veza | Solution Brief

Veza for Snowflake

Simplifying data security and access governance for Snowflake

As the migration of data to the cloud continues to accelerate, organizations increasingly look to cloud-native alternatives to traditional databases and storage systems. Meeting enterprise demands for scalability, elasticity, and concurrency, Snowflake has seen widespread adoption as the data lake of choice for analytics workloads and storage.

Your data in Snowflake needs to stay consistent, trustworthy, and secure, but security and governance are significant areas of friction for any organization that needs to share data across teams. As a result, security and data teams are under extreme pressure to ensure long-term data lake availability, integrity, and confidentiality.

Understanding and controlling permissions to data is largely an afterthought, especially in the early stages of a data lake deployment. Security programs need to implement and validate that authorization policies follow least privilege principles, both at the system level and granular permissions to Snowflake tables and columns.

Veza secures your Snowflake deployment by empowering your teams to understand and manage access governance and cloud entitlements for your Snowflake resources. Veza unravels the many layers of native Snowflake policies and access control structures (including local roles and local users), enabling you to manage human and non-human services (like service accounts for apps like Looker and Tableau) that access Snowflake data - ensuring you are driving business insights based on high-quality, trustworthy, and secure data.

Challenges for Snowflake customers

Organizations have recognized that to remain competitive, they must do more than simply collect data - they need to analyze and glean insights at an unprecedented pace.

Snowflake has enabled this for thousands of organizations but, in doing so, has introduced a new set of challenges in how organizations manage permissions to Snowflake data and protect sensitive data and insights. Primary challenges faced by modern organizations deploying Snowflake include:

- Breaking down the silos of identity (both human and service account) across identity providers (e.g., Okta and Azure AD), cloud providers (e.g., AWS, GCP and Azure), Snowflake, and business intelligence solutions (e.g., Looker and Tableau) - each with their own identity and authorization configurations
- Understanding and categorizing where sensitive data lives, who can access it, and how that access changes over time
- Identify what data a human or service account can read, edit, or delete ("effective" permissions)
- Monitoring for non-active or over-privileged accounts or dormant permissions that can access sensitive data on Snowflake to improve data access hygiene according to least privilege
- Reviewing compliance violations and configuring alerts to changes that might compromise the security posture of an organization

Meet Veza

The Data Security Platform that helps you answer ***who can*** and ***should take what action*** on what data in AWS

veza | snowflake

veza | Solution Brief snowflake

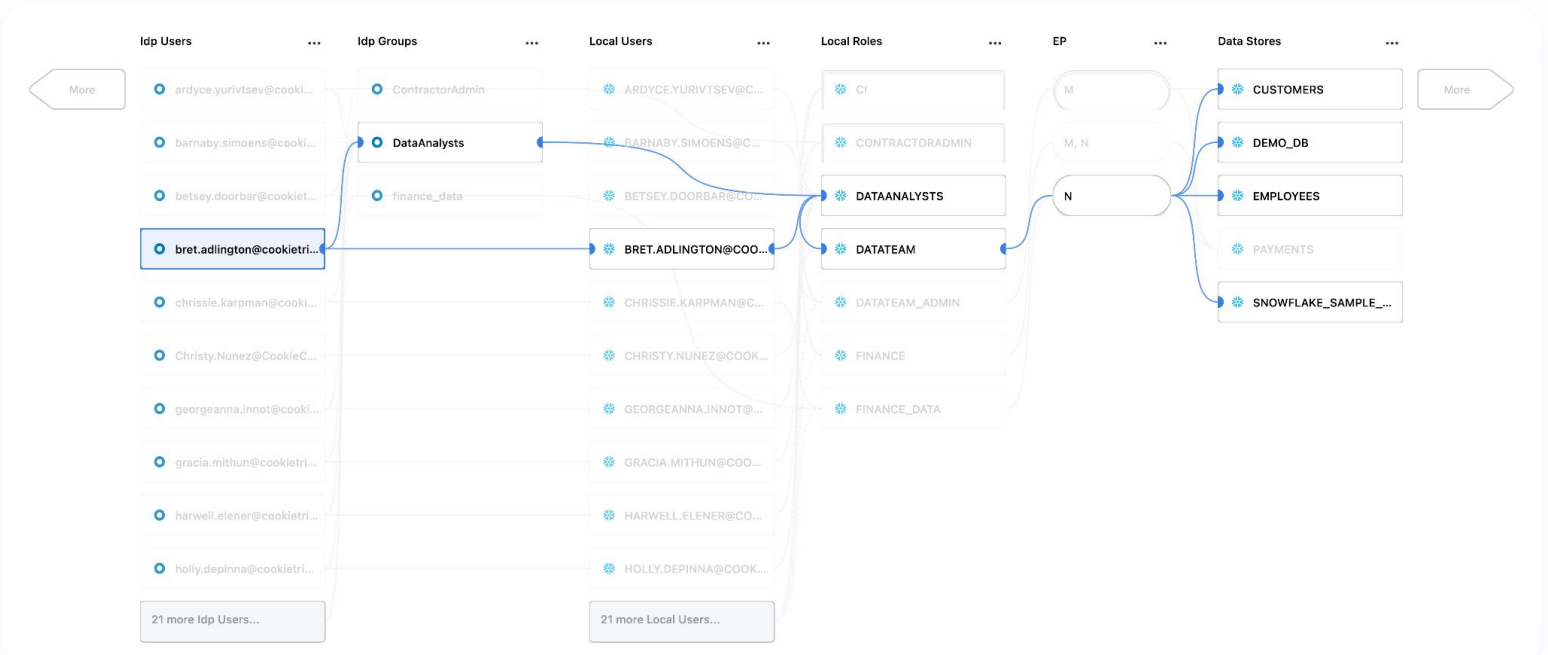
Why choose Veza for Snowflake data governance

Like other enterprise-grade data systems, Snowflake natively offers sophisticated authorization controls, combining aspects of both RBAC and DAC. However, most organizations need to understand authorization relationships native to Snowflake, as well as to all other systems in their environment - from identity providers, to cloud service providers (AWS, Azure, and GCP) to infrastructure systems, and to data stores. Veza assembles a complete and accurate picture of authorization policies by combining metadata from all these systems, including Snowflake, into a single human-understandable framework.

Here are a few examples of how Veza empowers you to manage your Snowflake deployment:

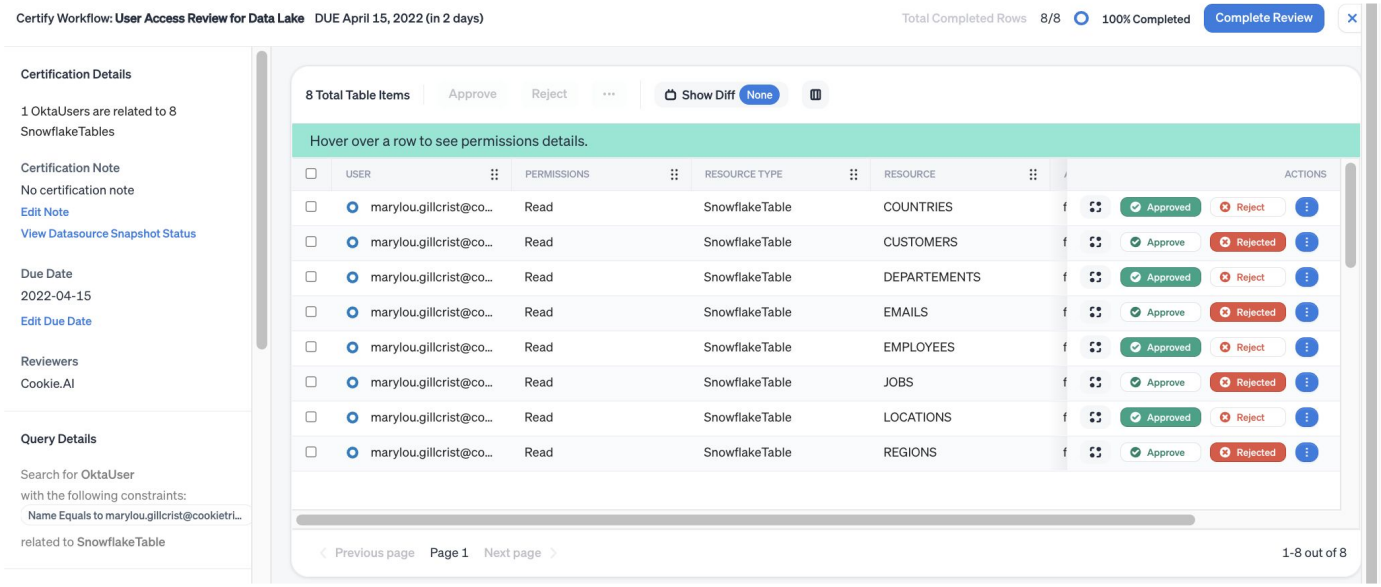
Search & Discover

- View all identities with Snowflake data access using the **Authorization Graph** - from any identity element, such as Okta User, Okta Group, Azure AD User, or Azure AD Group, to Snowflake resource entities (e.g., view/account/database/schema/table)
- Get visibility into Snowflake system-defined roles, user-defined roles, role hierarchies, and associated permissions using **Search**.
- See effective permissions of Snowflake access control and the impact of chains of roles and role hierarchy.



Compare & Correct

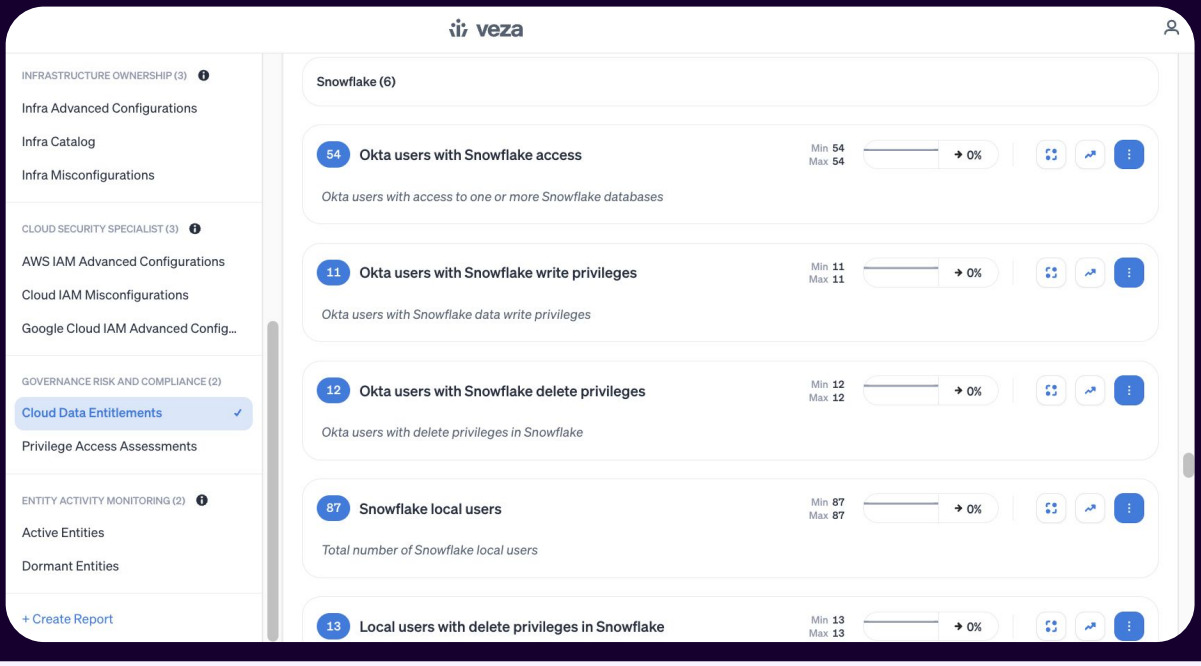
- Enable active monitoring of authorization changes in your Snowflake deployment with **Rules** and **Alerts**, based on Veza's suggested pre-built assessments or your own custom queries.
- Use **Violations** (both out-of-the-box and custom) to discover and be notified of deviations from least privilege standards for your Snowflake environment.
- Get actionable steps to maintain policy compliance with **Recipes**, offering security teams tools to identify, assign (via integrations with Jira, ServiceNow etc), track, and validate appropriate remediations.
- Establish workflows for **User Access Reviews, Privileged Access Reviews**, **and Cloud Entitlement Reviews** that target sensitive data, to ensure the proper security controls to are in place.



Define & Control

- Monitor federation to Snowflake data sets, discovering excess permissions and other violations and anomalies with **Insights**-built-in audit assessments for privileged access.
- Report on privacy, least privilege, and compliance (with both out-of-the-box and custom templates) that highlight your organization's data lake environment and security policies.
- Determine what permissions should be attached to new data lakes based on organization policies and current deployments.
- Collect authorization information across all your systems when completing a data lake asset access request.

veza | Solution Brief | snowflake



How to get started

Veza is easy to implement quickly and securely. Veza requires read-only permissions to access authorization metadata in target systems and is deployed without an inline proxy, so there is no added risk of downtime and data availability.

1. Connect your identity and cloud providers to Veza through read-only accounts, enabling the discovery of data objects and metadata.

2. Review the **Entity Catalog** in Veza for completeness, including all your Snowflake entities.

3. Begin using built-in **Insights** (**Reporting**, **Violations**, and **Alerts**) to quickly see and be notified of the highest priority issues for your Snowflake environments.

4. Inspect potential issues using the **Authorization Graph** to visualize and manage identity-to-Snowflake entity relationships.

5. Use **Heatmaps** and **Query Builder** to target your investigations and alerts for the authorization of Snowflake resources, using **Tags** to prioritize your most sensitive data.

It's as simple as that! To find out more about how Veza can integrate with many more enterprise systems, see our integrations page at www.veza.com/platform/integrations.

• Sign up for a free trial

About Veza

Veza is the data security platform powered by authorization. Our platform is purpose-built for multi-cloud environments to help you use and share your data more safely. Veza makes it easy to dynamically visualize, understand and control who can and should take what action on what data. We organize authorization metadata across identity providers, data systems, cloud service providers, and applications — all to address the toughest data security challenges of the modern era. Founded in 2020, the company is remote-first and funded by top-tier venture capital firms including Accel Partners, Google Ventures, Norwest Venture Partners, and True Ventures. To learn more, please visit us at veza.com.