Microsoft

Addressing Data sovereignty

Customer environments and application requirements are evolving

100's–1,000's of apps


VMs


Databases


Containers


Serverless

Diverse infrastructure


Datacenters


Hosters


Branch offices


OEM hardware


IoT devices


Edge

Multi-cloud

Five characteristics of a trusted hybrid cloud provider

Only Microsoft delivers across the board

1

Comprehensive continuum across on-premises, multi-cloud, edge, and disconnected scenarios

2

Allow you to maximize investment in existing infrastructure and bring cloud services to any infrastructure

3

Offer a control plane to manage and secure any resource on-premises and across multiple clouds

4

Support key needs including data sovereignty, regulations and operating in harsh environments

5

Have an ecosystem across hardware OEMs, SIs, and ISVs to support diverse needs and geos

Azure Hybrid

Innovation anywhere with Azure

Bring Azure services to any infrastructure

Modernize datacenters with Azure Stack

Extend to the edge with Azure IoT

Modernize datacenters with Azure Stack

Azure Stack Hub
Cloud-native integrated system

Disconnected scenarios
Data sovereignty
Application modernization

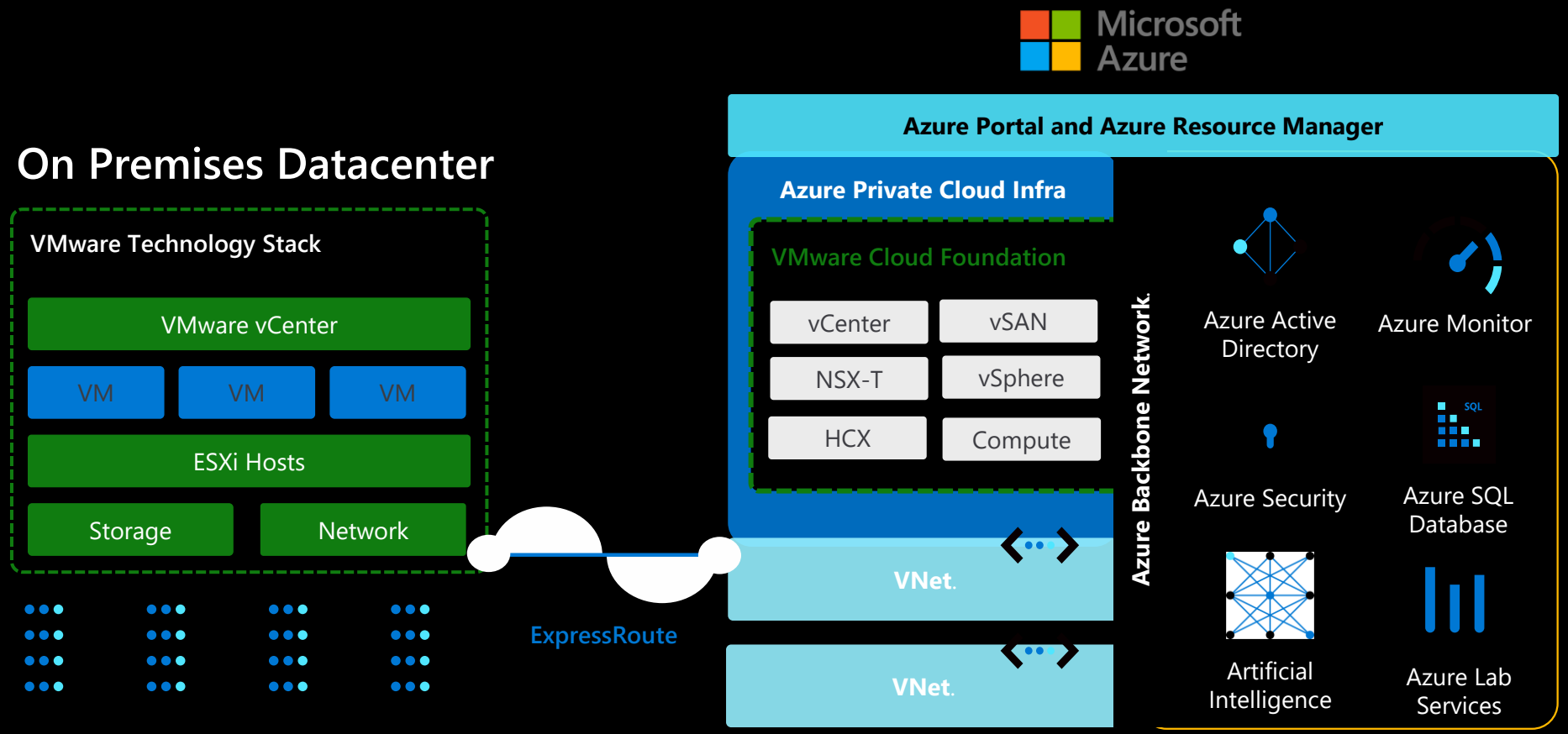
Azure Stack HCI
Hyperconverged solution

Scalable virtualization and storage
Remote branch office
High-performance workloads

Azure Stack Edge
Cloud-managed appliance

Machine learning at the edge
Edge compute and IoT solutions
Network data transfer to cloud

Azure VMware Solution – Run VMware natively on Azure



Help enforce data residency with governance

Azure Policy

Create, assign, and manage policies for data residency that assess your resources for compliance in real-time and enforce rules.

Allowed locations

Azure Policy enables you to restrict the locations your organization can specify when deploying resources. Use it to enforce your geo-compliance requirements.

Azure Blueprint

Easily create, deploy, and update compliant cloud environments with pre-designed data residency policies and controls.

Compliant environment

Using Azure Blueprint, you can include policies to automatically hard code the regions allowed for deploying resources in a cloud environment.

Discovering and classifying your data

Discovery Tools

Azure Data Catalog helps you easily discover, understand, and use enterprise data sources.

Searching
Match search terms against any property in the catalog.

Filtering
Select specific characteristics and only view matching assets.

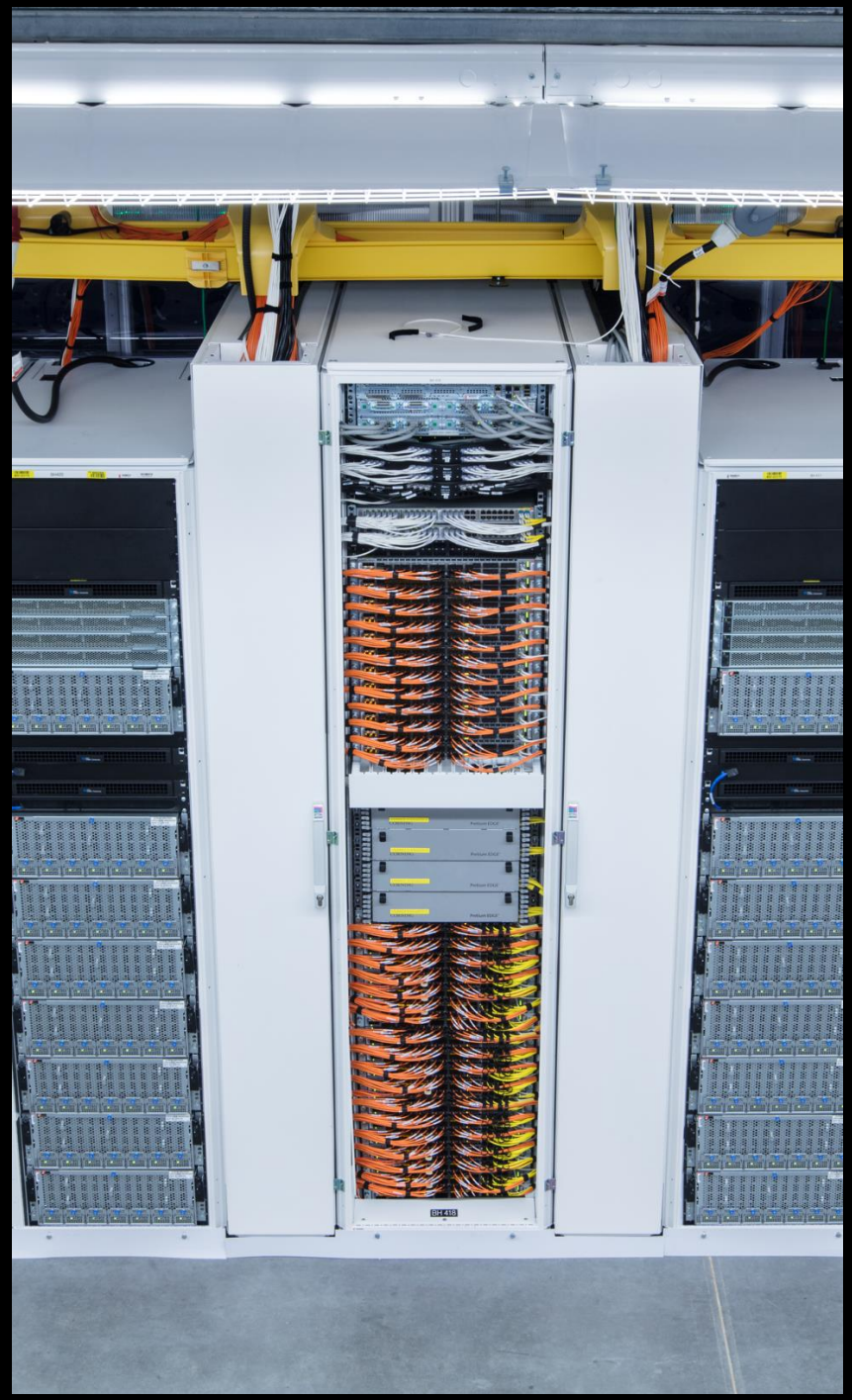
Classification Tools

Azure Information Protection (AIP) helps organizations classify and protect documents, emails, and other sensitive data.

Labels
Track and organize data by applying labels manually or automatically through policies.

Permissions
Assign access rights to data to control who can access it, and how.

Classification
Configure policies to classify, label, and protect data based on sensitivity.



Encrypting data at each phase

Standard data protection

At rest
Encrypt data when stored in blob storage, databases, etc.

Examples:
- Azure Storage Service Encryption
- SQL Server Transparent Database Encryption (TDE)

In transit
Encrypt data flowing between untrusted public or private networks

Examples:
- HTTPS
- TLS

Protect data in use

In use (in preview)
Encrypt data during computation and keep it within specified Geo

Examples:
- Trusted Execution Environments such as Intel SGX and VBS
- Homomorphic encryption

Thank you