APONO

Case Study

Scaling Access Security to Enable Successful Cloud Transformation with Apono

INDUSTRY	SIZE	HQ
Technology	400	San Francisco, CA

aws MySQL

94%
reduction of blast radius and attack surface risk in the first two months

80%
of requests are approved and granted in seconds

98%
spike in time savings reviewing, approving, and provisioning access

Meet the Company

The customer is a technology company that helps its clients remediate issues faster by providing actionable, AI-driven insights to resolve problems before they escalate.

Challenge

The Scale and Complexity of Privileges Complicate Cloud Security

A leading technology company handling sensitive customer data was transitioning to the cloud.

The team quickly realized that their existing solutions for managing privileged access in on-prem environments were ill-suited for their new hybrid infrastructure. They struggled to detect resources or entitlements within their cloud environment, leading to significant blind spots and increased security risks.

"Security in the cloud is about more than just managing credentials in a vault," says the team's AWS security engineer. **"I need more visibility and context than simply whether a user is or is not an admin."**

Solution

Securing Hybrid Environments with Granular J ust-in-Time Access Controls

As their infrastructure and databases expanded across cloud and on-prem environments, the security team partnered with Apono to gain better control over privileged access in their hybrid environment.

A key factor in the company's decision to choose Apono was its ability to continuously and automatically discover resources across cloud and on-prem environments.

Apono's unified view of all the company's resources made it simple to understand who had access and how it was used. The security team gained deep visibility into how engineers accessed their PostgreSQL and MySQL databases in AWS RDS for the first time.

Using this context, they implemented granular Just-in-Time access policies. Engineers with privileged access to production databases in AWS RDS could request short-term access to sensitive resources with their managers' approval via ChatOps platforms like Slack and Teams, as well as through Backstage and CLI. However, lower-risk databases—such as those lacking customer PII or other sensitive data—were governed by policies with longer time frames and automated approvals. This minimized friction while enhancing productivity.

"Apono's value isn't just in saving my team hours of effort by automatically discovering resources in our environment," says the AWS security engineer "It enables me to close the loop end-to-end by turning entitlements into secure access policies that eliminate standing privileges and reduce our risk of incidents."

Outcome

Transforming Security Controls into a Productivity Enabler

In the first two months after implementing Apono, the company reported a **94% reduction in their blast radius** due to Just-in-Time access controls eliminating their risky standing access. By limiting standing access, these policies acted as tight guardrails that prevented privilege abuse.

"One of our greatest achievements in the first month was shifting away from credential management and instead focusing on controlling access," says the AWS security engineer.

With Apono, productivity has surged. More than 80% of access requests were approved and provisioned within seconds by making lower- to medium-risk resources available through automated access policies. This process optimization saved engineers hundreds of hours that would have otherwise been spent waiting for approvals.

The DevOps team also experienced a dramatic improvement, **spending 98% less time handling access requests.** These time savings were largely due to Apono's dynamic **Access Flows**, which automatically adjust access policies as new context is collected. This reduced the team's need to manually maintain policies or create new ones as resources were discovered.

"We've succeeded in creating a frictionless experience for our developers, DevOps, product teams, and everyone who needs access to sensitive resources," says the AWS security engineer "And all while ensuring our security team retains full control and auditing capabilities."

"The most eye-opening moment of Apono's value came when I saw the gap between our previous state—where access was left open simply because the request process was too cumbersome—and our current state," he adds. "Now, requesting access is as simple as automating a request in Slack. This allows me to eliminate standing privileges without slowing down the business."

Next Steps

Following their successful rollout of Apono for databases in AWS and on-prem servers, the security team plans to expand Just-in-Time access controls to their **Azure cloud infrastructure and additional environments, including GitHub.**

About Apono

Founded in 2022 by Rom Carmel and Ofir Stein, Apono is redefining cloud security with its Cloud Privileged Access Platform. With decades of expertise in cybersecurity and DevOps, Apono enables organizations to adopt just-in-time, just-enough privilege access, seamlessly bridging the gap between security and engineering teams. Trusted by Fortune 500 companies, Apono's platform empowers enterprises to enhance operational efficiency while maintaining robust security controls. Recognized in Gartner's Magic Quadrant for Privileged Access Management for two consecutive years, Apono is at the forefront of innovation in secure cloud access management.

APONO

www.apono.io

@Apono_official

@aponoio