TeamSQL

TeamSQL’s Approach to Security

Introduction

TeamSQL's mission is to make the developer's, data analyst's and marketing expert's database management simpler, more efficient, and more productive in a collaborative way. To achieve that, we need to make sure your data is secure and protected. We’re committed to being transparent about our security methods.

Organizational security

TeamSQL has set up a security program, dedicated to assuring users have the highest confidence in the protection of their data.

Personnel security

TeamSQL’s personnel practices apply to all members of the TeamSQL "workers" (regular employees and independent contractors) who have direct access to TeamSQL’s internal information systems (“systems”) and/or unescorted access to TeamSQL’s office space. All workers are required to understand and follow internal policies and standards.

All workers must accept the confidentiality terms, pass a background check, and attend security preparation before getting initial access to systems. This preparation includes privacy and security topics, including device security, acceptable use, preventing malware, physical security, data privacy, account management, and incident reporting.

In termination of employment at TeamSQL, Security Team removes all access to TeamSQL systems immediately.

Security and privacy training

Through the occupation, all workers are required to perform a refresh of privacy and security practice at least annually. They are also required to accept that they’ve read and followed TeamSQL’s information security policies at least annually. Some workers, such as engineers, operators and support personnel who may have elevated access to systems or data, receive additional job-specific exercise on privacy and security. Workers are required to report security and privacy issues to appropriate internal teams. TeamSQL informs workers that failure to comply with acknowledged policies may result in results, up to and including termination.

TeamSQL

Protecting customer data

TeamSQL's security program's focus is to restrict unauthorized access to user data. Our team of dedicated security practitioners, working in partnership with peers across all our teams, take exhaustive steps to identify and mitigate risks, implement best practices, and continuously evaluate ways to improve.

Data encryption in transit and at rest

TeamSQL transmits data over public networks using strong encryption methods including data transmitted between TeamSQL clients and the TeamSQL service. TeamSQL supports the latest secure cipher suites to encrypt all traffic in transit, including TLS 1.2 protocols, AES256 encryption, and SHA2 signatures. TeamSQL monitors and upgrades the cipher suite options as the landscape evolves.

TeamSQL stores encryption keys in a secure server on a separated network with highly restricted access. Keys are never saved on the local filesystem, but are delivered at process start time and retained only in memory while in use.

Each TeamSQL customer’s data is hosted in TeamSQL’s shared infrastructure and segregated logically by the TeamSQL application. TeamSQL uses various storage technologies to guarantee customer data is protected from hardware malfunctions and recovers quickly when asked.

Server-Side Data Encryption

TeamSQL encrypts each entity using the **aes-256-ctr** algorithm after initializing the cipher with an Initialization Vector (IV). TeamSQL generates an IV for each entity. For each data row (representing one entity), TeamSQL generates one secret key using AES-256.

TeamSQL stores all of its generated encryption keys in an Amazon Web Services (AWS) S3 bucket. This bucket itself is encrypted with a key generated and maintained by AWS’ Key Management Service (KMS).

Network security

TeamSQL hosts the systems supporting testing and development activities in a separate network from systems supporting production for a more protected sensitive data. User data

submitted into the TeamSQL services are only permitted to exist in TeamSQL's production network. TeamSQL limits the administrative access of workers to the production network.

TeamSQL highly restricts network access to TeamSQL's production environment from public networks. TeamSQL deploys moderations against the distributed rejection of service (DDoS) attacks at its network boundary. TeamSQL restricts the settings to the production network configuration to only authorized employees.

The hosting provider retains administration of the network devices in TeamSQL's hosted production environment. Intrusion Detection / Intrusion Prevention (IDS/IPS) are performed using host-based controls.

Classifying and inventorying data

TeamSQL organizes data into levels and species the labeling and handling requirements for each level to protect the data better. User data is organized at the highest level.

Authorizing access

To minimize the risk of data exposure, TeamSQL adheres to the principle of least privilege—workers are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. To ensure that users are so restricted, TeamSQL employs the following measures:

- User authentication is needed to all systems and unique identification is performed.
- TeamSQL administration reviews each user's access and its level at least quarterly and ensure that its appropriate for the user's responsibilities.

Workers may be granted access to a small number of internal systems, such as the corporate TeamSQL instance, by default upon hire. Requests for additional access follow a documented process and are approved by the responsible owner or manager.

Authentication

TeamSQL applies multi-factor authentication for administrative access to systems to reduce the risk of unauthorized access. The passwords are auto-generated to assure uniqueness, longer than 12 characters.

All TeamSQL workers use an approved password manager that generates, stores and enters complex and unique passwords.

TeamSQL

System monitoring, logging, and alerting

TeamSQL monitors servers, workstations and mobile devices to retain and analyze a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on all servers in TeamSQL's production network are logged.

TeamSQL collects and stores production logs for analysis reports, and logs are stored in a separate network. TeamSQL restricts access to this network to members of the security team.

Endpoint monitoring
TeamSQL workstations run monitoring tools to detect suspicious code or insecure configurations. TeamSQL monitors workstation alerts and ensures significant issues are resolved in a timely manner.

Data and media disposal

TeamSQL removes customer data instantly after deletion, and hard deletes all information from currently running production systems, destroys backups within 14 days. TeamSQL follows industry standards and advanced methods for data destruction.

Controlling system operations and continuous deployment

TeamSQL takes actions to fight against the introduction of malicious code to the operating environment and guard against unauthorized access.

Controlling change

TeamSQL controls changes, especially changes to production systems to minimize the risk of data exposure, and practices change control requirements to systems that store data at higher levels of sensitivity. TeamSQL designs the requirements to ensure that changes potentially impacting user data are documented, tested, and approved before deployment.

Server hardening

TeamSQL disables unneeded and potentially insecure services, removes default passwords and applies TeamSQL's custom configuration settings to each new server before deployment to production.

TeamSQL

3rd party suppliers

TeamSQL relies on sub-service organizations to run its business efficiently.
TeamSQL takes appropriate steps to ensure its security posture is maintained where those sub-service organizations may impact the security of TeamSQL's production environment.
TeamSQL practices agreements that require service organizations adhere to confidentiality committals TeamSQL has made to its users. TeamSQL monitors the practical operation of the organization's safeguards by conducting reviews of its service organization controls before use.