Veza for Okta

Veza bolsters Okta's authentication capabilities with visibility into access—the granular permissions identities have to apps and data across your stack.

Veza allows you to definitively answer the question of:

Who can take **what action** on **what resources?**

Identity security challenges in Okta

Validating outcomes

IT teams respond to employee requests for access by adding employees to groups in Okta. But the granular permissions of groups are not visible in Okta, so it's difficult to be sure that the employee will actually get the access they need and, just as importantly, that they won't get a lot of access they don't need.

Enforcing use

While Okta allows IT teams to centralize provisioning, each of your cloud providers, data systems, and apps allow for local accounts and local admins. The result is a split between "official" access through Okta, and "shadow" access through local accounts.

Misconfiguration & risks

While Okta provides limited of out-of-the-box reporting, it lacks sophisticated access intelligence tools, like the ability to create custom queries to identify risky permissions or track adherences to best practices.

Blackstone

"Veza gives us both broader and deeper visibility into who has access to our data, and how they have access to that data, so we can trust and verify that all personnel only have the access they need."

Puneet Bhatnagar
SVP, Head of IAM – Cybersecurity

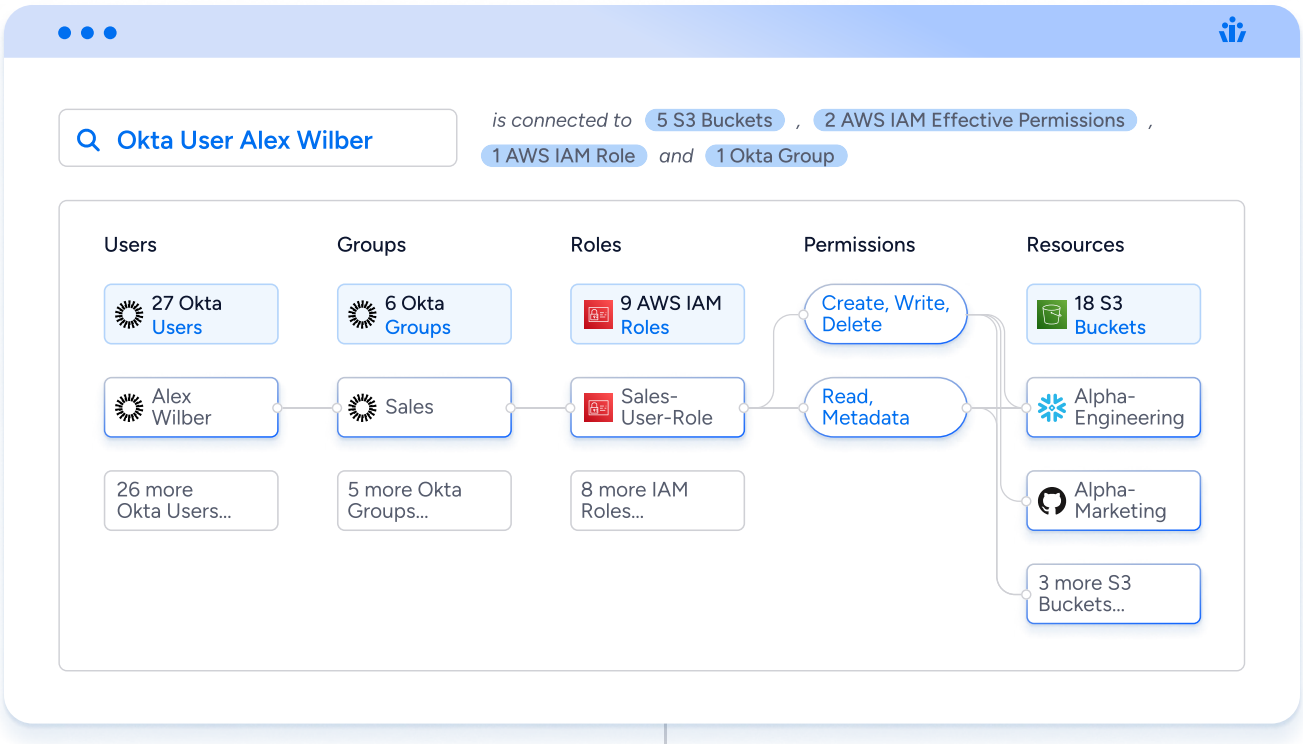
CHOICE HOTELS

"Veza brought something unique to the table...the Access Graph that lets us deeply understand the link between Okta to all of our different AWS accounts, to our databases, and Active Directory...to visualize that in 30 seconds is truly amazing."

Jason Simpson
VP of Engineering

How Veza can help

Veza is powered by its Access Graph, which gives organizations the ability to visualize access relationships between all identities and systems by connecting users, groups, roles, and permissions.



Key benefits

Reduced risk

Automate monitoring and remediation for misconfigurations, risks and best practice violations in Okta.

Least privilege

Understanding the effective permissions each Okta group grants allows you to shrink your attack surface and make efficient provisioning decisions that avoid excessive or unnecessary permissions.

Team efficiency

Bridge data silos and create a single control plane for identity governance, spanning not just Okta, but all identity providers, cloud infrastructure, data warehouses and on-premise systems.

Key features

Ensure effective & accurate provisioning

Validate the outcomes of your group assignments in Okta to make sure that employees receive the permissions they need, and no more.

Surface ungoverned identities

Compare local accounts in your cloud providers, data systems, and SaaS apps against Okta data to find and remove ungoverned accounts circumventing your Okta provisioning processes.

Identify misconfigurations & risks

Deploy out-of-the-box reports and custom access queries to identify IAM misconfigurations, like admins without MFA, dormant users, and sovereignty violations, plus risk factors such as privilege drift.