The Authorization Platform for Data Security

Prevent unauthorized access to sensitive data residing in any system

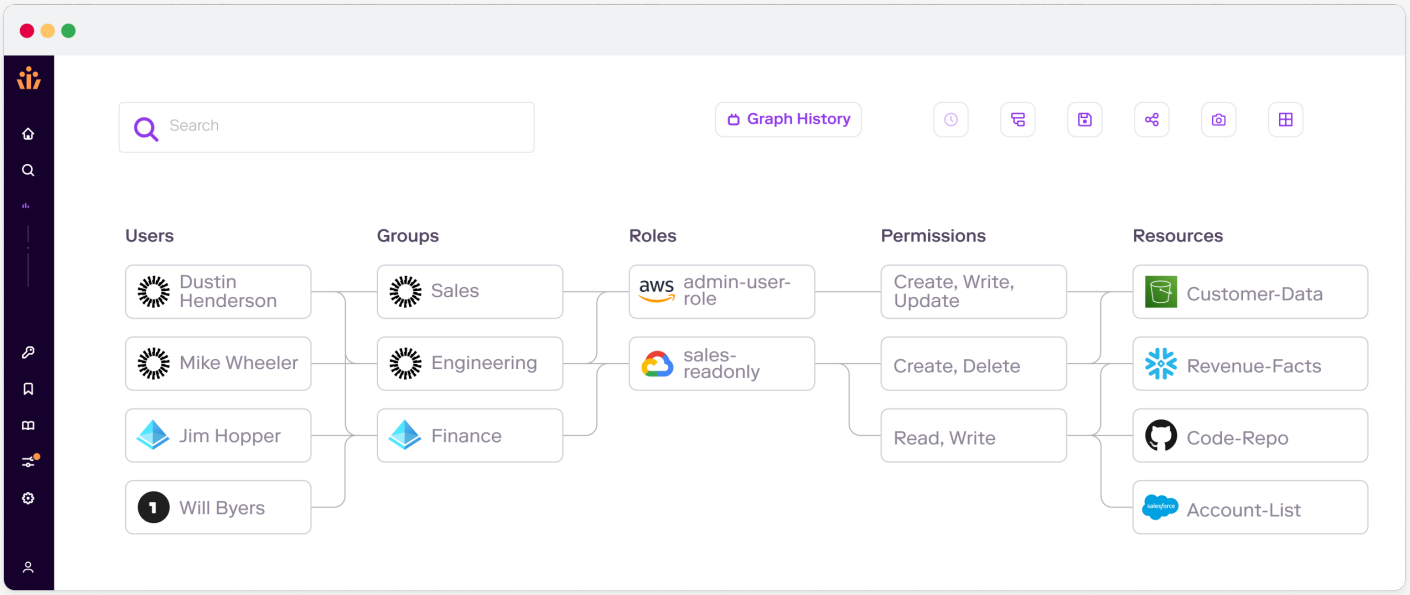
75% of security incidents stem from the misuse of identity and credentials. If everybody wants Least Privilege, why does nobody achieve it? The scale of the modern app, data, and cloud landscape makes it impossible to review millions of permissions with a manual process. Every day, companies accumulate unnecessary permissions or "access debt" due to errors, lack of time, and outdated technology. Access debt is the primary avenue for breaches, insider threats, ransomware, and IP theft.

Veza is reinventing how enterprises manage access to data anywhere. Our innovation is the Authorization Graph, which ingests authorization metadata from all enterprise systems, organizes the millions of permutations into a standard object model, and optimizes the data for fast analytics.

The Veza Authorization Platform makes it easy to find and fix access errors. And it works wherever you keep sensitive data: SaaS and on-prem apps, unstructured data systems, data lakes and warehouses, and cloud infrastructure services. While many companies have invested in identity and governance tools, these simply were not designed to solve the challenges of the modern cloud environment: access governance, privileged access, data governance, cloud IAM misconfigurations, and SaaS posture.

Only Veza makes it possible to answer the question "Who can do what with our data?"

The Authorization Graph maps your identities to roles, permissions, and resources, enabling real-time search, monitoring, and alerts.



Authorization Use Cases

SaaS Posture (SSPM)
Bring access governance to sensitive data in SaaS apps like Salesforce, NetSuite, and GitHub.

Privileged Access (PAM)
Monitor apps and systems for new access that violates policies.

Cloud Entitlements (CIEM)
Confirm access to resources, for both humans and machines, in AWS, GCP, and Azure.

Data Lake Security
Bring granular access control to cloud data lakes like Snowflake and Redshift.

Access Review Automation (IGA)
Automate access certifications and help decision-makers find the least permissive access.

Incident Response (ITDR)
Investigate the total span of access for any compromised identity or service account.

Compliance
Demonstrate complete visibility to satisfy requirements of SOX, ISO 27001, GDPR, CCPA, etc.

Unstructured Data Access
Prevent out-of-policy access to sensitive information in Box, SharePoint, S3.

Data Activity Monitoring
Detect unneeded or dormant access to maintain a state of least privilege.

Platform & Products

Search & Insights | Enterprise Workflows | Activity Monitoring

Veza Authorization Platform

Identity Graph | IAM Graph | App Graph | Data Graph | Resource Graph

Veza Integrations

50+ connections to data systems, SaaS apps, cloud services, and custom apps

Our team is always looking for ways to develop a more comprehensive view of access across all of our applications and cloud infrastructure to allow us to modernize the firm's access controls. We are excited to partner with Veza to help us accomplish this.

Adam Fletcher | Chief Security Officer

Blackstone

Benefits

Fortune 500 organizations and global enterprises, including Blackstone, Wynn Resorts, and Expedia trust Veza to reduce risk, lower costs, and ensure compliance.

- Instant identification of top authorization risks
- Real-time search to identify who can access what
- 86% faster access review campaigns
- 80% reduced score for privileged accounts
- Reduce impact of breaches with a least-privilege posture
- Avoid “security theater” by managing permissions at a granular level
- Achieve compliance (SOX, SOC, ISO 27001, etc.)
- Remove unused permissions without impacting business processes
- Reclaim unused SaaS licenses

The Veza Difference

Born in the cloud

As a cloud-native platform, Veza introduces no admin overhead when deploying product updates, including new features. Veza delivers 99.99% uptime.

Effortless Integrations

Our API-first approach enables Veza to integrate enterprise systems through two simple methods, out–of-box integrations or self-service with our Open Authorization API (OAA).

Graph of graphs

Veza’s proprietary Authorization Graph utilizes a streaming services engine to aggregate metadata across identity providers, cloud providers, cloud IAM, SaaS and on-prem apps, and data systems into a unified platform, purpose-built to scale for the needs of modern cloud environments.

RBAC, simplified

Role-based access control (RBAC) structures vary greatly from system to system. Veza normalizes RBAC across all systems, eliminating the need for customers to manually correlate users, roles, policies, and permissions.

Out-of-band (agentless/proxyless)

Compared to inline architectures, Veza has no installers, ports, or firewalls required for deployment, meaning there’s no risk of downtime or “man in the middle” attacks.

About Veza

Veza is the authorization platform for data security. Identity and security professionals use Veza to modernize access governance for the new data landscape. By automating the work of finding and fixing excessive permissions on a continuous basis, Veza helps organizations achieve Least Privilege. Veza’s unique approach ingests metadata from any app or data system, organizes it as an authorization graph, and makes it searchable in real-time. Global enterprises like Blackstone, Wynn Resorts, and Expedia trust Veza to protect sensitive data and automate access reviews. 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. To learn more, visit us at veza.com.