Microsoft Security

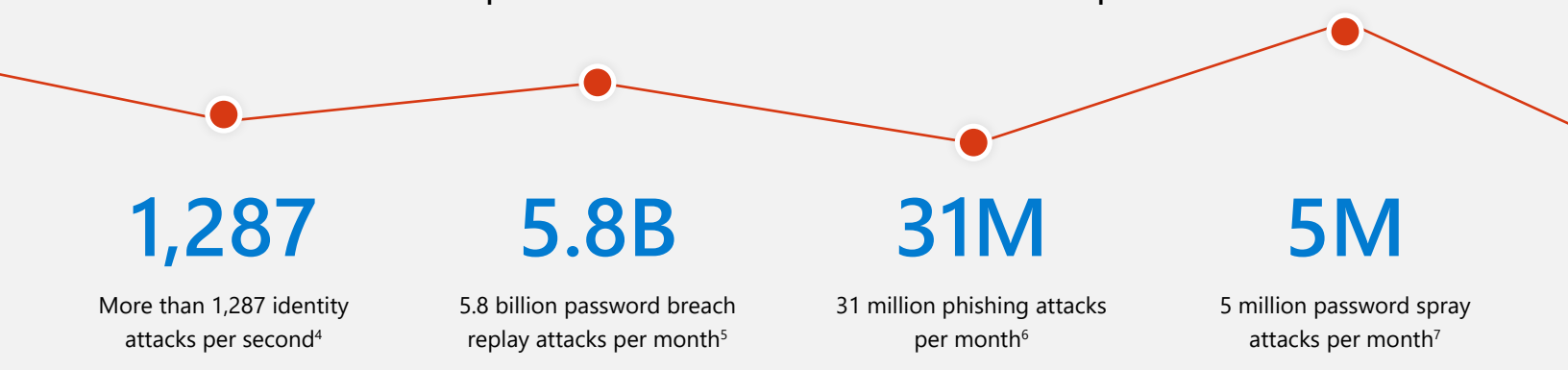# Microsoft Entra ID Protection

Sophisticated identity-based attacks on the rise

As organizations worldwide continue to embrace digital transformation and flexible work, an ever-changing threat landscape targets human and non-human identities. Whether password sprays or phishing, attacks are increasing in both frequency and sophistication. Identity compromise remains the most common method for attackers to breach digital estates,[1] highlighting the critical role of identity as the initial line of defense.[2]
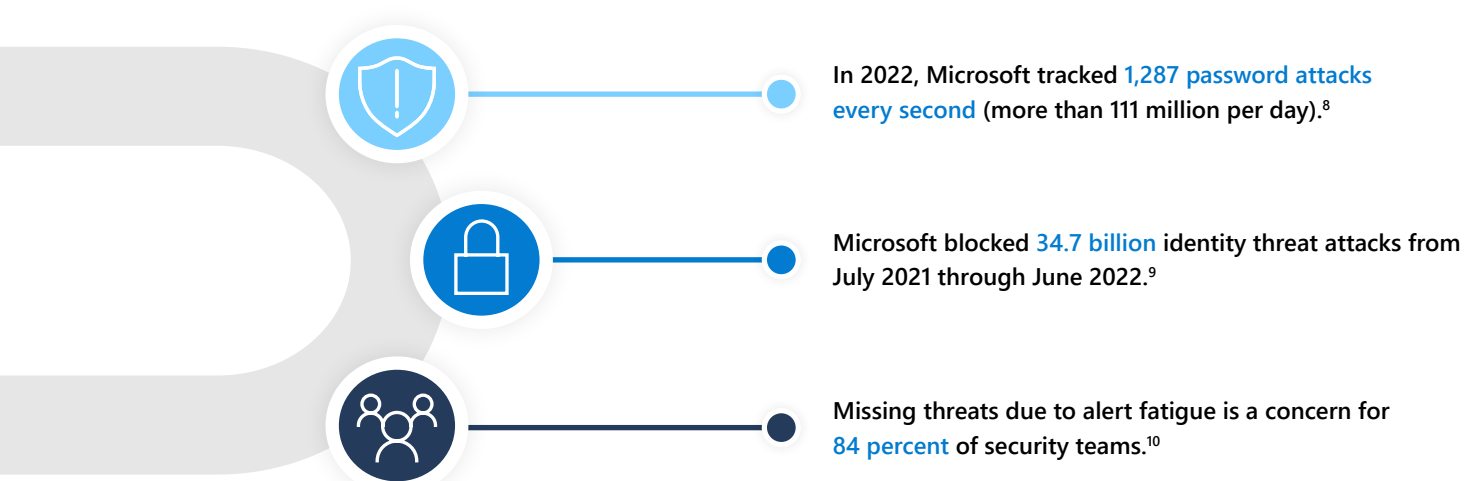
80%

More than **80** percent of breaches can be attributed to identity-based attacks, and that number is only going to grow.[3]

You can see this pattern in the vast number of attacks we intercept at Microsoft:

1,287
More than 1,287 identity attacks per second[4]

5.8B
5.8 billion password breach replay attacks per month[5]

31M
31 million phishing attacks per month[6]

5M
5 million password spray attacks per month[7]

Need for automation and real-time alerts

IT and identity leaders seek help automating identity-based risk detection and remediation, consolidating real-time alerts, risk detection data and policies within easily digestible dashboards, and integrating with other security tools.

- In 2022, Microsoft tracked **1,287 password attacks every second** (more than 111 million per day).[8]

- Microsoft blocked **34.7 billion** identity threat attacks from July 2021 through June 2022.[9]

- Missing threats due to alert fatigue is a concern for **84 percent** of security teams.[10]

How Microsoft Entra ID Protection can help

Microsoft Entra ID Protection blocks identity compromise in real time using high-assurance authentication methods, automated risk and threat assessment, and adaptive access policies powered by advanced machine learning. With our solution, you can:

- Analyze over **200 terabytes** of authentication data daily
- Evaluate sign-in anomalies along **100+ axes** in real time

Preventing identity attacks with Microsoft Entra ID Protection

Prevent identity compromise

- Enforcing risk-based, adaptive Conditional Access policies prevents identity compromise based on sign-in and user risk data integrated from various sources.
- Advanced machine learning and connected intelligence let you investigate risky users and sign-ins and automate remediation

Enforce policies

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

Deepen insights

- Review informative signals and reports in a single control plane.
- Gain risk insights and key recommendations with a simplified user interface that identifies high-risk users and sign-ins.
- Allow export and integration with security information and event management (SIEM) and extended detection and response (XDR) tools.

Take the next step

Learn more about Microsoft Entra ID Protection today.

[Try Microsoft Entra ID P2 trial]

[1] Verizon: Data Breach Investigations Report, 2008–2022
[2] Gartner Identifies Top Security and Risk Management Trends for 2022
[3] Verizon: Data Breach Investigations Report, 2008–2022
[4] Microsoft Entra: 5 identity priorities for 2023
[5] Microsoft Entra: 5 identity priorities for 2023
[6] Microsoft Entra: 5 identity priorities for 2023
[7] Microsoft Entra: 5 identity priorities for 2023
[8] Microsoft Entra: 5 identity priorities for 2023
[9] Microsoft: State of Cybercrime, 2022
[10] Mandiant: Global Perspectives on Threat Intelligence Report

Microsoft Security