

# Find and secure all data risks in the cloud without slowing down the business

If you store sensitive data in clouds such as:    

Our DSPM solution will help your security team understand:



Where data resides in your cloud



What type of data it is



Who or what can access the data



What your security posture gaps are



How to remediate issues fast



How to keep the data continuously secure



Easy-to-deploy and is spun up in minutes for actionability on day one

## Key questions asked by customers

### Where is the data?

What assets do we actually have? Are there new data stores to manage? Do we have snapshots, replicas, or backups?

#### How we help

- Discover all your data assets, including: snapshots, replicas, backups, DBs, buckets or blob storage, data warehouses
- All data types (structured, unstructured, native, self managed)
- Alert when new data stores have been created

### What is the data?

Which data is sensitive or critical? Does it contain PII? PHI? PCI? Where is sensitive data located?

#### How we help

- Classify the data (PII, PHI, PCI, secrets, custom data)
- Highlight sensitive data stores
- Provide full visibility into the exact locations of sensitive data (both within your clouds or in what geography)

### Who has access? How is the data being used?

Are there any abnormal user activities? Who is the owner of each data store? Are there new users from new or uncommon regions?

#### How we help

- Full control over who has access to each data store, and how and when data has been used
- Alert on over-privileged users, and get insights about abnormal usage of data
- Through AI-based usage calculations, identify the owner of each data store

### Is the data secure? What are my gaps?

Is our environment aligned with regulatory requirements? What are the top security issues to take care of right now? What is the best way to remediate violations and how complex is that process?

#### How we help

- Alert on violations of policy or best practices, prioritized by severity
- Get aggregated risk of each data store
- Remediate by opening an automatic issue ticket in your preferred system through integration or receive full remediation directions (including step-by-step CLI or console instructions, downtime notes, and remediation complexity estimation)
- Avoid security risks caused by outdated or irrelevant backups. Many times these end up being the source of the next data leak, mostly because they are improperly managed and forgotten about

# How It Works




### Find and classify

- Full picture of your data store inventory, across all your clouds
- Deep dive analysis to identify what data is sensitive and where it resides (both geographically and inside your environment)




### Usage and access

- Full visibility into who or what has permissions to access every sensitive data store, what is actually using that access, and when it has occurred
- Learn who or what can potentially access every sensitive data store
- Deep usage analysis to pinpoint the actual owner of each data store



### Policy engine finds violations and risks


- Translate policy into specific controls and identify violations
- Insight into your current data security posture and ways to improve it
- Alert when environments are not aligned with regulations and best practices
- Find and flag abnormal data security behaviors
- Detect abnormal activity of users, letting you intervene before it's too late



### Remediation


- Integrate into your existing systems (such as JIRA, Zendesk, Slack, etc.), to manage and shorten workflow
- Step-by-step remediation instructions to simplify the process
- Indication mechanism to ensure issues were actually addressed

## Complete Data Protection




### Data Flow

Know all usage and access of your sensitive data. Eureka then directs you to which data stores should have more restricted access



### Data Loss Prevention (DLP)

Ensure security concerns are being addressed and user activity is continuously monitored




### Detection & Remediation


Detect abnormal user activity, letting you intervene before it's too late

## Cloud Coverage and Integrations


### AWS




### Azure




### Snowflake



### Google Cloud



### Integrations



### Secure Your Cloud's Most Valuable Asset: Data

See how Eureka Security will find and address risks in minutes, no matter where data resides, and how it's deployed in your cloud

[Talk to Us](#)

