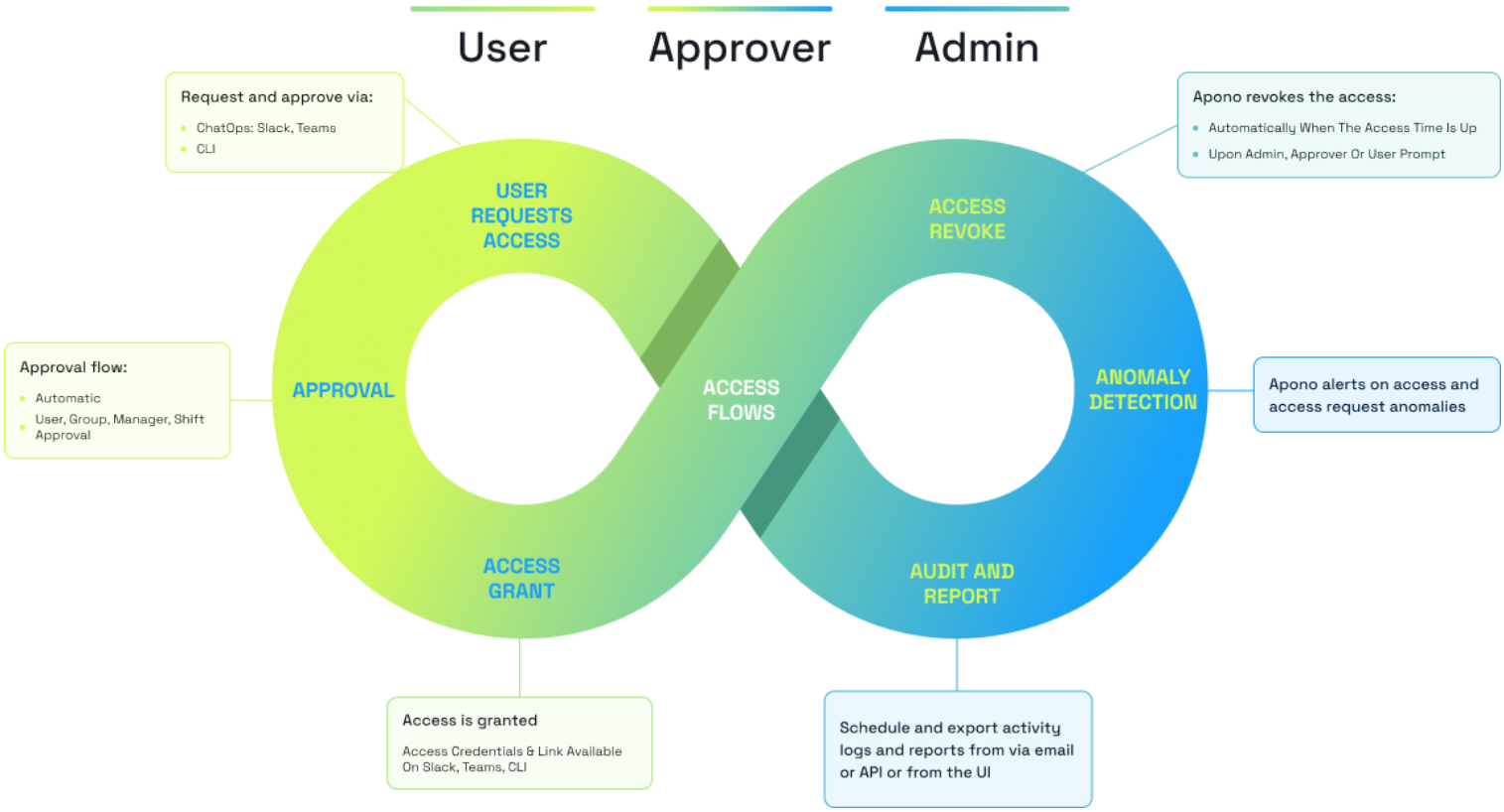
Why Choose Apono

Apono is the best solution for just-in-time, temporary access to sensitive cloud resources

---

Apono lets you automate static access policies by turning them into declarative, dynamic Access Flows. Integrate your cloud environment, CI/CD stack, cloud infrastructure and databases with Apono. Create Access Flows with our declarative UI or in Terraform, and your developers can use Slack, Teams or CLI to request and approve access.

Protect what matters without breaking a sweat.



The Apono Access Management Life Cycle

Who is Accessing Cloud Resources Right Now?

Do developers have admin/write access or read-only access to production?

Can you answer that, or must you sort through your cloud resources to find out? Of course, by the time you get to the last one, you'll have to recheck the first because so much time has elapsed, and access changes

constantly. While discussing it, how long would it take to revoke access to a production cloud resource in an emergency?

With Apono, you have a **single point of control** for managing access without creating a single point of failure.

Apono Access: Automated, Just-in-Time, Just-Enough

Use Apono for on-demand access to critical resources. Grant an engineer permission to fix a production issue in an emergency. Grant a data scientist access to a data lake when needed. Just as important is to revoke access once it's no longer needed.

Apono's permissions are just-in-time and also ephemeral. Access is automatically revoked when no longer needed. No more forgotten privileges or group memberships left open. Access begins and ends according to Access Flow definition.

Access Management that Scales

No need to manually change permissions for each resource on your cloud platform every time someone needs access to one of its resources. While access can be granted at a granular level, large-scale environments can be managed efficiently by creating Access Flows, for individuals and groups, to all cloud resources and assets.

Your environment is always evolving, and so does Apono. Use hierarchies, tags and exclude for dynamic access management.

Apono Integrates with Terraform

Are you using Terraform to manage your cloud platforms?

That's great because Apono is a Terraform provider and can be provisioned to work alongside your resources by adding code blocks to integrate them into Apono. When you bring up a resource, it will immediately benefit from Apono access management.

Apono lets you turn static access policies into dynamic Access Flows directly from Terraform. Reuse a simple build file to build the perfect workflows for your organization without ever leaving Terraform.

Designed for DevX

With Apono, you will work smarter with less effort to manage and gain access to your cloud resources. You will take control of your cloud resource inventory from one central location.

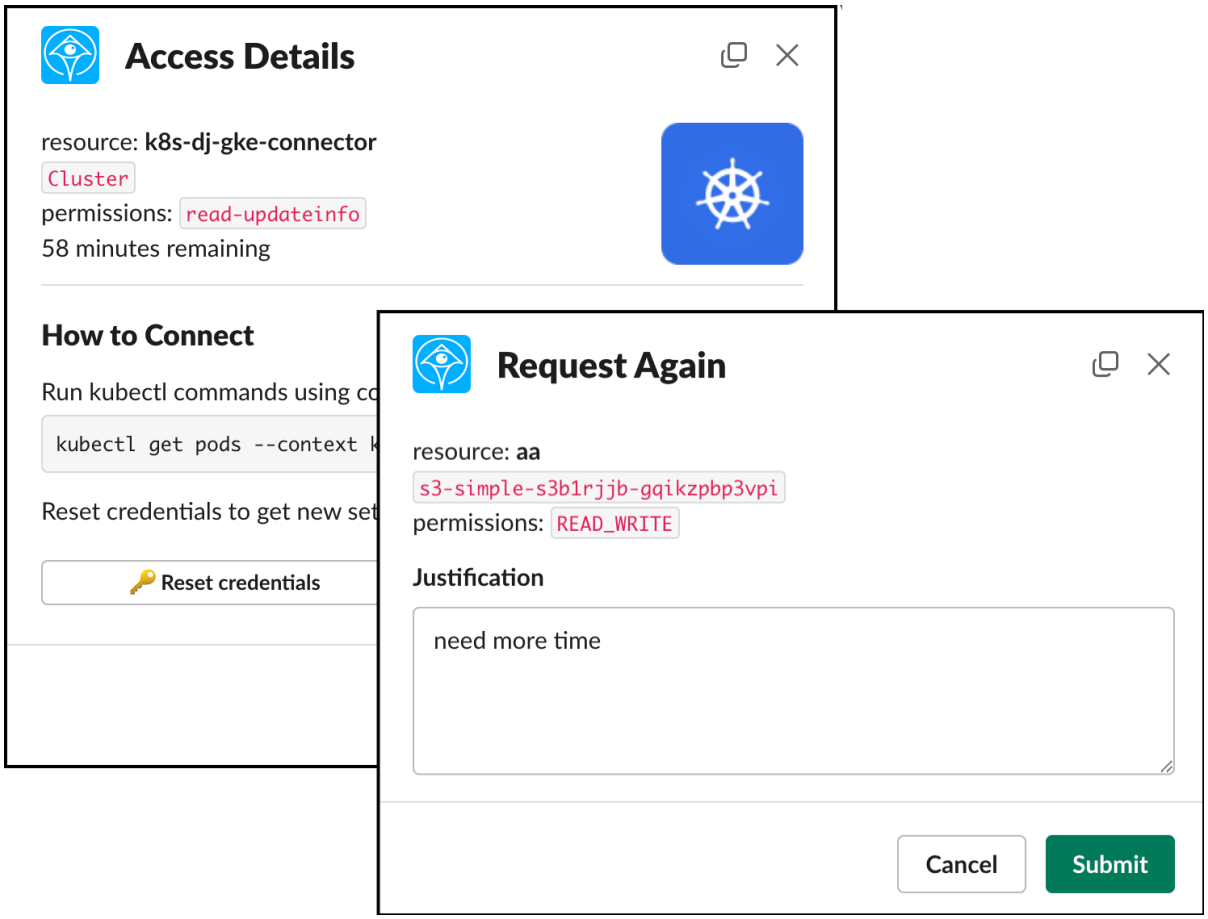
Apono's Access Flows prepare for contingencies, emergency access and regular maintenance. Onboarding becomes quick and easy, with our dynamic Access Flows and access bundles. There's no need for writing and maintaining home-grown scripts and complex workflows.

Your developers can request access bundles and get just the access they need exactly when they need it, no hassle.

Deployed Via Slack and Teams

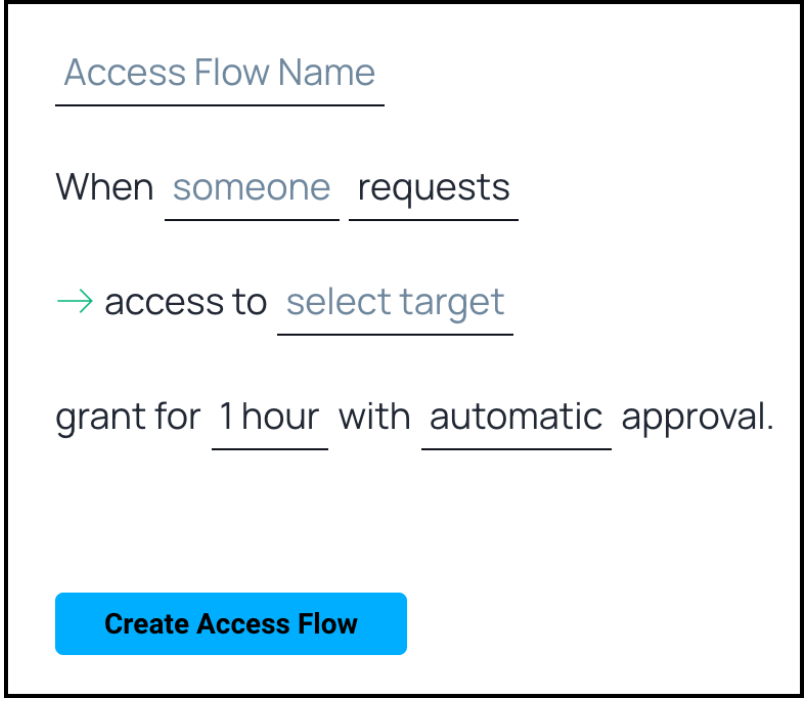
Developers and engineers love ChatOps and CLI, so why should they have to use another interface?

Apono integrates with Slack, Teams and CLI, so your R&D can use the tools they know to request & approve access, connect to the resources, and, after the access is automatically revoked, request the access again when they need it.

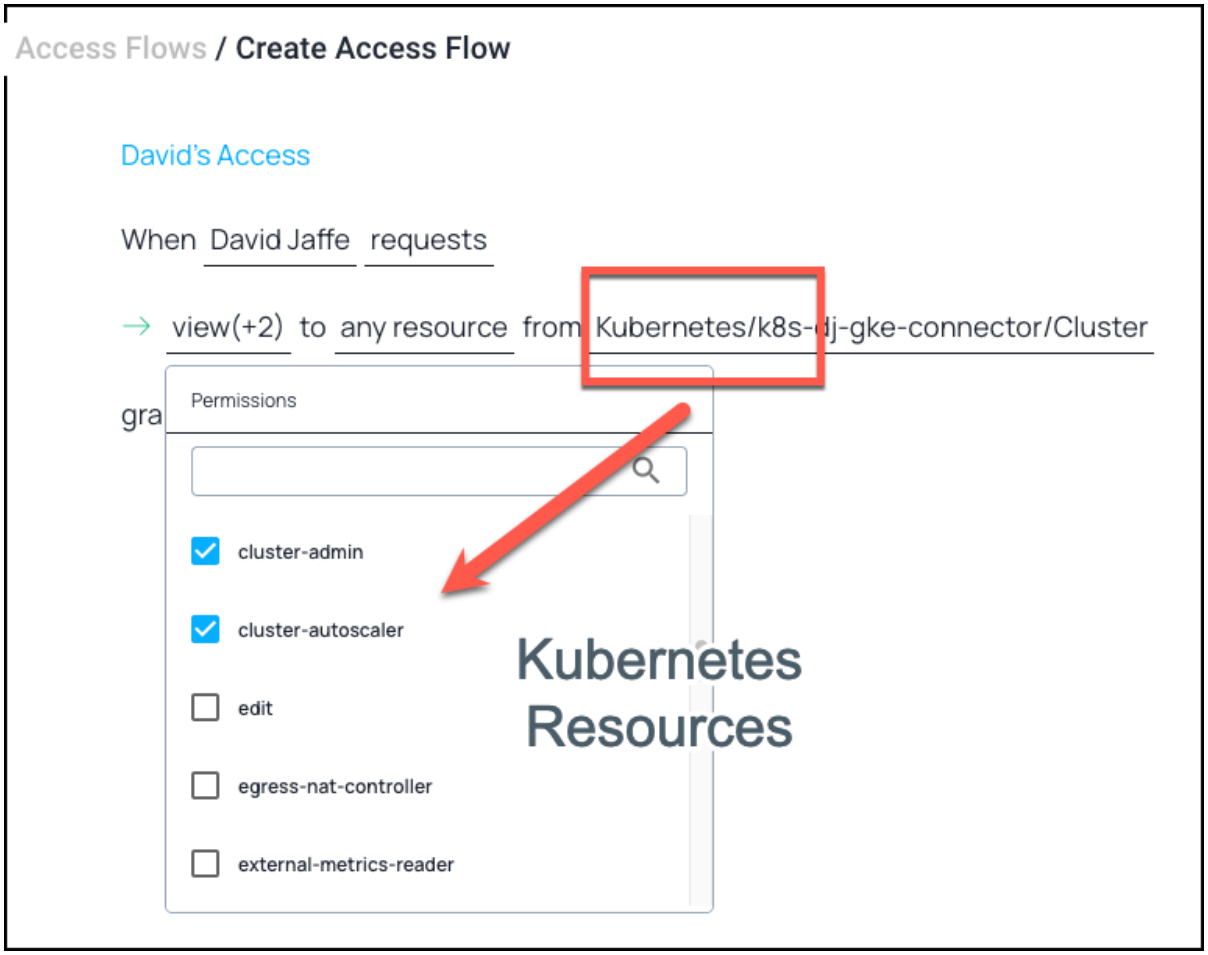


Speaks Your (Declarative) Language

Apono has developed a declarative, natural language format for defining access permissions. No need to edit config files. We call it **Access Flow**, and it looks like this:



Select a resource and then add (a) who is allowed to gain access (b) what kind of access (roles or permissions) to grant, (c) which specific resources in the integration to allow access to, (d) how long the access should last, (e) should access be approved automatically or by someone in the organization.



In fact, integrating with Apono and creating Access Flows has proven so intuitive that most Apono customers set up and **deploy access control for their entire organizations within two weeks.**

Keeps Your CISO Happy

Apono doesn't have access to any of your data. Ever.

How does it work? Install our connector in your environment, direct it to your secret store and you're done! The connector manages the data syncs to our app and handles access provisioning and de-provisioning to your services, without storing or caching secrets.

We call it **SasS with on-premise level of security**. And you can tell your customers that they can be confident that access to their data is protected.

A Home Run With SOX IT Controls

Apono's comprehensive access management covers your entire cloud, with Access Flows defined for every cloud service and resource type. Need to maintain least-privileges to production environments, financial data, PII, and other critical assets? Check!

Access requests and granted access are all logged, so you have a reliable audit of the access to your data. As part of your IT compliance reporting to SOX, HIPAA, GDPR, PCI DSS, SOC 2 and others, use Apono's audit logs and reports. Send them to external auditors, internal GRC and security teams, and export logs directly to ITSM, SIEM and compliance tools.

Updated 9 days ago

How Apono Works →