

Streamline Access Reviews, Removal, and Certifications

Real-world customer user stories



Meet ISO 27001 standards through data-centric audits and access reviews in AWS



Review Okta admins who have access to delete sensitive customer data in Snowflake



Secure your IP by certifying developer permissions to source code in GitHub



Automate access recertification campaigns through ServiceNow integration

The Problem

What makes access governance a challenge for organizations?

Growing industry regulations and compliance requirements have made certifying user access and permissions on all enterprise systems a critical project for any organization. While access governance is often an exercise in compliance, **the goal is to keep track of what data users and resources have access to and change or revoke access when necessary.** Being able to do this requires an automated, streamlined process that gives operators the information they need to be confident in their certifications.

In addition to industry regulations and compliance frameworks (e.g. PCI DSS, HIPAA, GDPR, SOX) that organizations must adhere to, the adoption of multi-cloud environments has made access and entitlement reviews highly complex. Current IGA solutions are not built for multi-cloud environments and lack:

- 1 Insight into authorization for every user across the enterprise ecosystem - not just people, but service account and machine identities, too
- 2 Management of entitlements and granular permissions beyond users and groups, for actual data (not just apps and infrastructure)
- 3 Standardization of how permissions are managed across resources making it difficult to certify access and entitlements for non-experts
- 4 Streamlined, business-friendly workflows for GRC and IAM teams to manage entitlement reviews

Ultimately, the lack of repeatable processes to manage user access reviews, with no visibility into granular data permissions leads to excess privileges that attackers can exploit.

The risk

Why solve access governance for data now?



Lack of control over sensitive data access

26% of respondents listed "loss of control of sensitive data" as a top issue with proliferation of cloud solutions¹. 19% of breaches are caused by lost or stolen credentials²



Higher costs

28% higher cost of a breach for organizations with high levels of compliance failures²



Not meeting business goals

80% of organizations seeking to scale a digital business will fail because they do not take a modern approach to data and analytics governance³

1. Veza survey of over 500 respondents conducted at security conferences from June-August 2022

2. IBM Cost of a Data Breach 2022

3. Gartner: Hype Cycle for Data and Analytics Governance and Master Data Management, 2021

How does Veza solve access governance and what's our differentiation?

Veza enables organizations to make context-aware decisions for access reviews, removals, certifications, and recertifications through a unified SaaS platform. We bring visibility to granular permissions for data objects and standardize effective permissions in simple business language (Create, Read, Update Delete) that is understandable by business users and non-experts alike.

By using Veza for access and entitlement reviews a **Fortune 500 Accounting & Tax Software technology firm reduced the time to complete certifications by 86%**. Veza's product impact at this Fortune 500 organization:

Reduced the time to complete **tens of thousands of rows of certification by 86%**.

More powerful attestation with **audit ready reports with granular details and insights into permissions**.

Eliminated the ability for reviewers to certify their own access to resources, previously 58% of reviewers were presented with certifications that included a self-review.

Automated notifications highlight important changes for reviewers, **96% of access reviews for a terminated user are correctly rejected**.

About Veza

Veza is the authorization platform for data. Designed for hybrid, multi-cloud environments, Veza enables organizations to easily understand, manage and control who can and should take what action on what data. We empower customers to leverage the power of authorization for an identity-first approach to security, addressing critical business needs tied to managing access governance, data lake security, cloud entitlements, privileged access, and more. Global enterprises like Blackstone, ASAPP, Barracuda Networks, Choice Hotels, and a number of Fortune 500 and emerging organizations trust Veza to secure their enterprise data. 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, follow the company on [Twitter](#), [LinkedIn](#) and [YouTube](#), and please visit us at veza.com.

