

# Activity Monitoring

Veza monitors activity by identities and roles on key resources to identify over-privileged permissions, right-size roles, and trim unneeded access and entitlements to sensitive resources.



Blackstone

*"When you combine access with Activity Monitoring you start to get into the question of whether an employee really needs the access they were given...Even if they're entitled to that access, having the ability to see that they're not using it enables us to make better decisions about the risks associated with keeping that access."*

Adam Fletcher • Chief Security Officer

## Key Benefits

### Track Activity to achieve Least Privilege

Know what resources users have actually accessed rather than just what they are entitled to access.

### Identify Over-Permissioned Access Risks

Identify and focus on managing your most over-privileged users, roles, and resources.

### Remove Unused Access

Automatically identify and remove unnecessary or dormant access to resources.

### Mitigate Permission Risk

Automatically right-size permissions for users and roles by removing unused permissions.

### Save Cloud Costs

Remove access to resources which are never used.

### Respond Rapidly

Speed up post-incident forensics by identifying what resources an attacker actually accessed.

## Key Features

### Monitor Activity

Collect and summarize log data from Snowflake, AWS IAM, AWS services, and other enterprise systems.

### Over-Privileged Access Score (OPAS)

Synthesize different access operations (e.g. read, delete, update) across any set of resources into a single numeric activity score to help you compare levels of activity for roles and users.

### Access stats

Show if, and exactly how many times, an identity has accessed a resource, and the exact time of the most recent access.

### Access Intelligence

Power rules and alerts with activity scores. For example: automatically create a workflow whenever Veza detects a new over-privileged user.

### Cloud Entitlements Dashboard

New dashboard for Security Engineering and Security Operations teams on most active users, dormant users, dormant roles, and more

# Supported Resources

Following is the list of supported resources for Activity Monitoring. We're adding new resources regularly, so keep checking back.

## Snowflake

DATABASE

TABLE

VIEW

## AWS

AWS S3 BUCKET

AWS KMS KEY

The screenshot displays two query builder panels on the left and their corresponding results on the right. The top panel shows a query for 'AWS IAM user' related to 'S3 Bucket' with an over-provisioned score threshold of 90. The results show 3 AWS IAM users with scores of 91%, 97%, and 93%. The bottom panel shows a query for 'AWS IAM user' related to 'Secrets manager' with an over-provisioned score threshold of 84%. The results show 2 AWS IAM users with scores of 84% and 81%.

**Query builder 1:**

- Query mode: Effective (selected), System
- Entity type: AWS IAM user
- Relates to: S3 Bucket
- Over provisioned score threshold: Operation >=, Threshold 90

**Results 1: 3 AWS IAM users**

| User          | S3 Buckets | Over provisioned score |
|---------------|------------|------------------------|
| aws_acc_admin | 104        | 91%                    |
| cai_admin     | 310        | 97%                    |
| cai_deployer  | 211        | 93%                    |

**Query builder 2:**

- Query mode: Effective (selected), System
- Entity type: AWS IAM user
- Relates to: Secrets manager
- Over provisioned score threshold: Operation >=, Threshold 84

**Results 2: 2 AWS IAM users** Critical

| User          | Secrets manager secrets | Over provisioned score | Full admin | Root  |
|---------------|-------------------------|------------------------|------------|-------|
| aws_acc_admin | 12                      | 84%                    | True       | False |
| cai_admin     | 5                       | 81%                    |            | False |