SHARDSECURE / ENTRUST

Solution Brief

Entrust KeyControl Vault for File Encryption

Protect sensitive unstructured data with ShardSecure

Overview

Ensuring data security is a critical necessity for modern-day businesses. 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 newer workloads and 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.

ShardSecure’s low latency and fast throughput architecture have minimal to no performance impact. Data on end devices can be accessed without requiring changes to existing applications.

The Entrust/ShardSecure partnership ensures that unstructured data in cloud environments is well protected against outages, attacks, and other forms of data compromise. ShardSecure’s integration with KeyControl Compliance Manager provides a singular dashboard view of keys across on-prem, public cloud, and hybrid cloud environments, including information about ownership, environment, purpose, and critical system.

In addition, the integration between ShardSecure and Entrust eShield HSM combines the benefits of ShardSecure’s file-level encryption with the secure key generation and management of Entrust’s nShield HSM (Hardware Security Module).

KEY FEATURES

- Secure unstructured data wherever it resides – on-prem, in the cloud, or in hybrid- and multi-cloud architectures
- Strong data privacy and security in a unified, multi-protocol platform across multiple cloud providers
- Separate data owner from infrastructure owner and cloud provider
- Agentless deployment with minimal performance impact
- Simple integration with existing applications and data workflows
- Highly available and scalable architecture
- FIPS 140-2 compliant
- Native integration with Entrust eShield HSMs (hardware security modules)

Benefits

Meet regulatory requirements for 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 like the EU’s General Data Protection Regulation (GDPR), the anticipated Schrems III ruling, and the CCPA/CPRA in the US, it’s becoming increasingly difficult for companies to protect their data, remain compliant, and take advantage of the cloud.

With ShardSecure, businesses can 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 Use Case 5 of the EDPB's recommendations for cross-border data transfers under the GDPR. The ShardSecure platform is a split processing technology that can be easily deployed in a multi-party processing environment, meaning that it allows organizations to store and process data safely under Use Case 5.

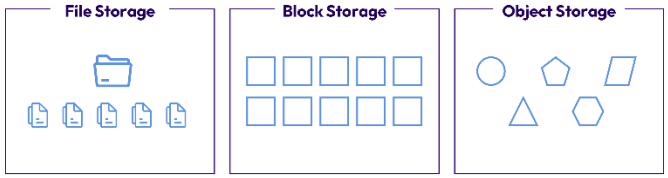
As cyber audit and assurance firm UHY Advisors states: "ShardSecure has the potential to lower cyber risks and compliance costs while maintaining compliance with the spirit of European and US data protection regulations."

Prevent unauthorized access

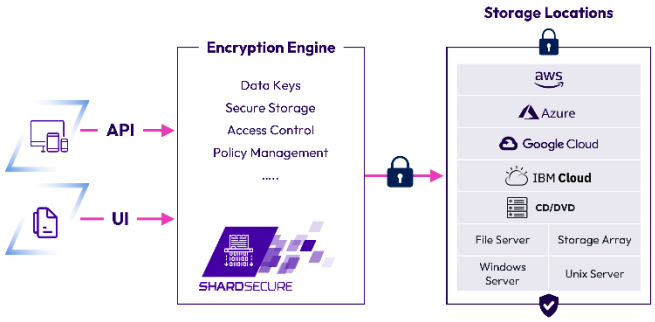
ShardSecure offers advanced data protection — even when storage locations or file systems are misconfigured or are vulnerable to attack. The platform also separates storage admin and cloud provider access from data access to support privacy, confidentiality, and compliance.

In the unlikely scenario that a malicious actor gains access to every storage location for a given data set, that data still cannot be reconstructed, since ShardSecure:

- Strips file content, filenames, file extensions, and all other metadata, meaning there is not enough identifying information for reassembly.
- Allows organizations to add a configurable amount of poison data to their real data.
- Makes the unauthorized reassembly of exfiltrated data impossible.



ShardSecure also requires multiple components to be used in concert for data reassembly, making it impossible for unauthorized users or attackers to reconstruct the data.



Simple integration & access

Despite its powerful data security and privacy features, the ShardSecure platform has minimal impact on existing applications and operations teams and delivers instant data access 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 traditional storage to applications, requiring minimal code changes to get started.

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

High performance

Introducing privacy and security almost always brings a performance cost. ShardSecure is a notable exception. By reading/writing in parallel and compressing pointers, the platform achieves high throughput and low latency.

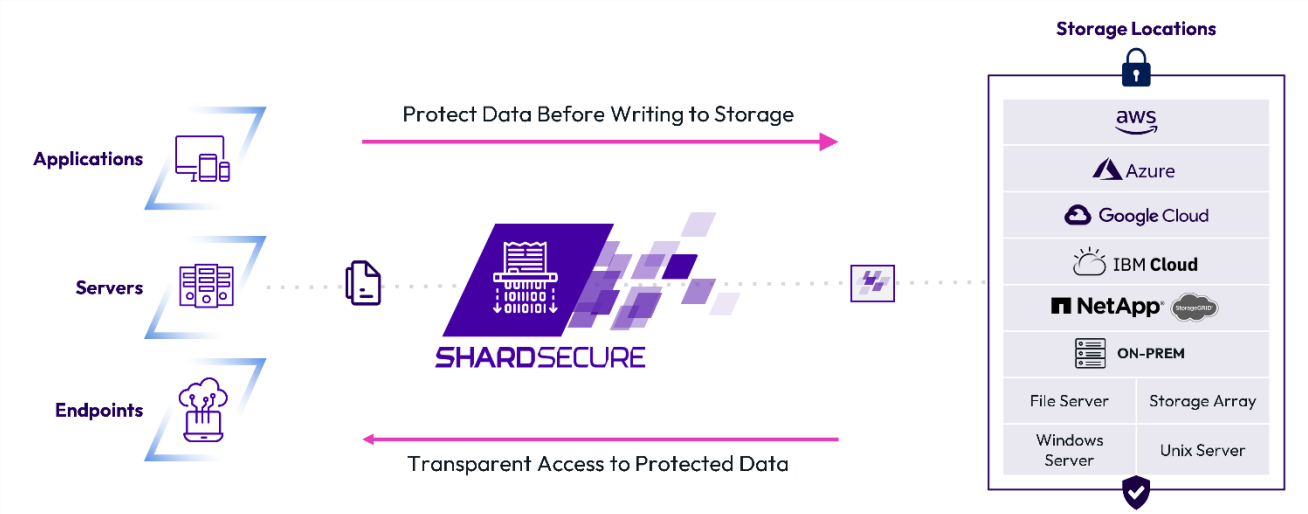
Additional use cases

Beyond the benefits listed above, ShardSecure

- Protects sensitive files so teams can collaborate safely and without losing functionality.
- Integrates with existing cloud backup solutions to further protect backup data.
- Accelerates cloud migration initiatives.
- Supports secure cold storage migration from on-prem to the cloud.

How it works

ShardSecure's abstraction layer sits between applications and storage infrastructure, where it performs advanced file protection. This approach allows for a simple plug-and-play implementation without changes to data flows.



The ShardSecure platform uses agentless end-to-end encryption to maintain the security and privacy of unstructured data on-prem, in the cloud, and in hybrid- and multi-cloud environments. The platform keeps data safe from unauthorized users, separating infrastructure administrator and cloud service provider access from sensitive data.

Technical Specifications

Storage integration

- Local disk
- NFS
- Microsoft SMB shares
- Amazon EFS and S3
- FUSE
- Google Cloud Platform
- Microsoft Azure Object Storage
- Backblaze
- Wasabi
- Alibaba Cloud

Management and monitoring

- Centralized management with Web UI and REST API
- Syslog integration

Supported hypervisors

- VMWare ESXi 7.0 (HW version 17)
- AWS, Azure, and GCP

Deployment media

- ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services Marketplace)

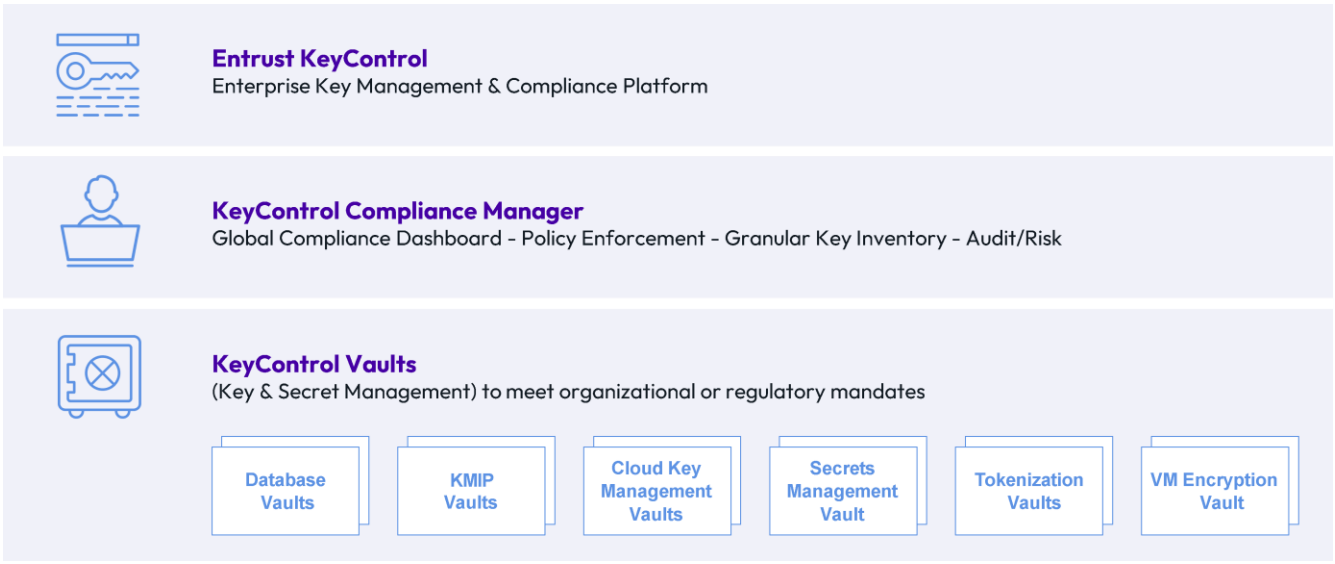
Certifications

- FIPS 140-2 Level 1 Certified
- FIPS 140-2 Level 3 compliance via Entrust nShield HSM on-premises or as a service

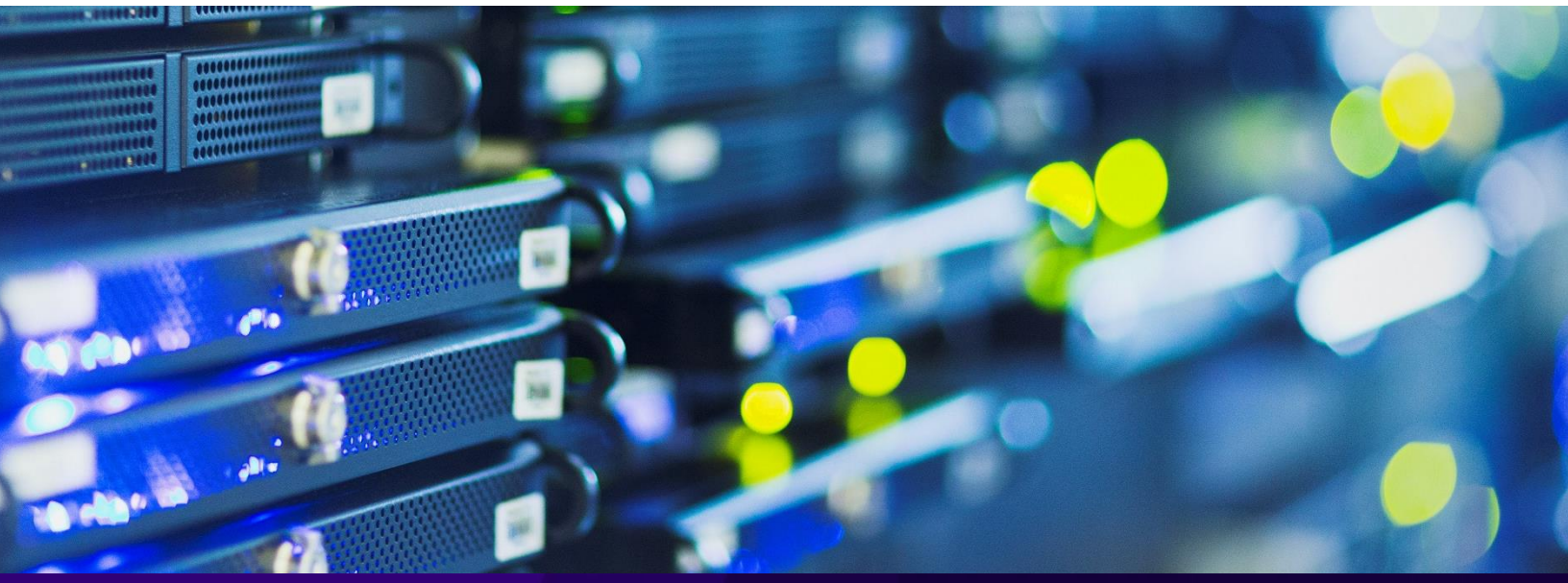
Entrust KeyControl Vault for File Encryption

Entrust KeyControl

Entrust KeyControl Vault's integration with ShardSecure is part of a suite of KeyControl Vaults, each designed to manage key lifecycles at scale on a use-case-by-use-case basis in virtualized environments across on-premises, multi-cloud, and hybrid deployments.



For more details on KeyControl, KeyControl Compliance Manager, and the range of vaults, download the Entrust KeyControl Solution Brochure.



@ShardSecure
@ShardSecure
@ShardSecure

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

info@shardsecure.com

SHARD SECURE