open banking payments SaaS offering. The requirement was for a scalable, secure architecture able to support fast changes and multiple products in parallel. The developers used a standard framework — a containerized Kubernetes cloud environment based on domain-driven design principles. In Kikapay's formative stages, the product team built multiple designs for different projects, constantly testing them in the market.

To keep up with the constant change, the MOHARA team integrated different AWS services, which led to a large number of IAM configurations, service accounts, roles and AWS services. Putting the product first, they often overprovisioned the security profile, intending to fix things later. In reality, when a new idea was prioritized, other products were sidelined, posing security risks.

"There was a lack of accountability, a lack of visibility into what was really going on in our AWS accounts," recalled Leo Thesen, Senior Engineer and Security Technical Lead, MOHARA. "We had a lot of vulnerabilities we couldn't see, and were managing our security profile manually."

They also needed a friendlier way to be transparent to non technical security stakeholders — Kikapay's founders, project managers, product owners, and MOHARA's engagement leads — individuals involved in product planning and delivery but not necessarily software development. And they sought to adhere to the fintech's obligations regarding industry compliance.

> "Ermetic became the guiding light, telling us 'this stuff is okay' and 'don't worry about this, tend to that.'"

Leo Thesen, Senior Engineer and Security Technical Lead, MOHARA

The Solution

MOHARA began using Ermetic for their Kikapay project about one year ago. Recounted Thesen, "Ermetic came in and automated our general security profile management, making sure we didn't have risks left open by sidelining a project. Today, Ermetic is like a mentor that tells us: slow down, you forgot some things or you've done it wrong here. It's quite helpful to have Ermetic as an all-watchful overseer of our security profile."

Keeping agile development processes secure.
Key to a successful development cycle for a cloud native startup is an engineering model that lets team size scale or shrink on demand, to meet changing project requirements like speed up a release cycle. Clarified Thesen, "But in moving engineers to different projects, with many hands touching many things, you incur security risk. You try managing it but wind up leaving IAM accounts untouched for years or don't rotate keys or give access to buckets you shouldn't."

Thesen saw that when a team grew, responsibilities shifted: he became less involved in security reviews as engineers took on more IAM configuration and infrastructure creation. "That's when privileges can get out of control, with access granted excessively just to get the feature out. These are things Ermetic really helps with, providing reminders for when team sizes scale."

The development team for Kikapay uses Terraform for their infrastructure changes, tracking all changes with a GitOps philosophy of accountability in code. Explained Thesen, "But going line by line isn't going to be possible at some point.

Ermetic reporting tools are fantastic here, to identify highest risks and put them in Jira for investigation, and for helping us see after a sprint if we incurred any issues, and prioritize them and put them in our security tech debt. We use Ermetic alerts to let us drive an investigation."

Security as one of the highest "ilities" in fintech

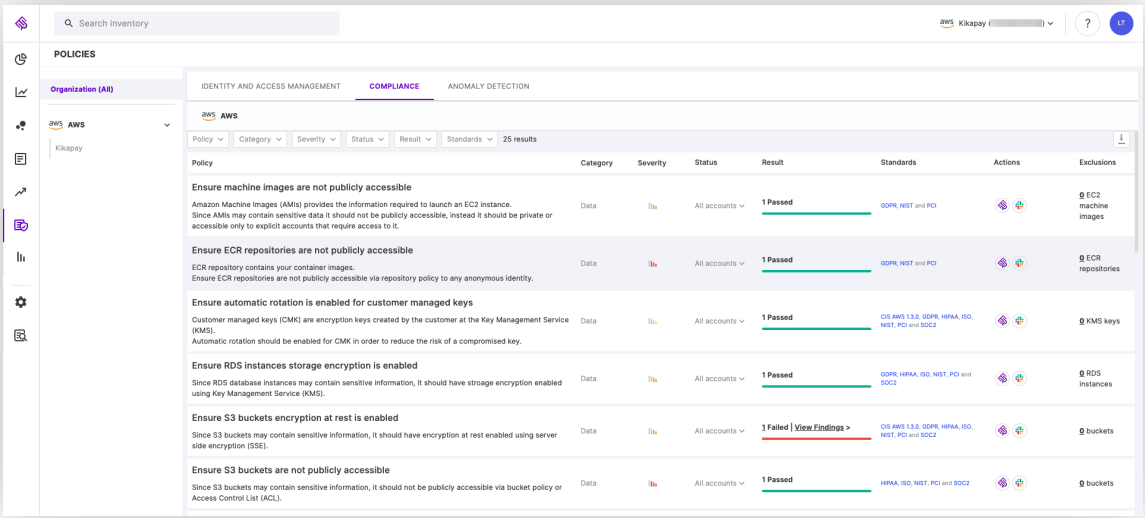
Thesen continued: "When you're working with a financial application in the cloud, security is one of your highest "ilities" — good security is a hallmark of good software. We faced our first security penetration test at the eight month mark: we had to pass it, and it was terrifying. In the cloud you have a million moving parts, attack points and vulnerabilities, especially in identity and access management."

"Ermetic became the guiding light, telling us 'this stuff is okay' and 'don't worry about this, tend to that,'" recalled Thesen. "Ermetic helps you know when to say your security is 'done for now.' It gave visibility into our cloud infrastructure — insights into what is actually happening in the system: are our configurations correct, are any IAM security possibilities providing back doors? Are secrets exposed, are packages outdated, are containers scanned before pushed? The third party testing company came in and was very complimentary — gave us a few tips and we were done in a few days."

Noted Etienne Smith, CTO, Kikapay, "Security audits in the cloud are no trivial matter. By enabling us to jump through the audit hoops, near effortlessly, Ermetic proved itself not just as a capable technology and time saver — it's actually helping us grow the business."

Addressing compliance and security posture using Ermetic

As a fintech company, Kikapay has to adhere to Financial Conduct Authority (FCA) compliance and many requirements regarding data retention and sensitive data transfer. "These compliance needs influence our architectural decisions and the risk profile we choose to create," said Thesen. "You can never do enough to enhance your security — more encryption, more logical barriers… that sort of thing — and Ermetic plays a big role in helping verify if our security profile is good enough for addressing our compliance obligations."



Kikapay uses Ermetic to ensure their security profile is aligned with financial and other compliance needs

He added: “There are a million ways to implement an architecture and there’s not much information about how to adhere to requirements in a cloud environment because it’s a world dictated by enterprise architecture. Ermetic is really good at setting up architectural paradigms and helping us adhere to best practices in terms of speed of development while ensuring that the security protocols have been set down."

Why not AWS native tools?

“Before implementing Ermetic, we used AWS’s Trusted Adviser a bit and the AWS IAM console to see permissions boundaries,” Thesen explained. “But AWS tools didn’t let us see enough… or take us to task when they were excessive.”

Added Thesen, “We get bombarded with new AWS features — I know they’ve come out recently with capabilities around access risk — but frankly, historically, I struggle to use AWS tools due to their poor UI. I got certified in AWS solutions architecture but the Ermetic platform is just so easy to use. Ermetic clearly puts UI and UX at the forefront; its user experience is a key attraction for us and how it interacts smoothly with our development cycle and project management processes, and offers great reporting tools. I doubt AWS, today or in the future, can be as quick and adaptable.”

Next steps

“Right now, we tightly govern the entry points into our system,” explained Thesen. “Going forward, we are planning a strategic self-service for SMB that will let KiKa prospects independently try out our large offering of payment options. Not having a touch point on the sales side will open our platform to much more risk from breaches. Ermetic will play a big role in what we deem good enough security and how we monitor it continuously to ensure we don’t incur new security regressions."

Conclusion

"Our mission is to build an evolutionary architecture that thrives under the constant change of a cloud infrastructure," said Thesen. "Ermetic enables us to be confident that our security profile is sufficient, for revisiting at another time. Ermetic lets us define thresholds as we set and reach security milestones, allowing for incremental change and improvement."

He added: "In the big, scary world of finance you need to make sure you don't slip up. Ermetic is our number one monitoring tool for showing the security state of our current production version and ensuring that a change to a service doesn't create risk, helping us prevent regression."

Summarized Smith, "It is increasingly obvious to me — and to all our security stakeholders — that Ermetic is enabling us to run our game changing online payment service more securely and easily."

About Ermetic. Ermetic helps prevent breaches by reducing the attack surface of cloud infrastructure and enforcing least privilege at scale in the most complex environments. The Ermetic SaaS platform provides comprehensive cloud security for AWS, Azure and GCP that spans both cloud infrastructure entitlements management (CIEM) and cloud security posture management (CSPM).

www.ermetic.com

Contact us