Microsoft Security

Microsoft Entra ID Protection

In today's complex, modern work environment, the sophistication and frequency of attacks from bad actors have increased, turning protecting identities into a daunting task. Attackers use compromised accounts to quickly bypass existing security protocols and then move laterally to gain access to sensitive data and resources. As identity is the first line of defense for any organization, it is crucial to have a solution that can proactively protect against compromised identity attacks.

Over 80% of hacking-related breaches involved the use of lost or stolen credentials.[1]

Block identity takeover in real time with Microsoft Entra ID Protection

Microsoft Entra ID Protection is a cloud-based identity solution that helps organizations prevent, detect, and remediate identity compromise in real time. By analyzing user and sign-in patterns based on integrated risk scores from various sources, ID Protection protects against identity-based attacks such as password spray, brute force, phishing, infected devices, and leaked credentials.

How Microsoft Entra ID Protection works

Microsoft Entra ID Protection empowers you to prevent identity compromise while gaining valuable insights into your security posture with three key capabilities:

- **Enforce risk-based adaptive access policies to prevent identity compromise.**
- **Safeguard access with high-assurance and phishing-resistant authentication factors.**
- **Gain deep insights into your identity security posture.**

Microsoft Entra ID Protection uses cloud-based machine learning to analyze over 200 terabytes of authentication data daily and evaluates sign-in anomalies along 100+ axes in real time.

Teams can also implement and manage sign-in and user risk policies.

- **Sign-in risk policies** address the probability that authentication wasn't authorized by the identity owner. Every sign-in undergoes risk assessment to calculate user and sign-in risks, which can be labeled as *None, Low, Medium*, or *High*. Organizations can define sign-in risk policies to automatically remediate sign-in risk based on assigned levels—a sign-in can be blocked, or users can be required to use multifactor authentication (MFA) to confirm their identity.
- **User risk policies** address the probability that a user's identity is compromised. Organizations can define risk-based policies to automatically remediate user risk—a user can be blocked, asked to pass an MFA challenge, or required to change their password securely.
- The risk signals trigger remediation efforts such as requiring users to perform MFA or reset their password using self-service password reset, or by blocking access until an administrator takes action.

[1] Source: Data Breach Investigations Report, Verizon, 2022

Consider these thresholds when establishing a user risk policy:

Low

A low threshold maximizes identity protection if your organization requires a higher security posture.

Medium

A medium threshold balances security and usability.

High

A high threshold reduces the number of times a policy is triggered and minimizes impact on the user.

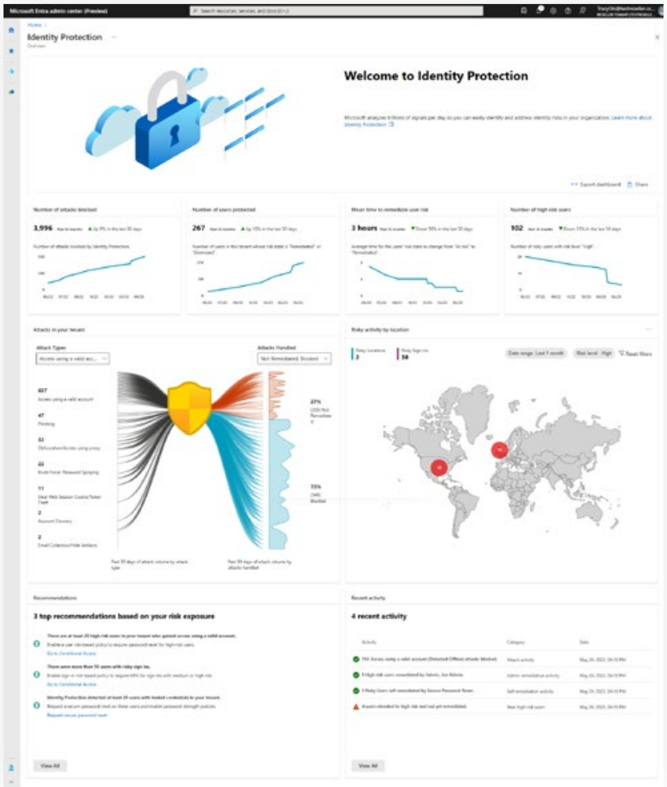
With advanced heuristics, user and entity behavior analytics (UEBA), and machine learning-based signals, Microsoft Entra ID Protection enforces risk-based adaptive access policies and investigates risky users and sign-ins. With extended Conditional Access policies, you can prevent use of stolen or replayed tokens as well as any sudden changes in location. Then you can measure the impact of the protections you deploy with ID Protection's dashboard. The simplified display center elevates identity security with a comprehensive snapshot of prevented identity attacks and common attack patterns, showing you likely attacks, providing recommended next steps, and capturing metrics on attacks that you have stopped.

Simplify the process with automatic remediation

Microsoft Entra ID Protection streamlines reporting and alert management, empowering IT and identity practitioners and Security Operations Center (SOC) analysts to work together and efficiently investigate alerts and user activity. The user-friendly interface automatically remediates high-risk users and sign-ins while providing valuable risk insights and recommendations to block identity attacks in real time. Administrators can view digestible metric cards and attack graphs, security posture over time, types of current attacks, and recommendations based on risk exposure, while highlighting the business impact of enforced controls.

Actionable insights from unmatched intelligence

Microsoft Entra ID Protection seamlessly integrates with other first- and third-party security solutions, including Microsoft Defender and Microsoft Sentinel, to enable unified remediation by correlating alerts. The user-friendly interface reduces the flood of reports into easily digestible, actionable insights.


Identity Protection
Welcome to Identity Protection
3,996
267
3 hours
102
3 top recommendations based on your risk exposure
4 recent activity
View All
View All

The dashboard shows likely attacks and recommendations.

Protect your identities today

Microsoft Entra ID Protection is available with Microsoft Entra ID Premium P2 license. Start with a Microsoft Entra ID P2 trial today. Visit the website for more information.

Microsoft Security