SHIELDIO

www.shieldio.com | 1-888-SHIELD-0

OVERVIEW

ShieldIO Opening Encrypted Data for Secure Search and Analytics

Reducing Risk and Compliance Complexity While Increasing Data Value

THE PROBLEM

Every organization, is faced with protecting their growing structured and unstructured data in data stores. In most cases the data contains sensitive details that need to be kept confidential while providing access based on user Role Based Access Controls. This data could be personal information that can identify an individual (PII), health information about an individual (PHI), credit or debit card details from purchases (PCI), or maybe intellectual property or other confidential data that is sensitive for the organization.

THE INHIBITORS TO COMPLIANCE

Using traditional approaches to secure structured and unstructured data, can lead to restricted access rights, with limited flexibility/availability resulting in either customer dissatisfaction limiting revenue potential or opening the data to external/internal accidental or malintent data breaches.

There are several concerns with standard encryption approaches, such as: keystore breaches, access vulnerabilities, inflexible restrictive access, lengthy implementation cycles. Some standard encryption products secure the data when it is stored in a database, however, they need to decrypt the data for use leaving the sensitive data vulnerable .

POTENTIAL COST

The costs of a data breach can be great including share price reduction, damage to a brand, dismissal of individuals, corporate and individual fines, loss of intellectual property, exposure of confidential information, and the cost of implementing customer retention tactics after a breach. Organizations cannot afford to be non-compliant.

THE SOLUTION

ShieldIO Secure Autonomous Drivers encrypts and secures your sensitive data using AES 256 without limiting data use and without breaking existing applications.

ShieldIO Secure Autonomous Drivers reduce risk of internal data breaches due to phishing attacks or malicious internal bad actors by encrypting data in use, in transit and at rest. Removing the need for a traditional keystores. Eliminating one of the major vulnerabilities of today's data encryption approaches.

With simplified implementation and deployment ShieldIO Secure Autonomous Drivers help enable regulatory requirements such as CCPA, NYCRR500, GDPR and others with zero impact on database commands.

Increasing your data value and enabling you to run all database commands on encrypted data without decryption.

WHAT IS IT?

Database Driver

> Connectivity
> Query Management
> Results Management

HOW DOES IT DO IT?

Harmonious Computing

> Distributed Processing
> Extreme Memory Management
> Separate Data/Process Access

WHAT DOES IT DO?

Resilient Data Use

> Encrypted Searching
> Encrypted Mathematics Sum
> Morphed Plain Data

WITHOUT KEYSTORE VULNERABILITY?

Enhanced Security

> Ephemeral keys means breaking AES 256 is harder
> No extra touchpoint to hack