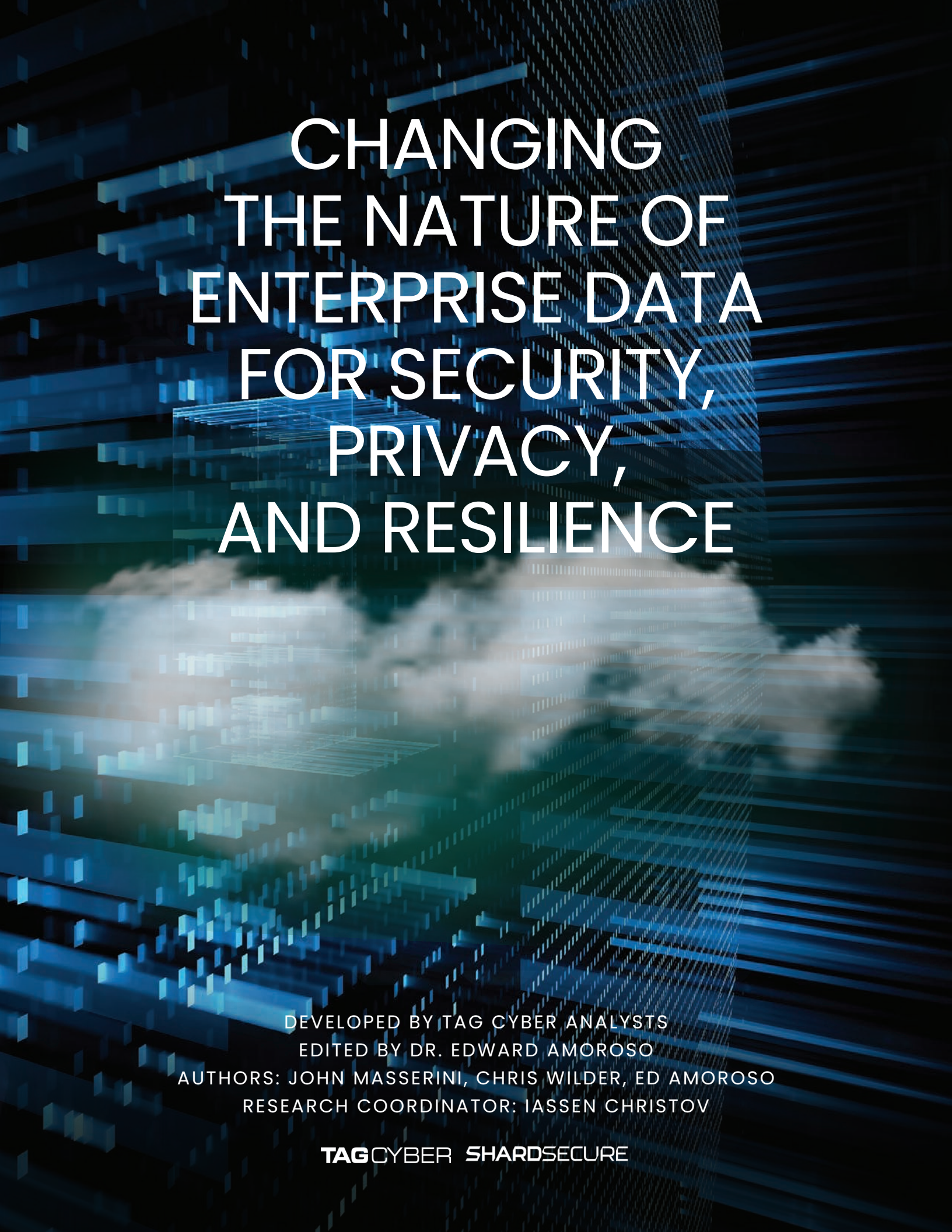


CHANGING THE NATURE OF ENTERPRISE DATA FOR SECURITY, PRIVACY, AND RESILIENCE

DEVELOPED BY TAG CYBER ANALYSTS
EDITED BY DR. EDWARD AMOROSO
AUTHORS: JOHN MASSERINI, CHRIS WILDER, ED AMOROSO
RESEARCH COORDINATOR: IASSEN CHRISTOV

TAG CYBER SHARDSECURE

INTRODUCTION: HOW IS SECURITY CLOUD-ENABLED?

BY DR. EDWARD AMOROSO

Companies often characterize the transition from perimeter-protected networks to hybrid multi-cloud as an infrastructure migration. Certainly, supporting this transition requires performing many hosting and network-related tasks, regardless of whether a company chooses to use Azure, GCP, or AWS, individually or in combination.

However, it is also true that this transition necessitates a careful review of the migration process of critical and sensitive data from LAN-hosted data centers to outsourced workloads and applications running in public cloud infrastructure. This process can be challenging, especially when the target architecture includes multiple cloud services.

In this book, TAG Cyber's analysts explore the protection of cloud-based enterprise data in the context of security, privacy, and resilience goals. To assist with this book, we leveraged the expertise of commercial vendor ShardSecure, whose platform provides effective controls for securing data, making it more resilient through a clever algorithm of data fragmentation and hosting.

CHANGING THE NATURE OF ENTERPRISE DATA FOR SECURITY, PRIVACY, AND RESILIENCE

DEVELOPED BY TAG CYBER ANALYSTS
EDITED BY DR. EDWARD AMOROSO
AUTHORS: JOHN MASSERINI, CHRIS WILDER, ED AMOROSO
RESEARCH COORDINATOR: IASSEN CHRISTOV

This book delves into the significant benefits of microsharding in cloud environments, and explores how ShardSecure's commercial platform revolutionizes data security, privacy, and resilience for modern enterprises.

CHAPTER 1

HOW IS SENSITIVE DATA PROTECTED THROUGH CLOUD MIGRATION?

BY ED AMOROSO, TAG CYBER

To date, the primary focus in cloud security has predominantly centered around protecting the underlying infrastructure. Teams have recognized that the systems, networks, and utilities that host cloud workloads can present substantial security risks without appropriate controls.

CLOUD SECURITY POSTURE

The security industry agrees that solutions categories can assist in reducing cloud risk. The most common solution category involves the management of cloud security posture—a method method of identifying and securing the attack surface that arises with cloud workload and application hosting.

Collecting accurate status information from the deployment is the cornerstone of effective cloud security posture management. This process provides visibility into relevant data and generates actionable intelligence to facilitate effective security-related preventive or response actions.

An entire industry relating to cloud security posture has emerged, resulting in cloud risk improvements. Enterprise teams now have a better way to secure their workloads, systems, and applications, leading to more organizations transitioning their business operations to the cloud.

CLOUD DATA SECURITY POSTURE

Securing data hosted in cloud workloads and applications is an often overlooked aspect of cloud security posture management. However, this should come as no surprise to security experts, as data poses the biggest challenge to protecting the enterprise, even in legacy environments.

Most cloud data security solutions typically encompass three primary tasks: identifying data migrated to the cloud, classifying this data within the cloud, and implementing measures such as obfuscation or access controls, often employing sophisticated encryption algorithms and procedures.

Microsharding is one method that has emerged for protecting data in the cloud, offering a useful and creative way to drive increased data resiliency.

Integrating these controls within cloud infrastructure is crucial and reduces the risk for organizations utilizing cloud data security posture solutions. Additionally, most organizations now partner with data inventory orencryption vendors (such as Azure or Amazon) to address data threats in cloud environments.

MICROSHARDING FOR ENHANCED POSTURE MANAGEMENT

Microsharding is one method that has emerged for protecting data in the cloud, offering a useful and creative way to drive increased data resiliency. This approach, called cloud data fragmentation (CDF), separates data into distributable pieces for dissemination across different hosting workloads.

ShardSecure, in particular, offers an effective solution for microsharding that is indicative of how this approach is likely to become an essential aspect of data security posture management. The team at TAG Cyber expects this approach to become a critical component of enterprise security architectures in the coming years.

The ShardSecure solution operates by breaking down critical data into multiple components, which are then separated, obfuscated, and stored across diverse cloud infrastructures. Back-end access by administrators and other cloud hosting insiders cannot result in a data breach because the data is microsharded across different storage entities (see Figure 1).

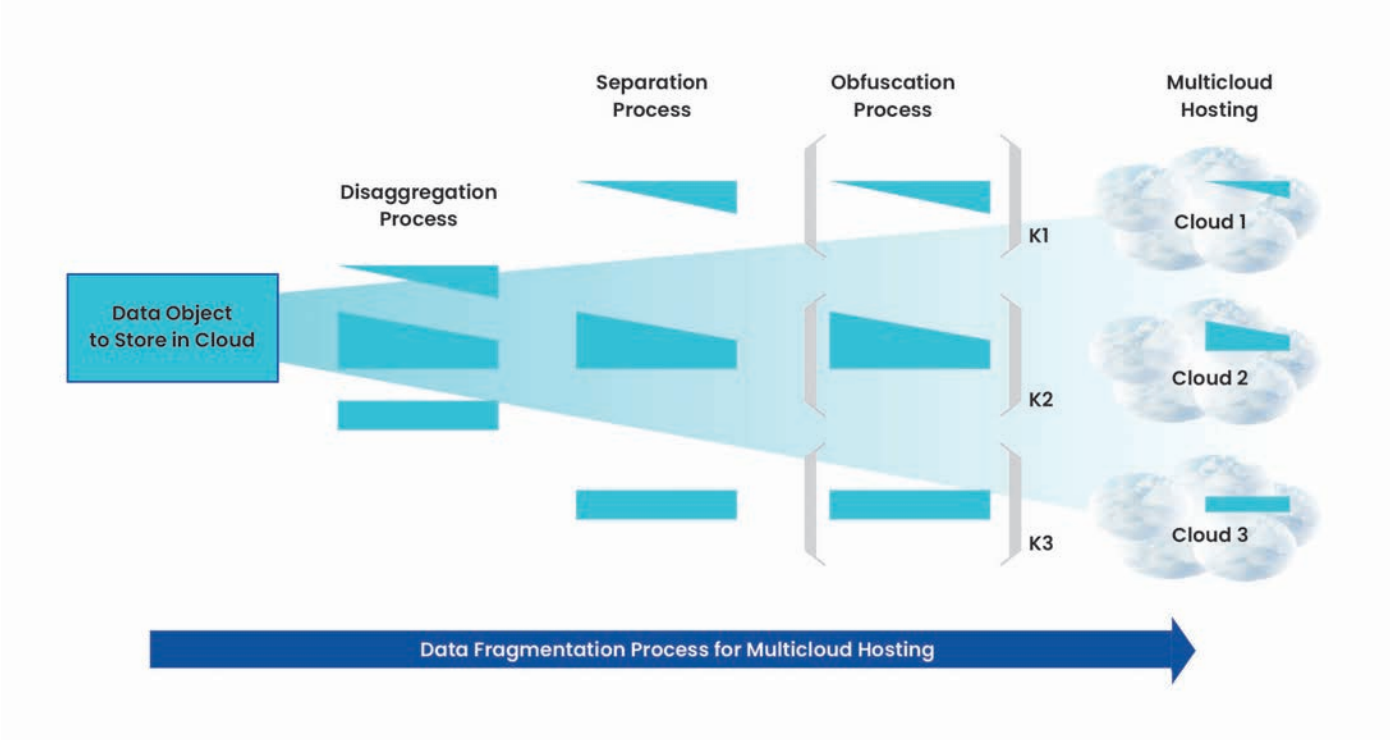


Figure 1. Microsharding Process

The microsharding process comprises multiple processing tasks providing cloud data protection. The algorithmic strategy for these processes includes:

- Disaggregation – The microsharding process involves breaking down data intended for cloud storage into its constituent parts. Disassembling reduces the threat of direct, back-end access by an insider or an intruder.
- Separation – Separating the disaggregated components (using back-end channels with administrative access) is a related task that further reduces the risk of unauthorized access.
- Obfuscation – This refers to rendering each disaggregated data shard undiscernible on inspection via encryption, blinding algorithms, and other practical means.

Microsharding is a complementary solution to cloud security measures that primarily address front-end risks. While existing cloud security focuses on controlling access to hosted data through identity, access controls, encryption, and other enforcement mechanisms, microsharding safeguards back-end access to data by administrators and other personnel within the cloud environment.

CHAPTER 2

WHAT DOES IT MEAN TO DESENSITIZE MULTI-CLOUD HOSTED DATA?

BY ED AMOROSO, TAG CYBER

The security process has traditionally relied on implementing protective measures, often called gauntlets, to mitigate risks associated with resource access. In other words, if a valuable asset is at risk of being accessed by unauthorized individuals or groups, security schemes typically incorporate firewalls, access controls, or other protective functions to prevent access.

This method of interceding between an entity requesting access and the resource of interest evolved from the earliest security models, such as James Anderson's reference monitor. While this approach remains central to cybersecurity protection, newer desensitization methods have emerged that offer a powerful complement.

TRADITIONAL METHODS TO PROTECT SENSITIVE DATA

As referenced above, James Anderson proposed nearly fifty years ago that implementing policy-based controls directly along the access path is the most effective way to protect data and other resources. Modern firewalls are a direct evolution of this approach, and it is now uncommon to come across practical environments without this type of security.

However, this type of in-line protection poses two cybersecurity challenges. First, if an intruder finds a path through the security gauntlet or circumvents it all together (often the case with complex firewalls featuring extensive access rule sets), it leads to unrestricted access to the entire resource.

Second, while security gauntlets protect front-end access to a resource, they do little to protect that resource from back-end administrative access. Even if firewalls are in place, there's little resistance against compromised or disgruntled administrators with direct access to the resource.

Some technologists use methods such as homomorphic encryption, which supports strong data obfuscation without stopping the use of queries and analysis.

USING DESENSITIZATION TO PROTECT DATA

An emerging alternative approach to safeguarding resources and data takes a somewhat different path from traditional security methods. Instead of placing a gauntlet between requesting entities, this novel method desensitizes the accessed resource. The outcome is a diminished advantage for successful intruders.

Many useful non-technical examples exist of desensitizing an asset to avoid compromise. Greying out sensitive text from a document, scattering one's apples across many baskets, and even removing valuables from a vulnerable location are all examples of asset desensitization.

The challenge lies in desensitizing data to mitigate access risks while maintaining the data's utility for authorized entities. Achieving this balance necessitates the skillful development of algorithms, protocols, and methods that effectively desensitize the data without incurring any data loss.

Some technologists use methods such as homomorphic encryption, which supports strong data obfuscation without stopping the use of queries and analysis. While this and related techniques are useful, they introduce considerable complexity. The next chapter presents a much simpler but (possibly) more powerful method.

MICROSHARDING AS A DESENSITIZATION METHOD

As outlined in the first chapter, microsharding breaks important data into tiny pieces separated, obfuscated, and stored across disparate cloud infrastructure. Back-end access by administrators and other cloud hosting insiders cannot result in a data breach because of the dissemination of microsharded data across multiple storage locations.

The data fragmentation approach is valuable because it does not preclude using gauntlets such as firewalls and access controls. In addition, while the approach breaks up data into individually desensitized pieces, tools are available to ensure that authorized users can access the data they need to support their mission.

From a TAG Cyber analyst perspective, this controlled access is essential to any multi-cloud environment, especially for data storage in highly sensitive contexts. Measurements reveal that microsharding has little to no performance impact, with no barrier to deployment for most enterprise teams. We encourage teams to spend time reviewing the commercial solution from ShardSecure.

CHAPTER 3

HOW CAN AN ENTERPRISE REDUCE THE RISK OF CLOUD-BASED RANSOMWARE?

BY JOHN MASSERINI, CHRIS WILDER, ED AMOROSO, TAG CYBER

ShardSecure's data resilience scheme includes data replication, where fragmented or microsharded copies of data are created and stored in diverse locations.

Data resilience protects against data loss or corruption and mitigates the risk of cloud-based ransomware attacks while facilitating swift data recovery. By integrating efficient cloud-based data resilience schemes, organizations can effectively combine timely backup and recovery systems to restore their data during an attack. These schemes leverage a distributed architecture, storing data across multiple servers or storage devices, enabling organizations to recover their information even if malicious actors compromise one or more servers.

In addition to backup and recovery, data resilience schemes also incorporate preventive measures to mitigate data loss or corruption. For instance, ShardSecure's data resilience scheme includes data replication, where fragmented or microsharded copies of data are created and stored in diverse locations. This approach ensures data integrity and prevents loss caused by hardware failures or other unforeseen issues.

WHAT IS MICROSHARDING OR DATA FRAGMENTATION, AND WHY IS IT IMPORTANT?

Data sharding allows organizations to scale their storage capacity and improve the performance of their data storage systems – especially when dealing with large amounts of data. In the context of ShardSecure's data resilience scheme, a related approach known as microsharding serves several important functions.

Microsharding enhances the resilience of the data storage system by mitigating the risk of data loss or corruption resulting from hardware failures or other issues. Distributing an organization's data across multiple public clouds, servers, or storage devices makes it more challenging for attackers to encrypt all the data in a ransomware attack, forcing attackers to compromise multiple servers or storage devices to achieve their goal.

As a result, microsharding decreases the likelihood of a successful ransomware attack and minimizes the impact on business operations. In addition to increasing the resilience of the data storage system, microsharding reduces the risk of bottlenecks or other performance issues, resulting in a faster and more efficient data storage system.

MICROSHARDING FOR DATA RESILIENCE CAN REDUCE THE THREAT OF RANSOMWARE.

Using data resilience schemes can significantly reduce the risk of ransomware attacks by making it more difficult for external actors to carry out an attack successfully. By storing data across multiple servers or storage devices, organizations can recover their data even if one or more servers are compromised. Additionally, the data privacy aspect of microsharding can neutralize the threat of double extortion ransomware, where attackers threaten to release an organization's sensitive information.

More broadly, deploying a data fragmentation, distributed storage, and replication strategy ensures business continuity and protects against ransomware attacks and financial and reputational impact.

Organizations seeking to improve data resilience should consider the schemes offered by ShardSecure. Microsharding can help organizations increase the strength and performance of their data storage systems and reduce the risk of data loss or corruption.

CHAPTER 4

HOW CAN ENTERPRISE ADDRESS THE GDPR AND CROSS-BORDER DATA PROTECTION?

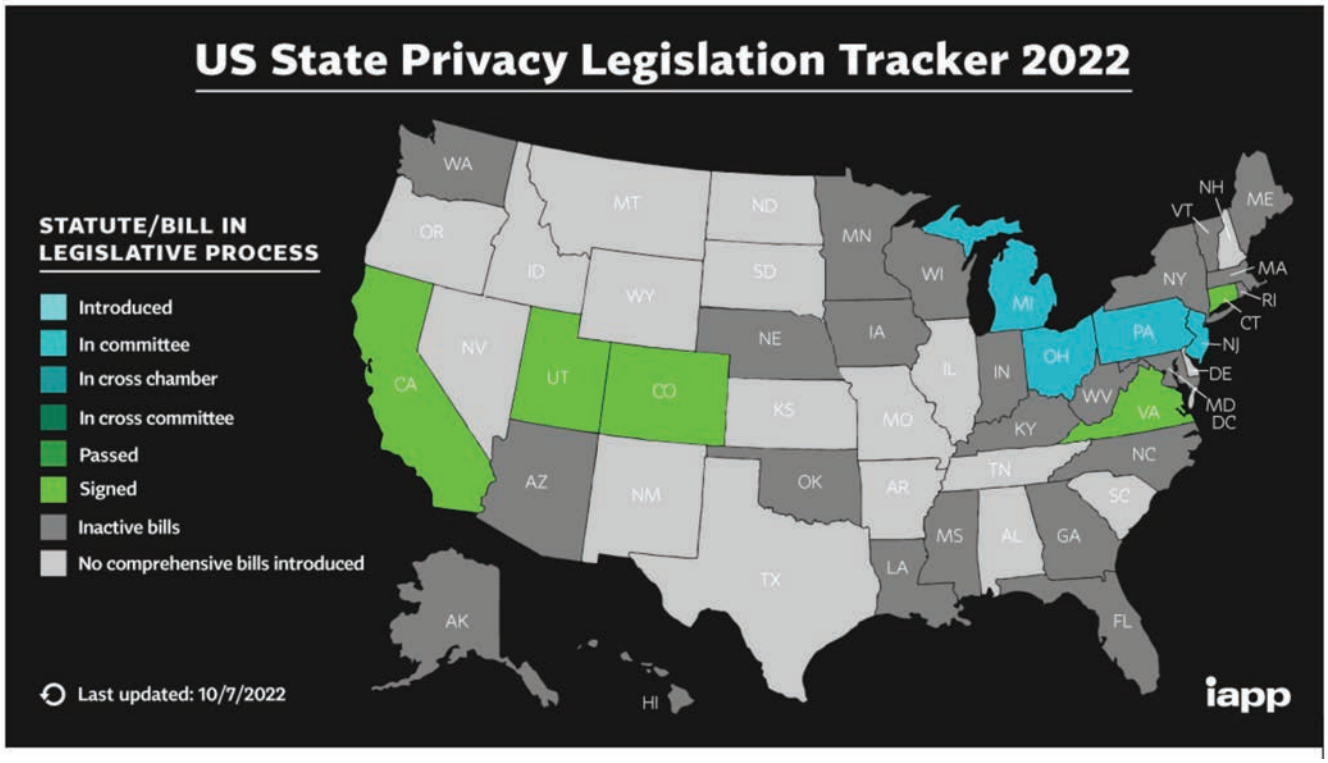
BY DAVID NEUMAN, SENIOR ANALYST, TAG CYBER

The General Data Protection Regulation (GDPR) is a comprehensive data protection law adopted by the European Union (E.U.) in 2016. It applies to organizations or entities that do business in the E.U. The GDPR has 99 articles outlining the rights and responsibilities of individuals and organizations concerning personal data. Under this law, organizations face penalties of up to 4% of their annual global revenues for non-compliance.

While the E.U. law has some stringent requirements and penalties, several data protection laws worldwide are similar to the GDPR. Examples include:

- **The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada.**
- **The Privacy Act in Australia.**
- **The Data Protection Act 2018 in the United Kingdom.**
- **The Lei Geral de Proteção de Dados Pessoais (LGPD) in Brazil.**
- **The California Consumer Privacy Act (CCPA) in the United States.**

Data protection legislation in the U.S. is complicated because each state can pass its own laws. Ten of the 50 states have done or are currently doing so, as depicted in the chart below from the International Association of Privacy Professionals (IAPP).



Enterprises with cross-border or multinational operations that process personal data must take a more holistic approach than traditional methods to protect that data.

WHAT ARE THE CHALLENGES?

Laws such as the GDPR and other emerging international requirements represent two overarching challenges.

- **Data privacy and regulatory compliance.** Data, including account numbers, credit card data, and other personally identifiable information (PII), is an organization's crown jewel because they need it to serve customers and drive their business. However, data protection laws are complex and can prevent business scalability and agility. In other words, the need to meet data privacy and regulatory obligations can significantly drive up costs and drive down the business efficiencies and innovation needed for competitive advantage.
- **Losing control of data.** Under GDPR, organizations must master their data sovereignty, which is a daunting task in the age of cloud storage. Firms heavily invest in security for sensitive data, yet the complexity of the data ecosystem raises serious questions. Currently, they face dual perils: the risk of losing data control due to threats like ransomware and the risk of data extraction via malintent or ineptitude.

ShardSecure's technology helps protect an organization's sensitive data by making it incomplete, unintelligible, and useless to bad actors, cloud providers, and IT administrators.

HOW CAN ORGANIZATIONS TURN THESE CHALLENGES INTO OPPORTUNITIES?

Considering innovative approaches to data security can also lead to business-enabling opportunities. For example, solutions that provide stronger data security and privacy may help an organization to meet its regulatory obligations and scale its business.

Organizations like Shardshare that adopt a CDF approach will be able to safely move data among locations, regions, platforms, and providers without additional complexity and gain defense-in-depth – regardless of where their data is stored. With a CDF or microsharding approach, for instance, encryption keys are compromisable, but an attacker still cannot reassemble the fragmented data distributed across multiple locations.

ShardSecure's technology helps protect an organization's sensitive data by making it incomplete, unintelligible, and useless to bad actors, cloud providers, and IT administrators. This technology also makes shared responsibility a moot point because sensitive data is no longer sensitive. In addition, it shields data from malicious activity and accidental exposure due to misconfigurations and other human errors.

IN SUMMARY

Regulations like the GDPR will continue to impact privacy and security significantly, and more regulations governing industries are likely on the way. ShardSecure's approach allows companies to meet complex cross-border regulatory obligations. The level of data protection provided by their microsharding solution also transcends traditional security capabilities, supports business growth, and earns customer trust.

CHAPTER 5

HOW DATA SHARDING HELPS ORGANIZATIONS TO IMPROVE CLOUD AND MULTI-CLOUD DATA SECURITY

BY CHRIS WILDER, TAG CYBER

Distributing data across multiple resources allows your organization to leverage the capacity of multiple servers or storage devices, reducing the need for costly upgrades or expansions.

Data security has become a critical concern for organizations of all sizes, especially as more data is generated and processed in cloud-based environments. Data sharding is one promising approach to enhancing data security. This technique breaks up large datasets into smaller, more manageable parts called "shards" and distributes them across multiple storage devices or servers. While data sharding can provide numerous benefits, including improved security, increased resilience, and reduced costs, it can also present some challenges, such as the need for specialized expertise and infrastructure.

IMPROVED SECURITY AND RESILIENCE WITH DATA SHARDING

Data sharding can significantly improve your organization's security posture and resilience by reducing the risk of data loss or theft. By distributing data across multiple resources, the attacker will only gain access to a small fraction of the data, minimizing the impact of a breach—even if one shard or storage device is compromised. Additionally, data sharding enables redundancy and backup strategies, such as replicating shards across multiple servers, which can improve fault tolerance and reduce the risk of data loss due to hardware failure.

ENHANCED EFFICIENCY WITH DATA SHARDING

Implementing data sharding can enhance flexibility by enabling more efficient use of storage and processing resources. Distributing data across multiple resources allows your organization to leverage the capacity of multiple servers or storage devices, reducing the need for costly upgrades or expansions. Sharding can also improve the performance of applications that rely on large datasets, increasing productivity and minimizing downtime.

SHARDSECURE: ADVANCED DATA SHARDING SOLUTION

Implementing data sharding can be complex and resource intensive, but that's where companies like ShardSecure provide value. ShardSecure offers an advanced solution for data sharding explicitly designed to enhance security and compliance in cloud-based environments.

ShardSecure built its solution on a process called Microsharding. This patented process breaks down data into smaller pieces than traditional sharding methods, reducing the risk of data loss/theft and enabling more efficient storage and processing resources. Additionally, ShardSecure's solution includes advanced encryption and access controls, further enhancing security by ensuring only authorized users can access the data.

ShardSecure's solution also provides real-time monitoring and alerts, which can help security teams quickly detect and respond to security incidents, reducing the impact of a breach. In addition, ShardSecure's solution can help organizations meet regulatory requirements and protect their sensitive data from cyber threats by providing comprehensive security and compliance capabilities.

USE CASES FOR SHARDSECURE'S SOLUTION

One specific use case for ShardSecure's solution is in regulated industries such as healthcare or financial services. Companies in these industries are often subject to strict data privacy and security regulations, and data sharding can help them meet these requirements. By using ShardSecure's solution, these companies can improve their security posture, reduce the risk of data breaches, and meet compliance requirements.

Another use case for ShardSecure's solution is in multi-cloud environments. As organizations increasingly adopt multiple cloud providers for their infrastructure, managing data security across various technologies can become challenging. Organizations can use ShardSecure's solution to ensure consistent protection and compliance across all cloud environments, regardless of the underlying infrastructure.

TAG'S TAKE

Data sharding offers numerous benefits for organizations looking to improve data security, increase resilience, and reduce costs. By distributing data across multiple resources, sharding can significantly reduce the risk of data loss or theft, enhance fault tolerance and recovery from hardware failures, and improve the efficiency of storage and processing resources.

However, implementing data sharding can be complex and resource-intensive, requiring specialized expertise and infrastructure. Moreover, improper sharding implementation and management can introduce new security risks.

For this reason, companies like ShardSecure offer an optimal solution for data sharding. Leveraging ShardSecure's solution allows organizations to enhance security and compliance in their cloud-based environments.

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.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Dr. Edward Amoroso Authors: John Masserini, Chris Wilder, Ed Amoroso Research Coordinator: Iassen Christov

Publisher: TAG Cyber, a division of TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.