

Solution Brief

ShardSecure versus “harvest now, decrypt later”



The cyberattacks of the future are happening in the present

The “harvest now, decrypt later” (HNDL) strategy represents a looming threat, particularly for data stored at rest. In HNDL attacks, cybercriminals collect encrypted data in order to decrypt it later with the help of future advancements in computing power. Currently, encrypted data is not useful to an adversary when it is intercepted or unlawfully acquired without the corresponding decryption keys. However, traditional encryption algorithms may not stand the test of time, with the advent of quantum computing and other cryptographic breakthroughs threatening to render current encryption methods obsolete.

As organizations store increasing volumes of sensitive data, there’s a growing concern that this data will be exfiltrated today and decrypted tomorrow. “Although a CRQC [cryptographically relevant quantum computer] does not exist today, the possibility of one is a relevant threat now,” wrote the UK’s National Cyber Security Centre in 2020. The HNDL scenario poses a significant risk for a wide range of data stored at rest, including personal identifiable information (PII), intellectual property, financial records, and national security data. If this sensitive data is harvested now, future advancements may well enable cyberattackers to decrypt it in the future, leading to privacy breaches, IP theft, and other serious consequences.



The protective shield of microsharding: a novel defense strategy

Microsharding offers a groundbreaking approach to safeguard data at rest from the HNDL threat and mitigate the risks associated with this attack method. Microsharding shardsecure.com

involves breaking data into tiny, unintelligible fragments, or “microshards,” and distributing these microshards across multiple storage locations. This ensures that a complete dataset is never stored in a single location, significantly complicating unauthorized access and decryption efforts.

The ShardSecure platform is based on our patented microsharding technology. It offers advanced data security, privacy, and resilience by applying a dual-protection layer:

Data Sensitization: Data is shredded into four-byte microshards and mixed with poison data to ensure that individual microshards remain incomprehensible even if they’re accessed.

Distributed Storage: Then, the unintelligible microshards are dispersed across various locations. An attacker would need to compromise multiple storage locations and then accurately reassemble the shards to be able to access the original data, an exceedingly difficult task.

Mitigating quantum threats

A significant advantage of microsharding is its inherent resilience against quantum computing threats. Quantum computers, though potentially capable of breaking traditional encryption algorithms, will likely struggle with the fragmented and dispersed nature of microsharded data. The complexity of collecting, reassembling, and decrypting microshards across disparate locations introduces a multi-layered challenge that even quantum computing might find insurmountable (at least in our current theoretical models).

Advanced security without the performance impact

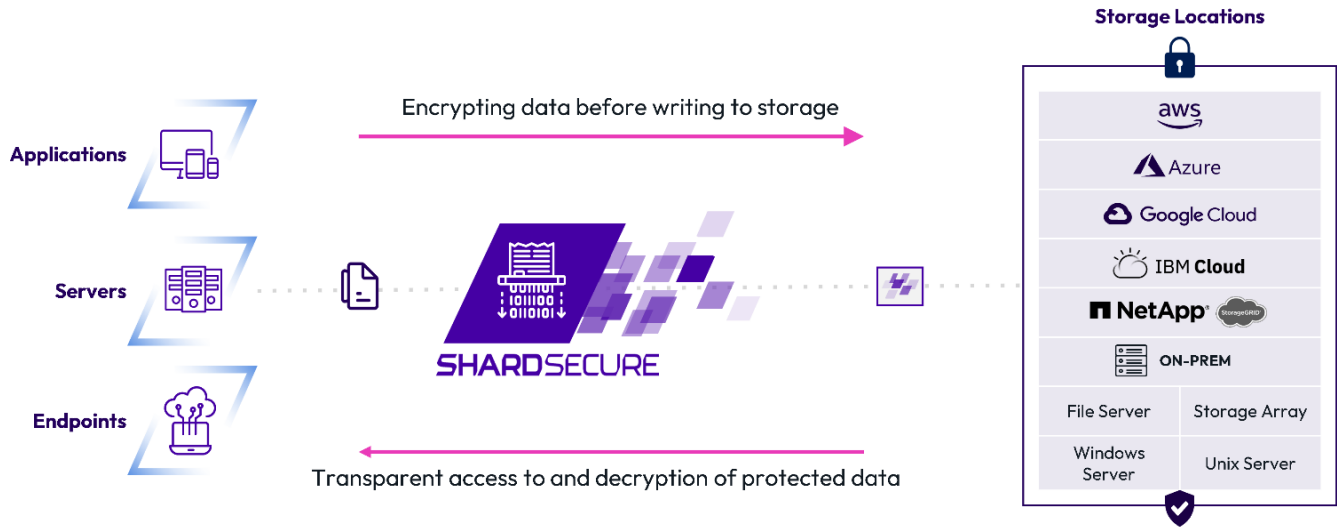
The microsharding process requires a robust infrastructure that can handle the distribution and management of microshards, ensuring data integrity and availability while preventing unauthorized access. The ShardSecure platform offers just such an infrastructure. It does not impact data

retrieval times or system performance; instead, it relies on efficient algorithms and network optimizations to ensure that security benefits do not come at the expense of user experience or operational efficiency.

Unified, multi-protocol platform across multiple clouds

ShardSecure supports interfaces like S3 for object storage, iSCSI for block storage, and SMB/NFS for file storage.

Since the ShardSecure platform acts as an abstraction layer, it can consolidate all storage interfaces into one, even though each cloud provider may support a different data storage interface. This approach reduces the complexity associated with migrating data to a multi-cloud architecture and implementing backup solutions across the enterprise.



Conclusion

As the threat landscape evolves, so must our strategies for protecting sensitive data. The “harvest now, decrypt later” strategy represents a significant risk, particularly as we’re poised on the brink of quantum computing breakthroughs. Microsharding offers a promising solution by protecting data through encryption, fragmentation, and distributed storage, complicating the efforts of adversaries. Leading industry analysts have called microsharding a quantum-safe technology, especially as an interim data protection approach during the long transition to quantum-safe encryption. With ShardSecure, organizations can fortify their defenses today and safeguard their data against the looming quantum threat of tomorrow.


Learn More

ShardSecure delivers strong data privacy, security, and resilience in a unified, multi-protocol platform that works across multiple cloud providers. Our platform offers robust data resilience, ransomware risk mitigation, protection for AI/ML models and training data, and support for regulatory compliance. To learn more, [follow us on social media](#) or [visit us online](#).

 @ShardSecure

 @ShardSecure

 @ShardSecure

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

 info@shardsecure.com

**SHARD
SECURE**