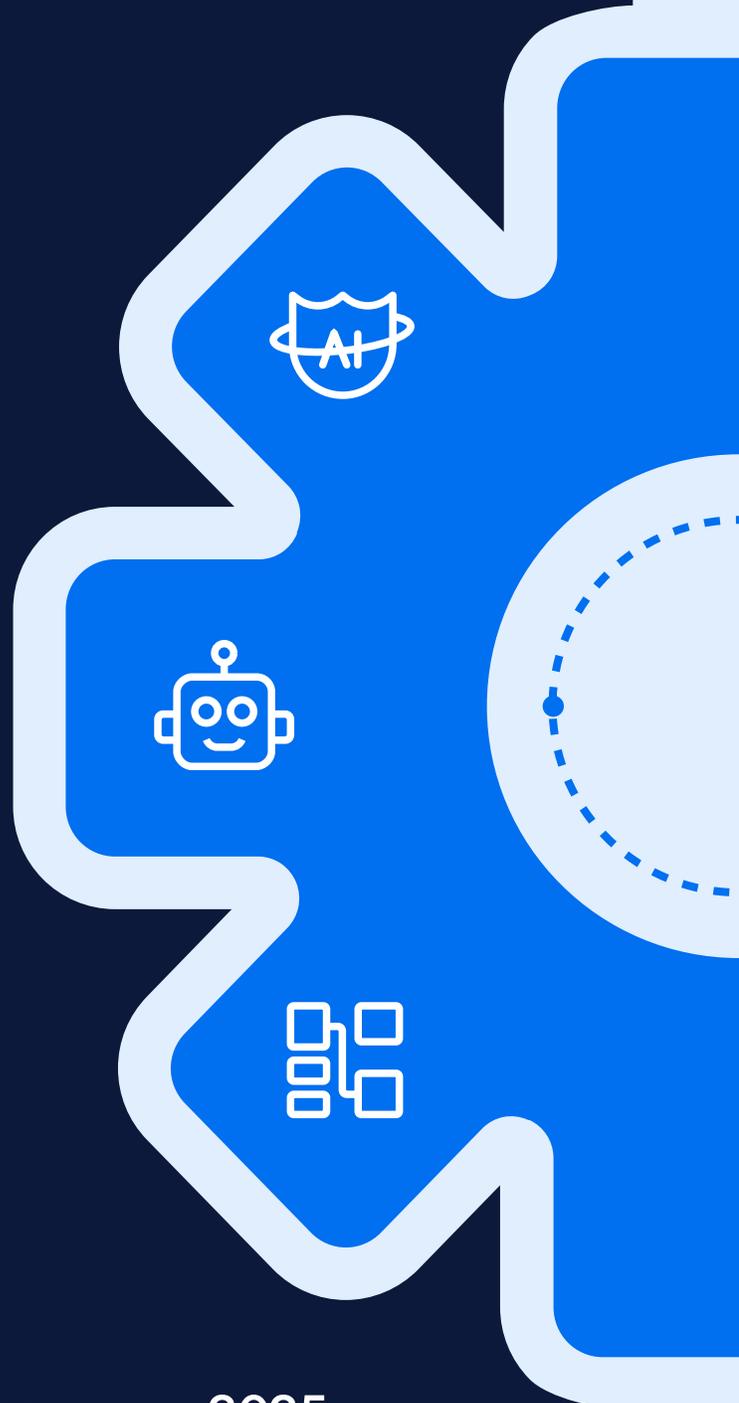




# 10 Veza Capabilities You Might Be Missing



# NHI Discovery & Lifecycle

## Enterprise-Grade Machine Identity Discovery and Governance

Purpose-built to discover, monitor, and govern non-human identities (NHIs) across AWS, Azure, GCP, Salesforce, and more. Includes dashboards for dormant and risky NHIs, credential hygiene insights, Connected App discovery, and owner accountability via bulk assignment and deprovisioning alerts.

The screenshot displays the Veza NHI Security dashboard. The left sidebar contains navigation options: Access Hub, Dashboards, Access Visibility, Access Intelligence, Separation of Duties, Access Monitoring, NHI Security (highlighted), Access Reviews, Lifecycle Management, Integrations, Help, Settings, and Account. The main content area is titled 'NHI Risks' and provides risk insights for NHI entities, Keys and Secrets, and Access Credentials. It features a 'Top Queries With Risks' section with three cards: 377 AWS IAM Access Keys with Full Admin Access (ar 136% | 160), 125 Dormant Access Keys with 'Full Admin' Access (ar 19% | 105), and 112 AWS Secrets Manager secrets not rotated for 90 days (ar 22% | 92). Below this, there are sections for AWS and Azure risks. The AWS section includes: 72 AWS EC2 Instances with Medium Blast Radius (10% - 70%) of... (ar 5% | 160), 12 AWS EC2 Instances with IAM Roles attached that have managed policies (ar 7% | 105), and 18 Non-human AWS IAM Users with last programmatic access before 30 days (ar 18% | 92). The Azure section includes: 103 Azure AD Service Principals (Enterprise Apps) assigned the... (ar 46% | 160) and 81 Azure AD Users with no recent activity but assigned Azure AD (ar 70% | 160). Each card includes a 'tri Critical' indicator and a line graph showing risk trends.

01

# Access Intelligence

## High Fidelity Insights, Meet Veza Actions

New dashboards (with key risk indicators as KRIs) for privileged access, service accounts, and identity insights. All dashboards now support built-in actionability - launch reviews, rules, and alerts directly from tiles. Risk explanations and mitigations are more prominent, with improved export, layout, and traceability.

The screenshot displays the 'AWS Activity Report' dashboard. At the top, there are navigation links for Home, Favorites, Dashboards, and Reports. The dashboard title is 'AWS Activity Report' with a subtitle: 'Gathering insights for Access Keys, User Activity, Secrets Manager, Dormant Resources, and key high risk activities.' Below the title, it shows 'Made by Veza', 'Last modified by John Ferrigan on January 31, 2025', 'Public', and 'Last synced 15 minutes ago'. There are filters for 'Last 30 Days', 'Integrations', 'Risks', 'Labels', 'Hide Empty Queries', and 'Changed Results Only'. The dashboard is titled 'AWS IAM User Insights' and contains five KRI tiles:

- AWS IAM Users with Console Access that have never logged in via Password:** 8 (-11% (9))
- Dormant AWS IAM Users with Console Access:** 17 (-6% (18))
- AWS IAM Users with that have Programmatic Access and are Dormant:** 55 (-5% (58))
- AWS IAM Users with that have Programmatic Access and are Semi-Dormant:** 43 (+23% (35))
- Semi-Dormant AWS IAM Console Access:** 19 (+36% (14))

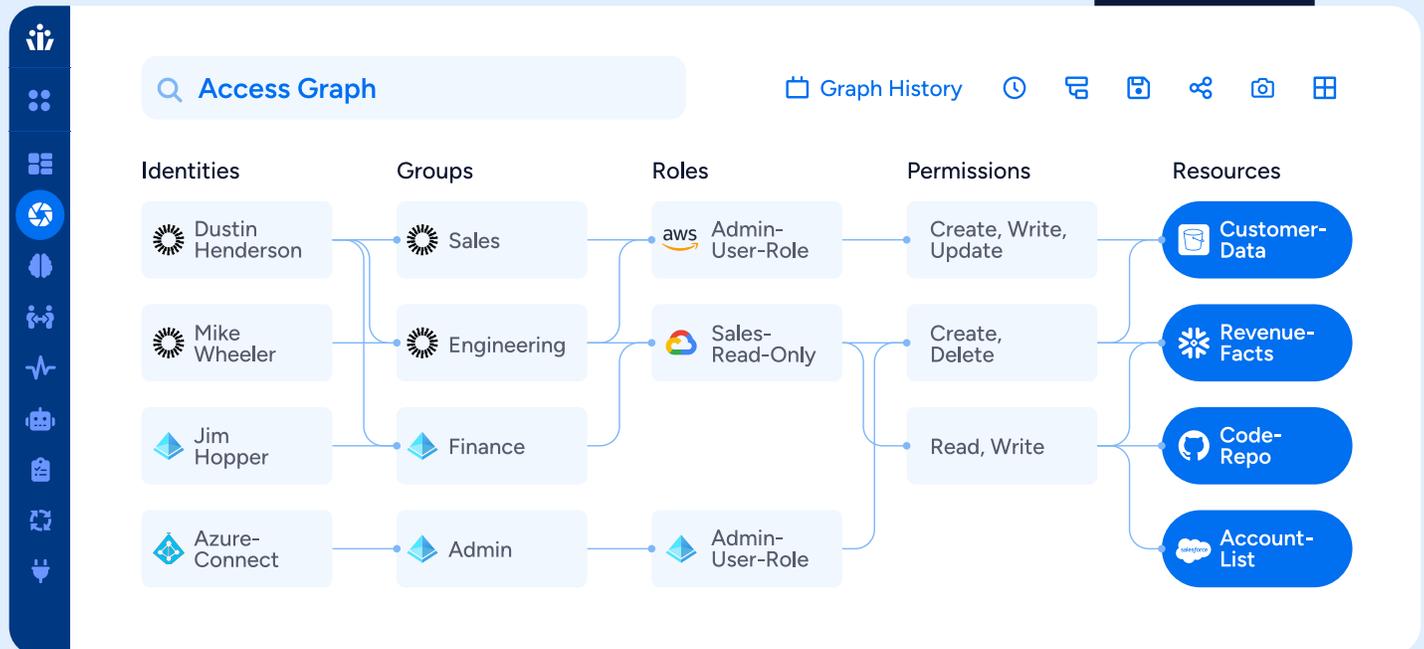
A central menu is open over the 'Dormant AWS IAM Users with Console Access' tile, listing actions: Send Email, Send Slack, Create ServiceNow Incident, Create Jira Issue, Deprovision Entra User, Deprovision Azure User, Orchestrate with Tines, Orchestrate with Torq, Sync with Latest Data, and Open in Graph.

02

# Veza Query Language (VQL)

Precision for Power Users for advanced use cases of Separation of Duties, Threat Hunting, Outlier Detection and more

Unlock the full power of the Access Graph with VQL - purpose-built for identity investigations. Use SQL-like syntax to track access flows across systems and form complex, multi-hop relationship queries in minutes.



## Exclude Specific Paths

Find AWS IAM Users related to S3 Buckets but not through an IAM Group:

```
SHOW AWSIamUser  
RELATED TO S3Bucket  
NOT WITH PATH AwsIamRole;
```

## Filter by Over-Provisioned Score

Retrieve AWS IAM Roles with an over-provisioned score greater than 85:

```
SHOW AWSIamRole  
RELATED TO S3Bucket  
WITH query options  
(over_provisioned_score > 85);
```

03

# Access Hub

## Self Service Access Entitlements Management

Fully redesigned catalog with grid layout, split views (requests vs. approvals), icons and recommended roles, employee access dashboard, manager access dashboard, JIT duration enforcement, full access action history, and support for third-party ITSM fulfillment.

**My Team**

Welcome back, **Gary Ward** [View My Access](#)

Reviews Remaining **103** | Items Remaining **406**

**Due this week**  
No reviews have a due date for this week.

**My Direct Reports**

<b>AB</b> Andrew Bishop Director 10 open reviews	<b>ES</b> Erin Stanley Account Executive 17 open reviews
<b>SW</b> Sharon Wood Marketing Manager 14 open reviews	<b>AW</b> Alex Wilber Recruiting Lead 9 open reviews
<b>AR</b> Adam Richards Vice President 2 open reviews	<b>SF</b> Stephanie Foster Head of Sales, APAC 11 open reviews
<b>LY</b> Lionel Yates lyates@evergreentrucks.com 6 open reviews	<b>KJ</b> Kristine Jenkins kjenkins@evergreentrucks.com 11 open reviews

04

# Separation of Duties (SoD)

## Ownership & Cross-System Coverage

Supports SoD enforcement within and across systems, giving teams unified visibility into risky combinations - no matter where they occur. Assign owners to SoD rules and track updates via "Last Updated By" metadata. Bulk export and improved rule insights included.

The screenshot displays a user interface for managing Separation of Duties (SoD) rules. It features a sidebar with navigation icons, a main content area with query parameters, a line graph, and a table of records. A dropdown menu is open over the graph, showing options like 'Open in Query Builder', 'Schedule Export', 'Alert on Change', 'Create Rule', 'Launch Access Review', and 'Add to Report'.

**Query Parameters**

Time Range: Past 30 days

**5 Records**

Name	Type	Permission Set 1	Permission Set 2	Risk Score	Email	Last Login	Account Created
Harry Potter	WorkdayAccount	Add Salary	Payroll Reconciliation, Bank Reconciliation	100	HPotter@alphax.com	2 Years	2 Years
Tom Riddle	WorkdayAccount	Add Commission	Payroll Reconciliation	77	TRiddle@alphax.com	-	2 Years
Ginny Weasley	WorkdayAccount	Add Salary	Payroll Reconciliation, Bank Reconciliation	80	GWeasley@alphax.com	7 Days	2 Years
wd-support	WorkdayAccount	Add Salary, Add Commission	Bank Reconciliation	70	Support@alphax.com	9 Months	2 Years
wd-tenantowner	WorkdayAccount	Add Commission	Payroll Reconciliation	100	Admin@alphax.com	2 Years	2 Years

05

# Lifecycle Management

## Purpose-Built for Identity Teams

Real-time Lifecycle Dashboard, draft-first policy creation, granular identity overrides, mover grace periods, Microsoft onboarding automation, and secure day-one password-reset workflows.

**Lifecycle Management Overview**  
Manage automatic provisioning and deprovisioning of access throughout the user lifecycle.

**Policies**  
5

- UKG  
UKG-HRIS Employee  
10 Identities  
Running
- Workday Employee Policy  
Workday Worker  
375 Identities  
Running
- Evergreen Trucks HRIS 1  
Evergreen\_HRIS HRIS Employee  
5 Identities  
Running

3 most recently updated policies [View all](#)

**Access Profiles**  
64

**Identities**  
398

**Integrations**  
Total: 15 | Errors: 3 | Recently Created: 2

- GCP-sigmacorp  
Updated 10 months ago  
Partial Error
- Evergreen Trucking  
Updated 21 days ago  
Error
- Azure Veza  
Updated 7 days ago  
Partial Error
- Salesforce veza-4e  
Success

Top 5 integrations, prioritizing errors first. [View all](#)

**Access Requests**  
0

**Get Started**  
Create access requests to provide access to software.

**Errors**

Event Type	Timestamp	Identity	Message
------------	-----------	----------	---------

# Access Reviews

## Streamlined & Configurable for Enterprise Scale

Launch reviews from anywhere: dashboards, queries, SoD rules, or LCM workflows. Auto-expire or auto-reject overdue reviews. Reviewer UI upgrades include grouped views, progress tracking, and stats-rich exports.

The screenshot displays the 'Access Reviews' interface. The main section is titled 'Snowflake Local User to Local Role' and shows a progress bar for '0 of 24 Items Signed-off'. Below this, a table lists 8 total items with columns for USER (Name, User Unique Id, Risk Score) and ROLE (Name, Risk Level). The right-hand side features a 'Details (#2 of 8)' panel for the 'ACCOUNTADMIN' role, showing access to 1 Snowflake Account and 11 Snowflake Databases. At the bottom, there are buttons for 'Approve', 'Reject', and 'Sign Off', along with a keyboard navigation tip.

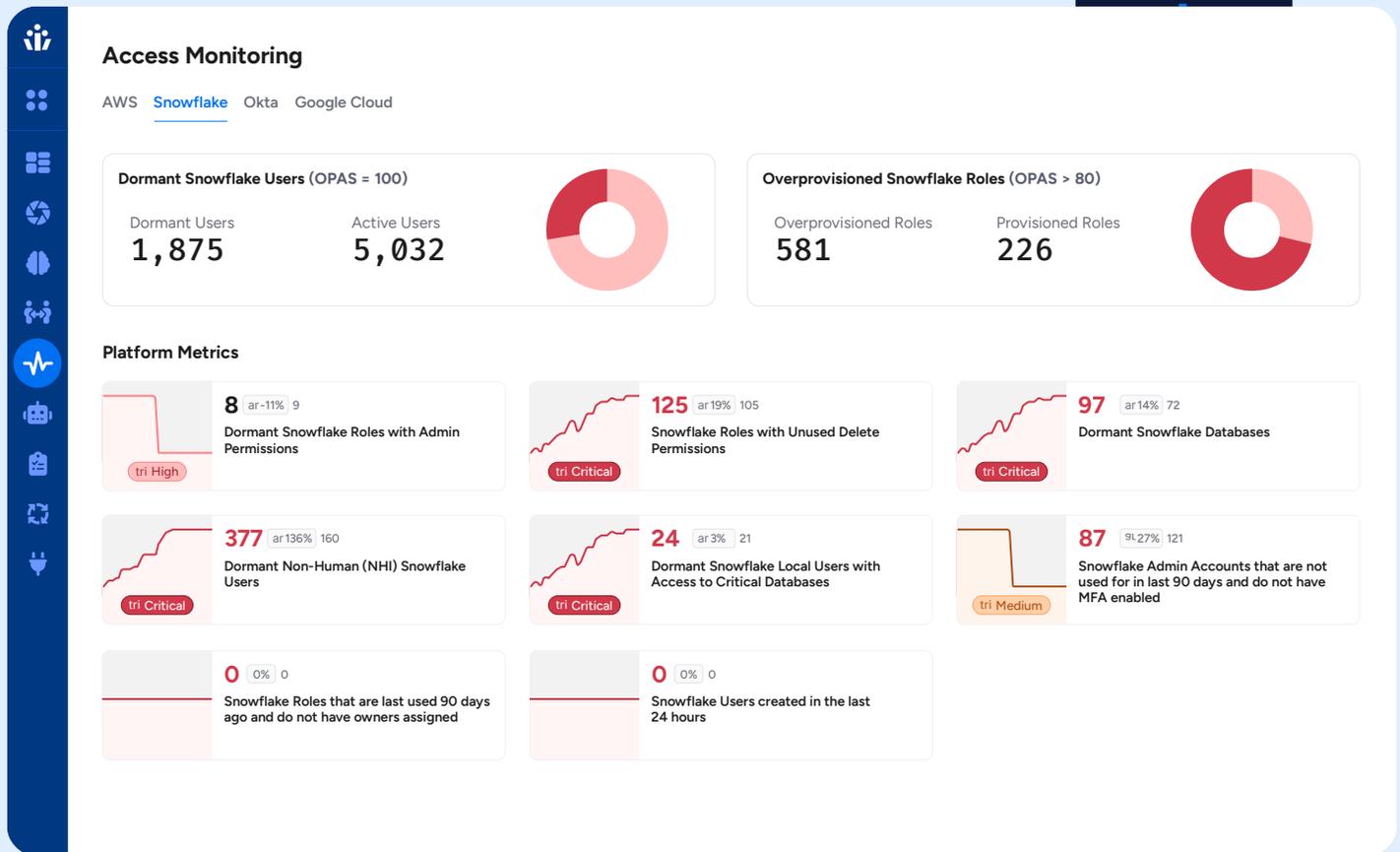
USER			ROLE	
<input type="checkbox"/>	Name	User Unique Id	Name	Risk Level
<input type="checkbox"/>	ANDERS_MEANY	ANDERS_MEANY@SIGM...	SALES_WRITE_DELETE	Low
<input type="checkbox"/>	ANDREW_BISHOP	ANDREW_BISHOP@SIG...	ACCOUNTADMIN	Critical
<input type="checkbox"/>	ANDREW_BISHOP	ANDREW_BISHOP@SIG...	IT	Low
<input type="checkbox"/>	ANDREW_BISHOP	ANDREW_BISHOP@SIG...	OKTA_PROVISIONER	None
<input type="checkbox"/>	ANDREW_BISHOP	ANDREW_BISHOP@SIG...	ORGADMIN	None
<input type="checkbox"/>	ANDREW_BISHOP	ANDREW_BISHOP@SIG...	SALES	Low
<input type="checkbox"/>	ANDREW_BISHOP	ANDREW_BISHOP@SIG...	DATA_SCLUS	Critical
<input type="checkbox"/>	ANDREW_BISHOP	ANDREW_BISHOP@SIG...	FINANCE	Low

07

# Access Monitoring

## Visibility into What's Actually Being Used

Go beyond theoretical access and monitor who's actually using their access to apps, data, and cloud services. New updates include the Over Provisioned Access Score (OPAS) for datasets/tables, "Last Viewed" for KMS keys, and comprehensive activity tracking for IAM users.



# IAM Conditional Access Detection

Surface AWS permissions granted under unsupported conditions, revealing blind spots in IAM policy logic and enforcing cleaner, more secure access paths.

The screenshot displays the Veza AWS IAM Insights dashboard. The left sidebar contains navigation options: Access Hub, Dashboards, Access Visibility, Access Intelligence, Access Monitoring, NHI Security, Access Reviews, Lifecycle Management, Separation of Duties, Integrations, Documentation, Administration, and user information for hnorum@veza.com and Root. The main content area is titled 'AWS IAM Insights' and includes a 'Dashboard Library' header. Below this, there are filters for 'Time Range' (Past 30 Days), 'Hide Empty Queries', 'Changed Results Only', '+ Integrations', '+ Risks', and '+ Labels'. There are also dropdowns for 'Account Groups' and 'Accounts'. The dashboard features four alert cards under 'Top Queries With Risks' and one under 'Privilege Escalation'. Each card shows a percentage of 0% and a count of items, with a 'Critical' status indicator.

Alert Category	Count	Percentage	Status
AWS IAM Roles with AWS iam:PassRole permission...	11	0%	Critical
AWS IAM Roles with iam:PassRole permission o...	13	0%	Critical
AWS IAM Users with AWS iam:PassRole permission...	7	0%	Critical
AWS EC2 Instances with IAM Role attached that...	20	0%	Critical

09

# New & Enhanced Veza Integrations

Added integrations for MongoDB, Kubernetes (EKS), Dropbox, Coupa, Dynamics 365 ERP, Microsoft Teams, SCIM (OAuth2), and more. Plus deeper entitlement metadata discovery, grouped integration types, and per-source key risk dashboards.

