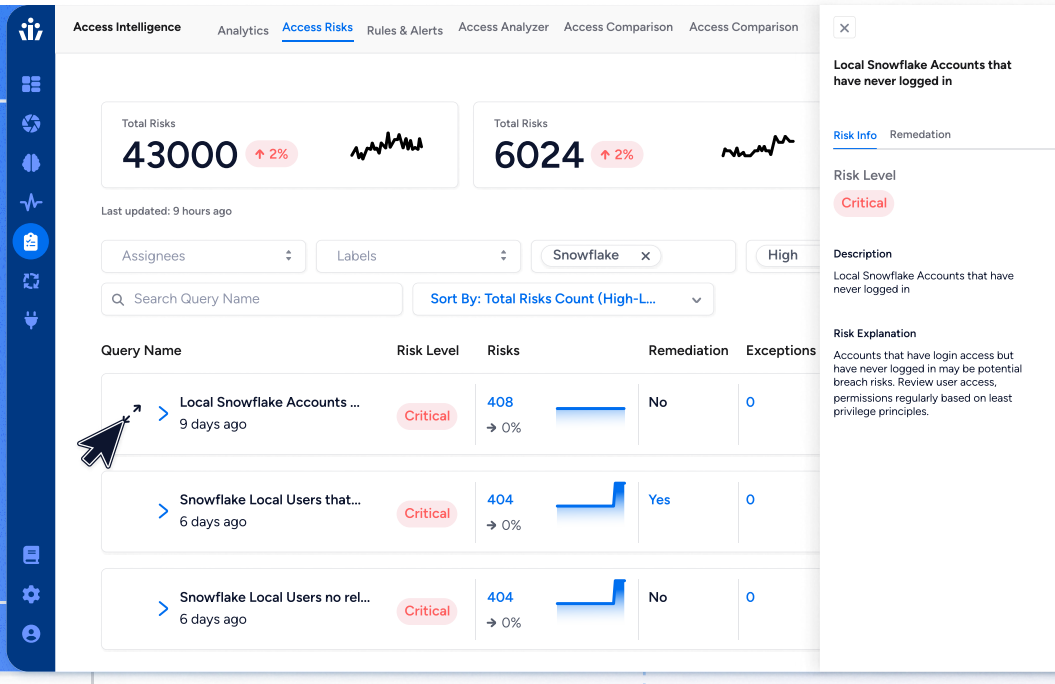
Access Intelligence

Detect privileged users, dormant permissions, policy violations, and misconfigurations with Veza's 2,000+ pre-built queries. Veza shows you where to focus for maximum impact and automates remediation to resolve issues efficiently at scale.



Key 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 models of systems like AWS IAM, Snowflake, and Salesforce.

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 excess access. Use Veza to delegate access decisions to business managers who best understand specific systems.

Key Features

Risks

Continuously scan permissions to identify deviations from best practices, security misconfigurations, and other anomalies. Veza recommends specific actions to resolve identified risks.

Alert Rules

Define automated actions based on the results of custom queries. Initiate alerts and remediation leveraging your ITSM tools such as Slack, Jira, ServiceNow, and more.

Access Monitoring

CIEM monitoring to determine whether identities actually use the access they have to key data resources like Snowflake tables and AWS IAM.

Separation of Duties (SoD)

Monitor access within and across systems to surface identities with potential SoD violations.

Automated Dashboards

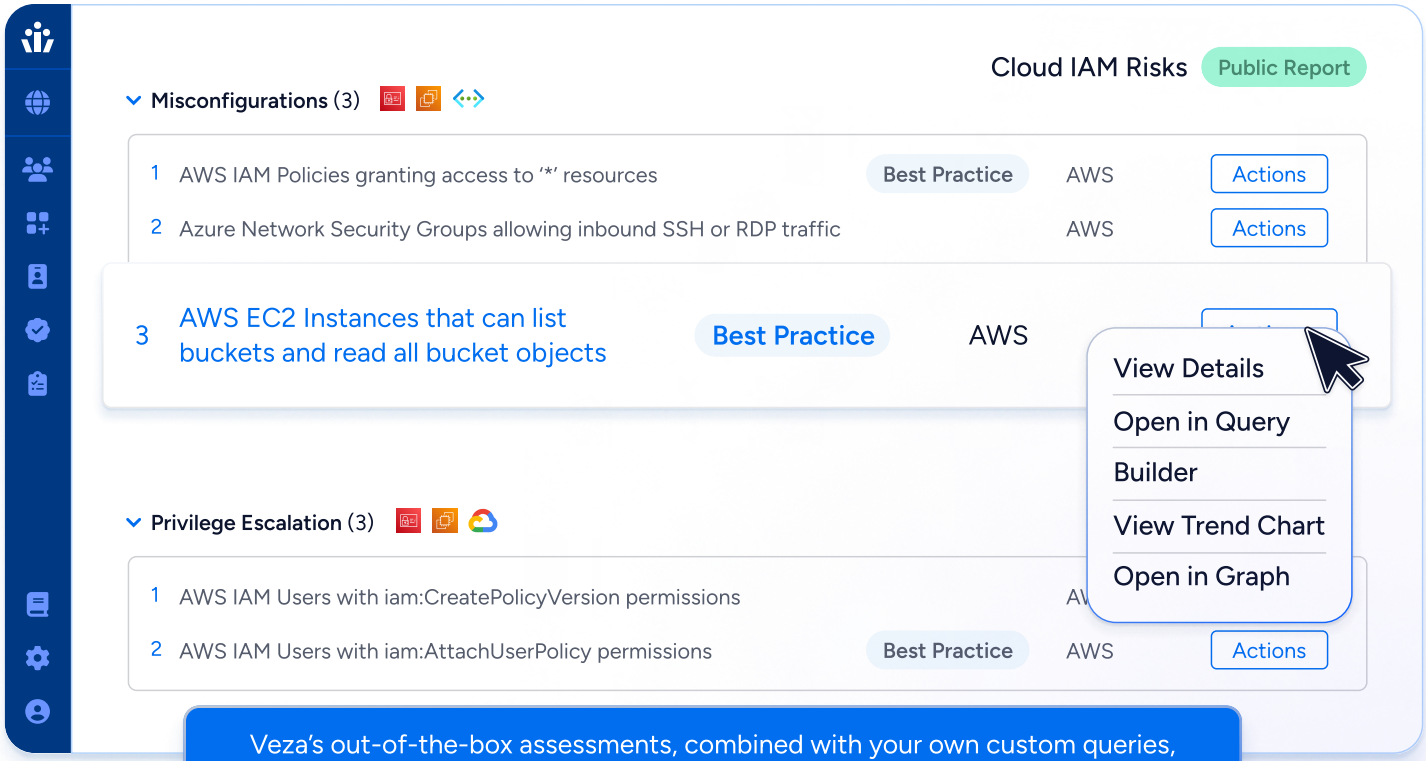
Real-time insights into identity security use cases, such as Identity Security Posture Management (ISPM), Identity Threat Detection and Response (ITDR), and SaaS Security Posture Management (SSPM).

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

Built on the Veza Access Platform

Veza is the identity security company that powers Intelligent Access. The platform enables companies to monitor privilege, investigate identity threats, automate access reviews, and bring access governance to enterprise resources like SaaS apps, data systems, cloud services, infrastructure services, and custom apps.

Legacy Solution Challenge	Veza Solution
Security teams lack system-specific understanding of dozens of complex access models (RBAC, ABAC, etc).	Veza provides out-of-the-box insights to surface risks like misconfiguration, excess privilege, and dormant unusued access.
Periodic audits ignore emerging risks until the next audit occurs.	Veza enables continuous monitoring for policy violations to reduce risks before they become audit issues.
Audits require manual assembly of reports from multiple tools.	Veza ingests and organizes data from all of your enterprise systems for automated monitoring and alerts.
Decision-makers rely on guesswork or self-reporting to determine whether access is genuinely needed.	Veza tracks usage activity on sensitive resources, like Snowflake tables, to identify unneeded access that can be removed.
Business users must learn each system's specific authorization structures to make policy decisions.	Veza translates each system's authorization model into a common language of effective permissions that business users can easily understand.



Veza's out-of-the-box assessments, combined with your own custom queries, deliver up-to-date and actionable intelligence on access risks, identity misconfigurations, and excess privilege across your on-premise systems, cloud infrastructure, and SaaS apps.

Advanced Access Intelligence

Elevate your identity security posture with our Advanced Access Intelligence, designed for users seeking next-level capabilities in managing and securing their identity and access set up. This advanced tier offers:

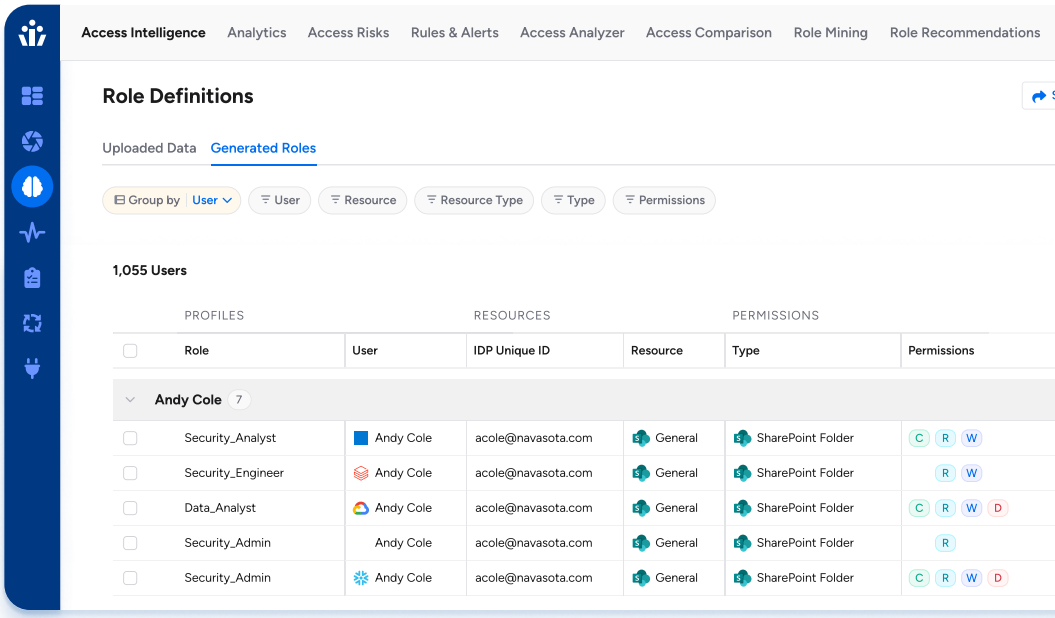
Least Privilege Using Advanced Role Engineering features

1

Use Access Recommendations to optimize user permissions with precision.

2

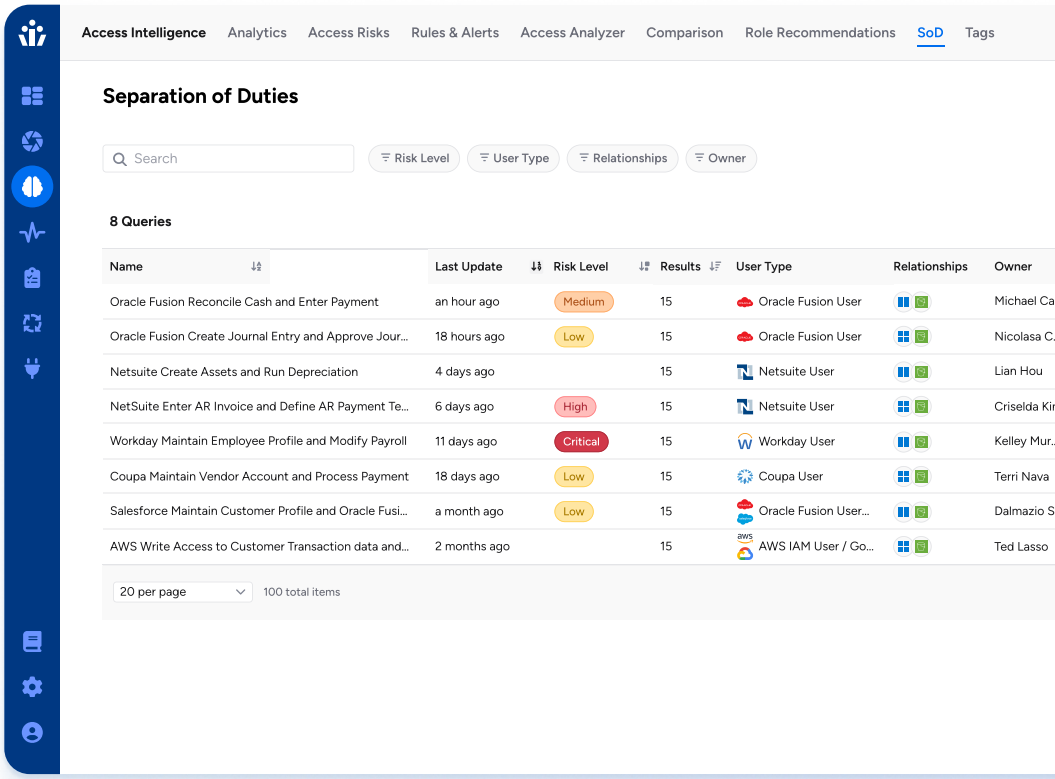
Use Role Mining & Role Definitions to automatically recreate roles from scratch reducing redundancy, and manual overheads.



Actionable Separation of Duties (SoD) Management

Our advanced Separation of Duties (SoD) features not only detect potential violations but also enable detailed auditability and effective remediation, safeguarding against access risks and maintaining a secure posture.

Leverage these advanced, cutting-edge features to harness the full potential of Access Intelligence, driving security and efficiency at scale with delightful experiences.



Extended Feature List

Cloud IAM Analysis for Least Privilege & Misconfigurations

Insights for Cloud IAM, including AWS IAM, Azure RBAC and GCP IAM

Okta Analysis

Insights for Okta entities, including Okta users, groups and roles

Active Directory Analysis

Insights for AzureAD entities, including Active Directory users, groups, service accounts, domains and OUs

Data Misconfiguration Analysis

Misconfigurations for critical data systems and their connections with IdPs

Infrastructure Misconfiguration Analysis

Misconfigurations for infrastructure resources (security groups, VMs, etc)

Snowflake Misconfiguration Analysis

Misconfigurations for the entire Snowflake environment, including identites and data

Github Misconfiguration Analysis

Misconfigurations for the entire Github environment, including identites and data

Salesforce Misconfiguration Analysis

Misconfigurations for the entire Salesforce environment, including identites and data

AWS Misconfiguration Analysis

Misconfigurations for the entire AWS environment, including identites and data

GCP Misconfiguration Analysis

Misconfigurations for the entire GCP environment, including identites and data

Dormant Entity Analysis

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

AWS IAM Advanced Configuration Analysis

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

Privileged Access Dashboard

Insights on privilege access across all systems, for identities, groups, roles and service accounts

Cloud IAM Insights

Insights for Cloud IAM, including AWS IAM, Azure RBAC and GCP IAM

Identity and Privileged Access Insights

Insights for identity and privileged access across all integrations

Data Insights

Insights on data systems across all integrations

Customizable Reports

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

Reports Library

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

Extended Feature List Cont'd

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

User Analysis

Construct user related insights and configure alerts, rules and reports from an english translated, simplified builder

Group Analysis

Construct group related insights and configure alerts, rules and reports from an english translated, simplified builder

Role Analysis

Construct role related insights and configure alerts, rules and reports from an english translated, simplified builder

Separation of Duty

Visibility into compliance controls through upgraded querying capabilities - support AND/OR

User Comparison

Compare access of two identities across all users, groups, roles, resources etc.

Rules 2.0

Create rules on an entity's property changing and create multiple rules for a query

Blast-radius Analysis for Potential Access Remediation

Get a wholistic view of the end-to-end impact of removing access across all systems(IdP, SaaS, Data, etc.)

Access Monitoring for Snowflake

Monitor who is accessing what for Snowflake users to Snowflake tables up to the permissions and access used, with system and effective level granularity

Overprivileged Scores for Snowflake roles / users

Overprivileged Scores for Snowflake roles/users to show the percentage of access actively used to assist with least privilege

Trigger Alerts on Overprivileged Score

Configure rules on Overprivileged Score (OPS) to alert 3rd-party integrations(ServiceNow, Jira, etc) on dormant access

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 Access 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.

© 2025 Veza, Inc. All Rights Reserved | *veza.com*