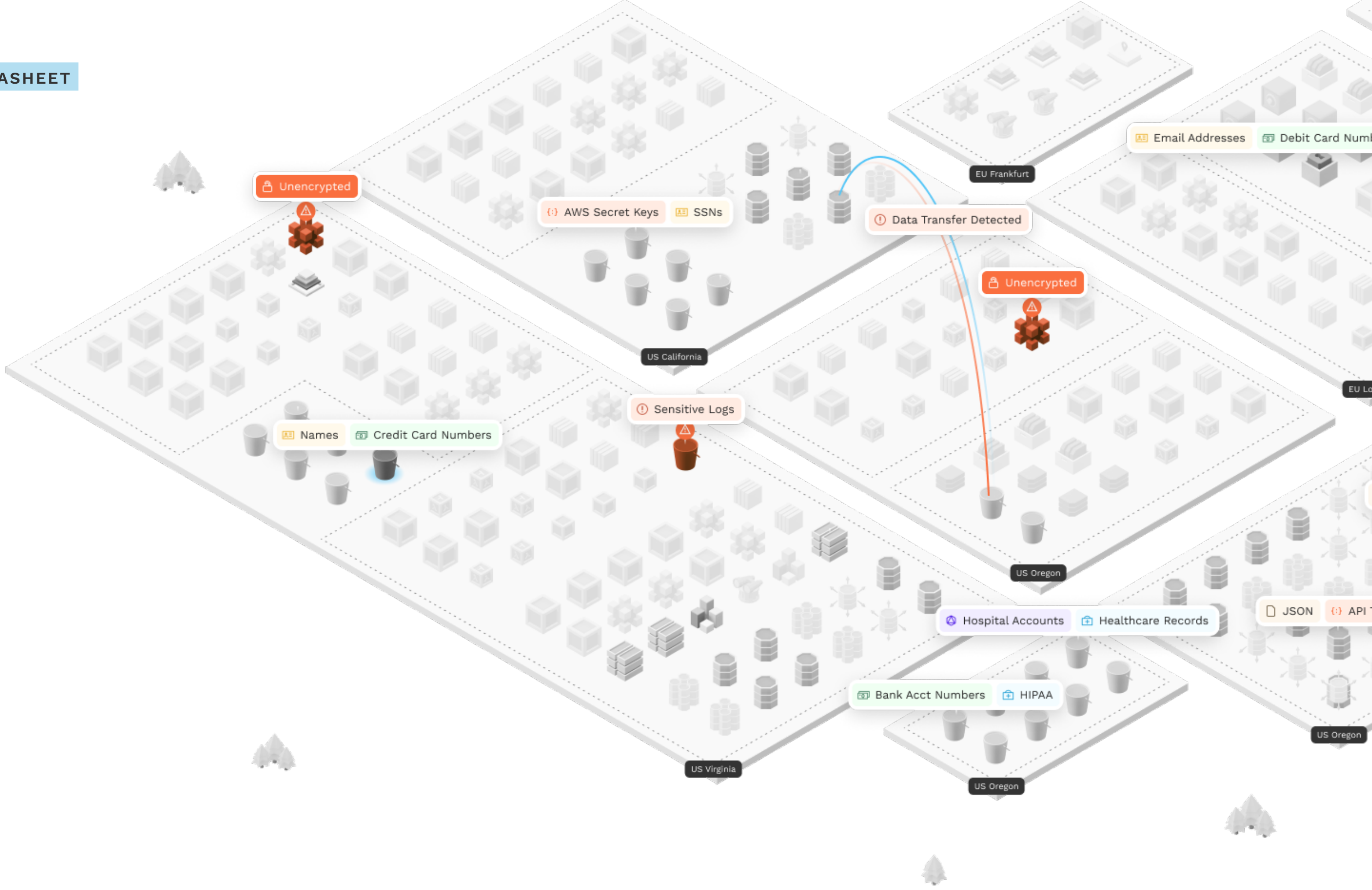
DATASHEET



OPEN RAVEN

Know your data.
Keep it safe.

Our Approach

Open Raven is a cloud native data platform directly aimed at restoring visibility and control of customers' data, automating an organization's ability to prevent breaches, defend against attacks and meet their compliance needs. Today, fundamental questions such as "Where's our data?", "What types of data do we have?", and "Is it secured properly?" are too time consuming and expensive to answer. Open Raven eliminates blind spots by fully mapping a cloud estate, classifying data at petabyte scale, and enabling effortless policy-based monitoring that fits existing workflows.

Answer hard questions about your cloud data without breaking a sweat, or your budget

Discover

Discover native and non-native data stores across your entire AWS cloud estate, all regions and accounts. Easily answer the fundamental question “where is my data?”

Mapping

Mapping allows teams to visually interact with all resources across regions. Know your data risks by quickly understanding all internet facing resources and their connections. Use interactive filters to see over 100 different scenarios.

Classifying

Classifying your data is finally scalable (Petabyte) and cost-effective. Locate sensitive data at rest and build rich context for your security and cloud teams. Use default classifications or customize your own for improved accuracy and precision.

Monitoring

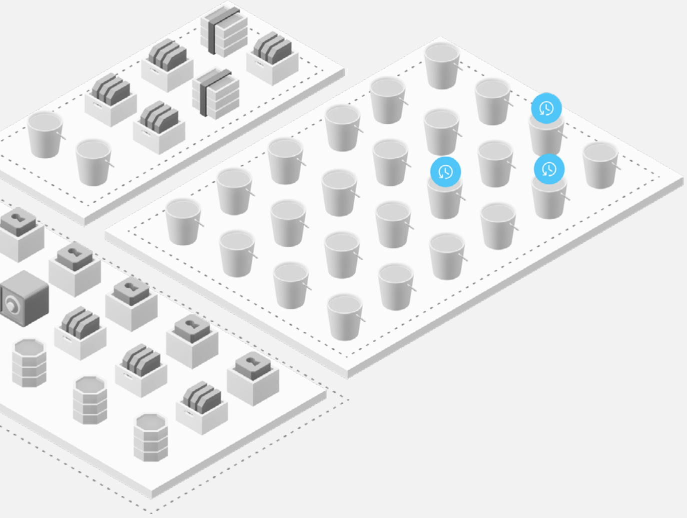
Monitoring provides a hands-free analysis of data, infrastructure or both at the schedule and frequency of your choosing. Fit proactive alerting into your workflow with pre-built integrations for G Suite, O365, Slack and more.

Policies

Policies enable the automation of data security, privacy and compliance. Customize policies for continuous monitoring, or 1-time assessments, for more effective incident prevention in less time.

Act

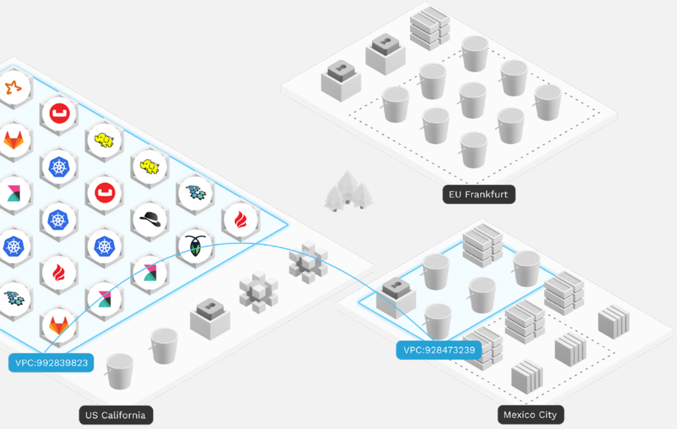
Act faster and more confidently on alerts, preventing problems from becoming incidents by making your SOC data-smart. Make remediation faster, better and easier by removing manual steps in reporting out to your SIEM (e.g., Splunk) via API or 1-click integrations.



Master Ransomware

Ransomware attacks have reached an intensity that has broken through prevention defenses and sent cyber insurance premiums skyrocketing. Knowing you can quickly recover from an attack is essential, but requires far too much manual effort and an excessive number of products. Proactively eliminate gaps in ransomware preparedness with unified infrastructure, backup and data-intelligence in Open Raven.

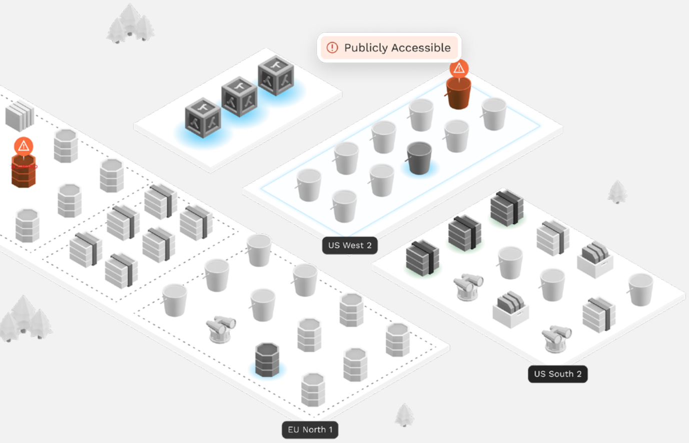
- Know what must be protected
- Use seamless AWS Backup integration to protect critical data and assets
- Harden defenses with built-in ransomware policies
- Prioritize response and recovery with in-depth data-intelligence



Inventory Cloud Data

Open Raven is like Google Maps for cloud security. Easily see across your organization to spot anomalies such as unexpected connections and misplaced resources. Automate data classification for an up-to-date, centralized data catalog that makes analysis and reporting a breeze. From visual mapping to Splunk-based search and dashboards, Open Raven makes quick work of previously time-consuming audits and reports.

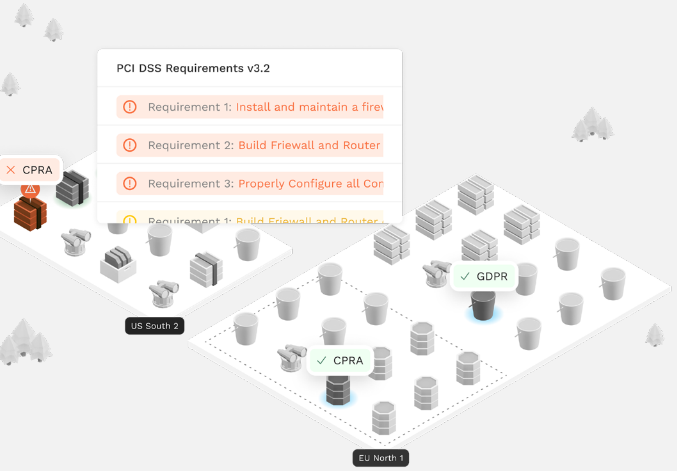
- Automate mapping of cloud assets across entire organizational accounts
- See internet accessible assets, trace-back to security groups, and see VPC peering relationships
- Use 1-click asset attribute filters to quickly see over 100 different scenarios
- Use built-in Splunk search for detailed reporting and investigation



Find and Act on Exposed Data

Automate locating native and non-data data services to avoid surprises and unnecessary costs. By combining a data catalog of sensitive data with assessment of infrastructure controls, identify and resolve data exposure such as credentials in JSON-based log files or improperly protected customer personal data.

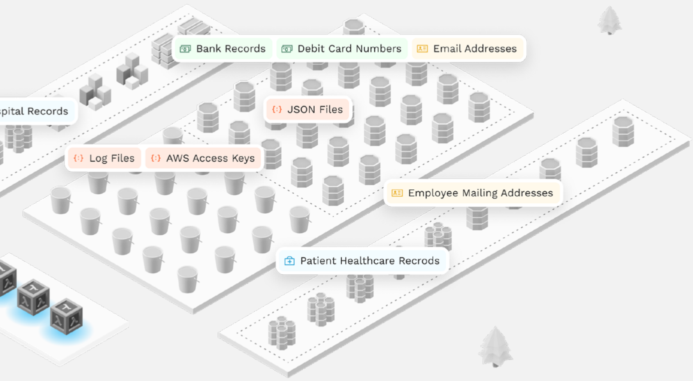
- Know your data and where it resides
- Choose from over 100 default data classes or create your own
- Monitor for policy violations e.g., payment card details in an unencrypted S3 bucket
- Integrate alerts into your SIEM workflow for easier and faster remediation


PCI DSS Requirements v3.2
Requirement 1: Install and maintain a firev
Requirement 2: Build Friewall and Router
Requirement 3: Properly Configure all Con
Requirement 1: Build Friewall and Router
CPRA
US South 2
GDPR
CPRA
EU North 1

Automate Data Policy Monitoring

Easily translate data contracts and business rules into policies with automated monitoring. Whether PCI DSS, HIPAA, GDPR, CPRA, HITRUST or other, rest easy knowing your team will receive alerts when data falls out of proper protections: region, public accessibility, encryption status, logging, use of backups and more.

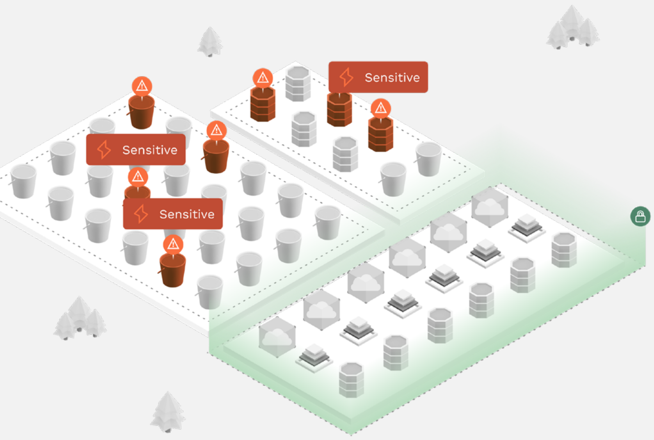
- Utilize default policies and rules or customize your own
- Automate geofencing by data type
- Easily identify stale data that falls outside of retention limits
- Empower SOCs with the data context they need, automatically



Audit and Report on Data Privacy

Open Raven automatically discovers and maps data locations so that inventory and classification, not to mention reporting, starts with a solid foundation. Select from over 150 data classes or create your own to pinpoint data at rest across a cloud environment, leveraging serverless functions for both speed and cost savings.

- Export cloud asset reports as needed
- Easily provide up-to-date infrastructure diagrams
- Fine-tune reports with built-in Splunk search and reporting functionality



Keep Developer Secrets Safe

Open Raven has a wide range of data classes covering developer secrets, from SSH and AWS API keys to the ability to create custom classes and rules that perfectly suit the task at hand. Serverless classification and monitoring identify when secrets from Github, AWS, SaaS services or others are exposed in log files, templates or unexpected locations. Results can be explored in the Data Catalog in a redacted format with the exact location noted and deep linked to the AWS Console for quick remediation.

- Add another layer of security for DevSecOps
- Easily use built-in or customized developer secrets classes
- Use policies to enforce security controls for secrets
- Streamline resolution of identified issues with clear context and direction

How it works

The Open Raven platform delivers comprehensive protection over the cloud. Set-up within minutes to find where your data is located across your entire infrastructure, from data lakes to data warehouses.

We designed Open Raven to be a platform we would want to use ourselves. One that scales effortlessly with predictable cost. That can be readily extended and integrated. A platform that balances rich context and visualization with a need for minimal access and data stored.

Ready in Minutes

Single-tenant SaaS for balancing cost, ease of use and privacy.

Integration Ready

Firehose API, open core design and use of widespread projects ease integration and customization. Built-in Splunk integration allows for custom search and reporting. Hands-free AWS Backup integration simplifies protecting critical data and services with appropriate backup plans and policies.

Safe & Private

Your data stays where it is. Open Raven is cloud-native, and runs with read-only access in your environment, analyzing metadata and displaying results in an intuitive web interface.

Cloud Native

Discovery & classification based on APIs, AWS config, Cloudtrail & serverless analysis (AWS Lambda). No agents, no network scanners.

ACME CORP
AP SOUTH
EU WEST 1
S3
λ
OPEN RAVEN

How we stack up

	Open Raven	AWS Macie	CSPM	Nextgen DLP
Focused On	Data + Infastructure	Data	Infastructure	Data
Data Type	At rest	At rest	NA	In motion
Method of Analysis	Serverless, Native APIs	API only (S3 bucket restricted)	Agents, APIs	Sidecar, APIs
Data Service Discovery	Native & non-native	S3 only	Native	NA
Visual, Interactive Mapping	●●●●	○○○○	●●○○	○○○○
Data Classification	●●●○	●●○○	○○○○	●●○○
Rule-based Policies	●●●○	○○○○	●●●○	●●●○
Open Architecture	●●●●	○○○○	●●○○	●○○○
Licensing	Per data store, data quantity	Pay as you go, complex	Pay by resource/asset	By data volume