



Solution Brief

ShardSecure for Kubernetes



Introduction

Kubernetes (also known as K8s) is an open-source platform maintained by the Cloud Native Computing Foundation. It allows organizations to automate their application development, deployment, scaling, and management processes in the cloud. Kubernetes offers tools for a range of technology domains, including AI, machine learning, blockchain, data management, the Internet of Things (IoT), 5G, etc. As a result, many organizations are accelerating their Kubernetes investments for both existing applications, as well as new workloads.

Kubernetes, however, is not without its challenges. For example, K8s clusters are not secure by design, the platform is notoriously complex to manage, and skilled engineers can be difficult to find. However, its ability to help organizations scale at speed is making it an important part of the cloud adoption journey.

To address some of these challenges, ShardSecure developed an advanced data security, privacy, and resilience platform that is purpose-built to support these types of environments. By deploying the ShardSecure platform, companies can take advantage of all the benefits that Kubernetes has to offer, while still protecting their data from unauthorized access, mitigating ransomware attacks, maintaining high availability, and enabling compliance with privacy regulations.

Complexity & Resource Constraints

Many solutions address only a single aspect of data security, resilience, or privacy, but data protection needs to extend to every part of the organization. With budget cuts looming, technologies that can address multiple pain points at once are in high demand.

Most data security solutions tend to increase complexity and require changes to user workflows and applications because they typically rely on traditional encryption techniques. These solutions often use agents, which may be incompatible with newer architectures and are difficult to scale.

Growing Volumes of Data

Unstructured data makes up at least 80% of enterprise data and is growing at four times the rate of structured data. But despite this rapid increase, current solutions for securing unstructured data tend to impact performance and are resource intensive. File-level protection that enables both flexibility and compliance is becoming a must-have.

Privacy Regulations

Data privacy has never been more important, and regulations like the GDPR are making an already challenging environment even trickier to navigate. Unfortunately, traditional data security and privacy solutions can't keep up with changing regulations. With the continual release of new and emerging guidelines, meeting compliance requirements has become a moving target for most organizations.



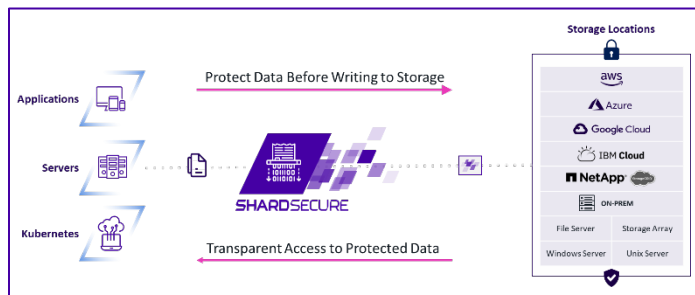
ShardSecure Data Security & Privacy

At ShardSecure, we believe that all organizations can enjoy the flexibility of storing their data wherever they want — on-prem, in the cloud, or in hybrid-cloud architectures. With strong data security, ransomware mitigation, robust data resilience, support for cross-border regulatory compliance, and simple plug-and-play integration, our technology offers a multifaceted solution to a complex set of challenges.

Agentless Data Security

In the past, organizations protected their data from unauthorized access with agent-based encryption solutions. Unfortunately, traditional agent-based solutions tend to slow performance by 5% to 40%. They are also difficult to manage and scale and may be incompatible with Kubernetes environments and other cloud services.

ShardSecure offers an innovative, agentless alternative to agent-based file-level protection with “set and forget” management. The ShardSecure platform secures data from threats without the cost and complexity of agent-based solutions and provides strong data confidentiality and resilience in the process.



ShardSecure’s abstraction layer sits between applications and storage infrastructure, where it performs advanced file protection. This approach allows for simple plug-and-play implementation without changes to the underlying Kubernetes infrastructure or associated workloads.

ShardSecure’s low latency and fast throughput architecture has minimal to no performance impact and data access is maintained without requiring changes to existing applications.

Automatic Self-healing

ShardSecure maintains strong data integrity with multiple health checks to detect unauthorized data tampering, alert security teams of a potential attack, and automatically reconstruct compromised data in real-time. This ensures that data remains accurate and unaltered, not just available.

ShardSecure’s configurable data migration feature allows admins to automatically migrate data to a safe alternate location in the event tampering is detected. If a specified number of data integrity check failures take place, all the data in the affected storage location can be automatically migrated to the secure location with no downtime.

Data Exfiltration

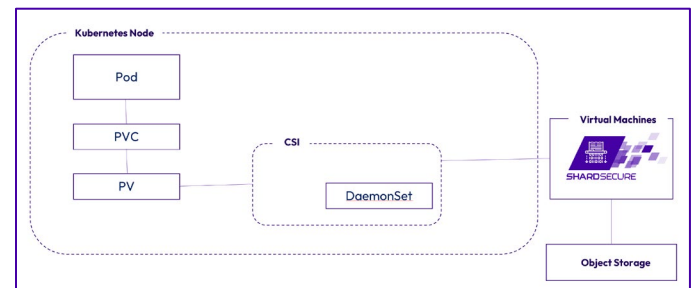
The ShardSecure platform mitigates the impact of double extortion ransomware attacks, where criminals

threaten to release or sell sensitive data that they have exfiltrated prior to encrypting it. Since the ShardSecure platform renders data unintelligible to unauthorized users, exfiltrated data is of no value to attackers.

Scalable Persistent Storage for Kubernetes

ShardSecure offers a wide variety of interfaces for different types of data storage services. To support the growing trend of Kubernetes adoption, ShardSecure developed a Container Storage Interface (CSI) to simplify the deployment, integration, and support in Kubernetes environments. The CSI plug-in runs as DaemonSet on existing Kubernetes nodes and provides a standard interface for pods to provide secure, resilient, and scalable persistent storage.

The ShardSecure platform also enhances automation by automatically provisioning disk space for pods in Kubernetes, without the need to manually add any additional servers or services.



ShardSecure can also expose an S3-compatible API and act as an abstraction layer that sits between an application and object storage. Applications, servers, and Kubernetes workloads would then access object storage via ShardSecure’s S3-compatible API. In addition, object storage can be in multiple regions with multiple cloud providers.

Data Privacy

A growing number of jurisdictional data privacy regulations make it difficult for businesses to store data where they want. With strict cross-border data privacy laws, it’s becoming increasingly difficult for companies to protect their data, remain compliant, and take advantage of the cloud.

ShardSecure enables multi-national organizations to use the cloud storage providers of their choice, in the geographic locations and jurisdictions of their choice, to mitigate data transfer risk and address data sovereignty and compliance concerns. Data can be distributed across different regions of a single cloud provider, across multiple cloud providers, or across a hybrid mix of on-premises storage and one or more cloud providers.

ShardSecure also meets the requirements of the EDPB’s Use Case 5 in Schrems II. The ShardSecure platform is a split processing technology that can be deployed in a

multi-party processing environment, meaning that it allows organizations to store and process data safely under Use Case 5.

As cyber audit and assurance firm UHY Advisors states: “ShardSecure has the potential to lower cyber risks and compliance costs while maintaining compliance with the spirit of European and US data protection regulations.”

ShardSecure has been named a Gartner Cool Vendor in the August 2023 Cool Vendors for Privacy report.

Key Features & Microsharding

ShardSecure’s patented Microshard technology protects data at rest and makes sensitive data unintelligible to unauthorized users. When data is shredded using the ShardSecure platform, the resulting microshards are too small to contain sensitive data. Mixing the microshards and distributing them helps to ensure unauthorized users never have a complete, intelligible data set should storage be compromised.

Microshard size can be configured to eliminate the possibility of sensitive data and contextual metadata existing, and poison data can be added before microshards are distributed to storage locations as an additional layer of protection.

Migration & Flexible Storage Options

The ShardSecure platform allows organizations to choose the type of storage architecture that works best for them, depending on their architecture. With ShardSecure, data can be distributed across different regions of a single cloud provider, across multiple cloud providers, or across a hybrid mix of on-prem storage and one or more cloud providers. It allows users to configure the number and locations of storage buckets, so data can be stored in any geographic location or jurisdiction.

ShardSecure works with cloud providers ranging from AWS and Azure to Google Cloud Platform and Alibaba Cloud, giving organizations the freedom to embrace the infrastructure that best suits their needs and business goals. Whether they prefer to keep some data on-prem or use several different cloud providers in different parts of the world, companies can rest assured that their data will remain safe from unauthorized users.

The ShardSecure platform supports a wide variety of storage destinations, including:

<ul style="list-style-type: none">• Local disk• Amazon EFS and S3• Google Cloud Platform• Kubernetes CSI• Wasabi• Backblaze• Dropbox• NFS	<ul style="list-style-type: none">• Microsoft Azure Blob• Microsoft SMB shares• IBM Cloud Object Storage• Alibaba Cloud• Box• FUSE
--	---

Simple Integration & Access

Despite its powerful data security, privacy, and resilience features, the ShardSecure platform has minimal impact on existing workloads, applications, and users, delivering instant data access and fast data migration among different storage locations with just a few clicks.

A vendor-agnostic solution that works in the background as a zero-downtime event, the ShardSecure platform appears and behaves like a traditional storage interface to applications, requiring minimal code changes for deployment.

Since the platform is also transparent, user workflows are not impacted. There are no visible changes to employee UX, and retraining employees or redesigning applications is unnecessary. This allows for a seamless integration with existing operations.

Conclusion


Data security, privacy, and resilience have never been more important, and the threats to organizations have never been greater. Regardless of where sensitive data resides — on-prem, in the cloud, or in a hybrid- or multi-cloud architecture — it needs to be protected and secure. ShardSecure provides this security and privacy, while keeping you in control of your data, and offers agentless file-level protection, robust data resilience, advanced data privacy, support for compliance with cross-border regulations like the GDPR, and ransomware mitigation. By leveraging ShardSecure’s innovative microsharding approach and Kubernetes support, organizations can improve their data security and be better prepared for future threats.

For more information about ShardSecure, [visit us online](#), follow us on [social media](#), or [schedule 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**