veza ⇄ aws Solution Brief

Veza for AWS

If AWS is a cornerstone of your cloud infrastructure, excessive or misconfigured access permissions in AWS IAM can be your 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 AWS?

Identity security challenges for AWS Customers

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

Almost every aspect of your AWS environment is highly configurable, including identity access. The AWS IAM manual runs to over 1200 pages, with over 100 distinct permissions for S3 alone! Add in the challenge of resolving interactions between identity and resource-based policies, access control lists (ACLs), and permissions boundaries, and it's extremely difficult to predict what access a particular identity will have to a resource.

Scale

Security and governance teams are managing many more resources and identities in AWS than in the on-prem world, especially when you account for machine identities and service accounts. 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.

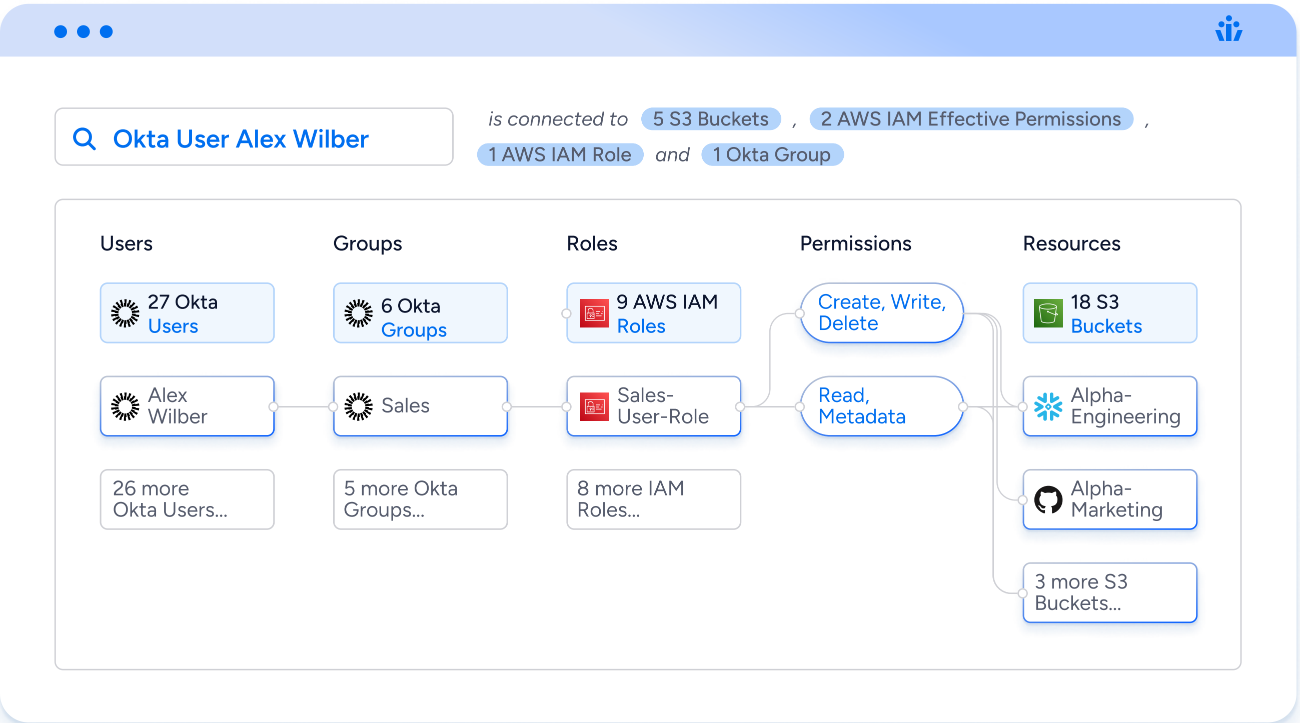
Siloed access data

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

> 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 AWS, leaving the question: How can you manage what you can't see? Moreover, companies can save money and hassle by finding a platform that visualizes access to all systems: cloud infrastructure, on-premise apps, SaaS apps, and data lakes.

How Veza can help

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



Okta User Alex Wilber

is connected to 5 S3 Buckets , 2 AWS IAM Effective Permissions , 1 AWS IAM Role *and* 1 Okta Group

Effective permissions

Effective permissions translate AWS 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 AWS. For example, Veza would show that "Okta user Alex Wilber can delete data from the finance bucket in S3."

Authorization graph

Veza's Authorization 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. Automated monitoring of access permissions for misconfigurations and excess privilege helps you 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 AWS and your identity providers, giving a complete picture of the access granted to federated identities, revealing governance blindspots, like local users or personal email addresses in AWS IAM.

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 AWS 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 AWS services

Veza connects to the full range of AWS services to manage identity security across your cloud infrastructure, including AWS IAM itself, data systems like S3 and Redshift, Compute resources like EC2 and Lambda, and more.

CLOUD PROVIDERS & CLOUD IAM | DATA SYSTEMS | RESOURCES & INFRASTRUCTURE

- AWS Cognito
- AWS DynamoDB
- AWS EC2
- AWS EMR
- AWS IAM
- AWS IAM Identity Center
- AWS KMS
- AWS Lambda
- AWS Redshift
- AWS VPC
- AWS RDS
- AWS RDS Aurora
- AWS RDS DocumentDB
- AWS RDS MySQL
- AWS RDS Oracle
- AWS RDS PostgresQL
- AWS RDS SQL Server
- AWS S3
- AWS Security Groups
- AWS EKS

Three steps to identity security with Veza and AWS

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.

Step 2: Triage your less obvious security risks with blast radius analysis to reveal identities with access to a large number of AWS 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 AWS, all based on the effective permissions of identities.

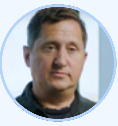
Step 3: Build a program of automated access control. Identify your data crown jewels, monitor continuously for new access and create workflows for access remediation. Sleep a little easier knowing you're proactively fixing excess privilege and misconfigurations as they occur, not after they empower an attacker.

Customer insights

PayNearMe uses Veza to continuously enforce the principle of least privilege across their AWS environments, and to dramatically reduce the burden of access reviews for compliance. Check out their full story here.

Sean Todd
CISO
PayNearMe

> *Using Veza allows me to sleep better at night because I know that there is an automated tool watching our systems. Even if one of our infrastructure engineers decides to make changes in the middle of the night...I know that we'll be getting alerts if those changes make us less secure.*



> *What once had taken weeks, we were able to do with Veza in minutes*

Ziggy Brode • Data Security Engineer
PayNearMe

Get started with Veza for AWS

To learn more about how Veza can bring identity security to your AWS environment, take a self-guided tour of our AWS integration or 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.

Extended feature list

AWS IAM Analysis for Least Privilege & Misconfigurations

Insights for Cloud IAM, including privileged users, privilege escalation & lateral movement

AWS Misconfiguration Analysis

Misconfigurations for the entire AWS environment, including identities and data

AWS IAM Advanced Configuration Analysis

Analysis on advanced configurations for all Cloud IAM, including Deny, Permission Boundary, etc

Dormant Entity Analysis

Dormant entity analysis, including users, groups, roles, service accounts, etc

Custom Rules

Monitor the result of any query and take a predetermined action, such as alerting a Slack group, or creating a workflow in ITSM or SOAR tools.

Risks

Track access violations, misconfigurations and hazardous behavior with auditing capabilities, supporting data for the last 6 months

Authorization Risk Dashboard

Customizable dashboard showing top authorization risks for AWS

User Analysis

Construct insights for users, groups and roles, and configure alerts, rules and reports from an english translated, simplified builder

Access Monitoring for AWS

Monitor which users are accessing AWS resources, like S3 buckets and KMS credentials. Identify and remove unused access.

Reports Library

Catalog of all reports with support for individual, team and organizational level visibility

Customizable Reports

View Veza s out of the-box reports and create your own by utilizing saved queries

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

Support for Cross-AWS-Account AssumeRole Relationships

Highlight the assumeRole relationship across AWS accounts

Query Builder for any-to-any relationship

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

User and Entitlement Access Reviews

Automated workflows to review access based on users

Automatic Reviewer Assignments for Certifications

Automatic certification row assignments to user's manager or the owner of the entitlement

Flexibility for access review delegation

Allow deny list and multiple fallback options to assign access reviewers

Customizable behaviors for certification completion

Allow access workflow creator to define the behaviors of certification completion: auto-complete when all certification items are signed-off or auto-complete when the certification reaches its due date

Filtering and Smart Actions for certification line items

Smart actions to bulk approve/reject/re-assign all certification items that fit a criteria

Notifications and 3rd-party integration for certification actions

Email notifications for per-reviewer reminder on certification status, Slack and ServiceNow integrations on accept/reject actions for each certification item