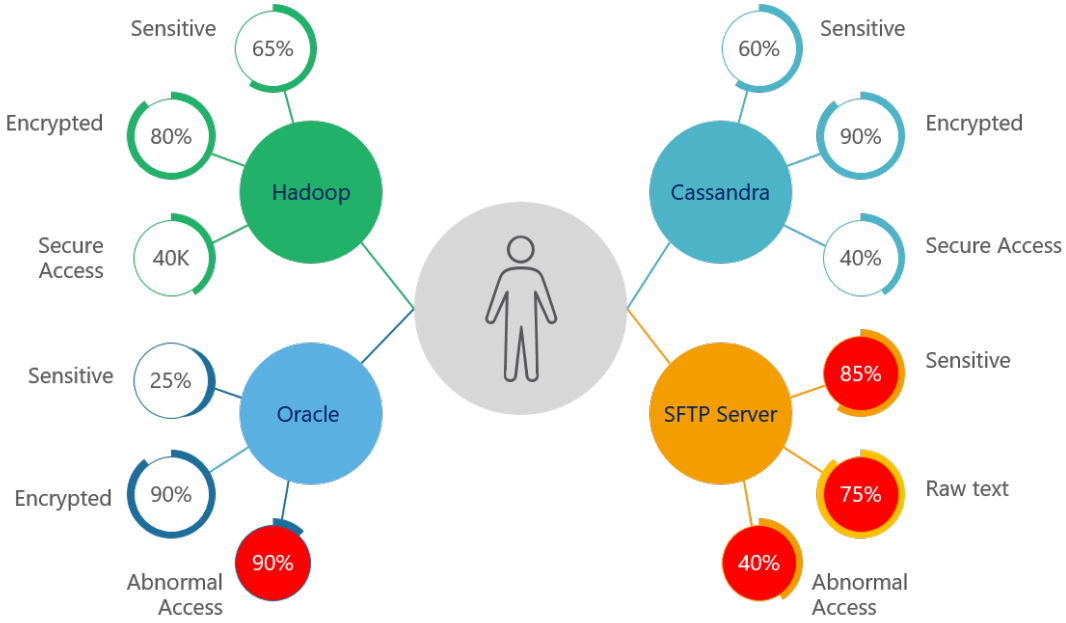
Pricchaa Inc.
Protect Sensitive Data

Autonomous Usage Monitoring and Anomaly Detection



Solution for Mitigating Data Breach Risks in Big Data Ecosystem

Nearly 90% of healthcare organizations experienced one or more data breaches ~ Ponemon Institute

43% of US businesses had one or more data breaches ~ USA Today

Only a third of sensitive data stored in cloud based applications is encrypted ~ Help Net Security

630.414.1231 info@pricchaa.com www.pricchaa.com/bigdata

Data Breach Risks in Big Data Ecosystem

With the accelerating use of high velocity, high volume complex data in a variety of formats and in new platforms (NoSQL, Hadoop, Cloud), detection of data breach risks is challenging. Hadoop, No-SQL, IoT systems are not designed with security in mind. Seamless monitoring of regular data and big data ecosystem for security to address the following is cumbersome.

- Who is accessing the data? What data are they accessing?
- Is someone trying to access data that they don't have access to?
- Are there any anomalous access patterns ?

Traditional security tools were architected for regular/small data and their older architecture cannot process Big Data efficiently. NoSQL data sources are not easy to handle and requires significant configurations.

New Paradigm for Data Security

- *Big Data Architecture*– Must handle large data volume easily
- *New data source compatibility*- Must handle NoSQL, Hadoop etc.
- *Autonomous*- Must detect unknown and unexpected data breach risks/ threats

Pricchaa : Autonomous Usage Monitoring and Anomaly Detection

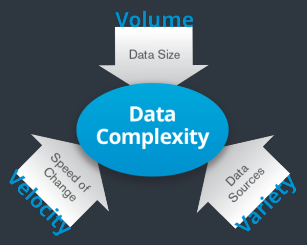
Pricchaa identifies data breach risks without coding. It's powered by Machine-learning to detect sensitive data in multiple data sources and autonomously create 1000's of monitoring rules without any manual intervention. Real time usage activities are analyzed leveraging powerful machine learning algorithms to detect abnormal pattern. More specifically, Pricchaa provides the following capabilities:

1. Detect sensitive data in structured and unstructured data sources (e.g. PDF, Image etc.) and set autonomous monitoring policies
2. Encrypt data elements while preserving format and referential integrity (optional)
3. Detect insecure access and policy violation in real-time
4. Identify anomalous user activity

10 X Faster Than Most Solutions

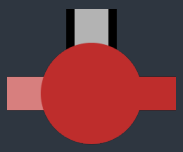
About Pricchaa

Pricchaa helps organizations to identify and proactively protect sensitive information across applications including Regular Data, Big Data, Test Data and email environments. Leveraging machine learning, a 'plug-n-play" framework, and innovative encryption technology, our platform is uniquely positioned to ensure compliance of both structured and unstructured data located in the cloud or On-Premise



Built for Big Data

Designed for handling big data using commodity hardware. Architected for faster processing. Linearly scalable



Cross Platform

File System: Linux, Windows, HDFS, S3

RDBMS: MS SQL, ORACLE

Big Database: REDSHIFT, HIVE

Encryption

Encryption preserves the format and maintains the relationship between various data sources. No orphan record is created because of the encryption.

Machine Learning

Leverages machine learning algorithms to detect sensitive data and to identify anomalous user behavior

cloudera CONNECT · Hortonworks · amazon web services | Partner Network · Microsoft Partner