veza | Solution Brief

The Veza Data Security Platform

How We Enable Teams to Safely Leverage Their Cloud Data

Overview

Doing business today requires trusting a rapidly expanding set of identities to access, use, and share your data in the cloud. But risk multiplies as data access grows ever more complex, and harder to centrally control and manage. This problem is exacerbated by the convergence of certain key trends around data:

The amount of data is still growing fast

We live, work and play remotely and online now (even more in the COVID era), creating an ever growing quantity of data exhaust which must remain reliably accessible. As a result, organizations have to find a way to capture, store, and retrieve more data than ever before.

Data is more valuable than ever

For most organizations, data remains their most valuable asset. Driven by rapid advances in data science, artificial intelligence (AI) and machine learning (ML), businesses increasingly depend on data-based decision-making. But as enterprises find new ways to leverage their data, this creates additional risk exposure, and ransomware has become a top global executive concern. If threat actors capture your customer data, operational data, or source code, it can cripple your company for a long time, and create front-page news.

Data is finally moving to the cloud

The last stage of digital transformation is here: On the heels of earlier migrations of infrastructure, apps, and compute to the cloud, enterprise data—the "crown jewel" of every organization—is finally leaving the on-prem data center. Purpose-built cloud data solutions like Snowflake are increasingly the solutions of choice.

The convergence of these trends has led to an immense increase in complexity for organizations trying to manage data security, in the form of a distributed, dynamic web of data, relationships and access points that are incredibly difficult to track. Truly understanding who can access what data across this complex environment requires pulling together traditionally siloed data sources, including identity management (like Okta or Microsoft Azure AD), permissions systems of Cloud Service Providers (like AWS IAM, Azure RBAC, and GCP IAM), and system-level permissions from services, apps, and systems like S3, Github, and Snowflake. Each of these data sources is immensely complex on its own—at last count, the AWS IAM User Guide was 1,091 pages long, and Azure RBAC's documentation is even longer. And different systems use different languages: For example, permissions and local users are defined differently in S3, Snowflake, and SQL Server. It's a daunting, and growing, challenge.

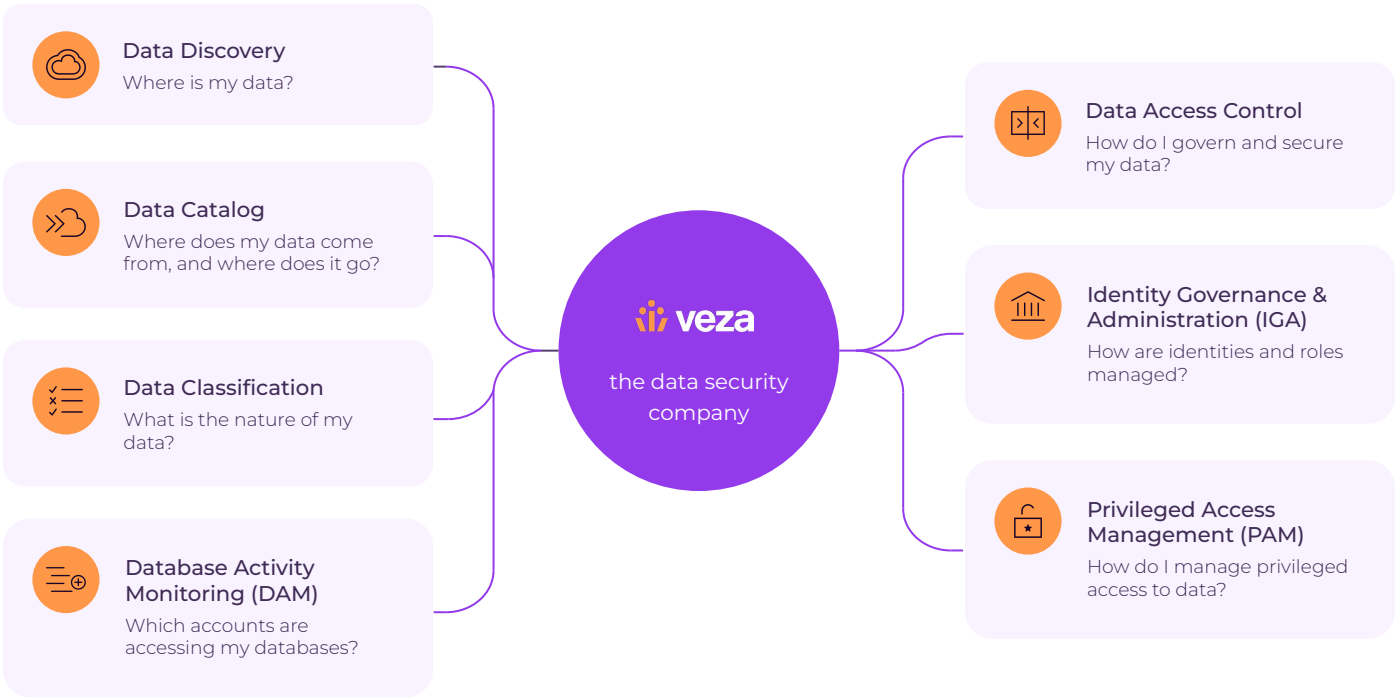
Enterprises need to be able to answer the fundamental question of data permissions: Who has access to what. And that requires gathering and piecing together data and relationships across all the different permutations of users, service accounts, and groups, and different flavors of IAM policies, and understanding how to parse and compare the various permission languages of different services. It's very difficult for even seasoned professionals just to understand the actual reality of what's in place now—an organization's "effective permissions"—never mind tracking dynamic changes to users and infrastructure, or designing a solution when something goes wrong that doesn't create unseen collateral damage. Cutting through all this complexity is the challenge of the day.

And the clock is ticking: The expanded cloud data access your users are enjoying today is already multiplying security risk. Cyber-threats are multiplying and growing more costly; ransomware is now the #1 threat for CISOs and boards. It's becoming increasingly difficult and expensive to meet security and privacy compliance requirements without tools purpose-built to solve this problem. In the same way that you can't simply lift and shift Oracle DBs to a cloud data center and expect to get the outcome you need, legacy on-premise security systems simply don't work in a zero-trust cloud environment—securing cloud data requires a completely new security stack.

It's becoming clear that the cloud data solutions that organizations need won't be coming from Cloud Service Providers like AWS, Azure, and GCP, who have a fundamental conflict of interest in their business need to drive customers solely to their own infrastructure services. And traditional data security solutions that only deal in identity are becoming widely recognized as "security theater," allowing companies to pass audits without providing the information needed to meaningfully reduce security risks. Technical solutions that can see granular permissions-level information (e.g., which accounts can encrypt what data) are emerging as the best way to understand and reduce the risk.

So what is cloud data security starting to look like?

Meet Veza: The Data Security Platform Built On The Power of Authorization



Veza is the only data security program purpose-built to solve the number one problem in data security today—authorization. Working across hybrid-cloud and multi-cloud environments, Veza makes it easy for organizations to cut through the chaos and dynamically visualize, manage, and control data permissions, so they can definitively answer "who can and should take what action on what data" and confidently leverage their data.

Our platform pulls metadata from identity systems like Okta and Azure AD, from cloud service provider permissions systems like AWS IAM, GCP IAM, and Azure RBAC, and from data systems and apps like SnowFlake, SQL Server, Azure SharePoint, and GitHub.

All this information is mapped into one authorization metadata graph, producing a canonical model of Effective Permissions detailing exactly which users can create, read, update, or delete which data. Any organization's complex sea of permissions maps to a single comprehensive view that business users can understand, so they can address key business processes including cloud entitlements, privileged access, and data access governance.

Business Initiatives

Veza's cloud data security platform helps organizations complete their digital transformations, and centrally control their data at scale.

Redefine Zero Trust Security Through Data

Provide trusted data access in the cloud by deeply understanding and centrally controlling authorization across apps, data and cloud services

Securely Accelerate Adoption of Cloud Data

Transform your business by safely shifting data from ground to cloud, providing security without sacrificing accessibility

Modernize Data Security to Protect Against Ransomware

Data is the prize threat actors want—stay in control of your data by providing support for strong privileged access standards

See Veza in action!

See our Core Authorization Platform demo.

Watch now

Technical Projects

Our customers deploy Veza in a number of ways to solve today's toughest data security and access management challenges.

Implement data lake security

Give data owners new tools to secure and govern modern data lake repositories, including Snowflake, Redshift, GCP BigQuery, and more

Secure authorization for any app

Understand data access across all enterprise apps, including custom apps, with Veza's Open Authorization API

Modernize privileged access for data

Right-size permissions for cloud data resources, to enable privileged access while preventing privilege abuse

Streamline access governance

Make life easier for your governance, risk, and compliance teams with comprehensive certification workflows

Demystify complex Cloud IAM systems

Empower Cloud Ops, DevOps and DevSecOps teams with a thorough understanding of all effective permissions

Manage granular cloud data entitlements

Provide context-aware entitlement reviews to materially assist with audits and regulatory reviews

Manage runtime authorization

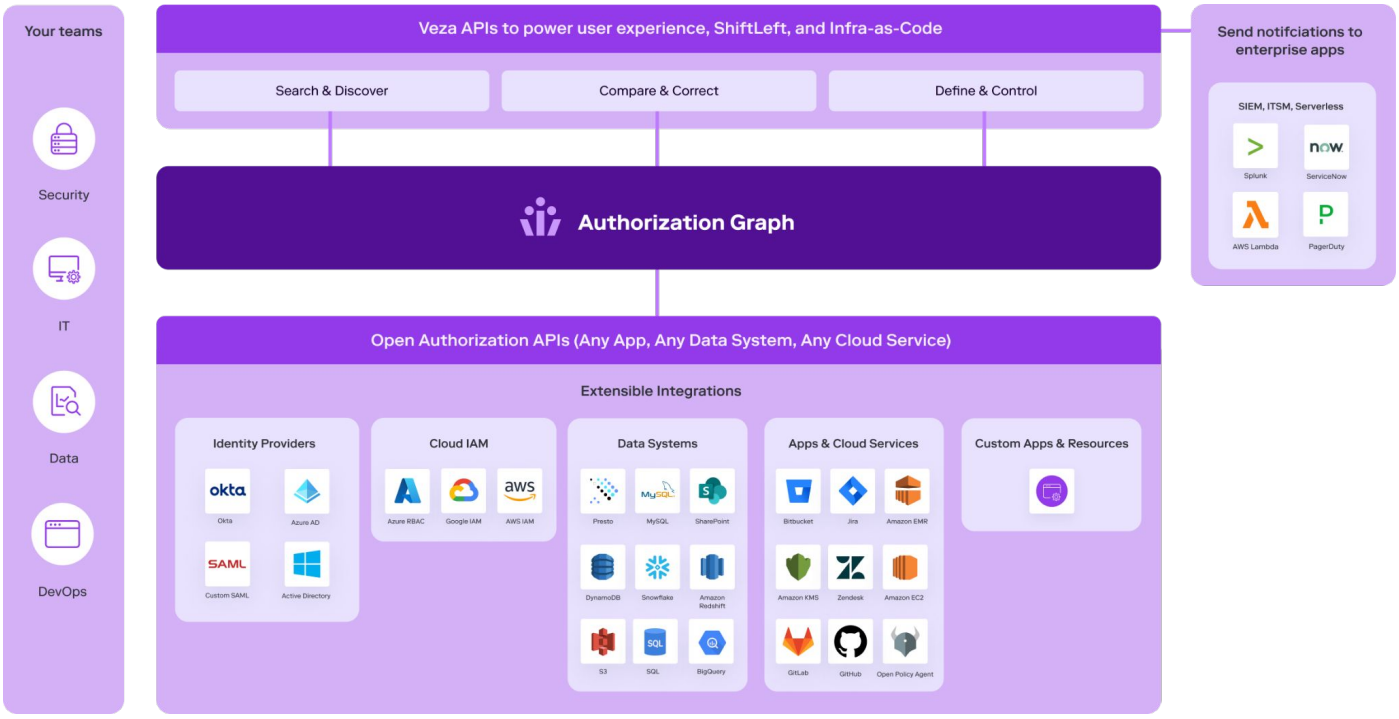
Design, implement, and enforce repeatable access controls on time, all the time, for all identities and all access points

Control proliferation of identities, secrets, and service accounts

Clean up external and internal "identity debt," conduct AD Identity Analysis, and validate role management and governance

Veza Core Authorization Platform

Veza Core Authorization Platform is a distributed-systems engine optimized for extracting authorization metadata, loading it into the Veza authorization metadata store, and supporting real-time querying of that metadata store. The Veza platform is built on four principles: a Data Model that can ingest any number of small objects, a Persistence Model providing distributed state management, an Object Model that organizes authorization metadata in a canonical way, and a Deployment Model that provides flexible support for organization's on-prem, hybrid-cloud, and multi-cloud systems.



The platform is tailor-made to handle scale and complexity, including a large number of metadata entities, temporal based changes in data sets, and high cardinality of data sets. These platform investments are at the heart of enabling the data security applications today's fast-growing companies need, like universal search, real-time query analysis, analytics and data access monitoring, access and entitlement workflows, and consistent authorization across multiple systems. Furthermore, Veza is built to seamlessly support massive AI/ML based capabilities, from access recommendations to natural language based universal search and more.

Veza Object Model

Veza Object Model is a uniform object model that intelligently collates and categorizes authorization metadata from a wide range of data sources, including Identity Providers (IdPs), Cloud IAMs and hundreds of different individual apps, data systems, and cloud services.

Parsing authorization metadata across all of these systems is a challenge, because it's heterogeneous in many ways, including:

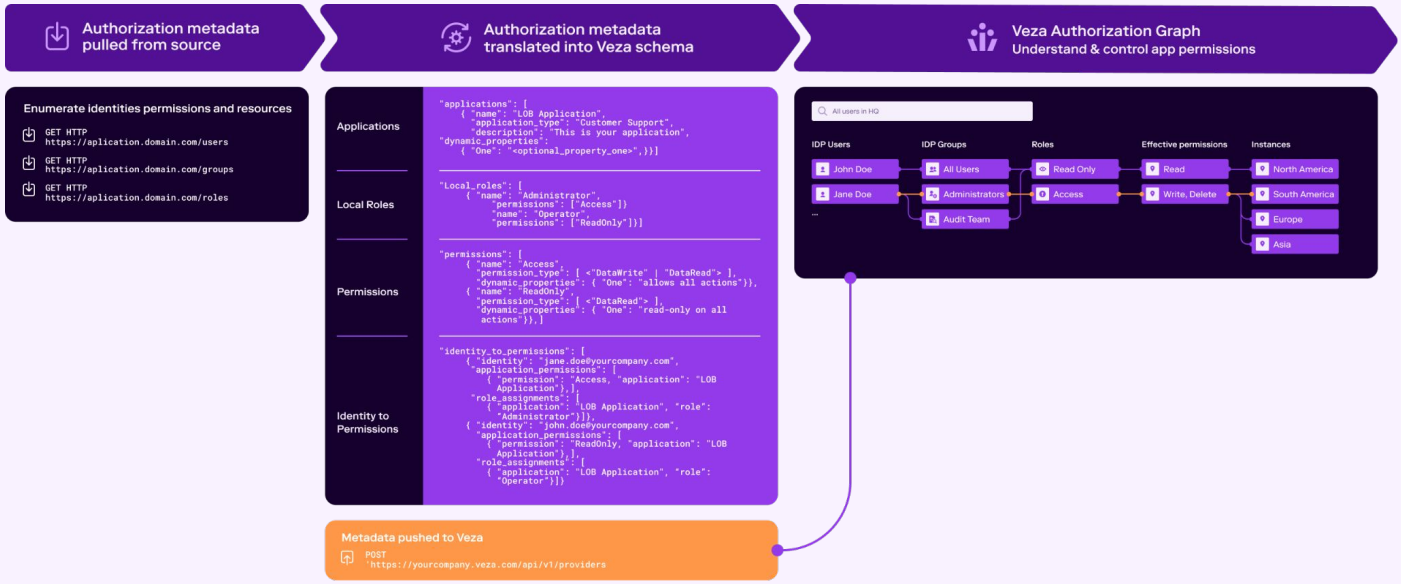
- The cardinality of authorization metadata can range from hundreds to millions, depending on data sources and data granularity, because it's a product of different permissions and potentially hundreds or millions of fine-granular data units (e.g., table columns).
- There are many different types of authorization schemes that must be understood and mapped, such as Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and tag-based access control schemes.

- Even for the same access control scheme (e.g., RBAC), different data stores can implement the control differently, meaning permissions across different data stores can be vastly different.
- Modern authorization systems have multiple complicated authorization layers where authorization can be granted or denied. For example, there might be several entities in the system granting a certain access, while a single, higher layer entity denies access—this must be properly accounted for across all affected paths in the authorization system.

These heterogeneous, extracted authorization metadata are effectively impossible to parse in real time without a purpose-built tool to normalize them so that customers can truly understand the authorization within their environments—and that's why a Canonical Object Model (COM) is needed.

Veza Open Authorization API (OAA)

Many of the most critical integrations are built natively into the Veza platform and work right out of the box. But sometimes a need to integrate systems arises—apps, data systems, etc.—for which there isn't yet a native integration. So Veza created the Open Authorization API (OAA), to enable easy integration to an ever wider range of data sources through a standard interface. OAA enables Veza, customers, and partners to create new, necessary integrations faster, allows integration of custom apps that would be unlikely to be included into a standard product roadmap, and allows customers to leverage internal expertise regarding how these custom apps should grant authorization.



OAA works by providing a standardized format for uploading authorization information to Veza. These schema maps are processed to integrate each new application into Veza's Authorization Metadata Graph, our comprehensive map that identifies which identities have what permissions to what resources. Once the new application is integrated via OAA into Veza, it acts like any other data source, becoming visible in Veza when querying the list of resources a user has access to, when specifying reports, and when configuring alerts.

Veza Product Design and User Experience

Interaction and usability are at the heart of the Veza platform, and providing intuitive solutions that help our users solve complex problems has remained our focus since Day 1. We provide our customers with a simple, elegant way to visualize the full complexity of modern identity-data relationships, and provide curated and custom reports, alerts and violations, and much more. From the initial configuration to the most complex product pages, we strive to bring clarity, consistency, and aesthetic integrity to each operation, so our users get a consistent, fast, and reliable first-class experience.

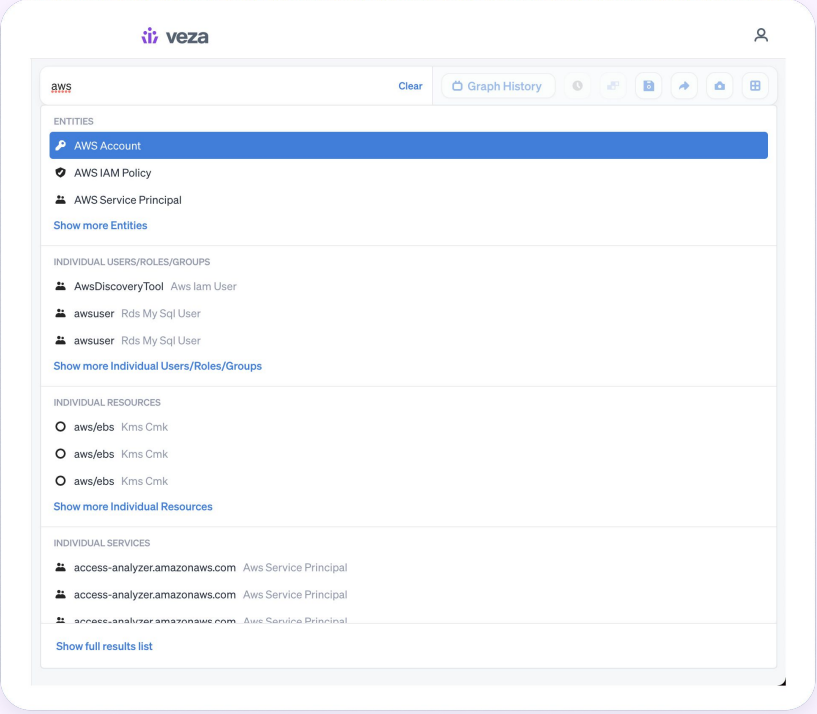
Configuring Veza is a quick and easy process; it typically takes under an hour to have a functional system up and running. As soon as Veza has ingested data from any configured cloud providers, it will immediately start showing information about Veza-identified violations and security risks revealed by the new data.

From the Veza landing page, these surfaced results can be explored in expertly curated assessments, collected views of discovered violations, and Veza-created alerts. All of this information can be viewed and manipulated in the Privilege Graph, a visual representation of the identity-data relationships that includes details on all the entities in these relationships. To explore additional representations of your identity-data relationships, creating queries for the Authorization Graph and for the Query Builder deliver other kinds of insights.

Veza Product Features

Search

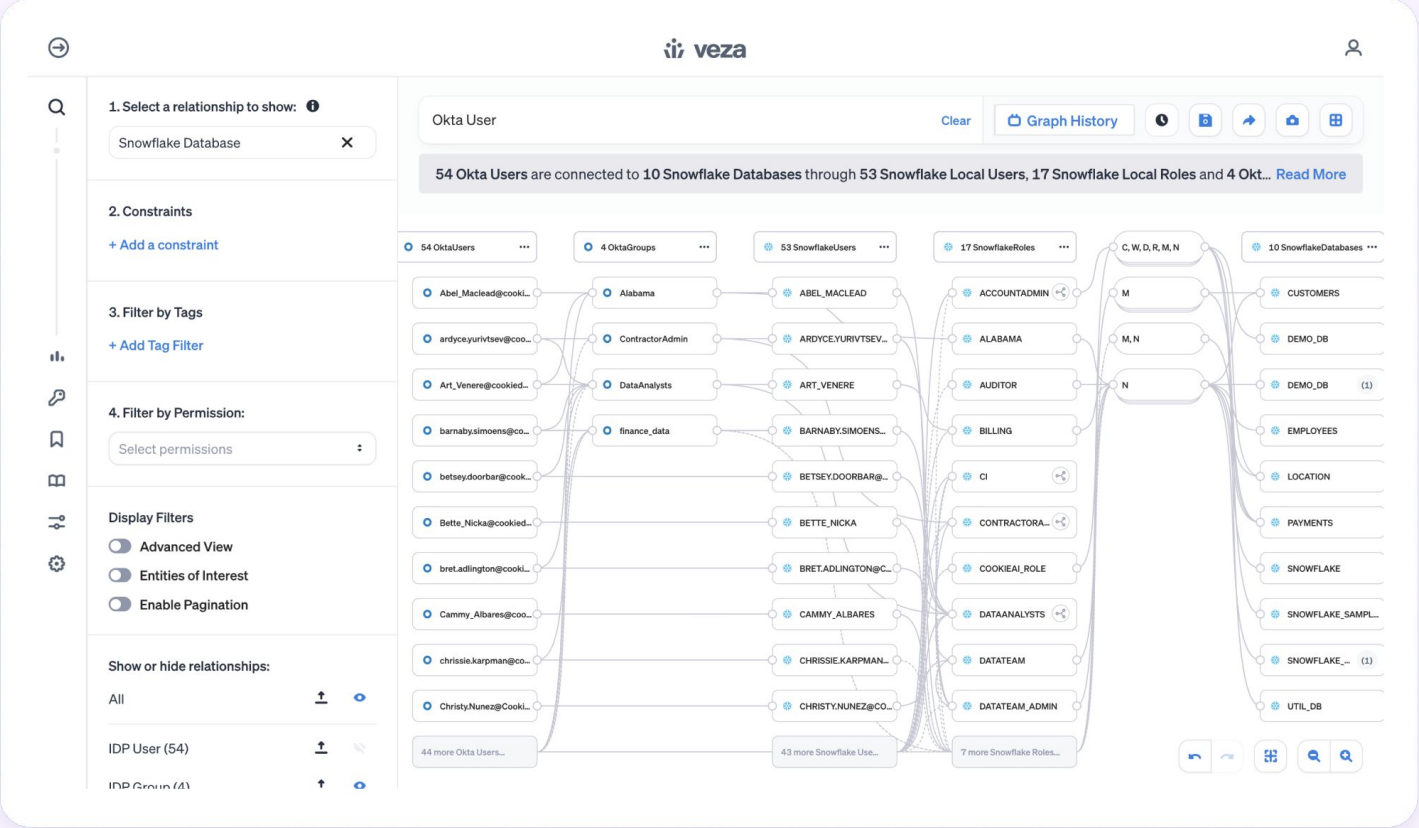
Veza provides consumer-like, real-time search delivered through an intuitive interface so users can explore and manage the identity-centric authorization relationships across their environment. Veza administrators can operationalize search results for access reviews, compliance audits, risk assessments, incident detection and response, and more. The search interface includes many modern innovations for large scale data gathering and rendering, including node bundling, edge bundling, pagination, node-specific actions, edge-specific actions, drill-up and drill-down controls for advanced users, time-based historical views, and a range of constraints and filters.



Authorization Graph

The Veza Authorization Graph gives organizations a centralized control plane for visualizing the authorization relationships between all users (humans, service accounts, etc.), apps, and data sources, including relationships based on authorization entities like users, groups, and roles in Cloud IAM solutions like AWS IAM, GCP IAM, and Azure RBAC. It simplifies the complexity of understanding authorization structures across key enterprise tools by presenting one simplified, centralized, comprehensive view of effective permissions (CRUD) for any enterprise identity and any data source.

Your teams can see which Okta users have delete permissions on Snowflake tables, which Azure users can create and delete AWS S3 buckets, which users are currently allowed to create and delete code repositories in GitHub, and much more.

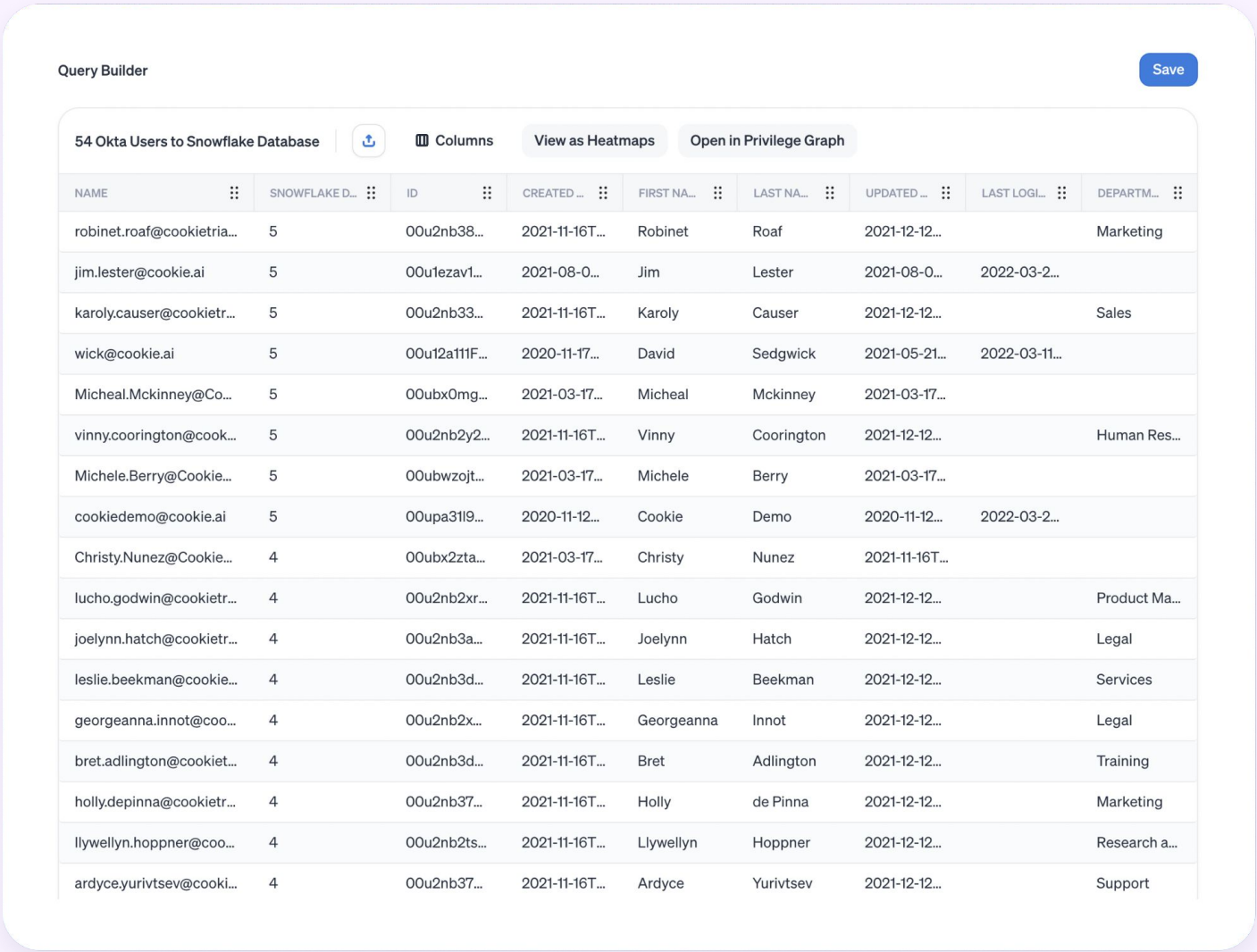


Query Builder

Our rich query engine enables complex filtering, sorting, and constraining of authorization metadata. Entity type selection can produce resource-centric or user-centric queries: For example, users can search for all S3 buckets with entitlements tied to Okta users, or for all Okta accounts with access to AWS S3 buckets.

Search options include:

- Refine queries by choosing a specific entity to query on
- Relay results to the Authorization Graph for further investigation, or switch to Heatmaps to quickly identify the most-privileged users or most-accessible data stores
- Apply one or more constraints to restrict the entities displayed in results
- Examine environment changes over time—run a search against a specific point over the last N days, or identify what's changed within a date range using snapshot data



NAME	SNOWFLAKE D...	ID	CREATED ...	FIRST NA...	LAST NA...	UPDATED ...	LAST LOGI...	DEPARTM...
robinet.roaf@cookietria...	5	00u2nb38...	2021-11-16T...	Robinet	Roaf	2021-12-12...		Marketing
jim.lester@cookie.ai	5	00u1ezav1...	2021-08-0...	Jim	Lester	2021-08-0...	2022-03-2...	
karoly.causer@cookietr...	5	00u2nb33...	2021-11-16T...	Karoly	Causer	2021-12-12...		Sales
wick@cookie.ai	5	00u12a111F...	2020-11-17...	David	Sedgwick	2021-05-21...	2022-03-11...	
Micheal.Mckinney@Co...	5	00ubx0mg...	2021-03-17...	Micheal	Mckinney	2021-03-17...		
vinny.coorington@cook...	5	00u2nb2y2...	2021-11-16T...	Vinny	Coorington	2021-12-12...		Human Res...
Michele.Berry@Cookie...	5	00ubwzojt...	2021-03-17...	Michele	Berry	2021-03-17...		
cookiedemo@cookie.ai	5	00upa31l9...	2020-11-12...	Cookie	Demo	2020-11-12...	2022-03-2...	
Christy.Nunez@Cookie...	4	00ubx2zta...	2021-03-17...	Christy	Nunez	2021-11-16T...		
lucho.godwin@cookietr...	4	00u2nb2xr...	2021-11-16T...	Lucho	Godwin	2021-12-12...		Product Ma...
joelynn.hatch@cookietr...	4	00u2nb3a...	2021-11-16T...	Joelynn	Hatch	2021-12-12...		Legal
leslie.beekman@cookie...	4	00u2nb3d...	2021-11-16T...	Leslie	Beekman	2021-12-12...		Services
georgeanna.innot@coo...	4	00u2nb2x...	2021-11-16T...	Georgeanna	Innot	2021-12-12...		Legal
bret.adlington@cookiet...	4	00u2nb3d...	2021-11-16T...	Bret	Adlington	2021-12-12...		Training
holly.depinna@cookietr...	4	00u2nb37...	2021-11-16T...	Holly	de Pinna	2021-12-12...		Marketing
llywellyn.hoppner@coo...	4	00u2nb2ts...	2021-11-16T...	Llywellyn	Hoppner	2021-12-12...		Research a...
ardyce.yurivtsev@cooki...	4	00u2nb37...	2021-11-16T...	Ardyce	Yurivtsev	2021-12-12...		Support

Tags

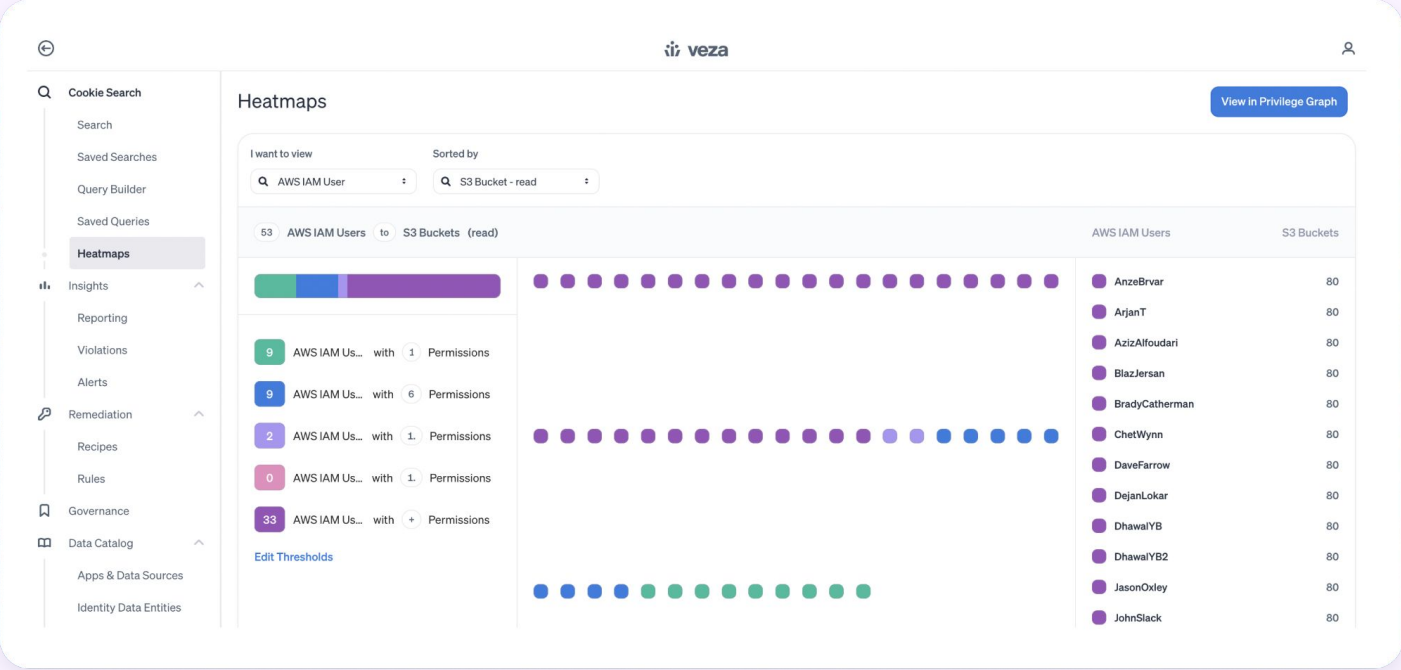
Tags are properties, consisting of an admin-defined key and value, that help security and data teams organize authorization entities, locate resources associated with specific workloads, environments, or ownership groups, and track kinds of data. For example, tagging certain data as “sensitive” helps customers meet requirements to determine who has access to sensitive datasets. Tags can be created in Veza and applied to any identity principal, cloud IAM object, or application entity; AWS tags, for example, are supported right out of the box.

Entity Catalog

The entity catalog contains all resources discovered by Veza, grouped by entity type (Identity, Data, App, and Infrastructure). Depending on which providers are connected in an ecosystem, its entity catalog could include AWS Accounts, Azure RBAC roles, AWS IAM policies, Okta users/groups, SQL logins, and Snowflake accounts, as well as other data resources and custom applications. Veza’s comprehensive catalog provides the counts and attributes associated with all discovered entities.

Heatmaps

Heatmaps provide a powerful visual representation of how privileges are distributed across applications and data, enabling organization teams to quickly identify users with excessive privilege, the most-accessible data stores, and other important visualizations.

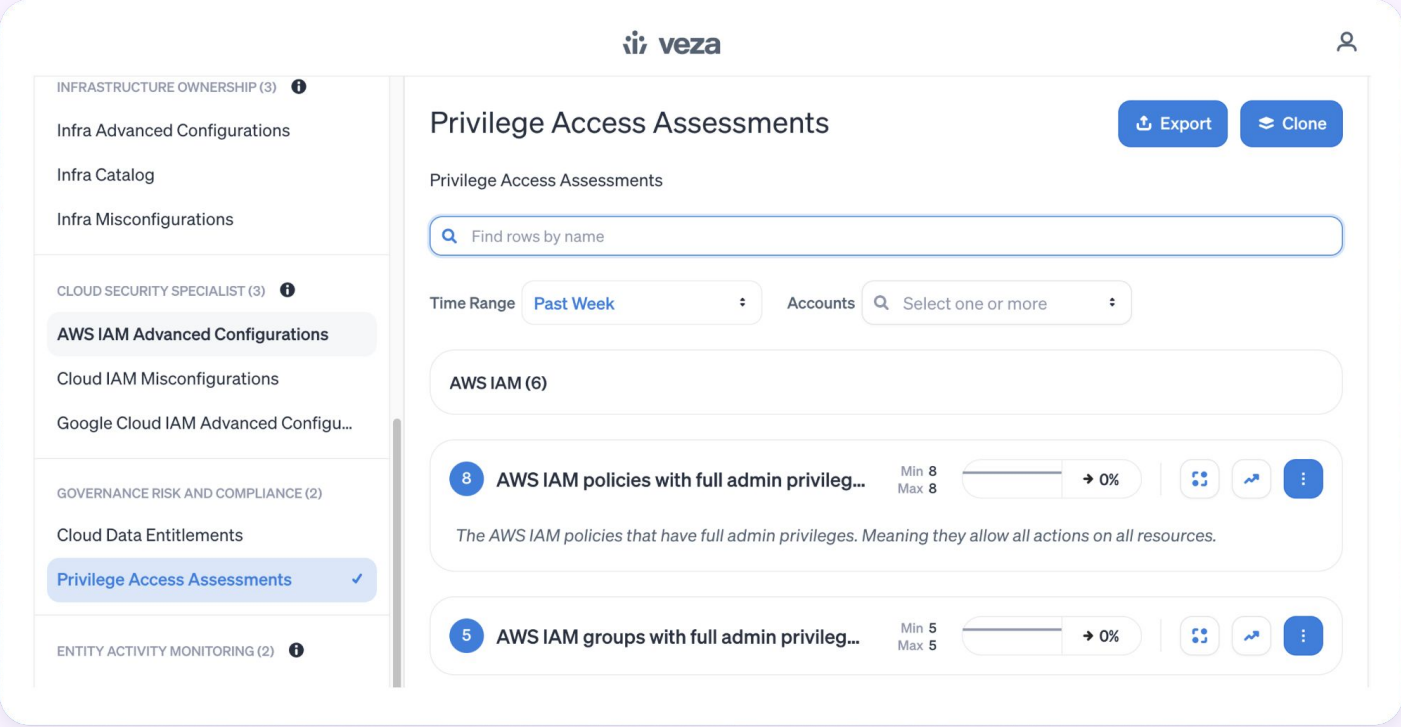


Veza customers can easily generate a heatmap of any selected principal or resource type to visualize how many IAM roles or policies are associated with each entity of that type. Operators can customize thresholds to modify how results are displayed, and can pivot the results to the Authorization Graph for further investigation.

Insights

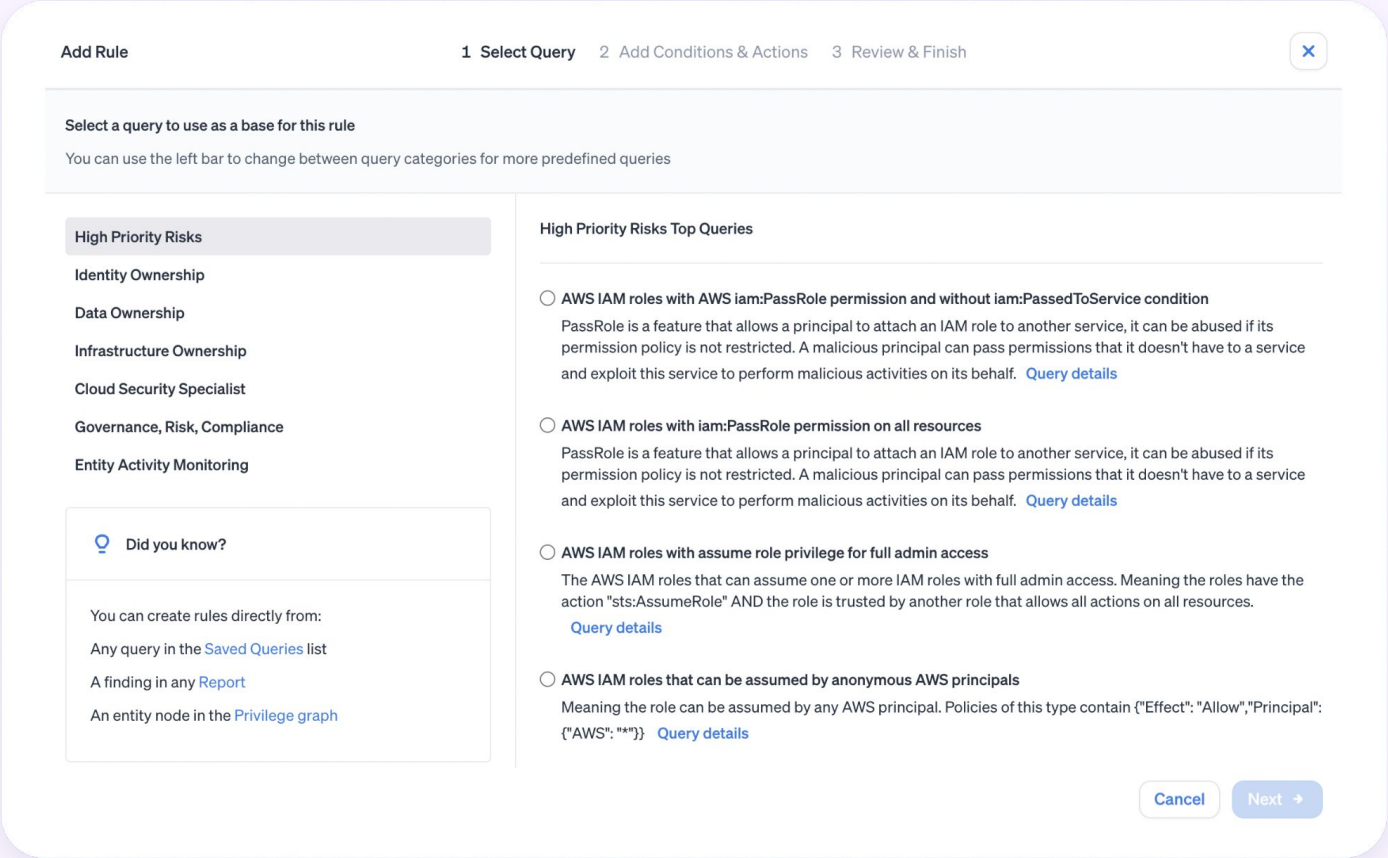
Insights are an array of out-of-box assessments that provide comprehensive and actionable intelligence across critical data authorization areas. Over 500+ built-in queries track common data access vulnerabilities, identify compliance violations like users with excessive privileges, perform analysis of groups and roles, and collect metrics from data sources.

These insights can be consolidated in reports focused on specific data security risks, for example grouped into categories based on the report's audience or based on common areas of interest like IAM misconfigurations, dormant entities, or over-privileged identities. Users can also create custom reports by grouping out-of-box or custom queries.



Rules

Rules are a mechanism within the Veza platform that allows customers to define actionable steps that should be taken as a result of native observations like assessments, insights, and violations. This allows users to configure very specific definitions of conditions, severity levels, and notification endpoints (Slack, JIRA, etc.) and tailor their responses to observed conditions. Rules can be created to look for changes in the results of any pre-existing or custom queries; when such changes are detected, notifications can appear in Veza's navigation sidebar or optionally pushed to downstream enterprise apps using webhooks.

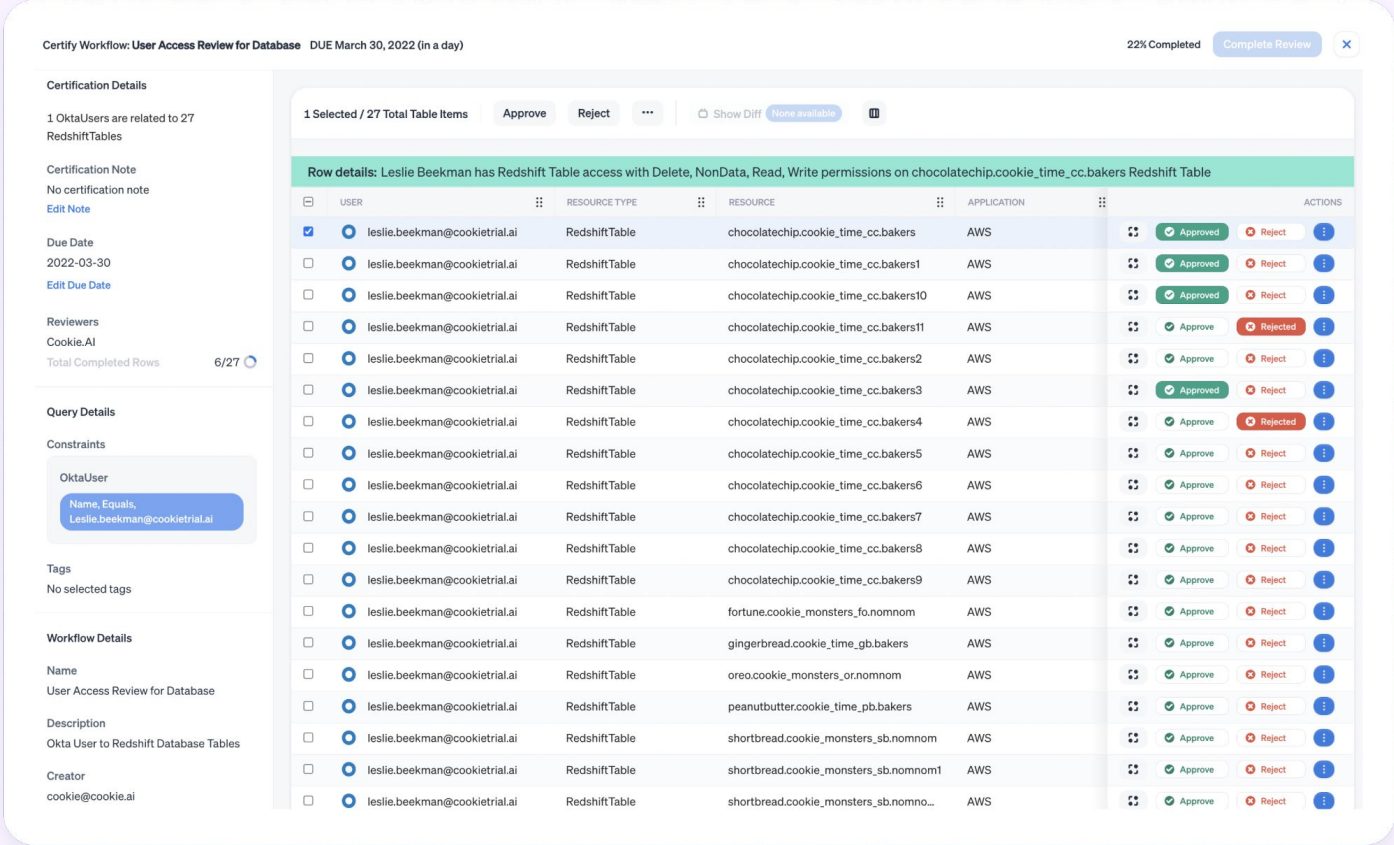


Webhooks

Webhooks notify downstream services, via an HTTP post, when an authorization change occurs or when reviews for user access and/or data entitlements happen. Once a webhook is configured, you can use it to enable a wide range of automated processes, such as updating an issue tracker in Jira, creating a service desk ticket through ServiceNow, or sending a Slack alert.

Workflows

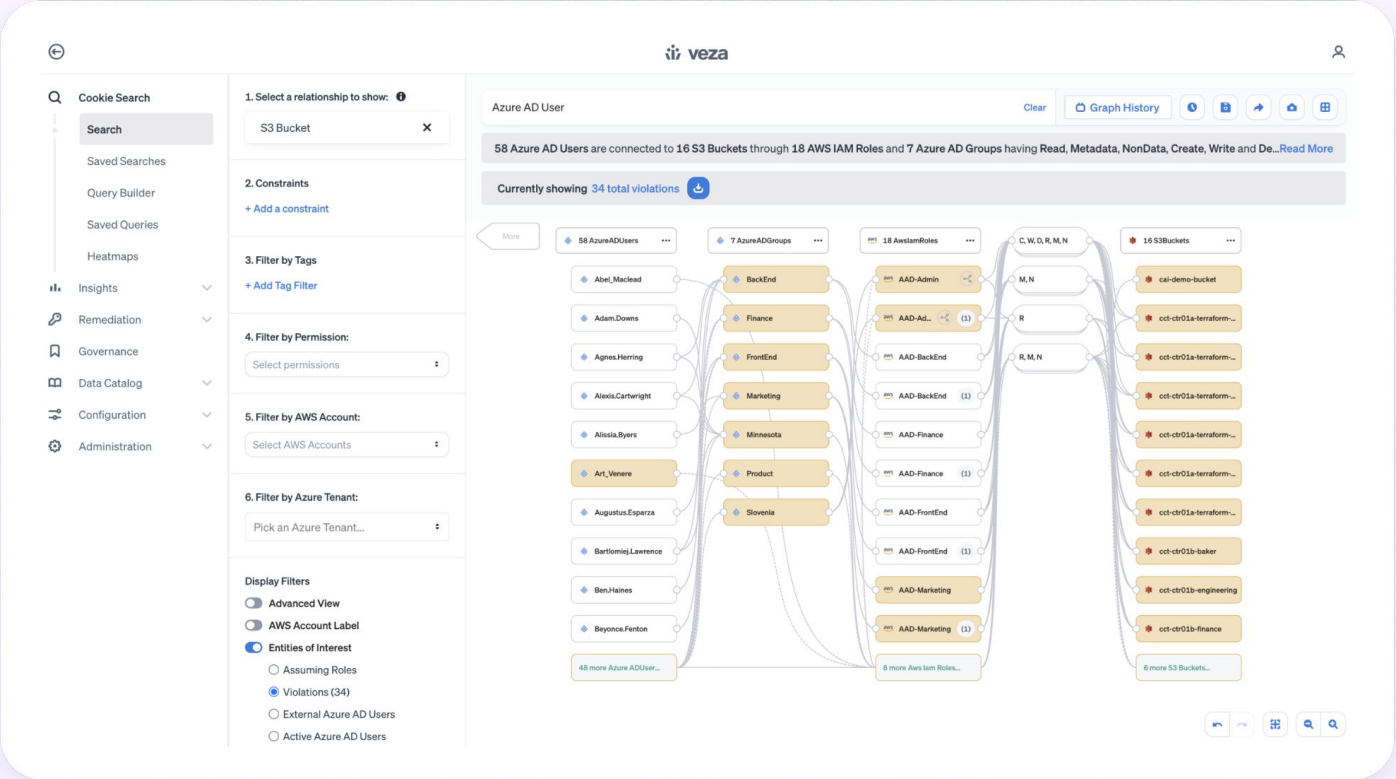
Veza's platform allows customers to create certification workflows for user access and entitlement reviews. Your teams can see account type (human, service principal, service account), resource type, effective permissions, and resource name organized in a comprehensive authorization framework designed for ease of use by operators, auditors, compliance officers, and GRC teams. Reviewers can manage actions on each resource, like approving, rejecting, making a note, and sending notifications to other enterprise apps. And they can integrate business systems like ServiceNow and Slack, via native webhooks, to further automate access and entitlement approvals and rejections. For example, users can create a service desk ticket in ServiceNow when an access review results in rejection.



Using Workflows, Veza administrators can create new access (identity-oriented) or entitlement (resource-oriented) reviews and assign them to the appropriate manager or resource owner, setting a due date for completion. A reviewer can view any changes in permissions since the last certification event, for efficient prioritization, and can approve or reject each identity-to-data privilege relationship using the certification interface. Once completed, the certification becomes a permanent record and can be used as evidence of compliance.

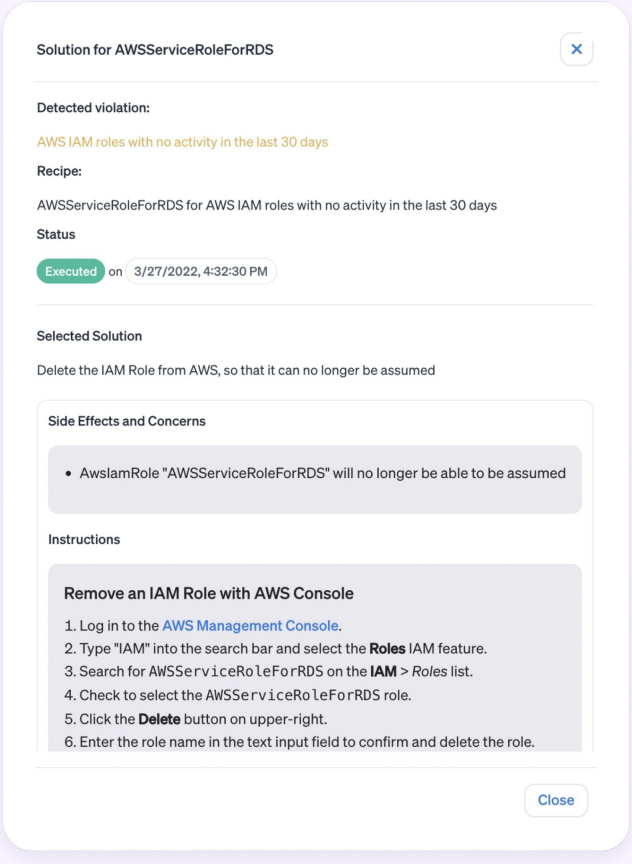
Violations

Veza continuously scans effective permissions, using saved queries categorized as violations, to find deviations from industry best practices and providing quick visibility into data security access misconfigurations and anomalies. If a query is categorized as a violation, the offending authorization relationships and entities are highlighted in reports, the Authorization Graph, and in the Violations panel. Veza administrators can define violations using custom queries or by marking a pre-built assessment as a violation, allowing for customizable monitoring and flagging.



Recipes

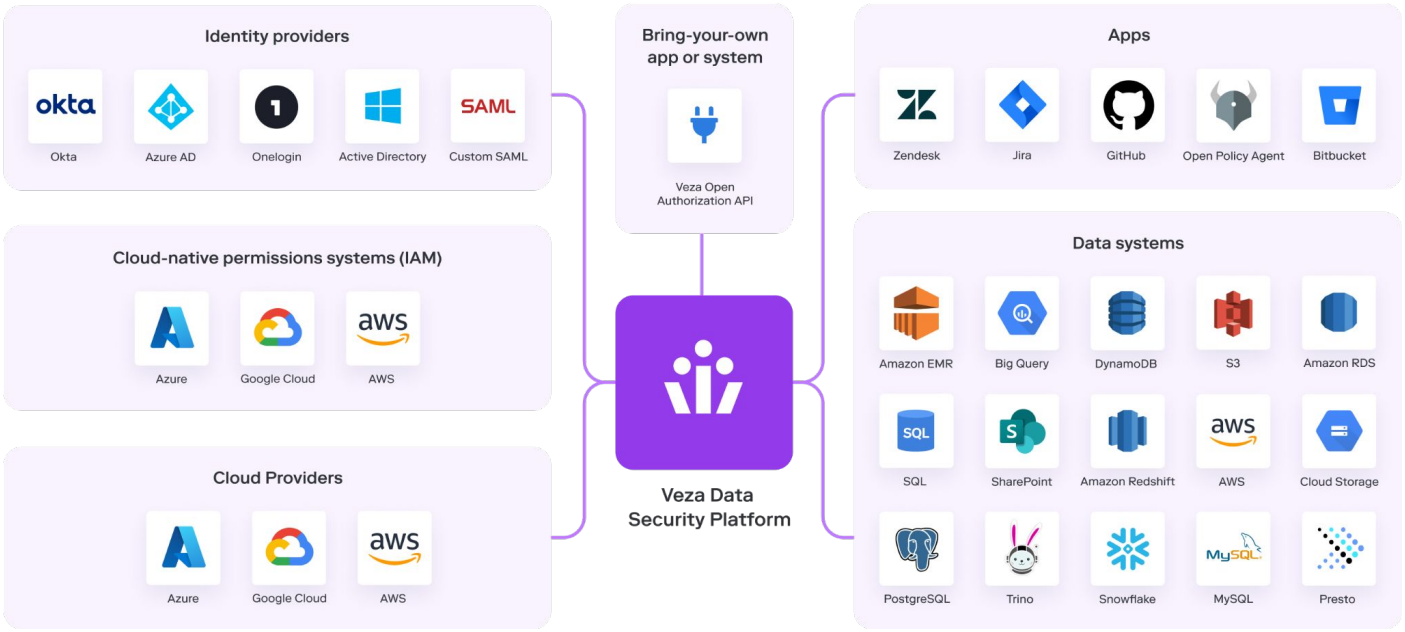
A recipe is a collection of remediation actions that Veza users can run to maintain policy compliance and fix violations that breach data authorization best practices. Recipes also provide details about the side effects of proposed solutions, and can help determine what would constitute a successful change.



Integrations: Apps, Data, Cloud Services

Veza Integrations

Veza provides out-of-box integrations with a wide range of leading identity providers, Cloud IAM solutions, apps, and data systems, extending deep insights into authorization across each customer's entire connected enterprise.



Identity providers insights

- Identify and visualize all nested users and groups
- Locate service accounts
- Discover roles and associated permission sets

Data systems insights

- Automatically discover system-specific authorization metadata
- Parse and collect high cardinality and granular data sets: tables, columns, folders, etc
- Visualize and map relationships from identity entities through authorization (roles/policies) to granular data entities (tables/columns)

Cloud-native permissions systems (Cloud IAM) insights

- Understand hierarchical layers of IAM controls (users, policies, roles) that enable access to cloud data resources
- Understand federated authorization from identity providers to Cloud IAM entities, cloud services and cloud resources

Cloud providers insights

- Enjoy convenient out-of-box configuration with all cloud service providers
- Quickly build an authorization entity network through Veza auto-discovery
- Leverage tags for resource classification, including tagging sensitive resources

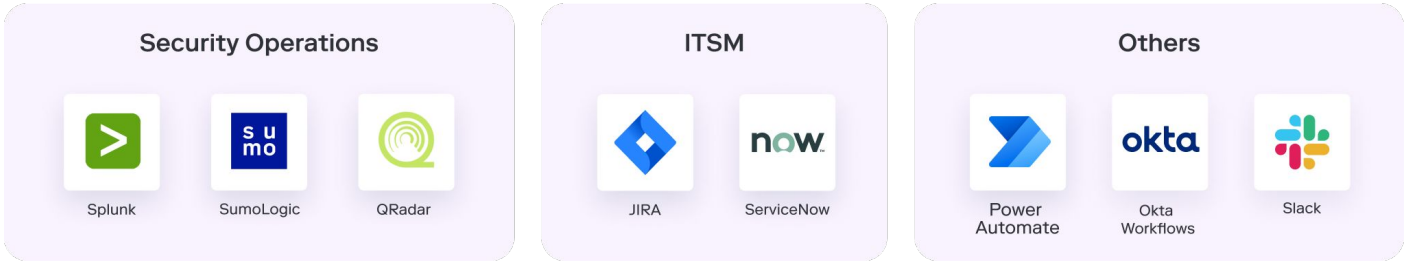
Apps insights

- Discover application-specific authorization structures (roles/groups/permissions)
- Visualize relationships from identity to application-specific actions and permissions
- Include your own apps and systems via our Open Authorization API

Outbound Integrations

Orchestrate and automate your response to data security risks

Integrate with your existing enterprise apps, so your data, IT, IAM, and security teams can operationalize insights into well-defined business processes and workflows.



Security Operations and Analytics

Enhance visibility and response to data risks through detailed authorization information, events, alerts, and comprehensive reports.

ITSM

Improve data and application entitlements management, and automate certification events like access approval or rejection.

Other apps

Simplify business processes tied to audit and compliance activities, like automating the creation of an access workflow when a role or department change is detected, and notifying a manager via Slack whenever a new entitlement review begins.

Check out our integrations page for more information!

Integrations

Product Security: Trust and Compliance

Our security values, laser-focused on building trust, inform everything we do.

Establish trustworthiness

We design all our business, development, and operational processes to maintain the confidentiality, integrity, and availability of our customers' data.

Demonstrate trustworthiness

We stand ready to explain and demonstrate the safeguards we've implemented and meet customers' security obligations to their customers.

Deepen trustworthiness

Because technology, regulations, and business change quickly, we continually adapt and improve our safeguards to ensure the data our customers entrust to us is always protected.

Veza is both SOC 2 Type I and SOC 2 Type II compliant, demonstrating our dedication to security and compliance across all our processes, people, and technology. SOC 2 Type II is a milestone, but we continuously invest in security and compliance over time. Our next security and compliance milestone is ISO 27001.

Veza: The Authorization Standard

Our product helps each customer understand, manage, and control data access, and is delivered in two acts.

In Act 1, we focus on building visibility: strengthening search and discovering the reality of authorization so customers can answer the critical question "who has access to what?" This foundational step creates the data structures of the Authorization Metadata Graph upon which the entire product suite will be built.

In Act 2, we empower customers to compare their actual state with the ideal state, so we can work together to correct issues in an incremental and actionable way that improves data security, adheres to best practices, and reduces risk. And we continually launch new product offerings to provide functionality for new user groups and new use cases like for Security Operations, DevOps, and distributed Data Owners.

We have built a comprehensive authorization mapping system, and tested and refined it in the crucible of real-world customer environments. And we can leverage this proven model for your organization. Our end goal is to enable each customer to truly define and control authorization across their enterprise, and as Veza demonstrates its accuracy, effectiveness, and trustworthiness in your resource environments, you'll quickly understand the value of having an authorization standard and powerful data access controls at your fingertips.

Conclusion

We live in an exciting era, where technology is advancing at a blistering pace, and our ability to find and use data to solve the world's most challenging problems has never been greater. However, this new opportunity comes with new risks, including cybercriminals and rogue nation-states actively working to exploit any security weaknesses so they can wrest control of your data for profit. Even the most optimistic experts within the security community predict that, for any given enterprise, a security breach is a question of "not if, but when."

Those who have said "With great power, comes great responsibility" have never been more correct.

Authorization is not a new problem. But the rapid shift to the cloud, and the explosion of new data and app systems that allow us to take full advantage of cloud efficiencies, can leave organizations exposed. Sadly, the systems that kept our data stores safe on premise can't be trusted to safeguard our new cloud reality, and neither can our cloud service providers. Today, arming your enterprise to safely leverage its data assets means enabling the right teams, automated systems, and people with only the permissions they need, to minimize a potential attack's blast radius.

Organizations need new tools so they can freely leverage their data without putting the enterprise at risk. Veza's comprehensive permissions mapping, powerful visualizations, and deep tech-stack integration can get you there quickly. Begin your journey to trust with confidence.

To learn more about how Veza fits into your data security initiatives, visit us at www.veza.com.

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, Bain Capital, Ballistic Ventures, Google Ventures, Norwest Venture Partners, and True Ventures. To learn more, please visit us at veza.com.