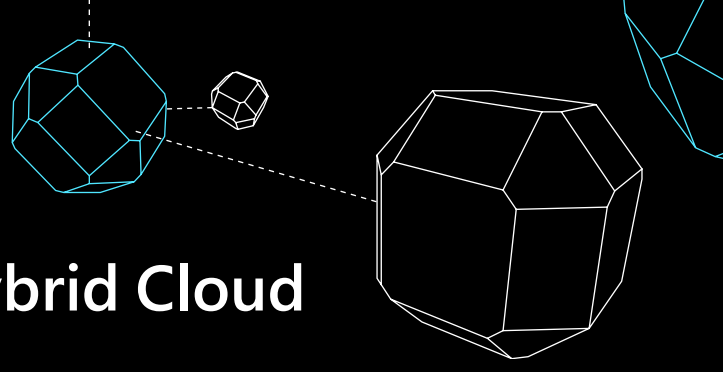
Microsoft Azure

Three Fundamentals of Hybrid Cloud



Hybrid cloud has become a strategic asset for many companies as they take steps toward digital transformation. A hybrid cloud approach—one that can span on-premises, multiple clouds, and even edge environments—can deliver significant business value, as long as it's supported by a solid foundation.

What does a solid foundation look like? While every company's structure will vary, all hybrid solutions depend on strength in three fundamental components: networking, identity and access management, and security.

As you develop your strategy for deploying hybrid solutions, make sure that these three fundamentals are stable and scalable to support your hybrid cloud environment. Start with the high-level strategies below—and download the Cloud Anywhere: Azure for Hybrid, Multicloud, and Edge Environments e-book for more comprehensive guidance and common use cases.

Fundamental 1: Networking

Networking is the primary component of every hybrid cloud environment. There are a multitude of ways to create a cost-effective network that is reliable and secure. Because networks depend on several areas of functionality, it's important to focus on these key areas:

Connect and Extend

Businesses need to utilize VPN, ExpressRoute, and Virtual WAN technologies to connect existing resources and extend their own networks.

Protect

Think of every connection as a potential entry point to the network. Companies should safeguard these points with the best available tools such as DDoS protection, firewalls, and web application firewalls.

Deliver

Great customer experiences require a network specifically built for application delivery, such as Azure Front Door and application-gateway technologies.

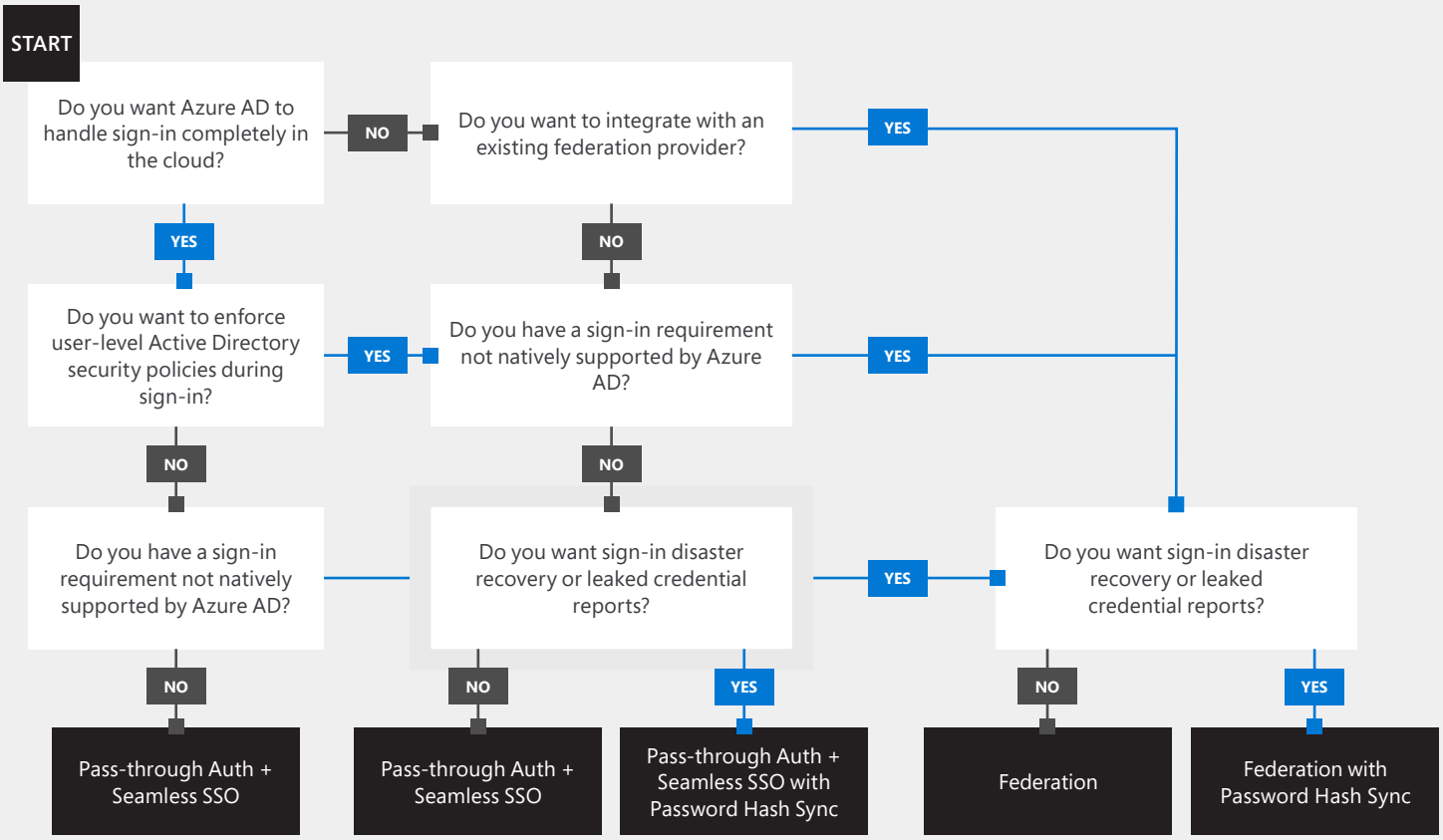
Learn more about your hybrid cloud networking options here >.

Fundamental 2: Identity and access management

The approach to identity is a core decision impacting the overall cloud strategy. Organizations may be using a mixture of on-premises and cloud applications, with workers requiring access across environments in a variety of locations. Integrated management of this access is crucial. Identity is the new control plane; giving businesses control of users and devices, and providing a variety of connected endpoints including applications, sensors, and bots.

Use the decision tree to see a variety of factors and the effects to be considered for identity and access management.

Decision Tree



Learn more about Azure Active Directory > and Hybrid Identity >

Fundamental 3: Security

Approaches to security evolve as operations and applications expand across on-premises, multicloud and edge infrastructure. Azure offers two key services that help simplify security management across hybrid cloud environments:

Azure Security Center

Azure Security Center - Manage 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. Learn more about Azure Security Center >

Azure Sentinel

Provides IT teams 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. This allows for scalable, cloud-native, security information and event management (SIEM) as well as a security orchestration automated response (SOAR) solution. Learn more about Azure Sentinel >

To explore the above topics and read about common hybrid use cases, download the Cloud Anywhere: Azure for Hybrid, Multicloud, and Edge Environments e-book.