



[www.shieldio.com](http://www.shieldio.com) | 1-888-SHIELD-0

#### WHITE PAPER

# Developer Shield Enabling Encrypted Data for Secure Development

## Making 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), and 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 risk of accidental or malicious internal data breaches. There are good reasons why project managers prefer to use the real production data when developing, testing or maintaining application code rather than mocked data-sets. Typically, real data provides a more exhaustive test bed eliminating more of the bugs prior to production release. However, there are risks and vulnerabilities associated with exposing real production data to both internal, external, local, and/or offshore developers. These include exposing intellectual property, sensitive data, and data that is subject to regulations, such as GDPR.

### ISSUES

- > Producing erroneous results when 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

## MODERN ENCRYPTION:

Real time Homomorphic encryption—the Holy Grail of data encryption now ready for testers and developers—Securely use your data without decrypting— data stays secure at rest, in transit and in use.

## DEVELOPER SHIELD BENEFITS

- > Safely running analytics and search across the entire (encrypted and plain) data set derived from production without ever decrypting the data
- > Local & off-shore developers testers can test against complete test data sets without 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 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

## 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 impacted 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 development and test database structures by providing each developer/tester with their own virtual local copy.

Developer Shield is built on ShieldIO AES 256 Realtime-Homo-

morphic Encryption Secure Autonomous Drivers enabling mathematic equations, full-text search SQL statements to be executed without decrypting the encrypted fields enabling access to real production data while the sensitive data remains encrypted at rest, in transit and in use.

Developer Shield encrypts the sensitive data 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 or decrypting this sensitive information. Developer Shield provides these capabilities to accelerate development by:

- > Virtualizing the database instance across multiple desktops, meaning that each tester/developer is in essence siloed, ensuring the 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 sufields
- > Enabling searching and analytics on encrypted data without the necessity to decrypt
- > Eliminating the reliance on a secured crypto keystore

Developer Shield takes a complete snapshot of the live database and clones 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.