

Labelbox Secures Kubernetes Access with Apono

INDUSTRY

SIZE

HQ

URL



AI



200



San Francisco, CA

labelbox.com



98%

Attack Surface Reduction

92%

of manual approvals were <2hrs

90%

reduction in requests for risky access



Meet Labelbox

Labelbox is the data factory for generative AI, providing high-quality, differentiated data to leading model builders and enterprise AI teams. Labelbox customers include Fortune 500 enterprises and leading AI labs.



Challenges

Excessive Kubernetes Privileges Expanded Access Risk

As a cutting-edge provider of AI data services, Labelbox is a significant user of dynamic technologies like Kubernetes to serve its customers. While speed is a top priority, so is security.

Labelbox's Sr. DevSecOps Engineer Aaron Bacchi sought to tighten controls around engineers' access privileges to their Kubernetes pods, cutting down the availability and scope of access privileges.

Aaron found that engineers retained access to privileged Google roles which were infrequently needed. These roles allowed them to perform risky actions on pods, including editing and viewing secrets. He sought a solution to eliminate excessive standing access without slowing down their work.



Solution

Migrating from Over-privileged Standing Access to Just-in-Time RBAC Roles

Recognizing his problem, Aaron interviewed his engineers to understand what they needed. He compiled several use cases for how they use their access to Kubernetes pods when they interact with them directly.

"I was able to create these fine-grained custom RBAC roles in Kubernetes that provide exactly the privileges needed for specific tasks, and then I manage access to those roles via Apono," says Aaron. **"Now, engineers can combine narrow roles together like Lego bricks to achieve their goals."**

By breaking up risky privileges into more specific capabilities that his engineers actually needed, Aaron reduced his overall risk from an overly powerful Google role without harming his engineers' ability to do their jobs.

Now, all access to Kubernetes is available on a temporary, time-bound basis that is fully monitored and controlled by Labelbox's access policies.

Reducing the Blast Radius Without Impacting Productivity

Aaron smoothed the transition to Just-in-Time by giving his people time to use the more fine-grained RBAC roles in Kubernetes before removing the highly privileged Google engineer role from service.

Aaron made access to the privileged RBAC roles available upon request without initially removing anyone's access privileges. This allowed him to significantly reduce his blast radius from an account takeover. In making the roles

requestable instead of revoking them, he was able to avoid pushback from engineers who still needed this access. Surprisingly, out of the 50 people eligible to use them, only a fraction (10 or so) requested access.

“My manager was excited about tightening up our Kubernetes security,” says Aaron, reflecting on how the engineers self-sorted into groups: those who needed access to riskier privileges and the vast majority who did not. This change eliminated unnecessary risk by preventing standing access from being left open 24/7.



Outcome

Implementing Risk-based Access Management

In adopting a Just-in-Time approach that eliminated his risk from standing access to sensitive Kubernetes pods, Aaron had the breathing room to implement risk-based tiering for Labelbox’s access policies.

For low-risk resources in the development stage, all users retained view-only privileges. The friction level was also ratcheted up as the risk level rose with the range of actions a user could take in increasingly sensitive environments. Aaron created policies for automated approval of medium-risk actions requestable through Apono.

“They don’t have to wait for a human,” he says, explaining that they can get that access for eight hours at a time, seamlessly able to make necessary changes in their staging environment in a way that is monitored and controlled to meet his risk tolerance and security policies.

For his most sensitive resources like production, an engineer would still need to request access and get manager approval to make any changes there. In addition, the engineer would have to use MFA through Apono.

“There’s a little more friction for production changes, but that’s how it should be because of the seriousness of that environment,” he says.

This way, everyone still could gain access to resources with the privileges they needed, but it was now fully monitored and under control. It reflects a rational ratcheting up of friction as risk rises, which is great for maintaining system security and compliance.

Next Steps

As more features and services are created and offered by Labelbox, new teams are formed around them, which requires establishing the correct balance of access to critical systems.

Aaron plans on enabling his team members to take a more proactive role in creating Access Flows in order to accommodate the newly formed teams. He plans to roll this initiative out using the new RBAC roles in Apono for secure management of access that will allow different stakeholders appropriate levels of privileges such as creating Access Flows or viewing for auditing purposes, while restricting the highest level admin role for power users like himself.

This plan comes as part of his overall effort to increase transparency and training across Labelbox, educating engineers on how to most effectively access resources using automation where possible to empower greater productivity.

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