SHARDSECURE

White Paper

Improving Business Continuity with ShardSecure®

Overview

Information security is based on the three pillars of data confidentiality, integrity, and availability. Confidentiality tends to dominate the focus of most security discussions, while integrity and availability are often overlooked. That's changing now as the ongoing pandemic, increasing geopolitical risk, and climate risk-related events are disrupting organizations in ways executives and security leaders never imagined. A global study of 456 business continuity and resilience professionals finds the appreciation for business continuity has risen in 79% of organizations surveyed, with 33% describing it as "very much increased."

Maintaining business continuity is incredibly difficult during times of uncertainty, so the importance of data integrity and availability is now on par with data security. Your applications, users, and customers must be able to use data securely, and also reliably, even in the midst of disruption. To that end, our Microshard technology includes numerous capabilities to improve the availability, reliability, and resiliency of your critical data.

Capabilities to Achieve Business Continuity

Data Integrity Checks

All Microshard data are hashed (fingerprinted). 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 will reconstruct the affected Microshard data.

MicroshardTM Technology: An Introduction

Our patented Microshard technology desensitizes sensitive data in the cloud rendering it unintelligible and of no value to unauthorized users. We do this through a three-step process to shred, mix, and distribute your data to multiple storage locations of your choice–multi-cloud or hybrid cloud environments.

Shred: Data is shredded into four-byte microshards which are too small to contain sensitive data such as birthdates, identification numbers, and so on. The size of the microshards is configurable and policies may be applied to optimize the microshard size according to file type.

Mix: Microshards are mixed with poison data in multiple, logical Microshard containers. Identifying information like file extensions, file names, and other metadata is removed, increasing the complexity for unauthorized reassembly. The amount of poison data to be added is also configurable.

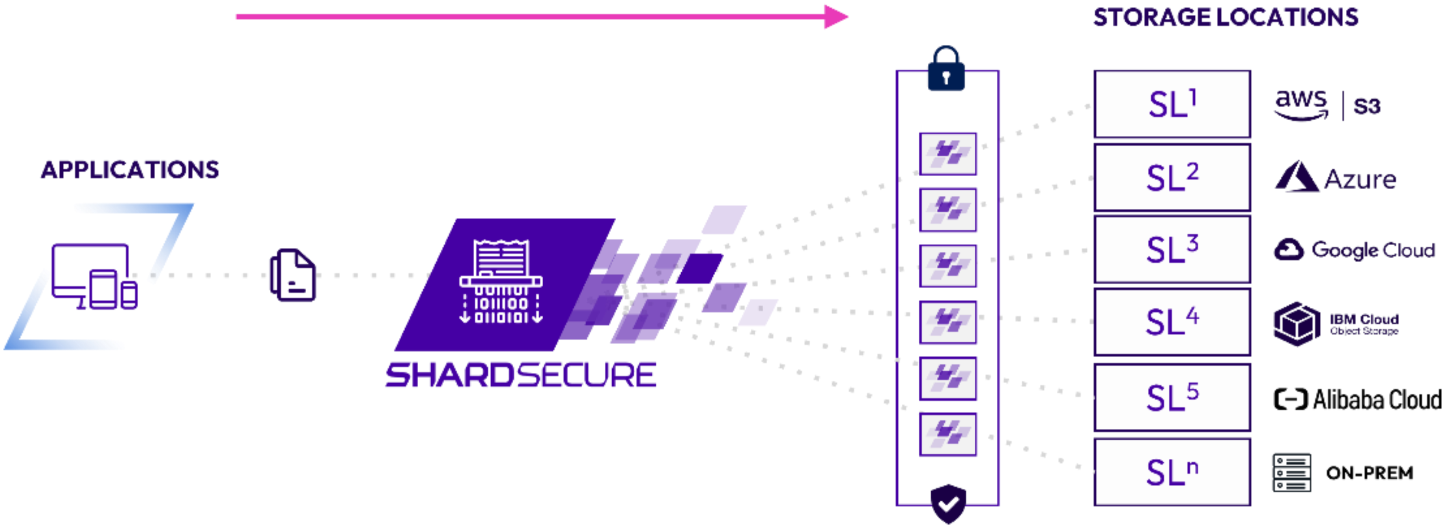
Distribute: Microshard containers are distributed across multiple, customer-owned storage repositories in multi-cloud or hybrid-cloud configurations. By doing so, each storage location contains a 1/n-1 fraction of the complete data set, with one Microshard container reserved for parity data.

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 – tampering, ransomware, deletion – 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, misconfigured firewall, 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.



Responsive Storage

An error is generated any time that self-healing data repairs any data, and our solution monitors that error rate. When a user-defined error threshold is reached for a given storage location, whether due to availability or cyberattack, the affected data automatically reconstructed and then migrated to a alternate storage location, without any impact to your data, applications, or uptime.

Failover and High Availability

Instances of ShardSecure are software-based, virtual clusters. However, to provide geographical redundancy and business continuity, disparate virtual clusters can be deployed in different regions, in different clouds, or in a combination of on-premises and cloud. The clusters will synchronize the instructions to reassemble Microshard data in the event of an 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.

Data Agility

ShardSecure makes migrating data between regions or even clouds easy, secure, and transparent. If you need to migrate data from one storage location to another for availability or performance reasons, as part of a cloud migration or for cost issues, a few clicks can start that process. The data migration happens in the background and is a zero-downtime event, with no impact to your applications. In addition, all data is moved in its Microshard form, meaning the data is still secure and unintelligible in case of a man-in-the-middle attack. The data is also encrypted in transit, providing multiple layers of security and privacy.

Scheduled Tasks

ShardSecure automatically executes periodic tasks and proactive checks of the system and the data it protects. This includes data integrity checks, cleaning expired objects, obfuscating metadata, and validating network connectivity to backend storage. This helps ensure high reliability and availability.

Conclusion

There is no better time to focus on business continuity and disaster recovery than now. Organizations that are getting ahead of widespread business disruptions are revisiting their strategies to address data integrity and availability. Our Microshard technology provides capabilities including self-healing data, high availability and failover, responsive storage, file integrity verification, data agility, and scheduled tasks to improve business continuity today and in the face of ongoing uncertainty.

For more information on how ShardSecure is helping leading organizations in sectors including financial services, pharmaceuticals, technology, and biotech strengthen their resiliency, 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

SHARD SECURE