One platform for enterprise-wide access governance

Veza's solution unlocks the truth of access permissions, powering security and governance initiatives.

Privileged Access Monitoring

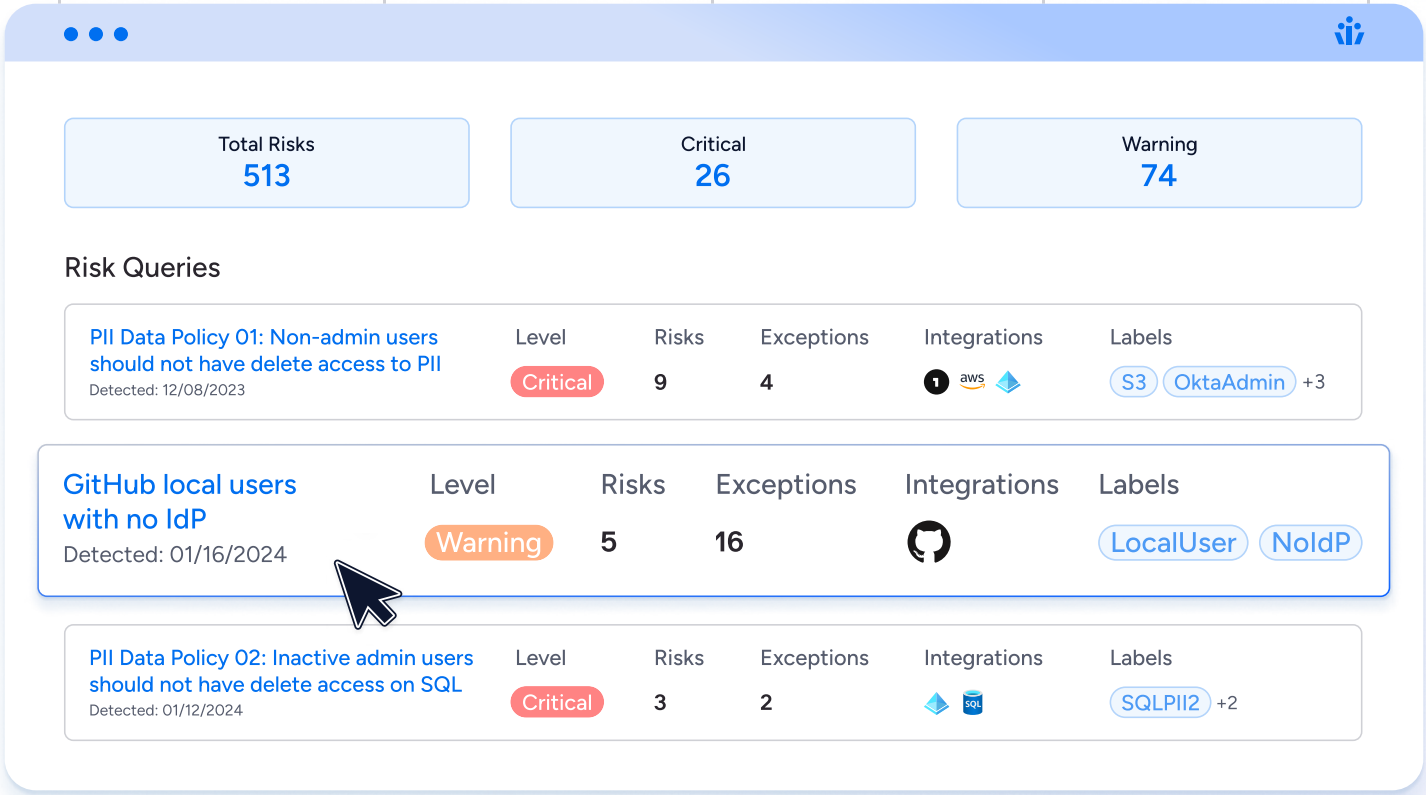
Continuously monitor authorization to your data crown jewels in any on-premise or cloud environment.

Identify and reverse privilege drift.

Monitor for new privileged accounts, including local admins not governed via your IDP.

Always know when a new identity gains access to sensitive data.

Discover Separation of Duties violations and toxic privilege combinations.



Cloud Access Management

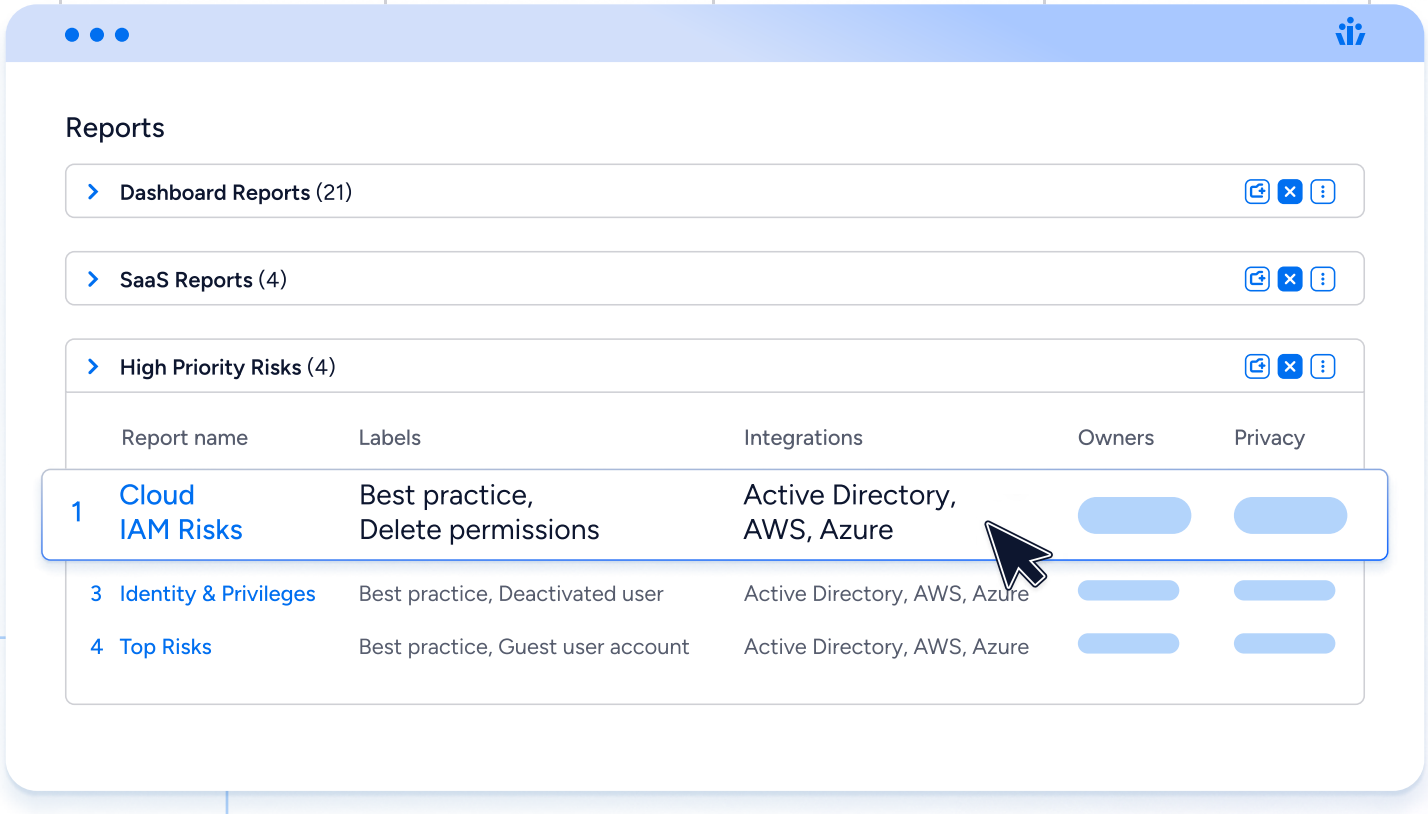
Untangle the complex web of cloud IAM to know exactly who can do what across AWS, Google, Azure, and Oracle cloud environments.

Find and fix cloud IAM misconfigurations that enable privilege escalation and lateral movement.

Root out inactive IAM users, dormant service accounts and ungoverned local users.

Fix your top cloud access risks before they can be exploited by an attacker.

Identify your high blast radius users: identities with broad access to cloud resources and represent the greatest risk if compromised.



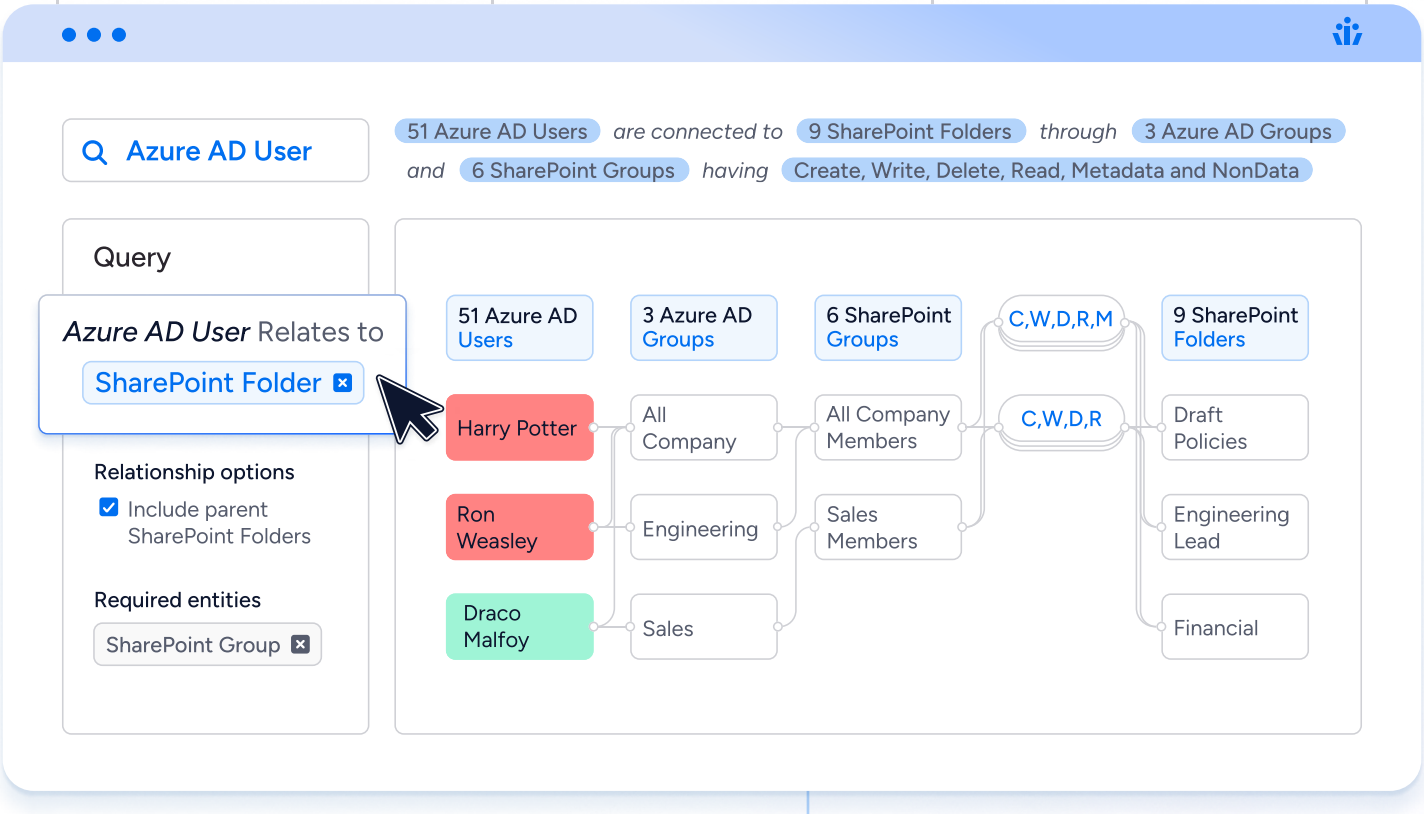
Unstructured Data Access

Understand and control access to unstructured data, in your data lakes, ML datasets, shared drives, and cloud storage.

Continuously monitor for new access to sensitive data in storage buckets, fileshare systems, and data warehouses.

Integrate with data tagging and classification tools to build sophisticated access queries. For example, can identities outside the finance team access any resources containing PCI data?

Assess blast radius by finding users with unnecessary or broad access to Sharepoint sites, data lakes, and shared drives.

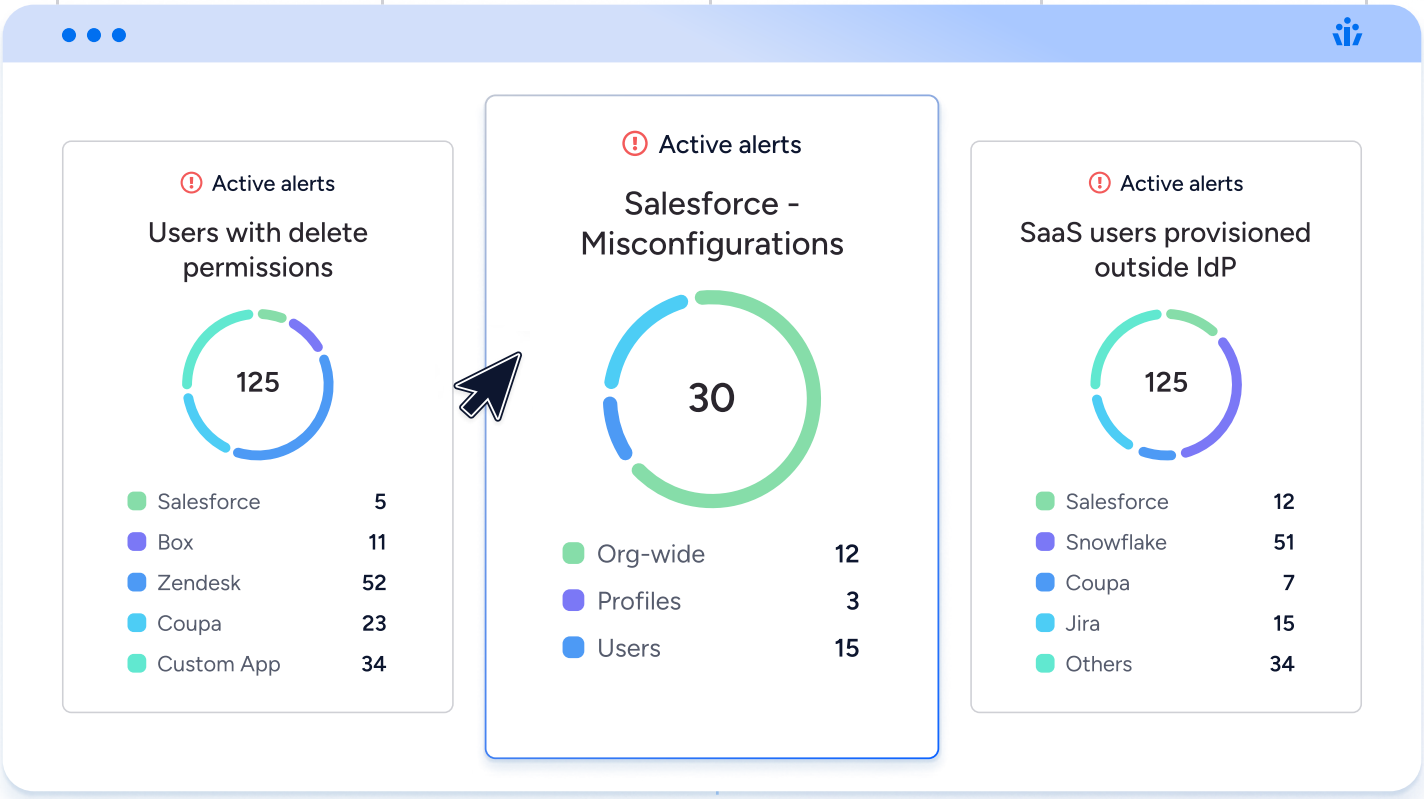


SaaS Access Security

Understand what actions users can take on sensitive data in apps like Salesforce, Box, GitHub, Zendesk, Netsuite, Coupa, and many more.

Protect the integrity of your source code. Identify external users and contractors who can make production changes to key GitHub/GitLab/Bitbucket repositories.

Find and fix orphaned or dormant accounts that can be exploited by attackers.	Enforce MFA enrollment across all of your apps.	Find users with excessive permissions in apps like Salesforce and Netsuite.	Slash your SaaS bill by removing unused licenses.

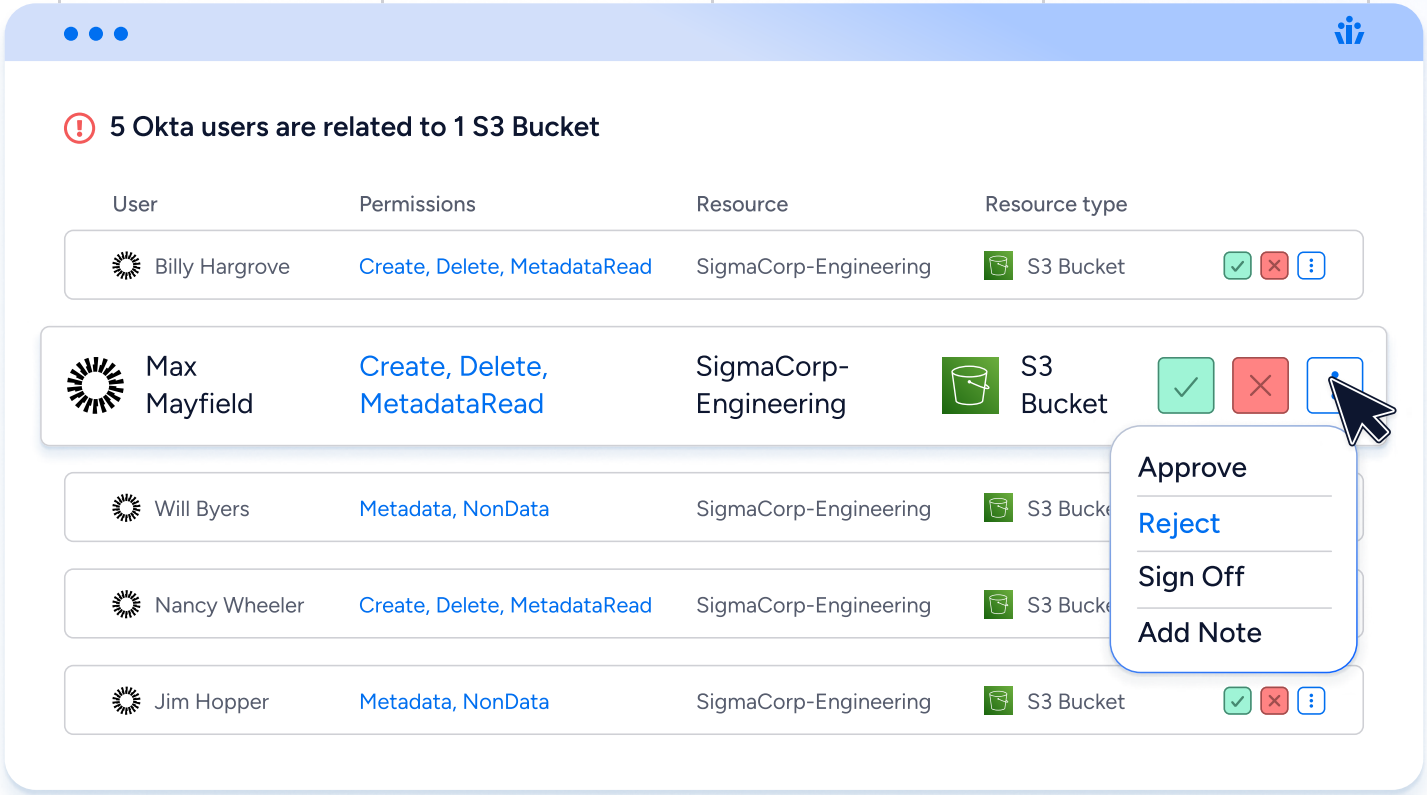


Access Review Automation

Enforce least privilege and compliance with periodic access reviews and certifications based on the granular, effective permissions of identities.

Automatically compile review and certification campaigns covering your cloud environments, on-premise systems, and SaaS apps.

Delegate decision making to employee managers or data owners.	Integrate with SOAR and ITSM systems like ServiceNow and Jira to implement access review decisions consistently and fast.	Demonstrate compliance with SOX, ISO 27001, GDPR and other frameworks.	Complete your governance and compliance obligations 7x faster than with manual reviews.



About Veza

Veza is the identity security company. Identity and security teams use Veza to secure identity access across SaaS apps, on-prem apps, data systems, and cloud infrastructure. Veza solves the blind spots of traditional identity tools with its unique ability to ingest and organize permissions metadata in the Veza Authorization Graph. Global enterprises like Wynn Resorts, and Expedia trust Veza to visualize access permissions, monitor permissions activity, automate access reviews, and remediate privilege violations. Founded in 2020, Veza is headquartered in Los Gatos, California, and is funded by Accel, Bain Capital, Ballistic Ventures, GV, Norwest Venture Partners, and True Ventures. Visit us at veza.com and follow us on LinkedIn, Twitter, and YouTube.