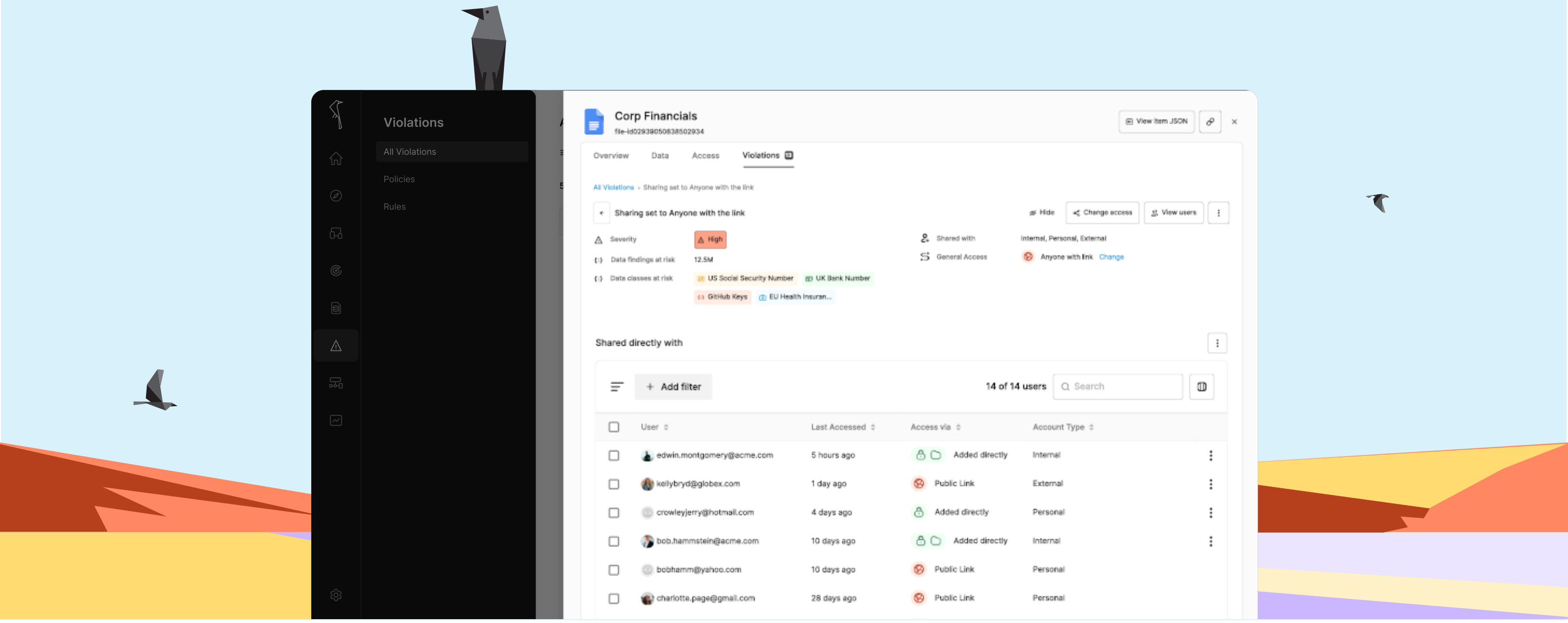
Open Raven

SaaS Data Loss Prevention



Corp Financials
file-id02938050838502934

All Violations › Sharing set to Anyone with the link

Sharing set to Anyone with the link

Severity	High
Data findings at risk	12.5M
Data classes at risk	US Social Security Number UK Bank Number GitHub Keys EU Health Insuran...
Shared with	Internal, Personal, External
General Access	Anyone with link

Shared directly with

14 of 14 users

□	User	Last Accessed	Access via	Account Type
□	edwin.montgomery@acme.com	5 hours ago	Added directly	Internal
□	kellybryd@globex.com	1 day ago	Public Link	External
□	crowleyjerry@hotmail.com	4 days ago	Added directly	Personal
□	bob.hammstein@acme.com	10 days ago	Added directly	Internal
□	bobhamm@yahoo.com	10 days ago	Public Link	Personal
□	charlotte.page@gmail.com	28 days ago	Public Link	Personal

Data visibility, sharing, and aging control, and streamlined offboarding for Google Drive.

An organization’s most sensitive data often lives in SaaS services such as Google Drive, from payroll information and financials to confidential contracts. Protection methods often include little more than authentication and the decision-making abilities of people more concerned about the task at hand than leaking data.

Other essential data risk management tasks, such as offboarding people and partners or conducting retention audits, are too manual and complex— even with the help of Google DLP or a CASB. The SaaS DLP capabilities of the Open Raven Data Security Platform provide clear visibility into sensitive data in Google Drive and beyond while automating policy enforcement.

Benefits

Discover and classify shared sensitive data in Google Drive

Automatically find and classify sensitive files using 300+ default data classes, from personal information to developer secrets. Data and file identification is fully customizable and complete, allowing for creation of new data classes and “group” classes like PII or PHI. Accuracy assured via AI and extensive testing using Mockingbird.

Audit and control access permissions

Google Drive simplifies productivity and collaboration, yet security teams have real challenges enforcing company data governance policies, restricting 3rd party access, and making timely access changes when offboarding employees. With Open Raven, security teams can maintain consistent visibility and conduct periodic audits of access permissions while mitigating data breaches, leaks, compliance lapses, and improper sharing of confidential data.

Eliminate hidden risk from overshared or externally shared files

Sensitive files in Google Drive that are either overshared or shared externally represent significant security and compliance risk, potentially exposing high risk data to unauthorized users. Such exposures can lead to data breaches, privacy violations, and compromise of confidential data. Open Raven quickly identities files with excessive risk and enables automated response actions.

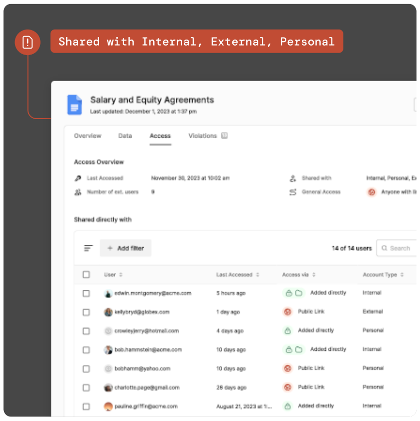
Identify stale sensitive data

Dealing with data sprawl in Google Drive poses a significant challenge for security teams. While imposing file creation restrictions enhances security, it can hamper productivity and teamwork. Files and folders often remain in gDrive long after their usefulness expires or beyond retention requirements resulting in stale data. Open Raven empowers security teams to establish policies detecting stale files containing sensitive data. Access can be restricted or files tagged for removal, effectively curbing risks and lowering expenses.

Use Case

Enforce data security policies for file and folder sharing

Google Drive makes it all too easy to share sensitive data with the wrong party and demands persistent vigilance and end-user training. Enforcing corporate data security policies via scripts doesn't scale or offer enough functionality. Security teams need a modern take on enforcing policies and preventing data loss.



Shared with Internal, External, Personal

Salary and Equity Agreements
Last updated: December 1, 2023 at 1:37 pm

Access Overview

Last Accessed	November 30, 2023 at 10:02 am	Shared with	Internal, Personal, Ex
Number of ext. users	9	General Access	Anyone with li

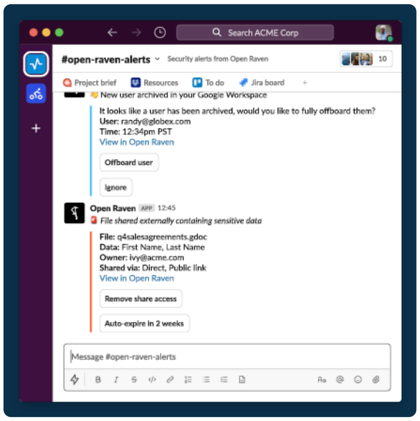
Shared directly with

14 of 14 users

□	User	Last Accessed	Access via	Account Type
□	edwin.montgomery@acme.com	5 hours ago	Added directly	Internal
□	kellybryd@globex.com	1 day ago	Public Link	External
□	crowleyjerry@hotmail.com	4 days ago	Added directly	Personal
□	bob.hammstein@acme.com	10 days ago	Added directly	Internal
□	bobhamm@yahoo.com	10 days ago	Public Link	Personal
□	charlotte.page@gmail.com	28 days ago	Public Link	Personal
□	pauline.griffin@acme.com	August 21, 2023 at 1:...	Added directly	Internal

Visualize sensitive data sharing risk

Google Drive makes it easy for anyone to share files and folders and virtually impossible for security teams to know what sensitive data has already traveled beyond company boundaries. Gain critical visibility into shared sensitive data by combining sensitive data context with user, permission, and domain details.



#open-raven-alerts Security alerts from Open Raven 10

New user archived in your Google Workspace

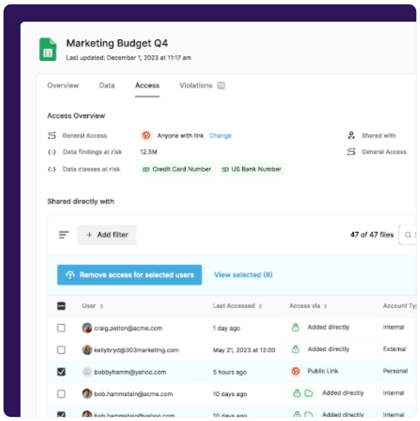
It looks like a user has been archived, would you like to fully offboard them?
User: randy@globex.com
Time: 12:34pm PST
View in Open Raven

Open Raven APP 12:45
File shared externally containing sensitive data

File: q4salesagreements.gdoc
Data: First Name, Last Name
Owner: ivy@acme.com
Shared via: Direct, Public link
View in Open Raven

Easily get back in full control - without tons of work

Security teams need to balance security with productivity. Restrict sensitive sharing too much and productivity drops and users complain. Unrestricted sensitive data sharing increases risk.
With Open Raven, security teams can achieve the right balance by implementing granular domain and user-level restrictions. Authorized business partners and contractors? Allow. Personal email addresses and everything else? Deny.



Marketing Budget Q4
Last updated: December 1, 2023 at 11:17 am

Access Overview

General Access	Anyone with link Change	Shared with	
Data findings at risk	12.5M	General Access	
Data classes at risk	Credit Card Number US Bank Number		

Shared directly with

47 of 47 files

▬	User	Last Accessed	Access via	Account Ty
□	craig.pelton@acme.com	1 day ago	Added directly	Internal
□	kellybryd@303marketing.com	May 21, 2023 at 12:00	Added directly	External
☑	bobbyhamm@yahoo.com	5 hours ago	Public Link	Personal
□	bob.hammstein@acme.com	10 days ago	Added directly	Internal
☑	bob.hammstein@yahoo.com	10 days ago	Added directly	Internal

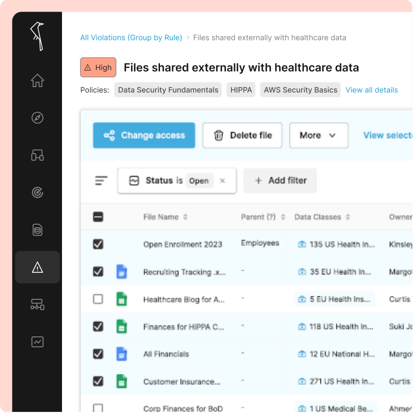
Automatically remediate policy violations

Workflow automations enable taking action across individual or groups of files or at the folder and drive level. Configure automatic notifications for employee file owners. Set sharing expiration dates.

Use Case

Fully offboard people and remove all of their sharing

Merely revoking access and transferring file and folder ownership upon the departure of employees or partners is not sufficient to remediate all data security risks. A thorough offboarding process requires addressing and rectifying the sharing activities of these individuals.


All Violations (Group by Rule) › Files shared externally with healthcare data

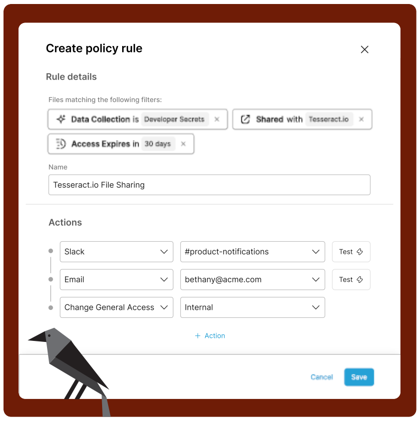
High Files shared externally with healthcare data

Policies: Data Security Fundamentals HIPPA AWS Security Basics View all details

	File Name	Parent (?)	Data Classes	Owner
☑	Open Enrollment 2023	Employees	135 US Health In...	Kinsley
☑	Recruiting Tracking .x...	-	35 EU Health In...	Margo
□	Healthcare Blog for A...	-	5 EU Health Ins...	Curtis
☑	Finances for HIPPA C...	-	118 US Health In...	Suki J
☑	All Financials	-	12 EU National H...	Margo
☑	Customer Insurance...	-	271 US Health In...	Curtis
□	Corp Finances for BoD	-	1 US Medical Be...	Ahmer

Investigate and remediate sharing activity using sensitive data contex

Finding sharing risk in Google Drive using native tools is like finding a needle in a haystack. Open Raven makes it easy by providing the right tools and context. Receive alerts with full context. Search for sharing activity by data classes, domains, and email addresses.


Create policy rule

Rule details

Files matching the following filters:

Data Collection is Developer Secrets

Shared with Tesseract.io

Access Expires in 30 days

Name

Tesseract.io File Sharing

Actions

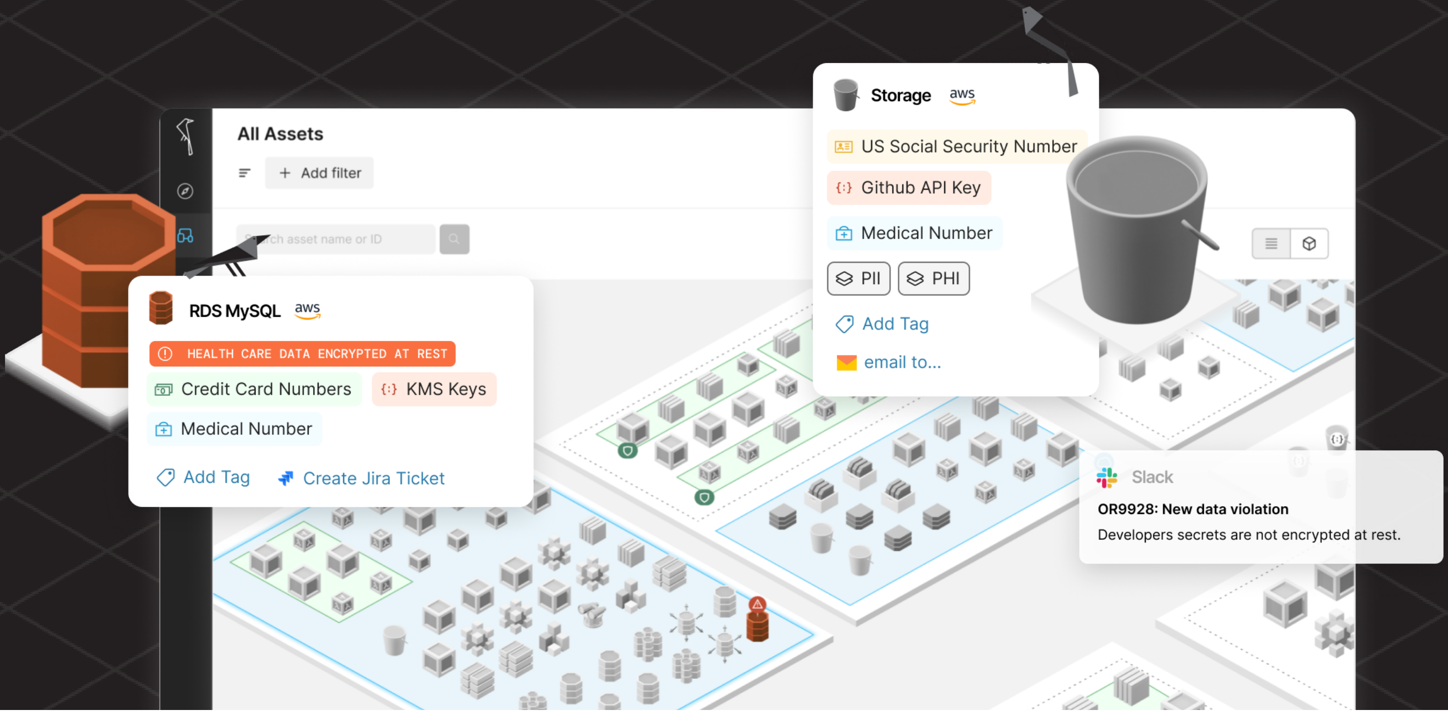
- Slack — #product-notifications — Test
- Email — bethany@acme.com — Test
- Change General Access — Internal

Implement granular sharing controls

Thorough access removal using native tools is often a manual and tedious process. Open Raven streamlines access removal by enabling administrators to take action on multiple files, folders, and drives, swiftly eliminate external access, restrict sharing to specific domains, and set expiration dates for sharing permissions.

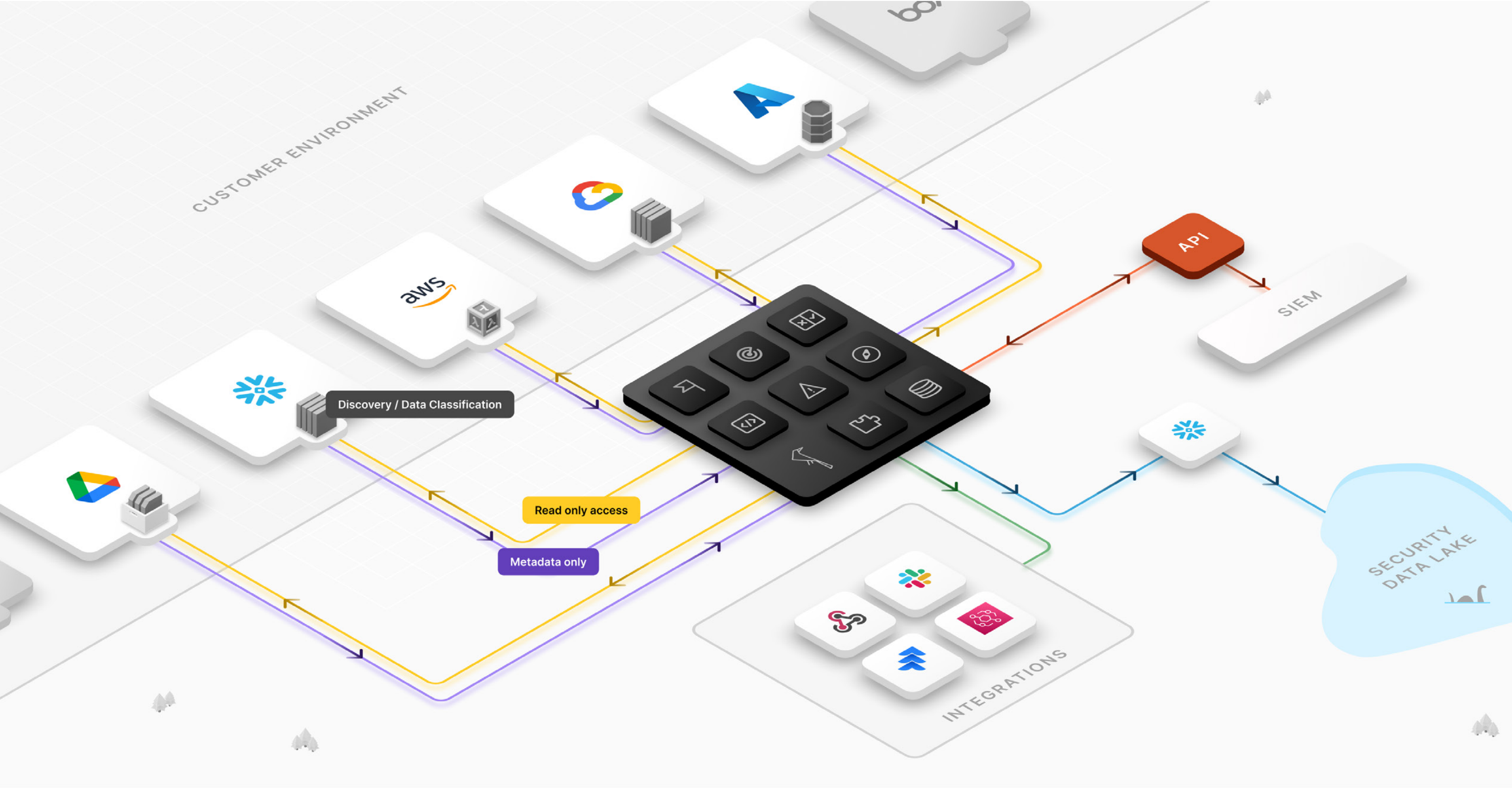
Data Security Platform

Data is the lifeblood of the modern economy. The companies at the forefront do an exceptional job equipping their data teams, yet security and cloud infrastructure teams don't have the tools to keep pace with explosive data growth. Security must automatically discover, classify, assess, and take action on sensitive data within hundreds or thousands of files and accounts, billions of objects, and petabytes of data. The Open Raven Data Security Platform provides 360-degree data visibility, works at cloud scale, is fully customizable, prevents attacks, eliminates unnecessary costs and risks, and streamlines compliance.



OR9928: New data violation

Developers secrets are not encrypted at rest.



Architecture

Secure and private by design

The Open Raven Data Security Platform is secure and private by design. No data security solution should create more risk than it aims to reduce by requiring data to be moved or transferred, requiring dangerous changes to security groups, or storing sensitive customer data.

> The platform is based on a single-tenant internal architecture with dedicated cloud infrastructure for each customer. This includes a dedicated AWS subnet and a single-tenant Kubernetes cluster, ensuring complete isolation between customers.

Open Raven harnesses a combination of native APIs, serverless functions and ephemeral compute – no dedicated scanners or agents – to locate, inventory, classify and ultimately protect data. The architecture ensures that no sensitive data is removed or copied into the Open Raven Data Security Platform at any time. The platform stores only metadata associated with discovered assets and scan findings, along with data previews. Data previews are small amounts of information related to findings that one can safely use to quickly triage the discovery and determine a course of action without the risk of exposing sensitive information. They are displayed in the Open Raven console as Data Previews, and the amount of data contained is configurable by the customer.

Why Open Raven?

Automated

Data location, inventory and classification are hands free. Policies do the work of identifying risk, automations provide "if this, then that" style actions in response to events.

Budget friendly

The power to handle petabyte-scale with the flexibility to fit your budget. Data scans allow for per scan budgets and cost 1/10th to 1/100th of competing approaches.

Secure and private

Your data stays where it is. Open Raven is cloud-native and runs with read-only access; no agents or dedicated compute. Only a configurable amount of metadata is sent to our platform.

Complete and accurate analysis

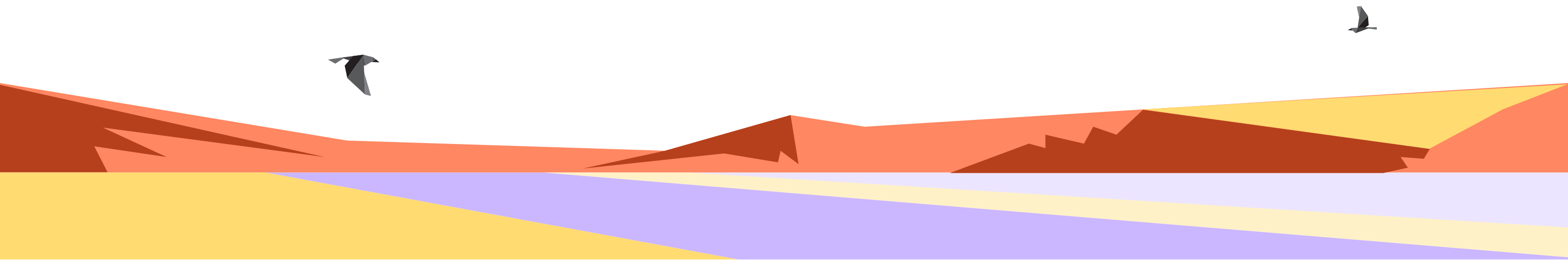
Complete visibility into all data at rest using 300+ default data classes including personal, financial and health data as well as developer secrets.

Open

Open Core design with projects available in GitHub, the ability to customize data classes., validator functions, rules, and policies, and easy operationalization through integrations and APIs.

Customizable

Create or customize data classes, data previews, scan budgets, rules, and policies.



Deployment and onboarding

Using CloudFormation or Terraform templates, it takes minutes to set up Open Raven and begin mapping and discovering data. The platform is cloud native SaaS and uses a familiar “connect vs. install” model where accounts, projects or full organizations can be connected so that new resources can be automatically discovered at any breadth. Open Raven uses no dedicated compute and minimal permissions— all work is performed over serverless functions or native APIs.

Getting started with the Open Raven is straightforward and typically follows a phased approach that begins with full, automated location of all native and non-native data services. The result of this initial step is a detailed listing of all data resources that can be interactively filtered and explored to quickly spot sensitive data, risky external sharing, and other anomalies.

The following phase is data discovery and classification. For large environments, this is typically accomplished by analyzing higher risk areas first, such as public facing data stores or unmanaged resources where sensitive data may be present.

These scans create an organization-wide data catalog of all identified, sensitive data so that it can be understood and protected. Scheduled, incremental scans keep the data catalog updated with no effort and negligible cost.

Taking action to manage data risk is the following phase which is driven by a range of rules-based policies aimed at eliminating data leaks (e.g., toxic data, exposed data, etc.) and compliance problems (e.g., customer data out of region, production data in test, etc.). Applying the policies to the data catalog results in precision, detailed alerts that can be triaged in platform or sent to existing workflows inside Slack, email or ticketing systems such as Jira. No organization’s data or security needs are the same: it’s both common and straightforward to make new data classes and rules to make the Open Raven platform perfectly suit your environment.

Open Raven can be further integrated with the rest of your security tooling using our APIs for scanning or data extraction, AWS Event Bridge, or a Snowflake-based repository of platform data that can be readily added to your existing data lake.

Customer phases and activities

1 Onboarding

Complete questionnaire

Connect SaaS workspaces

Initial discovery of individual and shared drives

Enable policies

Custom rules and data classes

User training

2 Scanning

Initiate historical data scanning

File enumeration

Initiate forward scanning

Cost analysis

Data catalog training

3 Tuning

Review data findings

Identify and flag false positives

Adjust custom data classes

Export data catalog

Alert training and creation

Custom rules and policies

Initiate forward scanning

4 Triaging

Review alerts

Risk assessment and prioritization

Close or ignore violations

Adjust custom rules

Tag assets

Export violations

Setup integrations

5 Operationalizing

Automations

Cost analysis

Add new users and consumers of Open Raven data

How we stack up

	Open Raven	Google DLP	CASB
Data Classes	300+	150	Varies
Accuracy	Tested at scale using open source testing tools with published results. Accurate by default, using verification functions for challenging data classes.	Google's "predefined content detectors" are sensitive to false positives; you are asked to select a "likelihood threshold", where you have to make tradeoffs between false positives and completeness.	Variable, but data classification is not a primary focus, often relying on simplistic techniques.
Customization	Fully customizable data classes that combine regex, keywords, keyword adjacency, and an optional validator API to confirm/deny the match and a customizable preview generation method.	Organizations can create a custom detector using only regex or a word list. Restricted to a maximum of 20 regex detectors and 10 word list detectors.	Variable by CASB, from basic to more.
Historical & Current Analysis	Full historical and present day analysis active by default, at scale.	Both are available, historical analysis often prohibitively expensive at scale.	Present day analysis often the only option; no historical scanning or scale restricted.
Unified Data Catalog	From AWS S3 to GCP BigTable and Snowflake, all sensitive data can be explored inside the Open Raven Data Catalog.	No central data catalog.	Focused on SaaS, weak or no coverage of IaaS/ PaaS data services.
Policies	Cover a wide range of issues from gDrive to IaaS and PaaS; defined after data discovery, flexible	Defined at outset, before data is known, forcing configuration without context.	Focused on SaaS services; breadth versus depth.
Open Architecture	Open Core, APIs, integrations.	Closed source, APIs available.	Closed source, APIs and integrations.