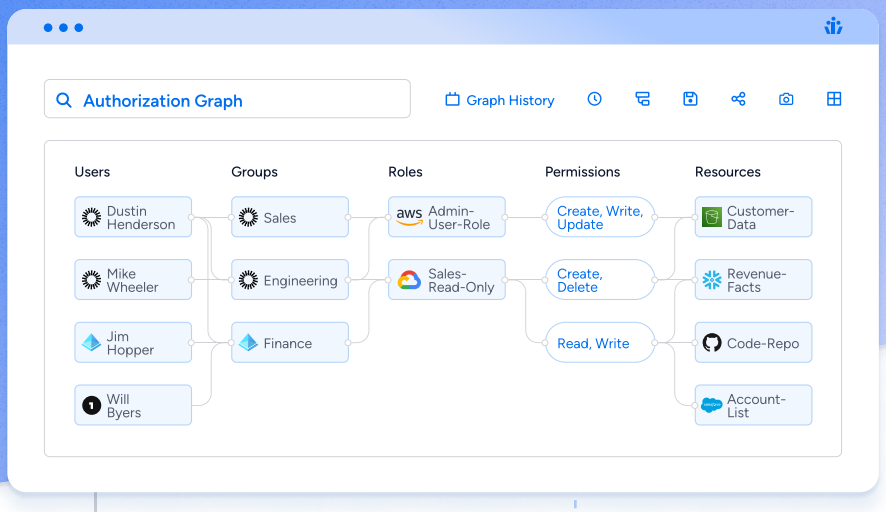
veza

Product Data Sheet

Access Search

Visualize and control who has access to data across all enterprise systems. Only Veza analyzes permissions to resources for all identities (human or machine), helping security teams reduce risk before and after attacks.



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 unneeded privileged accounts and unused access.

Continuous Compliance

Build queries and alerts to automatically scan for access that violates policies required for frameworks like SOX, SOC 2, NIST, and GDPR.

Threat Investigation

Quickly assess the detailed access of compromised identities to prioritize incident response.

Key Features

Access Search

Visualize the current effective permissions for all identities (human and service accounts) in all systems, in near real-time regardless of search. The scope of the scale includes apps, data warehouses, and cloud services like AWS IAM, GCP IAM, and Azure RBAC.

Query Builder

Build rich queries with filtering, sorting, and complex operands that span multiple systems. Leverage tags to search access to sensitive data types.

Risk Visualization

Automatically identify and prioritize risky permissions with heatmaps.

Time Travel

Use historical views of the Authorization Graph to surface permissions changes that should be reviewed, recertified, or revoked.

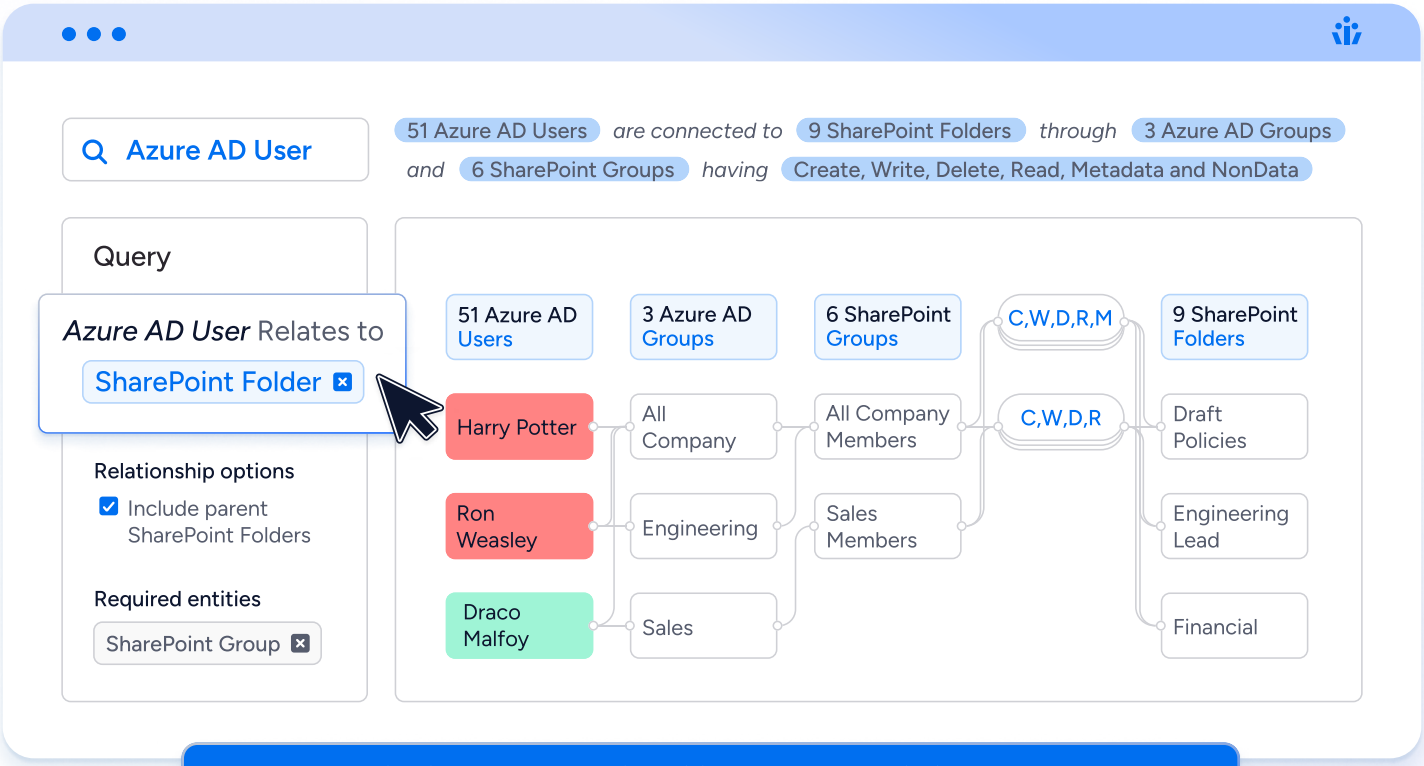
API Queries

Create and run queries using Veza's RESTful APIs and use the results to enrich data in your existing tools, workflows, and solutions.

Built on the Veza Access Control Platform

Veza is the Access Control Platform that enables Next-Gen IGA. Our 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.

Legacy Solution Challenge	Veza Solution
Determining the effective permissions for an identity to a specific resource is time-consuming and requires specialized knowledge of each system's permissions logic and language.	Instant access to effective permissions in easy-to-understand terms: Create, Read, Update, Delete (CRUD).
Difficult to identify permissions changes that may create risk across a large, diverse, and dynamic IT infrastructure.	Veza Authorization Graph Time Travel makes identifying and evaluating changes easy.
Difficult to operationalize ad-hoc manual investigations.	Queries can be saved and used to monitor and remediate permissions.



The Authorization Graph maps identities to roles, permissions, and resources, enabling search, monitoring, alerts, and remediation.

Extended Feature List

Authorization Graph Real-Time Search

Real-time graph search for any-to-any relationship with constraints on properties and tags

Risk Visualization in Authorization Graph

Highlight risks in authorization graph search results

Explain Effective Permissions in Authorization Graph

Explain the effective permissions for any identity-to-resource relationship

Authorization Graph Time Travel

Explore Authorization Graph for a specific point in time

Authorization Graph Saved Search

Save user-created Veza Graph search queries

Authorization Graph Integration-Aware Quick Links

Quick links for common Graph search views based on active integrations

Authorization Graph NLP output for search result

Authorization graph search results in plain English

Visualize Local Users/Local Groups in the Authorization Graph

Show all local users/groups for any identity-to-resource relationship

Support for Cross-AWS-Account AssumeRole Relationships

Highlight the assumeRole relationship across AWS accounts

Authorization Graph Hide/Show Entities

Flexibility to show/hide entities on the path of any-to-any relationship search result

Show all data sources for any user(s)

Show all data sources that users have access to in an authorization graph search result

Share Authorization Graph Search

Share the authorization graph search result as a URL

Entity-Aware Inspection in Authorization Graph Search

For authorization graph search results, the ability to inspect details, related identities/tags/groups for a particular entity in the search result

Query Builder for any-to-any relationship

Create queries to display results in a table format, supporting all constraints

Limit output based on query result for Query Builder

Only show query results that are above a predefined threshold for the number of results

System Query Mode for Google Cloud

Show the configured (as opposed to effective) permissions across multiple Google Cloud and Workspace Organizations

Tag-based Entity Search

Search entities based on any native tag (e.g., AWS, GCP or Veza-created tag)

Explain Effective Permission for Snowflake

Added support "Explain effective permissions" for Snowflake

Source/Destination Queries

Source/Destination and summary entities query in Query Builder

Enhanced constraints on queries

Support for regex, time, and exists constraints

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.