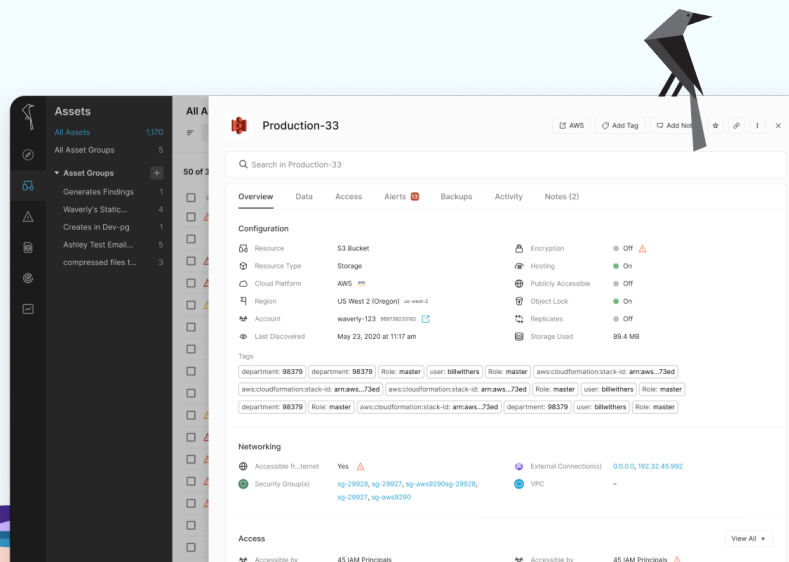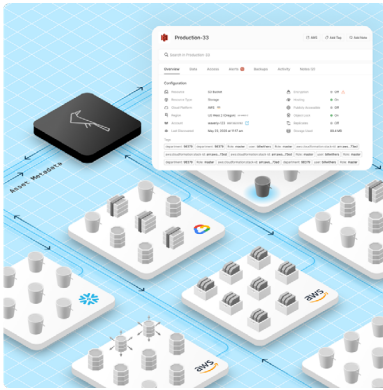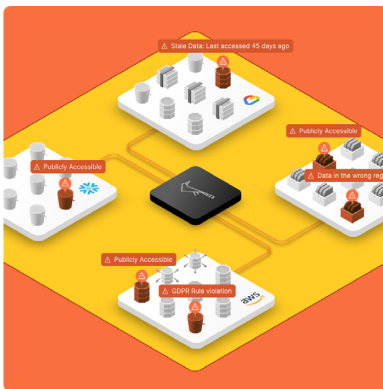Open Raven

Data Security Platform

Automate data discovery, classification, posture assessment, attack detection and prevention – at cloud scale.

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 monitor sensitive data within hundreds or thousands of accounts, billions of objects, and petabytes of data. The Open Raven Data Security Platform works at cloud-scale, is fully customizable, and enables organizations to gain 360 degree visibility. It enables organizations to prevent attacks, eliminate unnecessary costs and risks, and streamline compliance.

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, and identify risk. 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.
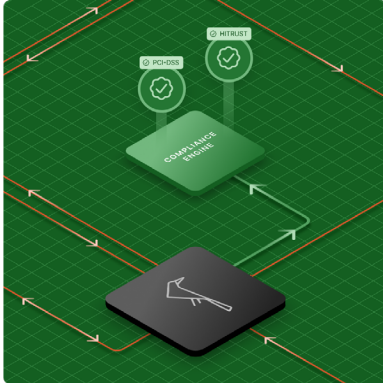
Streamline compliance

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.
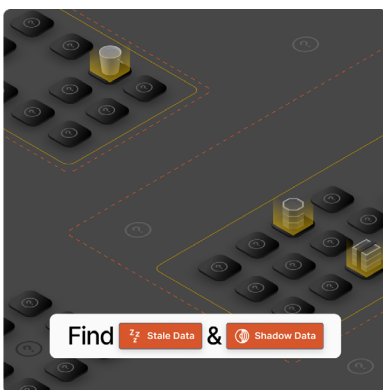
Eliminate unnecessary costs and risk

Between 60% and 90% of cloud data is "dark" - data that is never touched, used or perhaps even seen. Open Raven pinpoints all data locations and highlights sensitive data, showing where both costs and risks can be reduced by eliminating unnecessary data and services.

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%), budget, 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 for infrastructure configuration issues 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 to configuration and enable enforcement of data sharing agreements and proof of compliance for audit mandates. Automated alerts indicate when guardrails have been violated.

Audit S3 access permissions

Reduce the time needed to audit S3 access permissions from days or hours to minutes. Open Raven automatically analyzes access permissions and provides clear answers to critical questions, including who has access to specific buckets and those with sensitive data, VPC peering relationships that allow for data transfer, and permissions that allow for access by external 3rd parties.

Eliminate stale and shadow data

60-90% of all data goes unused, or dark, quietly accumulating in the cloud. Open Raven scores data stores using a staleness rating that makes it straightforward to spot unnecessary resources and data that can be safely removed to drive down cloud risk and your monthly bill.

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.
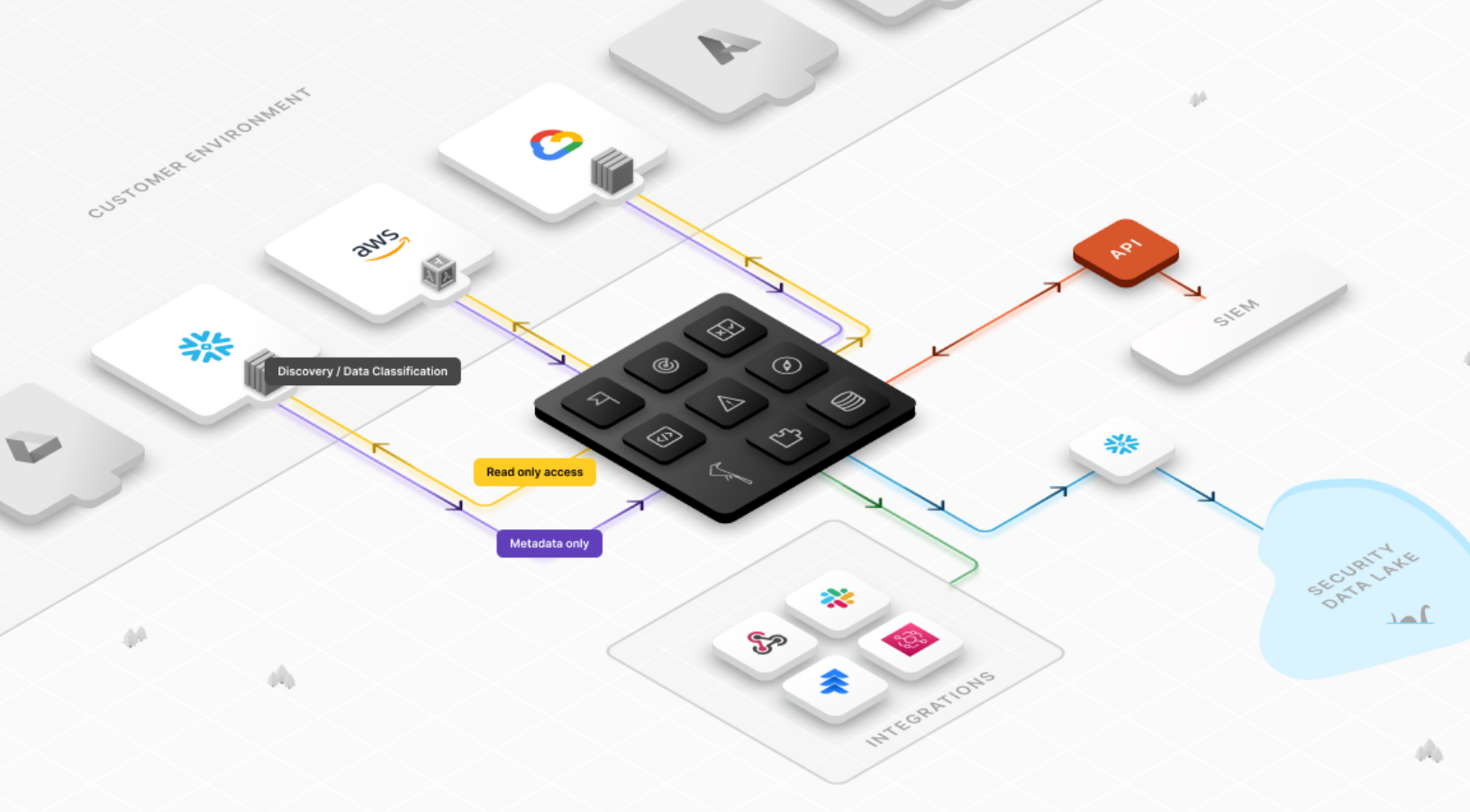
Secure and private by design

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 employs a single-tenant internal architecture and provisions dedicated cloud infrastructure for each customer. The infrastructure includes a dedicated AWS subnet and a single-tenant Kubernetes cluster, ensuring complete isolation between customers.

Open Raven uses a unique serverless architecture for data location, inventory, deep analysis, and accurate classification of cloud data where it lies without opening holes for potential attackers to exploit. 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 snippets. Data snippets are small amounts of information related to findings that security analysts can safely use to quickly triage the discovery and determine a course of action without the risk of exposing sensitive information. Snippets are displayed in the Open Raven console as Data Previews, and the amount of data contained in a snippet is configurable by the customer.

Why Open Raven?

Secure and private

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

Budget friendly

The power to handle petabyte-scale with the flexibility to fit your budget. An optimized, serverless architecture with controllable scans provides predictable costs and outcomes.
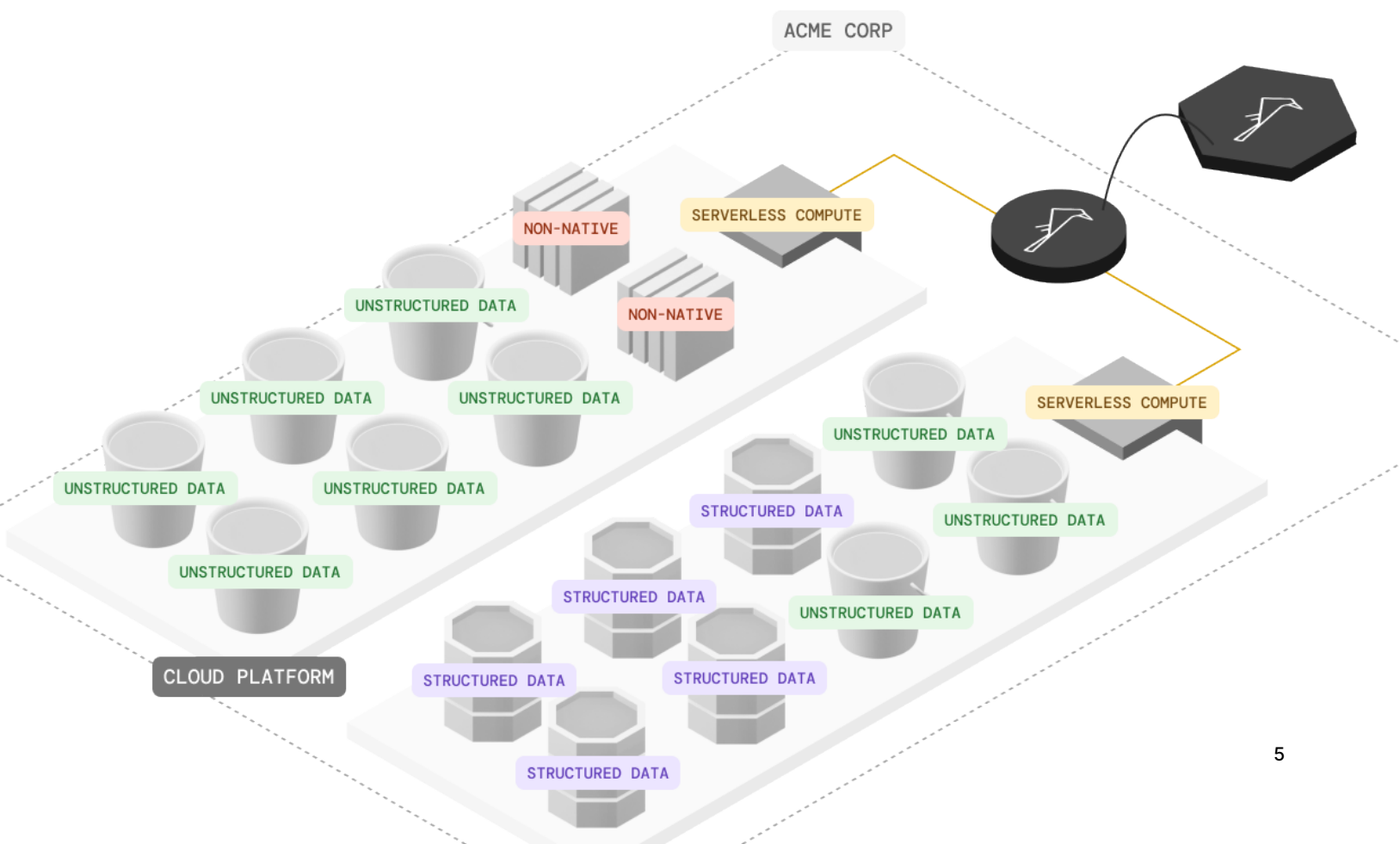
Customizable

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

Complete and accurate analysis

Complete visibility into all data at rest using more than 200 data classes, powered by regular expressions, machine learning, and robust validator functions.

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.

ACME CORP

NON-NATIVE

SERVERLESS COMPUTE

UNSTRUCTURED DATA

NON-NATIVE

UNSTRUCTURED DATA

UNSTRUCTURED DATA

SERVERLESS COMPUTE

UNSTRUCTURED DATA

UNSTRUCTURED DATA

UNSTRUCTURED DATA

STRUCTURED DATA

UNSTRUCTURED DATA

UNSTRUCTURED DATA

STRUCTURED DATA

UNSTRUCTURED DATA

CLOUD PLATFORM

STRUCTURED DATA

STRUCTURED DATA

STRUCTURED DATA

5

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

Open Raven

How we stack up

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