veza | Security you can see

Veza for Snowflake **Solution Brief**

# Access Governance for Snowflake

*Enforce access policies on sensitive data to achieve least privilege and meet compliance requirements*

Snowflake enables companies to gain a competitive edge by managing and analyzing data at scale. However, it also introduces a new set of challenges in how organizations manage and secure access to sensitive data. As the adoption of Snowflake increases, organizations face difficulties in answering "who can take what action on data" using included access control mechanisms. Despite Snowflake's built-in security and governance features, such as RBAC, column-level security, and row-level access policies, security and data teams struggle to manage the scale and complexity of access permissions throughout their data cloud. To secure access to data without slowing down team performance, you need a single source of truth from which user permissions are managed.

## Veza secures your Snowflake Data Cloud

### Visualize

Enable identity, security, and IT compliance/risk teams to understand the full scope of access permissions for all users and roles with Veza Search.

### Monitor

Understand how access to data changes over time with Veza Insights and discover over-provisioned user accounts and roles with Veza Activity Monitoring.

### Remediate

Achieve continuous compliance with automated workflows for user access reviews and entitlement management with Veza Workflows. Reject access requests and remove unwanted access through downstream integrations with Jira, ServiceNow, Slack, and webhooks.

### Control

Ensure that only active accounts in identity providers can access tables with sensitive data. Reduce expenses by controlling access to datasets & efficiently managing licenses.

## Challenges

- ! Understanding access for your entire data estate and identifying risks associated with different levels of data sensitivity
- ! Proliferation of local users, local roles, privileged users, and external users
- ! Governing external data sharing in Snowflake
- ! Identifying excess permissions and unused access to data for all users (humans, service accounts)
- ! Lengthy and expensive processes for meeting compliance as a result of manual efforts or purchasing third-party consulting services
- ! "Security theater" - rubber stamping of entitlement certifications
- ! Dormant access to Snowflake objects (databases, tables, etc.)

## Benefits

- ★ **Reduce the risk of data breaches and IP theft**
- ★ **Automate access reviews and certifications and meet regulatory compliance (SOX, ISO27001, SOC, GDPR)**
- ★ **Maintain least privilege and rightsize access to data based on usage**

## Use Cases

- ★ Data Lake Security
- ★ Access Review Automation
- ★ Privileged Access Violations

## RBAC Entities Supported

Accounts · Tables · Local Users · Local Roles · Schemas · Databases

> *As a fintech company our customers rely on us to maintain a strong compliance posture to keep their data secure. Veza has helped us implement governance standards within our Snowflake deployment by giving my team visibility to manage all identities and their access to data in Snowflake. Veza empowers my teams with the insights they need to manage and mitigate risks.*

Steven Hadfield
Sr. Staff Product Security Engineer

SoFi

## 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 Blackstone, 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.

## Who uses Veza for Snowflake

### Security and IAM Teams

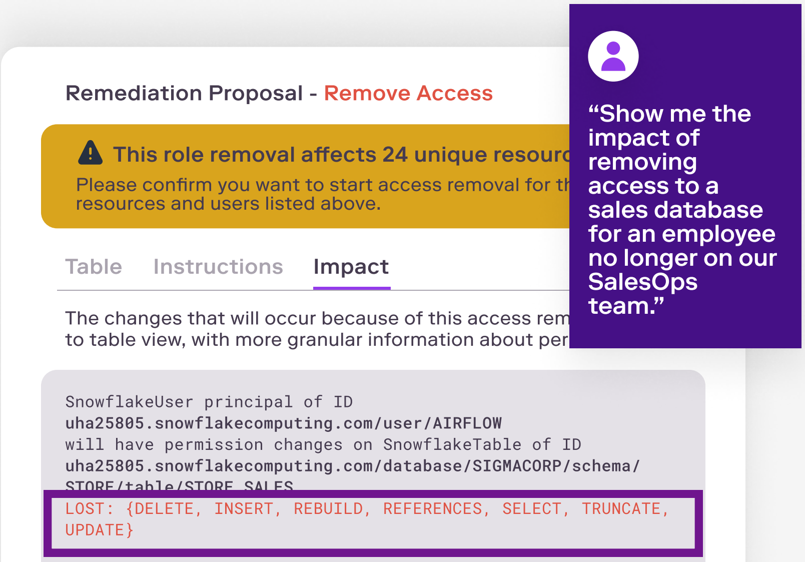
- ✓ Visualize all identities with access to sensitive data and understand their scope of permissions (create, read, write, delete)
- ✓ Monitor for permissions changes on privileged Snowflake objects to maintain least privilege
- ✓ Fix excess permissions through alerts for dormant access to tables, views, and databases
- ✓ Identify orphaned local Snowflake users to close access control gaps
- ✓ Mitigate risk as a result of frequent M&A activity through visualizing and managing relationships between new users and sensitive data in Snowflake
- ✓ Control variable expenses by identifying underutilized user licenses and controlling access to datasets

### GRC and Audit teams

- ✓ Verify that Snowflake resource access controls comply with GDPR, CCPA, CPNI, and other relevant regulations
- ✓ Perform end-to-end access reviews from access certification to renewal, to remediation in a shared interface
- ✓ Automate remediation of excess permissions, facilitated by webhooks

### Data Owners

- ✓ Validate Snowflake local roles, local users, and permissions assigned to the roles
- ✓ Assess users who have access to sensitive data sets on Snowflake
- ✓ Assess Snowflake roles to help assign new users and associated access to Snowflake



Remediation Proposal - Remove Access

⚠ This role removal affects 24 unique resourc

Please confirm you want to start access removal for th
resources and users listed above.

The changes that will occur because of this access rem
to table view, with more granular information about per

```
SnowflakeUser principal of ID
uha25805.snowflakecomputing.com/user/AIRFLOW
will have permission changes on SnowflakeTable of ID
uha25805.snowflakecomputing.com/database/SIGMACORP/schema/
STORE/table/STORE_SALES
LOST: {DELETE, INSERT, REBUILD, REFERENCES, SELECT, TRUNCATE,
UPDATE}
```

"Show me the impact of removing access to a sales database for an employee no longer on our SalesOps team."