

Securing Databases in the Cloud

A Look at the Security Features of SingleStore Managed Service by
SingleStore

Jake Bernardes
January 2021

Table of Contents

Table of Contents	2
Securing the Database in the Cloud	3
Architecture	4
Connectivity	4
Encryption	5
Authentication	6
Workload Isolation	6
Logging and Monitoring	6
Business Continuity & Disaster Recovery	7
Information Security Certifications	7
Conclusion	7

Securing the Database in the Cloud

The number of SaaS based workloads will grow from 78 million in 2015 to 380 million by 2021. Following this trend, businesses are also moving their databases to hosted solutions. As businesses entrust our data to third party solutions we increase the risk around the storage of Personal Identifiable Information (PII), financial and banking information (PCI), and protected health information (PHI). It becomes increasingly important for SingleStore to demonstrate to our customers, and your customers, that we put security at the heart of our business and are building a solution that offers both performance and protection.

SingleStore Capabilities



FEATURE CATEGORY	
Encryption at rest	●
Encryption in transit	●
Customer Isolation	●
Logging & Monitoring	●
Back Ups	●

Architecture

The following diagram shows the high level architecture of SingleStore Managed Service by SingleStore, highlighting the relevant security features:

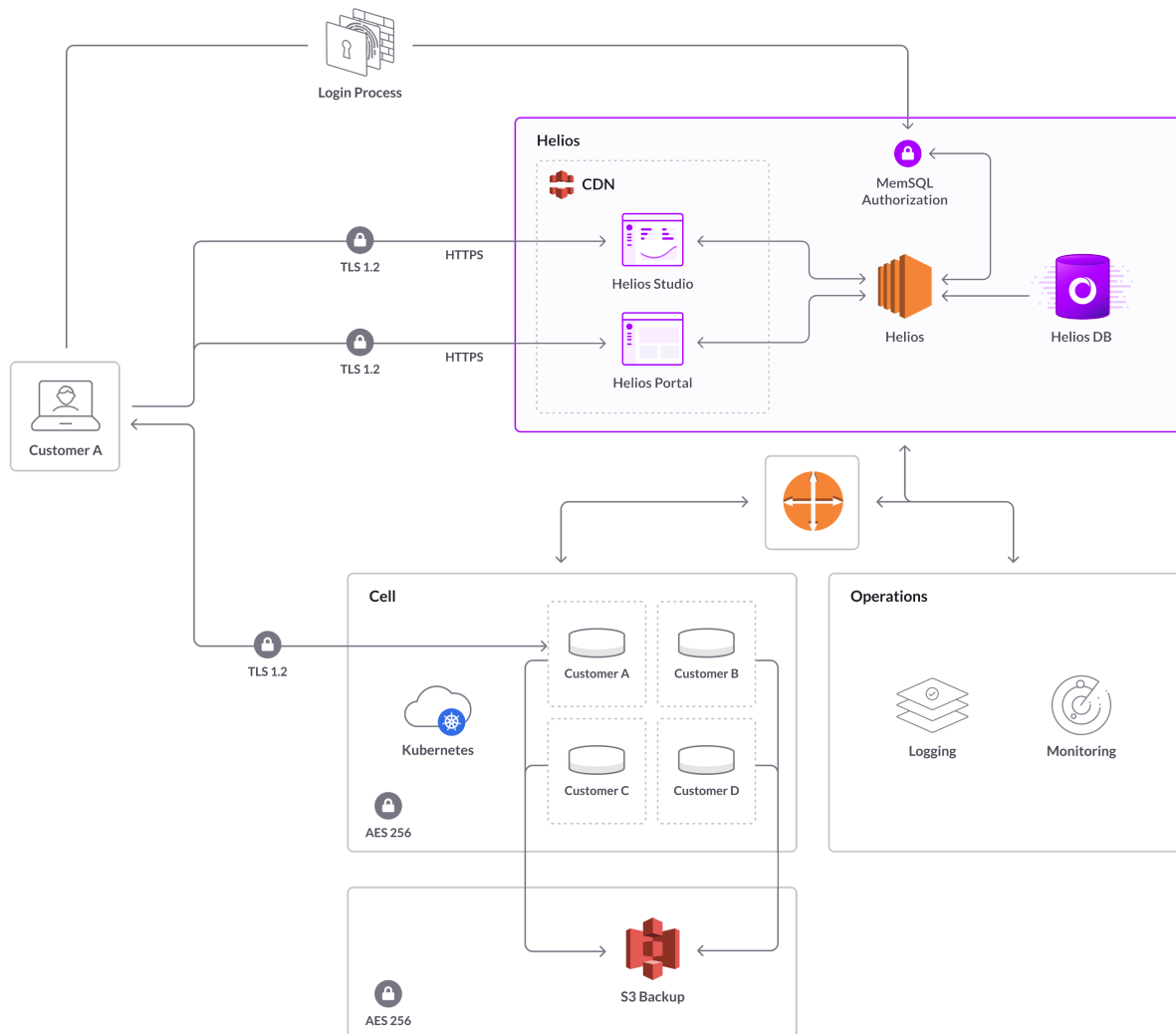


Figure 1. SingleStore Managed Service Security Architecture

Connectivity

The privacy of your data is important to us. We don't want our mail opened or our phone calls listened to. We don't want people we don't trust to know where we are going or how

we are getting there. Similarly we want to ensure our data and the data entrusted to us gets from you to us in a secure and efficient manner.

We empower our customers to secure their data from attackers. We use a layered approach to security, starting with IP whitelisting to ensure only devices you trust, and have given access to, can access your cluster or your data. We then ensure that the data passing between your trusted devices and SingleStore Managed Service is encrypted with TLS 1.2 to protect it from being intercepted during transit. *Unless you explicitly grant access your data then they cannot gain access to it.*

SingleStore Managed Service supports PrivateLink for customers on Amazon Web Services (AWS), which ensures data does not leave a customers AWS environment and is not exposed to the wider internet.

Encryption

Data is personal and invaluable to us as individuals but data has also become the world's most valuable commodity and we give much of it for free through social media and the rise of connected devices. That said, we don't shout our credit card numbers on the street, nor do we put up flyers detailing the personal information we don't want others to know. We expect businesses to value our data the way we do and to protect it from others.

Encryption encapsulates the processes and controls used to ensure our data remains inaccessible to unauthorized users and to protect our data between the end user, client apps, and servers involved. Let's think of it like a bicycle. At SingleStore we like bikes. When we travel with our bikes we put them in special boxes and lock those boxes so no one can steal our valuable property while it's in transit. Then when we get to our destination we lock our bike anytime we aren't using it so no one can steal it while we aren't looking. That's protection in transit and protection at rest. In accordance with best practice SingleStore applies both encryption to *data in transit* and *data at rest*.

Data in transit - For all connections to the database SingleStore supports TLS 1.2. Transport Layer Security (TLS) uses a combination of symmetric and asymmetric encryption focusing on the uses of key pairs, a public key and a private key.

Data at Rest - SingleStore utilises the best practice solution provided by the cloud hosting partner, this is AES-256 for AWS, Google Cloud and Azure. This is an encryption algorithm using a 256 bit key length and is currently the strongest encryption algorithm available.

Authentication

Authentication is the process of verifying an individual or device. It ensures that the data that matters to you and your customers is only accessed and viewed by individuals and devices to which you have granted permission.

SingleStore Managed Service Portal authenticates with your SingleStore account using secure JWT authentication. This is then shared across the SingleStore Managed Service Portal and associated forums. Let's talk about Bob. Bob wants to buy a beer at a concert. Bob first goes to the wristband tent (Identity Provider), where an employee verifies his identity and that he meets the requirements to buy a beer. If he does he will get a wristband. Bob then walks over to the beer tent (Service Provider) who has the beer Bob actually wants. The beer vendor sees Bob's wristband and hands him a beer.

SingleStore provides a customer admin with the power to provision and control access within their organization and to take responsibility for who can see what and when.

SingleStore supports integration with third party identity providers to further secure and automate the authentication process.

Workload Isolation

No one wants to share a private dinner conversation with the table next to them, and we know our customers don't want to share their data and workloads with other businesses. SingleStore Managed Service is powered by Kubernetes, ensuring clusters are isolated from each other and guaranteeing both confidentiality and integrity of your data.

Some customers host data or adhere to specific regulations that require additional isolation controls. Customers requiring full isolation can obtain a dedicated environment for additional cost.

Logging and Monitoring

With data being today's currency it's important to know who can access it, who has viewed it, and why. SingleStore currently has access to all internal logs ensuring there is a full audit trail.

SingleStore exposes cluster logging and monitoring to customers to enable you to proactively understand the activity within your cluster and react to suspicious or abnormal user behaviours.

Business Continuity & Disaster Recovery

Disasters happen in our daily lives. We have all lost something at some point and wished we had made a copy of it. To protect against data loss all data stored within SingleStore Managed Service is backed up daily and retained for seven days. The data is stored in S3 to provide assurances in case the need arises.

Information Security Certifications

SingleStore has undergone an 18 month project to transform the way the business approaches information security and data privacy. We have now secured industry-leading security certifications including ISO 27001 and SOC 2 Type 2. SingleStore is also fully compliant to the requirements of HIPAA, CCPA and GDPR.



As we grow, SingleStore continues to mature its information security posture and is passionate about meeting the security and compliance requirements of our customers.

Conclusion

Data security is a core fundamental at SingleStore, and we leverage best-in-class methods for ensuring data is protected throughout its lifecycle. In addition to the systems and practices we have already implemented for data security, we have continued investment in measures and certifications to ensure SingleStore stays on the cutting edge of security.

If you have further questions regarding security on SingleStore Managed Service then please reach out to us at security@SingleStore.com.