ceocfointerviews.com

Issue: October 14, 2019

CEOCFO Magazine

ShieldIO is enabling Organizations to Perform Search on Encrypted Data without Decrypting It using their revolutionary patented Real-Time Homomorphic Encryption™

AJ Jennings
Founder and CEO

ShieldIO
www.shieldio.com

Contact:
ShieldIO, Inc.
888-744-3530
info@shieldio.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

"ShieldIO provides cyber resilience through our patented Real-Time Homomorphic Encryption™; which put simply is the ability to run a mathematical process on encrypted data without decrypting it."- AJ Jennings

CEOCFO: ***Mr. Jennings, the first thing I see on the ShieldIO site is "Cyber Resilience For Today's Data." How are you providing that?***

Mr. Jennings: ShieldIO provides cyber resilience through our patented Real-Time Homomorphic Encryption™; which put simply is the ability to run a mathematical process on encrypted data without decrypting it. This method unlocks the ability to enable data encryption-in-use and becomes irreplaceable to organizations looking to gain valuable data insights from regulated or secure data. For example, in a data research scenario, companies need to understand a certain segment of information, but you don't want to expose plain text data such as personally identifiable information (PII), private healthcare information (PHI), credit card transactions (PCI) or other secure data. Researchers need access to the output of the data query but not the exposure of the data behind the query.

ShieldIO has enabled organizations to perform search on encrypted data without decrypting it. We are delivering this capability through what we call Secure Autonomous Drivers. The drivers are a standard database, JDBC, ODBC, .NET, EF and other database drivers that reside next to the existing database driver and manage the encryption, query parsing, and all of the pass-through from the application to the database and back, without the need to decrypt the data.

CEOCFO: ***What was the biggest challenge in creating this solution?***

Mr. Jennings: Many different types of Homomorphic Encryption have existed in academia and think tank science labs for going on thirty years. All of these iterations of Homomorphic Encryption have a couple of

different issues with them. One is that they are incredibly latency intensive from a compute infrastructure standpoint. It takes a tremendous amount of computing power to process searches on encrypted data. When the first homomorphic algorithms came out, they were one hundred trillion times slower searching encrypted data than searching decrypted data. Over the years, companies like IBM, Microsoft, and others, in their labs, have reduced that latency down to about fifty thousand times slower in searching encrypted data than searching decrypted data. Even with these advancements, Homomorphic Encryption was still unusable in a real-world datacenter, however.

ShieldIO has overcome that hurdle through our patented memory management. We attended an Oracle event last year, where we demonstrated searching an Oracle database that was encrypted faster than searching the same decrypted Oracle database. We have taken Homomorphic Encryption out of the science lab and put it into practical production environments. That was one of the biggest hurdles; overcoming that memory management problem of latency on the encrypted search that has plagued what many people call the 'Holy Grail' of encryption.

CEOCFO: ***Are people surprised and skeptical even though you are showing them that it can be done?***

Mr. Jennings: Yes, we get a multitude of jaw-dropping, "Okay, how did you do that" or "I do not believe it" or "How is that possible," statements from customers, partners and analysts alike. Therefore, yes, we do get many skeptics. We were just at Oracle OpenWorld, where Larry Ellison announced that Oracle was reselling ShieldIO as part of their Oracle Cloud Infrastructure third party paid listings, and even then, people that would come by the booth still did not believe that we could do a real-time search on encrypted data without decrypting it. People have to see it.

When you talk to people that are deep in security and encryption, they understand column level encryption; they understand data masking and tokenization and the multitude of other methodologies that have existed for thirty plus years. They still find it hard to believe that someone has finally cracked the code of being able to search encrypted data in real-time without decrypting it.

CEOCFO: ***Who is using ShieldIO? Who should be using ShieldIO?***

Mr. Jennings: As CEO, I'm obligated to say everybody should! However, realistically, we have focused deployments in the healthcare, e-commerce, and financial markets where PII, PHI and PCI data are highly regulated yet the need to monetize that data is critical. We hear about data breaches daily in the financial and healthcare community, so obviously, that is an area where we target and play very well. Those three segments are certainly the sweet spots for ShieldIO.

Other areas of focus are in insurance, research, and IOT. Just think about the volume of private data these endpoint devices generate. That data requires end-to-end encryption and use, so that's an area we're working on with partners and watching very closely.

CEOCFO: ***Are there different solutions for different industries or is it one basic solution with some tweaks?***

Mr. Jennings: That is a good way of categorizing what we've done. We believe in a platform approach vs. a multiple point product engineering effort. As such, we've built a platform based on our Real-Time Homomorphic Encryption™, called the Autonomous Data Security platform, and everything else that we do builds from that.

While that sounds simple, it's far from a trivial effort. There are many nuances involved in delivering our targeted products for analytics; working with multiple databases; enabling different application sets, and so on. However, this effort has enabled ShieldIO to be both database as well as application-agnostic in terms of our deployment capabilities. We do not discriminate as to what type of database you have as we deploy as a database driver, so we work with all of them. We work with almost all applications as well, whether you're using Tableau, Good Data, Oracle Analytics, or Microsoft BI; again, we do not discriminate here.

Additionally, we are location agnostic. So, whether your environment is on-premise, in the cloud, or you have a hybrid model, which most people have today, we enable data encryption-in-use for all environments. ShieldIO works with Google, Amazon, Oracle, Microsoft, and a multitude of other cloud platforms, as well as most all the on-premise database architecture and application suites that you will find out there.

CEOCFO: ***With seemingly limitless potential, where are you focusing your efforts? Who is you reaching out to you? How are you reaching out?***

Mr. Jennings: We are going to market primarily through our partners and focused on the predominant cloud ecosystem vendors and their customers. It is much more cost-effective for ShieldIO to manage a partner like Oracle, where they have thirty thousand salespeople with active customer needs vs. ShieldIO investing in its own direct salesforce.

Today, we are going to market through Oracle, Teradata, Arrow Electronics, and multiple resellers and managed service providers. We have other top tier cloud vendors that will announce they are reselling ShieldIO soon.

CEOCFO: ***Is this easy for the resellers to understand? Do technical people understand, or is there a certain amount of education for the people that might be presenting to the end client?***

Mr. Jennings: There are two levels of education that I see. One is at the thirty thousand foot view, for the general business and technology consumer. What they see are the four and one half billion data breaches that occurred in 2018 but what they feel is, "When I went to Home Depot, all of my credit card information was stolen, and I had to cancel my credit card." Others read about or are impacted by very public breaches like Capital One and Amazon Web Services. People experience these emotionally and financially driven issues daily and wonder, "Why is that happening, how can my data be protected?"

At the technical level within organizations, the DBA experiences that jaw-drop moment we spoke about earlier. That is the "I do not believe you can do that, how did you accomplish it, that is impossible" moment, and the hurdle there is you have so many corporate and industry pundits.

Strangely enough, there are CEOs of companies we consider competitors that have tried their hand at Homomorphic Encryption and failed but are out publishing articles on why Homomorphic Encryption will never be implemented in the real world data center. Enter ShieldIO, where we tell the technical teams, “Now you have the ability to never decrypt the data and enable encryption at rest, in-flight and in-use.” That’s when the DBAs get the technology and value behind what we’re doing.

CEOCFO: ***Where does price come into play? How do you find the right price point and what has been the response to your pricing?***

Mr. Jennings: Our total cost of ownership is far below who we consider competitors in this space. Most security vendors sell breach mitigation and professional services and offer encryption as sort of a side note. We do not do that. We do not require lengthy professional service engagements or modifications to the database or applications to deploy our product. It takes a matter of hours or days, not weeks or months or years to implement ShieldIO.

ShieldIO is exceptionally price-competitive from a simplicity of deployment and technology perspective. We are a true disruptor in our space. It is one of the reasons that Oracle announced ShieldIO as a resold partner product for OCI. Oracle knows that our encryption-in-use solutions are a catalyst to help convert their four hundred thousand Oracle on-premise customers to OCI and Autonomous Database. dOne of the biggest barriers to cloud migration has been security. People do not believe that their data is going to be secure in the cloud. We can help alleviate these concerns for Oracle and other cloud vendors customers.

CEOCFO: ***What surprised you as ShieldIO has developed and come to the point where you are today?***

Mr. Jennings: So many things have surprised me! What continues to shock me daily is more about the market though. As you can imagine, as CEO of a cybersecurity company, I get a veritable plethora of newsfeeds in the morning. When I wake up, I see ten new breaches that took place overnight by some nation-state or individual hacker organization and it’s sickening to me. Think about what happens when a breach happens. Amazon and Capital One announced a massive record breach; I believe it was near one hundred and sixty million users that had their data breached. We heard about it, we read about it in the news and then the next day it was gone! We forgot about it! Even if you were a Capital One customer, you forgot about it.

There is a complacency that exists in the market, even though these things happen daily, and that is just absolutely overwhelming and astonishing to me.

CEOCFO: ***Why look at ShieldIO? Why is this the answer for cybersecurity?***

Mr. Jennings: ShieldIO is a departure from traditional data security and encryption methodologies. Real-Time Homomorphic Encryption™, again, has been penned as the ‘Holy Grail’ of encryption methodologies, yet it has never been brought to market as latency issues have plagued it. ShieldIO has solved this problem for the database administrator and the

data center in general. Enabling data for insights in real-time while maintaining its encryption without decrypting it is a tremendous advancement in capabilities and that's why ShieldIO will be successful in this data-driven economy.