# Syskit Point

## Azure Networking

By default, the Front-end and Back-end app services are accessible from the Public Internet. The rest of the utilized Azure resources – Key Vault, Azure SQL Server, Azure Cosmos DB, and Storage Account – are secured behind firewalls and private connections.

When deploying Syskit Point, there are two options available when considering Azure network resources:

### 1. Deploy Syskit Point from Azure Marketplace

- Consider this to be your 'plug-and-play' option
- New Azure network resources are automatically created, and configured when you deploy Syskit Point without the need to perform additional configuration
- Syskit Point is ready to use and secured after the deployment

### 2. Deploy a custom ARM template

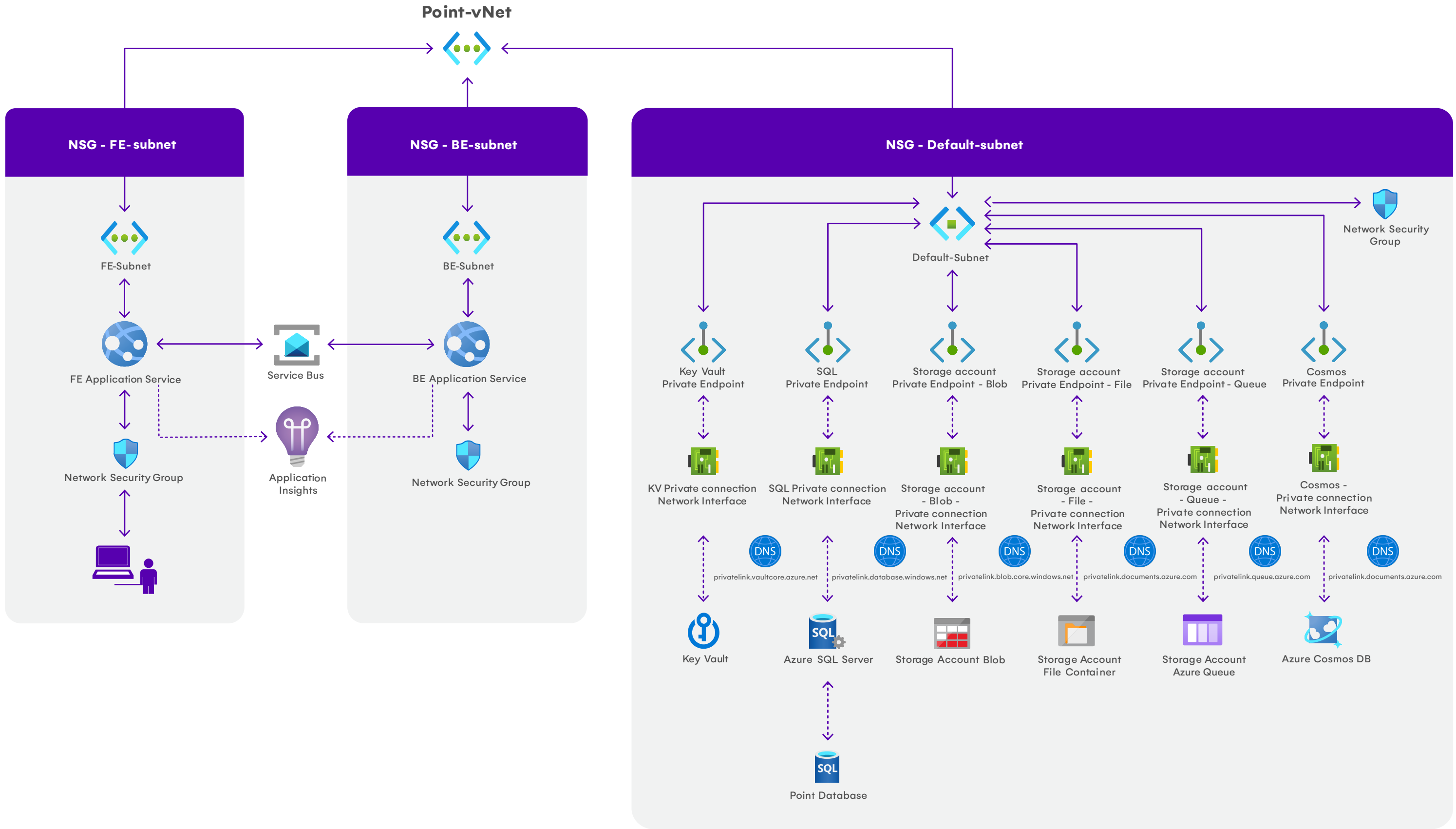
- Use when you want to integrate Syskit Point into already existing Azure network resources
- Custom ARM templates are used when deploying Syskit Point
- No Azure network resources are created when deploying Syskit Point through custom ARM templates
- Syskit Point is ready to use but not secured after the deployment – additional configuration of Azure network resources is required

Please note!
For use cases requiring custom deployment and manual configuration of Azure network resources, don't hesitate to contact us to provide you with custom ARM templates.

### Architecture Diagram

When Syskit Point is deployed from Azure Marketplace, a virtual network is created named point-vnet, with three subnets:

- fe-subnet (1)
- be-subnet (2)
- default-subnet (3)


Point-vNet
NSG - FE-subnet
FE-Subnet
FE Application Service
Network Security Group
Service Bus
Application Insights
NSG - BE-subnet
BE-Subnet
BE Application Service
Network Security Group
NSG - Default-subnet
Default-Subnet
Network Security Group
Key Vault Private Endpoint
SQL Private Endpoint
Storage account Private Endpoint - Blob
Storage account Private Endpoint - File
Storage account Private Endpoint - Queue
Cosmos Private Endpoint
KV Private connection Network Interface
SQL Private connection Network Interface
Storage account - Blob - Private connection Network Interface
Storage account - File - Private connection Network Interface
Storage account - Queue - Private connection Network Interface
Cosmos - Private connection Network Interface
DNS
privatelink.vaultcore.azure.net
privatelink.database.windows.net
privatelink.blob.core.windows.net
privatelink.documents.azure.com
privatelink.queue.azure.com
privatelink.documents.azure.com
Key Vault
Azure SQL Server
Storage Account Blob
Storage Account File Container
Storage Account Azure Queue
Azure Cosmos DB
Point Database

# Azure Networking

The subnets have Network security groups associated with the default rules applied. By default, inbound traffic is denied, and outbound traffic is allowed. If you wish to limit outbound traffic, please contact us .

The following applies to fe-subnet:

- Takes up 3 IP addresses + 5 Azure reserved addresses
- Used by a Front-end app service that provides end-users with a web interface
- Accessible from the Public Internet

The following applies to be-subnet:

- Takes up 3 IP addresses + 5 Azure reserved addresses
- Used by a Back-end app service responsible for retrieving data from a Microsoft 365 tenant by utilizing several Microsoft APIs
- Accessible from the Public Internet

The following applies to default-subnet:

- Takes up 11 IP addresses + 5 Azure reserved addresses
- Used by the following Azure resources:
    - Key Vault
    - Azure SQL Server
    - Azure Cosmos DB
    - Storage Account – Blob
    - Storage Account – File
    - Storage Account – Queue
- Secured with private connections for each resource

**Please note!**
As the Front-end and Back-end app services are accessible from the Public Internet by default, use Azure App Service access restrictions to add another layer of security to Syskit Point app services.