

# Securing Microsoft Azure Data Access Endpoints

---

EXPLORING DATA AND ENDPOINT CONSIDERATIONS



**John Savill**

TECHNICAL ARCHITECT

@ntfaqguy <https://savilltech.com>

# Course Overview



**Explore the Key Considerations Related to Data Endpoint Security**

**How Data Services Integrate with Virtual Networks**

**Securing Resource Endpoints**

# Module Overview



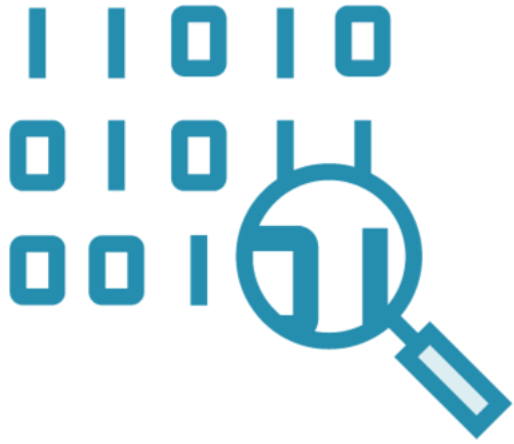
**Types of Data Service in Azure**

**Azure Networking Fundamentals**

**How Data Services Are Exposed**

**Defense in Depth with Identity  
and Network**

# Why This Is Important



Data is the most important asset to organizations

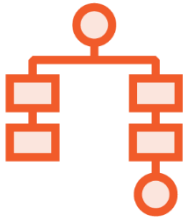


When storing data in the cloud it is critical to understand and secure the access to the data endpoints

# What Is Data?



Data in computer terms is a collection of bits



These bits may be expressing numbers, characters, images, videos, CAD drawings and much more



How data is stored varies depending it's type and use

# Data Storage Types

Different types of data require different types of storage structure and format. Some common ones used in Azure for application services are:

## BLOB

Unstructured data. Variations available purposed for random access or append only operations. Massive scale commonly accessed via APIs

## FILES

Unstructured data accessed via a file system API

## RELATIONAL DATABASE

Data stored against a defined schema utilizing rows and columns with unique keys stored in tables, e.g. SQL Server

## NON-RELATIONAL DATABASE

No fixed schema or table structure. Data commonly represented as collections of documents which may utilize a format such as JSON or XML



**Azure is a multi-tenant service**

**Most services in Azure are shared by multiple customers**

- Don't worry, isolation is assured for customer instances!

**Some services are also available as dedicated deployments**

- These typically have different network capabilities

# Virtual Network Basics



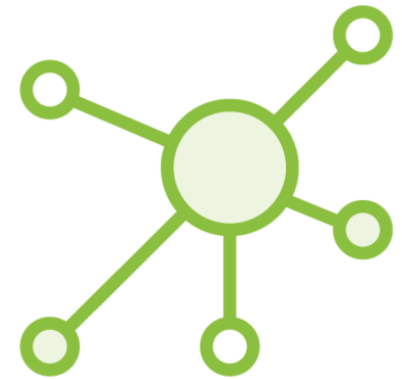
A virtual network is a construct created in Azure



Live within a subscription within a region



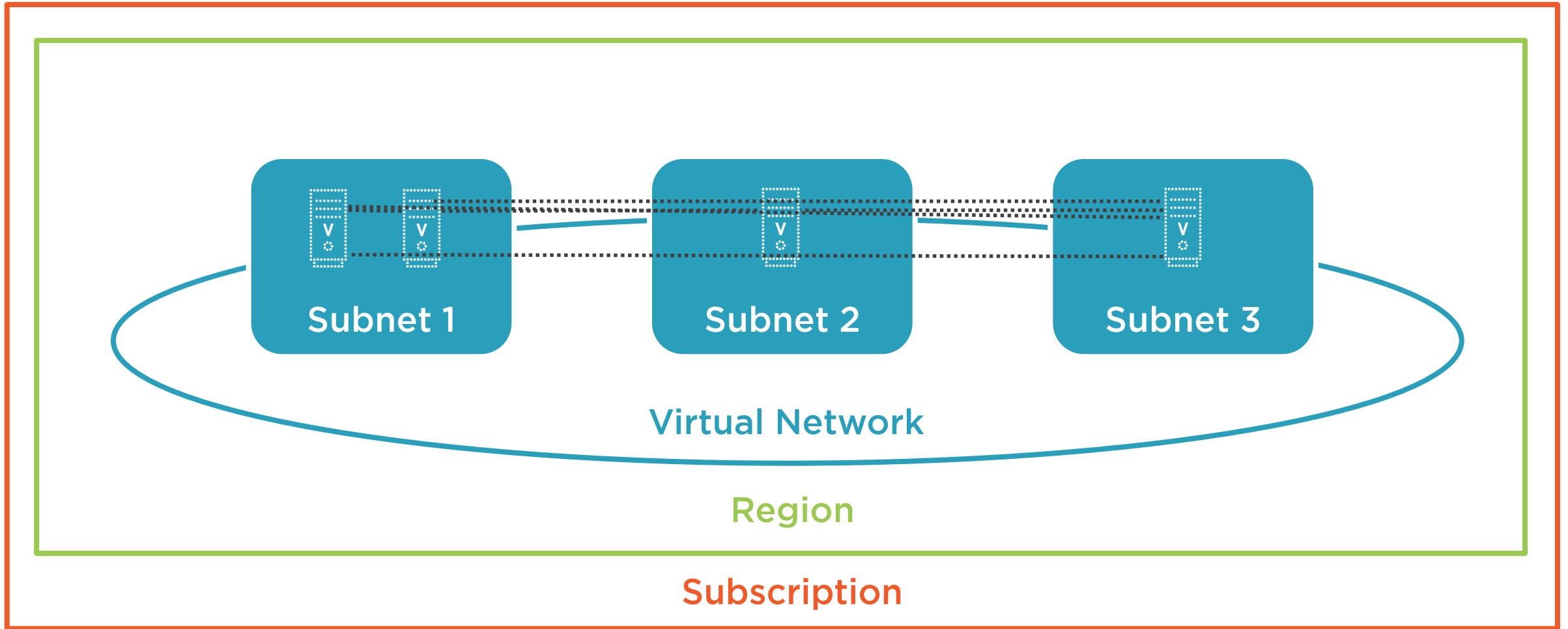
Has one or more IP ranges assigned to it



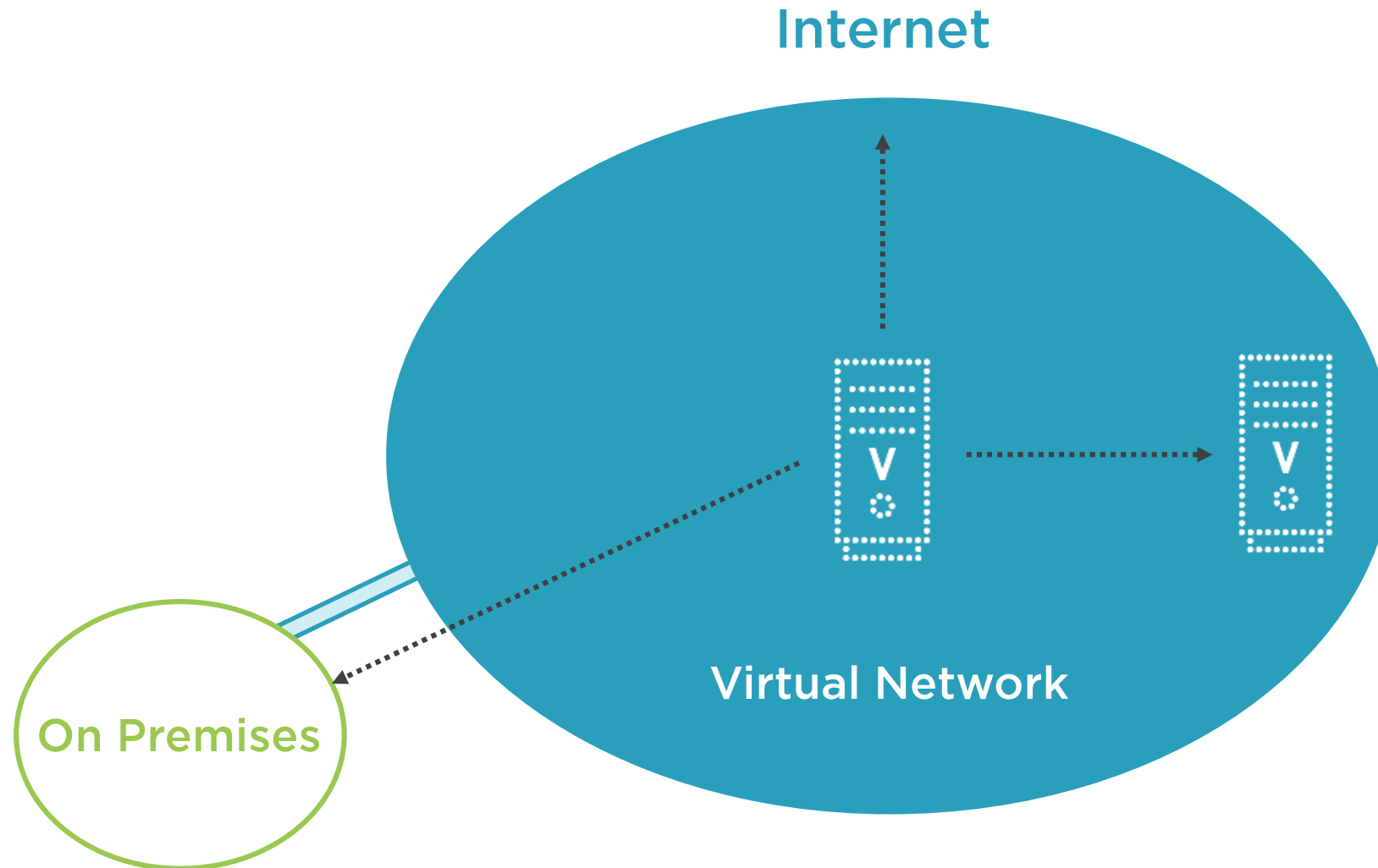
Virtual subnets are created in the virtual network to break up the network range



# Virtual Networks



# Communication in Azure



# Communication in Azure

Internet



Azure



Virtual Network



# Default Service Endpoints

- Services must be available to be utilized
- The default endpoint, i.e. the point of contact is typically Internet facing
- Multiple instances may use the same set of infrastructure
- The customers resource endpoint by default may be open to any connection
- This may need to be changed!

# Defense in Depth

Where possible layers of protection should be utilized

At minimum when considering data service endpoints we think of:



Network



Authentication

# Summary



Types of Data Service in Azure

Azure Networking Fundamentals

How Data Services Are Exposed

Defense in Depth with Identity  
and Network

Next Up:  
Integrating Data Services  
with Virtual Networks