SHIELDIO
WE MAKE DATA SECURE

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

DEVELOPER SHIELD OPENING ENCRYPTED DATA FOR SECURE DEVELOPMENT

Making dark data available for confidential access without impacting the integrity of development and testing cycles

The Problem

Sensitive information, e.g., Personal Identifiable Information (PII), Personal Health Information (PHI), Credit or Debit card details from purchases (PCI) are a part of every organization's databases. Allowing sensitive data from production applications to be copied and used for development and testing environments increases the potential for accidental or malicious internal data breaches. There are good reasons why project managers prefer to use the real production data rather than mocked data-sets when developing, testing or maintaining application code. Typically, real data provides a more exhaustive test bed and is easier to get, however, there are risks & vulnerabilities associated with exposing real production data to both internal and external local and/or offshore developers. These include exposing intellectual property, sensitive data, and data that is subject to regulations, such as GDPR. Lastly, the database's integrity and structure can be at risk when multiple testers and developers are working on changes to the same live database structure.

Concerns with Current Approaches

Current approaches to securing and managing development databases create a data inconsistency across the stages of development. This can increase the likelihood of delayed deployment and sensitive data exposure.

During the development cycle the accuracy, manageability and flexibility of the data can be negatively impact due to:

- Masking the sensitive data resulting in skewed testing and analytics
- Creating false data-sets that produce test results and analytics which are not relevant to the actual data
- Encrypting the sensitive data in such a way that hides the data from scripts producing skewed results
- Creating volatile test databases due to concurrent development access

The Solution

Developer Shield enables testers and developers both locally or offshore, access to real data for their projects, while securing and ensuring that PII, PHI, PCI or other sensitive and compliance related data is not accessible. It allows secure development with real data eliminating the need to create a mock data-set that does not properly simulate the production environment. Developer Shield protects and preserves the test data by providing each developer/tester their own local copy.

Developer Shield encrypts the sensitive data and so that it becomes impossible to be viewed in plain text. It provides full search, query and analytic access to the data, including the secured encrypted database fields, without revealing this sensitive information. Developer Shield provides these development accelerating capabilities by:

- Virtualizing the database instance across multiple desktops, meaning each tester/developer is in essence siloed, ensuring original test data is preserved
- Creating an individual virtual data-set that each developer/tester is able to utilize, change, delete, update and search, without impacting other developers /testers
- Encrypting individual database fields and/or subfields
- Enabling searching and analytics on encrypted data without the necessity to decrypt
- Removing the reliance on a crypto keystore

Developer Shield takes a complete snapshot of the live database, cloning it, while encrypting individual fields. Then the secure database is replicated and virtualized across multiple desktops, enabling individual developers/testers to work within a siloed view of the data.

Developer Shield alleviates major concerns of the DBA, developers, database modelers, testers and project managers while delivering game changing benefits

Developer Issues	Developer Shield Benefits
▪ Producing erroneous results as the developers and testers are using masked data ▪ Impacting other testers/developers by altering the live test database, e.g., developers changing the data or structure of the test database ▪ Need for ongoing DBA support to rebuild or replicate the corrupted test or development database ▪ Data breaches caused by developers and testers having access to sensitive data such as PII, PHI, PCI or data subject to GDPR that originated from production databases	▪ Safely running analytics and search across the entire (encrypted and plain) data set derived from production ▪ Offshore developers can have complete test data without the risk of exposing sensitive information ▪ Developers can develop and test with their own virtual desktop data without the risk of modifying the live test database or interfering with others ▪ Quality assurance and developers can have a comprehensive test data which can be refreshed on demand without the need for assistance from DBAs ▪ Protecting the data from internal and external data breaches due to exposing sensitive information from test data derived from live production systems