Microsoft Azure

Active Directory Overview

Gold
Microsoft Partner

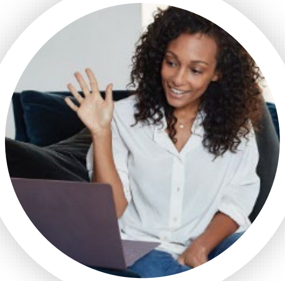
eTrepid®

Empowering business to compute with clarity®

Identity challenges for today's organizations

Explosion of apps, on and off the corporate network, needing secure access

Shift to a remote workforce requiring seamless, productive experiences



Evolving compliance regulations with data privacy and security implications

Demands for increased productivity, security, and IT modernization

Gold
Microsoft Partner

eTrepid®
Empowering business to compute with clarity®

Azure Active Directory—the world’s largest cloud identity service

Thousands of organizations, millions of active users, billions of daily requests

200K +

Azure AD
Premium organizations

345M +

Azure AD
Monthly active users

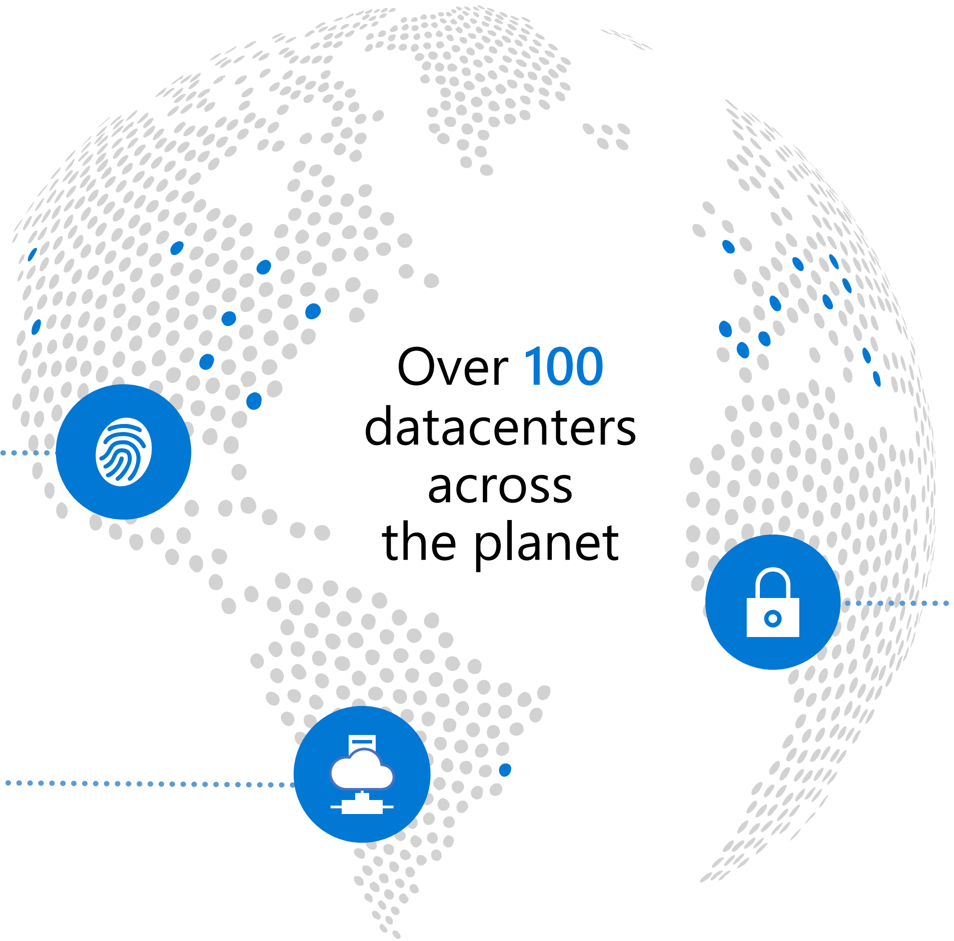
30B +

Azure AD
Daily authentication requests

Gold
Microsoft Partner
eTrepid®
Empowering business to compute with clarity®

Engineered for availability and security

Cloud-native, hyper-scale, multi-tenant architecture



Each **physical datacenter** protected with world-class, multi-layered protection, and engineered for maximum availability

Over **100** datacenters across the planet

Secured with cutting-edge **operational security**

- Restricted access
- 24x7 monitoring
- Global security experts

Global cloud infrastructure with secure hardware and data segregation

Gold
Microsoft Partner
eTrepid®
Empowering business to compute with clarity®

Microsoft Azure Active Directory

Secure access for a connected world

Secure adaptive access

Seamless user experiences

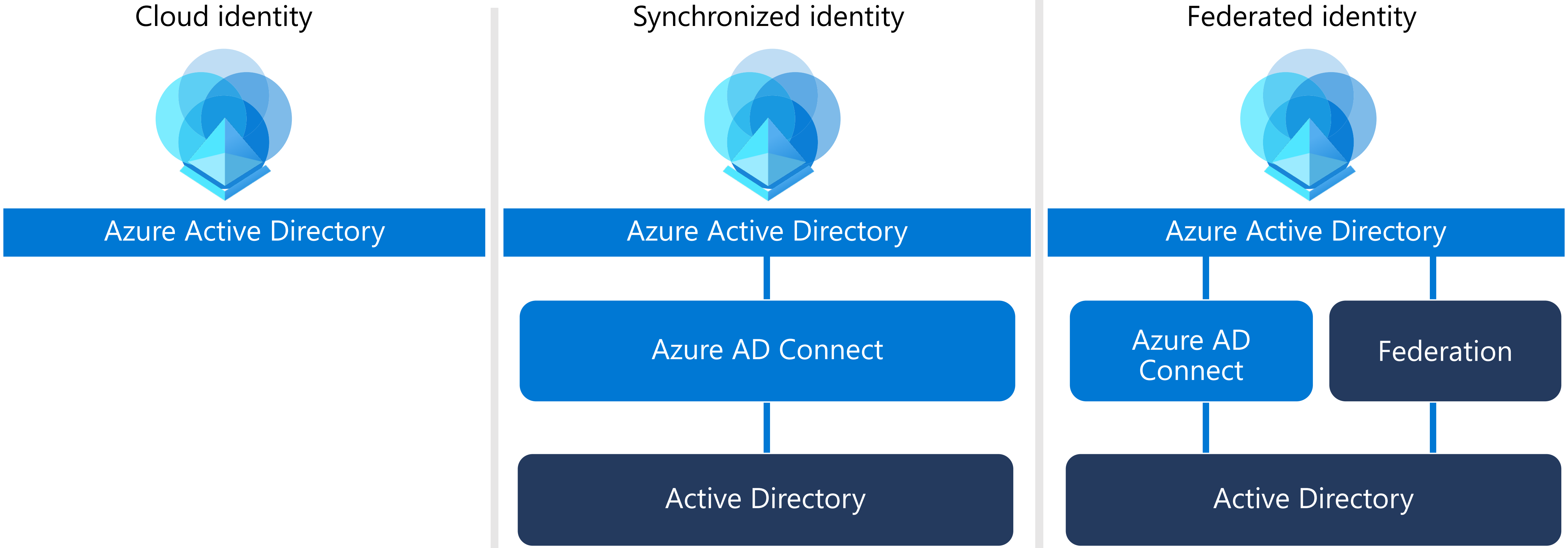
Unified identity management

Simplified access governance

Gold
Microsoft Partner

eTrepid®
Empowering business to compute with clarity®

Azure Active Directory integration scenarios



Cloud identity

Azure Active Directory

Synchronized identity

Azure Active Directory

Azure AD Connect

Active Directory

Federated identity

Azure Active Directory

Azure AD Connect

Federation

Active Directory

Independent cloud identities

Single identity, enabling a same or single sign-on experience with Password Hash Sync or Pass-through Authentication

Single federated identity, enabling single-sign-on experience and on-premises multi-factor authentication options

Gold
Microsoft Partner
eTrepid®
Empowering business to compute with clarity®

Common misconceptions

Misconception	Reality
Azure AD joined devices have no access to on-premises resources.	Azure AD joined devices can access on-premises resources if Azure AD Connect has been deployed to synchronize your on-premises identity information to the cloud. Or, you can connect your on-premises resource to Azure AD using Azure Secure Hybrid Access through Microsoft Application Proxy or a supported 3rd party application controller.
Windows Hello for Business requires Azure AD join.	For cloud deployments, you can use Windows Hello for Business with Azure Active Directory joined, Hybrid Azure Active Directory joined, or Azure Active Directory registered devices. Windows Hello for Business also works for domain joined devices.
UPNs Do Not Matter for Hybrid Join.	Hybrid Azure AD join works with both, managed and federated environments depending on whether the UPN is routable or non-routable.
Apps and resources that depend on Active Directory machine authentication will work with Azure AD joined devices.	Apps and resources that depend on Active Directory machine authentication don't work because Azure AD joined devices don't have a computer object in AD.

Gold
Microsoft Partner

eTrepid®
Empowering business to compute with clarity®