




Summary

 2 minutes

We've covered a lot of topics in this module, but rightfully so, as security is such an important part of any architecture. Let's review what we've covered.

Defense in depth

We've talked through how to approach security in your architecture through defense in depth. Looking only at firewalls or antimalware alone isn't enough to slow down attackers. Use a layered approach and address security at each layer.

Identity management

We've talked through identity management, and how identity becomes an integral piece of the architectural puzzle. Azure AD has a number of features and capabilities to improve the identity security story for your environment.

Infrastructure protection

Protecting the access to your infrastructure ensures that the resources you create are administered by only those who should be administering them.

Encryption

Encryption is often the last layer of defense against access to your data. By using encryption, you make your data unreadable to anyone without the decryption keys. You should identify and classify your data, then align with encryption requirements from your business and any regulations your organization must adhere to.

Network security

Finally, we talked through securing your network. We looked at ways to secure traffic flow between applications and the internet. We described some ways to secure traffic flow amongst applications. And we wrapped up by looking at how to secure traffic flow between users and an application.

Module incomplete:

[Go back to finish >](#)
