UHY Advisors
Tax & Business Consultants

UHY Advisors NY, Inc.

1185 Avenue of the Americas, 38th Floor
New York, NY 10036-6101

Phone 212-381-4700
Fax 212-354-6445
Web www.uhyadvisors-us.com

Microsharding a high performance alternative to current data protection

By Warren Zafrin, UHY Advisors June 2019

Our world is in a constant state of change. Our society has become a canvas of digital points of business data and personal information. In this new era of personal and professional interaction privacy has become next to impossible. In this state of constant change one factor continues to remain constant, if a nefarious source wants our data they can obtain it. Our information is spread between our personal computers, visited websites, cloud providers, and commercially “trusted” sources. However, if a “Hacker” gains access to anyone of these sources they have the ability to compromise our information and decrypt all personal information let us call it our digital DNA. Furthermore, in this new age of readily accessible computing power cybercriminals have the resources to exploit our vulnerabilities and steal our data. Empowered with advanced computing power and time, cybercriminals can steal our encryption keys and decrypt even our encrypted data. If advancements in computing power continue to progress at the current speed today’s cryptography has the potential to be rendered useless and expose not only current data but enable the decryption of previously stored messages.

This paper aims to assess the potential impact of protecting data using ShardSecure’s Microshard technology as opposed to current methods. It does so by describing an alternative data protection strategy with possible advantages over encryption. The insight has been gained from technical evaluation, in-person interviews and secondary sources (articles, books, reports, blogs and white papers). Importantly, the paper makes an implicit underlying assumption that there will still be a need to protect personal as well as commercial data and there will always be cybercriminals wanting to steal the data.

Effectively managing data loss continues to be a challenge for companies across regulated industries, and especially those in financial services. This is in part because data protection is generally approached differently across companies. Varying protection requirements and sharing policies are deployed across a wider range of applications. For example, in application development it is acceptable to use different storage mediums, communication process and data sizes. Sharing data today is measured on ease of accessibility (cloud vs. on premise), platform compatibility (SharePoint vs. SMB), and the ability to meet current standards and frameworks based on whether there is an identifiable vulnerability or regulatory mandate (GDPR vs. NYS DFS).

Governments have significantly increased their focus as the protectors of data and through regulation have substantially raised compliance costs of data. The New York State Department of Finance has determined data protection as the number one threat within their jurisdiction and has made cybersecurity compliance, and the encryption of data mandatory as of March 1, 2019. As a result, companies are engaging in data diversification. Companies are developing strategies that avoid excessive data concentration because of the associated risks in case of a data breach or loss. As a result traditional cybersecurity measures remain no match for the increasing sophistication and pace of cybercrime.

When it comes to security and data protection there is no such thing as sure thing. There are solutions however that make it not worth the effort for the most sophisticated cybercriminal to steal the data. ShardSecure's data protection is one of those protection strategies that make the criminal look for easier prey somewhere else. When it comes to modern data protection standards, ShardSecure, in practical terms, makes it almost impossible for cyber criminals to benefit from stolen data. Quite simply, it is because the technology makes the data uninterpretable even if the criminal is capable of finding and hacking into stolen data.

Encryption remains a popular way to secure information on the web, on our personal computers and on our enterprise storage systems. That doesn't mean encryption is always the right solution. There are benefits and disadvantages to using encryption. Most users are familiar with encryption software but unfamiliar with Microsharding.

There is very little doubt that encryption is a strong data protection method. Encryption uses strong cryptography algorithms protecting all data stored on the media or in transit. If the data is stolen from the current user or system the data is still inaccessible if without a correct key. With the advances in computing power if the cybercriminal has the resources and desire to decrypt the data, making use of stolen private keys with the right motivation a cybercriminal can decrypt the data. In the case of encryption, every time when you try to read the data, the authentication key is demanded to decrypt data. In the case of transmitting encrypted data the messages are larger and require additional processing power to forward. Encrypting data at-rest or in-transit slows down computing either from your computer or the network resources. Encrypted data is also difficult to recover if the encryption keys are damaged or lost, making the data secure but also rendering it useless in case of recovery.

ShardSecure partitions the data into small binary datagrams (down to single-digit bytes), creating microshards of data which can be dispersed to various storage locations including local disks and multiple cloud providers. The platform consists of a microsharding engine that is configured and driven by policies. The policy engine is configurable by the administrator determining not only the size of the microshard but the location as well. Locations are determined through policies both directing where to save the microshard but also based on context of how large the microshard should be. The larger the microshard the greater the performance while smaller microshards increase the security of the data. The next version of the platform will also incorporate policy-based sharding driven by the content of the data as well as the context. Microshards can be shared across multiple locations including local storage as well as cloud storage. The dynamic microsharding engine receives the data through a RESTful API, queuing the data in RAM and then sending the information to the thread engine that distributes the microshards across the data stores. Thread engines can be configured to balance the load of the microsharding as well as dynamically take the load if one of the engines goes down. Through the policy engine data can be directed to remain within geographic and regulatory boundaries. Overall the ShardSecure's technology platform makes it impractical and very difficult for hackers to find and break into the locations of the microshards and find the pointers to reassemble. This makes microsharding an interesting technology to protect sensitive information such as personal identifiable information (PII) because the microshards cannot be identifiable or traced back to the original data forms. On the future roadmap is the ability to duplicate microshards for disaster recovery as well as increase performance in real memory to make microsharding databases possible with no performance hit.

In practice, sharding is traditionally complex however ShardSecure and their policy manager engine takes most of the complexity out. ShardSecure shards the data automatically once the policy engine is set up. This makes the microsharding and user interface independent from the data storage. Applications, webservers video and in the future databases can securely spread their data across local storage and cloud providers without the overhead of traditional encryption.

ShardSecure’s technology can be layered on top of encryption to create defense in depth for the most sensitive data. Operating alone without encryption, the technology eliminates the costs and overhead to manage encryption keys while maintaining strong protection of data. Microshards as tiny as single-digit bytes are not readable or identifiable without ShardSecure’s reassembling technology. This makes ShardSecure a solid data protection alternative to encryption but without the overhead. In our opinion, microsharded sensitive data is no longer sensitive. As a result, ShardSecure has the potential to lower cyber risks and compliance costs while maintaining compliance with the spirit of European and US data protection regulations.

Warren Zafrin is the leader of the risk advisory services group at UHY Advisors. Throughout his 25 years of capital markets and technology strategy experience, Warren has supported many of the top 10 companies in the world and has managed project teams across the US, Canada, Europe, and Asia.