P O L A R

Polar Security Data sheet

Platform Essentials

- SOC2 and ISO 27001 compliant
- Read-only permissions required
- Unique Data Security Posture Management (DSPM) platform
- Cloud-native SaaS solution
- Zero-impact to business application performance
- Agentless, cloud native installation for discovery
  For security and privacy reasons, a secured analyzer is required for classification of data in the customer environment

Supported Platforms

Cloud Providers

- Amazon RDS
- Amazon DynamoDB
- Amazon DocumentDB*
  *Discovery only.
- Amazon S3
- Amazon EC2
- Azure Blob Storage
- Google Cloud Storage
- Google Big Query

SaaS

- Google Drive
- One Drive
- Slack
- Microsoft 365
- Confluence
- JIRA

File Extensions

- Text File
- ORC
- YAML
- PDF
- Log File
- Terraform
- BSON
- Avro
- SQL
- Parquet
- JSON
- CSV File
- Redis
- Sqlite
- Excel File
- Word File

Data stores found on Amazon EC2

- mySQL
- SQLite
- Redis
- MongoDB
- Text file
- CSV file
- Log file

Supported Classifiers

Supporting over **30** different classifiers including:

- Credit Cards, Crypto Wallets and other financial details
- Personal and identifiable (PII) details
- Health information
- Passwords, Tokens, and other development secrets
- Customer specific sensitivities*
- and more.

*Support for custom sensitivities is available on demand

Security Overview

Polar Security is here to make your data security & compliance journey as smooth as possible:

Data at transit:
All communication to Polar Security backend are done using encrypted HTTPS (using TLS v1.2)

Data at rest:
Fully encrypted using AES-256 (provided by AWS KMS).
For more information, refer to AWS Securing Data at Rest.

Data protection:
We are using our own platform to make sure that our customers and our data is not at risk.

Following NIST crypto standards.

Sensitive data never leaves the customers' account and region.