Pricchaa Inc.

Protect Sensitive Data

Solution for Encrypting Test Data

Nearly 90% of healthcare organizations experienced one or more data breaches in 2015 ~ Ponemon Institute

43% of US businesses had one or more data breaches in 2014 ~ 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/testing

Data Breach Risks in DevOps

As DevOp organizations leverage the power of big data, cloud, and the internet of things to deliver new services and products, they need to take appropriate steps to manage and mitigate the data breach risks. In their test data.

In addition to setting up correct security protocol for protecting data housed in DevOps data servers, organizations need to establish an appropriate level of encryption to protect sensitive information such as PII and PHI data to prevent employee and third party related exposures and errors. Only Four percent (4%) of the 5.3 Billion records exposed since 2013 due to data breaches was encrypted and hence did not result in any negative impact.

Best Practices Managing Data Breach Risks in DevOps

1. Classify sensitive data prior to acquisition by leveraging rule-based and machine learning algorithm to detect and classify sensitive data in both structured and unstructured data prior to their extraction onto the test environment.
2. Encrypt sensitive fields while preserving format: and maintaining referential integrity . Use automated solution to encrypt field level information both in structured and unstructured data.
3. Encrypt test data at rest to add a second layer of security for non-sensitive data.
4. Encrypt sensitive data elements prior to sharing with the third party testing vendor.
5. Look for internet exposure if test server and application is deployed in the cloud.

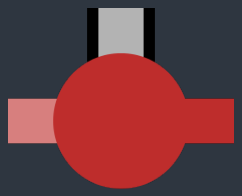
Pricchaa Solution for Test Data Encryption

1. Identify sensitive data elements automatically or using user specification
2. Encrypt sensitive data elements while preserving format and referential integrity between all source systems.
3. Maintain referential integrity throughout the project lifecycle including incremental test data
4. Decrypt test results for validation

GET UP AND RUNNING IN FOUR HOURS

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



Cross Platform Support

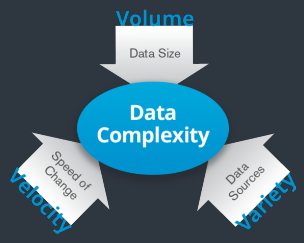
File System: Linux, Windows, HDFS, S3, SAS

RDBMS: MS SQL, ORACLE

Big Database: VERTICA, REDSHIFT, TERADATA, HIVE

Format Preserving and Referential Integrity

Encryption preserves the format and maintains the relationship between various data sources. No orphan record is created because of the encryption. Encryption keys can be stored for decryption of the test results



Built for Big Data

Designed for handling big data using commodity hardware. Architected for faster processing. Leverages advanced algorithm to encrypt and decrypt data

cloudera CONNECT Hortonworks amazon web services Partner Network Microsoft Partner