POLAR

Polar Security Data sheet

Unmanaged data stores

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

Note: Data stores found on Compute instances (AWS EC2, GCP VM, Azure VM)

SaaS Applications

- Google drive
- One Drive
- Slack
- Sharepoint (Attachments only)
- Salesforce (Attachments only)

Supported Classifiers

Supporting over **20** different classifiers including:

- Credit cards and other financial items
- Personal and identifiable (PII) information items
- Health information
- Development secrets
- and more.

Note: Support for custom classifiers 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.

Sensitive data never leaves the customers' account and region.

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.