SHIELDIO
WE MAKE DATA SECURE

WHITEPAPER

Real-Time Homomorphic Security:

Transform Data Security with ShieldIO’s Secure Autonomous Drivers™

No matter where data is stored – in memory, on-premise, cloud, or hybrid environments – data stores are a complex mixture of data.

Sensitive Protected Health Information (PHI), Personally Identifiable Information (PII), and/or Confidential Corporate and Classified Government information, that is under legal obligation to remain secure, is routinely housed with regular business activity data (also called dark data). This dark data could yield valuable insights for an organization, but is underutilized due to legitimate legal and security concerns. In fact, data security is still viewed as an inhibitor of innovation, with 66% of IT professionals citing security as their greatest concern in adopting a cloud computing strategy.[1]

Enterprise data breaches have become an everyday occurrence and the resulting corporate financial losses have become commonplace, yet data security solutions have remained focused on policies, detection and post-breach analysis – not proactive prevention. The result is that companies place limits on data access and miss the opportunity to convert valuable data assets to insights that drive revenue and profits.

Currently, no solution in the market provides secure, flexible access to complete data stores. The lack of adequate data security solutions, coupled with the challenge of data critical to insights being housed with sensitive data, are real obstacles for organizations that could benefit from cloud integration for data access and analytics.

ShieldIO maintains the integrity of the data enabling compliance to national and international regulations, without impeding data use. We do this leveraging current cryptography methods, together with Real-Time homomorphic encryption. All without exposing a proven security threat that comes from having a Keystore and super-user access to the data.

Secure Autonomous Drivers™ from SHIELDIO are a simple-to-implement and secure solution that acts as a layer between the user/application and the back-end data, enabling comprehensive security on all stored data. Secure Autonomous Drivers™ uniquely encrypt data, mitigating internal and external threats while protecting data at rest, in transit and in use. All of this is done while maintaining database functions, searching, analytics and use of the encrypted data, which can be accessed from existing customer applications or analytics tools. With Secure Autonomous Drivers™, enterprises can securely deploy innovative applications, cloud services, and analytics that drive enterprise profits and transform data security from a cost center to a profit driving data economy without opening data to massive, widespread, and malicious security threats.

ShieldIO Secure Autonomous Drivers™ Making Traditional Data Security Solutions Obsolete?

While there are many methods for securing networks and applications and a variety of masking and encryption technologies, most of the existing solutions are obsolete and don’t actually protect data, rather they focus on putting the security in the hands of a few data admins or detection and breach analysts. These have all proven to be ineffective in protecting sensitive data, and these solutions don’t address the internal threats from an insider who has access to Keystores, storage systems, etc. that give them even more direct access to data misuse than a third-party hacker. In fact, a recent Internal Threat Report suggests that an overwhelming 90% of organizations felt vulnerable to insider attacks, with the top three risk factors enabling the insider threat vulnerability including excessive access privileges (37%), endpoint access (36%), and information technology complexity (35%).[2]

The inability of network or application level security, data masking applications and other tools to stop both the external and the insider threat means that organizations remain in a constant state of threat.

For example, most of today’s popular encryption algorithms leave open huge security loopholes for anyone with admin privileges, backdoors, the ability to attack Keystores, or are too slow for enterprise implementation. These include:

> Traditional Homomorphic Encryption is slowand requires a public key to enable search. This also means it requires a Keystore to hold the private key to enable the encryption. The person with access to the Keystore has access to your data.

> Data Masking is generally created as an intermediate layer between the data store and the user. The masking gateway accesses the data as an administrator and transforms (masks) the data on a user query, but the stored data remains in clear text and is vulnerable. Masked data impacts results as it isnot clear data.

> Transparent Data Encryption encrypts the data file on disk, stopping anybody from reading it, while it is at rest on the disk drive. However, as soon as it is loaded in to the database, it is decrypted and available to be viewed by all who have admin privileges.

> Column Level Data Encryption is generally implemented with a Keystore, which means that those with access to the store also have access to the data. However, just as importantly, if this is implemented post production, it requires wholesale changes to the database and the calling applications, leading many implementations to require data disturbance and reconfiguration with 1,000's of man hours, leading to asevere risk of project cost overrun and failure.

> Full Disk Encryption is encryption at the hardware level and works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key. This method relies upon a key holder and/or admin privilege. Anyone with key access has access to your data.

All of these systems utilize encryption Keystores to manage the decryption process. This leaves a massive hole in the organization's security, which a large number of database hacks exploit on a daily basis. Furthermore, many other solutions focus on locking down data with user permissions and added layers that render data less usable/flexible.

Data hacks no longer need to be the norm. Unlike the traditional data security solutions that rely on network or application level security, data access policies, data masking applications and other encryption algorithms that have been proven to leave open massive security threats, Secure Autonomous Drivers™ have no reliance on a Keystore. Instead, it uses an AI engine to manage the encryption process, utilizing parallel processing and High-Performance Computing (HPC), to completely mitigate any access to data by attacking a Keystore. SHIELDIO encrypts down to the sub-field level with each encryption process being handled with a uniquely derived key which is never stored, eliminating internal and external threats while protecting data at rest, in transit, and in use.

SHIELDIO Secure Autonomous Drivers™ manage the encryption process without changing the table structure or requiring database view modifications or application modifications. This enables full encrypted analytics utilization and search without compromising the security of the data, equating to quicker implementation time to securing your valuable data.

The Secure Autonomous Drivers™ solution is revolutionary in these critical ways:

> It utilizes a unique encryption processes that secures data at rest, in transit, and in use

> It enables encrypted data to be searched, understood and generate analytics without a performance penalty or the need to ever decrypt it the data

> Protects sensitive data from external and internal threats without changing the data structure or requiring policies

> Data stays secure no matter where it is stored: in memory, on-premise, Cloud, or hybrid environments

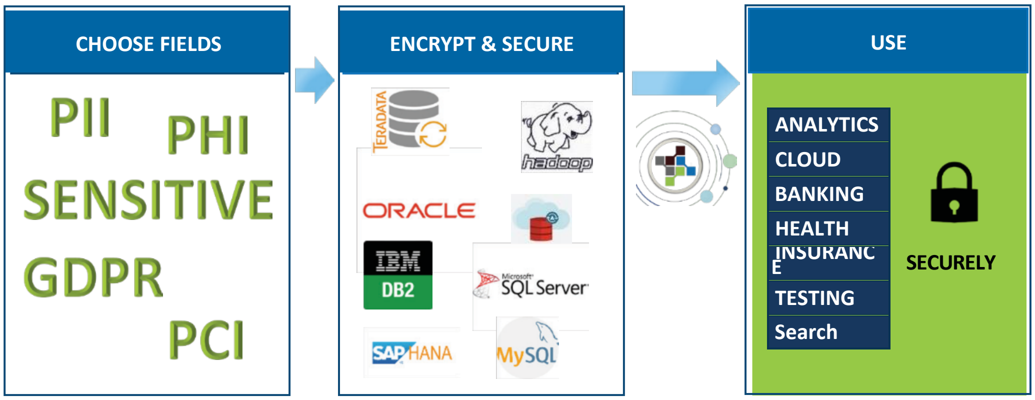
> It is easy and fast to implement: no changes to the underlying database structure, access rights or applications

With Secure Autonomous Drivers™, not only are breaches preventable; it drives the innovation and insights that lead to growth by providing secure and flexible data access.

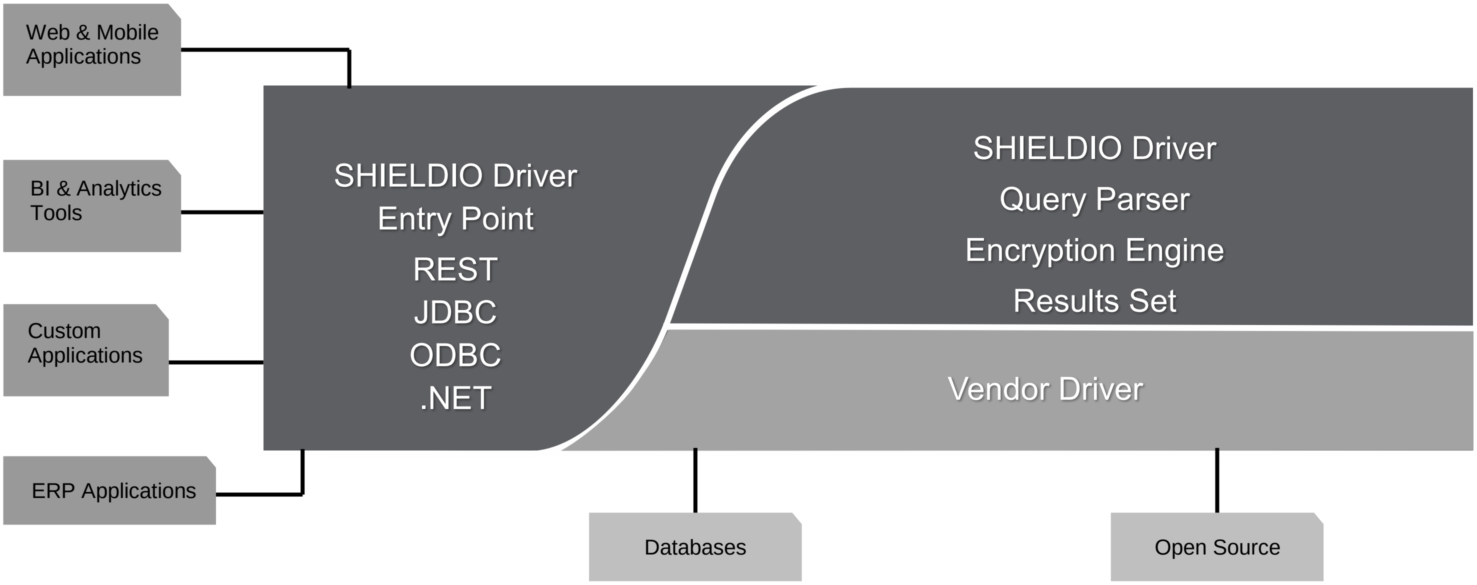
SHIELDIO Secure Autonomous Drivers™ How do they Work?

Secure Autonomous Drivers™ are installed as standard JDBC, ODBC, or .NET drivers and reside between the applications/users/edge devices and the database. Secure Autonomous Drivers™ work directly on the database without requiring calling message alteration. SHIELDIO Secure Autonomous Drivers™ manage the data sources, choosing which fields must be serviced from which data source (original or secured). It passes queries across to relevant sources, and when results are returned based on the callee having the required database/ application level permissions, it will reconfigure the data results, bringing all the sources together. The Secure Autonomous Drivers™ then decrypt where possible or required, passing a single result set to the callee.

Secure Autonomous Drivers™ Use Case Diagram



Secure Autonomous Drivers™ Architecture

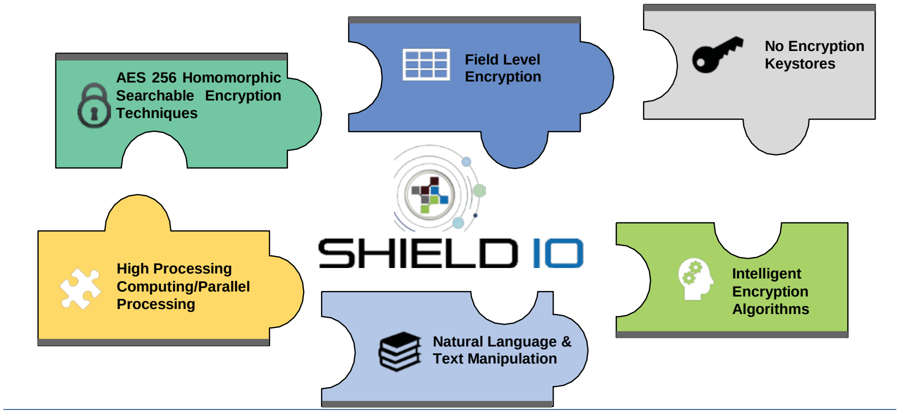


The Groundbreaking Technologies of ShieldIO Secure Autonomous Drivers™

Let's take a deeper look at the unique technologies that comprise the powerful Secure Autonomous Drivers™ solution:

The SHIELDIO Security Engine

The SHIELDIO Secure Autonomous Drivers™ offer a breakthrough in data security primarily because they utilize Keystore-less encryption driven by Artificial Intelligence to eliminate the obsolete paradigm around traditional data protection using Keystores. Each encryption process is managed using AI algorithms for a uniquely derived, in-memory key that is never stored, thus protecting data at rest, in transit and in use. Secure Autonomous Drivers™ dynamically encrypt and protect sensitive data without changing the underlying structure, access rights, or application access. Using SHIELDIO Secure Autonomous Drivers™ eliminates the ability for a hacker to access a Keystore, and thereby access to the database.


AES 256 Homomorphic Searchable Encryption Techniques
Field Level Encryption
No Encryption Keystores
SHIELD IO
High Processing Computing/Parallel Processing
Natural Language & Text Manipulation
Intelligent Encryption Algorithms

Utilizing multiple patent pending algorithms, the Encryption Engine manages asynchronous and synchronous AES encryption and the Byzantine Fault Tolerance algorithms. Every data piece is uniquely encrypted down to the sub-field level and each field or sub-field has a unique key. The AI engine selects how to make up the key. The keys are created with different algorithms by the system. Each call uses cryptographic random generation to allocate which AI algorithm to use. The algorithm will be used to create the content that generates the derived key using the AES 256 encryption from the CryptoPP library. The content that the derived key is built from is drawn up via 12 separate items, again using a cryptographic random generation, and is mangled prior to being used to develop the derived key. This means that should anyone hack the code; they would have to do the following on each encrypted item. *(Each field is encrypted with a unique key)*

1. Work out which items were used to create the derived key.

2. Work out which algorithms were used to mangle the byte array.

3. Work out in which order these have been placed. This is a sum equivalent to 12 items multiplied by itself and again by 6 so (12^12)6. That's nearly fifty-four trillion possibilities and far and above any other encryption solution in market. This enables us to never repeat key positioning and never form a pattern.

This would have to be done for each item that has been encrypted and will be unique to each, whether that is a field, a sub-filed or an internal message. With each system having unique identifiers that the system uses to create the derived key, it would be near impossible to recreate it in order to hack the database in its entirety as demonstrated above. Now, instead of having a single point of access to gain entry to the data, each field or sub-field is a separate access point, making an internal or external threat's job much more difficult, time consuming and expensive. For example, a Social Security Number can be broken up into three sub-fields and encrypted using three AI derived encryption keys which evaporate.

Real Time Homomorphic Encryption

Using Real-Time Homomorphic encryption and Secure Memory Management, the Secure Autonomous Drivers™ are able to carry out the same level of calculations that a database is capable of doing. This includes: SUM, AVG ADDITION, MULTIPLICATION, SUBRTRACTION and AGGREGATE queries. This allows applications and users to run SQL queries on encrypted data to search, applications to run analytics, or gain access to unsecured data based on secured information.

AI Algorithms

Secure Autonomous Drivers™ utilize an Artificial Intelligence (AI) engine to manage the underlying encryption process, thus completely eliminating both an external hacktivist or an internal malcontent employee's ability to access data by infiltrating and stealing the highly susceptible Keystore. Each encryption process is managed using AI algorithms for a uniquely derived, in-memory key that is never stored. The keys are created with different algorithms by the system. Each call uses a cryptographic rand to allocate which algorithm will be used to make the content that moves on to be used to create the derived key, and the AI engine selects which key to use.

High Performance Computing Method

The Secure Autonomous Drivers™ harness High Performance Computing (HPC) methodologies to power the AI processes and, along with the application of parallel processing, enable the system to scale while securing. Because of this, the SHIELDIO Secure Autonomous Drivers™ can utilize available memory and CPU's to their full permitted upscaling with the addition of hardware resources, thus enabling the system to be scaled to any database size.

Advanced Search Algorithms

Utilizing different search algorithms, Secure Autonomous Drivers™ are able to access data quicker than other systems and return only the results required. It can place a full-text search or SQL query on encrypted data without a decryption prerequisite. This allows applications and users to run SQL queries on encrypted data to search, allowing applications to run analytics, or gain access to unsecured data based on secured information.

Natural Language Understanding (NLU)

Secure Autonomous Drivers™ relies on NLU to manage from where the service needs to access data and is critical to ensuring the solution runs properly.

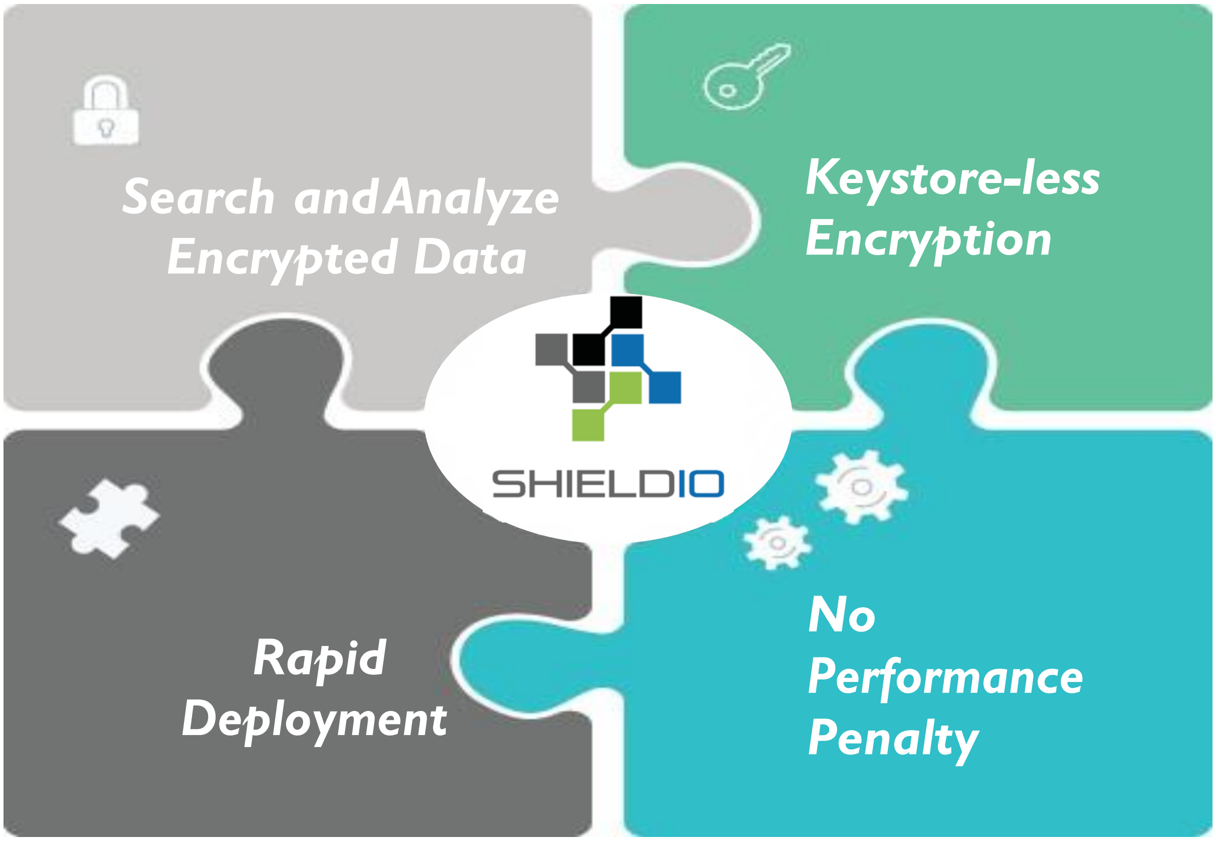
It works like most human brains work. When a request comes in, it determines if it is a command or question, then it does entity recognition, looks and finds the answer from the correct database(s), performs any additional processing math, and then formats the response and passes it back. This negates the need for convoluted learning processes in advance and makes data usable as quickly as it is accessible.

Fuzzy Search Logic

The patent pending Fuzzy engine takes previous results and creates a 'fuzzy' search, enabling matching of data that would not have been found on the initial pass.

Conclusion

Secure Autonomous Drivers™ from SHIELDIO are a data security solution unlike anything else on the market today. The technology has the power to change how enterprises interact with their data across all databases: in memory, on-premise, Cloud, or hybrid environments and impact every industry today. It offers a secure solution for enterprises to get complete data access and visibility, but most importantly, doing it with the security and control that enterprise customers demand. By utilizing deep memory management, in-memory application storage and processor parallelization, SHIELDIO is able to encrypt at field and sub-field levels without loss of application performance, as well as enabling the application to run without compromising scalability. Additionally, Secure Autonomous Drivers™ are cross platform, meaning they can run on different processor types, server, cloud services as well as embedded Industrial Internet of Things (IIoT) devices.



Search and Analyze Encrypted Data

Keystore-less Encryption

SHIELDIO

Rapid Deployment

No Performance Penalty

RESOURCES

[1] www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#7f382cfb6261

[2] www.csoonline.com/article/3238867/2018-crowd-research-partners-insider-threat-report-hopes-and-fears-revealed.html