Microsoft

Overview Of Microsoft Azure

2018 Global Azure BOOTCAMP

Mr. Wisit Thongphoo

FB: ITGeist

Microsoft Azure

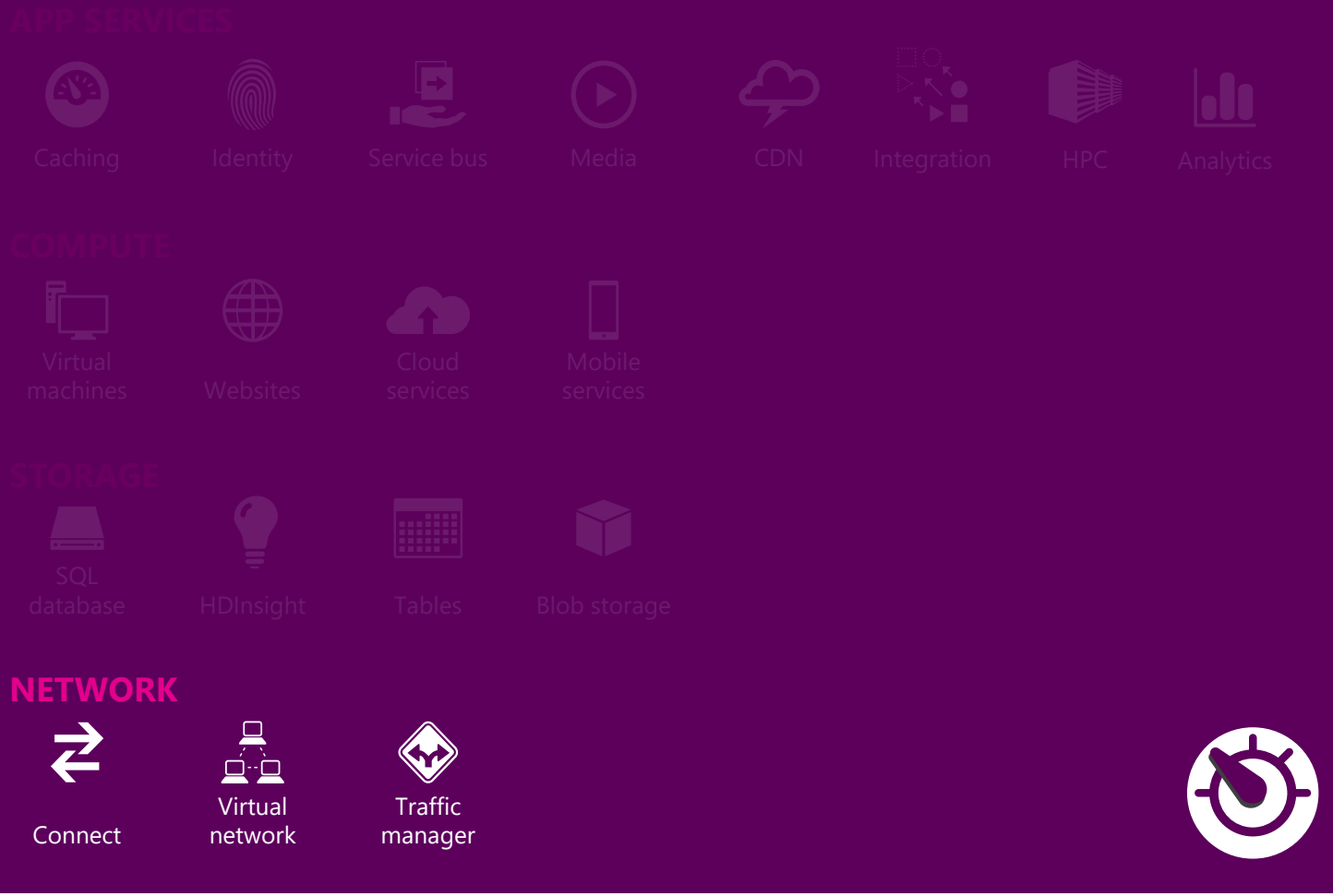
An Open and Flexible Cloud Platform that enables you to quickly build, deploy, and manage solutions across a global network of Microsoft-Managed Datacenters.

USAGE-BASED PLATFORM SERVICES

An open and flexible Cloud platform that enables you to quickly build, deploy, & manage solutions across a global network of Microsoft-managed datacenters.

Distinct Rates for each of these Service "meters"

Customers are billed for usage against one or more of these meters



44
Azure Regions
More than Any Cloud Providers

Microsoft Azure Services

Azure Platform Services

Security & Management
- Portal
- Active Directory
- Multi-Factor Authentication
- Automation
- Key Vault
- Store / Marketplace
- VM Image Gallery & VM Depot

Compute
- Cloud Services
- Service Fabric
- Batch
- Remote App

App Services
- Web Apps
- API Apps
- API Management
- Mobile Apps
- Logic Apps
- Notification Hubs

Developer Services
- Visual Studio
- Azure SDK
- Team Project
- Application Insights

Hybrid Operations
- Azure AD Connect Health
- AD Privileged Identity Management
- Backup
- Operational Insights
- Import/Export
- Site Recovery
- StorSimple

Integration
- Storage Queues
- Biztalk Services
- Hybrid Connections
- Service Bus

Media & CDN
- Media Services
- Content Delivery Network (CDN)

Analytics & IoT
- HDInsight
- Machine Learning
- Data Factory
- Event Hubs
- Stream Analytics
- Mobile Engagement

Data
- SQL Database
- SQL Data Warehouse
- Redis Cache
- Search
- DocumentDB
- Tables

Azure Infrastructure Services

Virtual Machines
- Windows
- Linux
- Containers

Storage
- BLOB Storage
- Azure Files
- Premium Storage

Networking
- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- Application Gateway

Global Infrastructure

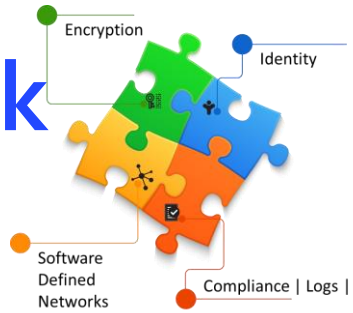
Azure Virtual Datacenter

Deploying workloads to the Cloud introduces the need to develop and maintain trust in the Cloud to the same degree you trust your Existing Datacenters.

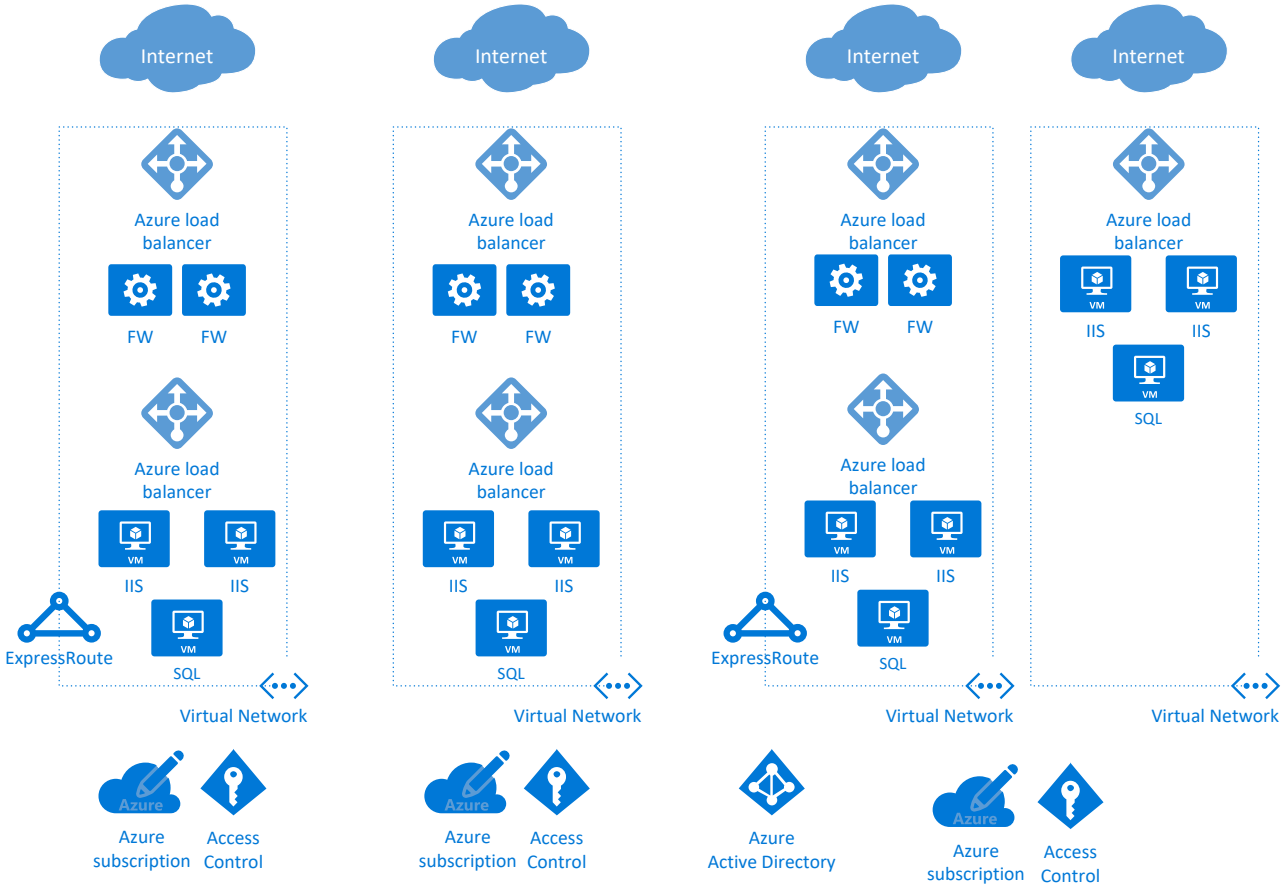
In the Azure Virtual Datacenter Model, you can apply isolation policies, make the cloud more like the physical datacenters you know, and achieve the levels of security and trust you need.

Four components any enterprise IT team would recognize make it possible: **Software-Defined Networking, Encryption, Identity Management, and the Azure platform's underlying Compliance Standards and Certifications.** These four are key to making a Virtual Datacenter a trusted extension of your existing infrastructure investment.

Azure Virtual Datacenter-Software Defined Network

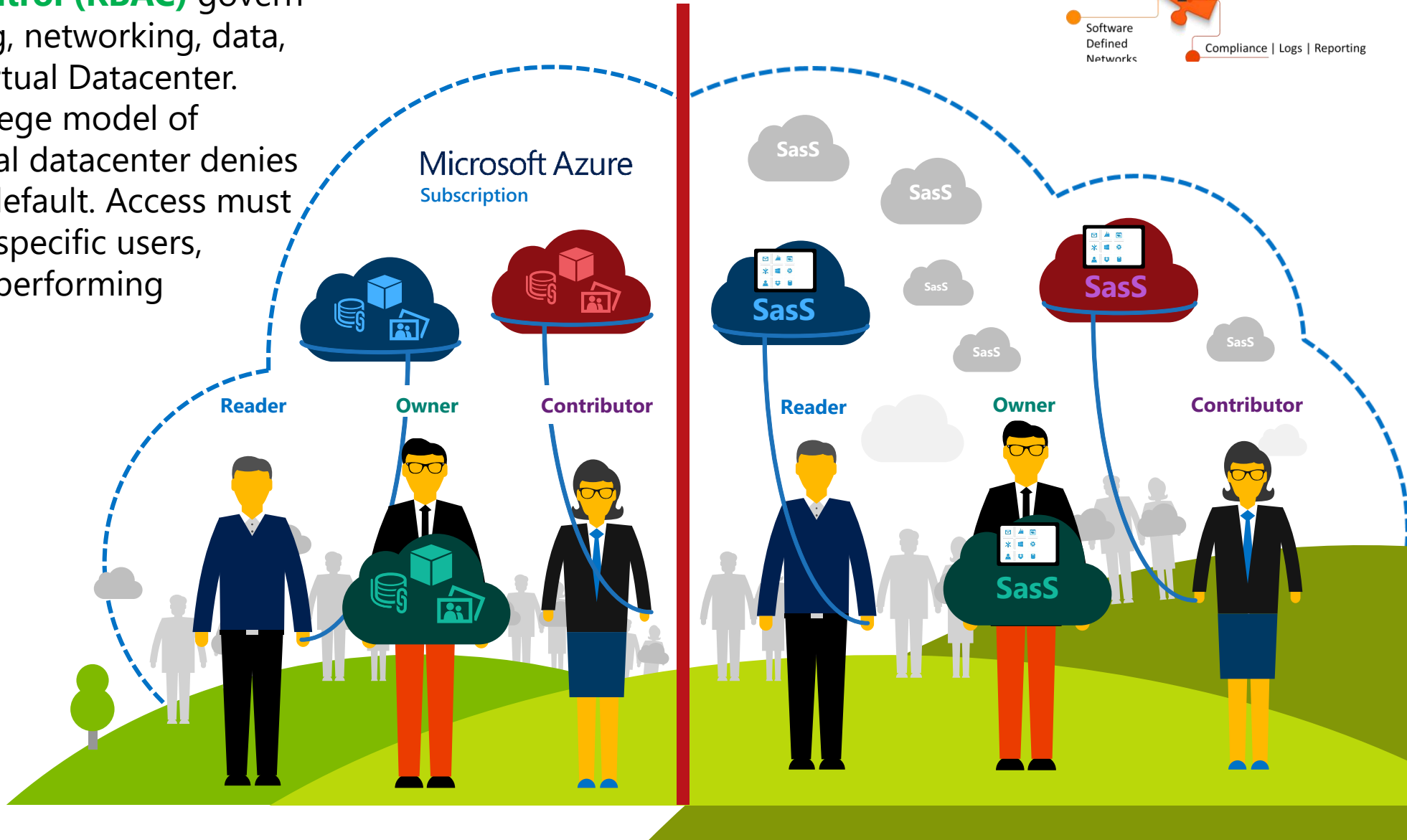


Provides virtual abstractions for your physical network elements, such as network topologies, firewalls, intrusion detection mechanisms, load balancers, and routing policy. You can create, configure, and manage network topologies, support isolation, and provision perimeter networks.

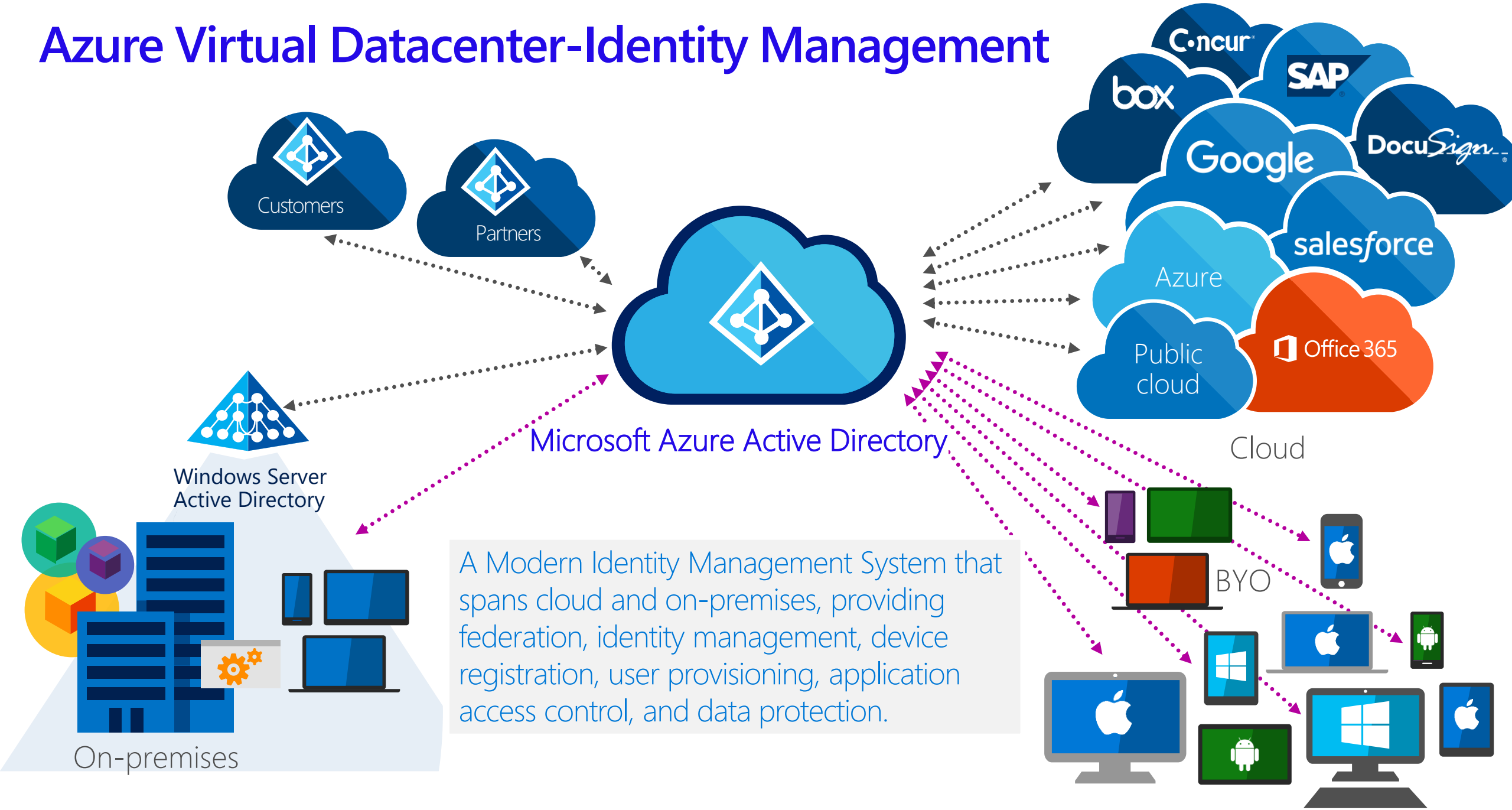


Azure Virtual Datacenter-Identity Management

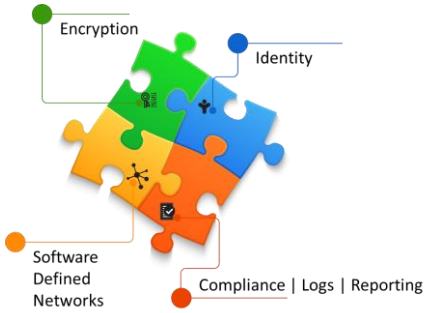
Role-Based Access Control (RBAC) govern access to the computing, networking, data, and applications in a Virtual Datacenter. Based on the least privilege model of access control, the virtual datacenter denies access to resources by default. Access must be explicitly granted to specific users, groups, or applications performing particular roles.



Azure Virtual Datacenter-Identity Management

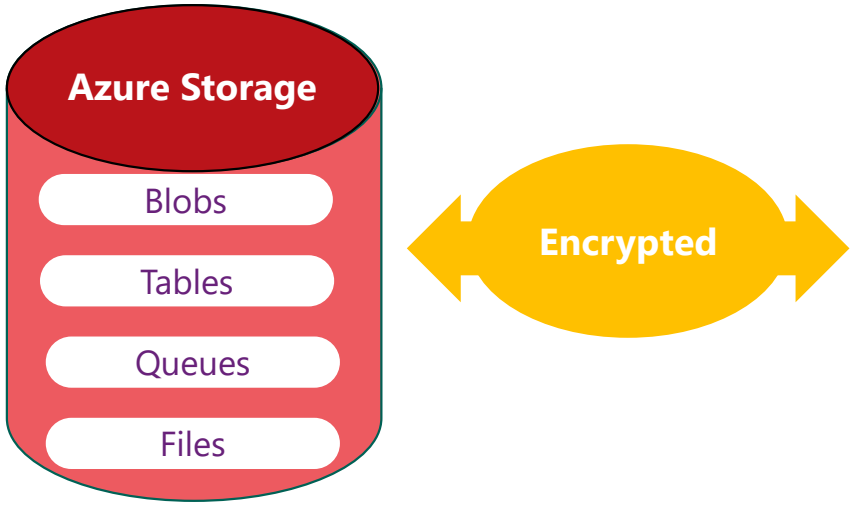


Azure Virtual Datacenter-Encryption



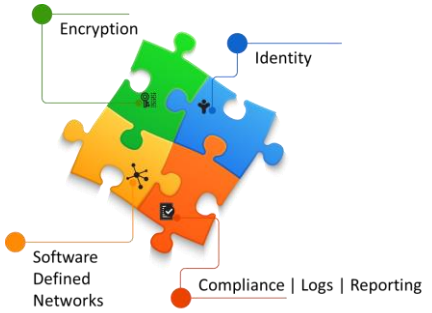
Data at Rest

Data at rest is also encrypted, including data stored on Azure Storage

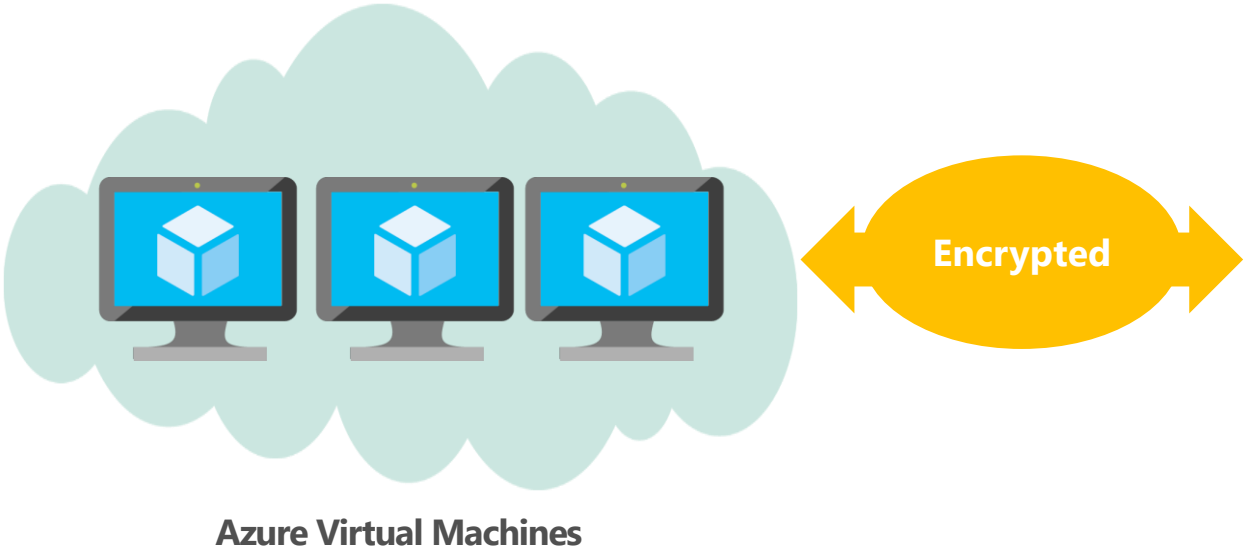


Azure Storage Service Encryption (SSE) provides encryption at rest for all Azure Storage services by encrypting data before writing it to storage. SSE decrypts the data immediately prior to retrieval. SSE-enabled Azure Storage accounts can handle encryption, decryption, and key management in a totally transparent fashion. All data is encrypted using 256-bit AES encryption, and both Microsoft-managed and customer-managed encryption keys are supported.

Azure Virtual Datacenter-Encryption



Azure VM ‘s OS & Data Disk (Azure Disk Encryption)



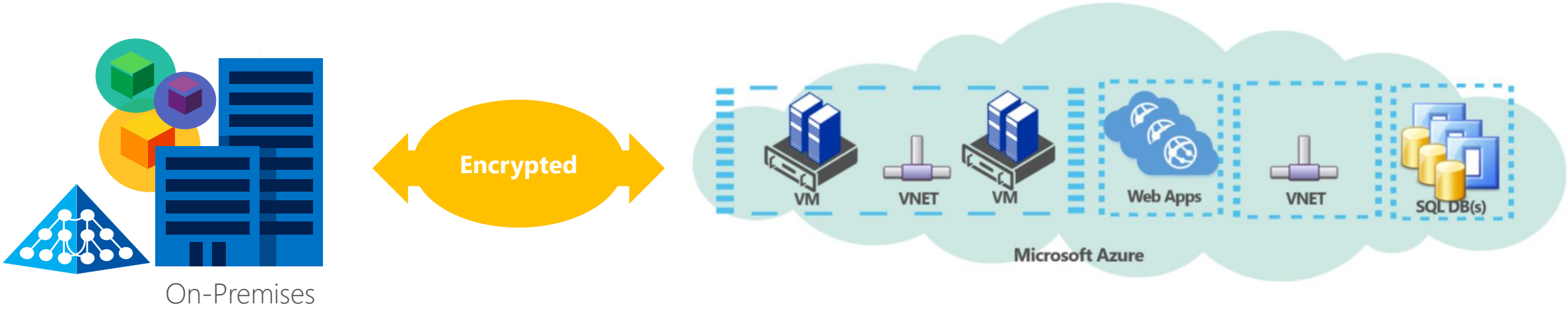
Azure Virtual Machine Encryption supports two models for encrypting virtual machines which provide volume encryption for the operating system and data disks:

1. The BitLocker feature of Windows
2. The DM-Crypt feature of Linux

Azure Virtual Datacenter-Encryption

Data in Transit

The Azure Virtual Datacenter Model uses encryption to enforce isolation of data as it moves between:



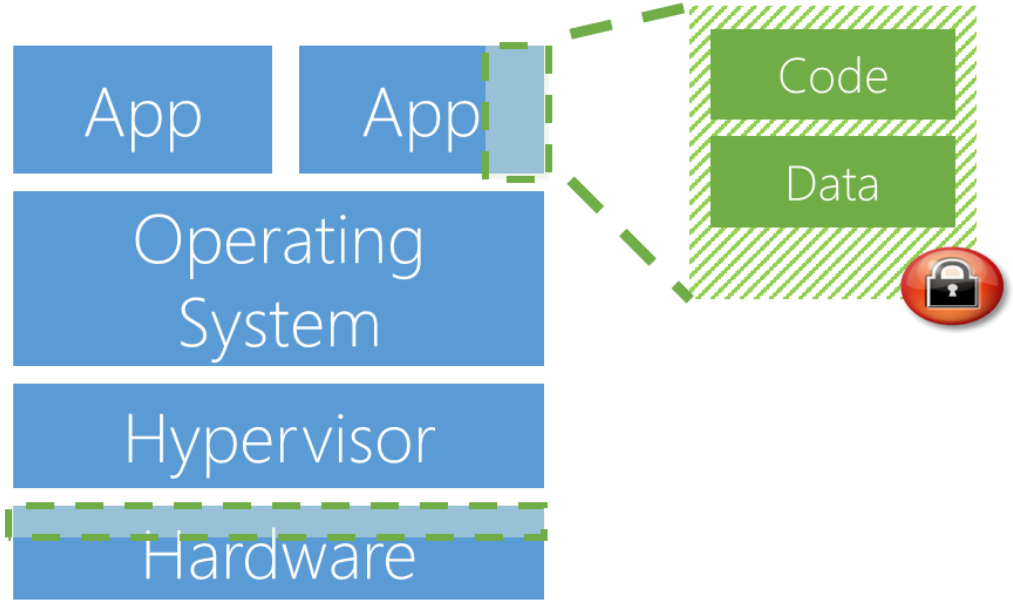
- On-premises networks and the Virtual Datacenter. Data passes through either an encrypted site-to-site virtual private network (VPN) connection or an isolated, private ExpressRoute.
- Applications running in a different virtual datacenter (that is, from one Virtual Datacenter to another).
- Applications running in the same Azure Virtual Datacenter.
- Platform services, including both internal and external endpoints—storage accounts, databases, and management APIs.

Azure Virtual Datacenter-Encryption

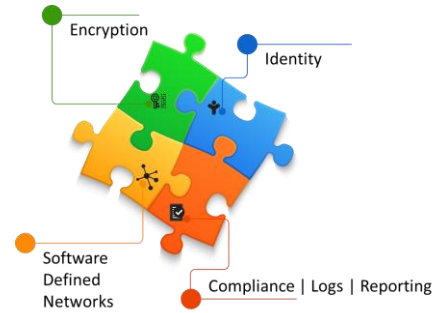
Data in Process

Azure platform is support for Confidential Computing through Trusted Execution Environments (TEE) using technologies such as enclaves. Intel Secure Guard Extensions (SGX).

With Azure Confidential Computing, we're developing a platform that enable developers to take advantage of different TEEs without having to change their code. Initially we support two TEEs, Virtual Secure Mode and Intel SGX. Virtual Secure Mode (VSM) is a software-based TEE that's implemented by Hyper-V in Windows 10 and Windows Server 2016 Hyper-V.



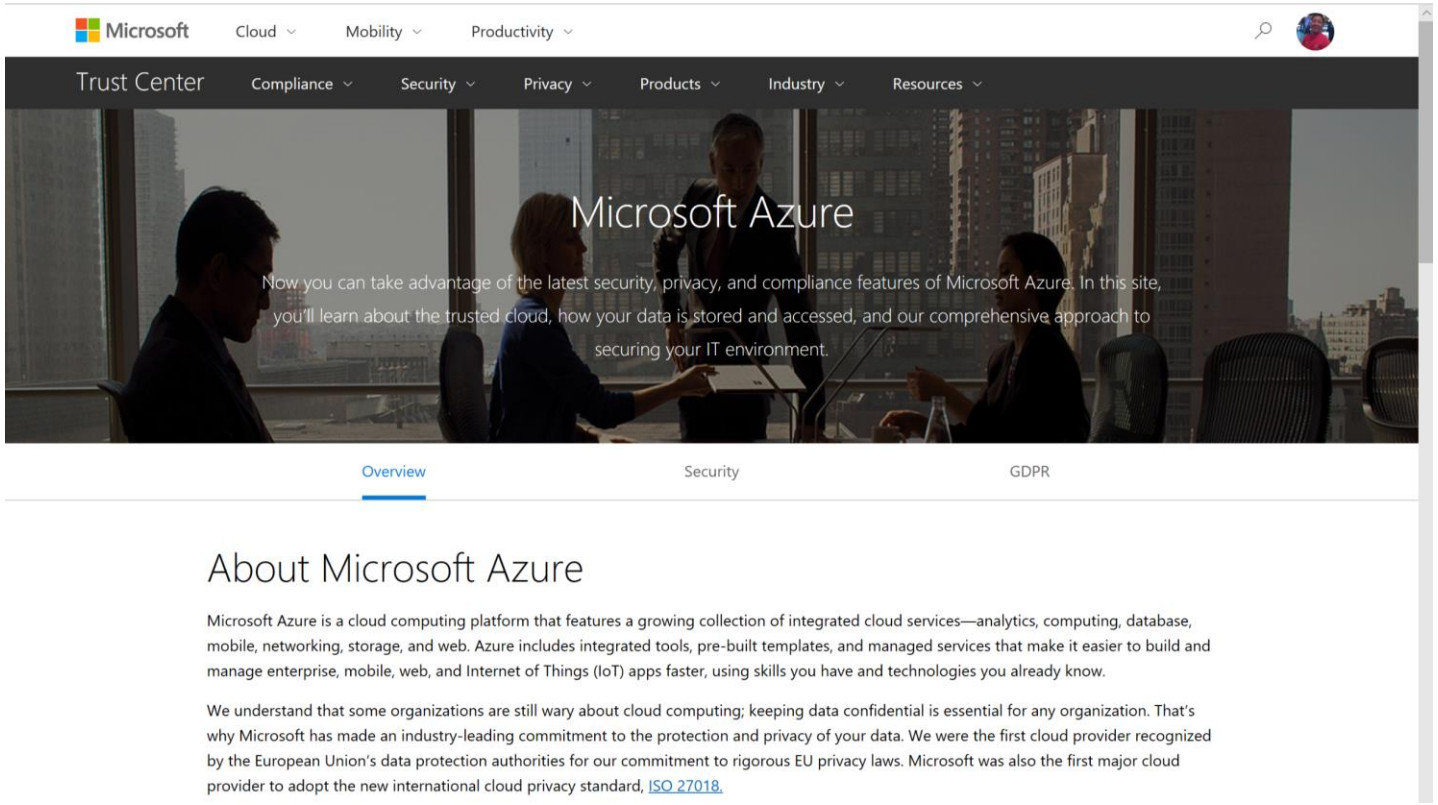
Azure Virtual Datacenter-Compliance



Azure Infrastructure and Services meet a broad set of international, industry-specific, and country-specific compliance standards. To help ensure the safety of your data, Microsoft also verifies how compliance is achieved through rigorous third-party audits that validate Azure's adherence to standards-mandated security controls. In addition, virtual datacenters make extensive use of automated compliance monitoring, logging, and reporting

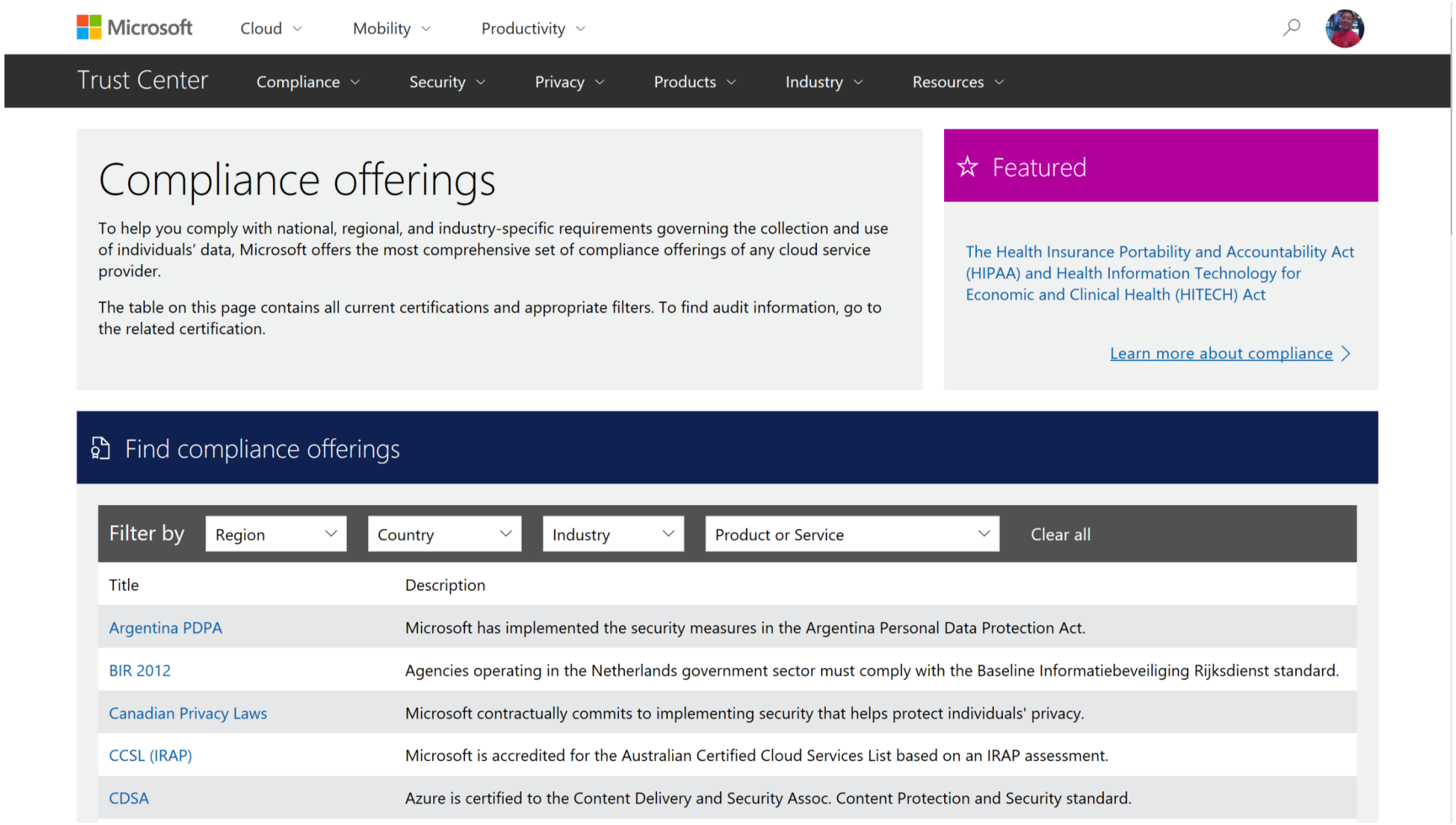
Azure Virtual Datacenter-Compliance

Microsoft Trust Center where Microsoft proves to its customers a trustworthy platform. From the center, Microsoft shows not only compliance achievement but also security privacy and its practices.

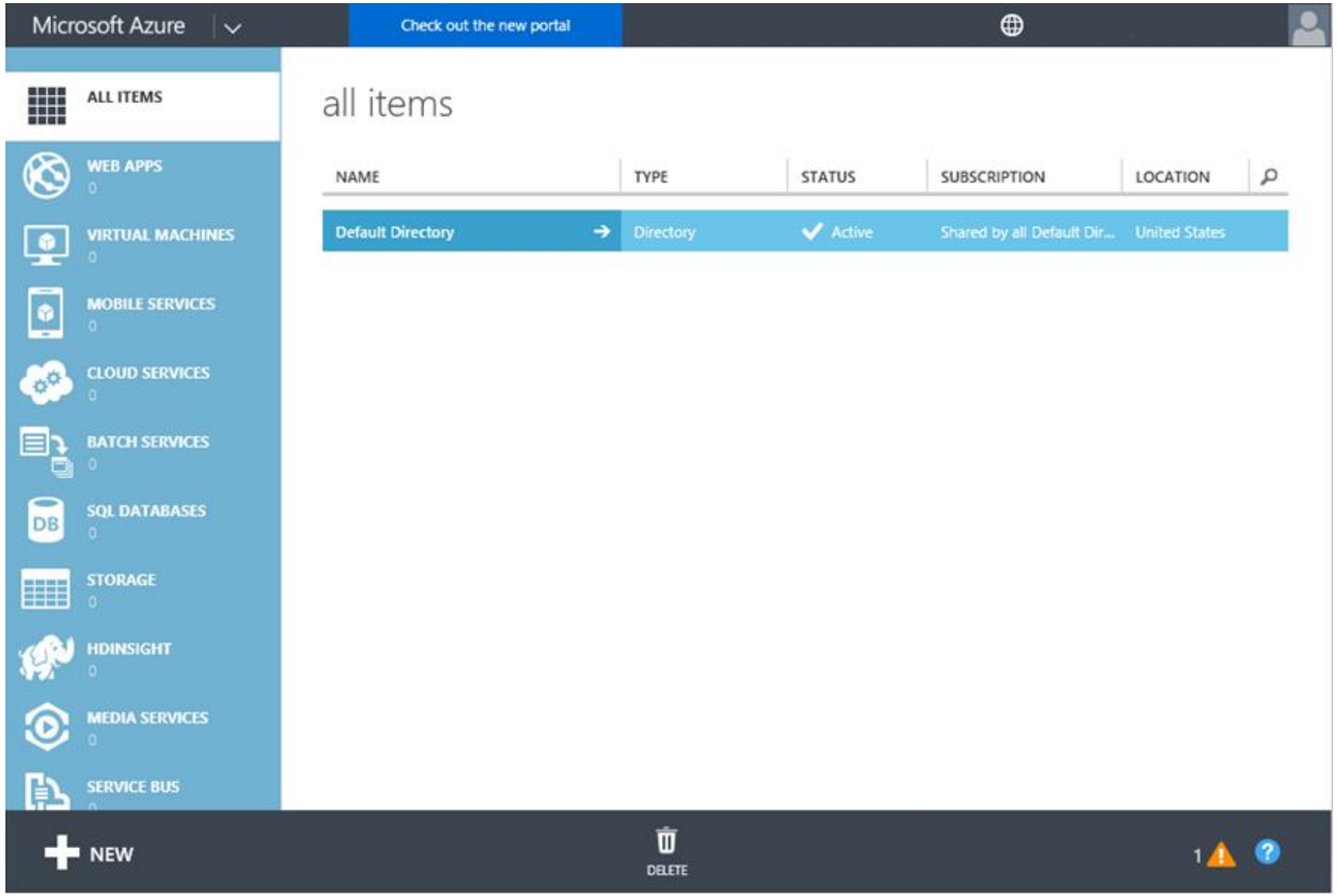


https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure

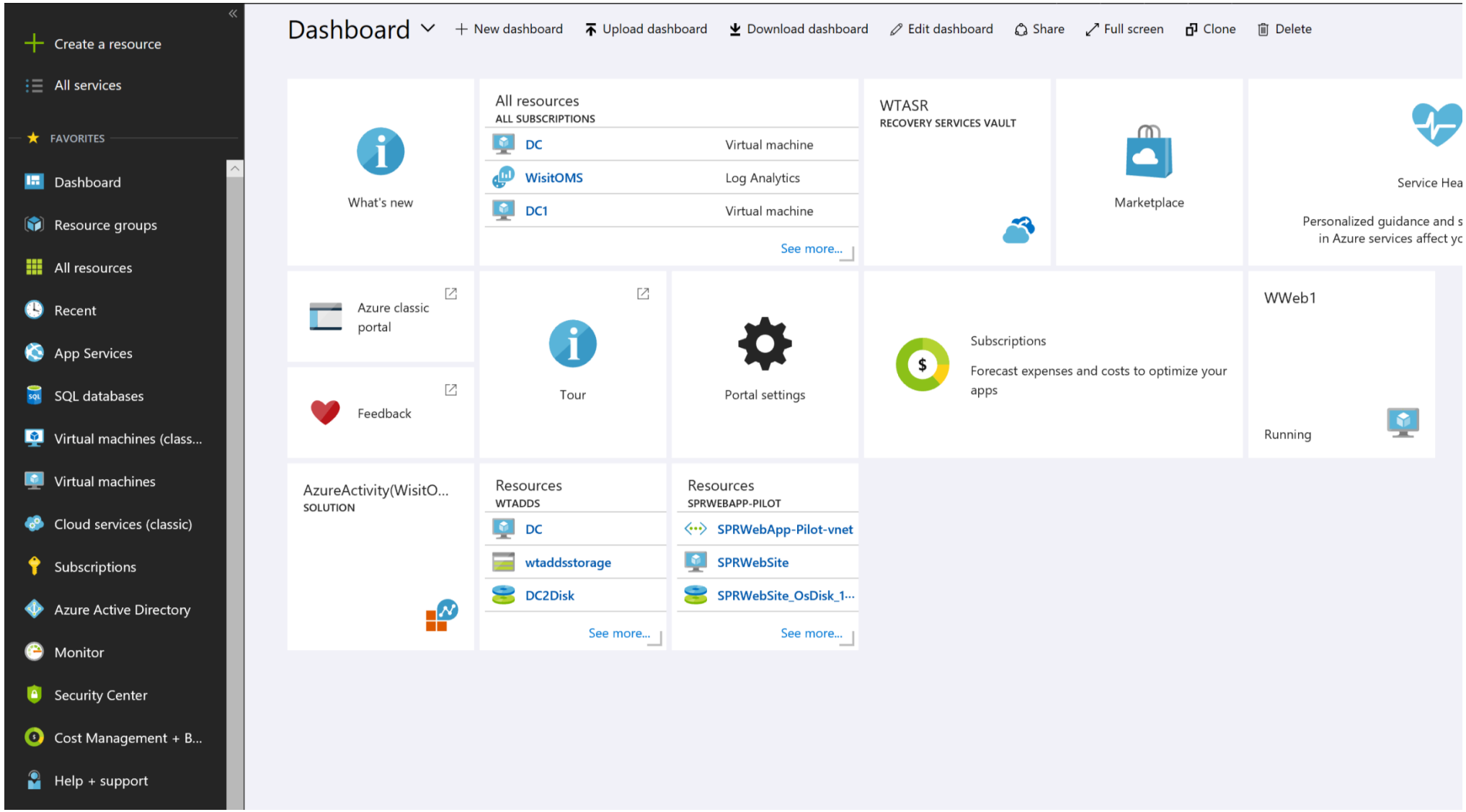
Azure Virtual Datacenter-Compliance



Azure Service Management (ASM)-Classic Portal

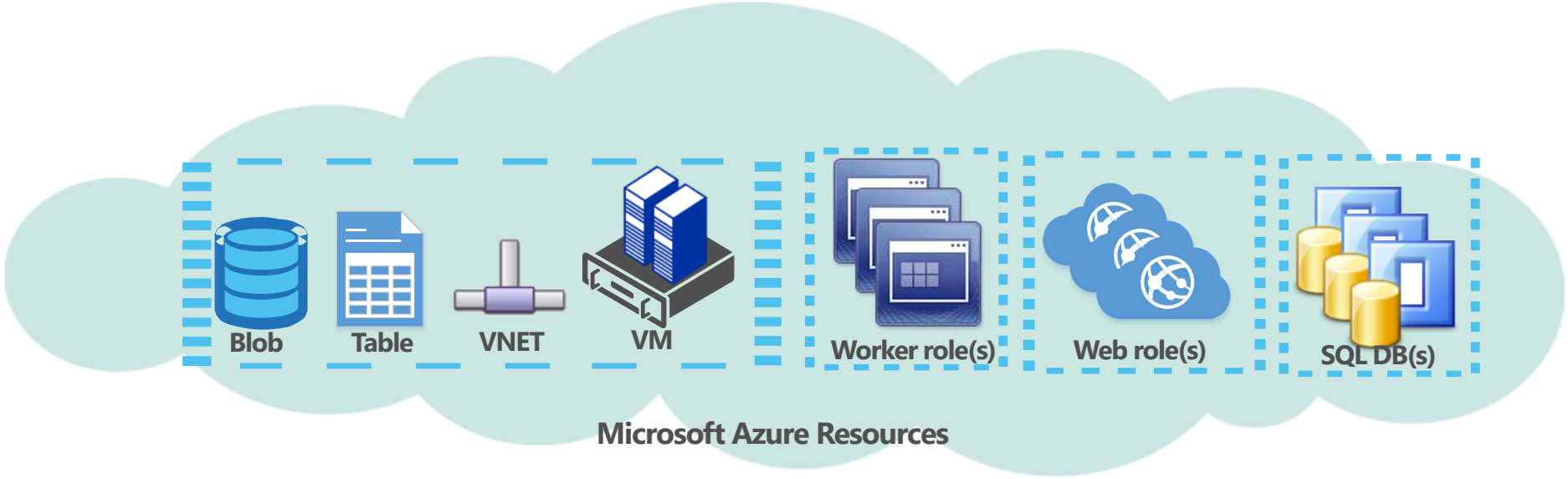


Azure Resource Manager (ARM)-Azure Portal



ARM Concept & Terminology

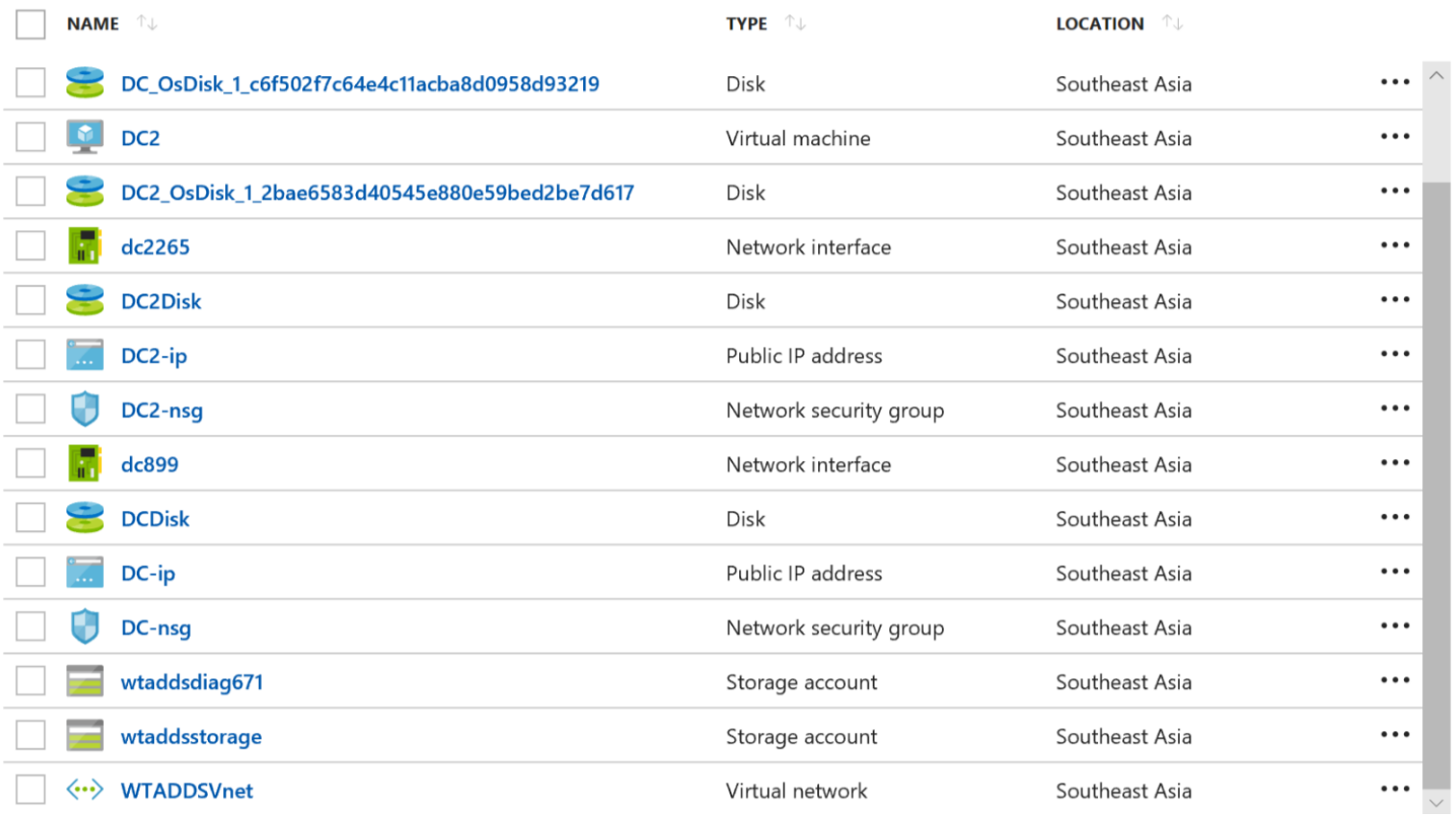
With the Azure Resource Manager (ARM), Everything in Azure is a Resource.



Examples of resources are a virtual machine, network interfaces, public IP address, storage accounts, virtual networks, and more. ARM is based on concepts related to resource providers and resource consumers. Azure provides resources and services through multiple resource providers that are consumed and deployed in groups.

ARM Concept & Terminology

Resource Groups are a unit of deployment in the ARM. They are containers grouping multiple resource instances in a security and management boundary. A resource group is uniquely named in a subscription. Resources can be provisioned on different Azure regions yet belong to the same resource group.



NAME	TYPE	LOCATION
DC_OsDisk_1_c6f502f7c64e4c11acba8d0958d93219	Disk	Southeast Asia
DC2	Virtual machine	Southeast Asia
DC2_OsDisk_1_2bae6583d40545e880e59bed2be7d617	Disk	Southeast Asia
dc2265	Network interface	Southeast Asia
DC2Disk	Disk	Southeast Asia
DC2-ip	Public IP address	Southeast Asia
DC2-nsg	Network security group	Southeast Asia
dc899	Network interface	Southeast Asia
DCDisk	Disk	Southeast Asia
DC-ip	Public IP address	Southeast Asia
DC-nsg	Network security group	Southeast Asia
wtaddsdiag671	Storage account	Southeast Asia
wtaddsstorage	Storage account	Southeast Asia
WTADDSVnet	Virtual network	Southeast Asia

Azure Deployment Model-ARM Benefits

Grouping: ARM allows grouping of resources together in a logical container. These resources can be managed together

Role-Based Access Control: Granular roles and permissions can be assigned to resources providing discreet access to users. Users can have only those rights that are assigned to them.

Deployment Support: ARM provides deployment support in terms of templates enabling DevOps and Infrastructure as Code (IAC). The deployments are faster, consistent, and predictable.

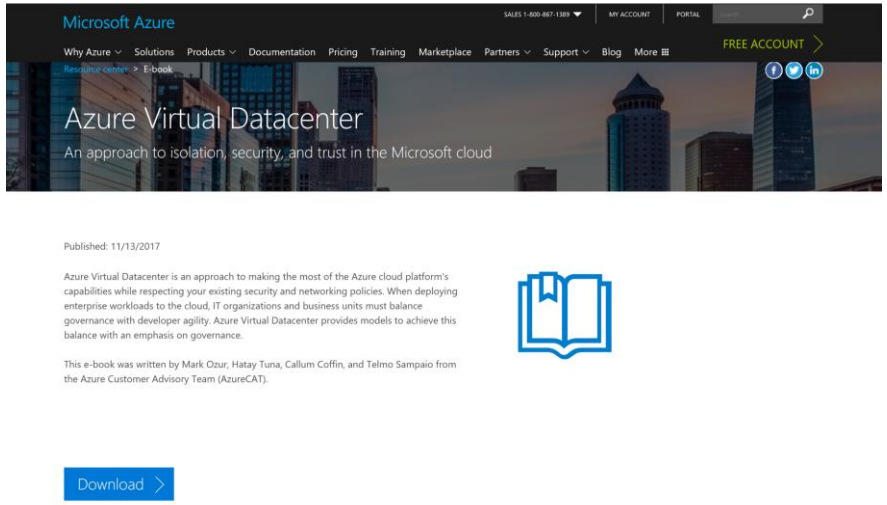
Superior Technology: Cost and billing of resources can be managed as a unit. Each resource group can provide their usage and cost information.

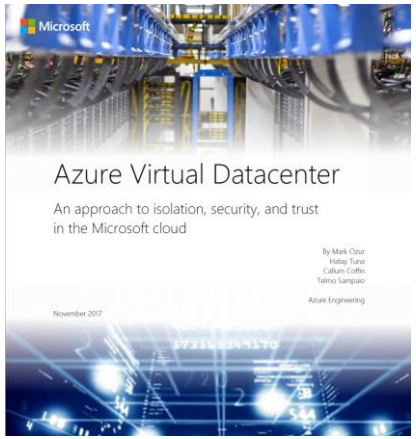
Manageability: ARM provides advanced features such as security, monitoring, auditing, and tagging features for better manageability of resources. Resources can be queried based on tags. Tags also provide cost and billing information for resources tagged similarly.

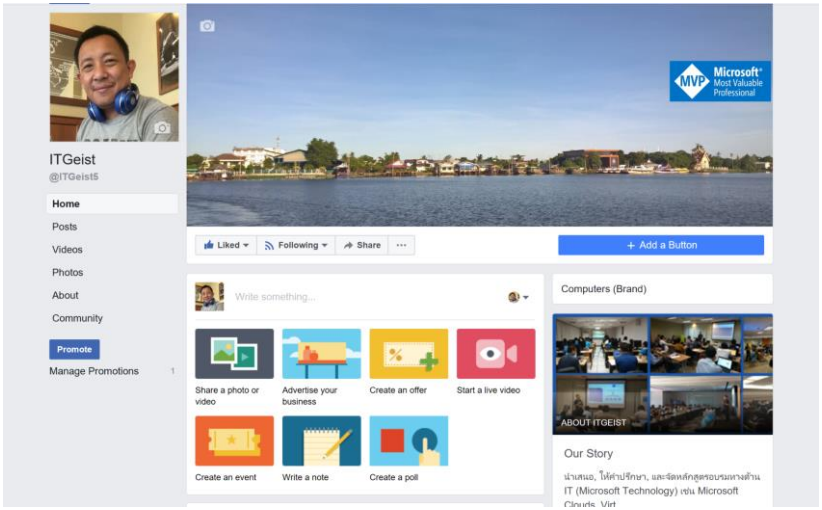
Migration: Easier migration and update of resources within, as well as from across resource groups.

Resources:

E-Book: https://azure.microsoft.com/en-us/resources/azure-virtual-datacenter/







Microsoft

Thank You ☺