Azure Multi-Factor Authentication

Powered by Microsoft

Multi-Factor Authentication (MFA) is central to an effective password vulnerability risk reduction tool. While a username and password combination authentication is something an end-user knows, MFA enhances the authentication experience by challenging the user with a prompt for something they have such as a token, single use code, or device.

Cloud-native Security at your fingertips

Microsoft has developed a Cloud based MFA solution to be utilized as part of their suite of security tools with Azure Active Directory. Basic license users can enable MFA with the Azure Security Default settings; however, utilizing conditional access policies to address varying use cases requires P1 or P2 licensing.

*Source: Ponemon Institute 2019 Cost of a Data Breach Report

Azure MFA Differentiators

- Ability to integrate with existing SSO solutions or be configured with Azure Active Directory for SSO
- Integration with Cloud and On-Premise applications
- Acceleration of adoption through mandatory enrollment for critical applications
- Ability to make risk based decisions when requiring additional authentication through MFA

Expand Security

- Integrate on-premises and in-cloud technologies through Azure SSO or external identity providers
- Integrate with legacy infrastructure platforms that require RADIUS based MFA prompts during authentication

Threat-driven monitoring

- Integration with Microsoft Azure Identity Protection framework to target enrollment of high risk accounts
- Utilize Conditional Access Policies to drive MFA enforcement for risk based sign-in attempts.

Increase efficiencies

- Capable to integrate with Azure Self-Service Password Reset for a seamless identity validation experience for end-users
- Flexible to provide all end-users with a variety of MFA token factors for greater convenience
- Self-service capabilities to manage MFA registration of token factors helping reduce help desk dependencies

Let PwC help you rapidly deploy Azure MFA and enhance security for critical applications and infrastructure.

Two solutions, tailored to your needs

Rapid Release

You have:

- Existing Microsoft Licensing to enable Multi Factor Authentication
- A heavy existing Microsoft footprint or a forward-looking Azure-first strategy
- Azure AD SSO Capable Environment

You want:

- Enhanced Security across business Critical Systems
- Expedited adoption for critical user communities

PwC & Microsoft can:

- Deliver a modern, capable multi factor authentication solution
- Run a workforce enrollment strategy for expedited adoption
- Perform ongoing assessments of critical applications for onboarding and readiness

Rapid Replace

You have:

- An existing Azure Active Directory subscription with synchronized users
- Ability to utilize an existing identity provider or integrate with Azure SSO
- A heavy existing Microsoft footprint or a forward-looking Azure-first strategy

You want:

- To add an additional verification process during authentication to critical applications
- To utilize your existing Azure Active Directory investment

PwC & Microsoft can:

- Integrate your existing critical applications with Azure MFA services
- Facilitate end-user enrollment campaigns for rapid adoption and enforcement

Flexible Architecture

Azure provides flexibility in identity providers and authentication factors

Analytical Threat Intelligence

Integrates with Microsoft's Intelligent Security Graph for unique threat intelligence and analytics

Enhanced User Enrollment

Ability to facilitate adoption through change management initiatives and targeting key user communities.

Contact us for further information

Gary Loveland, Principal
gary.loveland@pwc.com
+1 714 273 1475

Scott MacDonald, Principal
scott.l.macdonald@pwc.com
+1 248 379 7465