Introduction

2 minutes

Security is one of the most important aspects of any architecture. Ensuring that your business data and customer data are secure is critical. A public data breach can ruin a company's reputation as well as cause significant personal and financial harm. In this module, we'll discuss key architectural security considerations as you design an environment on the cloud.

As we learn about architecting our cloud solutions with security as a primary consideration, we'll see how one fictional Azure customer puts these principles to work:

Lamna Healthcare is a national healthcare provider. Their IT organization has recently started to move the majority of their IT systems to Azure. They have a mixture of custom apps, open-source apps, and off-the-shelf applications, with varying architectures and technology platforms. We'll learn what they need to do to migrate to the cloud while keeping their systems and data secure.

> **Note**
>
> The concepts discussed in this module are not all-inclusive, but represent some of the important considerations when building a solution on the cloud. Microsoft publishes a broad set of patterns, guidelines, and examples on designing applications on Azure. It is highly recommended that you look through the content in the Azure Architecture Center as you start planning and designing your architecture.

Learning objectives

In this module, you will:

- Learn how to take a defense in depth approach to securing your architecture.
- Learn how to protect your identities.
- Learn what technologies are available to protect your Azure infrastructure.
- Learn how and where to use encryption to secure your data.
- Learn how to protect your architecture at the network level.
- Learn how to leverage application security best practices to integrate security into your application.

Next: Defense in depth

Continue >