kogni

Kogni discovers sensitive data in your enterprise data sources, secures it, and continuously monitors for new sensitive data. Kogni helps organizations comply with regulations such as HIPAA, PCI, GDPR, PHI, FERPA, and others.

Highlights

- **Discover sensitive data** in enterprise data sources with minimal overhead.
- **Comprehensive dashboard** of sensitive data across enterprise data sources.
- **Secure sensitive data** through pre-built workflows.
- **Protect sensitive data** using masking, redaction, encryption, and tokenization.
- **Secure data as it is ingested** either transparently via Kogni Agent or via plugins for Sqoop, NiFi, StreamSets, etc.
- Continuously **monitor data sources, and alert** in case of policy violations.
- **On-premise** and cloud datasource support.
- **User defined classifiers** to identify sensitive data unique to your organization.

Data Security Challenges

Knowledge of sensitive data in enterprise data sources is tribal, not institutional. This creates challenges around monitoring data security within an enterprise in a centralized manner.

Lack of structured focus on securing data, governance, and visibility leads to information security and compliance issues.

Most enterprises are focussed on securing data using perimeter security via firewalls. Globally, data security community accepts that data breaches are inevitable. It is not a question if the perimeter security will be breached, the only question is, when?

The Kogni Approach to Data Security

Kogni helps enterprises move beyond perimeter security and enables them to focus on data-centric security.

Kogni **discovers**, **secures,** and **monitors** sensitive data in enterprise data sources. Kogni's approach to data security reduces the impact of a data breach, helping enterprises comply with regulations, and also enables data governance initiatives by monitoring for policy violations.

Discover

Scans enterprise data sources for sensitive data stored in text and images.

Secure

Secures sensitive data in Hadoop/Data Lake as it gets ingested.

Monitor

Continuously monitors data sources, and alerts in case of policy violations.

Why Use Kogni?

DATA SECURITY CHALLENGES

- Are your systems compliant with regulations (HIPAA, GDPR, PCI, PHI, FERPA)?
- Do you know where your sensitive data is located?
- Is the data in our data lake secure enough?
- Are you storing sensitive data in the cloud?
- Do you know who is accessing your sensitive data?
- Will your data breach/security risk increase with the transition to Big Data solutions?

KOGNI VALUE PROPOSITION

- Inspects Hadoop, S3, NoSQL, RDBMS data sources for sensitive data
- Transparently secures sensitive data as it is ingested into data lake (Hadoop, S3) with zero code change and with little overhead to the performance of the ingestion process
- Supports both on-premise and cloud data sources
- Continuous monitoring of data sets, access controls and alerts in case of policy violations
- Offered as a managed service.

BUSINESS BENEFITS

- Compliance with regulations such as HIPAA, PCI, PHI, GDPR, FERPA, and other
- Reduce regulatory compliance costs
- Reduced losses from a data breach
- Secure use of data assets enabling business growth
- Accelerate big data Implementations - with security and governance

Kogni Architecture

Kogni is powered by Spark for speed and scalability. Kogni has connectors to a wide variety of data sources and integrates with a number of monitoring tools. Kogni's simple architecture makes it easy to deploy and delivers faster time to value.