SHARDSECURE

Solution Brief

ShardSecure for the CIA Triad

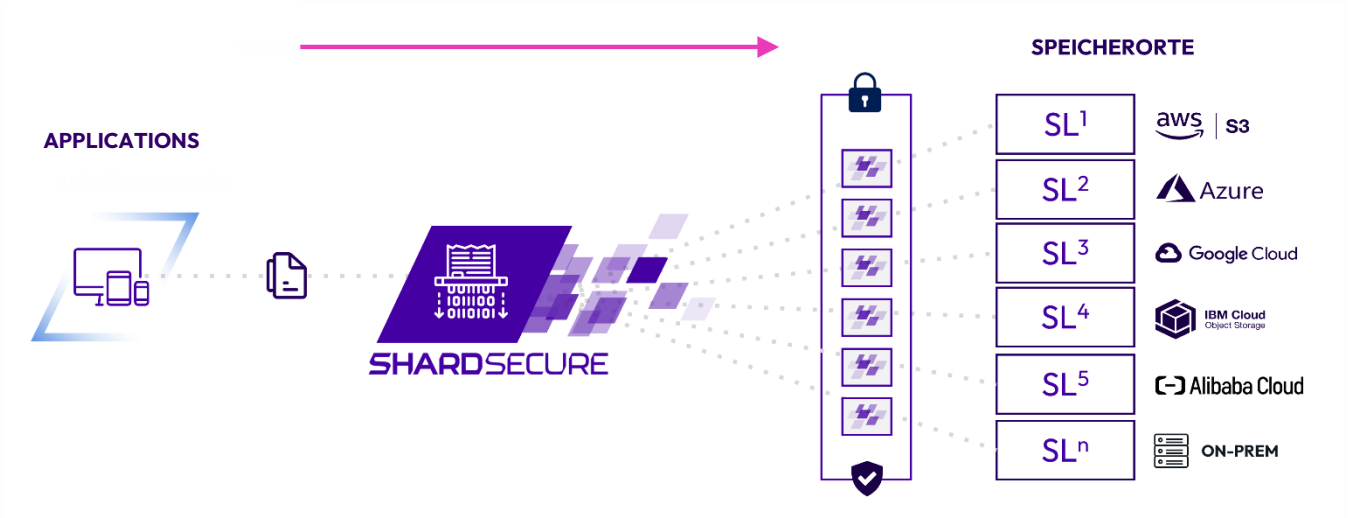
Information security is based on the three pillars of confidentiality, integrity, and availability – the CIA triad. ShardSecure's patent-pending Microsharding technology inherently upholds the triad. Microsharding is a three-step process that consists of shredding, mixing, and distributing your data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

ShardSecure for data confidentiality

Data confidentiality is grounded in how we treat the data to make it incomplete, unintelligible, and of no value to unauthorized users.

Data desensitization: The first step in Microsharding is to "shred" files into four-byte Microshards, which effectively removes the sensitivity of the data. Microshards are typically too small to contain a complete birth date, ID number, address, or other kinds of sensitive data. Next, the Microshards are mixed into multiple containers along with poison data to make it more unintelligible to unauthorized users.

Data distribution: To preserve data confidentiality even more, the containers are then distributed across multiple, segmented locations of your choosing, in the cloud, on-premises, or a combination of both, making unauthorized reassembly virtually impossible.



Copyright © 2024, ShardSecure, Inc.

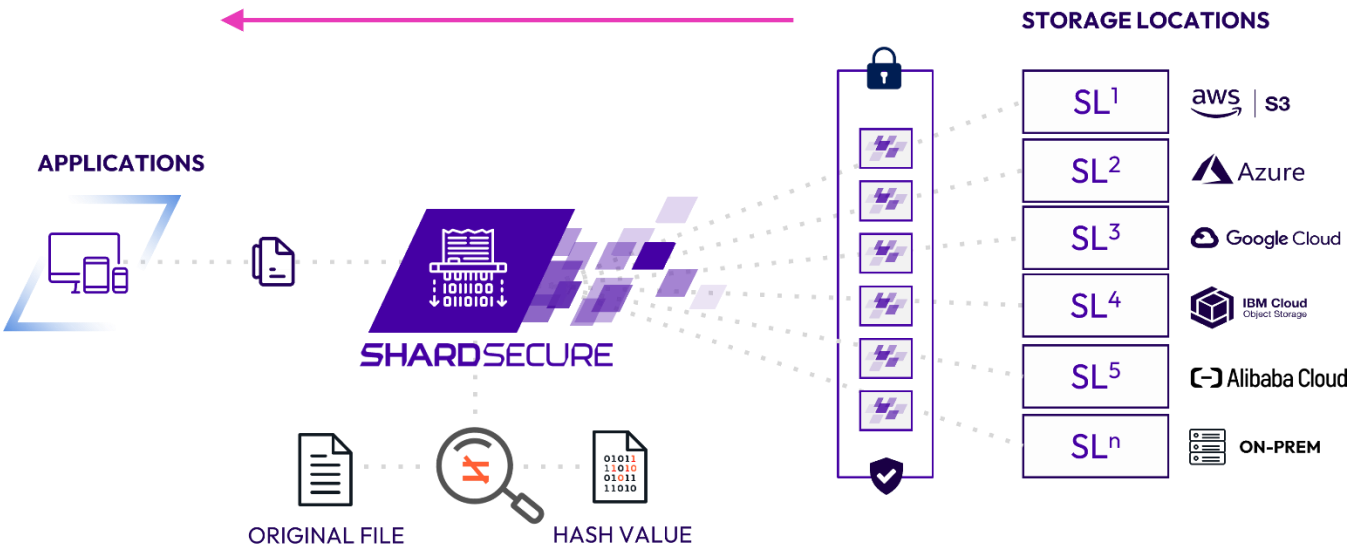
ShardSecure for data integrity

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.

Indicator of compromise: Microsharded data should never be modified at rest. If the hashes are mismatched, this is an indicator of compromise. We will generate an alert to your SOC, SIEM, SOAR, etc., for additional action or investigation.

File restoration: We don't stop at alerting. We will restore the affected Microsharded data to its last known good state and reassemble the unaltered file in real-time for your authorized users. This is the same process we use should the Microsharded data be tampered with, encrypted, or deleted.

Reduced risk from human error or cyberattacks: Should Microsharded data in one of your multiple storage locations become compromised due to malicious activity or human error, like misconfigurations that expose storage to the internet, data integrity is maintained seamlessly.



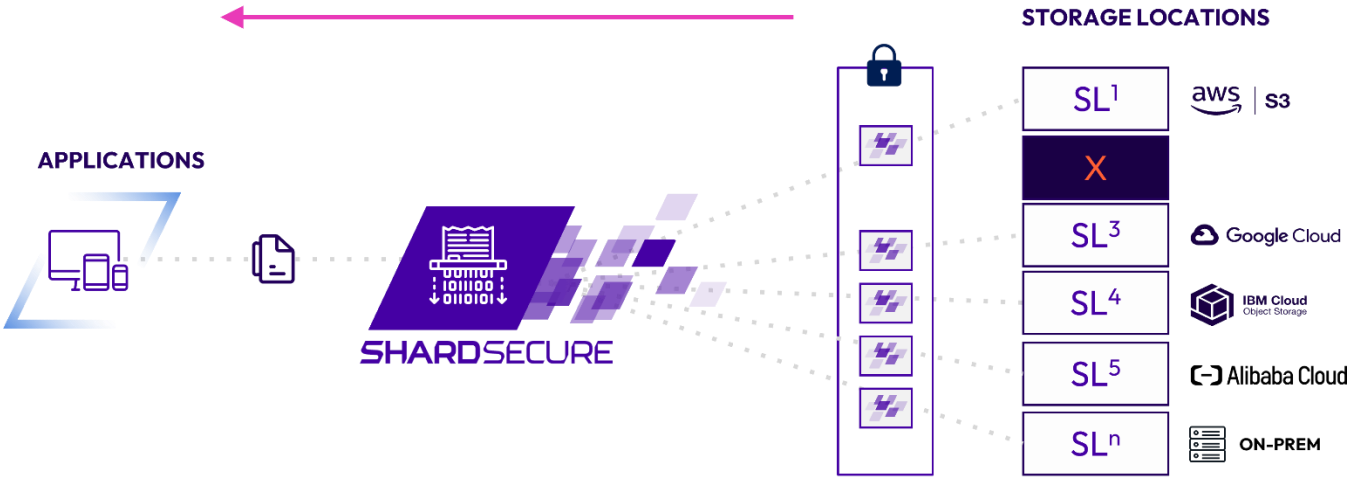
Copyright © 2024, ShardSecure, Inc.

ShardSecure for data availability

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
@ShardSecure
@ShardSecure

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

info@shardsecure.com