

White Paper



Our patented Microshard™ technology desensitizes sensitive data in the cloud. Its three-step process works to shred, mix, and distribute data to multiple storage locations of your choice, and its self-healing data helps to neutralize the impact of cloud ransomware and other attacks.

Shred: Microshard technology begins by shredding data into four-byte microshards that are too small to contain a birthdate, an ID number, or any complete piece of sensitive data. The size of the microshards is configurable, and policies may be applied to optimize the microshard size according to file type.

Mix: Next, poison data is added and the microshards are mixed into multiple logical Microshard containers. Identifying information like file extensions, file names, and other metadata is also removed, making unauthorized reassembly even more complex. The amount of poison data to be added is also configurable.

Distribute: After being mixed, the Microshard containers are distributed across multiple customer-owned storage repositories in multi-cloud or hybrid-cloud configuration. Each storage location contains a 1/n-1 fraction of the complete data set, with one Microshard container reserved for parity.

Mitigating the impact of cloud ransomware with microsharding



Overview

Ransomware has grown exponentially over the past few years. The European Union Agency for Cybersecurity (ENISA) noted a 150% rise in ransomware attacks between 2020 and 2021, and the average ransom payment is at an all-time high of \$812,360.¹ When additional expenses — including third-party remediation services, regulatory fines, higher cyber insurance premiums, lost wages, lost time, and equipment replacement — are factored in, it's no wonder that recovering from an attack costs businesses an average of \$1.85 million in 2021.

With enterprise data increasingly moving to the cloud, organizations are now beginning to document cloud ransomware incidents as well as typical on-premises attacks. To help mitigate the impact of ransomware — including both data encryption and data exfiltration aspects — Microshard technology provides advanced security for your sensitive data in the cloud.



Features To Help Neutralize the Effect of Cloud Ransomware

Self-Healing Data

Cloud ransomware typically functions by encrypting data so that authorized users can no longer access it. Microshard technology's self-healing data allows it to reconstruct data that ransomware attackers have encrypted.

By creating slight overlaps of the distributed Microshard data across the different storage locations, the ShardSecure engine can rebuild data containers and return them to their unaffected state in real-time. Similarly, if a data storage location becomes unavailable for any reason — an outage, a network issue, a misconfigured firewall — the same process reconstructs the unavailable Microshard data.

This process happens transparently and with an automated control. That means that ransomware repairs can begin automatically and in a way that is transparent to users, often avoiding major outages.

¹ Palmer, D. *Ransomware: It's a 'golden era' for cyber criminals — and it could get worse before it gets better*. ZDNet. Retrieved July 15, 2022, from <https://www.zdnet.com/article/ransomware-its-a-golden-era-for-cyber-criminals-and-it-could-get-worse-before-it-gets-better/>

Data Integrity Checks

Microshard technology's self-healing capability is made possible through multiple data integrity checks to detect unauthorized modifications — including those caused by cloud storage ransomware.

Using an automated control, multiple data checks detect changes like those caused by cloud storage ransomware and respond by rolling back data to its earlier state. This means that real-time ransomware repairs can begin automatically and in a way that is transparent to users.

If a Microshard container fails a data integrity check during the reassembly process, the user's security team is alerted and the affected container is reconstructed to its unaffected state. This automated control means that this recovery process begins without manual intervention so that users can continue working unaffected and organizations can maintain business continuity.

Thwarting Data Extortion Attempts

The three-step Microshard process helps to protect sensitive data in the cloud by eliminating its sensitivity. Even if a customer storage location is compromised, Microshard data is distributed to multiple customer-owned storage locations. This provides a layer of abstraction between applications and the storage locations.

Thus, Microshard technology creates a spatial challenge for ransomware attackers who intend to exfiltrate data for the purpose of extortion — an increasingly common aspect of ransomware attacks. Instead of gaining confidential data that they can threaten to publish, an attacker who accesses a Microshard data container will only gain an unintelligible fraction of that material. With poison data added and all identifying metadata removed, the original sensitive data becomes virtually impossible for a threat actor to reassemble.

This effectively removes the means of extortion from the ransomware attack, since there is nothing intelligible for attackers to threaten to publish.

Business Continuity

Microshard technology improves business continuity by maintaining data confidentiality, integrity, and availability — the three pillars of the CIA triad. Its self-healing data, high availability and failover, responsive storage, file integrity verification, and data agility all help to ensure that users can continue to access their data securely and reliably during disruptions and outages.



Conclusion

From purchasing a cyber insurance policy and keeping systems patched to providing employee training on phishing attempts, organizations can take many steps to help protect themselves against ransomware. But even with the best security protocols in place, accidents happen.


Microshard technology offers a way to neutralize the impact of both the data encryption and data exfiltration aspects of cloud ransomware. To protect your sensitive data at rest, Microshard technology offers self-healing data, high availability and failover, responsive storage, file integrity verification, data agility, and more.

For more information on how ShardSecure is helping organizations in financial services, pharmaceuticals, biotech, and social media strengthen their data security, [visit us online](#) or book a demo.

 @ShardSecure

 @ShardSecure

 @ShardSecure

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

 info@shardsecure.com

**SHARD
SECURE**