Microsoft

Azure Active Directory Identity Protection

Data breaches and stolen credentials are increasing, and a security incident can originate and spread from any account. Hackers can move laterally to abuse any compromised identity and gain access to corporate resources, so it's important to proactively prevent fraud and protect all identities.

A part of the Microsoft cloud-based identity and access management platform, Microsoft Azure Active Directory (AD) Identity Protection lets you automatically protect against identity compromise by taking advantage of cloud intelligence powered by advanced detections based on heuristics, User and Entity Behavior Analytics (UEBA), and machine learning (ML) across the Microsoft ecosystem.

Prevent attackers from accessing and exploiting user identities by allowing identity owners to automatically remediate these risks. To assess and expose identity compromise, Azure AD Identity Protection optimizes heuristics and ML to examine over 40 terabytes of authentication data each day.

This information is transformed into signals and reports that alert admins of issues so they can take appropriate actions to mitigate or remediate them.

How Azure AD Identity Protection works

- ✓ **Identifies suspicious sign-in and user activity**
- ✓ **Prevents user identities from being compromised**
- ✓ **Generates alerts when risk thresholds are exceeded**
- ✓ **Mitigates risks automatically**

With heuristics and ML-based signals, Azure AD Identity Protection performs identity risk assessment every time a user signs in. If these signals—both real-time and offline—trigger your policies, then the user attempting to sign in will be blocked or asked for additional identification via multi-factor authentication (MFA).

Simplify the process

Many identity management solutions flood identity admins with reports and alerts. Intelligence from Azure AD Identity Protection helps identify and prevent identity attacks and security incidents. After automatic risk remediation based on the configured policies, the remainder of the risk is shown in modern reports and sent out via notifications according to the identity admin's preferences. This limits the volume of risk data that identity admins need to manually review.

Reduce the volume of risk data and alerts by configuring risk-based policies in your organization.

Sign-in A sign-in risk is the probability that an authentication request wasn't authorized by the identity owner. Every Azure AD sign-in undergoes risk assessment to calculate user and sign-in risks, which can be None, Low, Medium, or High. Organizations can define sign-in risk-based policies to automatically remediate sign-in risk—a sign-in can be blocked or a user can be required to use MFA to confirm their identity.

User User risk is the probability that an identity is compromised. Much like when evaluating sign-in risks, Azure AD Identity Protection analyzes suspicious actions every time a user signs in. Organizations can define risk-based policies to automatically remediate user risk—a user can be blocked, asked to pass an MFA challenge, or made to securely change their password.

To resolve an identified risk, create a conditional access policy or work through it manually. Unresolved risks lead to risky sign-ins and users. The user risk level is then calculated and labeled either **Low**, **Medium**, or **High** to represent the probability of a compromised identity.

Azure ATP with Cloud App Security and Azure AD Identity Protection

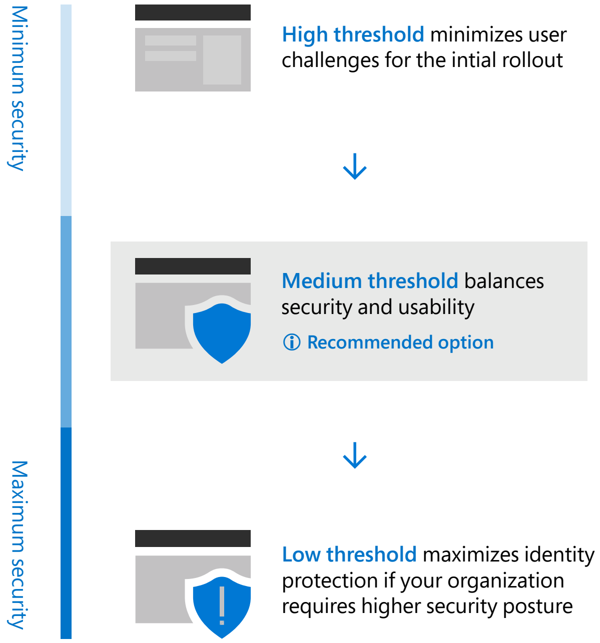
Together, Azure ATP, Azure AD Identity Protection, and Microsoft Cloud App Security are a complete identity protection solution and provide a unified investigation experience for identities in a hybrid organization, correlating data across on-premises and cloud apps. When used together, customers get these added values:

✓ **Detection** Identify suspicious user activities from a single dashboard.

✓ **Investigation** Provide security analysts with a single control plane to investigate alerts and user activities.

✓ **Response** Prevent compromises with risk-based policies that challenge or block risky sign-ins or remediate or block risky users.

Consider these thresholds when establishing a user risk policy:



High threshold minimizes user challenges for the intial rollout

↓

Medium threshold balances security and usability

ⓘ Recommended option

↓

Low threshold maximizes identity protection if your organization requires higher security posture

Get started with Azure AD today

Don’t wait for a breach to implement best security practices. To keep your organization safe, keep each user secure. Partner with a robust solution that’s built for modern threats, shaped by intel gathered from across the Microsoft ecosystem, and used by 90 percent of Fortune 500 companies for their enterprise security.

Start with a **free Azure AD trial** today.