

SHARDSECURE™ ENGINE



THE SHARDSECURE ADVANTAGE:

The only solution capable of breaking data into shards small enough to break the atomic unit of value without sacrificing performance.

DATA SECURITY CHALLENGES:

- Sensitive data is vulnerable to costly breaches, most often caused by cloud misconfigurations
- Traditional encryption-only solutions are costly to buy and implement, and TCO is growing as keys need to be managed and changed for more and more endpoints
- Organizations are in a co-evolution race as cracking computers get faster and keys get longer
- The financial and reputational risks of storing sensitive data in the cloud prevent organizations from taking advantage of cloud's flexibility

SHARDSECURE SOLUTION:

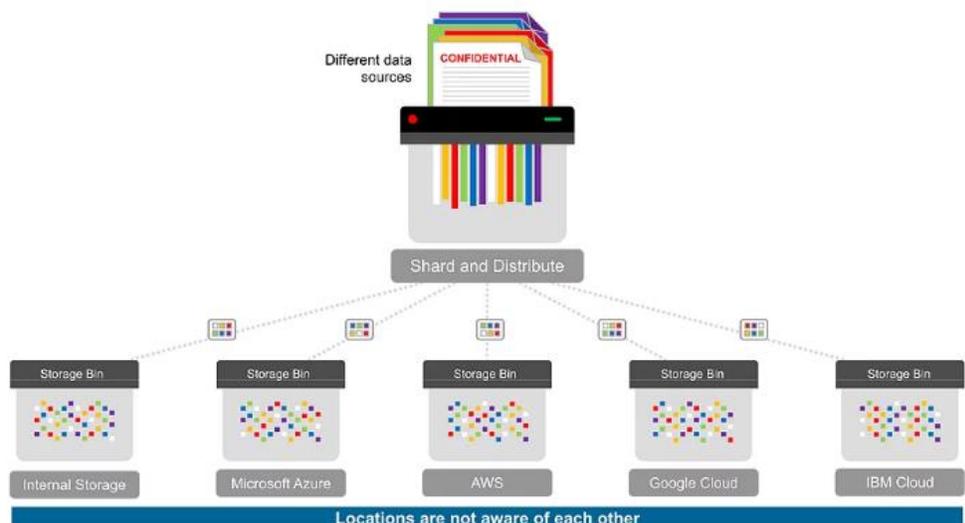
- Add a critical layer of defense to mitigate the risk of misconfigurations in the cloud
- Lower sensitivity of data and reduce compliance costs
- Regain control of cloud data, ensuring no single provider has the entire dataset
- Improve workflow and operational efficiency with data protection that doesn't impact performance
- Future-proofs data protection strategy in the age of quantum computing

ACCELERATE CLOUD ADOPTION BY DRASTICALLY REDUCING SENSITIVITY OF DATA

ShardSecure's Microshard™ technology breaks data into tiny bits and distributes them across multiple locations, making it virtually impossible for hackers to reassemble and providing a critical layer of protection that helps customers accelerate cloud adoption.

MULTIFACETED PROTECTION:

1. Microshard fragments can be set small enough to break the atomic unit of value. False shards can be added to “poison the well” to amplify protection.
2. Microshard data is distributed across multiple locations, making it nearly impossible for criminals to locate, identify and access. It can be distributed to:
 - > Local storage
 - > Google Cloud
 - > Amazon (AWS)
 - > IBM Cloud
 - > Microsoft Azure
 - > Oracle Cloud
3. Microshard data is reassembled for the legitimate users without sacrificing performance.



SHARDSECURE™ ENGINE

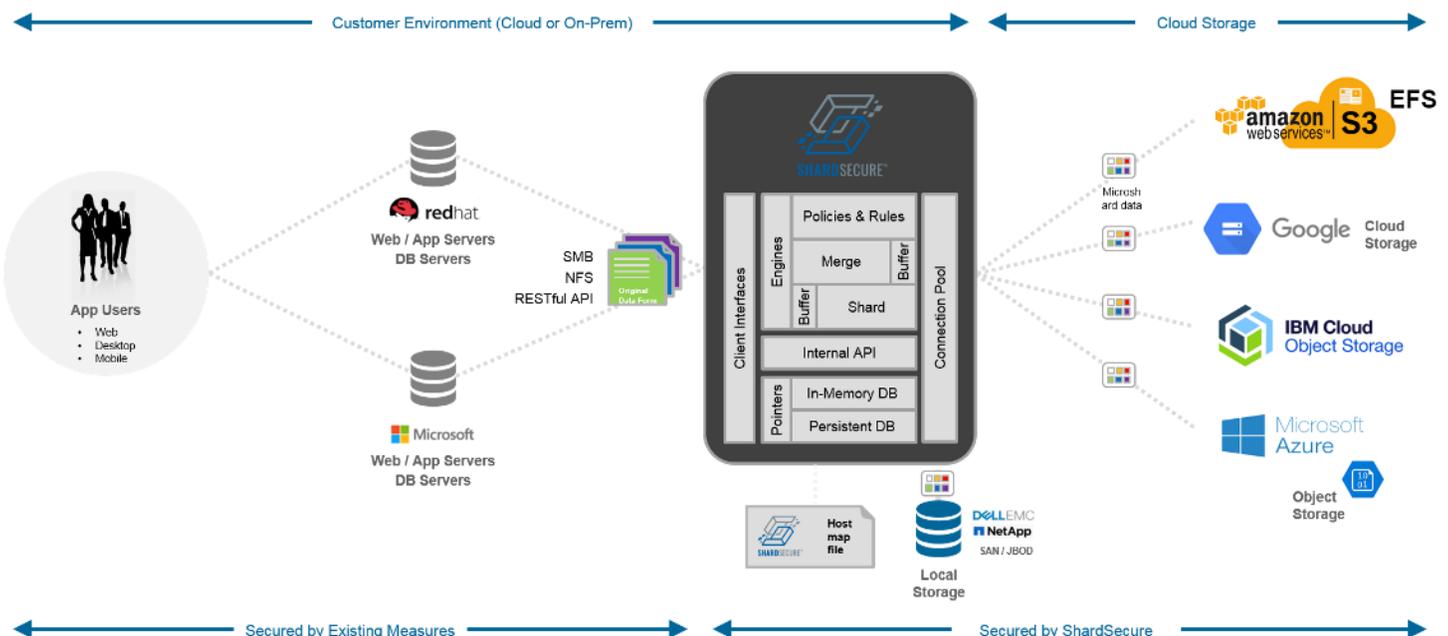


SHARDSECURE BUSINESS BENEFITS

- **Reduce Compliance Burden:** Microsharded data is fragmented and distributed rendering it unreadable and of no economic value to cyber criminals, reducing overall compliance burden.
- **Increase Productivity:** Embrace the scalability and flexibility of the cloud knowing company and customer information has been de-sensitized by ShardSecure. Improve workflow and operational efficiency with data protection that doesn't impact performance.
- **Stay a Step Ahead of Cyber Threats:** Microshard technology provides a critical layer of protection and can be layered on top of encryption to provide strong protection today and a path to achieve quantum-safe security in the coming years.
- **Lower cost and RTO:** move from on-prem backups with Iron Mountain to cloud, save on storage costs and reduce Mean Time to Recovery.

HOW IT WORKS

- ShardSecure is easy to deploy as a virtual machine or container either on-premises or in the cloud. The product looks like a disk and is application-agnostic (supporting files, database and streaming video).
- Data is protected via Microshard technology: broken into tiny bits before being distributed to multiple local and cloud storage locations. Locations are unknown to each other.
- Using pointers in the ShardSecure engine, Microshard data for legitimate users is reassembled back into its original form without sacrificing performance.



SHARDSECURE™ ENGINE



SHARDSECURE USE CASES:

- **Cloud Enablement:** Cloud misconfigurations are the number one cause of data breaches in the cloud. Microsharding drastically reduces the sensitivity of data in the cloud, protecting against security events caused by improperly configured data. ShardSecure is easy to deploy and manage with a virtual machine or as a container in the cloud, so customers can embrace the benefits of cloud knowing their data has been rendered meaningless and inaccessible to would-be hackers.
- **Secure File Sharing:** ShardSecure makes it possible for the most security-conscious organizations to share sensitive files and documents between locations, with third parties, and on-premises with high confidence. Microsharded data is only reassembled and accessible to parties with proper access credentials.
- **Lower Compliance Costs:** Government agencies like the New York State Department of Finance, who classes data protection as the number one threat within their jurisdiction, have begun mandating cybersecurity compliance, discouraging companies from excessive data concentration that puts them at risk for breach or loss. ShardSecure lowers these compliance costs, as Microshard data is broken into indiscernible bits and distributed such that it is no longer considered 'sensitive'.
- **Secure Cloud Backup:** Between regulatory and service requirements, the amount of data organizations are required to back up continues to skyrocket. The cloud provides rapidly scalable, flexible storage to meet those demands, but security concerns prevent organizations from embracing those benefits. By reducing data sensitivity with ShardSecure, organizations can confidently migrate backups to the cloud without fear of data breach and increased compliance costs.

