veza

Core Authorization Platform

Veza is the data security platform built on the power of authorization. Our platform empowers organizations to understand and control **who can and should take what action, on what data.** Our Authorization Metadata Graph integrates with cloud identity providers, cloud IAM, cloud services, apps, and data systems to discover system-specific authorization metadata, translating the complexity into a simple language of effective permissions, delivered through a SaaS-based control plane. Veza delivers actionable insights into least privilege risk, remediating over-permissioned accounts, correcting cloud IAM misconfigurations, addressing privilege access and drift, managing access certifications, and more.

Our customers use Veza to:

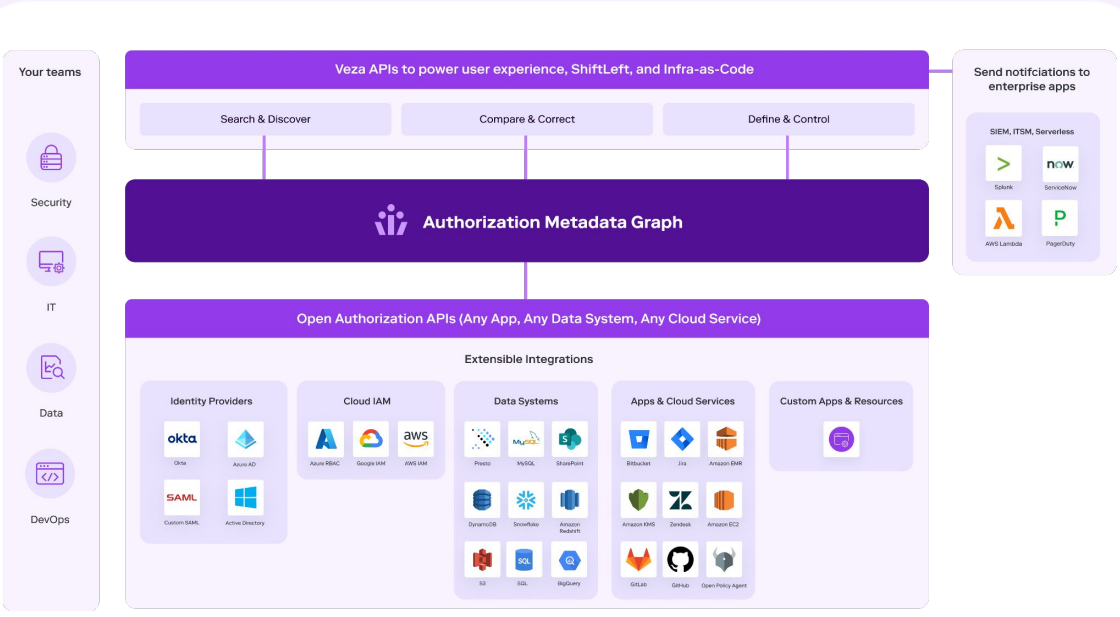
- Redefine Zero Trust Security Through Data
- Securely Accelerate Adoption of Cloud Data
- Modernize Data Security to Protect Against Ransomware

Key projects Veza helps with include:

- Implement Data Lake Security (Snowflake, RedShift etc.)
- Secure authorization for Any App (GitHub, JIRA, etc.)
- Modernize Privileged Access for Data
- Streamline Access Governance

Veza's data security platform

built on the power of authorization



veza

Key features

Authorization Metadata Graph for end-to-end visibility into identity-to-data relationships

- The foundation of the Veza platform. Veza translates the complexity of system-specific metadata into a simple language of effective permissions (CRUD), all visualized in a single control plane via the **Authorization Graph.**

Search & Discover

- **Search** - a consumer-like, real-time search that enables users to explore and manage identity-centric authorization relationships in their environment. Security, data, and operations teams can operationalize their findings for user access reviews, audits, compliance tracking, data access risk reviews, privilege access, entitlement reviews, etc.
- **Query Builder** - a rich engine and query language that supports complex inspection, filtering, sorting, and constraining, even on the most complex metadata sets. Data and security teams can easily mine large datasets to gather intelligence and insights, enabling them to meet even the strictest requirements for access governance, privilege access, cloud entitlements management, and more.
- **Tags** - easily add searchable properties to authorization entities across your multi-cloud ecosystem, and apply them to principals, groups, policies, and resources. For example, with Tags you can search for resource-centric entitlements on Snowflake tables containing sensitive data. Alternatively, use existing tags from your AWS deployment to filter within Authorization Graph and Search for refined results.
- **Heatmaps** - a one-click view into how privileges are distributed across your data systems. Use Heatmaps to identify over-privileged users, most-accessible data stores, locate entities with broad privileges, etc.

Compare & Correct

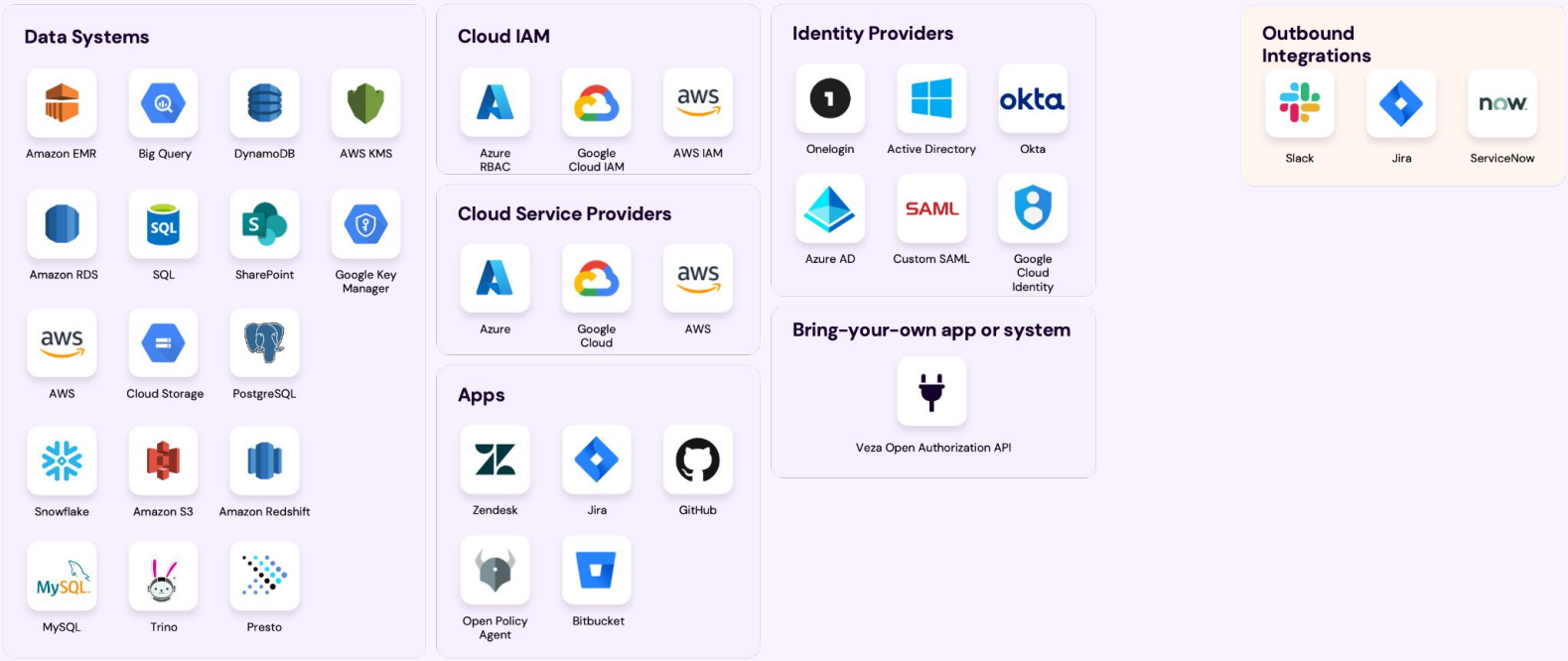
- **Webhooks** - enable business processes such as updating an issue tracker in JIRA, creating a service desk ticket through ServiceNow, or sending Slack notifications to your SecOps team.
- **Alerts** - continuously monitor for authorization changes in your environment and optimize your organization's data security posture.
- **Rules** - set triggers to inform teams when privilege drift is detected across your data systems.
- **Recipes** - step-by-step instructions to remediate data access best practices in critical systems such as AWS IAM. Recipes also provide details about the side effects of proposed solutions that help determine what constitutes a successful change.

Define & Control

- **Insights** - out-of-box assessments for identity analysis, Cloud IAM misconfigurations, role governance, compliance reviews, privilege governance, etc.
- **Violations and Alerts** - quickly detect misconfigurations, vulnerabilities, and deviation of data authorization best practices, including receiving automated alerts when meaningful changes occur in the authorization structures across all integrated services and providers.
- **Entity Monitoring** - captures information generated from cloud IAM systems, identity providers, and data sources for users to understand time-based usage of the Cloud IAM and data permissions. For example, track scenarios like the number of AWS IAM users or groups created in the last 24 hours. Built-in assessments help security and data teams identify stale permissions and prioritize the removal of dormant entities.

Extensible Integrations

- Veza supports integrations with leading identity providers, Cloud IAM systems, cloud services, apps, and data systems, requiring only read-access to discovery data sources. Our Open Authorization API enables organizations to integrate custom applications and services to Veza for a comprehensive set of answers to who can take what action on custom applications.



To learn more about how Veza fits into your data security initiatives, visit us at www.veza.com.

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.