APONO

Datasheet

Apono Space Management

Secure, scalable access governance for fast-growing engineering organizations

Why Growing Organizations Need Space Management

As teams scale across clouds and environments, access governance stops matching how organizations actually operate. Policies pile up across teams, visibility becomes too broad, and small changes in one place can quietly affect another. Security teams are forced to closely supervise every update to avoid cross-team fallout, while proving clean segmentation for audits or customer reviews becomes increasingly difficult.

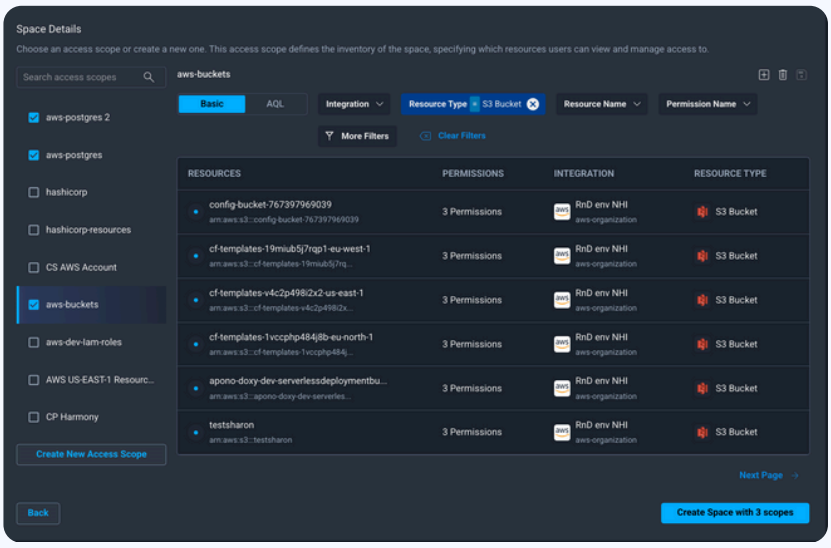
Space Management creates the boundaries needed to keep teams efficient and sensitive environments protected.

Common challenges include:

- Blurred boundaries create privilege exposure
- Global admins slow engineering workflows
- Compliance requires clear segmentation controls

Establish Governance for Every Team

Space Management creates isolated governance zones within a single tenant, allowing teams to manage their own access flows, scopes, and bundles. Users see only the resources relevant to their domain, reducing noise and preventing cross-team impact. Security maintains global oversight without becoming a bottleneck.



Key Benefits

Safely delegate access governance

Prevent cross-team privilege errors

Reduce risk across every cloud environment

Why Space Management Matter for Governance

As organizations scale, access policies spread across teams and environments in unintended ways. Changes in one area can quietly affect another, weakening governance and increasing risk. Space Management restores structure by isolating policies per team while security defines global guardrails.

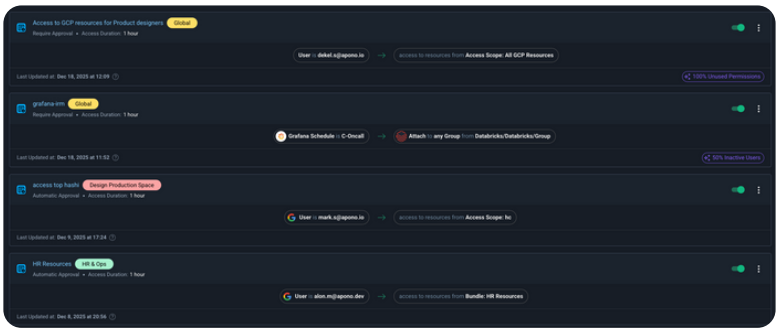
How Space Management Works

Space Management creates isolated governance zones inside a single Apono tenant. Each space has its own access flows, bundles, and scopes, while integrations like AWS and Kubernetes remain shared. Admins operate only within their assigned space, while security retains global visibility and consistent enforcement of Zero Standing Privilege.

Build Trust with Proven Segmentation Controls

Space Management enforces the boundaries required by enterprise and regulated customers. Clear segmentation demonstrates how sensitive systems stay isolated and how internal access is restricted to the right teams.

These controls map directly to SOC 2, ISO 27001, HIPAA, and SOX requirements for separation of duties and environment isolation, helping organizations win security-sensitive deals with confidence.



Benefits of Apono

Isolate Access Governance Per Team

Each team manages only its own access logic within defined boundaries, reducing privilege overlap and preventing cross-environment misconfigurations.

Strengthen Compliance with Clear Segmentation

Auditors and customers gain confidence from strict separation of duties and clean boundaries aligned with regulatory expectations.

Reduce Privilege Exposure Across Environments

Scoped visibility limits unnecessary access and reduces potential privilege sprawl.

Accelerate Engineering with Secure Delegation

Teams update their own workflows inside defined boundaries, eliminating central bottlenecks while maintaining consistent security guardrails.

Limit Inside Impact with Boundaries

Restricting administrative reach reduces misuse of privilege and contains the blast radius of insider-driven errors or threats.

Keep Workflows Stable Across Teams

Changes in one space cannot affect another team's configuration, preserving operational stability.

Enforce Consistent Security Guardrails

Global policies apply across all spaces, ensuring uniform enforcement of Zero Standing Privilege.

Improve Customer Confidence in Access Controls

Clear segmentation shows strong internal access governance, strengthening trust with enterprise and regulated buyers.

Scale Access Management without Complexity

Spaces Management supports organizational growth without duplicating integrations or overextending administrative overhead.

Control Access with Granular Precision

Permissions stay tightly scoped to each team's environment, preventing unnecessary organization-wide access.

About Apono

Founded in 2022 by Rom Carmel and Ofir Stein, Apono delivers a Cloud Privileged Access Platform purpose-built for modern, fast-moving environments. With support for both human and non-human identities, Apono helps security and DevOps teams enforce least privilege at scale without slowing down delivery.

Trusted by Fortune 500 enterprises and recognized in Gartner's Magic Quadrant for Privileged Access Management two years running, Apono is shaping the future of secure cloud access.

APONO

www.apono.io

@Apono_official

@aponoio