Cloud Data Microsharding for Financial Services

Prepared by
Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
eamoroso@tag-cyber.com

Version 1.0
July 1, 2021

Microsharding for data stored in multi-cloud environments reduce the risk of back-end access from unauthorized administrators. This includes either intentionally malicious access or unintentional access driven by malware. The financial services industry is shown to benefit particularly from such cyber risk management.

Introduction

The cyber risk of hosting of sensitive data in public cloud infrastructure has begun to diminish as practitioners have obtained access to new tools, platforms, services, and methods for improving security. Commercial vendors, in particular, have provided excellent solutions to address cloud entitlement management, cloud access visibility, cloud security posture management, and cloud data encryption.

Each of these improved controls, however, focus on the risks of unauthorized access to cloud data through the normal access channels. By way of analogy, these security methods focus on protecting normal access through the front door. While this is obviously important and necessary, such solutions have not addressed the uncomfortable issue of back-end access to data through cloud administrative access.

One must recognize that when data is hosted in public cloud services, the possibility emerges that back-end access to data might not include proper controls. Security teams address this through service level agreements (SLAs) with hosting providers, but few controls are in place to ensure that malicious attacks to cloud infrastructure do not open up such access and place hosted data at risk.

A promising technique being used to address this multi-cloud hosted data risk involves the use of *microsharding*. Derived from data management and encryption algorithms, the method is designed to address the cyber risks of back-end access to data hosted in cloud infrastructure.

Conveniently, the approach is also well-suited to multi-cloud hosting, which has become common in most modern hybrid architectures.

In this article, we highlight the benefits of microsharding for companies in the financial services sector. We show how the unique cloud-based protections for data are well-suited to the threats and evolving technologies being deployed into financial services companies. A practical case study is used to demonstrate how microsharding might be easily deployed and supported to reduce cloud data risk.

Understanding Microsharding

The microsharding process is designed to break up important data into multiple components that are separated, obfuscated, and stored across disparate cloud infrastructure. The result is that back-end access to the data by administrators and other cloud hosting insiders cannot result in a data breach, because the data has been sharded across multiple cloud storage entities (see Figure 1).

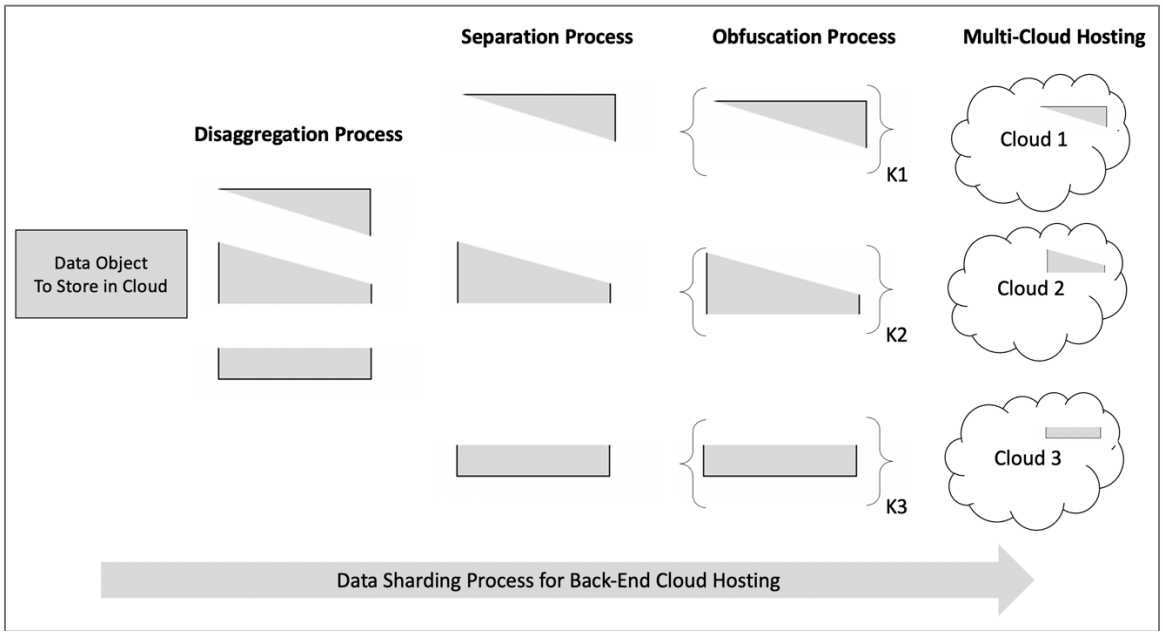

Figure 1. Microsharding Process

The component aspects of microsharding are arranged into a processing pipeline that collectively create the cloud data protection. Each of these component processing methods contribute to the overall security scheme. Insights into the algorithmic strategy for these processes are listed below:

- *Disaggregation* – Breaking up data to be cloud-stored into constituent parts is an important aspect of the sharding process. By disassembling in this manner, the threat of direct, back-end access is greatly reduced.

- *Separation* – The separation of the disaggregated components is a related task that further drives down the risk of unauthorized access using back-end channels with administrative access.
- *Obfuscation* – Obfuscation refers to the process of rendering each disaggregated data shard undiscernible on inspection. This can be done with encryption, blinding algorithms, and other practical means.

The most unique aspect of the microsharding process is that it complements the plethora of cloud security solutions that address front-end risk. That is, existing cloud security is all about ensuring that the overt path to hosted data is controlled by identity, access, encryption, and other policy enforcement mechanisms. Microsharding provide protection for back-end access to the data by administrators and other cloud hosting personnel.

Microsharding for Financial Services

The advantage of microsharding for Financial Services teams is that sensitive application-level data stored into multiple clouds can be disaggregated, separated, and obfuscated to reduce the back-end threat. In the financial services sector, this can be a valuable cyber security and framework compliance tool which helps with familiar requirements such as the following:

- *Payment Card Industry Data Security Standard (PCI DSS)* – The familiar PCI DSS focus on protection of cardholder data, so to the degree that such information is stored and analyzed, microsharding offers an excellent additional security control.

- *Gramm-Leach-Bliley Act (GLBA)* – The GLBA regulates collection, safekeeping, and use of financial data – which is the essence of what microsharding does for multi-cloud hosted data. This makes microsharding a valuable safeguard with respect to GLBA rules.

- *Federal Financial Institutions Examination Council (FFIEC)* – This council provides guidelines and recommendations to financial institutions for data protection. Microsharding can be a valuable component of a bank's adherence to FFIEC frameworks.

Obviously, microsharding will be well-suited to any industry focused on protecting data stored in multi-cloud environments. Critical infrastructure, in particular, will benefit from the additional protection from back-end administrative access. As the technique becomes more commonly applied and required, one might expect to see it used regularly in less intense threat environments as well, including by small and medium sized businesses.

Action Plan

Enterprise buyers and security practitioners working in financial services are advised to review their commercial options for microsharding support in public and hybrid cloud infrastructure, as well as within any virtualized data center environment. Some useful questions that might be asked of prospective cloud hosting providers or cyber security vendors offering this technology include the following:

- How does the microsharding work across multi-cloud infrastructure? Does it work in the cloud environments which are important to my present and planned deployments?

- How does the microsharding protect my data from back-end threats that emerge for administrators and other users with access to the hosted workloads?

- What types of user support, report generation, compliance assistance, and other functional capabilities exist within the platform?

Resources

https://shardsecure.com/resources/beat-the-cloud-data-breach
https://www.infosecurity-magazine.com/blogs/path-data-protection/

About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.