REPORT REPRINT

ShieldIO offers encryption-in-use, minus the challenges of homomorphic encryption

OCTOBER 31 2019

By Garrett Bekker

The company has attempted to 'modernize' homomorphic encryption technology by leveraging standard AES 256 libraries and 'extreme memory and processing management' to deliver encryption-in-use for databases.

451 Research®

Introduction

In a sense, modern enterprises and data security are directly at odds. Security measures such as encryption can be inconvenient, but most importantly, encrypted data typically can't be used unless it is decrypted at some point, which makes the data vulnerable. The result of this conundrum is that firms will frequently leave data unencrypted and bear the risk of exposure.

ShieldIO is one of a handful of firms that have emerged recently to address what is commonly referred to as encryption-in-use. The essential idea is to allow operations to be performed on encrypted data without ever decrypting it. There are several ways to provide such 'magic,' including using secure enclaves like those provided by Intel's SGX technology, secure multi-party computation (SMPC) and homomorphic encryption (HE).

One of the main challenges with HE is that the mathematics are impractical and require massive systems to run, so HE has historically been constrained to research and very limited commercial applications. ShieldIO has attempted to 'modernize' HE technology with what it calls 'Harmonious Encryption,' leveraging standard AES 256 libraries in lieu of HE libraries, along with 'extreme memory and processing management' and separation of components.

451 TAKE

ShieldIO's goal is to protect users' data while simultaneously letting firms use it, but without the massive IT overhead or performance issues that are typical with HE. The decision to deliver HE via standard AES 256 libraries and a driver that can work on small web servers to massive Hadoop systems without extensive hardware implementations is clever, and dovetails well with a focused go-to-market strategy targeting database security and cloud-migration use cases. That said, ShieldIO is a very early-stage startup in a market that has yet to show broad commercial adoption, despite substantial interest.

Context

ShieldIO is headquartered in Reno, Nevada, and was founded in September 2018 by CEO AJ Jennings (previous roles at Citrix, Cisco and Brocade) and CTO Simon Bain. The company recently emerged from stealth mode, and currently has about 10 employees.

Products

ShieldIO recently came to market with its Autonomous Data Security technology that can search and do mathematical equations on encrypted data within a database without needing to install any servers or gateways. The core of its offering is the ShieldIO Secure Autonomous Driver, which can run on a wide variety of platforms – from a Raspberry Pi to a Hadoop cluster – without any need to make changes to the underlying database.

The driver essentially intercepts database queries, manipulates them and passes them to the database driver. The database runs the query and passes the results back to ShieldIO to manipulate the results within the driver, including decrypting the results, changing the metadata or performing operations (such as sums or averages), and then passes the results on to the user. Data is only ever decrypted in memory within the driver, and then passed to the application that is calling it (if it has rights for it). Configuration is done via a JSON file that tells the application which fields to encrypt or which fields to perform mathematical operations on.

In terms of performance, ShieldIO claims to have eliminated the performance bottleneck associated with HE with what it calls Harmonious Encryption. This involves breaking down the various compute components – database connections, query connections, memory and processing – and optimizing them with 'extreme' memory and processing management.

ShieldIO also does not rely on centralized key stores that can serve as a valuable asset for attackers to target. Keys are created using standard AES 256 crypto libraries in combination with proprietary algorithms that take random inputs from the surrounding environment – the system, the network, etc. – and format them into a $(12\wedge12)^6$ matrix that is used to create keys. All keys are salted and hashed, and most importantly, dissolved immediately after use.

ShieldIO offers two main products: SecureShield and DeveloperShield. SecureShield is the main product and provides full encryption-in-use capabilities. DeveloperShield is for test and development use cases that allow for the same calculations as SecureShield, but upon 'morphed' data that is mathematically impossible to decrypt. The goal is to provide developers with realistic data without ever exposing the data to them.

Strategy

Vendors providing encryption-in-use technologies differ widely in terms of both the underlying technology and the various use cases they address. ShieldIO is focused squarely on database encryption, and views its technology as complementary to standard transparent database encryption or column-level encryption available from vendors such as Oracle, Micro Focus, Protegrity or Thales.

In terms of go-to-market strategy, ShieldIO will rely heavily on three types of partners: database vendors, resellers and distributors, and consulting partners. With respect to database vendors, ShieldIO will target existing database customers that have on-prem databases they wish to migrate to the cloud but are concerned about security. ShieldIO is now available via the Oracle Marketplace, and we anticipate the company will pursue similar arrangements with other cloud providers, such as GCP or Azure.

ShieldIO plans to focus on securing structured data in traditional databases and big data (Hadoop, Hive, Impala, Greenplum, MongoDB, etc.), and currently has co-selling deals with Oracle and Teradata. ShieldIO supports MySQL, PostgreSQL and any database that interacts with JDBC drivers, with drivers for ODBC, OLE and .NET in the works. The vendor also plans to release an SDK that will let enterprises build their own drivers for applications or databases that ShieldIO doesn't directly support.

ShieldIO is also working with distributors like Arrow to deliver HE as a complement to customers that have new projects but may already have column-level crypto from the likes of Protegrity or Micro Focus. In addition to its partner focus, ShieldIO is also doing direct-to-enterprise sales, and sees the SMB market as an underserved opportunity.

Competition

ShieldIO sees traditional data-at-rest encryption vendors such as Micro Focus, Protegrity, Thales or PKWARE as potential competitors, although we see the latter as more complementary and potential partners since they all lack HE. We see ShieldIO as more directly competitive with an emerging group of encryption-in-use vendors, some of which we have detailed in prior reports (Enveil, Fortanix), that use a variety of approaches ranging from secure enclaves to SMPC to HE. Vendors in this category are essentially a loose coupling, since they differ widely not only in terms of the underlying technology, but also the problems they are looking to solve, ranging from database and email encryption to key management.

In the secure enclave camp, the leading proponents include Fortanix and Microsoft's Azure Confidential Compute offering. Vendors offering secure multi-party compute technology include Israel-based Unbound (formerly Dyadic), US-based Baffle, InPher and Preveil. ShieldIO is likely to be most competitive with encryption vendors attempting to provide a new take on homomorphic encryption, including Duality and Enveil.

SWOT Analysis

STRENGTHS

ShieldIO has the ability to do search and math on encrypted data without ever decrypting it or using key stores. Its software driver-based technology helps avoid the cost and management overhead of extensive hardware and software implementations.

WEAKNESSES

ShieldIO is a very early-stage startup in a market that has yet to show broad commercial adoption, despite substantial interest. ShieldIO currently has a JDBC driver, with drivers for ODBC, OLE and .NET in the works.

OPPORTUNITIES

Its focused go-to-market strategy targeting database security and cloud-migration use cases could lead to traction with large database vendors and cloud providers.

THREATS

Most database vendors eventually acquired or built their own encryption technology, and should they do the same with HE, it could cut off ShieldIO's primary route to market.