Veza for Google Cloud

If Google Cloud is a cornerstone of your cloud infrastructure, excessive or misconfigured access permissions in Google Cloud IAM can be your single biggest vulnerability. Veza is the identity security platform enabling you to answer the question:

WHO CAN TAKE WHAT ACTION ON WHAT **SERVICES AND DATA** IN GOOGLE CLOUD?

Identity security challenges in Google Cloud

AWS provides a modern, scalable, and cost-effective approach to hosting applications and data that has made it mission-critical for many organizations. But as cloud infrastructure like AWS continues to replace on-premise systems, identity and security teams face new challenges:

Complexity

Identity access in Google Cloud is highly configurable, with over 40 distinct permissions for cloud storage alone. Add in the challenge of resolving interactions between IAM policies and Access Control lists, and it becomes extremely difficult to predict what access any particular identity will have to a resource.

Scale

Security and governance teams are managing many more resources and identities in Google Cloud than in the on-prem world, especially when you account for non-human identities (NHIs). Traditional security and governance tools and processes—which assume a limited number of sensitive resources and rely on HR systems as a source-of-truth on identity—are still catching up.

Siloed access data

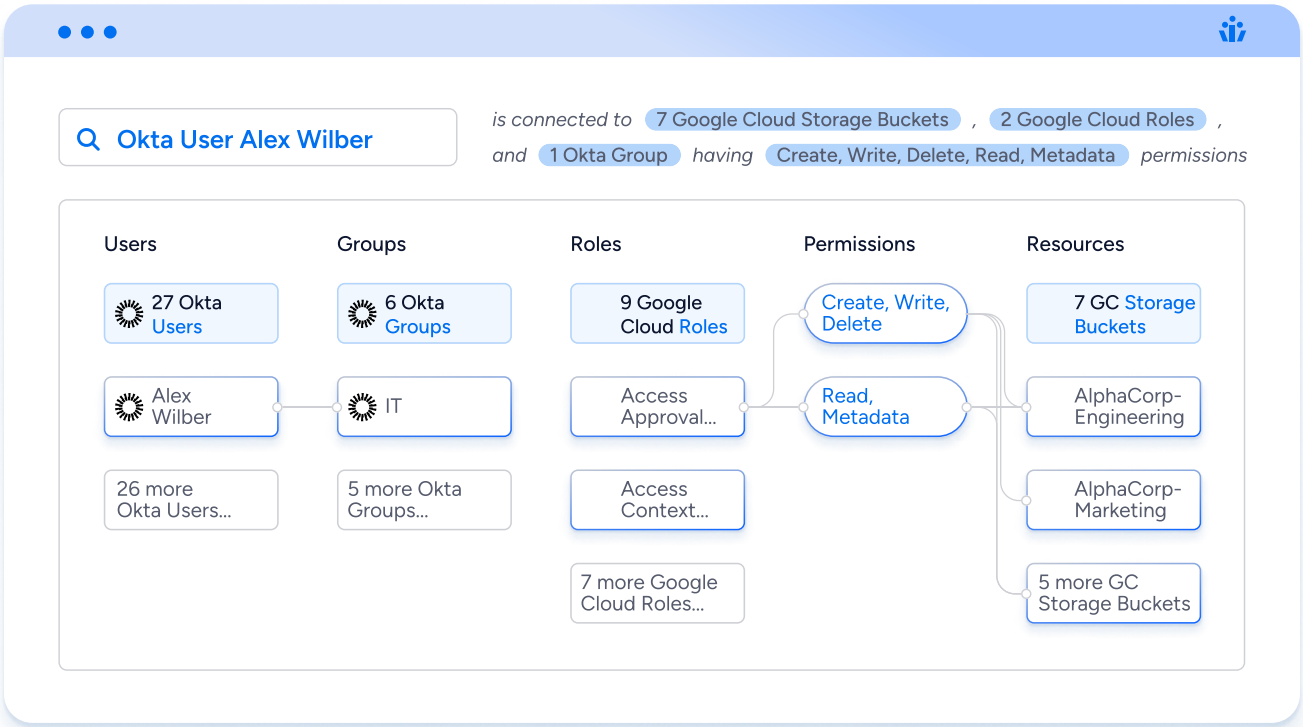
Because of the federation of identities across multiple identity platforms (IdPs) like Okta, Active Directory, and Azure AD, access data is split into multiple silos. Google knows the permissions assigned to local IAM roles and users. Your IdP knows which users and groups can assume a role. Neither can connect a federated identity to its specific permissions in Google Cloud.

> Despite a proliferation of tools that claim to offer Cloud Infrastructure Entitlement Management (CIEM), few have been able to offer visibility into the effective permissions of identities in cloud services like Google Cloud, leaving the question: How can you manage what you can't see? Moreover, Google Cloud is only one piece of your access puzzle. Your identity solution needs cover access to all systems: cloud infrastructure, on-premise apps, SaaS apps, and data lakes.

© 2024 Veza, Inc. All Rights Reserved

How Veza can help

Veza is powered by its Access Graph, which gives organizations the ability to visualize relationships between all identities and systems by connecting users, groups, roles, and permissions. The graph simplifies the process of understanding access across enterprise tools by presenting one comprehensive view of "effective permissions" for any enterprise identity or resource.



Effective permissions

Translate Google Cloud IAM permissions into simple, human-readable language of create, read, update, and delete, and resolve complex policy interactions to give actionable intelligence on who can do what in Google Cloud. For example, Veza would show that "Okta user Alex Wilber can delete data from the engineering bucket in Google Cloud Storage."

Access AI

Veza's Access Graph is built on a graph database that tracks the full path from an identity to a specific permission and is built to handle complex queries at scale. With Access AI, you can now ask questions in plain language to find and fix problems faster, while reducing the burden on security and governance teams. Veza watches continuously for policy violations and new privileged accounts, so you can comply with internal controls and external regulations.

Agentless

Veza maintains agentless read-only connections to both Google Cloud and your identity providers, giving a complete picture of the access granted to federated identities, revealing governance blindspots, like local users, inactive users or orphaned accounts in Google Cloud IAM.

© 2024 Veza, Inc. All Rights Reserved | veza.com

Benefits

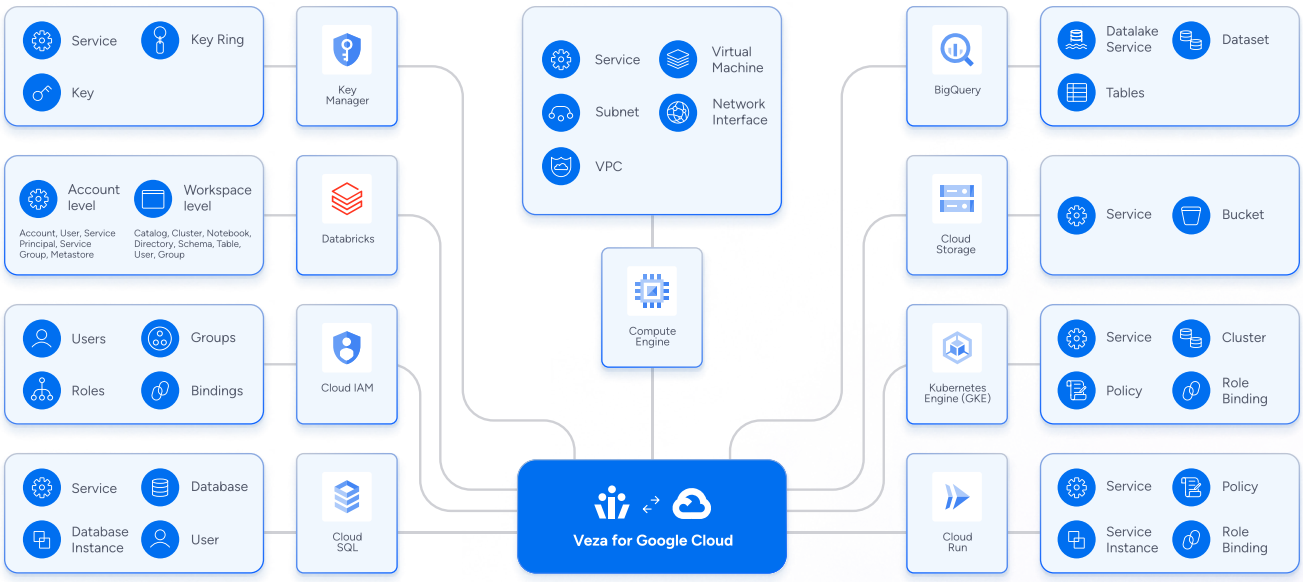
Reduced Risk
Surface and prioritize identities with the highest privilege, risk, or policy issues across all enterprise systems, without having to master the complex access model of Google Cloud IAM.

Least Privilege
Reduce risks and simplify audits by continuously identifying and remediating identity misconfigurations, dormant permissions, and over-permissioned identities.

Team Efficiency
Reduce manual, repetitive tasks by leveraging automation to detect and remove dormant access. Use Veza to delegate access decisions to business managers who best understand specific systems.

Full coverage of Google Cloud services

Veza connects to the full range of Google Cloud services for intelligent access across your cloud infrastructure, including Google Cloud IAM itself, Cloud Storage, Big Query, Compute Engine, Key Manager, & more



Three steps to Intelligent Access with Veza and Google Cloud

Step 1: Set up the agentless, read-only API integration in minutes. On day one, get out-of-the-box intelligence on common access risks and misconfigurations. Close exploitable security gaps like dormant accounts and roles and orphaned local users. Identify all local and federated users with admin privileges. Uncover all non-human identities and understand the access they have to sensitive resources in Google Cloud.

© 2024 Veza, Inc. All Rights Reserved

Step 2: Triage your less obvious security risks, with blast radius analysis to reveal identities with access to a large number of Google Cloud resources, or resources accessible to a large number of identities. Slash manual compliance work by automating the process of compiling and conducting access reviews and certifications in Google Cloud, all based on the effective permissions of identities. Use role mining intelligence to clean up your role-based access control (RBAC), trimming over-privileged, dormant, and unused roles.

Step 3: Build a program of automated access control. Identify your data crown jewels, monitor continuously for new access and create workflows for access remediation. Maintain least privilege by utilizing tools like Role Recommendations to easily respond to access requests with a least privilege role assignment. Sleep a little easier knowing you're proactively fixing excess privilege and misconfigurations as they occur, not after they empower an attacker.

Customer Story: Bluecore gets complete visibility across Google Cloud

Bluecore is a cloud-native organization, hosted entirely in Google Cloud since day one. CISO Brent Lassi's team sought a solution that could meet three primary criteria:

Supportability — *could it be supported entirely by Bluecore's security and IT organization*

Extensibility — *could it plug into other systems via APIs and automation?*

Observability — *could it pivot and drill down data to an almost infinite depth?*

Only Veza made the cut.

Brent Lassi
CISO
Bluecore

"The most critical thing about data security is knowing what you have. You need to know where it is, how long you've had it, and how well it's protected. Veza helps me do all of it. It was hard to find something that didn't treat Google Cloud like a third-class citizen...I was reassured to see that Veza took Google very, very seriously from the get go."

Get started with Veza for Google Cloud

To learn more about how Veza can bring identity security to your Google Cloud environment visit veza.com/schedule-demo to schedule a personalized demo.

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.

© 2024 Veza, Inc. All Rights Reserved | *veza.com*