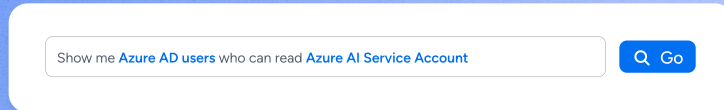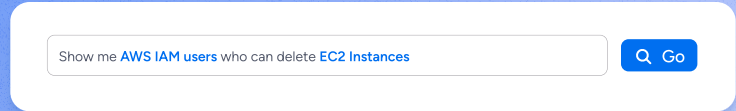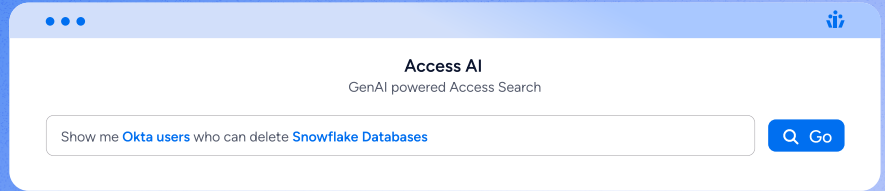# Access AI

Veza helps organizations strive towards the principle of least privilege, with Generative AI-powered capabilities to help Security & Identity teams prevent, detect, and respond to identity-based threats. Access AI brings GenAI based capabilities to all Veza products.

Access AI
GenAI powered Access Search

Show me **Okta users** who can delete **Snowflake Databases**   🔍 Go

Show me **AWS IAM users** who can delete **EC2 Instances**   🔍 Go

Show me **Azure AD users** who can read **Azure AI Service Account**   🔍 Go

Key Benefits

Least Privilege

Visualize and control effective permissions for all identities in all systems (apps, on-premise, cloud services, data systems). Discover and remediate identity misconfigurations, dormant permissions, unneeded privileged accounts and over-permissioned identities.

Reduced Risk

Surface and prioritize identities with the highest privilege, risk, or policy issues across all enterprise systems, without having to master the complex access models of systems like AWS IAM, Snowflake, and Salesforce.

Operational Efficiency

Reduce manual, repetitive tasks by leveraging Access AI to detect and remove excess access. Use Veza to delegate access decisions in natural language to business managers who best understand specific systems.

Key Features

Access Search

Access AI enables identity, security, app, and data teams to use Veza Access Search in natural language across identities, birthright groups, access roles, policies, permissions, and resources. Capabilities include:

- **Attribute-driven:** *Show me Okta Users who have MFA disabled and can read from AWS S3 - buckets.*

- **Conditional scenarios:** *Show me Okta users who have access to AWS S3 buckets via Okta Group memberships.*

- **AND/OR conditions:** *Show me Azure AD users who are guests and who have administrator roles.*

Access Intelligence

Discover risky users, resources, trends, and other access risk insights in natural language. Veza Risk Intelligence Dashboards are now powered by Access AI.

Role Recommendations

Tailored least privilege role recommendations for access requests, that simulate the full impact of access before it's granted.

Built on the Veza Access Platform

Veza is the identity security company that powers Intelligent Access. The platform enables companies to monitor privilege, investigate identity threats, automate access reviews, and bring access governance to enterprise resources like SaaS apps, data systems, cloud services, infrastructure services, and custom apps.

Role Recommendations

Integration
Snowflake

User
ANN.TIMES@EXCORP.COM

Resource Type
Snowflake Table

Resource Name
CATALOG_SALES

Effective Permissions
DATA_READ

Roles Filter Query
Snowflake Roles

⌄ Recommendation 1   DATA READERS   `Least Privileged`

Resource Type	Current Access	New Access	Change	Effective Permissions	System Permissions
Snowflake Table	0	2	+2	Read	Select

⌄ Recommendation 2   ENGINEERING_WR_CO

Resource Type	Current Access	New Access	Change	Effective Permissions	System Permissions
Snowflake Table	0	3	+3	Delete, NonData, Read	Delete, Insert, Rebuild, References, Select, Truncate, Update

⌄ Recommendation 3   ENGINEERING_WR_CT

Resource Type	Current Access	New Access	Change	Effective Permissions	System Permissions
Snowflake Table	0	3	+3	Delete, NonData, Read	Delete, Insert, Rebuild, References, Select, Truncate, Update

> " *To operate with least privilege, companies must be focused on their identity posture. With the modern enterprise moving away from standing access, success now depends on having the appropriate tools and automated solutions. Nearly every discovery made by Veza's AI has prompted an immediate response from our team. With hundreds of thousands of entitlements to oversee, leveraging AI-driven automation has been essential to staying proactive.*

Matthew Sullivan • Infrastructure Security Team Lead, Instacart