SHARDSECURE

White Paper:

Mitigating the impact of ransomware attacks with ShardSecure

Overview: the ever-growing threat of ransomware

The threat of ransomware attacks has grown steadily over the last several years. Cybersecurity Ventures notes that a business suffers a ransomware attack every 11 seconds, while the Verizon Data Breach Investigations Report estimates a 13% rise in attacks last year. By 2031, it's projected that there will be a ransomware attack every 2 seconds.

The cost of ransomware attacks is also growing significantly. The average ransom payment is at an all-time high of over $1.5 million per incident. When additional expenses — including third-party remediation services, regulatory fines, downtime, and lost revenue — are factored in, it's no wonder that recovering from an attack now costs businesses an average of $3.32 million per incident. Research also indicates that the enterprise shift to the cloud brings new threat vectors and an increase in attacks that focus solely on data exfiltration.

This white paper explores the complex challenges posed by ransomware. It also discusses how the ShardSecure platform mitigates the various impacts of a ransomware attack, including both data encryption and data exfiltration attacks, with features like self-healing and robust data resilience.

The multifaceted threat of ransomware

The potential consequences of a ransomware attack are severe. Organizations face not only the immediate disruption of their operations but also the long-term impacts of reputational damage, financial loss, and legal consequences.

Losing data and data access

The most familiar consequence of a ransomware attack is its central feature: preventing victims from accessing mission-critical data. By encrypting data, attackers can bring entire businesses, systems, and services offline.

It's important to note that very few organizations are able to regain all their data after an attack, even if they cooperate with attackers. According to a 2022 Sophos report, organizations that paid ransoms recovered only 61% of their data, and only 4% of organizations recovered all their data. Even if a business is able to restore its systems without any data loss, the downtime is likely to be costly. For Fortune 1000 companies, a single hour of downtime may cost up to $1 million.

When ransomware goes undetected

The problem of ransomware is compounded by variants that spread by evading detection. These more sophisticated forms of ransomware are able to infiltrate networks without being detected by conventional security measures, enabling attackers to inflict greater damage, demand higher ransoms, and infect data backups. Some ransomware also targets backups intentionally. For example, one variant includes the capability to lock cloud-based backups when systems continuously back up in real-time (i.e., during persistent synchronization).

Double extortion and data exfiltration

In double extortion ransomware, cybercriminals exfiltrate sensitive data from their victims to use as blackmail. The attackers then 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. Data exfiltration has become an increasingly common element of ransomware attacks, since it gives cybercriminals more leverage and raises the chance that they'll receive payment.

A thriving industry: RaaS, AI, and supply chain attacks

The forecast for cloud ransomware remains grim. The rise of the ransomware-as-a-service (RaaS) model has led to an increase in the number of attacks, and new tools like AI have

facilitated more effective phishing. These developments have lowered the barrier-to-entry for cybercriminals, allowing even those with limited technical expertise to stage major attacks. Meanwhile, organized ransomware gangs have become increasingly sophisticated in their tactics, techniques, and procedures (TTP), gaining in-depth knowledge of cybersecurity vulnerabilities and exploiting technical weaknesses to infiltrate systems.

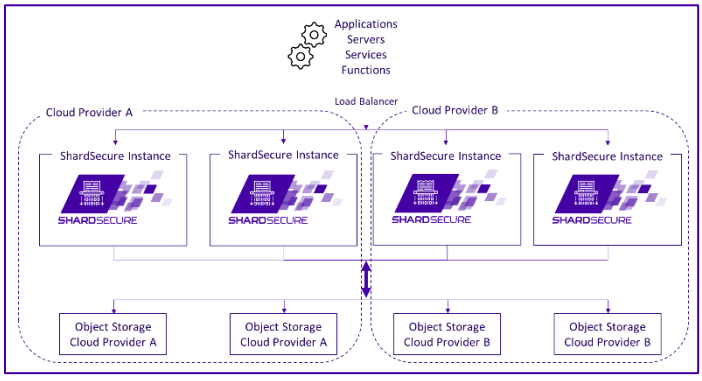
With no end in sight, the consensus is that ransomware is no longer an "if" but a "when." Organizations must take a proactive approach to their cybersecurity, implementing robust data protection solutions to safeguard their sensitive data from ransomware.

Mitigate ransomware attacks with ShardSecure

The ShardSecure platform's data integrity checks, high availability, and self-healing features mitigate the impact of ransomware attacks. The platform extends protection wherever data is stored: on-prem, in the cloud, or in hybrid- or multi-cloud architectures. Below, we explain how the ShardSecure platform mitigates ransomware attacks and helps organizations maintain their business continuity.

Robust data resilience to maintain data access during an attack

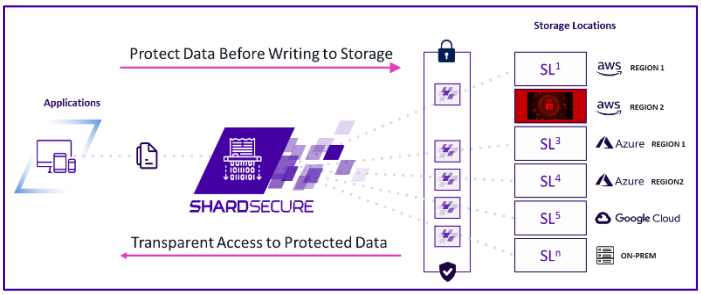
The ShardSecure platform offers robust data resilience, including high availability and data integrity, to help companies maintain data access during a ransomware attack.



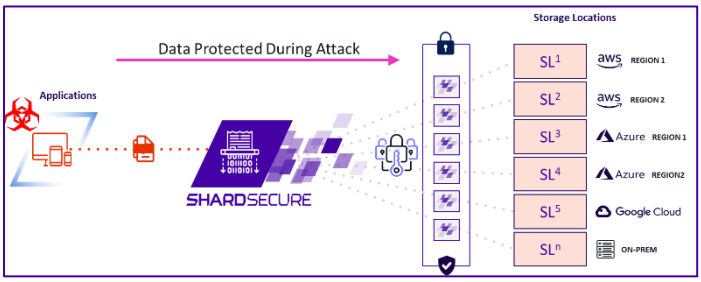
To achieve high availability, each instance of ShardSecure is a virtual cluster that can run on-prem, in the cloud, or in hybrid-cloud architectures. Customers can configure two or more virtual clusters for failover, which provides high availability across multiple clouds as well as in hybrid-cloud environments that use a mix of on-premises, private cloud, and third-party public cloud providers like AWS, Azure, and GCP.

Automatic data migration to prevent repeated attacks. 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 time frame, 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.

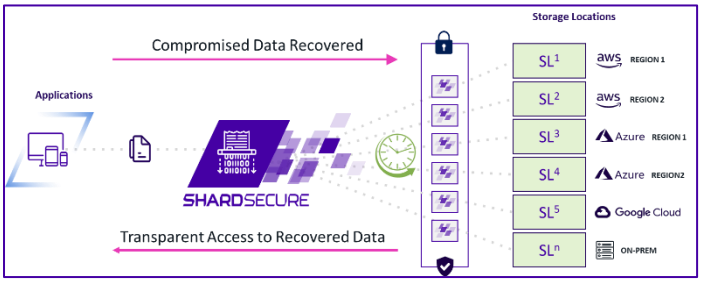
Automatic self-healing to reconstruct lost or compromised data. When a storage location fails a data integrity health check because of a ransomware attack or other forms of data tampering, the ShardSecure platform's self-healing feature automatically reconstructs the affected data. The feature works 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 attackers, who will sometimes delete data if they are unable to exfiltrate it for profit.



Immutable storage interface and rollback for rapid ransomware recovery. Credential abuse occurs when ransomware attackers use stolen credentials to gain unauthorized access to critical data and encrypt it. To mitigate the risk and potential damage caused by credential-based ransomware attacks, ShardSecure offers features like object locking and an immutable storage interface to ensure that valuable data remains available, accurate, and secure.



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 traditional recovery techniques from time- and labor-intensive last-resort backup solutions.



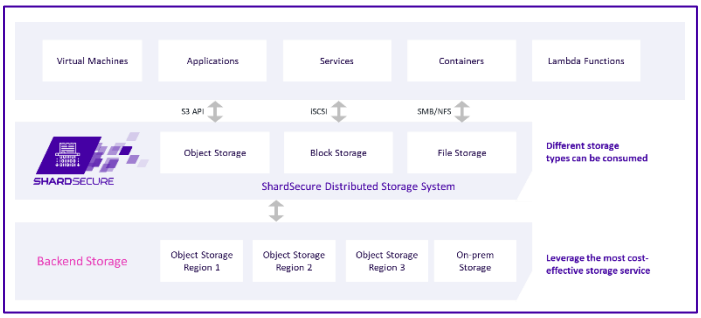
Automatic alerts to the SOC in the event of an attack. When a storage location fails a data integrity health check, the ShardSecure platform also sends an automatic alert to the SOC team. This feature acts as an early warning for security teams to enable faster detection, investigation, and remediation, thereby reducing the chance of the ransomware evading detection.

Protection against data exfiltration

The ShardSecure platform mitigates double extortion 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. Our innovative approach to file-level encryption offers advanced privacy for sensitive data, regardless of its storage location.

Unified, multi-protocol platform across multiple clouds

The ShardSecure platform offers simple, agentless integration and management without the overhead and complexity of traditional data security solutions, and with no need to modify application behaviors or data flows. The platform is infrastructure- and vendor-agnostic and is completely transparent to existing 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 the need to expend significant resources to maintain complex systems.

Conclusion

As the digital landscape becomes increasingly interconnected, the damage caused by ransomware attacks continues to grow. The number and cost of attacks are on the rise, and the challenges for organizations are both numerous and complex.

The ShardSecure platform mitigates ransomware with robust data resilience, automatic self-healing, SOC alerts, and protection against data exfiltration.

Its features help organizations protect sensitive information and avoid the financial losses and reputational damage of ransomware attacks.

For more information on how ShardSecure is helping organizations in financial services, healthcare, manufacturing, and biotech 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