Microsoft

Protect identities and secure access to resources

Data breaches often start with just one compromised account. In 2020, Microsoft saw a 230 percent increase in password spray attacks. It's never been more critical to be protected against identity compromise.

Microsoft Azure Active Directory (Azure AD) provides a complete tool set for organizations to protect access to their resources and data—whether on-premises or in any cloud service—using strong authentication and risk-based adaptive access policies without compromising user experience.

Azure AD offers a robust set of identity security capabilities to help organizations secure against breaches, enforce granular access controls, and prevent identity compromise. Key capabilities include multi-factor authentication (MFA), risk-based adaptive access policies, in-session monitoring and control, AI-driven user and sign-in risk detection, and automated remediation.

Secure access to resources

Microsoft research has shown that credentials are 99.9 percent less likely to be compromised when using multi-factor authentication (MFA). Azure AD offers a flexible set of secure MFA options—ranging from calls and one-time passcodes to the simpler and more secure passwordless authentication methods like Microsoft Authenticator and Windows Hello for Business.

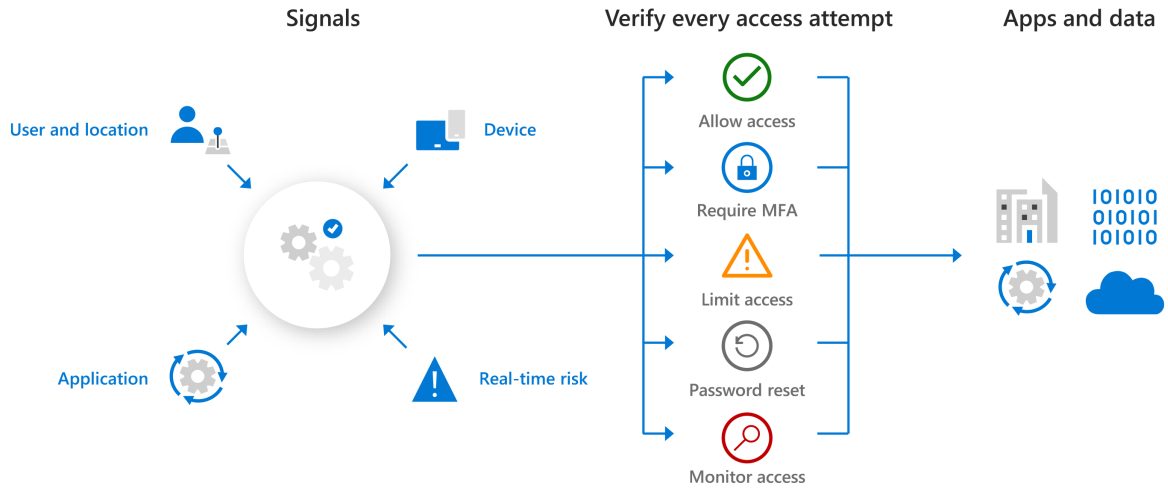
Azure AD also helps improve your identity security posture by automatically detecting and preventing users from using known weak passwords. And preconfigured security settlings help admins close common authentication-related gaps such as not requiring admins to perform MFA, blocking legacy authentication protocols, and more.

Enforce granular access control

Once a user is authenticated, it's critical to enforce access controls to only provide access to the resources they need to do their job. Azure AD Conditional Access enables organizations to enforce fine-tuned adaptive access controls—such as requiring multi-factor authentication or limiting access to read only—based upon user context, device, location, and session risk information. This is a key capability for a robust Zero Trust strategy where policies and real-time signals are required to determine when to allow access, block, limit access, or require additional proofs like multi-factor authentication.

Conditional Access can be integrated with solutions like Microsoft Cloud App Security and Microsoft Intune to provide more control—such as enforcing a read-only decision inside of apps or blocking access for a compromised device until it's remediated.

Microsoft



Automate risk detection and remediation

With a massive increase in identity-related attacks, detecting and responding to compromised accounts quickly is critical to limiting the impact of a breach. Microsoft Identity Protection uses advanced machine learning to deliver real-time continuous detection, automated remediation, and connected intelligence to investigate risky users and sign-ins, addressing potential vulnerabilities.

Prevent compromise

Stop phishing, password spray, and breach replay while simplifying user experience.

Strengthen Conditional Access Policies

Enhance Conditional Access policies with real-time user and sign-in risks.

Investigate and remediate risks

Get reports of risky users, sign-ins, and events for simplified, end-to-end investigation and remediation.

Continuous Access Evaluation (CAE)

Azure AD now supports auto-revoking access in near real time for Microsoft Exchange Online, SharePoint Online, and Teams when critical events or policy violations are detected—such as changes in user risk, user account deletion, user password reset, or user moved to an untrusted location.

Protect your identities today

Don't wait for a security breach to protect your identities. Prevent identity compromise to dramatically reduce organizational risk exposure. Partner with a robust solution that offers a complete tool set for protecting identities and securing access to resources and data.

Try Azure AD today.