Mitigate Cloud Ransomware

Discover how the ShardSecure platform’s data integrity checks, high availability, and self-healing feature mitigate the impact of ransomware.

Whether data is stored on-premises, in the cloud, or in hybrid- or multi-cloud architectures, ransomware is a growing threat. Attackers are using ransomware-as-a-service (RaaS) and AI technologies to facilitate more sophisticated attacks, and the cost is only rising. According to 2022 figures, one in ten targeted organizations paid ransoms of $1 million or more. That doesn’t take into account the additional costs of recovery, remediation, and regulatory fines if data is exposed.

With the average ransom costing over $800,000, organizations need advanced data security and robust data resilience to protect themselves against attacks. Below, we explore how the ShardSecure platform mitigates cloud ransomware and helps organizations maintain their business continuity.

The ShardSecure platform performs data integrity checks that are able to detect when data has been encrypted, deleted, or otherwise modified by ransomware attackers. When a discrepancy is detected, the platform’s self-healing feature automatically reconstructs the affected data. It does so transparently and without disrupting users or data flows.

The same self-healing feature also works to reconstruct data that has been deleted by ransomware attackers, who will sometimes delete data if they are unable to exfiltrate it for profit. Additionally, it protects backups, which are sometimes targeted by malicious actors before the main attack is launched.

Providing high availability for business continuity

One of the many dangers of a ransomware attack is the cost of downtime. By encrypting critical data, attackers can bring systems and services offline.

The ShardSecure platform helps companies maintain their business continuity with high availability at multiple levels. First, each instance of ShardSecure is a virtual cluster that can run on-prem, in the cloud or hybrid. Second, customers can configure two or more virtual clusters for failover, which provides high availability across multiple clouds as well as in hybrid-cloud environments that use a mix of on-premises, private cloud, and third-party public cloud services.
Maintaining data confidentiality in double extortion attacks

A common technique used by ransomware attackers is to exfiltrate sensitive data from their victims to use as blackmail. Attackers will threaten to expose the stolen data on the internet — often by selling or publishing it on the dark web — if the ransom is not paid.

The ShardSecure platform mitigates double extortion attacks by rendering data unintelligible to unauthorized users. With our technology, attackers who access an organization’s storage locations may be able to exfiltrate data, but that data will remain unexploitable. It cannot be reconstructed by unauthorized users, so it cannot be used for extortion.

Migrating data automatically

The ShardSecure platform’s automatic data migration feature allows customers to configure alternate storage locations. User-configured thresholds may be set such that if X number of data integrity checks fail in Y timeframe, then all the data in the original location is automatically migrated to the backup location. This migration happens in the background with no downtime, ensuring a seamless transition to the secure alternate location while the problem is being investigated.

Streamlining implementation and management

The ShardSecure platform offers simple, agentless integration and management with no need to change application behaviors or data flows. Without the overhead and complexity of traditional data security solutions, it is infrastructure vendor-agnostic and completely transparent to SaaS services and applications.

Each instance of the ShardSecure platform is a virtual cluster that may be deployed on-site or in the cloud. The S3-compatible API, SMB/NFS, and iSCSI interface make it simple for applications to migrate to ShardSecure with minimal to no configuration changes.

As a result, ShardSecure has minimal impact on development and operations teams. The ShardSecure platform works in the background as a transparent, zero-downtime event, and data protection is achieved without expending significant resources on running and maintaining complex systems.

Learn More

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