# Data Security

Last Modified on 06/10/2026 11:06 pm EDT

Digioh takes security seriously. Here is what you'll learn in this article:

- Gain insights into Digioh's rigorous security measures to protect your data.
- Understand how technologies like SQL firewalls, auditing, threat detection, and data masking work to enhance security.
- Learn how these security features help maintain compliance and protect against potential threats.
- Feel confident in implementing and benefiting from these security practices in your own systems.

## SQL Database - Firewall and Firewall rules

To help protect your data, firewalls prevent all access to our database server until we specify which computers have permission using firewall rules. The firewall grants access to databases based on the originating IP address of each request.

## Auditing

SQL Database Auditing tracks database activities and helps you maintain regulatory compliance by recording database events to an audit log in our Storage account. Auditing enables us to understand ongoing database activities, as well as analyze and investigate historical activity to identify potential threats, suspected abuse, and security violations.

## Threat detection

Threat Detection complements auditing by providing an additional layer of security intelligence built in our SQL Database. It works around the clock to learn, profile, and detect anomalous database activities. We are alerted about suspicious activities, potential vulnerabilities, SQL injection attacks, and anomalous database access patterns. We can easily respond to alerts by following a protocol that we have in place.

## Data Masking

SQL Database Dynamic Data Masking limits sensitive data exposure by masking it to non-privileged users. Dynamic Data Masking automatically discovers potentially sensitive data in our SQL Database and provides actionable recommendations to mask these fields, with minimal impact on the application layer. It works by obfuscating the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.

## Compliance

In addition to the above features and functionality that help our application meet various security

compliance requirements, our SQL Database also participates in regular audits and has been certified against a number of compliance standards.