Understanding identity threat protection

Digital transformation and a priority shift towards enabling a hybrid workplace has thoroughly redefined the network perimeter for virtually every organization. In response, many IT leaders are in the process of rapidly moving towards using identities as the core of their cybersecurity strategy access—if they haven't already.

This has resulted in a significant increase in identity-based attacks as cybercriminals shift their focus to the largest opportunities. As IT leaders rely more heavily on identities for their security strategy, it becomes imperative that they're proactively protecting their identities against compromise.

1 IDENTITY-BASED ATTACKS ARE INCREASING

Using tactics like password spraying, phishing, and breach replays, cybercriminals have been increasingly focused on trying to compromise personal and professional accounts.

300%

Microsoft has seen a **300% rise** in identity-based attacks in the past year

45%

of CISOs report seeing an increase in phishing campaigns and identity fraud

2 MORE VISIBILITY AND PROTECTION IS NEEDED

With the increase in threats, IT leaders are looking for help to better manage alerts and proactively prevent compromise.

72%

of tech execs want to be alerted to sign in threats

88%

of IT leaders want to be able to prevent user information from being compromised

21,000 HOURS

Time spent annually by security analysts triaging false positives

– Ponemon Institute

3 IDENTITY PROTECTION IS MORE VITAL THAN EVER

In March 2020 alone, Microsoft detected **4.9 billion** attacker-driven sign ins and over **150k** compromised accounts—and these attacks are picking up speed.

IT teams who proactively leverage identity protection can prevent attackers from accessing and exploiting identities before a threat occurs.

4.9B

ATTACKER-DRIVEN SIGN-INS IN ONE MONTH

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.

4 HOW MICROSOFT CAN HELP

As we see above, there are two core identity protection challenges IT leaders need help with—help managing alerts and better protection to proactively prevent identity compromise.

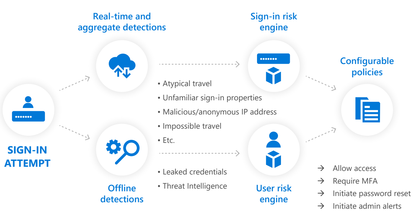
Microsoft Azure Active Directory Identity Protection uses cloud intelligence powered by advanced heuristics, User and Entity Behavior Analytics (UEBA), and machine learning (ML) to automatically detect and prevent identity compromise across your digital ecosystem.

Identity Protection evaluates and protects you from two types of risk:

USER RISK
Probability that a user identity is compromised

SIGN-IN RISK
Probability that an authentication wasn't authorized by the identity owner

You can configure risk policies and notifications to fine-tune how Identity Protection handles risk detections. These policies enable your organization to make decisions—such as requiring multi-factor authentication, blocking access, etc. —based on risk scores to fit your organization's unique risk appetite.

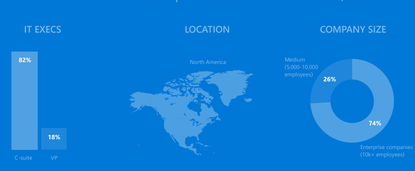


Investigating events is key to better understanding and identifying weak points in your identity security strategy. Azure AD Identity Protection provides comprehensive reporting to help you investigate risk users, risky sign-ins, and risk detections.

Admins can then choose remediation actions such as password reset, dismiss, confirm user compromise, investigate further with Microsoft Defender for Identity, and more. And through the Microsoft Graph API, organizations can integrate this data with other sources they may have access to.

Learn more about Azure AD Identity Protection today.

RESPONDENT BREAKDOWN | DATA COLLECTED FROM APRIL 15-30, 2020



Insights powered by PULSE

Microsoft