

Apono Enforces Access Accountability for a Cybersecurity Leader

INDUSTRY

 Cybersecurity

SIZE

 700+

HQ

 New York City

 aws

Reduced
Excessive
Admins by

93%



Required
justifications for
access requests



Simplified
management
for fast time-to-value

Meet the Company

This customer is an international cybersecurity firm that protects mission-critical infrastructure from cyber threats.



Challenges

Overcoming Security Debt Pains Scaling from Startup to Large-Scale Business

The company has experienced exponential growth in recent years as the global risk to critical systems has expanded. As part of the maturity process from a startup to a leader in their field, the company is taking significant steps to strengthen its processes and security posture.

In beginning to dive into their AWS environment, the company's cloud security architect had several concerning discoveries.

One of the key findings was that there were too many admins everywhere. "Lots of folks with full star access," says the cloud security architect, "Too many cooks in the kitchen is an expression that came up quite a few times because we have 40 accounts but 80 or so admins, any of which could cause severe damage to the company tomorrow."

The second was the lack of audit logging. "It was maybe our biggest blind spot," he says, explaining that it was not just the lack of visibility into overly permissive users but the ability to track down and find who did what in their cloud environments.

The cloud security architect sought a solution to reduce the number of admins and restore accountability.



Solution

Efficiently Implementing Just-in-Time Access with Game-Changing Auditability

Early in their search, the company considered several access management solutions on the market. However, after initially testing competing solutions, they found they were not sufficiently mature to meet their needs.

"These platforms were overly complex to manage and required a lot of maintenance," says the cloud security architect, adding that they were missing the rightsizing feature that Apono offers.

After comprehensively evaluating the market solutions, the cloud security architect advocated for Apono.

"All of it seemed to be a bit more mature, and frankly, just a superior platform to what the others were offering," he says, explaining that, "With Apono, within five minutes, I was able to start setting up a Just-in-Time access flow and configure it with its simple user interface."

One of the standout capabilities that has dramatically improved is the capacity to monitor access.

"I'm seeing better auditing, better logging, and the ability to track sessions," says the cloud security architect. **"I love the visual user story feature of Apono. That was a game changer for me and a big part of why I chose the Apono platform.** If you crack open an access request, you can see what they did in a single pane of glass, which is definitely not something you can do with CloudTrail."



Outcome

Justifying Access and Restoring Accountability

The company is up and running with Apono in the AWS environments and continues to expand to the rest of the company.

For the cloud security architect, the first significant and noticeable win within the first month of using Apono was bringing the number of admins in key accounts down from 80 to six.

However, the achievement he is most excited about is how Apono has enabled his small team to quickly and seamlessly implement a structured, Just-in-Time, least-privilege access management process that is fully monitored and auditable.

"People are accountable for their work," he says, noting, "If somebody goes in and breaks something, we can find it easily and know who did it. **Every request must have a justification, and Apono's ability to be that critical gatekeeper has been a major value and win for us.**"




Next Steps

Having succeeded with AWS, the next step for this cybersecurity leader is to roll out for Azure, followed by GCP. After they have JIT and JEP for their cloud infrastructure, the architect has his eyes set on tackling use cases specific to data center access, expanding security access to more critical areas of the business.

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. © 2025 Apono Inc; All rights reserved.

APONO

 www.apono.io
 @Apono_official
 @aponoio