

How do cloud permission risks impact your organization?

As more organizations adopt multicloud infrastructures, identity permissions continue to increase across the 3 leading cloud platforms: Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP). Without proper visibility into who has access to what, organizations are leaving their critical cloud infrastructure at risk of permission misuse and potentially a breach.



The shift to multicloud presents new permission challenges

40,000+
permissions across major clouds and counting

1%
of permissions are actually used

> 50%
of these permissions are considered high-risk

> 60%
of Identities are inactive

> 50%
of Identities are Super Admins

Permissions

The ability for an identity to perform an action on a resource.

High-risk Permissions

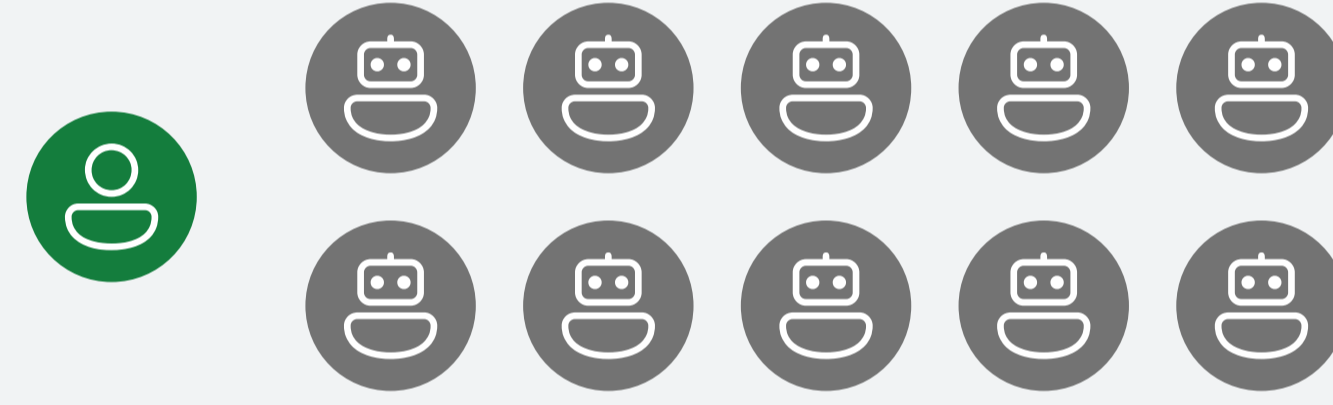
Any permission that, if used improperly, can cause service disruption, service degradation or data leakage.

Super Admin

A powerful account that can create and modify configuration settings to a service, add or remove identities, and access and delete data.

The rise of human & workload identities increases complexity across clouds

1:10 User identities to workload identities



User Identities

- Employees
- Customers
- External partners

Workload Identities

- Apps
- VMs
- Scripts
- Containers
- Services

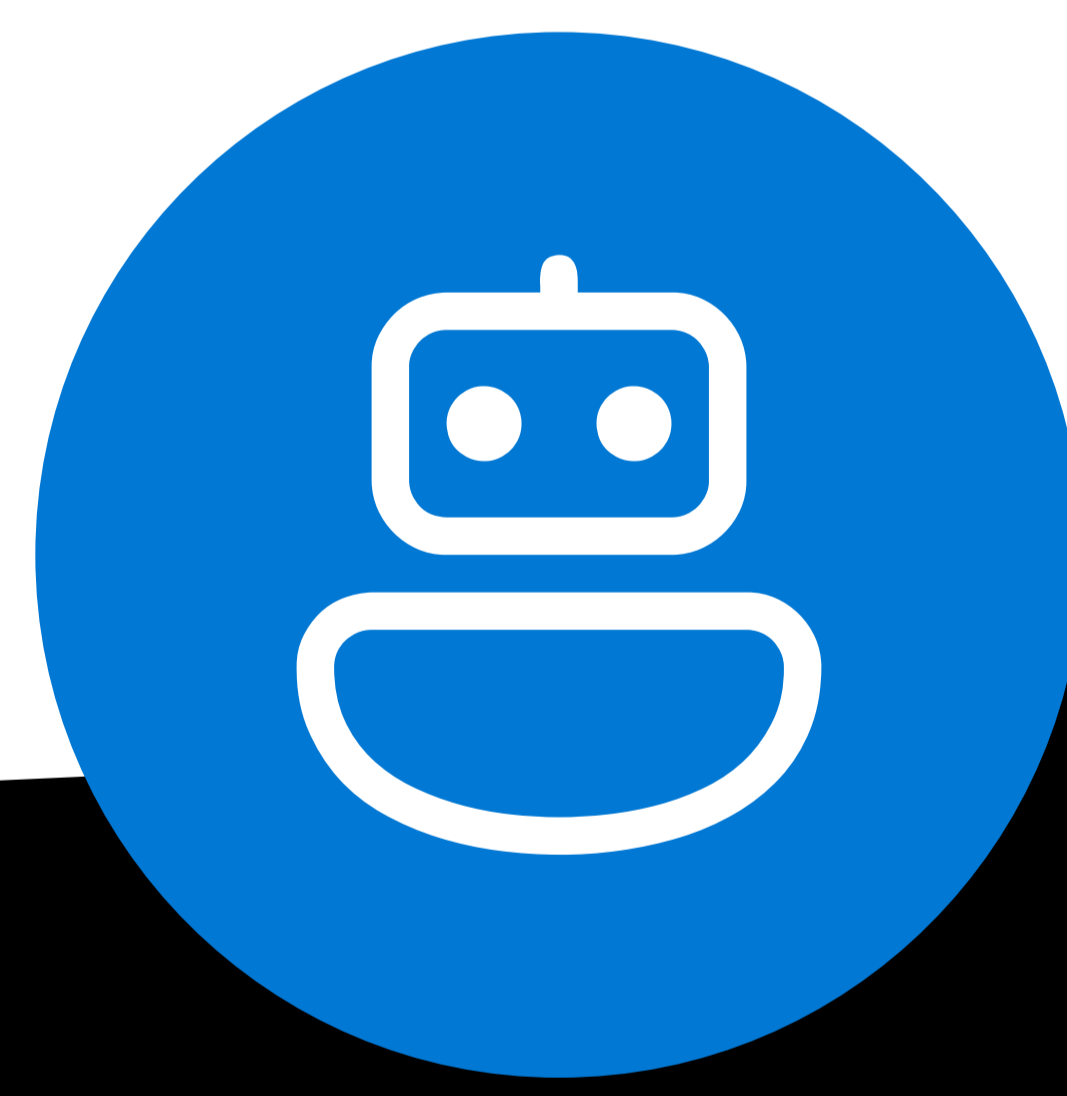
> 80% Of workload identities are inactive, double the percentage of 2021.

With access to all resources, Super Admins present a huge threat to your infrastructure



< 2%

of permissions available to Super Admins are actually used



> 40%

of Super Admins are workload identities

How can you prevent your cloud permissions from expanding your attack surface?

Discover

Assess your permission risks and identify what identity has been doing what, where they've been doing it, and when they've been doing it



Remediate

Grant permissions on-demand and just-in-time to ensure the principle of least privilege



Monitor

Continuously monitor permissions usage across clouds to prevent security threats