REPORT REPRINT

Encrypt, tokenize or mask? ShardSecure offers a new take on data security: 'microsharding'

APRIL 23 2020

By Garrett Bekker

The emerging data security provider was founded on a fairly simple premise: Split sensitive data into tiny pieces and distribute them across multiple locations so that the individual pieces are meaningless in the wrong hands, a process known as 'sharding.'

451 Research®
Now a Part of
S&P Global Market Intelligence

Introduction

It's no secret that the pace of data breaches continues practically unabated. Not surprisingly, there has been a steady stream of new data security technologies coming to market that aim to help reduce the threat of data breaches as well as deal with the growing assortment of data privacy regulations and mandates around the globe, such as GDPR and CCPA. ShardSecure is an emerging data security vendor that was founded on a fairly simple premise: Split sensitive data into tiny pieces and distribute them across multiple locations so that the individual pieces are meaningless in the wrong hands, a process known as 'sharding.'

451 TAKE

The concept of sharding is not new and has been applied primarily in storage applications to improve the I/O performance of RAID arrays by allowing for parallel processing of separate shards of data. ShardSecure has applied this principle to security, with an added twist that allows for less latency via 'microshards' that can be as small as a few bytes, as well as a variety of optimization techniques. The company can also work across hybrid environments, with support for on-premises instances as well as multiple public clouds and cloud file shares such as Box and Dropbox. It has a seasoned management team and some high-profile backers that should help open some customer doors. ShardSecure's initial challenge, in our view, will be how to position itself within the broader data security ecosystem, and help customers understand how microsharding can complement existing data obfuscation techniques like data masking, encryption and tokenization.

Context

New York City-based ShardSecure was founded in 2019 by several security industry veterans with experience at Bayshore Networks, Novell, Netegrity (acquired by CA Technologies in 2004) and early identity-as-a-service vendor Nordic Edge (sold to Intel in 2011). The vendor is run by CEO Bob Lam, who previously cofounded IoT security pioneer Bayshore Networks and held multiple executive roles, including COO. Nordic Edge cofounders and Netegrity veterans Jesper Tohmo and Christer Roslund serve as CTO and VP of engineering, respectively, while former TD Ameritrade CTO Lou Steinberg is chairman.

ShardSecure recently secured $2m in seed funding led by SineWave Ventures, with participation from Sweden-based early-stage VC Industrifonden, Internet Security Systems and JouleX CEO Tom Noonan, 500 Startups, and others. Along with Noonan, former Secure Computing CEO John McNulty sits on ShardSecure's advisory board. The company has a pending patent on its performance and resiliency features applied to security use cases. 451 Research estimates that ShardSecure has less than 20 fulltime employees.

Products

In simple terms, ShardSecure breaks data into small bits and 'scatters' them to various local and cloud-based storage locations to make it nearly impossible for attackers to access the data. The company can also distribute fake shards to make it theoretically more difficult for an attacker to reassemble the shards.

In terms of architecture, ShardSecure can be deployed either on-premises or in the cloud; as a virtual appliance that sits in front of a storage array or a blade in a storage appliance, database or mounted disk system; or as a VM image (VMI) in front of an AWS S3 bucket or object storage from Google Cloud Platform (Cloud Storage), IBM (IBM Cloud Object Storage), Microsoft (Azure Object Storage) or Oracle Cloud Infrastructure. To distribute the shards, the vendor has created drivers for each cloud supplier.

ShardSecure also has a rules engine that determines how and where to distribute the shards, the size of the shards, etc., to give customers control over where the data goes. The size of the shards can depend on the data type – for example, streaming video files might become bigger shards than text files. Data can be streamed up and down, and the vendor utilizes caching and compression techniques to minimize latency and accelerate performance.

To reassemble the shards, ShardSecure deploys pointers within its VMs or VMIs that determine where the data resides and reassemble the data into its original form providing that the requesting party knows all of the locations where the data has been distributed and has access to them. Additionally, the company tokenizes these pointers for an added layer of security, which provides for reduced latency since tokenization effectively compresses the pointers. It's also important to note that these locations are unrelated and not known to each other.

ShardSecure could potentially serve as an extra layer of security on top of existing encryption tools. One potential weakness of encryption is that if the keys are ever compromised, either via a rogue insider or somehow during a breach, the attacker gets full control of the encrypted data. ShardSecure can serve as an extra layer of protection for encryption by microsharding the encryption keys, which would make it nearly impossible for an attacker to reassemble. The vendor supports a variety of both structured and unstructured data types, including files, databases and streaming data, as well as cloud file-sharing systems such as Box and Dropbox.

Strategy

ShardSecure is pursuing several go-to-market routes, including selling subscriptions directly or indirectly via strategic technology resellers and VARs to enterprises in key verticals such as financial services, healthcare and government, as well as offering a SaaS product through AWS Marketplace or other online marketplaces. The company could also pursue OEM relationships or partnerships with established storage or cloud vendors, perhaps with data security providers as an alternative to standard encryption. We also see an opportunity to position ShardSecure as a compliance play for enterprises dealing with privacy mandates and seeking a way to lower the sensitivity of the data and perhaps take them out of scope for regulations such as PCI, HIPAA and GDPR.

Competition

Since microsharding is a relatively unique approach to securing data, one could argue that ShardSecure has few direct rivals. To the extent that microsharding is viewed as an alternative to standard encryption, ShardSecure could vie indirectly with established encryption vendors such as Thales (Gemalto), PKWARE and Micro Focus, many of which also provide tokenization, although they could be potential partners as well. Additionally, ShardSecure could be considered an alternative to data masking and data obfuscation offerings like BizDataX, IRI FieldShield, Privacy Analytics (IQVIA) and Solix, as well as larger firms with masking capabilities such as Broadcom (CA Technologies), Dataguise, Delphix, HPE, IBM, Imperva (Camouflage Software), Informatica, Microsoft (Blue Talon) Oracle and Protegrity. We have also detailed the rise of encryption-in-use providers such as Baffle, Duality, Enveil, Fortanix, Inpher, Preveil and ShieldIO that allow operations to be performed on encrypted data and analytics models, often for privacy and compliance purposes.

SWOT Analysis

STRENGTHS

ShardSecure has a veteran management team with high-profile backers, the ability to protect data with less overhead than standard encryption or need to modify applications, and support for multiple cloud offerings as well as Box and Dropbox, etc.

WEAKNESSES

ShardSecure is early stage and looking to establish a niche within the broader data security sector.

OPPORTUNITIES

To the extent that microsharding can render PII non-sensitive, ShardSecure could help companies reduce compliance costs by taking data out of scope for privacy regulations like GDPR, HIPAA, CCPA, SOX, etc. Microsharding could also serve as an alternative to encryption without the associated challenges of key management and overhead.

THREATS

Large data security and data management vendors typically offer a variety of data obfuscation techniques that may be viewed as sufficient for many enterprise needs.