SHARDSECURE®

CLOUD-ENABLE YOUR DATA

SOLUTION BRIEF:

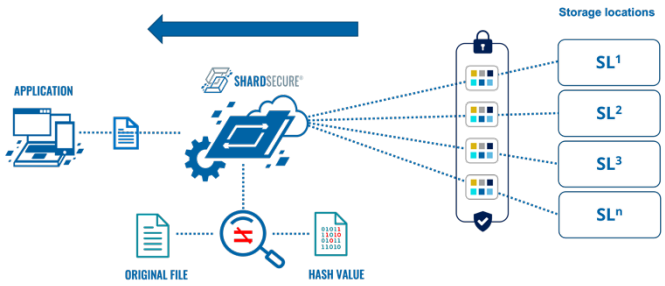
SHARDSECURE FOR CLOUD-BASED RANSOMWARE

Information security is based on the three pillars of confidentiality, integrity, and availability – the CIA triad. ShardSecure's patent-pending Microshard™ technology inherently upholds the triad. Microshard technology is based upon a three-step process that consists of shredding, mixing, and distributing your data across multiple storage locations, and protects your data by making it unintelligible and undesirable in the wrong hands.

In this solution brief, we will specifically focus on the area of integrity and how ShardSecure helps to protect you from cloud-based ransomware attacks.

ShardSecure for data integrity

Data integrity is built-in from the start. Before the Microshard containers are distributed to storage, we create a hash of the Microsharded data. As we reassemble the Microsharded data, we create another hash of the Microsharded data and compare the two hashes to make sure they are identical.



Microsharded data should never be modified at rest. If the hashes are mismatched, this is an indicator of compromise. To us, the reason for the mismatch – including encryption of the Microsharded data - is irrelevant. We simply rebuild the affected data from its last known good state, reassemble the Microsharded data as usual, and present the user with their clean file as it was saved.

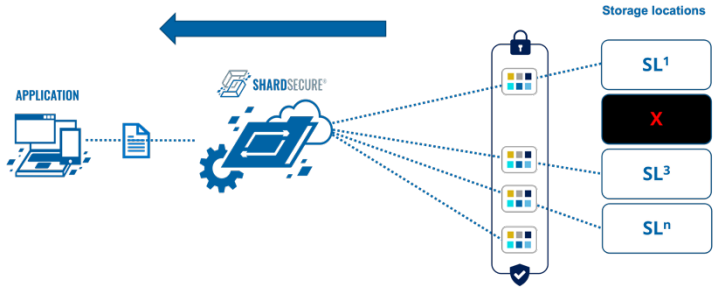
This process may also serve as an early form of detection as we will generate an alert immediately upon detecting the mismatch and alert your SOC, SIEM, SOAR, etc., for additional action or investigation. Additionally, it is a straightforward process to move your affected data to a different, uncompromised location during your incident response process and without affecting your users' ability to continue working as they normally would during the incident.

ShardSecure for data availability

It is worth discussing the fact that some attackers, if unable to access or alter their victims' data, will turn to more destructive tactics. ShardSecure provides native support for multi-cloud, multi-region, and/or on-prem storage configurations, and the solution's enterprise-ready high availability capabilities support any combination of storage options and configurations.

Business continuity: Should one of your independent storage locations become inaccessible for any reason, our Microshard technology quickly rebuilds the data from the unavailable location and delivers a complete file to the user. So, you can keep working during an outage.

Failover capabilities: We recommend that you deploy your ShardSecure virtual appliance clusters in two different locations, for example on-premises and in the cloud, to reduce the risk of downtime and avoid a single point of failure. User activity is seamlessly directed to the operational location if one location becomes inaccessible.



Visit us at https://shardsecure.com to learn more and to schedule a demo. Follow us on social media.

SHARDSECURE®

+1 (800) 760 9445

info@shardsecure.com

@ShardSecure

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