SHARDSECURE

Solution Brief

Mitigate Cloud Ransomware

Discover how the ShardSecure platform mitigates 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. Currently, the average ransom payment is at an all-time high of over $1.5 million per incident, and that doesn't include the additional costs of recovery, remediation, and potential regulatory fines.

With an attack happening every 11 seconds, organizations need advanced data security and robust data resilience to protect themselves. Below, we explore how the ShardSecure platform's features can mitigate cloud ransomware and help organizations maintain their business continuity.

High availability

One of the key dangers of a ransomware attack is the cost of downtime. The ShardSecure platform helps companies lessen downtime and 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 in hybrid architectures. 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 providers like AWS, Azure, and GCP.

Automatic self-healing and SOC alerts

When a storage location fails a data integrity health check because of a ransomware attack or other forms of data tampering, the ShardSecure platform's self-healing feature automatically reconstructs the affected data. The feature works transparently and without disrupting users or data flows, allowing organizations to maintain business continuity during an attack. The self-healing feature also works to reconstruct data that has been deleted by ransomware or malware attackers.

Additionally, when a storage location fails a data integrity health check, the ShardSecure platform sends an automatic alert to the SOC team. This feature acts as an early warning for security teams to enable faster detection, investigation, and remediation.

Protection against double extortion attacks

The ShardSecure platform mitigates data exfiltration and double extortion ransomware attacks by rendering data unintelligible to unauthorized users. If an attacker manages to directly access an organization's storage locations to exfiltrate data, that data remains illegible and unexploitable. It cannot be reconstructed by unauthorized users, so even the most sensitive information cannot be published or used for extortion.

Automatic data migration

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 Tier 1 storage is automatically migrated to Tier 2. This migration happens in the background with no downtime, ensuring a seamless transition to the secure alternate location.

Immutable storage interface and rollback for rapid recovery

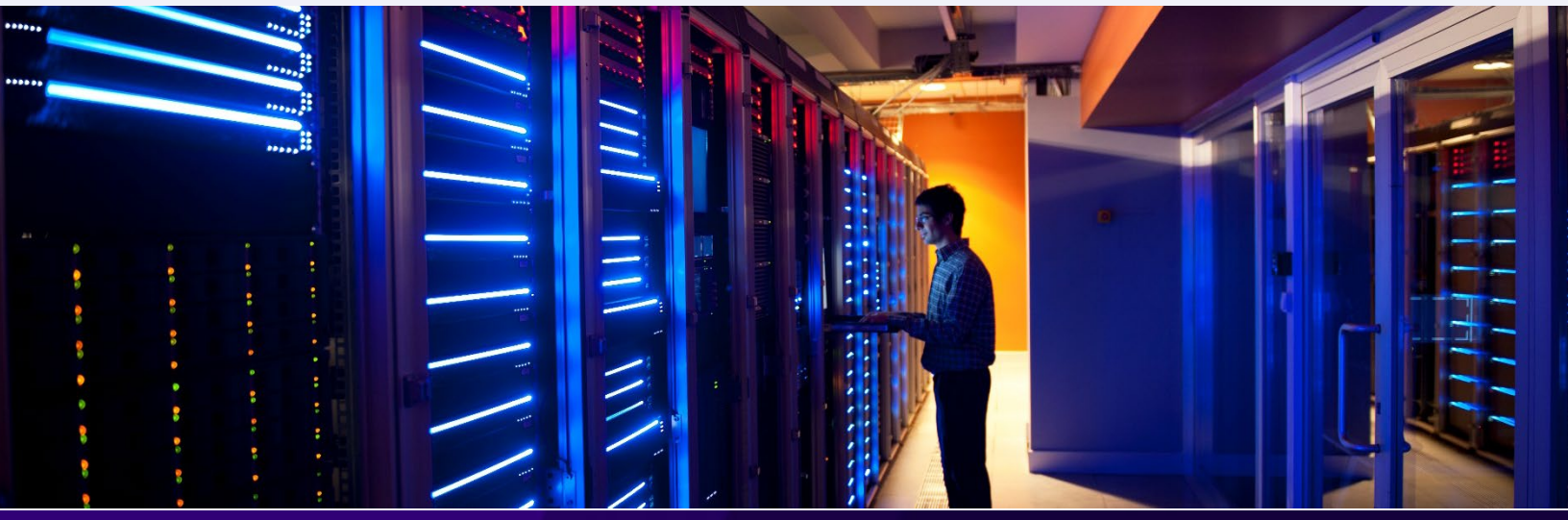
To mitigate the risk and potential damage caused by credential-based ransomware attacks, ShardSecure also offers features like object locking and an immutable storage interface. In the event of a credential-based ransomware attack, data can be rolled back and restored to any point in time prior to the attack, supporting rapid recovery efforts. These capabilities greatly reduce the dependance on time-intensive traditional recovery techniques like last-resort backup solutions.

Unified, multi-protocol platform across multiple clouds

Finally, the ShardSecure platform offers simple, agentless integration and management without the overhead and complexity of traditional data security solutions. The platform is infrastructure- and vendor-agnostic and is completely transparent to existing services and applications. The S3-compatible API, SMB/NFS, and iSCSI interface make it simple for applications to migrate to ShardSecure with minimal to no configuration changes, and the platform works in the background as a zero-downtime event. As a result, ShardSecure achieves data protection and ransomware mitigation with minimal impact on development and operations teams.

Learn more

ShardSecure delivers strong data privacy, security, and resilience in a unified, multi-protocol platform that works across multiple cloud providers. Our platform supports robust data resilience, cloud ransomware mitigation, protection for AI/ML models and training data, and regulatory compliance. To learn more about our technology, 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