✓ 100 XP ▶

Introduction

2 minutes

Data security is critical when protecting your customer's privacy and your organization’s reputation. Businesses have closed due to financial damage or ruined reputations. Customers have had their data accessed unlawfully because of security breaches exposing their personal details, and again, possibly causing financial harm.

Suppose you work at an online retailer. To support the online marketplace your company provides, you store an assortment of data from your customers, such as phone numbers, addresses, and credit cards. You also store data that is critical to the health of your business, such as financial account balances and intellectual property. If exposed or maliciously accessed it could jeopardize the health of your business and the trust your customers place in you. It's your responsibility to make sure this data stored in your databases is as secure as possible, to protect both your customer data and your business data.

Put yourself in the shoes of an attacker. If you were trying to maliciously attack a system, would a single layer of protection or multiple layers of protection make it more difficult to gain access to the data? Defense in depth is a strategy that employs a layered approach to slow the advance of an attack aimed at acquiring unauthorized access to information. Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure.

Azure SQL Database is a great service for the storage of relational data, and there are a number of built-in capabilities you can use to ensure your data is secure and practice defense in depth. We'll look at ways to secure your SQL database by configuring the database firewall, securing access, encrypting communication, and other techniques for database security. With this layered approach, you can help ensure your data is secure.

Learning objectives

In this module, you will:

- Control network access to your Azure SQL Database using firewall rules
- Control user access to your Azure SQL Database using authentication and authorization
- Protect your data in transit and at rest
- Audit and monitor your Azure SQL Database for access violations

---

Next unit: Exercise - Set up sandbox environment

Continue >

✓ 200 XP

Knowledge check

5 minutes

Here's a few questions to review what we've discussed and check what you've learned.

Check your knowledge

1. Which of the following is the most efficient way to secure a database to allow only access from a VNet while restricting access from the internet?

- ○ An allow access to Azure services rule
- ○ A server-level IP address rule
- ● A server-level virtual network rule ✓

  A server-level virtual network rule will allow you to allow connectivity from specific Azure VNet subnets, and will block access from the internet. This is the most efficient manner to secure this configuration.

- ○ A database-level IP address rule

2. A mask has been applied to a column in the database that holds a user's email address, laura@contoso.com. From the list of options, what would the mask display for a database administrator account?

- ○ lxxx@xxxx.com
- ○ laura@xxxxxxx.com
- ● laura@contoso.com ✓

  When database administrator accounts access data that have a mask applied, the mask is removed, and the original data is visible.

- ○ Data not available

3. Transparent Data Encryption will encrypt which database files?

- ○ Database files only
- ○ Log files and backup files only
- ○ Backup files only
- ● Database files, log files, and backup files ✓

  Transparent Data Encryption encrypts all database, log, and backup files. When new Azure SQL databases are created, Transparent Data Encryption will be enabled by default.

4. Is encrypted communication turned on automatically when connecting to an Azure SQL Server?

- ● Yes ✓

  Azure SQL Database enforces encryption (SSL/TLS) at all times for all connections

- ○ No

Next unit: Summary

Continue ›

✓ 100 XP

Summary

3 minutes

In this module, you've seen how Azure SQL Database provides a wide array of tools and features to secure your data. By using these tools and features, you can put multiple layers of defense in place to thwart attacks and keep your customer and business data secure.

You've learned how to:

- Control network access to your Azure SQL Database using firewall rules
- Control user access to your Azure SQL Database using authentication and authorization
- Protect your data in transit and at rest
- Audit and monitor your Azure SQL Database for access violations

All of the aspects work together to secure your database. Your customers are important, your reputation is important, and that makes your database security important.

Further reading

To learn more about the concepts we've covered in this module, check out these other resources.

- Manage IP firewall rules for Azure SQL Server
- Manage Advanced Data Security settings for a SQL database

Module complete:

Unlock achievement