eureka

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

eureka.security

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- Avoid security risks caused by outdated or irrelevant backups.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

Deploy Eureka with 2 agentless options

01

Full SaaS

- Give Eureka permissions to scan your inventory and receive deep analysis from our SaaS
- Sensitive data will always remain within region & will not be stored by Eureka

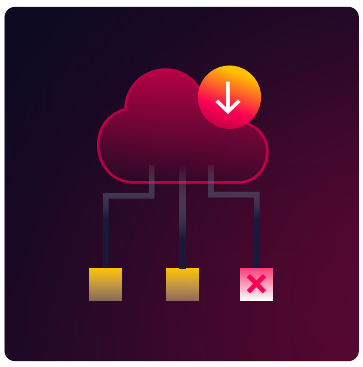
- **Benefits: Minimum effort. Nothing happens inside your environment**

02

Envoy

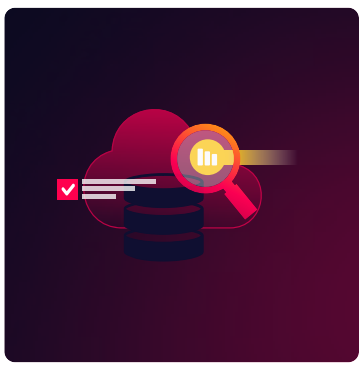
- Give Eureka permissions to deploy and run analysis within your environment
- Upon completion, the rest of the process occurs in our global SaaS

- **Benefits: No data will leave your environment at any step of the process**



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)

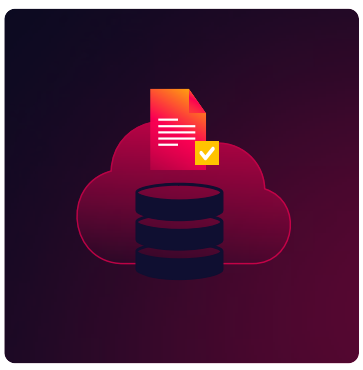


Usage and access

- 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

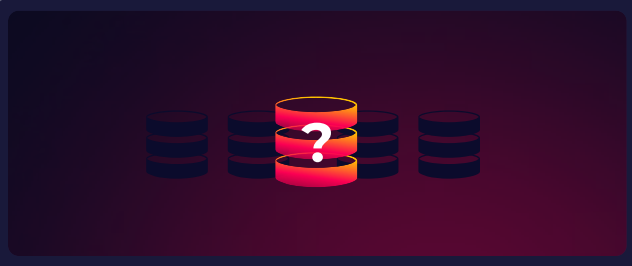
- Integrate into your existing systems (such as JIRA, Zendesk, Slack, etc.), to manage and shorten workflow
- Step-by-step remediation instructions to simply the process
- Indication mechanism to ensure issues were actually addressed

Eureka will remove data security risks by revealing

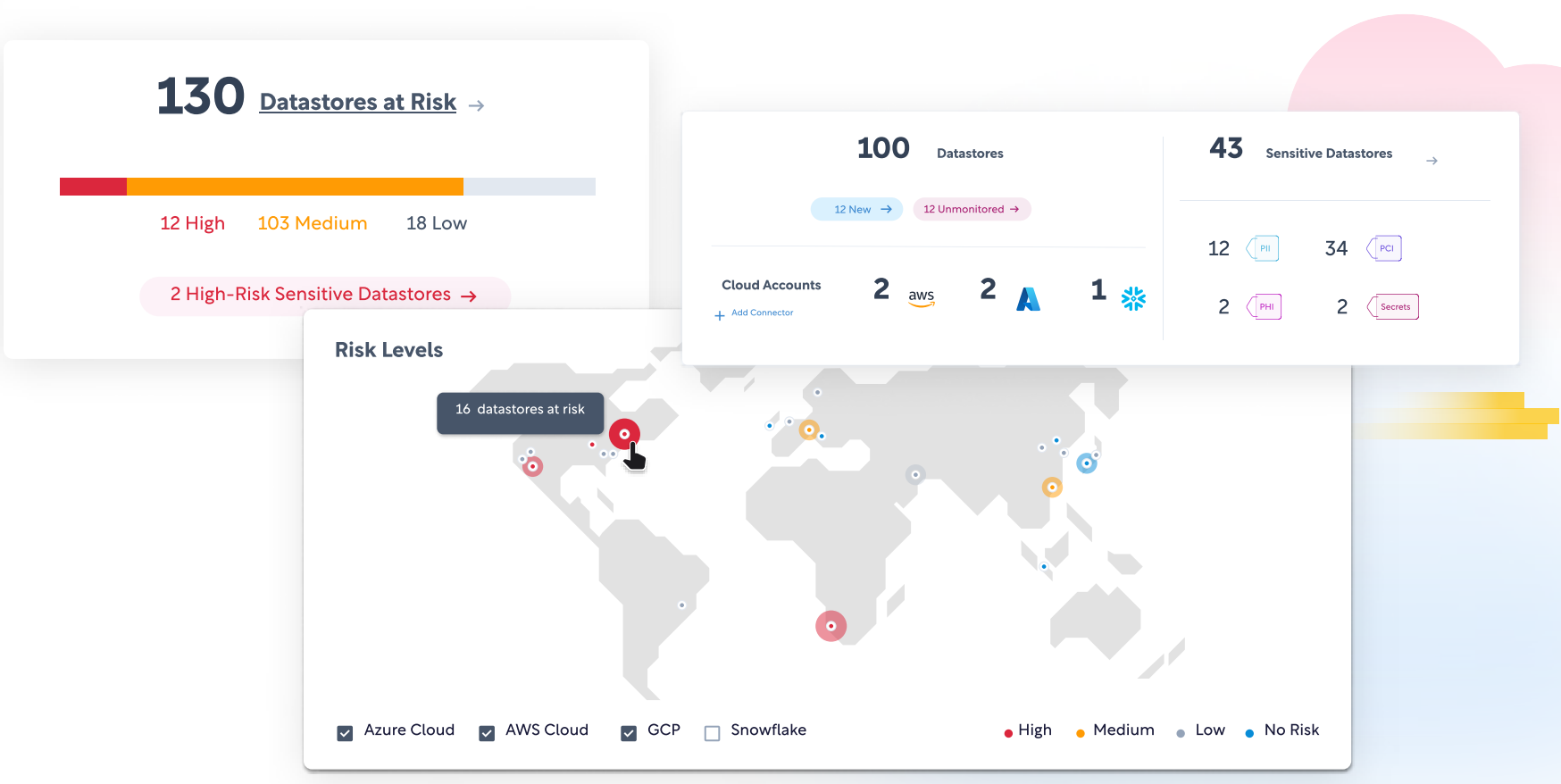
Data store misconfigurations

Misalignment with security compliance

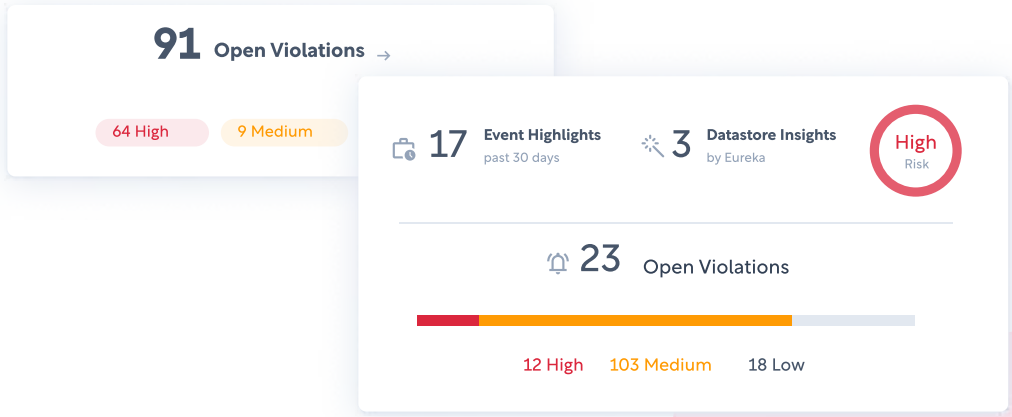
Excessive privileges



Unused or unmanaged “shadow data”



Example use cases



01 You don't have a complete view of all your data stores or can't pinpoint where sensitive data exists

The company stores data inside of hundreds of assets (including multiple CSPs and different types of data stores) and you can't zero in on sensitive data.

How we help - Have full data store visibility and pinpoint the exact locations of your sensitive data within seconds of deployment.

02 You can see the data stores but aren't managing them correctly

Your engineers are using a new data storage technology which the security teams aren't familiar with. Translating the same policies into different controls is challenging and can lead to issues with how data is managed.

How we help - Implement best practices to keep your data stores secure by surfacing violations related to them and putting governance in place.

03 You have data stores that shouldn't exist

Teams often clone data stores. These companies do not have adequate security measures in place or a proper deletion process. This creates a lot of unnecessary data in the form of inactive data stores and orphaned snapshots.

How we help - Track these unnecessary and unmanaged data stores to create the proper security measures or delete them appropriately.

04 You can see the data stores but they should reside somewhere else

Replicas that are created of sensitive data stores and also hosted in a different region as the original are often very difficult to discover, but still cause real compliance issues.

How we help - Eureka will discover these replicas and alert you immediately, giving you concrete remediation instructions.

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

> Eureka's vision for cloud data security – using automation to provide seamless discovery, classification, and integrated processes for all stored organizational data – addresses these issues head on. This will revolutionize the space and significantly help my peers."
>
> **Rob Geurtsen - CISO**

Cloud Coverage and Integrations

AWS

Azure

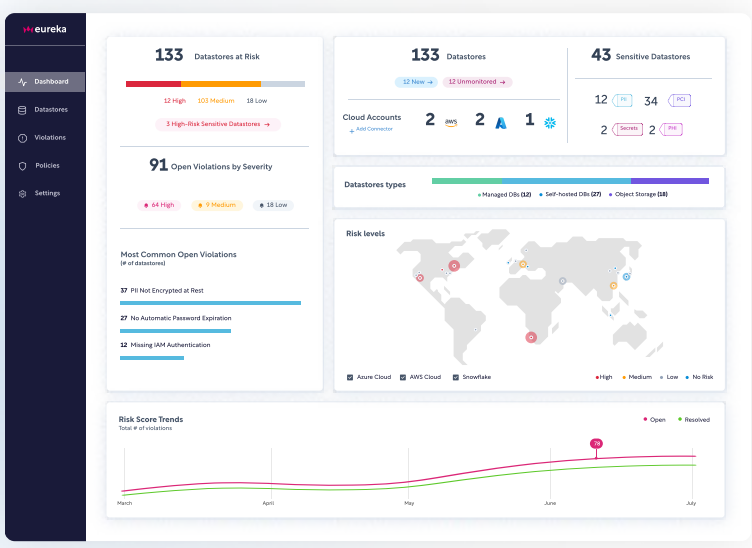
Snowflake

Google Cloud

Integrations

splunk>

Radar



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