veza | Solution Brief

Veza for Azure

Comprehensive visibility and control over data authorization to secure any resource in Microsoft Azure

Microsoft Azure provides organizations with the environment, tools, and building blocks to build and deploy new cloud services.

A critical function for securing the cloud is access management. Azure role-based access control (Azure RBAC) is the system that provides fine-grained access management to Azure resources. It can separate permissions within a team so that you can give the least privilege possible to users through out-of-the-box and custom roles. Azure RBAC is built on top of Azure Resource Manager (ARM), allowing organizations to define access controls on four levels of scope (management groups, subscriptions, resource groups, and resources) to manage who can see, create, update and delete Azure cloud services. Identities are stored in Azure AD and can be used within Azure itself when assigning roles and permissions or as a broader identity provider across many different systems beyond what Microsoft provides.

The relationship between Azure RBAC, ARM, and Azure AD is challenging to understand and manage and can result in enabling thousands of permissions at varying levels of scope. Veza makes sense of the relationships between human and non-human users, groups, roles, the permissions assigned, and surfaces varying access levels to subscriptions, resources, and Azure data assets. This allows you to understand who (both inside and outside of Azure AD) can access what resource, and what action they can take on data in Azure in addition to services outside of the Microsoft ecosystem.

Challenges for Azure Customers

Digital transformation fuels an exponential growth of both identities (e.g., business users, admins with high privileged access, and non-human service accounts) and modern software components, such as applications, containers, microservices, and scripts. These identities need access to resources in Azure like databases or application APIs that security teams struggle to maintain due to the immense complexity of these relationships.

Common challenges faced by organizations using Azure include:

- Traditional IAM tools are built for legacy systems and fail to manage and detect errors in data entitlements like the unmanaged accumulation of privileges, presence of dormant users and/or permissions, and ability to remediate and implement least privilege principles.

- As more organizations move to the cloud, so does their work with third parties. Azure has been innovative in enabling B2B features that allow to invite and grant access to users from other companies, but continuously monitoring whether third parties have the proper permissions to company data through Azure RBAC has become a new challenge.

Choose Veza to secure access to data and resources in Azure

Veza helps securely accelerate your organization's Azure adoption by providing visibility into the identity-to-data relationships that explain who can take what action on Azure services. Security, IT, Data, and DevOps teams can search, define, and correct authorization policies for Azure AD identities and Azure services and data stores, reducing excessive cloud data entitlements and over privileged accounts.

Organizations that use Veza to secure their Azure environment benefit from the ability to:

- Identify and explain in human-understandable language what data a human or service account can create, read, edit, or delete (CRUD) by parsing SQL access controls' raw permissions for granular resource objects (e.g., schema, database, table, or view).

- Gain full visibility and control over all externally exposed Azure resources and services.
- See Azure AD Guest Users and associated permissions, and monitor whether the company's data is exposed.
- Visualize users, roles, and applications with access to Azure VMs and virtual networks, and track which role assignment or group membership enables that access.
- Periodically certify authorization controls to ensure compliance and a strong security posture.
- Approve, reject, and certify user/group memberships, access to Azure AD granular data objects within enterprise applications, role modeling/governance/assignments, and permissions to any supported data services and resources.

Veza's support for Azure services resources spans across -

Azure RBAC

Azure AD

Azure SQL

Azure Resource Manager

Azure Virtual Machines

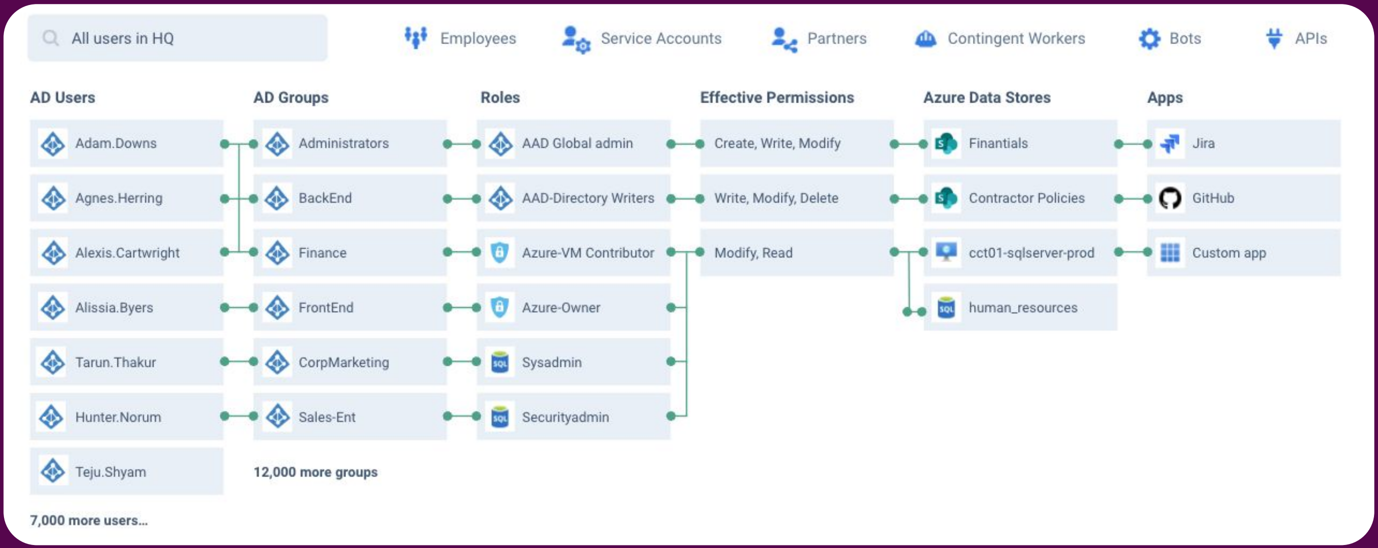
Azure Virtual Networks

Meet Veza for Azure

Authorization-Based Management for Access Reviews, Data Governance, Privileged Access, Cloud Entitlements, and more

veza | Microsoft Azure

Veza's data security platform enables you to understand data authorization and manage effective IAM permissions for Azure resources. Veza streamlines compliance audits, drives meaningful data insights into the access review processes and helps prevent ransomware by discovering data access permissions mistakes for Azure resources.



All users in HQ

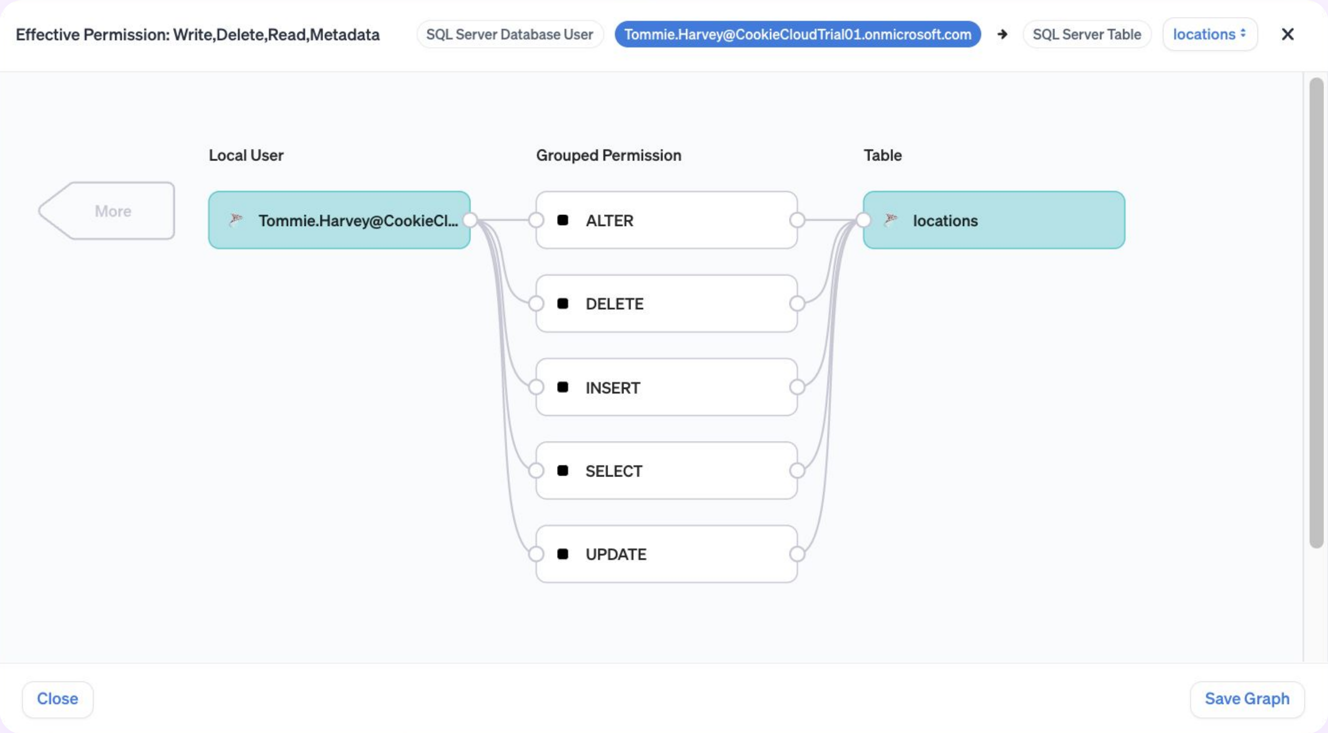
Employees | Service Accounts | Partners | Contingent Workers | Bots | APIs

AD Users	AD Groups	Roles	Effective Permissions	Azure Data Stores	Apps
Adam.Downs	Administrators	AAD Global admin	Create, Write, Modify	Finantials	Jira
Agnes.Herring	BackEnd	AAD-Directory Writers	Write, Modify, Delete	Contractor Policies	GitHub
Alexis.Cartwright	Finance	Azure-VM Contributor	Modify, Read	cct01-sqlserver-prod	Custom app
Alissia.Byers	FrontEnd	Azure-Owner		human_resources	
Tarun.Thakur	CorpMarketing	Sysadmin			
Hunter.Norum	Sales-Ent	Securityadmin			
Teju.Shyam	12,000 more groups				
7,000 more users...					

Here are some of the ways Veza empowers you to manage authorization for Azure resources:

Search & Discover

- See which users and applications can reach Azure resources (including VMs and virtual networks). The **Authorization Graph** simplifies the permission relationships between human and non-human users and Azure RBAC controls.
- Visualize and manage SQL resource-centric access controls (across system-defined roles, user-defined roles, database roles, and associated permissions). For example, who can access sensitive data in an Azure SQL database, and how are those permissions obtained?
- **Search** to track effective permissions resulting from the combined effect of group memberships, Azure Roles, and accounts assigned to a subscription, resource group, or individual service.
- Identify non-human accounts such as Azure AD Service Principals, and improve lifecycle management and permissions traceability for Microsoft and Line of Business (LOB) app APIs.



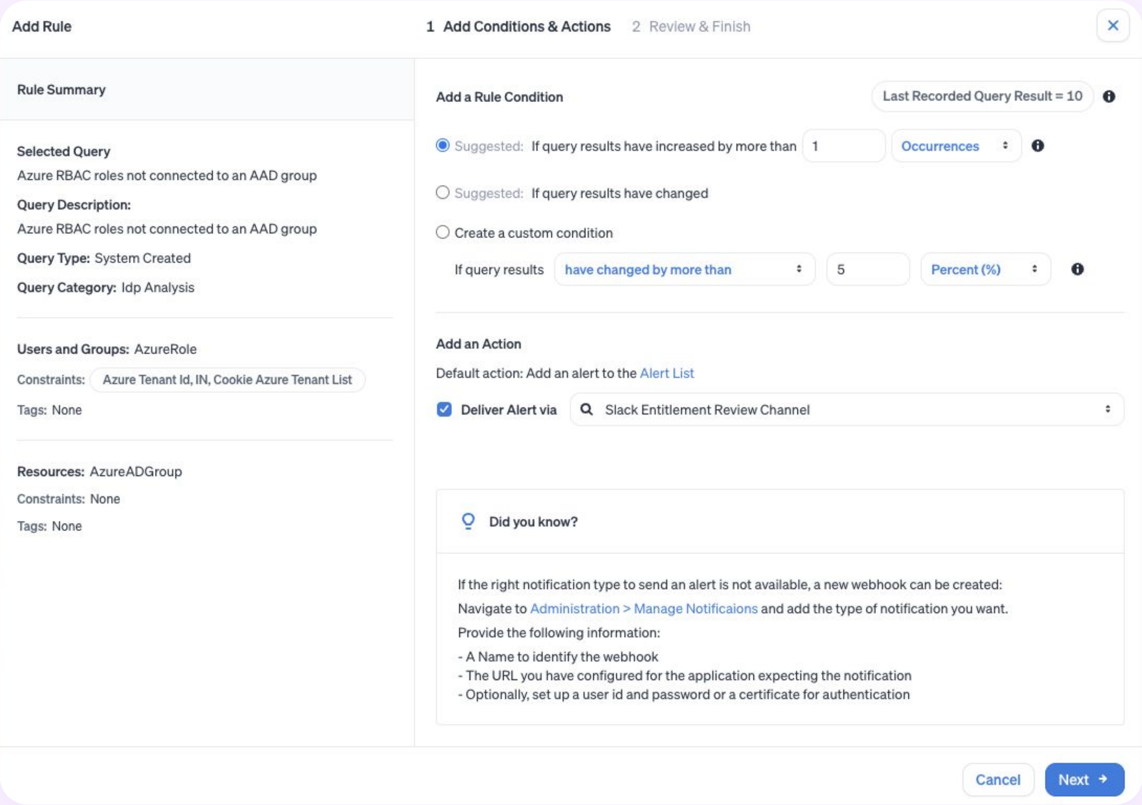
Effective Permission: Write,Delete,Read,Metadata

SQL Server Database User | Tommie.Harvey@CookieCloudTrial01.onmicrosoft.com → SQL Server Table | locations

Compare & Correct

- Monitor changes and get rapid insights into anomalies and risks specific to Azure using **Reports**. For example, track increases in the number of users with Domain Admin privileges, watch for Azure Network Security groups allowing HTTP inbound traffic and identify RBAC roles with static user mappings.
- Define security posture **Violations** for your organization to enable customizable flagging and monitoring of least privilege standards, such as highlighting dormant Azure AD users, identifying RBAC roles with static user mappings bypassing the use of security groups, or others.

- ✓ Create **Rules** to trigger alerts when privileges change within Azure, use email notifications and **Webhooks** to integrate with enterprise ticketing systems (e.g., Jira, ServiceNow, et al.), and CI/CD processes.
- ✓ Visualize changes between entitlement reviews. For example, focus on which users have gained new permissions to Azure SQL databases during a new certification event.
- ✓ Use step-by-step **Recipes** when deviations from policies are detected and modify a role assignment or remove a group membership to resolve data authorization infringements and maintain policy compliance.



Add Rule

1 Add Conditions & Actions 2 Review & Finish

Rule Summary

Selected Query
Azure RBAC roles not connected to an AAD group

Query Description:
Azure RBAC roles not connected to an AAD group

Query Type: System Created

Query Category: Idp Analysis

Users and Groups: AzureRole

Constraints: Azure Tenant Id, IN, Cookie Azure Tenant List

Tags: None

Resources: AzureADGroup

Constraints: None

Tags: None

Add a Rule Condition — Last Recorded Query Result = 10

● Suggested: If query results have increased by more than 1 Occurrences

○ Suggested: If query results have changed

○ Create a custom condition

If query results have changed by more than 5 Percent (%)

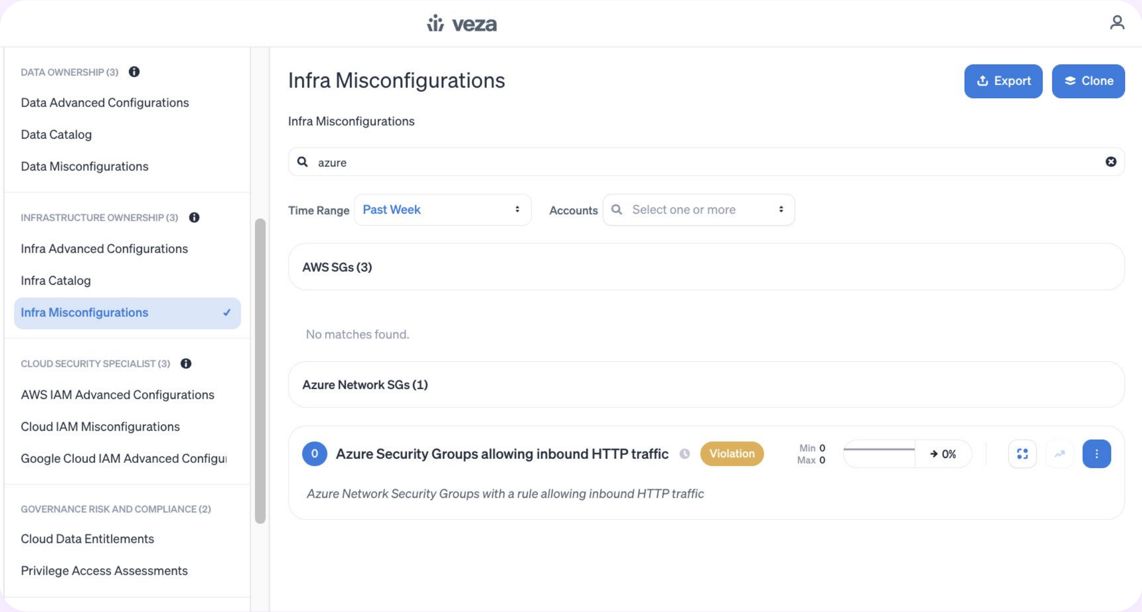
Add an Action

Default action: Add an alert to the Alert List

☑ Deliver Alert via Slack Entitlement Review Channel

Did you know?

If the right notification type to send an alert is not available, a new webhook can be created:
Navigate to Administration > Manage Notificaions and add the type of notification you want.
Provide the following information:
- A Name to identify the webhook
- The URL you have configured for the application expecting the notification
- Optionally, set up a user id and password or a certificate for authentication



veza
DATA OWNERSHIP (3)
Data Advanced Configurations
Data Catalog
Data Misconfigurations
INFRASTRUCTURE OWNERSHIP (3)
Infra Advanced Configurations
Infra Catalog
Infra Misconfigurations ✓
CLOUD SECURITY SPECIALIST (3)
AWS IAM Advanced Configurations
Cloud IAM Misconfigurations
Google Cloud IAM Advanced Configu
GOVERNANCE RISK AND COMPLIANCE (2)
Cloud Data Entitlements
Privilege Access Assessments
Export
Clone

Infra Misconfigurations

Infra Misconfigurations

azure

Time Range: Past Week — Accounts: Select one or more

AWS SGs (3)

No matches found.

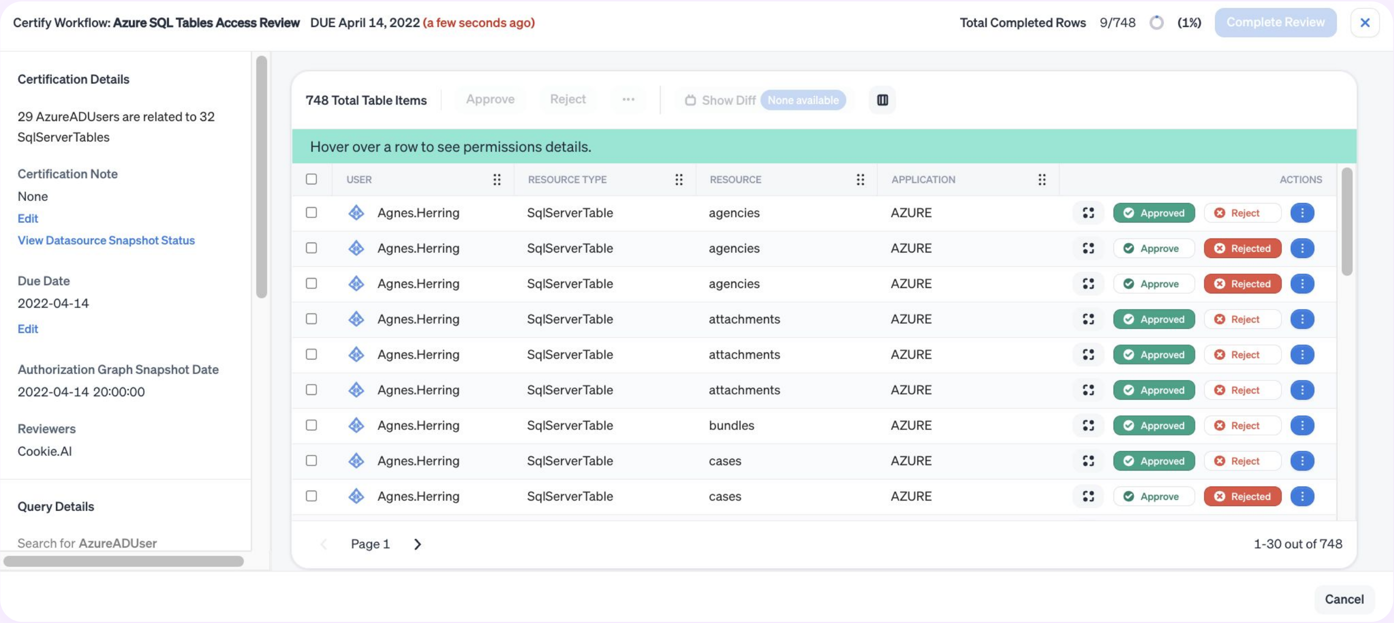
Azure Network SGs (1)

0 Azure Security Groups allowing inbound HTTP traffic — Violation — Min 0 Max 0 — → 0%

Azure Network Security Groups with a rule allowing inbound HTTP traffic

Define & Control

- Query and oversee Azure RBAC roles and permissions, and identify their scope of action — for example, find roles with excessive permissions mapping or users with the most Azure RBAC roles assigned to them.
- Create repeatable certification processes with Veza's **Access Review Workflows** product, and approve, reject, and certify group memberships, access to enterprise applications, role assignments, and authorization to data resources like Azure SQL.
- Instantly search and visualize Azure RBAC role assignments and resources using the **Authorization Graph**, and make decisions about effective permissions for new Azure deployments and services based on your organization's best practices.
- Gain visibility into external identities (Azure AD Guest Users) and associated permissions (what access and roles they have), remove any lingering access and reduce data theft and ransomware risks.
- Enforce implementation of zero trust controls for Azure resources through built-in audit assessments and least privilege **Insights** into privileged access, SQL data sets, overly permissive roles, segregation of duties, lingering access, etc.
- Utilize **Search** to find current data access entitlements within Azure resources when investigating the true blast radius of a data breach, and recommend appropriate follow-up actions/remediation to security teams.



Certify Workflow: **Azure SQL Tables Access Review** DUE April 14, 2022 (a few seconds ago)

Total Completed Rows 9/748 (1%)

Certification Details

29 AzureADUsers are related to 32 SqlServerTables

Certification Note
None
Edit
View Datasource Snapshot Status

Due Date
2022-04-14
Edit

Authorization Graph Snapshot Date
2022-04-14 20:00:00

Reviewers
Cookie.AI

Query Details

Search for AzureADUser

748 Total Table Items

Hover over a row to see permissions details.

□	USER	RESOURCE TYPE	RESOURCE	APPLICATION	ACTIONS
□	Agnes.Herring	SqlServerTable	agencies	AZURE	Approved Reject
□	Agnes.Herring	SqlServerTable	agencies	AZURE	Approve Rejected
□	Agnes.Herring	SqlServerTable	agencies	AZURE	Approve Rejected
□	Agnes.Herring	SqlServerTable	attachments	AZURE	Approved Reject
□	Agnes.Herring	SqlServerTable	attachments	AZURE	Approved Reject
□	Agnes.Herring	SqlServerTable	attachments	AZURE	Approved Reject
□	Agnes.Herring	SqlServerTable	bundles	AZURE	Approved Reject
□	Agnes.Herring	SqlServerTable	cases	AZURE	Approved Reject
□	Agnes.Herring	SqlServerTable	cases	AZURE	Approve Rejected

Page 1 1-30 out of 748

veza | Solution Brief Microsoft Azure

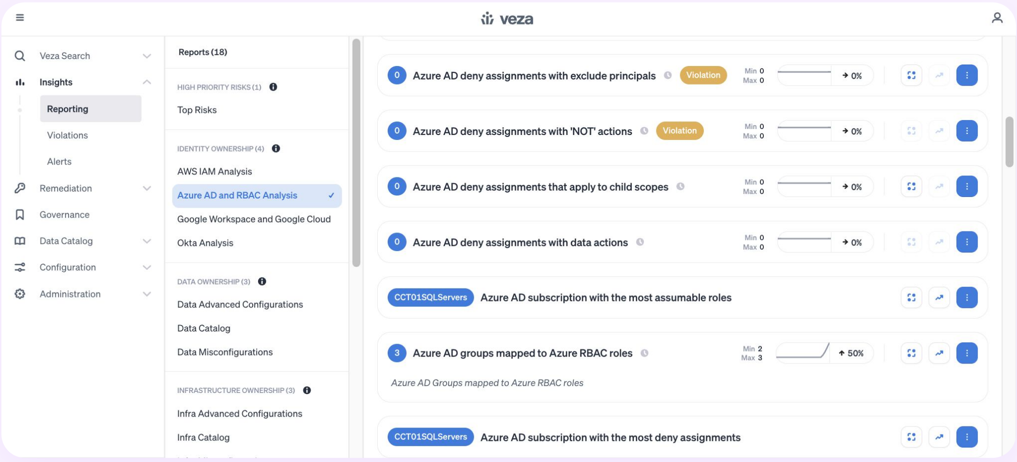
Getting Started

Veza discovers resources across Azure using an App Registration. Registering an application enables core features such as the authentication of the application and the possibility of granting permissions and access to other apps, services, or Azure resources. Before you can add Azure to read metadata about IAM objects and resources in Azure from the Veza UI, you will need to:

1. Go to Azure AD, navigate to App Registration and create a new application. Generate the application credentials (Secret) to access the APIs.

2. Grant admin consent to the application for API permissions on the Microsoft Graph. Read-only permissions are required to look for users, groups, roles, applications, reports, and more.

3. Begin reviewing an extensive list of pre-built assessments for Azure RBAC, Azure AD, and Azure Data services using **Dashboards** and **Reports**.



Reports (18)

HIGH PRIORITY RISKS (1)
- Top Risks

IDENTITY OWNERSHIP (4)
- AWS IAM Analysis
- Azure AD and RBAC Analysis ✓
- Google Workspace and Google Cloud
- Okta Analysis

DATA OWNERSHIP (3)
- Data Advanced Configurations
- Data Catalog
- Data Misconfigurations

INFRASTRUCTURE OWNERSHIP (3)
- Infra Advanced Configurations
- Infra Catalog

0	Azure AD deny assignments with exclude principals	Violation	Min 0 Max 0	→ 0%
0	Azure AD deny assignments with 'NOT' actions	Violation	Min 0 Max 0	→ 0%
0	Azure AD deny assignments that apply to child scopes		Min 0 Max 0	→ 0%
0	Azure AD deny assignments with data actions		Min 0 Max 0	→ 0%
CCT01SQLServers	Azure AD subscription with the most assumable roles			
3	Azure AD groups mapped to Azure RBAC roles *Azure AD Groups mapped to Azure RBAC roles*		Min 2 Max 3	↑ 50%
CCT01SQLServers	Azure AD subscription with the most deny assignments			

4. Perform queries using **Search** to explore and manage identity-centric authorization relationships within Azure. Create your own queries to define security **Violations**, quickly detect misconfigurations, data risks, and configure **Rules** and **Alerts** to inform teams when privilege drift is detected across your Azure portfolio.

If you're interested in learning more about how Veza can work alongside your existing Azure deployment to meet least privilege needs, check out our website at www.veza.com/platform.

● 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.