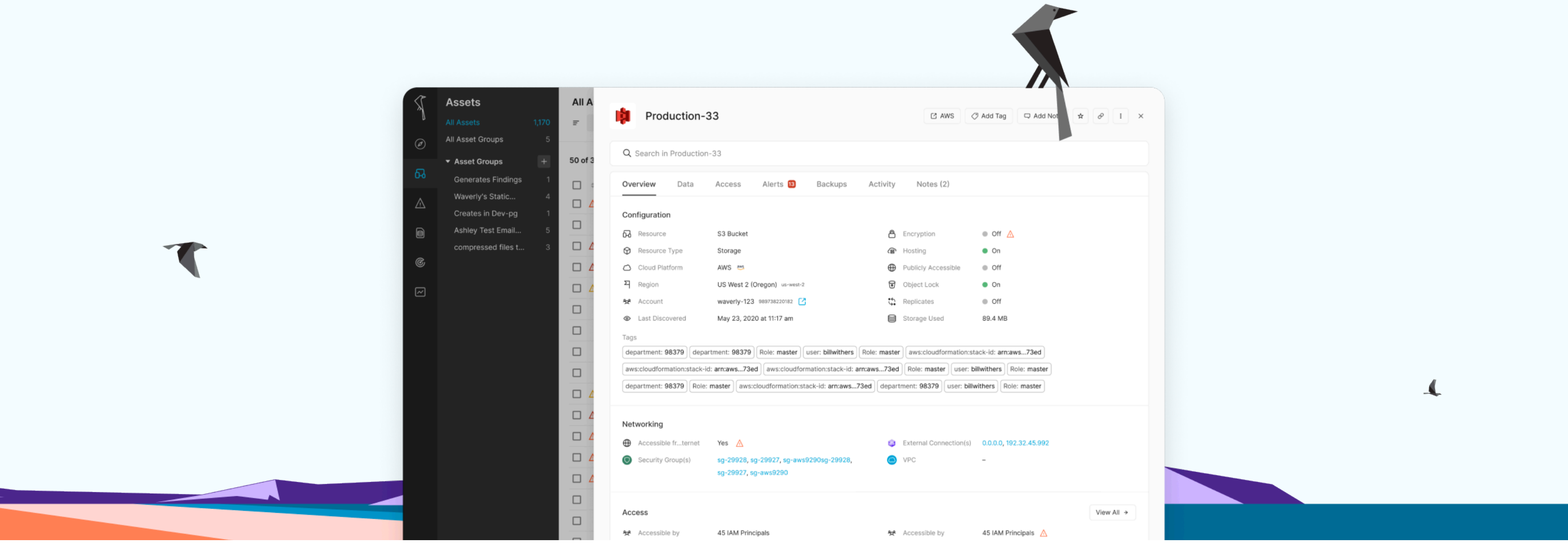
Open Raven

Open Raven Data Security Platform



Production-33

Configuration

Resource	S3 Bucket	Encryption	● Off ⚠
Resource Type	Storage	Hosting	● On
Cloud Platform	AWS	Publicly Accessible	● Off
Region	US West 2 (Oregon) us-west-2	Object Lock	● On
Account	waverly-123 989738220182	Replicates	● Off
Last Discovered	May 23, 2020 at 11:17 am	Storage Used	89.4 MB

Tags

department: 98379 | department: 98379 | Role: master | user: billwithers | Role: master | aws:cloudformation:stack-id: arn:aws...73ed | aws:cloudformation:stack-id: arn:aws...73ed | aws:cloudformation:stack-id: arn:aws...73ed | Role: master | user: billwithers | Role: master | department: 98379 | Role: master | aws:cloudformation:stack-id: arn:aws...73ed | department: 98379 | user: billwithers | Role: master

Networking

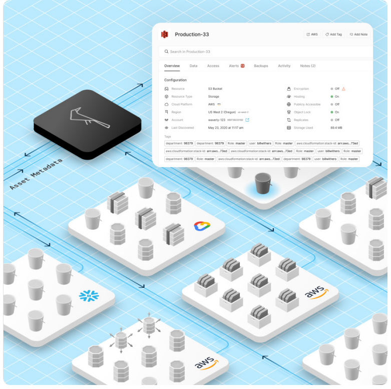
Accessible fr...ternet	Yes ⚠	External Connection(s)	0.0.0.0, 192.32.45.992
Security Group(s)	sg-29928, sg-29927, sg-aws9290sg-29928, sg-29927, sg-aws9290	VPC	–

Access

Accessible by	45 IAM Principals	Accessible by	45 IAM Principals ⚠

Automate Data Security Posture Management (DSPM), Data Loss Prevention (DLP), and Data Detection and Response (DDR) across IaaS, PaaS, and SaaS.

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.

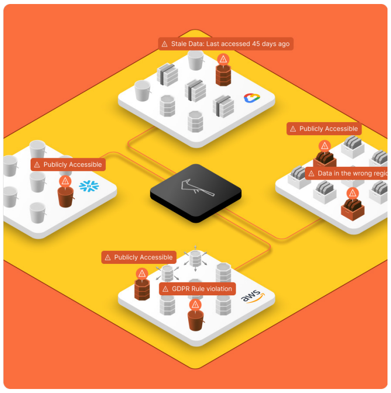


Resource: S3 Bucket
Resource Type: Storage
Cloud Platform: AWS
Region: US West 2 (Oregon)
Account: waverly-123
Last Discovered: May 23, 2020 at 11:17 am
Encryption: Off
Hosting: On
Publicly Accessible: Off
Object Lock: On
Replicates: Off
Storage Used: 89.4 MB

department: 98379 · department: 98379 · Role: master · user: billwithers · Role: master · aws:cloudformation:stack-id: arn:aws...73ed · aws:cloudformation:stack-id: arn:aws...73ed · aws:cloudformation:stack-id: arn:aws...73ed · Role: master · user: billwithers · Role: master · department: 98379 · Role: master · aws:cloudformation:stack-id: arn:aws...73ed · department: 98379 · user: billwithers · Role: master

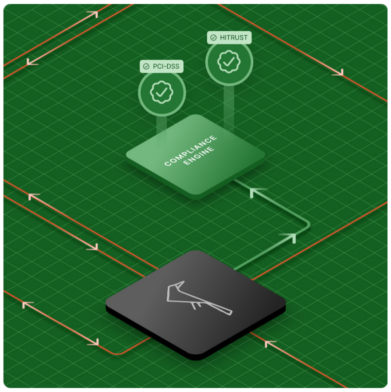
Comprehensive visibility

With the Open Raven Data Security Platform, security teams can quickly and automatically inventory data stores, classify data at petabyte-scale, pinpoint sensitive data, identify risk and take action. This provides immediate value, making it easy to spot shadow data and left-behind services, dangerous 3rd party network connections, unwanted data sharing relationships, and other risk factors.



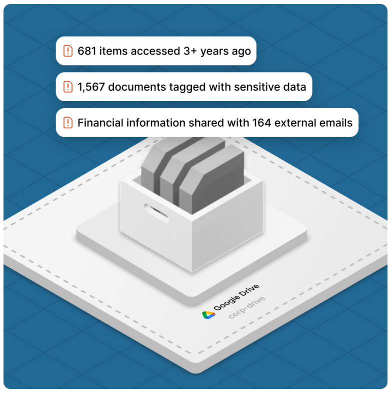
Prevent costly security incidents

Open Raven proactively identifies the conditions that lead to data leaks and breaches, allowing data to be secured or removed so that the team can avoid a time-consuming and expensive security incident. ~90% of breaches are due to human errors that can be readily detected and fixed.



Streamline compliance

Global companies need to know and control customer data in order to comply with GDPR, Schrems II and instill confidence in their international customers. Open Raven automates both locating a wide variety of customer data and creates guardrails that streamline responses to compliance efforts (e.g., SOC2, HITRUST) and helps keep data only where it’s expected to be.


681 items accessed 3+ years ago
1,567 documents tagged with sensitive data
Financial information shared with 164 external emails
Google Drive
corp-drive

Eliminate hidden risk from overshared and externally shared files

Externally shared Google Drive files with sensitive data represent significant security and compliance risks, potentially leaking high-risk data to unauthorized users. Such leaks can lead to data breaches, privacy violations, and compromise of confidential data. Open Raven quickly identifies files with excessive risk and enables automated response actions.

Use Cases

What's possible with Open Raven

Discover and classify data

Open Raven connects within minutes, works over native APIs and serverless functions, and analyzes data where it resides without moving or even touching it. Your functions run our analysis engine with you in full control of the sampling rate (0-100%), time constraints, and exclusion logic. Quickly analyze massive amounts of data or slowly build a catalog over time.

Assess the security posture of data

Open Raven automates both understanding and managing your data security posture. Rules-based policies, ranging from CIS Benchmarks to regulatory standards such as GDPR, precisely identify where data is at risk versus generalized alerts from a CSPM. Focus on the primary target of any leak or breach itself using data context versus chasing lower priority problems.

Establish guardrails for data

Open Raven's data guardrails provide automated, straightforward answers to the modern data sprawl problem. The rule-based policies monitor sensitive data for a wide range of conditions from location and configuration to access permissions and enable enforcement of data sharing agreements and proof of compliance for audit mandates. Automated alerts indicate when guardrails have been violated.

Enforce data security policies for file and folder sharing

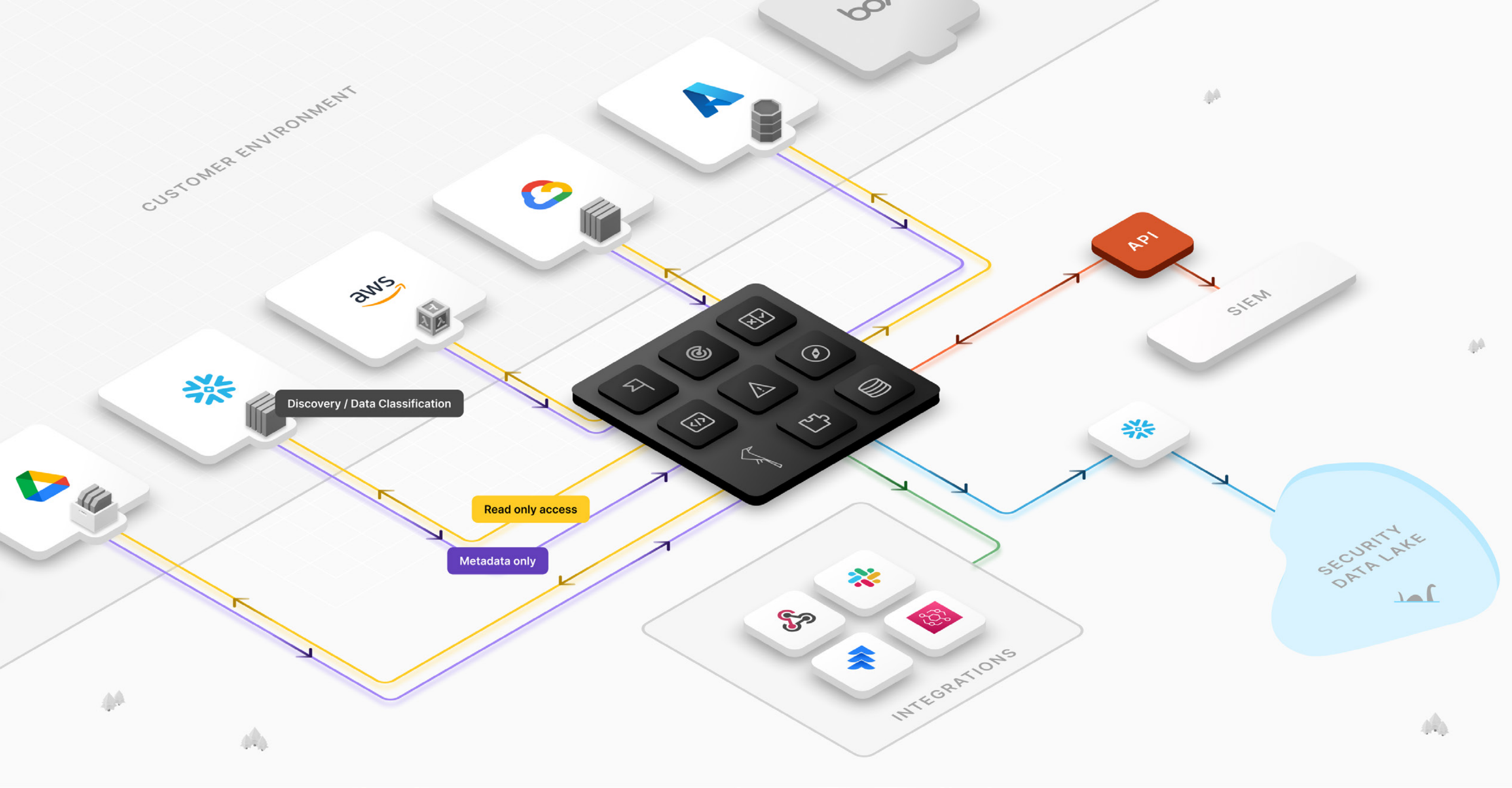
Google Drive makes it easy for anyone to share files and folders and virtually impossible for security teams to know what sensitive data has already traveled beyond company boundaries. Gain critical visibility into shared sensitive data by combining sensitive data context with user, permission, and domain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

Streamline offboarding of people and partners

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 analysis and response to the sharing activities of these individuals as well.

Prevent data-focused attacks

Monitor risk to your most sensitive and critical data with proactive, live detection of potentially malicious data events including suspicious movements, disrupted logging, privilege escalations, and anomalous access attempts. Monitoring events helps security teams keep tabs on their most important data, automatically and hands-free.



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

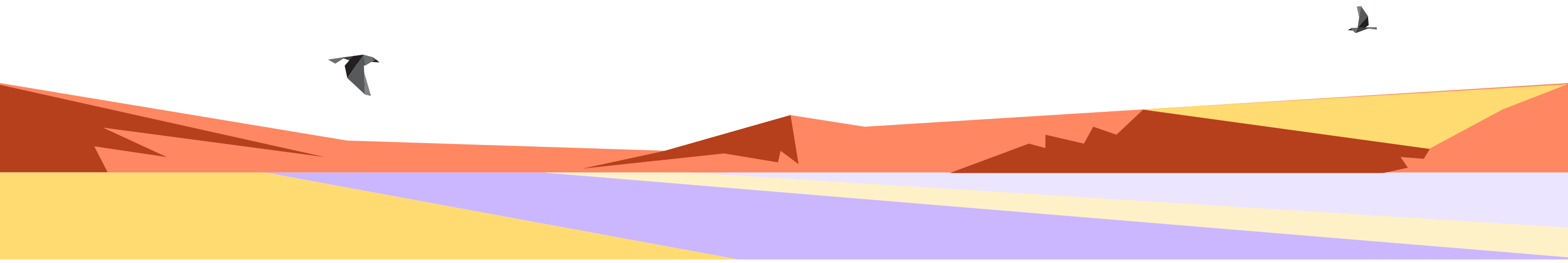
Complete visibility into all data at rest using 300+ default data classes including personal, financial and health data as well as developer secrets.

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 that is similar to modern cloud security posture management products 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 both a detailed listing of all resources and a map-based visualization that can be interactively filtered and explored to quickly spot orphaned resources, shadow data 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

Connect cloud accounts

Initial discovery of assets

Complete onboarding questionnaire

Enable policies

Setup custom rules and data classes

Asset group and scan creation training

2

Scanning

Develop Scan Methodology

Create custom asset groups

Initiate data scanning

Monitor results & workload impact

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

Enable data policies

4

Triaging

Review alerts

Risk assessment and prioritization

Close or ignore violations

Adjust custom rules

Tag assets

Export violations

Setup integrations

5

Operationalizing

Develop and execute recurring scans

End-to-end workflow Design

Cost analysis

Coverage reporting

Implement RBAC

Add new users and consumers of OR data

How we stack up

	Open Raven Data Security Platform	CSPM with DSPM Add-On	AWS Macie
Solution Type	Data Security Platform with DSPM, DLP, and DDR	CNAPP with DSPM add-on, no DLP or DDR	Platform primitive service, IaaS only, no DDR
Data Classification	Unstructured and structured	Structured, unstructured (limited)	Unstructured
Analysis Method	Default to 100% sampling with validation	Partial sampling	Sampling
Structured Data Scanning Method	Authenticated or snapshot	Snapshot	N/A
Data Service Discovery	Native and non-native	Native	S3 only
Visualization	Mapping (risk, compliance, aging/ cost, backup)	Attack path	Heat map
Scan Budgeting	Customizable, set per-scan with max budget defaults	No scan budgeting	No customization, reduce costs by scanning fewer resources
Data-specific Rules and Policies	Comprehensive, customizable	Limited	Limited
Open Architecture	Open Core, APIs, integrations	Closed source, APIs and integrations	Closed source, APIs available
Licensing	Per data store, data quantity (DSPM), users (DLP) — predictable	Priced by resource	Pay as you go, complex, unpredictable