SHARDSECURE

Solution Brief

59% of organizations surveyed claimed increased spending on backup solutions to mitigate the effects of ransomware[1]

Self-healing data preserves data integrity, neutralizes ransomware, and bolters business continuity

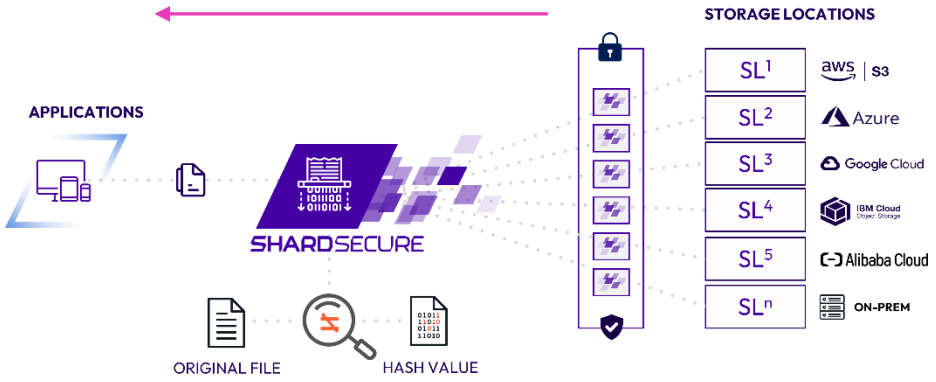
Neutralize Cloud Storage Ransomware

The need for advanced data security has never been greater as the number ransomware attacks continues to grow. A 2022 report by 451 Research notes that ransomware is driving organizations to improve their data protection. Fifty-nine percent of organizations claim they are spending more on backup services or backup storage because of the potential threat of ransomware1.

In this solution brief, we will provide and overview of how ShardSecure's self-healing data neutralizes cloud storage ransomware attacks and bolsters business continuity.

Self-healing data preserves data integrity

Microshard data is self-healing. Multiple data integrity checks are performed during the microsharding and reassembly processes. If a discrepancy is detected, our self-healing data will reconstruct the affected Microshard data returning the data to its original state without impacting business operations.



Microshard data should never be modified at rest and any attempt to do so is an indicator of compromise. Our solution may be configured to share alerts with your SIEM, SOAR, and your SOC team via Slack to initiate incident response or other investigative processes to help mitigate a larger attack.

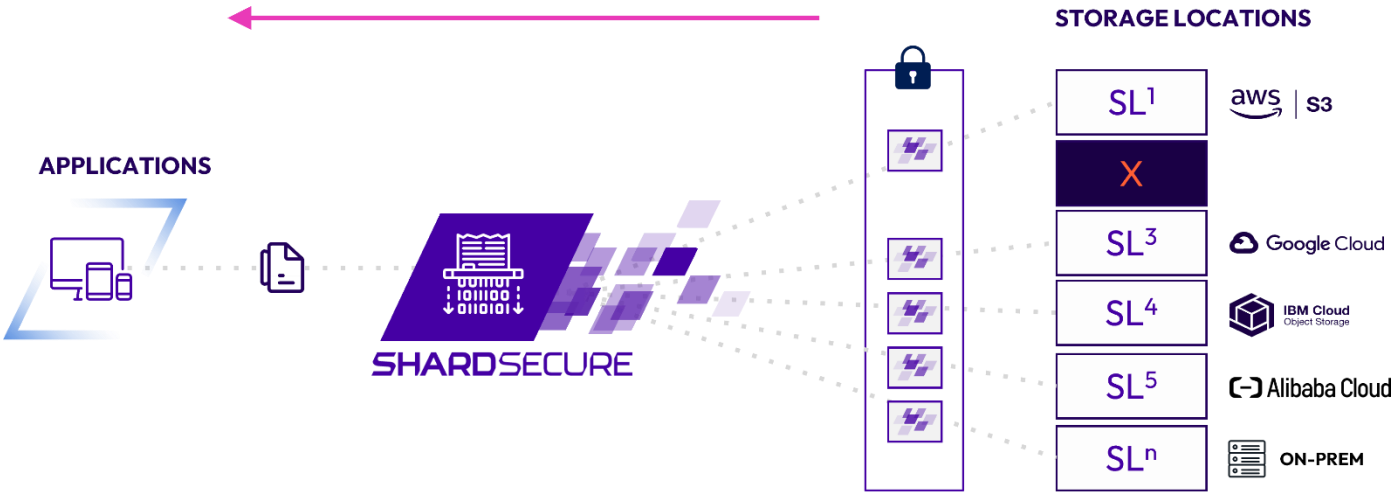
[1] Baltazar, Henry. (2022, March.) "High capex costs push cloud storage into a leading role for data protection – Highlights from VotE: Storage." 451 Research.

Protecting your backups and early detection

A common technique for ransomware attackers is to first infect a victim's backups before launching the primary attack. They will do so stealthily over a period of time long enough to ensure there are no clean backups, and then, they will launch the main attack. Without a clean backup, victims often have no other recourse than to pay the ransom. Microsharding your backups not only neutralizes ransomware attacks against your backup data, but a failed integrity check may serve as an early detection capability.

Another technique used by attackers is to exfiltrate data from their victims to use as blackmail by threatening to expose the stolen data on the Internet if the ransom is not paid. Microshard data is unintelligible and of no value to unauthorized users.

Some attackers will turn to more destructive tactics and delete data that they are unable to alter or steal. Because Microshard data is self-healing, any unauthorized deletions of Microshard data are simply reversed. Even if an entire storage location is unavailable, self-healing data reconstructs the affected Microshard data until the service is brought back online.



Automatic data migration

Each storage location may have an alternate location configured for the purpose of automatically migrating data from a potentially infected storage location to a clean one. User-configured thresholds may be set such that if X number of data integrity checks fail in Y timeframe, then all of the Microshard data in the original location is automatically migrated to the backup location. This prevents a cycle of re-encryption and self-healing each time a file is retrieved from and saved to an infected storage location. And in scenarios where an attacker has gained access to the original storage location, automatic migration suddenly removes all of the Microshard data to a location unknown to the attacker.

Learn More

Visit us at https://shardsecure.com for more information and to schedule a demo.

@ShardSecure
@ShardSecure
@ShardSecure

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

info@shardsecure.com