SHARDSECURE

White Paper

Microshard™ technology: An Introduction

Our patented Microshard technology is an alternative to encryption for data at rest. Microsharding desensitizes sensitive data, rendering it unintelligible and of no value to unauthorized users. We do this through a three-step process that shreds, mixes, and distributes your data to multiple storage locations of your choice—multi-cloud or hybrid-cloud environments.

Shred: Microshard technology begins by shredding data into four-byte microshards that are too small to contain a birthdate, an ID number, or any complete piece of sensitive data. The size of the microshards is configurable, and policies may be applied to optimize the microshard size according to file type.

Mix: Next, poison data is added and the microshards are mixed into multiple logical Microshard containers. Identifying information like file extensions, file names, and other metadata is also removed, making unauthorized reassembly even more complex. The amount of poison data to be added is also configurable.

Distribute: After being mixed, the Microshard containers are distributed across multiple customer-owned storage repositories in multi-cloud or hybrid-cloud configurations. Each storage location contains a 1/n-1 fraction of the complete data set, with one Microshard container reserved for parity.

Complementing or Replacing Encryption with ShardSecure®

Overview

Encryption is the traditional approach for securing data at rest and has been the method of choice for many IT leaders. In fact, certain laws and regulations specifically require encryption, so for compliance reasons alone encryption will remain an important layer of defense.

However, human error, poor cyber hygiene, and challenges with key management can provide threat actors and rogue insiders with access to high-value data. Since encrypted data is stored whole, meaning that an entire file is stored in a single location, unauthorized parties can gain access to the entire file. At that point, encrypted files can be deleted, decrypted with a compromised key, re-encrypted with ransomware, or exfiltrated by a well-resourced adversary with enough time and computer power to try to break the encryption. Consequently, encryption itself is not adequate to deter data intrusion and breaches by highly determined nation states. Particularly in countries that are advanced in quantum computing that can crack encryption faster, the capacity of a well-resourced adversary to decrypt data should be taken seriously.

Government alerts and resources warn of the increase in crafty attacks and geopolitical risk and urge organizations to act swiftly to mitigate threats. Fortunately, organizations now can consider another approach to data protection that is often compared to encryption but offers significant advantages due to its innovative "Shred. Mix. Distribute" process to desensitize sensitive data. Microshard™ technology includes numerous capabilities to strengthen data protection, neutralize ransomware attacks, and maintain data availability and performance—and it is quantum-safe.

Capabilities to strengthen protection of data at rest

Data Integrity Checks

In order to verify file integrity, all Microshard data are hashed (fingerprinted) and the hash is stored within the ShardSecure engine, not with the data at rest. This ensures that if a storage location is compromised by an internal or external threat actor, the hash of the file cannot be tampered with to hide any evidence of wrongdoing.

Each time a file is read by your application, ShardSecure ensures that the hash matches the hash that was created when the file was written to storage, ensuring the file the authorized user gets back is byte for byte identical to what was originally written. If there is a mismatch, our self-healing data capability will reconstruct the affected Microshard data.

Self-Healing Data

Self-healing data is a key capability that reconstructs data that has been tampered with in any way to its previous, unaffected state. Multiple data integrity checks are performed during the microsharding process to detect any changes that may have been made to the Microshard data at rest. If a Microshard container fails a data integrity check during the reassembly process, the affected container is reconstructed to its unaffected state and the application user continues to work unimpacted. The cause of the failed check—unauthorized deletion or modification, including encryption as a result of a ransomware attack—is irrelevant as the process is the same. It should be noted that a failed data integrity check is an indicator of compromise as there should be no modifications to the data at rest.

Self-healing data does this by creating slight overlaps of the distributed Microshard data across the different storage locations. This allows the ShardSecure engine to reconstruct the affected data transparently and in real-time.

Similarly, if a data storage location becomes unavailable due to any number of reasons—an outage, network issue, misconfiguration, etc.—the same process reconstructs the unavailable Microshard data in real-time. This ensures a high level of uptime, without having to restore data from backups in many outage scenarios. Users' work is unaffected and security teams are alerted to initiate investigation and response.

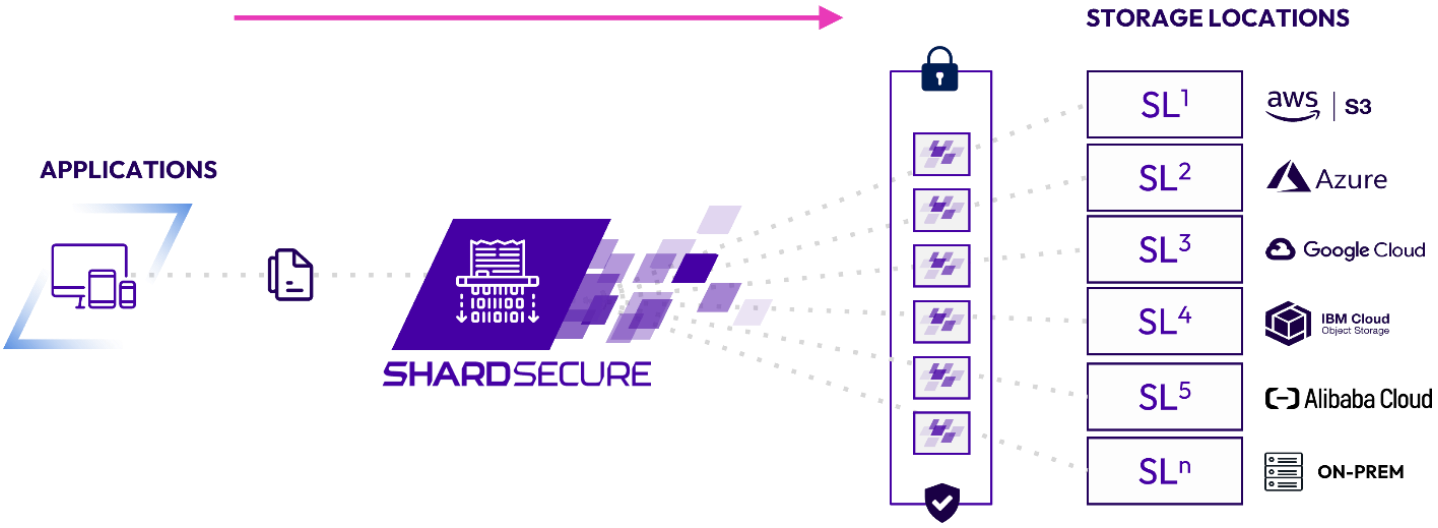

Figure 1 - During ShardSecure's three-step microsharding process, Microshard data is shredded into four-byte microshards, mixed into multiple logical containers, and distributed to multiple storage locations of your choosing to help ensure that no one location contains any identifiable data.

Data Desensitization

Microshards are as small as four-bytes, too small to contain sensitive data. Adding poison data and then mixing the Microshards and distributing them across multiple storage locations ensures each location only contains an unintelligible fraction of the whole data set. If a storage location is compromised and data is stolen, only a mixed-up fraction of the data set is exposed.

The level of complexity an authorized user would need to know in order to attempt the reassembly of a single microsharded file makes it virtually impossible. For instance, the person would need to know the storage locations to which each of the Microshard containers have been distributed and how to compromise each; which Microshard containers are part of the original file since all identifiers have been stripped; which Microshard data are legitimate and which are poison; and the correct order of the microshards which, for a 1MB text file shredded down to four-byte microshards, will number over 262,000, excluding poison data. This renders the data useless to unauthorized users and helps protect data confidentiality and privacy.

Keyless Data Access Control

Microshard technology does not rely on keys, so issues of key ownership, client-side and server-side key management, and credential abuse are non-existent. You maintain control over data access so that only authorized parties have access to the complete data set.

For organizations that manage their own encryption keys, keyless access significantly reduces the costs, administrative efforts, and risks that come with key management, as well as any performance issues caused by encryption.

Organizations using server-side encryption managed by their cloud provider are sometimes uncomfortable with third-party management. While cloud providers are trustworthy, user errors and misconfigurations can expose sensitive data. Microshard technology stores data in cloud locations of your choosing, and you control data access. This level of control over sensitive data is particularly important for any organization governed by stringent data privacy regulations.

High Availability and Performance

Instances of ShardSecure are software-based, virtual clusters. To maintain availability and performance, disparate virtual clusters can be deployed in different regions, in different clouds or in a combination of on-premises and cloud. Microshard technology reads and writes in parallel to and from multiple storage locations, so it does not require any hardware acceleration and can even improve performance when compared to certain encryption deployments. The clusters will synchronize the instructions to reassemble Microshard data in the event of a storage service outage, or for global load balancing to enhance performance. The global failover capability reduces the risk of downtime and avoids a single point of failure. User activity is seamlessly directed to the operational location if one location becomes inaccessible.

Quantum-safe Protection

Encryption is essentially a complex mathematical problem, and full data sets can be decrypted with enough time and resources. Faster computers, including quantum computers, won't help an attacker with Microshard data, since they only have access to a partial set of data and no way to reconstitute incomplete sets of data fragments, regardless of how strong their computation power is. Sensitive information remains unintelligible even if decrypted.

Integrated Defense-in-Depth

Organizations are replacing encryption with Microshard technology. However, combining encryption and microsharding is an option for companies that have already deployed encryption for data at rest, companies that are required to use encryption to meet regulations, or companies that desire an extra layer of data protection. ShardSecure integrates with existing encryption solutions for a deeper layer of defense-in-depth. Specifically, encrypted data can be microsharded and distributed to multiple customer-owned storage locations. Unauthorized users who compromise a storage location will only have access to an unintelligible fraction of that material.

Conclusion

Encryption has been the only option for securing data at rest, until now. Although encryption provides advanced data protection against certain kinds of cyberattacks, it does not inherently protect against ransomware, which itself uses encryption to hold files and systems hostage, and leaves entire files exposed if successfully decrypted. Encryption also introduces cost and complexity associated with key management, and it has no mechanisms to ensure data availability. Alternatively, our Microshard technology provides capabilities including data integrity verification, self-healing data, data desensitization, keyless data access control, and high availability and failover. This innovative approach to data protection overcomes the limitations of encryption, integrates with encryption as needed, and offers a quantum-safe option for the future.

For more information on how ShardSecure is helping leading organizations in sectors including financial services, pharmaceuticals, technology, and biotech strengthen data protection, visit https://shardsecure.com/

@ShardSecure
@ShardSecure
@ShardSecure

101 Avenue of the Americas
9th Floor, New York, NY 10013
United States of America

info@shardsecure.com