

**HCL**

**HCL Technologies**  
Microsoft Business Unit (MBU)

**HCL Unified Digital Access**

HCL's Unified Digital Access solution protects enterprise users and apps from cybersecurity attacks by aiding to right enterprise security posture with easy access to Apps and services. Our services help manage and govern identities effectively and watch-over sessions to have an enhanced security stance. HCL solution provides quicker provisioning/ de-provisioning of users thereby optimizing user & app onboarding processes, helps control access to accounts with elevated privileges and helps manage both internal and external user access to corporate/ non-corporate apps effectively.

## CHALLENGES

- Increased complexities in managing user identities and their access to corporate assets with increased digitalization
- Delays in provisioning/ deprovisioning lead to reduced productivity and cluttered identity lifecycle management
- Unmonitored sign-in by non-interactive service accounts
- Managing password resets burdens internal IT teams

## IDEAL SOLUTION

- Strong security foundation build with MFA, SSO, & SSPR (Self service password reset)
- Automated provisioning/ de-provisioning to internal & SaaS apps
- Privileged user lifecycle management along with audits
- Identity Analytics services

## DESIRED OUTCOMES

- Simplified Access governance for multi-cloud/ hybrid cloud, especially during Cloud migration with automated app onboarding
- Enforce strong access policies across all enterprise apps
- Reduction in identity attack surface

# HCL Technologies

## Unified Digital Access

HCL's Unified Digital Access services is an amalgamation of Identity & Access Management services based on Azure IAM which provides a comprehensive security across user identities, secure app onboarding, user provisioning/ de-provisioning, privileged access governance etc., all in an automated form.

The key features of our services are:

- Build strong security foundation through MFA, SSO & SSPR
- Advanced B2E services to manage enterprise users, devices and enable synchronization
- Manage B2C services by addressing enterprise CIAM demands
- Effective management of guest access, sending invites, and sharing resources to partners, service providers and vendors.
- Enforce least privilege principles
- AI/ ML based Identity analytics services with automated threat detection

### **STRONG ACCESS MANAGEMENT**

Strong & simplified Access Governance across enterprise & non-enterprise user access to applications thereby reducing identity attack surface

### **AUTOMATED APPROACH**

Enforcement of strong access policies across all apps with proactive threat detection and response for identity-based risks in an automated fashion.

### **END-TO-END IDENTITY SECURITY**

Azure Identity & Access Management solution helps secure workforce, partners and consumers in the most simplified yet robust manner.

# HCL Unified Digital Access+ Microsoft Azure Identity & Access Management

Microsoft Azure Identity & Access Management solution and HCL Managed Identity as a Service (MiDaaS) together helps customers onboard users, applications in an automated fashion while enabling strong authentication methods to reduce operational efforts and identity related risks. HCL services strengthens enterprise user credentials and enforces zero-trust based access policies across an enterprise environment with the help of Azure IAM.

1

## IDENTITY GOVERNANCE

Strong Identity & Access Governance for enterprise users, partners and third parties along with regular audits for privileged identities

2

## IDENTITY ANALYTICS

Robust Identity protection with automated threat detection, response & reporting across user base & application access.

3

## BUSINESS SUCCESS

Enjoy business success by enabling Azure B2E, B2C & B2B services.

# Customer success: Leading Oil & Gas super-majors

## Reduced Operational efforts & costs

### OPERATIONAL EFFORTS DECREASED

Productivity of operations team increased cost of help desk decreased through Azure B2B self service registration portal.



### STRONG AUTHENTICATION FOR PARTNER ACCESS

Azure One time-passcode feature enabled for Partner accounts to secure the authentications



### IMPLEMENTED BEST IAM PRACTICES

Followed best IAM practices to clean up current production Azure AD environment with respect to service, test, generic, positional, shared accounts.



# Relationship<sup>TM</sup>

BEYOND THE CONTRACT

9.3 BILLION USD | 150,000+ IDEAPRENEURS | 46 COUNTRIES