Azure E-Book Series

Microsoft Azure

Cloud anywhere:

Azure for hybrid and multicloud environments

Contents

01 /

Introduction

The cloud is the foundation of digital transformation. Companies that strategically leverage the hybrid cloud can capture significant value, value that differentiates them from their competitors with improved time to market and flexibility in managing costs and scale.

Today, 94% of companies use the cloud in some way,[1] but every company moves to the cloud at a different pace and has different strategies and priorities for what needs to be deployed to the cloud. Some will adopt cloud computing to solve an urgent business need; others will have a longer term, planful cloud migration. Either way, the ongoing effort to improve business operations and create an agile development process can have organizations working in IT environments that span across on-premises, multicloud, and edge infrastructure.

While some may argue that hybrid cloud is a stepping-stone to a fully in-the-cloud business, many companies recognize that a hybrid cloud strategy is not transitional, but a part of optimizing infrastructure over a wide variety of considerations. Hybrid cloud infrastructure is a natural evolution of information technology that typically happens at a gradual pace. Companies transition some of their hardware and software to cloud services and technologies, resulting in a computing environment that combines on-premises, multicloud, and edge computing, using software-as-a-service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Many enterprise IT managers—as many as 85% according to one study—have focused on hybrid cloud as the best model for their business.[2]

A key challenge for these companies, however, is providing a truly integrated solution across their environments for users, developers, and administrators. To help businesses deal with the increasing complexity of blended infrastructure—often with tens of thousands of applications—IT managers need to manage and maintain environments that span on-premises technology, multicloud services, and edge devices. This challenge is particularly serious for companies with legacy IT assets—or those with complex regulatory or edge computing requirements—that must keep up with the pace of innovation.

As the central IT team, you need to find a way to build and maintain a platform,

regardless of where in your environment it runs. You also need to manage your hybrid environment in a way that maximizes productivity and agility without ever sacrificing important concerns like security and compliance.

To help your IT team respond to the need to work efficiently in a complex environment, Azure offers services that help you to govern and manage across your environment, build apps and deploy them to any location, deploy and manage Azure services on Kubernetes clusters, and deliver security across your organization. With the ability to use on-premises, multicloud, or edge technologies to develop, deploy, manage, and secure your application infrastructure, Azure hybrid cloud gives your team the ability to easily integrate a variety of technologies in a scalable, reliable, and efficient architecture.

This e-book aims to show you best practices—including what you should look out for and the fundamental steps any company needs to take to enable hybrid environments. It also provides you with some insights into common use cases for hybrid cloud, some of which may be instantly relatable, and others which may present new ideas for how to work in a hybrid environment. After a quick description of three important factors in setting up a hybrid cloud environment—networking, identity management, and security—the e-book covers six different hybrid use cases, allowing you to explore topics that are most relevant to your business.

---

[1] RightScale. "2019 State of the Cloud Report." Flexera RightScale, Feb. 2019, p. 2. https://resources.flexera.com/web/media/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf. [PDF]

[2] Nutanix. "The Nutanix Enterprise Cloud Index 2019." Survey report. Nov. 2019. https://www.nutanix.com/enterprise-cloud-index

02 /

Hybrid infrastructure fundamentals

To build an optimal hybrid cloud infrastructure, businesses need to create a reliable, efficient, and secure foundation. The following section covers three fundamental areas that need to be understood to build that architecture: networking, identity and access management, and security.

If you are planning a larger-scale migration to the cloud, you can find guidance in the Cloud Adoption Framework for Azure, which aims to help IT professionals and cloud architects define their cloud strategy and migrate their on-premises workloads. The framework focuses on assessing the current infrastructure, migrating applications and infrastructure to the cloud, optimizing their architecture to reduce costs, and managing their workloads and data more securely. In addition, by helping developers take responsibility for their code—so-called shifting left—the resulting applications will be updated, patched, and secured more quickly.

The Cloud Adoption Framework focuses on bringing together heterogenous components of a company's infrastructure—and delivering a single management, deployment, and administrative platform.

For this guide, rather than covering all aspects of cloud adoption, we will instead take a look at three areas that are of particular importance for those organizations currently working in, or moving into, a hybrid or multicloud environment: networking, identity and access management, and security.

Hybrid fundamentals

01. Networking

There are many ways to create a reliable, yet cost-effective, network that can act as the backbone of a hybrid solution. Networks depend on several areas of functionality. When you think about your network architecture in the cloud, it's important that you focus on the following areas:

- Connect and extend: Businesses need to connect existing resources and extend their own networks by using technology such as VPNs, ExpressRoute, and Virtual WAN.
- Protect: Any connection could be an entry point to the network, so your company should protect itself with the best tools available, such as DDoS protection, firewalls, and web application firewalls.
- Deliver: A great customer experience requires a network built for application delivery, with Azure Front Door and Application Gateway technologies.

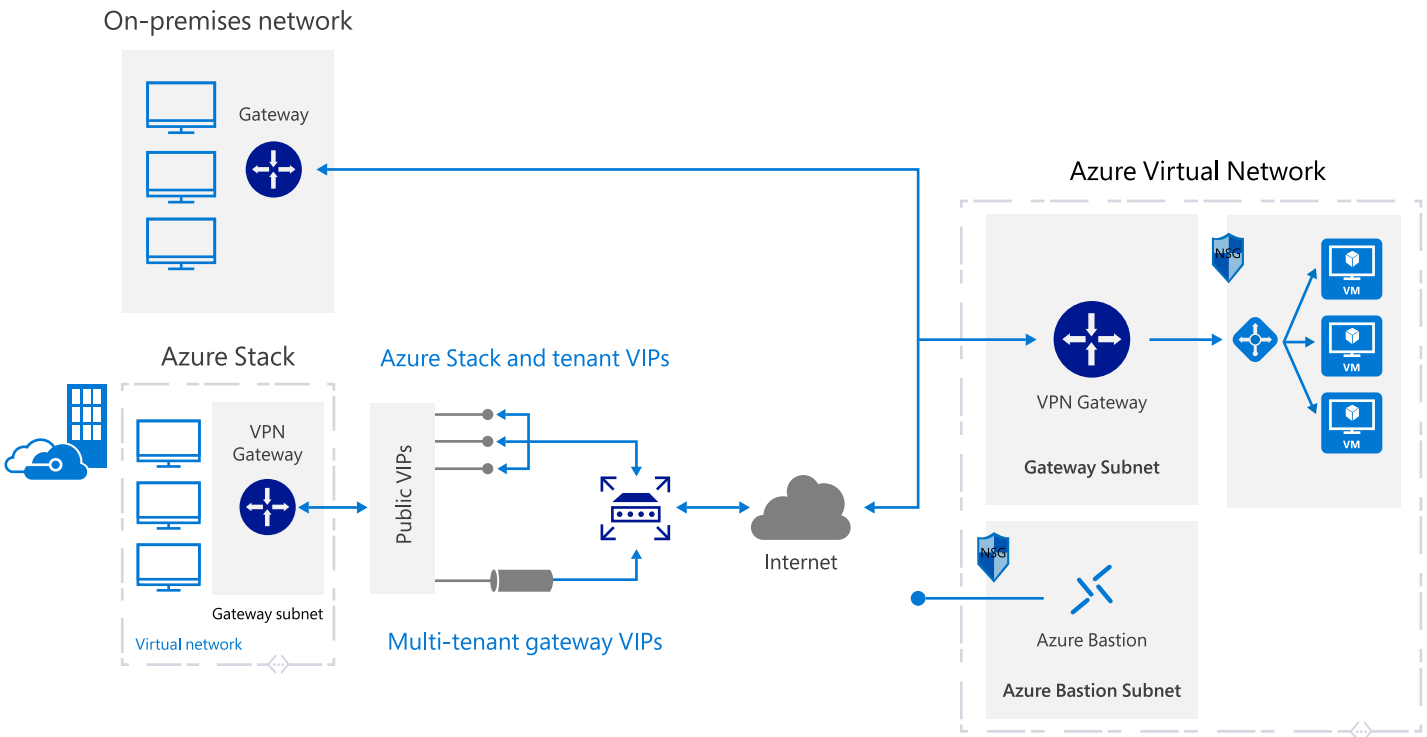
In this e-book we focus only on the most common scenarios for connecting and extending your existing network, as well as one basic service for application delivery. For more detailed information about Azure networking services please visit the documentation here: https://docs.microsoft.com/azure/networking/networking-overview

Connect and extend

VPN connection

A virtual network gateway sends encrypted traffic between an Azure Virtual Network (VNet) and an on-premises location using the public internet. This architecture is suitable for hybrid applications where the traffic between on-premises hardware and the cloud is likely to be light, or you are willing to trade slightly extended latency for the flexibility and processing power of the cloud.

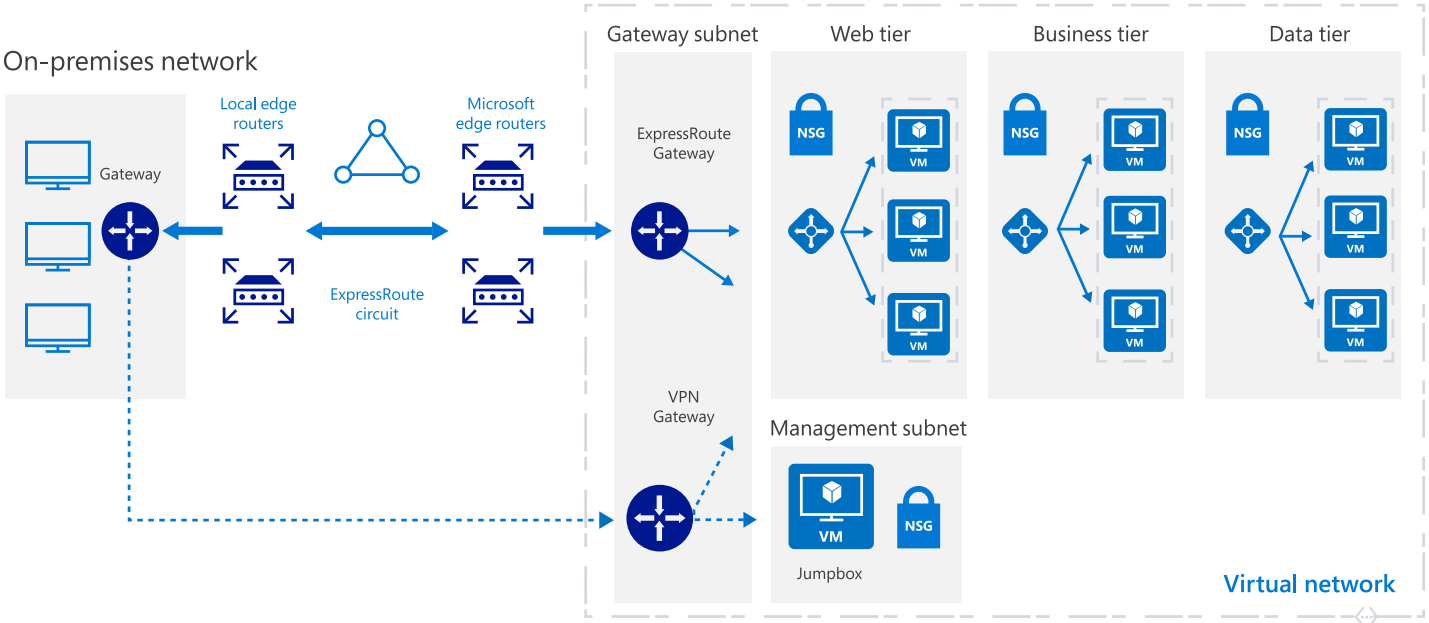
- Benefits: Simple to configure; cost-effective; much higher bandwidth available (up to 10 Gbps depending on the service).
- Challenges: Requires an on-premises VPN device; reliability. (Microsoft guarantees 99.9% availability for each VPN gateway, but the network connection may not be reliable).



ExpressRoute with VPN failover

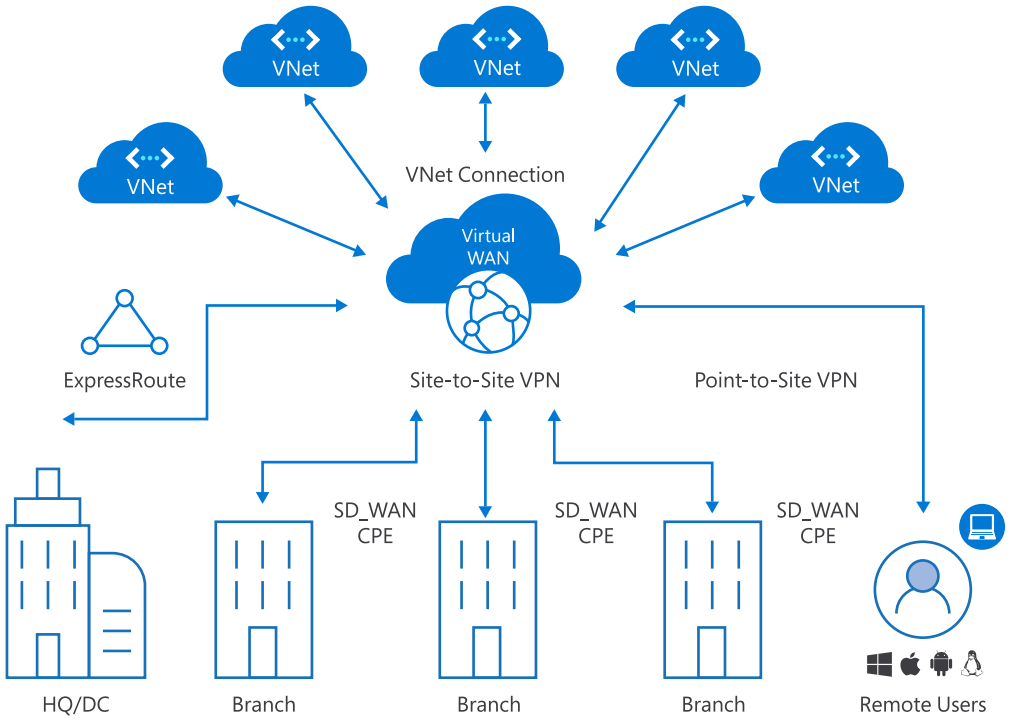
This option combines the previous two, using ExpressRoute in normal conditions, but failing over to a VPN connection if there is a loss of connectivity in the ExpressRoute circuit. This architecture is suitable for hybrid applications that need the higher bandwidth of ExpressRoute, and also require highly available network connectivity.

- Benefits: High availability
- Challenges: More complex to configure than a VPN connection, as both external links must be configured; requires redundant hardware and connections; more expensive



Virtual WAN

For companies with branch offices, Azure Virtual WAN can link those sites with optimized and automated network connectivity to, and through, Azure. Azure Virtual WAN brings together many Azure cloud connectivity services such as site-to-site VPN, user VPN (point-to-site), and ExpressRoute into a single operational interface, enabling global transit network architecture based on a classic hub-and-spoke connectivity model.
Read more about Virtual WAN here: https://azure.microsoft.com/services/virtual-wan/

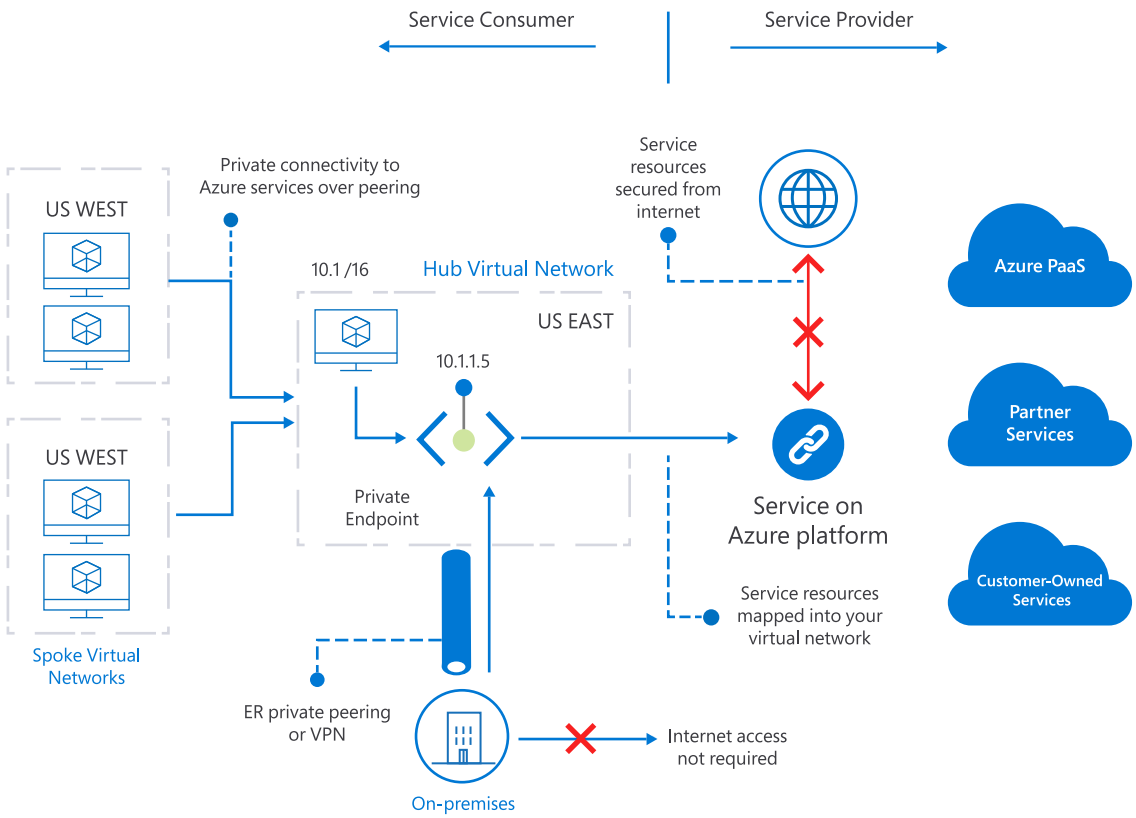


Private Link

Azure Private Link enables you to access Azure PaaS (for example, Azure Storage, Azure Cosmos DB, and SQL Database) and Azure-hosted customer or partner services over a private endpoint in your virtual network. Traffic between your virtual network and the service traverses over the Microsoft backbone network, eliminating exposure from the public internet.

With Private Link, your company can:

- privately access services on the Azure platform,
- access services running in Azure from on-premises over ExpressRoute private peering or VPN tunnels,
- gain protection against data exfiltration by mapping resources to a specific instance of the customer's PaaS resource,
- connect privately to services running in other regions, and
- extend to your own services by placing your service behind a load balancer to enable Private Link.



Deliver

Azure Front Door

Every internet-facing web application, whether serving a large audience or a small set of users in a single region, is by default a global application, placing demands on you to maximize performance for your end users and ensure the application is always-on across failures and attacks. Azure Front Door is a scalable and secure entry point for fast delivery of your global applications that gives companies application and API acceleration, load balancing of HTTP traffic, scalable SSL offloading, and a web application firewall at the edge. Learn more about Azure Front Door: https://azure.microsoft.com/services/frontdoor/

Hybrid fundamentals

02. Identity and access management

Today, corporations are using a more complex mixture of on-premises and cloud applications, with workers requiring access across environments, making integrated management critical. Identity solutions should leverage a common user identity for authentication and authorization to all resources, regardless of location. We call this *hybrid identity*.

Choosing the correct authentication method is the first concern for organizations wanting to move their applications to the cloud. The authentication method is a critical component of an organization's cloud infrastructure; it's the foundation of all the other advanced security and user experience features in Azure Active Directory (AD). Identity is the new control plane, giving the business control amid the chaos of users, devices, and a variety of connected endpoints, including applications, sensors, and bots.

To choose an authentication method, you need to consider the time, existing infrastructure, complexity, and cost of implementing your choice. These factors are different for every organization and will likely evolve.

Azure AD supports the following authentication methods for hybrid identity solutions:

- **Cloud authentication:** Azure AD handles the user sign-in process, which, coupled with seamless single sign-on, allows users access to cloud and on-premises applications without having to reenter their credentials. With Azure AD password hash synchronization, users can use the same username and password that they use on-premises without having to deploy any additional infrastructure, gaining the additional benefit that passwords are not stored in the cloud, which can help satisfy regulations and protect against outages. With Azure AD Pass-through Authentication, the servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud and which may be required by industry or government regulations.

- **Federated authentication:** For companies that cannot support in-the-cloud authentication due to regulatory requirements, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services, to validate the user's password. While this approach is not recommended, the authentication system can provide additional advanced authentication, such as smart-card-based authentication or third-party multifactor authentication—an improvement over strictly on-premises solutions.

Integrating your on-premises directories with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources. The solution synchronizes on-premises identities with Azure AD, while IT keeps the on-premises Active Directory running with any existing governance solutions as the primary source of truth for identities. Microsoft's Azure AD hybrid identity solution spans on-premises and cloud-based capabilities, creating a common user identity for authentication and authorization to all resources regardless of their location.

Hybrid identity also powers application management. Organizations often have hundreds of applications that users depend on to get their work done, with users accessing these applications from many devices and locations. With so many applications and access points, it's more critical than ever to use a cloud-based solution to manage user access to all applications.

Hybrid fundamentals

03. Security

As operations and applications expand across on-premises, multicloud, and edge infrastructure, security becomes complex. In this era of frequent data breaches, having a cloud platform that protects databases and unstructured data lakes is critically important. Azure gives companies two ways to manage security from a single place.

Microsoft Defender for Cloud

Microsoft Defender for Cloud allows businesses to manage their security postures across every infrastructure from a single portal by setting policies for different resources, monitoring for violations and anomalies, and performing common security tasks, such as patching, compliance testing, and configuration management. Security is a part of the fabric of Azure, giving companies capabilities that specific applications or services might not otherwise have.

Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native, security information and event management (SIEM) as well as a security orchestration automated response (SOAR) solution. The capability gives your IT team access to real-time security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

As breaches continue to affect business, quick discovery and remediation become essential for the security of your infrastructure. Microsoft Sentinel collects data across all parts of your hybrid cloud architecture and from other cloud providers as well, supporting multicloud strategies. By combining global and industry threat intelligence, the platform can also detect sophisticated attackers and reduce false positives. Microsoft Sentinel incorporates artificial intelligence (AI) to help companies respond more quickly, and in the right way, to investigate each threat.

Building on the full range of existing Azure services, Microsoft Sentinel natively incorporates proven foundations, like Log Analytics and Logic Apps. Microsoft Sentinel enriches your investigation and detection with the Microsoft threat intelligence stream and enables you to bring your own threat intelligence by adding AI and machine-learning features.

Microsoft Sentinel capabilities

03 /

Common hybrid use cases

01. Organize and govern across environments

Infrastructure exists in a variety of locations: from traditional branch offices and datacenters to edge locations like a factory floor, or in a cloud provider's infrastructure as a service offering. Those servers and clusters may be running Windows Server, Linux, or Kubernetes, either as a physical server or a virtual machine. Managing these different systems across locations, operating systems, and form factors has historically been difficult and inconsistent.

Example

An insurance company has IT assets with different regulatory requirements. Some of their workloads are in Azure, some in corporate datacenters, and recently, different public clouds. Each system—and potentially each location and form factor—has its own way of operating. The more devices and locations that are added, the more difficult the sprawl of technologies is to keep under control. As the sprawl of technologies expands, people skills and processes struggle to keep up with the changes.

Solution

There are millions of resources from over 200 different kinds of services in Microsoft datacenters and around the world. Azure Arc is a bridge that extends the Azure platform so customers can build applications and services with the flexibility to run across datacenters, edge, and multicloud environments. Azure Arc provides a consistent development, operations, and security model for both new and existing applications. Azure Arc runs on a both new and existing hardware, virtualization and Kubernetes platforms, IoT devices, and integrated systems.

- Organization and inventory: Resource groups, tagging, search, and index. For example,

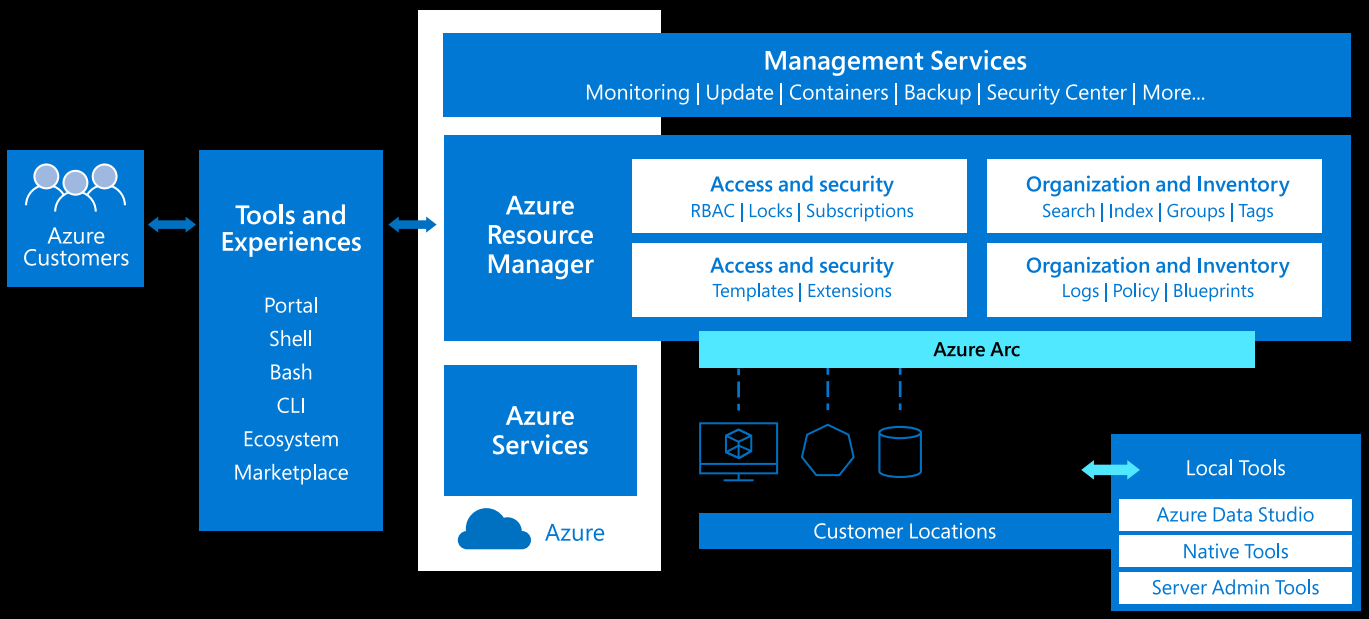
Azure Arc enabled servers can be tagged with "Cost Centers" and "Locations" and Azure can be used to search for all HR servers running in DC1.

- Governance and compliance: Logs, policy, blueprints. For example, Azure Policy can be used on Arc-enabled clusters and servers to provide central governance by defining guardrails.
- Access and security: Role-based access control, locks, and subscriptions. For example, an operations team can easily delegate control of a resource to a subset of administrators. Those administrators would be able to access resources and remediate issues as needed.
- Environments and automation: Azure templates and extensions. For example, a policy could be authored that required all resources in a specific resource group be managed by Microsoft Defender for Cloud via a virtual machine extension.

By linking resources and assets to the Azure Resource Manager, you can actively manage your company's environment, even if the resources reside in other cloud providers' infrastructure. The control plane is domain agnostic, so trust between domain controllers is not required and your teams can continue to use their local tools.

Azure Management

Single control plane for resources everywhere



Where to go next?

Azure Arc
Video: Organize all your servers outside of Azure with Azure Arc

02. At-scale Kubernetes application management

Containers have seen wide enterprise adoption and have become the standard for deploying business applications. Many new applications are written as microservices built on Kubernetes clusters. Even existing software is being modernized by rebuilding it as containers. But how can you manage these clusters and applications at scale without slowing down the innovation and developers in your company? To illustrate this further let's introduce a hypothetical use case.

Example

A retailer with hundreds of stores would like to move all in-store applications to containers running on Kubernetes clusters. The IT team is faced with the challenge of how to uniformly deploy, configure, and manage their containerized applications across multiple locations. The retailer needs to bootstrap a new store to fully run with a specific set of applications, while enforcing the necessary configuration and deployment practices. In addition, IT needs to be able to apply and monitor the state of applications and configuration in all stores, as well as their state of compliance.

Solution

Using Azure Arc, companies can deploy a new application to multiple locations easily, using a single policy to lock down network ports and other policies to handle common misconfiguration. As a service hosted on Azure Kubernetes Service (AKS) handles critical tasks like health monitoring and maintenance, mounting storage volumes, and tasking GPU-enabled nodes for parallel processing.

In addition, the application policies can be linked to specific GitHub repositories so that commits to the main branch of the application will deploy the software with all the correct policies in place. Using such continuous deployment technology, companies can easily

keep their applications up-to-date and compliant with their policies.

Finally, all the clusters at branch locations will be managed by Azure Arc and Azure Policy, giving the asset organization an inventory with a unified view in the Azure portal across all locations. The configuration and deployment can be done at scale, based on subscription, resource groups, and tags, using a GitOps-based model for deploying configuration as code.

Where to go next?

Azure Arc
Video: Managing K8 clusters outside of Azure with Azure Arc

03. Run cloud services anywhere

Companies are facing increasing data sprawl, with data not just collected on endpoint but also on-premises databases and cloud-based data storage buckets. The increasingly heterogenous data stores pose a significant problem for companies working with hybrid cloud infrastructure. A lack of a unified view of their data assets across all environments makes it far more difficult for companies to make use of their most valuable asset.

Example

An energy company aims for an efficient and fully automated operation utilizing artificial intelligence throughout their infrastructure. Customers operate various production sites and run utilities and services, from extraction to retail distribution. The company has massive data volume at the edge and needs real-time insights. The business needs to leverage existing OEM hardware and applications and automate IT systems to work at their massive scale. They want to deploy the latest innovations and apply consistent security and governance across their data infrastructure.

Solution

Azure Arc solves many of the problems that companies face with data distributed across hybrid cloud infrastructure. Azure data services enabled by Azure Arc deliver cloud elasticity to businesses' data infrastructure. The capability enables customers to scale their databases up or down dynamically in the same way as they do in Azure, based on the available capacity of their infrastructure. This capability can satisfy burst scenarios that have volatile needs, including scenarios that require ingesting and querying data in real time, at any scale, with sub-second response time.

The energy company can bring data services to whatever location needs access. A fully managed database service, such as Azure SQL Database, removes the burden of patching and upgrades for customers who have migrated their databases to Azure. An Azure Database managed instance creation allows you to pick where you want to deploy. You do not have to deploy into Azure; you can deploy to an environment on premises, or to another cloud provider.

With Azure Arc, for the first time, customers—such as the energy company—can access Azure's unique security capabilities from the Microsoft Defender for Cloud for their on-premises data workloads. They can protect databases with features like advanced threat protection and vulnerability assessment in the same ways they do in Azure.

Updates can be handled by upgrading a secondary system and failing over to the system after a sufficient testing period. These rolling upgrades allow a company to bring each database to a desired compatibility level.

Advanced data security gives you vulnerability assessments that allow you to find weaknesses in your security posture. Advanced Threat Protection can help you identify patterns that may represent specific threats.

Where to go next?

Azure Arc for data services, including SQL and PostgreSQL (Microsoft Ignite)

04. Regulatory, isolated, and disconnected workloads

Some organizations may require the ability to either run completely disconnected from public cloud or store sensitive data only outside of public cloud. These requirements can be the result of physical environments as well, as we will see in the use cases below.

Examples

Meeting isolation requirements

Critical industries, such as finance and manufacturing, may require that their systems and applications run in isolation. Government agencies often desire critical information to be stored and accessed only from within the four walls of the agency, absolutely without being connected to the internet. These requirements are often a security measure or a way to comply with regulatory requirements.

Disconnected computing at the edge

We often see hybrid cloud scenarios in which systems and processes are isolated from the internet because of intermittent connectivity. An easy-to-understand example involves cruise ships—satellite connectivity is both expensive and limited, so moving massive data can be cost-prohibitive and unreliable. If you want to be able to deliver first-class experience for your cruise guests anywhere, you want to have the same apps on board the cruise ship whether it is on land or at sea.

Data privacy and compliance

New regulations in data privacy are very common as many nations are in the process of updating their laws. This adds real business risk to companies operating globally as it can lead to a shutdown of services for a certain region and/or require investments to create a separate application to run on a separate system in a different location.

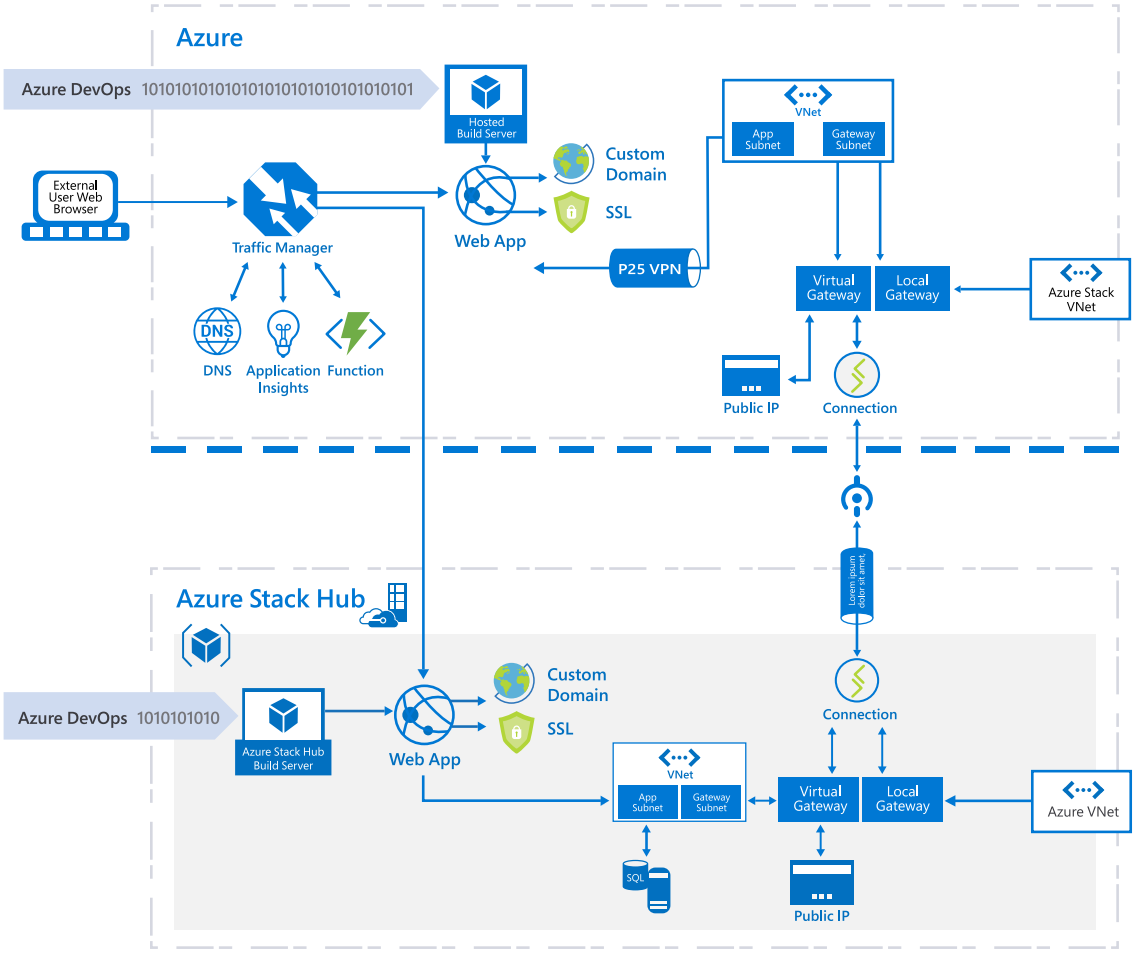
Solution

Azure Stack Hub is a fully optimized and purpose-built integrated system that runs Azure services no matter if you are connected to the internet or disconnected in a fully air-gapped way.

The technology allows companies to reuse code and run cloud-native applications consistently across their Azure and on-premises environments, while continuing to leverage IaaS and run virtualized workloads with optional cloud connectivity.

With Azure Stack Hub, companies can deploy applications to isolated or disconnected environments, whether a financial firm that needs to satisfy regulations or a transportation firm that has to adapt to unreliable connectivity. Data can be kept in the cloud or on-premises to satisfy data-residency requirements, and applications can be run from the cloud or on-premises to satisfy needs for disconnected workloads.

Azure Stack Hub



Ref: https://docs.microsoft.com/azure-stack/hybrid/pattern-cross-cloud-scale-onprem-data

Where to go next?

Azure disconnected deployment planning decisions for Azure Stack Hub integrated systems

Video: Azure Stack for hybrid compute and disconnected scenarios

Expanding the Azure Stack portfolio to run hybrid applications across the cloud, datacenters, and the edge

Azure hybrid patterns and solutions documentation

Azure Stack Hub overview

Azure Stack Hub Development Kit

05. Remote branch offices

Enterprises with branch offices are a challenge for hybrid infrastructure. Keeping identity services in synchronization, backing up data, and deploying applications become far more complicated when there are multiple locations that do not have dedicated IT staff. Any solution has to be able to quickly and easily deploy application and identity changes across remote offices, while allowing a central IT department to monitor for anomalies and violations.

Example

Businesses often need weeks or months to roll out application updates across multiple offices and infrastructures. A global bank with 300 offices worldwide takes a year to update every office across the globe. In addition, multiple locations make it difficult to avoid misconfiguration, such as open ports.

Rolling out new and updated applications to branch offices can pose problems for companies with tens or hundreds of such sites. Branches often need to run some apps on local servers in case of public internet availability as backup, or for latency issues.

In many remote office situations there is minimal IT staff available, which can make the deployment of applications to multiple sites challenging.

Solution

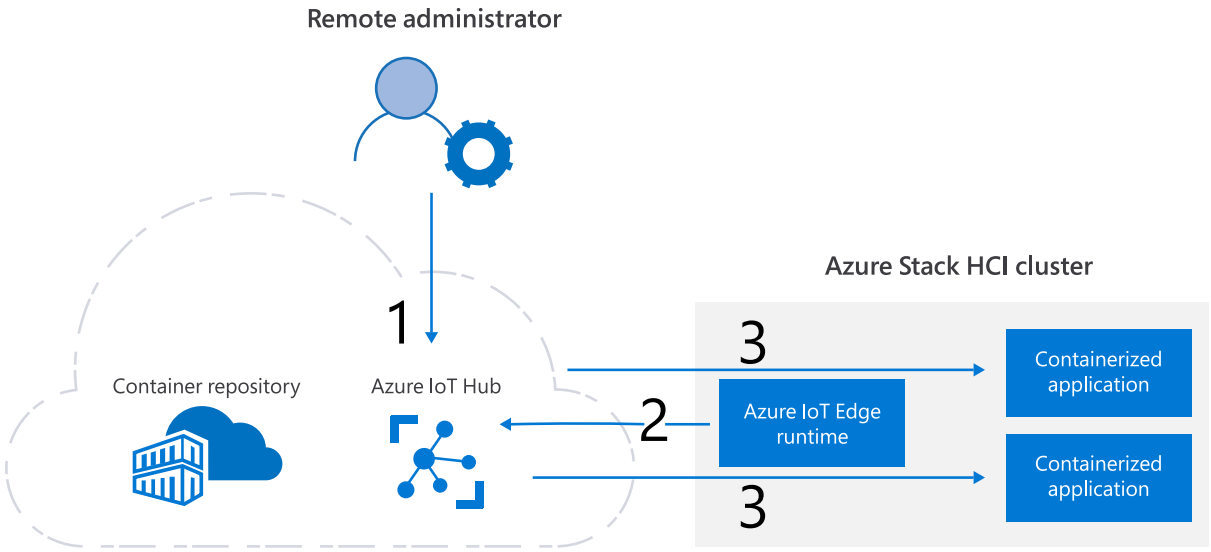
Azure Stack HCI provides hyperconverged infrastructure with industry-standard x86 servers with software-defined compute, storage, and networking. Easily start using the cloud for your hyperconverged infrastructure management with Azure integration built into the Windows Admin Center.

Meet the evolving IT demands of branch offices, retail stores, and field locations. Deploy your container-built

edge workloads and essential business applications in highly available virtual machines, and use Azure Monitor to get a global view of system health.

For offices with minimal IT staff, Azure IoT Edge can be used to ease the deployment of containerized applications to an Azure Stack HCI cluster with the help of an administrator working anywhere in the world. Azure IoT Edge is an engine that can be installed on a VM in Azure Stack HCI and that enables containers for the cluster. Azure IoT Edge also has Internet of Things (IoT) gateway functionality included, which enables the device on which it is installed to be managed remotely from the cloud via Azure IoT Hub.

Offices with minimal technical staff can use Azure IoT Edge to ease the deployment of containerized applications to an Azure Services HCI cluster with the help of an administrator working anywhere in the world.



Where to go next?

Branch office considerations
Two powerful ways to use Azure to back up your enterprise
Azure Stack HCI white papers

06. Deploy compute and AI on the edge

As the world digitizes, organizations generate more and more data at the edge. Data comes from many sources such as cameras, IoT sensors, and industrial automation. Organizations can benefit from analyzing, modifying, and filtering data where it is generated, and only transfer what they need to the cloud for further processing or storage.

Example

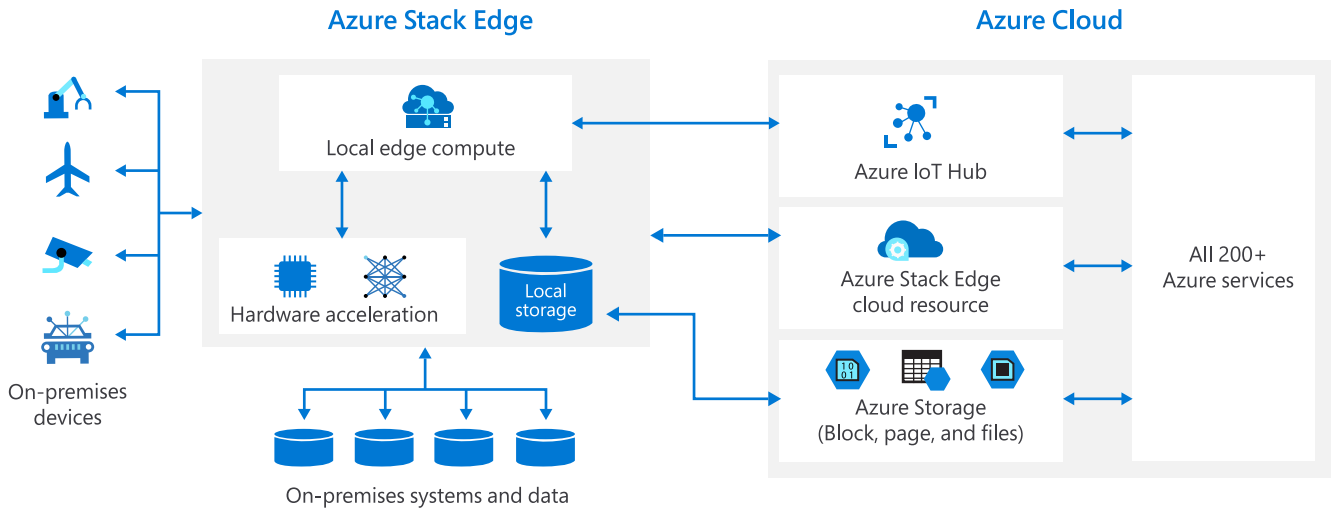
A retail floor has dozens of cameras in the store. Low or missing inventory is a high-impact business scenario that causes customer dissatisfaction, lost revenue, and can be time-consuming for staff.

Solution

Using Azure Stack Edge in the store to collect live feeds from in-store cameras of the shelves, and the AI capabilities of onboard FPGA or GPUs, you can run machine learning code that's trained on Azure and running locally on Azure Stack Edge to score scenarios and make decisions about inventory, customer needs, and shopping patterns.

With Azure Stack Edge you can speed up time to results by processing data close to its source, without waiting for a round trip to the cloud. Analyze, transform, and filter data at the edge, sending only the data you need to the cloud for further processing or storage. Use the cloud to push containerized applications to Azure Stack Edge devices at all your locations.

How Azure Stack Edge enables edge computing and machine learning



Azure Stack Edge combines IoT Edge and accelerated ML inferencing in a cloud-managed edge computing appliance delivered as an Azure service

Where to go next?

Azure Stack Edge

Azure IoT Edge

The future of computing: intelligent cloud and intelligent edge

07. Migrate and manage applications across VMware environments

For a successful hybrid approach, organizations must have a consistent solution that unifies management of machines across physical and virtual environments—and scales quickly. Customers running VMware workloads can now seamlessly run, manage, and secure applications across VMware environments and Microsoft Azure with a common operating framework.

Example

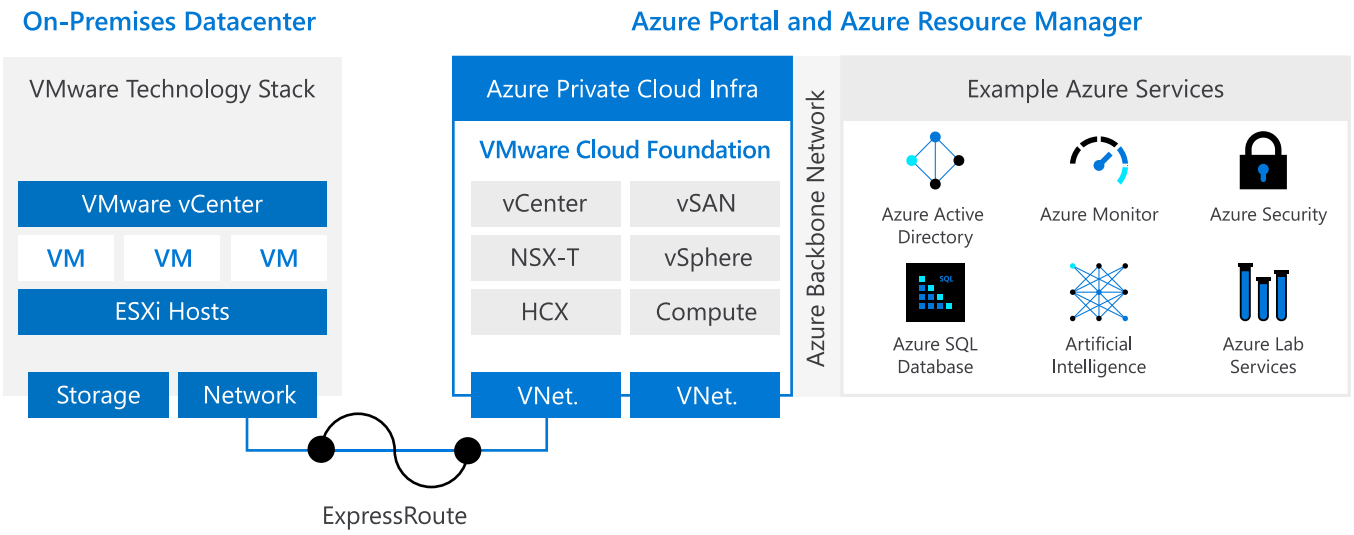
A global health crisis causes rapid, massive strain on a hospital's operations, which are running on VMware. The hospital needs to scale their IT infrastructure as staffing increases test their HR, patient management, and EMR systems—all while remaining HIPAA-compliant and managing recent budget cuts. The requisition process, approvals, and logistics to roll out new technical infrastructure can take 4–6 months or more. So, to maximize time and resources as they expand and contract their cloud-based systems, the hospital will need to be able to use existing IT skills, processes, and experience in VMware for efficient deployment and ramp up.

Solution

Azure VMware Solution delivers the infrastructure elasticity to expand and contract without capital expenditure, all while maintaining continuity for staff and processes. Among other leading industry standard certifications, the solution is also fully HIPAA-compliant, lowering barriers for adoption and accelerating speed to the cloud.

Using Azure VMware Solution, the hospital can scale quickly to meet the unexpected demand on their IT systems. By extending the hospital's current VMware environment into Azure with Azure VMware Solution, the hospital minimizes disruption with a consistent management experience across

on-premises environments and Azure. They can maximize previous investments, taking advantage of the tools and skills they're already using. Plus, the hospital can build on this foundation to seamlessly modernize over time, using Azure for unified management of resources.



Where to go next?

Azure VMware Solution
Azure VMware Solution documentation
AVS Demo

04 /

Conclusion

As companies push to digitally transform their businesses, hybrid computing is playing a significant role.

Businesses that successfully migrate operations to the cloud and augment operations with on-premises technology will have greater control over applications and will see a reduction in deployment and management costs. The result is more flexible operations, a standardized set of shared tools and services, and lower costs for the business.

Businesses rely on a hybrid cloud approach for many different reasons. And as more business operations and applications expand to include edge devices and multiple clouds, organizations are faced with the reality of having hundreds to thousands of applications, running across a wide range of infrastructure, spanning on-premises datacenters, multicloud, and the edge.

That's why your hybrid cloud strategy must evolve to enable innovation anywhere, while providing a seamless development, deployment, and ongoing management experience across all distributed locations. Companies focused on hybrid cloud infrastructure should:

- **Build on their terms**

  Deliver application innovation with ultimate flexibility—build any application and deploy consistently to wherever it's needed across on-premises, multicloud, and edge.

- **Operate seamlessly**

  Operate your on-premises, multi-cloud, and edge environments like a single environment and seamlessly manage all your resources with a single control plane in Azure.

- **Secure their enterprise**

  Implement integrated Azure security across your organization with confidence—get comprehensive security management, gain AI-enabled threat protection, and enable single sign-on access.

Take the next step

If you have any questions, reach out to your Microsoft account team, or use the contact link below.

Try Azure for free

Contact us