Apply Zero Trust principles to Azure IaaS infrastructure

A clickable deployment plan in the Zero Trust universe

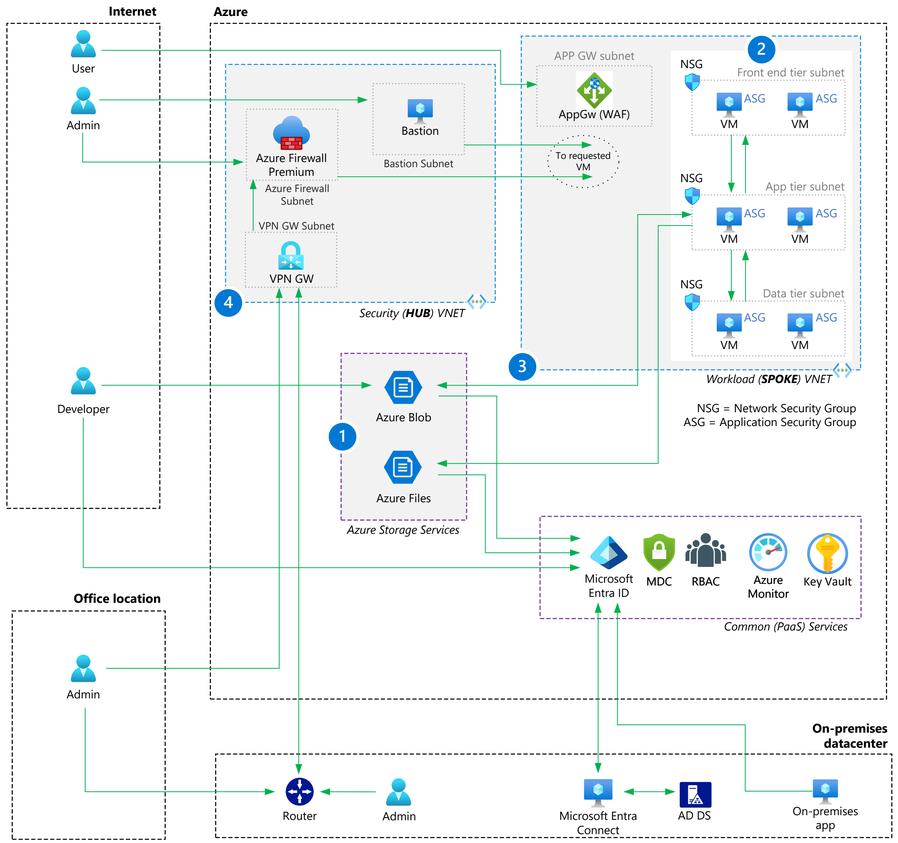
Deploying Zero Trust to Azure IaaS infrastructure

This poster represents the work of deploying Zero Trust to Azure IaaS infrastructure. This work is broken into separate sections and steps corresponding to the key components of infrastructure to deploy common workloads hosted in Azure IaaS. Read more at aka.ms/zero-trust-azure-iaas.

Reference architecture with the four key IaaS components

1. Storage
2. Virtual machines
3. Spoke VNets
4. Hub VNets

NOTE: You do not have to apply Zero Trust principles to these components in this order.



Steps to apply Zero Trust principles to Azure IaaS infrastructure to each component

1 Storage

1. Protect data in all three modes: data at rest, data in transit, data in use
2. Verify users and control access to storage data with least privilege
3. Logically separate or segregate critical data with network controls
4. Use Defender for Storage for automated threat detection and protection

2 Virtual machines

1. Configure logical isolation for virtual machines
2. Leverage Role Based Access Control (RBAC)
3. Secure virtual machine boot components
4. Enable customer-managed keys and double encryption
5. Control the applications installed on virtual machines
6. Configure secure access
7. Set up secure maintenance of virtual machines
8. Enable advanced threat detection and protection

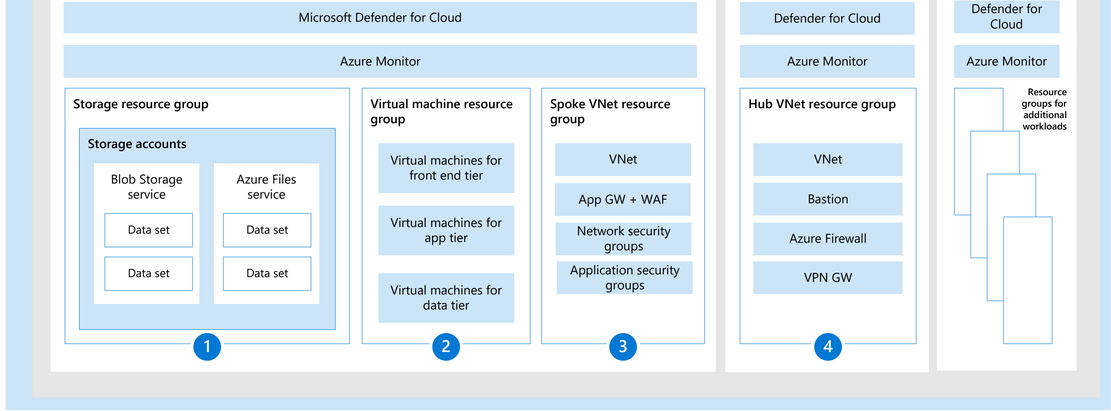
3 Spoke VNets

1. Leverage Microsoft Entra ID RBAC or set up custom roles for networking resources
2. Isolate infrastructure into its own resource group
3. Create a network security group for each subnet
4. Create an application security group for each virtual machine role
5. Secure traffic and resources within the virtual network
6. Secure access to the virtual network and application
7. Enable advanced threat detection and protection

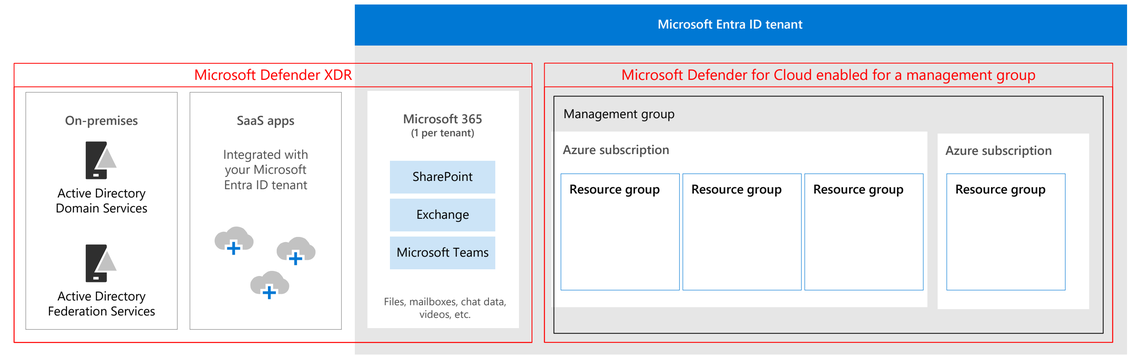
4 Hub VNets

1. Secure Azure Firewall Premium
2. Deploy Azure DDoS Protection Standard
3. Configure network gateway routing to the firewall
4. Threat protection

Logical architecture of tenants, management groups, subscriptions, and resource groups



Threat Protection with Microsoft Defender XDR and Microsoft Defender for Cloud



Additional posters for applying Zero Trust

Zero Trust deployment plan with Microsoft 365
aka.ms/zero-trust-m365-poster

Zero Trust deployment plan with Microsoft Copilot for Microsoft 365
aka.ms/zero-trust-copilot-m365-poster

Microsoft