Edgile CIAM on Azure Solution

Secure and cost-effective Identity as a Service for consumers and business partners

Microsoft Co-Sell Solution

edgile

a **wipro** company

Current CIAM Approaches – has gaps

- **Inconsistent Brand Marketing -** Clients having multiple log-in experiences. Branding is different and often not current. Modernizing is slow and costly and can put the firm at a competitive disadvantage

- **Disjointed Security -** Separate identity stores, data isolation and identity duplication. All vectors for attack. Difficult and expensive to apply modern security like adaptive authentication

- **Legacy Cost Structure -** Maintaining IAM databases for external users is expensive let alone CRMs for access issues. Modern advanced security like User Entity Behavior Analytics is expensive and often hard to justify until too late

Who Leads?

- Digital Officer?
- IT Security?
- Finance?

CIAM has cross organizational impact

Modernizing with Azure AD enables cloud security, streamlined user experience and lower costs

Edgile CIAM on Azure Solution Addresses Gaps

Best in class user experience

In digital commerce, being easiest to use and intuitive can make all the difference in successful or unsuccessful digital offering

Fully outsourced model

A true *Identity as a Service* model dramatically reduces cost by outsourcing the system requirements, monitoring and upkeep effort. Frees engineers for more value-added work
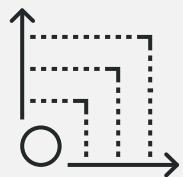
Security and Scaling

The Service is the Platform engineered in the cloud operating at 99.99% uptime Secured by 3,700 security engineers, $20b committed over the next 5 years

Accelerators, Insight and Agility

Edgile has built many CIAM systems on Azure with rapid feature release capability. Our 24/7/365 global managed service provides monitoring and data analytics

3

Engage with customers with Azure AD B2C

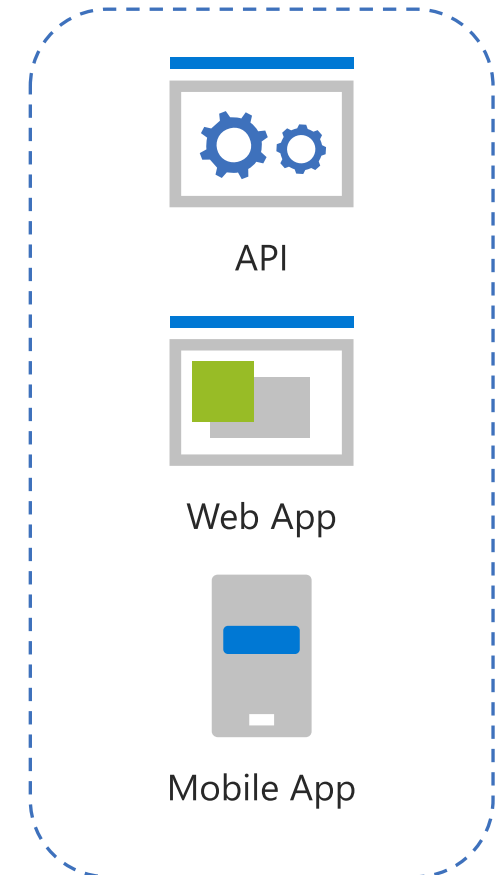Connect users with corporate or personal Azure AD identities, or any OpenID Connect provider

Business

Azure AD B2C

API

Web App

Mobile App

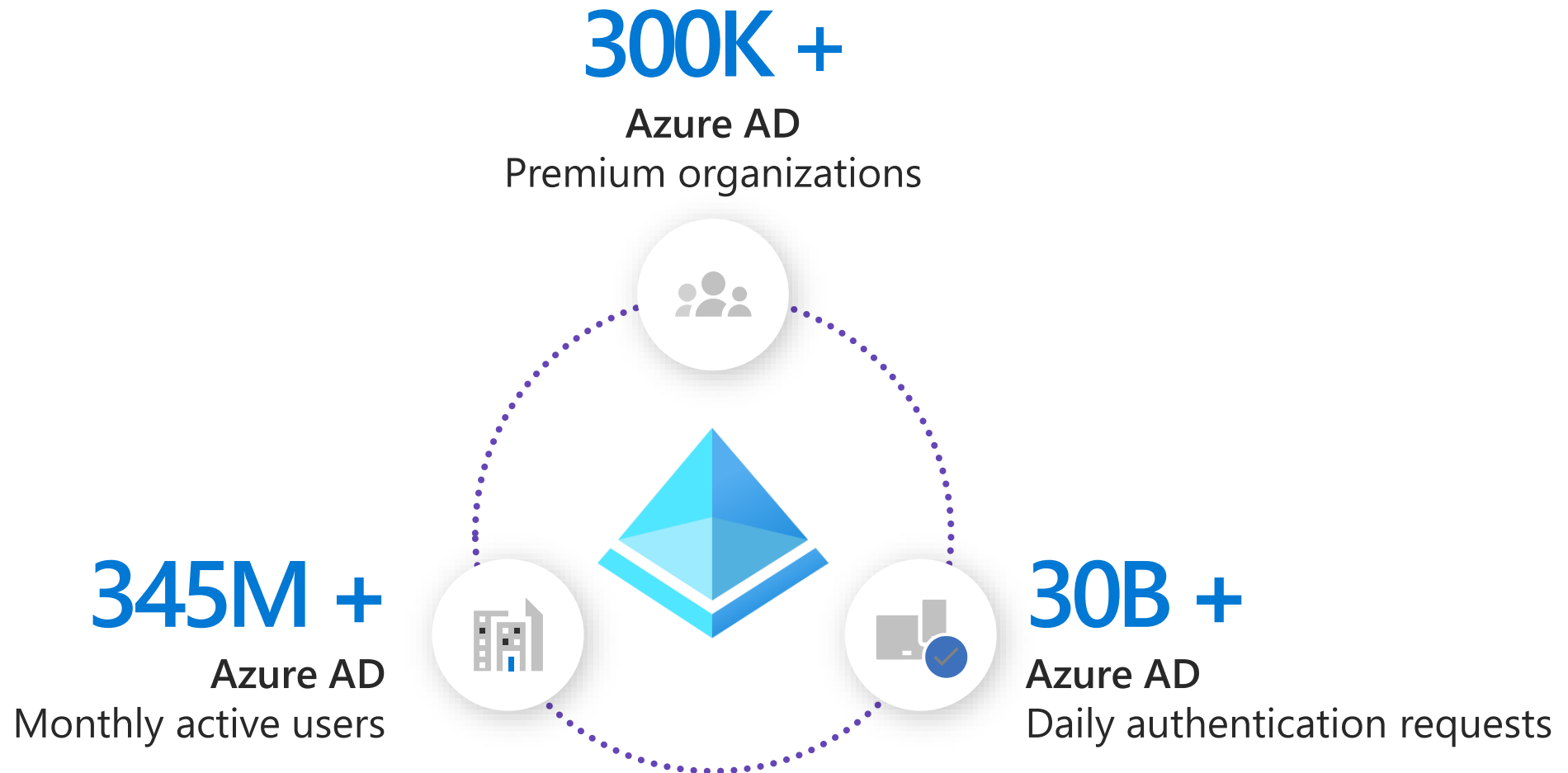Add external users with non-traditional IDs, including email one-time passcode

Add external users with MSA, social IDs, or other SAML providers

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

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

300K +
Azure AD
Premium organizations

345M +
Azure AD
Monthly active users

30B +
Azure AD
Daily authentication requests

Engineered for availability and security

Azure is a cloud-native, hyper-scale, multi-tenant architecture
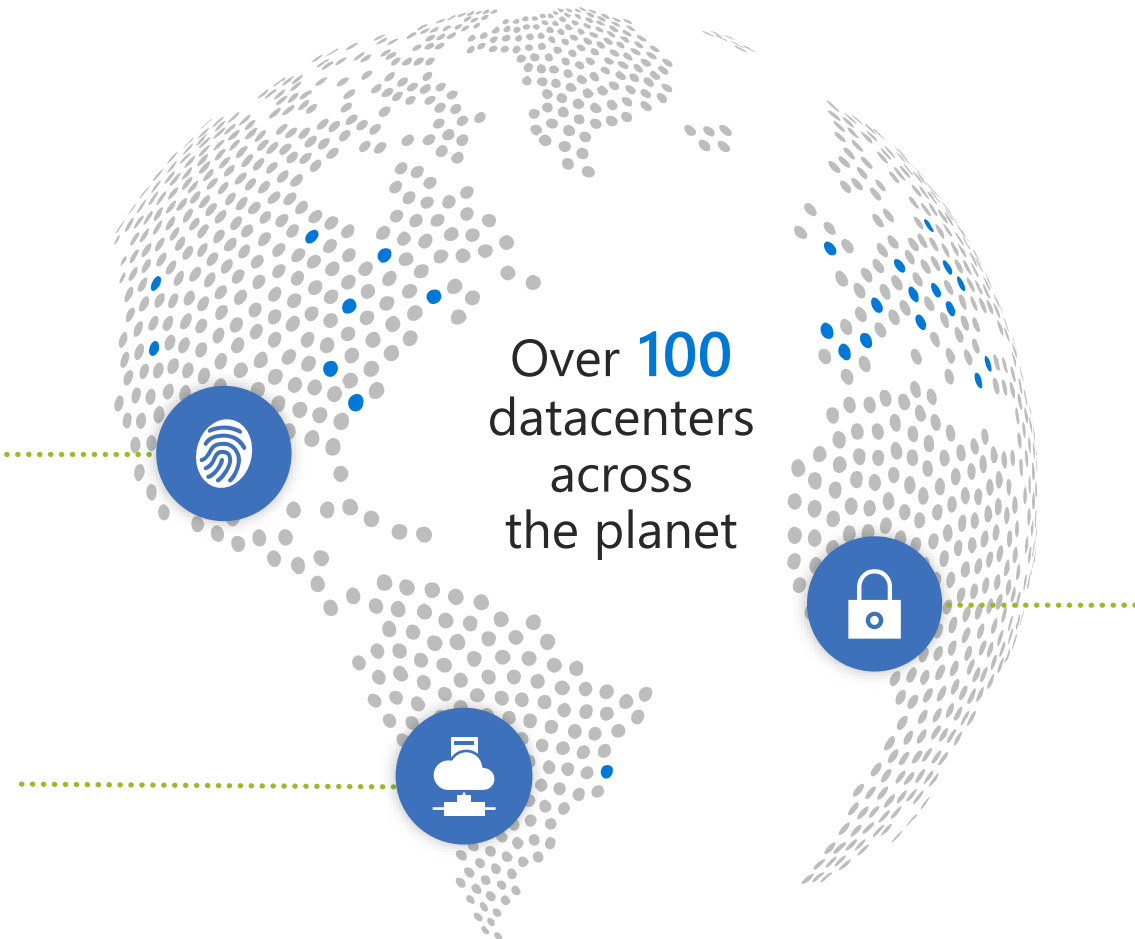
Each **physical datacenter** protected with world-class, multi-layered protection, and engineered for maximum availability

Global cloud infrastructure with secure hardware and data segregation

Over **100** datacenters across the planet

Secured with cutting-edge **operational security**

· Restricted access

· 24x7 monitoring

· Global security experts

Azure is the only cloud platform built by a security vendor

Microsoft earns $10B in security business revenue

More than **400,000 customers** and **90 of the Fortune 100** trust Microsoft SCI solutions.

Microsoft employs **3,700 security experts** and spends more than **$1B annually on security.**
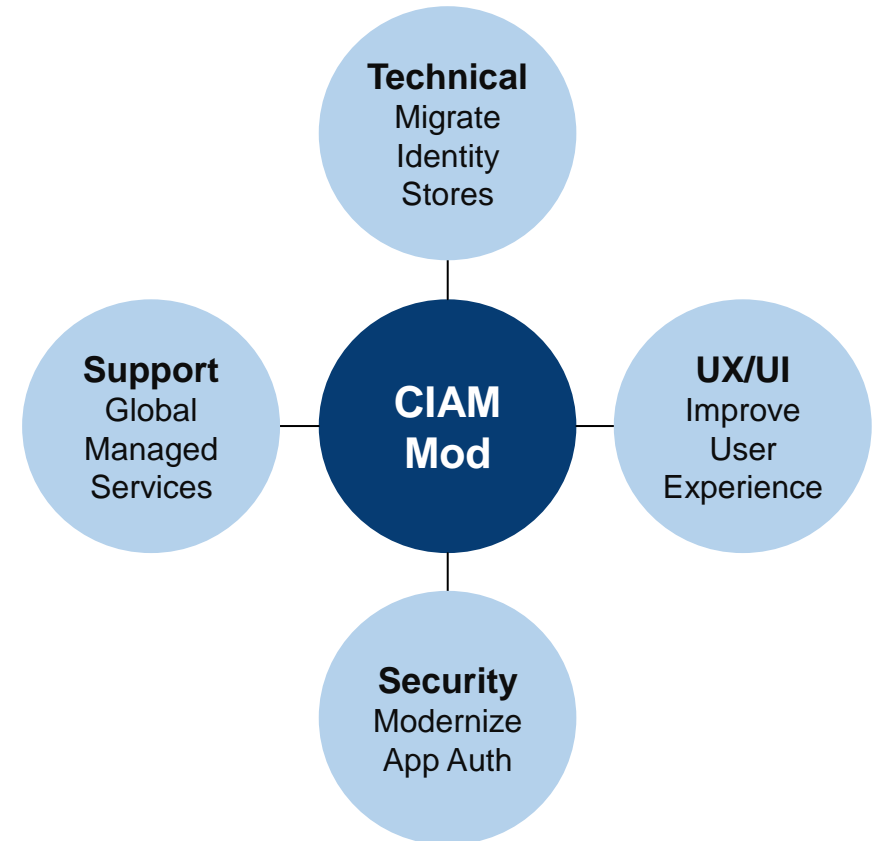
In 2020, **6 billion malware threats** were blocked by Microsoft Defender.

Microsoft takes in over **8 trillion signals** every 24 hours.

Edgile External Identities Group

- Staffed by Edgile's top identity, security, compliance and UX/UI experts

- A library of pre-configured custom workflows for sign-up, sign-in, 3rd party validation and more

- Deep experience in all sectors including retail, manufacturing and healthcare

- A senior UX/UI/web development team to modernize and streamline branding and user journeys

- 24/7/365 global Managed Services organization with business models ranging from monitoring and alerting to a complete turn-key solution

Technical
Migrate Identity Stores

Support
Global Managed Services

CIAM Mod

UX/UI
Improve User Experience

Security
Modernize App Auth

Complete CIAM transformation service from system and UX design, to in place transformation to fully managed solution
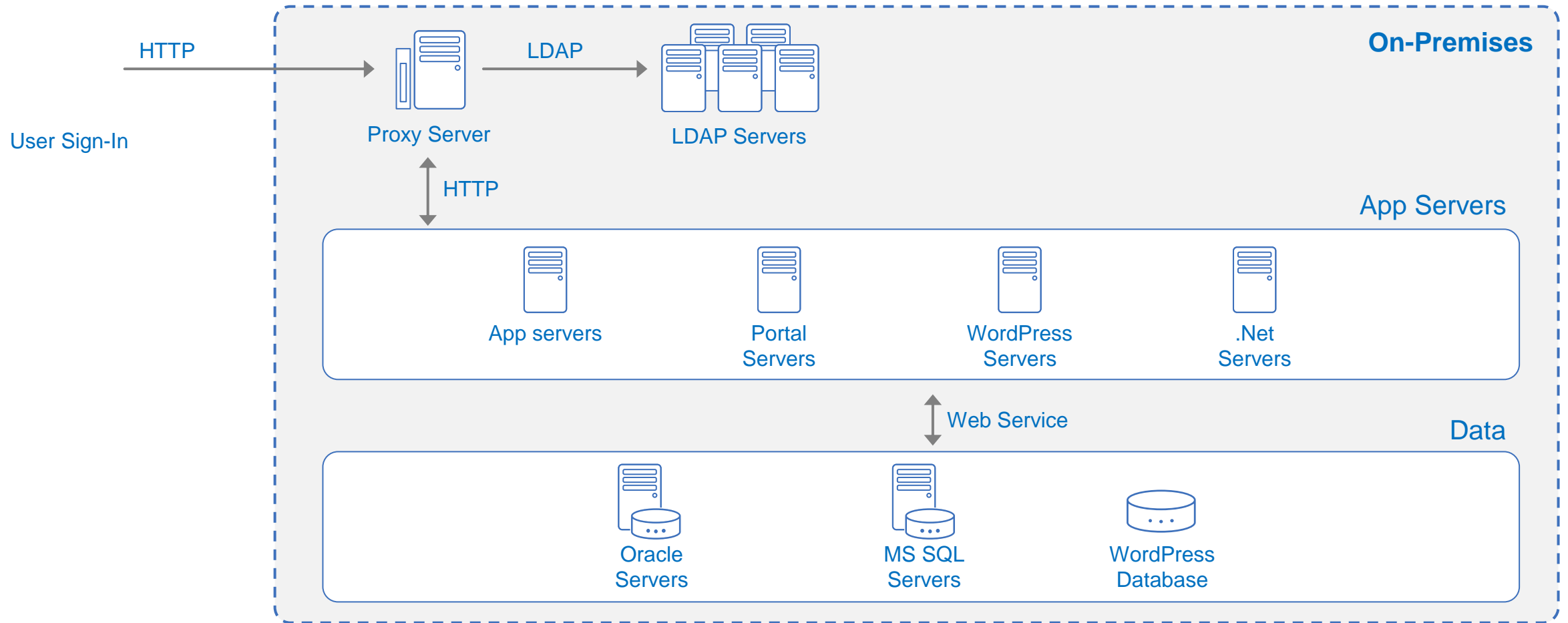
Cloud Security for External Identities

Traditional Approach

- All about capturing and holding identity and credentials

- Management burden, lost credentials, increased support and risk

- Various applications develop repositories build up over time

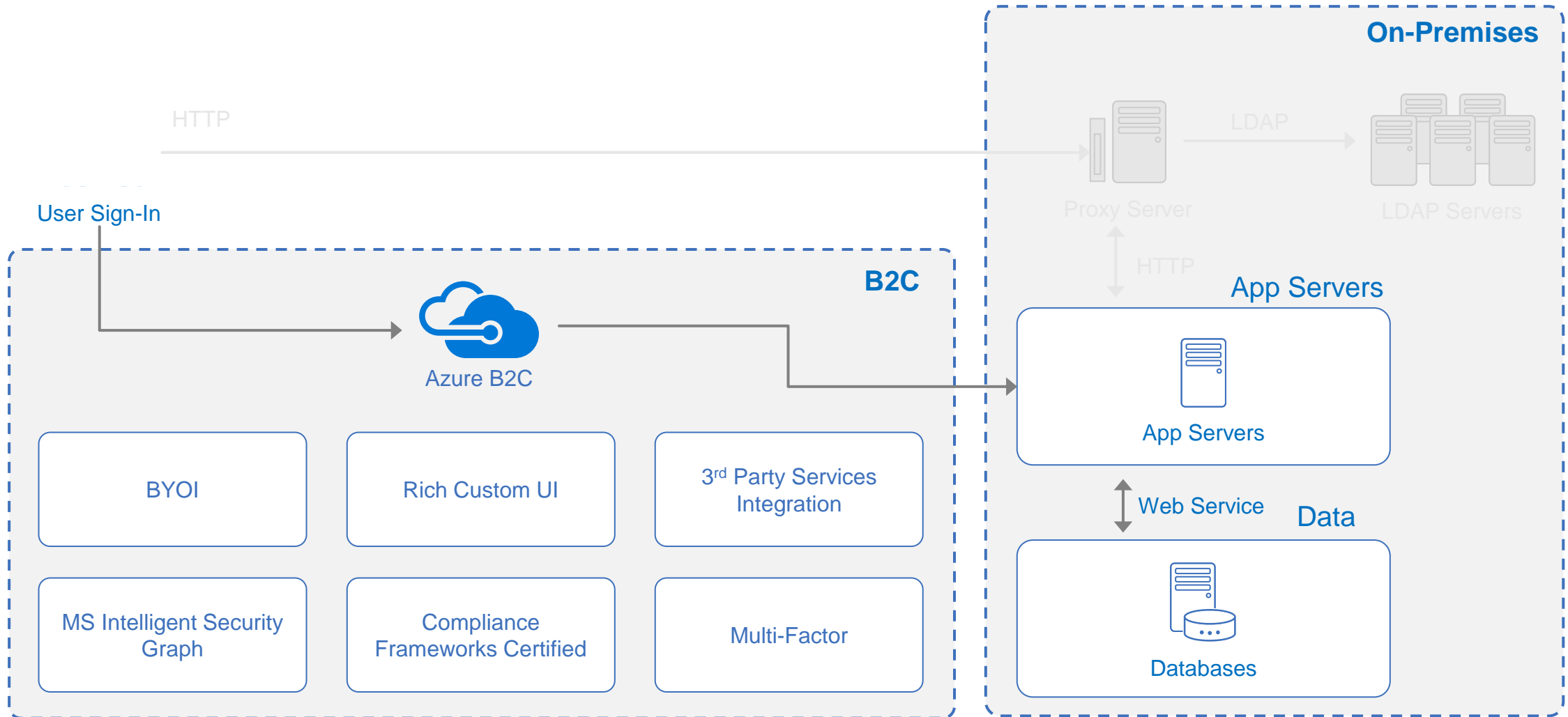- Very slow to adapt, enable new services

New Approach

- Cloud powered Microsoft Azure landscape

- Managed service = lower cost

- Flexible and customizable for different purposes

- Security and marketing working together

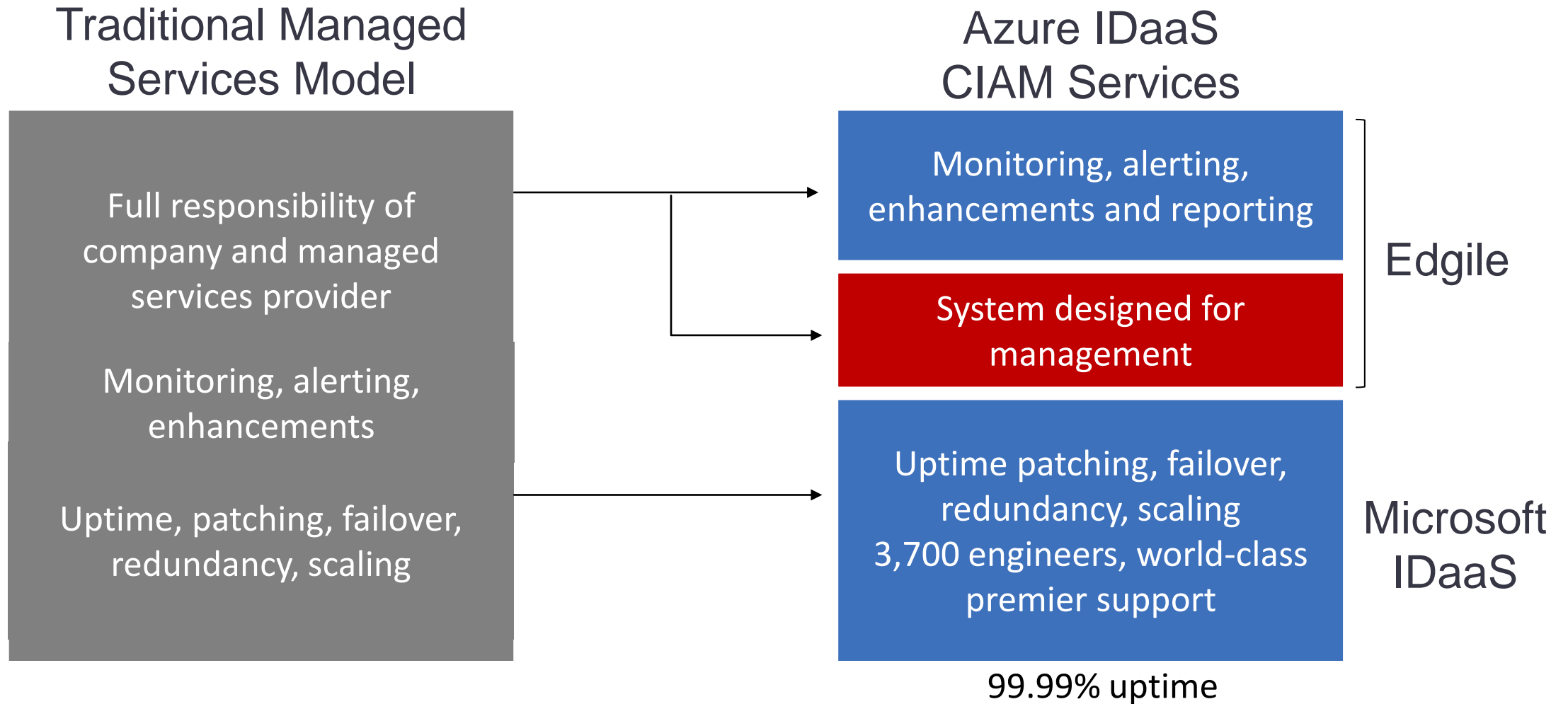# Traditional Approach

User Sign-In

HTTP

On-Premises

Proxy Server

LDAP

LDAP Servers

HTTP

App Servers

App servers

Portal
Servers

WordPress
Servers

.Net
Servers

Web Service

Data

Oracle
Servers

MS SQL
Servers

WordPress
Database

Modern Approach using Microsoft Azure AD B2C

On-Premises

HTTP — LDAP

Proxy Server   LDAP Servers

HTTP

User Sign-In

B2C

App Servers

Azure B2C

App Servers

BYOI	Rich Custom UI	3rd Party Services Integration
MS Intelligent Security Graph	Compliance Frameworks Certified	Multi-Factor

Web Service   **Data**

Databases

Managed Services Leverages Microsoft Global Infrastcture

Traditional Managed Services Model

Full responsibility of company and managed services provider

Monitoring, alerting, enhancements

Uptime, patching, failover, redundancy, scaling

Azure IDaaS CIAM Services

Monitoring, alerting, enhancements and reporting

System designed for management

Edgile

Uptime patching, failover, redundancy, scaling
3,700 engineers, world-class premier support

Microsoft IDaaS

99.99% uptime

CIAM Managed Services Support Model

Edgile Service Delivery Centers

North America

India
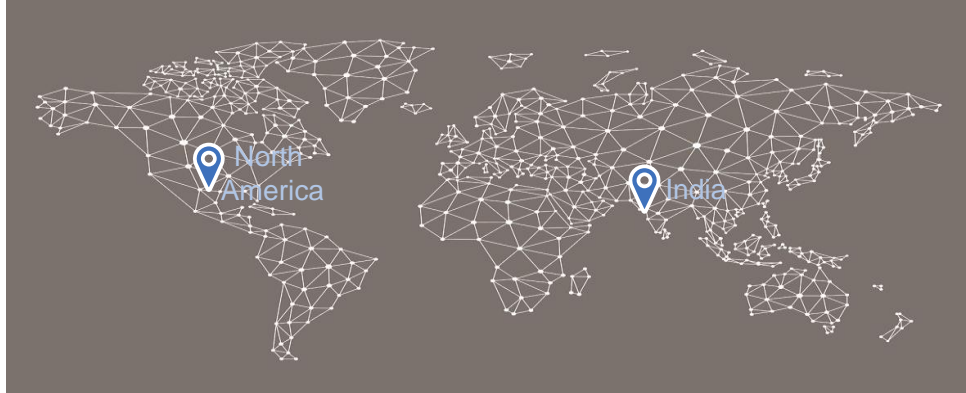
Service Includes

24/7/365 Monitoring and alerting

Maintain automated test harness and include updated test cases

Validate Microsoft updates to Azure AD External Identities system

Managed Services Support Model

24 x 7 live support

Service Levels for CIAM Service Operations

Severity	Definition	Response Time	Target Resolution Time
P1 - High	Complete failure or degradation of the CIAM platform making its services unusable	1 hour	4 hours
P2 - Medium	Partial failure or running at reduced performance impacting the service for all or subset of users	1 hour	8 hours
P3 - Low	Partial failure or reduced performance resulting in minimal or no impact for all or subset of users	2 hours	5 business days or more

CIAM on Azure – Quick Start Program

Analysis and Planning

- Discover current state identity architecture and UI/UX needs
- Explore desired future state
- Understand implementation, user base, app roles and authentication protocols

Sample B2C Application

- Configure AAD B2C directory
- Register sample browser application
- Demonstrate user experience with out-of-the-box Microsoft offerings

DevOps Production

- Ready production tenant
- Configure Azure DevOps to promote configuration as code into the production tenant

Future State Roadmap

- Create future state external identity conceptual architecture
- Plan for legacy IdP decommissioning
- Discuss application integration patterns

- 2-day Future State Planning Workshop:
  - External identities migration methodology
 - Patterns required to migrate key application to IAM platform

6 weeks

Case Study:
External Identity Transformation - MVP Healthcare

Problem Statement

Using legacy Identity Provider solutions for external identity management creates high licensing and support costs, with no interoperability between your current solution and a modern cloud approach.
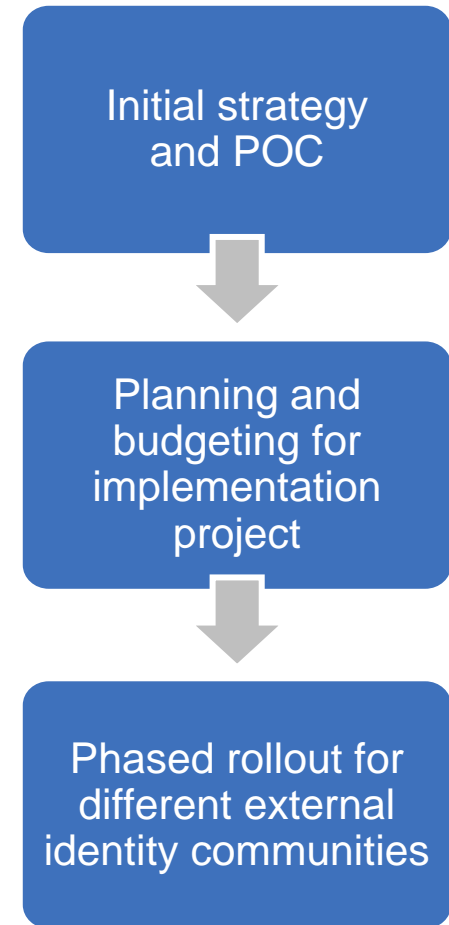
This typically leads to a less secure credentials management process, lacking in multi-factor authentication support.

Member

Provider

Broker

Employer
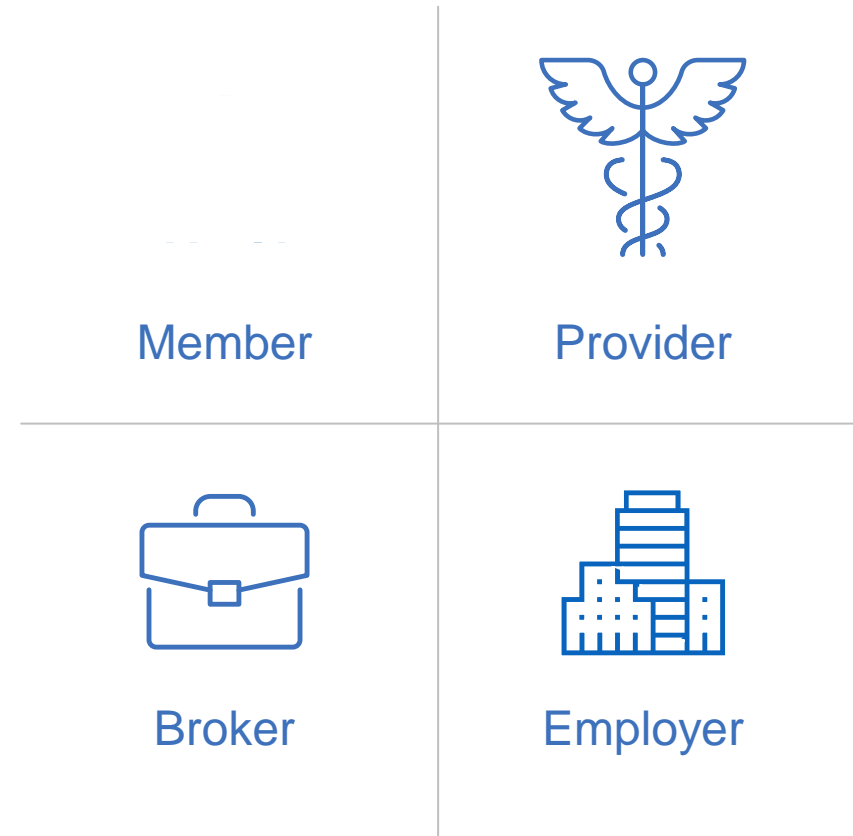
Approach and Solution

- Use Microsoft Azure AD B2C as the Identity Provider (IdP) for external identity management

- Streamline UI/UX for different user access portals providing common branding and seamless user experience

- Implement modern cloud identity solutions that ties into the existing MVP Healthcare technology stack

- Enhance credential management process by creating a cryptographically secure invite activation process

- Adopt Microsoft Azure Multi-factor Authentication for advanced use case scenarios

Initial strategy and POC

↓

Planning and budgeting for implementation project

↓

Phased rollout for different external identity communities

Results

- 700K+ accounts migrated from legacy solution to MS Azure AD B2C

- License cost savings with displacing legacy solution

- Bring-Your-Own-Identity model through social partners that eases adoption and saves on support hours

- World-class, streamlined UI to enhanced user experience and empower the brand

- Established patterns for app modernization and integration with standard cloud environment

- Adopted industry standard MFA and credential management processes
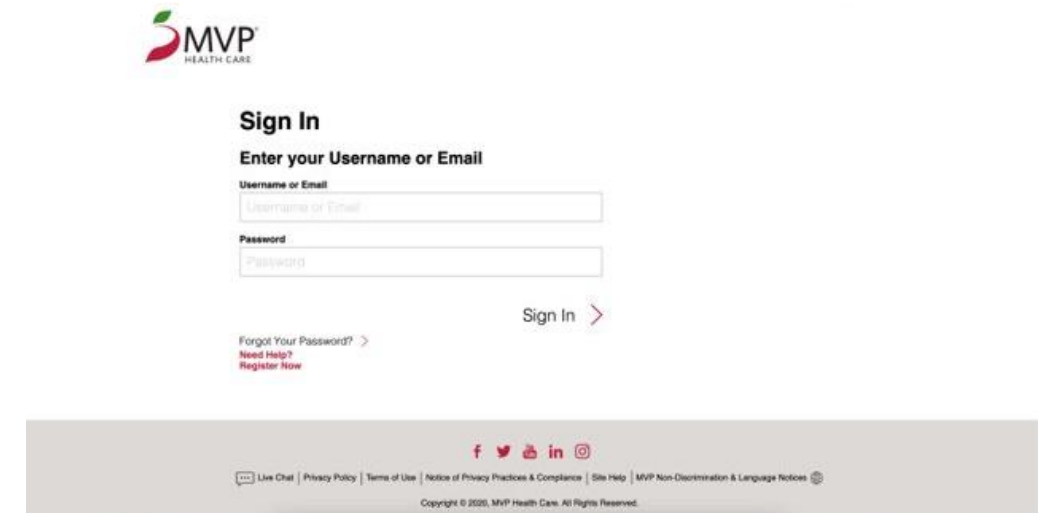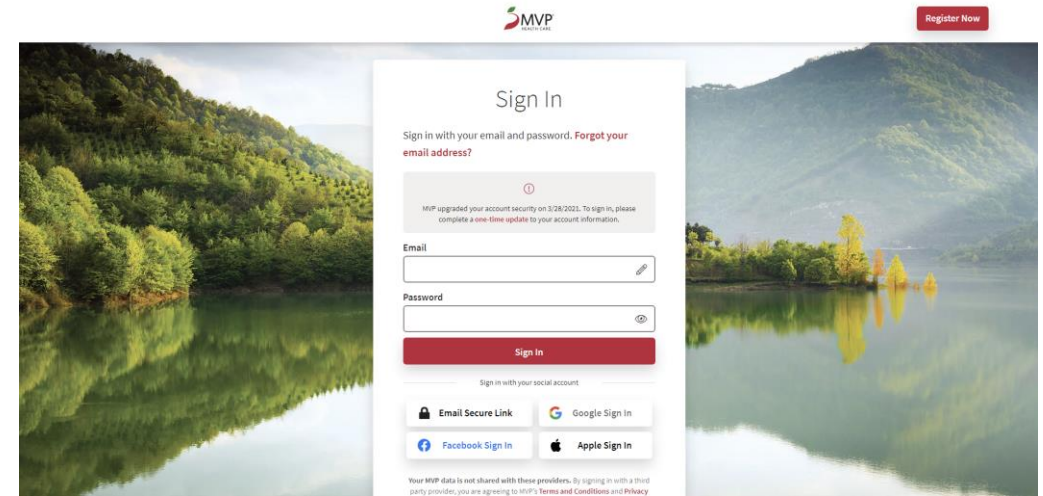
For more information visit www.edgile.com
or email info@edgile.com
subject: CIAM on Azure