SingleStore™

SingleStore Products

Shared Security Responsibility Model

SingleStore provides three different product offerings of its product: self-managed, cloud DBaaS and a hybrid cloud DBaaS model; these are accordingly named SingleStore Self-managed, SingleStore Helios and SingleStore Helios BYOC. All three differ in terms of responsibilities between the customer and SingleStore on a variety of subject matter areas which is described hereafter in this document.

- ❖ SingleStore Self-managed is aimed at customers who wish to run SingleStore Self-managed software in their own infrastructure;
- ❖ SingleStore Helios offers inherent security measures, establishing a safeguarded environment for running customer workloads;
- ❖ SingleStore Helios BYOC provides a similar managed experience to SingleStore Helios, but data sovereignty sits with the customer.

Regardless of the product offering by SingleStore, the responsibility for maintaining security is jointly borne by both customers and SingleStore. Our products have been meticulously designed to provide robust default security settings. Nevertheless, customers must assume responsibility for configuring additional security controls, commensurate with their organization's specific security requirements and posture.

	SingleStore Self-managed		SingleStore Helios		SingleStore Helios BYOC	
	Customer	**SingleStore**	**Customer**	**SingleStore**	**Customer**	**SingleStore**
Cloud Infrastructure	Customer handles all aspects related to the hosting infrastructure where SingleStore is to be deployed and managed.	N/A	Select the cloud provider and the region of choice and cluster size.	Provision the requested clusters in a private network Additional configurations described by users as available on the platform.	Providing the cloud account, assuming it's supported by SingleStore, configuring security settings, following industry best practices, and using Identity and Access Management (IAM) tools to control access to their resources.	Provisioning and managing the lifecycle of the resources required to bootstrap and manage a BYOC SingleStore Self-managed instance; Excluding the VPC and IAM Role assumed to perform the bootstrap and further updates on the instance, which the customer manages.

Customer Data	Create and manage customer data. Enforce secure access and storage according to own requirements, policies and capabilities.	N/A	Create and manage customer data.	Provide secure access and storage to customer data on the platform. Provide access and communication channels to the platform that ensure confidentiality, integrity, and authentication for customer data in motion.	Besides creating and managing their data, the customer is responsible for guaranteeing that the SingleStore's managed buckets are secure and unreachable from unwanted sources (in the sense that buckets are in the customer's cloud account)	Provide secure access and communication channels to the platform that ensure confidentiality, integrity, and authentication for customer data in transit. Manage the cloud-hosted buckets pre-provisioned by SingleStore storing customer's data.
Identity Management and Authentication	Configure and leverage chosen identity and authentication capabilities made available for SingleStore accordingly with its own requirements, policies and tech stack.	Ensure correct implementation and support of secure standard identity and authentication capabilities (e.g. local auth, JWT auth, SAML, Kerberos) on SingleStore (as is) and make them available for customers. Provide guidance and documentation through support cases/at onboarding/public documentation as applicable.	Access and manage the lifecycle of customer's user accounts Configure platform authentication method Establish password policies and security measures to protect user identities and credentials	Provide integration with customer's identity management platforms (SSO) Provide secure local identity management capabilities Provide secure access to user accounts on the platform Enable customer user account lifecycle management on the platform	Access and manage the lifecycle of customer's user accounts. Configure platform authentication method. Establish password policies and security measures to protect user identities and credentials.	Provide secure access to user accounts and account lifecycle management on the platform. Provide secure access to user accounts on the platform.

Network Isolation & Connectivity	Customer handles all aspects related to the network infrastructure where SingleStore is to be deployed and managed.	N/A	Set up network connectivity, encompassing firewall configuration, DNS configurations, Privatelink, VPC, and IP allowlisting, between the customer and the platform.	Enforce network security restrictions as per configurations made by the customer Resource allocation for establishing a Private Link connection.	Set up the VPC, following SingleStore's requirements and guidelines, where the BYOC Data Plane will be deployed. Managed the VPC, keeping it aligned with initial guidelines and requirements.	**Provide guidelines and hardened network and resource configurations.**
Access Control	Configure and leverage chosen access control capabilities made available for SingleStore accordingly with its own requirements, policies and tech stack.	Ensure correct implementation and support of access control capabilities (e.g. RBAC, RLS) on SingleStore (as is) and make them available for customers. Provide guidance and documentation through support cases/at onboarding/public documentation as applicable.	Define and configure an access control scheme on the platform, and assign roles and privileges. Manage SSL/TLS certificates and JWKS setups for clusters	Provide Role-Based Access Control (RBAC) as part of the platform Support secure token-based authentication/authorization on the clusters	Define and configure an access control scheme on the platform, and assign roles and privileges.	Provide Role-Based Access Control (RBAC) as part of the platform
(Management) API Controls / Access	N/A	N/A	Request API keys and securely manage their lifecycle as per customer's requirements	Generation of secure API keys and use of cryptographically strong algorithms Securely implementing API access	N/A (Currently not supported)	N/A (Currently not supported)

Security for data in transit	Configure and harden SingleStore secure communication settings. Manage the lifecycle all secret material related to encryption or authentication of data in motion (keys, certificates, etc.)	Implement industry-standard secure communication capabilities in SingleStore. Provide guidance and documentation through support cases/at onboarding/public documentation as applicable.	Require SSL/TLS connections to the cluster Ensure secure client configuration for connections to the platform and clusters	Establish industry-standard secure communication protocols and algorithms for data in transit to the platform Establish industry-standard secure communication protocols and algorithms for data in transit to the clusters Ensure secure certificate and key management for the platform	Responsible for all aspects of accessing data in motion, such as establishing secure connections to the cluster and ensuring secure client configurations;	Usage of self-signed SSL/TLS certificates
Encryption for data at rest	Configure and harden SingleStore settings as needed by own requirements, policies and tech stack. Manage the lifecycle of all secret material related to encryption at rest.	Allow for industry-standard encryption at rest capabilities in SingleStore. Provide guidance and documentation through support cases/at onboarding/public documentation as applicable.	For CMEK: Configure cloud provider KMS and key policy according to the customer's own requirements, and then configure CMEK on SingleStore Helios	Enable default encryption of data at rest with cloud provider-managed keys For CMEK: Connect to the customer-specified KMS and use keys for encryption at rest	N/A, enabled by default.	Enable default encryption of data at rest with cloud provider-managed keys.

Audit logging and monitoring	Configure and harden SingleStore settings as needed by own requirements, policies and tech stack. Monitor audit logging for SingleStore deployments.	Allow for industry-standard logging and auditing capabilities in SingleStore. Provide guidance and documentation through support cases/at onboarding/public documentation as applicable.	Configure audit levels and audit log destinations Monitor audit logs for customers' cluster(s)	Stream audit logs to external resources based on configuration from customers Enable audit logging for the database automatically Monitor the platform's audit logs	N/A	N/A
Performance monitoring and alerting	Customer handles all aspects related to the performance monitoring of SingleStore and the infrastructure where SingleStore is to be deployed and managed.	Implement performance monitoring and management capabilities in SingleStore. Provide guidance on performance improvements and optimizations through support cases and product onboarding.	Configure real-time alerts and performance thresholds. Configure external tools for monitoring and alerting. Access to customer metrics and logs via Grafana dashboards.	Configure performance captures and monitoring capabilities. Monitor the platform's performance logs and alerts.	Configure real-time alerts via setting up their own SMTP mailgun service registering to it the monitoring infrastructure of the BYOC cell. Access to customer metrics and logs via Grafana dashboards.	Configure performance captures and monitoring capabilities. Monitor the platform's performance logs and alerts.
Patching and maintenance	Subscribe to SingleStore's patches and updates and apply them as soon as they become available.	Provide security patches and updates. Run internal vulnerability and patch management processes.	Ensuring client software used to interact with the platform and clusters is up-to-date and patched.	Automatically apply security patches and updates. Run internal vulnerability and patch	Ensuring client software used to interact with the platform and clusters is up-to-date and patched. Ensure BYOC's host cloud account is updated with	Applying security patches and updates on infrastructure and resources managed by SingleStore.

				management processes.	the latest security and configuration best practices.	Run internal vulnerability and patch management processes on infrastructure and resources managed by SingleStore.
High Availability and Disaster Recovery	Customer handles all aspects related to the SingleStore deployment and controls necessary to achieve a highly-available deployment.	Provide guidance on how to achieve a more resilient /highly-available deployment of SingleStore, along with disaster recovery capabilities.	Can create and manage own custom backups following customer's backup, business continuity and/or disaster recovery policies and plans Configure backup and recovery capabilities and provisions as per what's offered by the platform	Perform automated backups which are stored in case of unexpected disaster (these backups can be restored by filing a request with Support) Implement automated failover and replication mechanisms (if configured by the customer)	Can create and manage own custom backups following customer's backup, business continuity and/or disaster recovery policies and plans. Configure backup and recovery capabilities and provisions as per what's offered by the platform.	Perform automated backups which are stored in case of unexpected disaster (Enterprise/Premium plan only, these backups can be restored by filing a request with Support)
Application Security and Compute Platform	Ensure a secure operating and computing environment where SingleStore is to be hosted. Code written to interface with external functions and/or to create user-defined functions (UDF) must be validated and	Ensure the software follows security engineering principles and is tested for security weaknesses regularly. Run incident detection and response mechanisms internally.	Code written to interface with external functions and/or to create user-defined functions (UDF) must be validated and checked for security issues. Validate the trustworthiness/security of any third-party services intended to	Provide a secure operating and computing environment. Run incident detection and response mechanisms internally. Manage network egress and ingress at the network layer and access control to data.	Code written to interface with external functions and/or to create user-defined functions (UDF) must be validated and checked for security issues. Validate the trustworthiness/security of any third-party services intended to be leveraged on Helios computing	Assumes and operates with the mindset that everything is Private. No public IPs or ports are exposed at any point Incident detection happens by internal alerts or via customer support tickets with resolution being performed directly by SingleStore in the case of simple infrastructure troubleshooting/updates or jointly with the Customer for scenarios

	checked for security issues. Validate the trustworthiness/security of any third-party services intended to be leveraged by SingleStore through integrations.	Validate the security of the software supply chain used by CI/CD procedures and tooling.	be leveraged on Helios computing capabilities or through integrations. Secure system access for users inside and outside the customer's environment.	Ensure the platform’s software and infrastructure follows security engineering principles and is tested for security weaknesses regularly. Validate the security of the software supply chain used by CI/CD procedures and tooling.	capabilities or through integrations. Secure system access for users inside and outside the customer's environment.	requiring elevated permissions to the cloud environment (with SingleStore assuming a supportive role). No network management; operating on the level that only private load-balancers can be created. Validate the security of the software supply chain used by CI/CD procedures and tooling.
Secrets Management	Customer handles all aspects related to secret management of SingleStore.	N/A	Ensure proper access control to secrets configured within the platform Employ secrets lifecycle management as per customer’s policies	Securely store and encrypt customer secrets	Ensure proper access control to secrets configured within the platform Manages the lifecycle of secrets as well as their distribution end-to-end	No access to any customer BYOC secrets
Compliance	Customer handles all aspects related to their own compliance against applicable standards, frameworks and regulations.	N/A	Configure the environment(s) to meet the requirements applicable to the customer’s own compliance and regulatory needs. Should the customer intend to store and	Maintain compliance and uphold Information Security and Data Protection standards and requirements that apply to our product and business (namely ISO27001 and SOC 2 Type II).	Same as for SingleStore Helios. Note however that the data sovereignty in Helios BYOC is on the customer side and while SingleStore does provide the guidelines and requirements to secure data on the customer’s environment, the ultimate responsibility of securing	Same as for SingleStore Helios.

			manage PHI data on Helios, a BAA should be set up with SingleStore.	Support compliance inheritance of HIPAA.	the cloud environment where customer data resides relies on the customer itself.	
Usage of Generative AI (Artificial Intelligence)	N/A	N/A	Ultimately responsible for safe generative AI adoption within their tenant and for the data leveraged in AI features made available by SingleStore. Maintain human-in-the-loop for business use-cases relying on AI (trust but verify). Where a choice is required to select the underlying AI models to be used, customer is accountable for that choice.	Provide a secure platform for enabling generative AI use-cases that synergize with SingleStore's database capabilities that customers can benefit from Make sure SingleStore's AI platform stays compliant with data protection and regulatory standards, and keep track of changes as AI-related regulations continue to develop. Scrutinize generative AI technology, implement vetting processes for bias, safety, accuracy and security	N/A	N/A