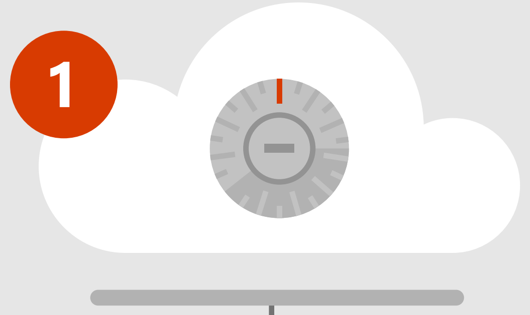
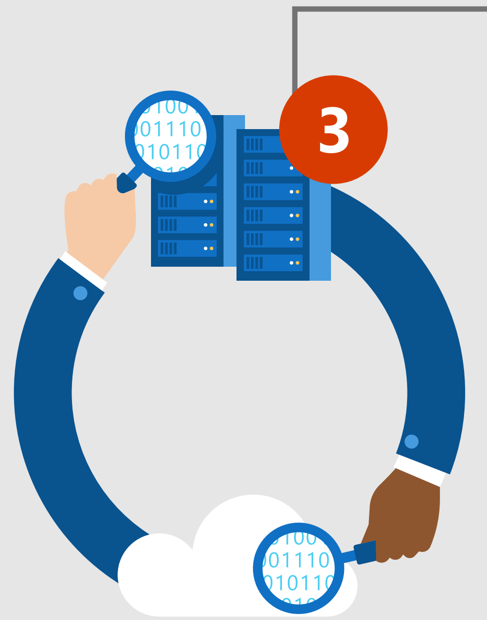
Comprehensive identity protection across Azure Active Directory Identity Protection and Azure Advanced Threat Protection

81% of breaches are caused by credential theft.



It is hard to find security solutions that work well together and are comprehensive at the same time.

In most large organizations, IT teams tasked with administering identity and access and the teams tasked with responding to a breach are different and may or may not be working hand-in-hand.



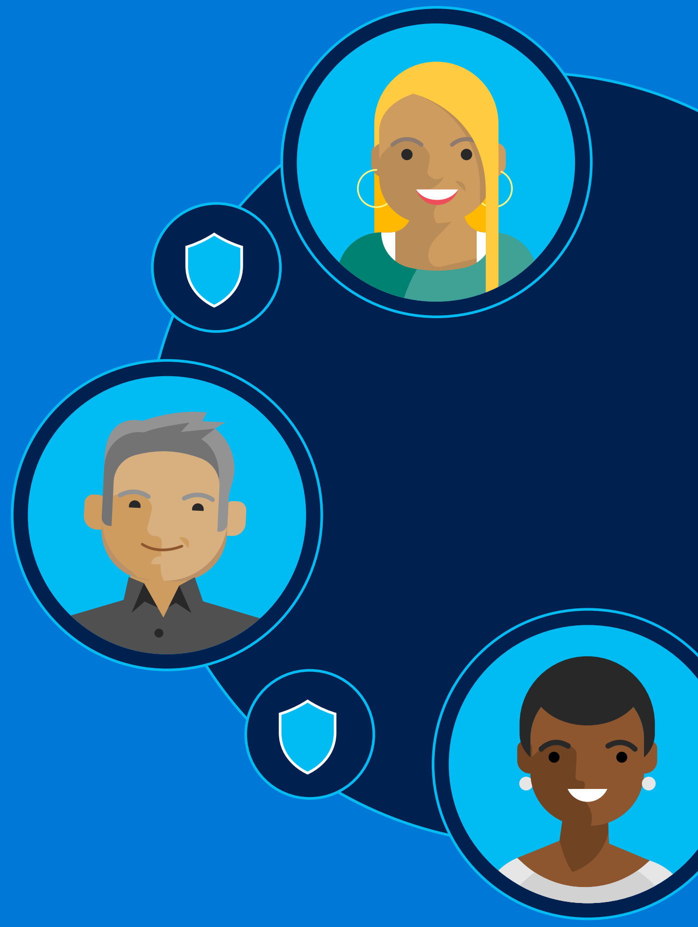
Additionally, user identities may exist in varying proportions across cloud and on-premises.

To help you overcome these challenges, Microsoft offers two solutions

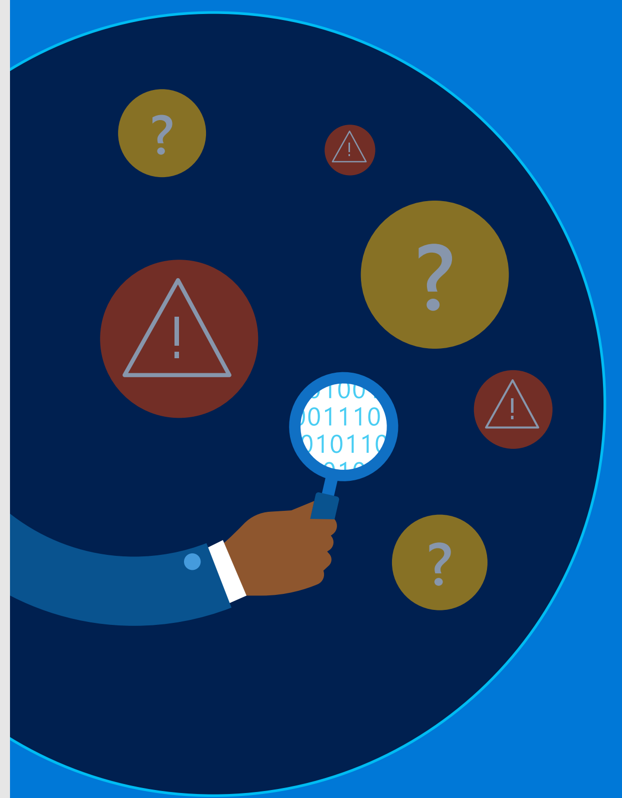
One aligned with the priorities of the identity admin and the other aligned to the security operations professional:

Azure AD Identity Protection:

Protection built right into Azure Active Directory, **Azure Active Directory Identity Protection** uses **dynamic intelligence and machine learning** to automatically detect and protect your organization from identity attacks. **Learn more about Azure AD Identity Protection.**



Azure Advanced Threat Protection:



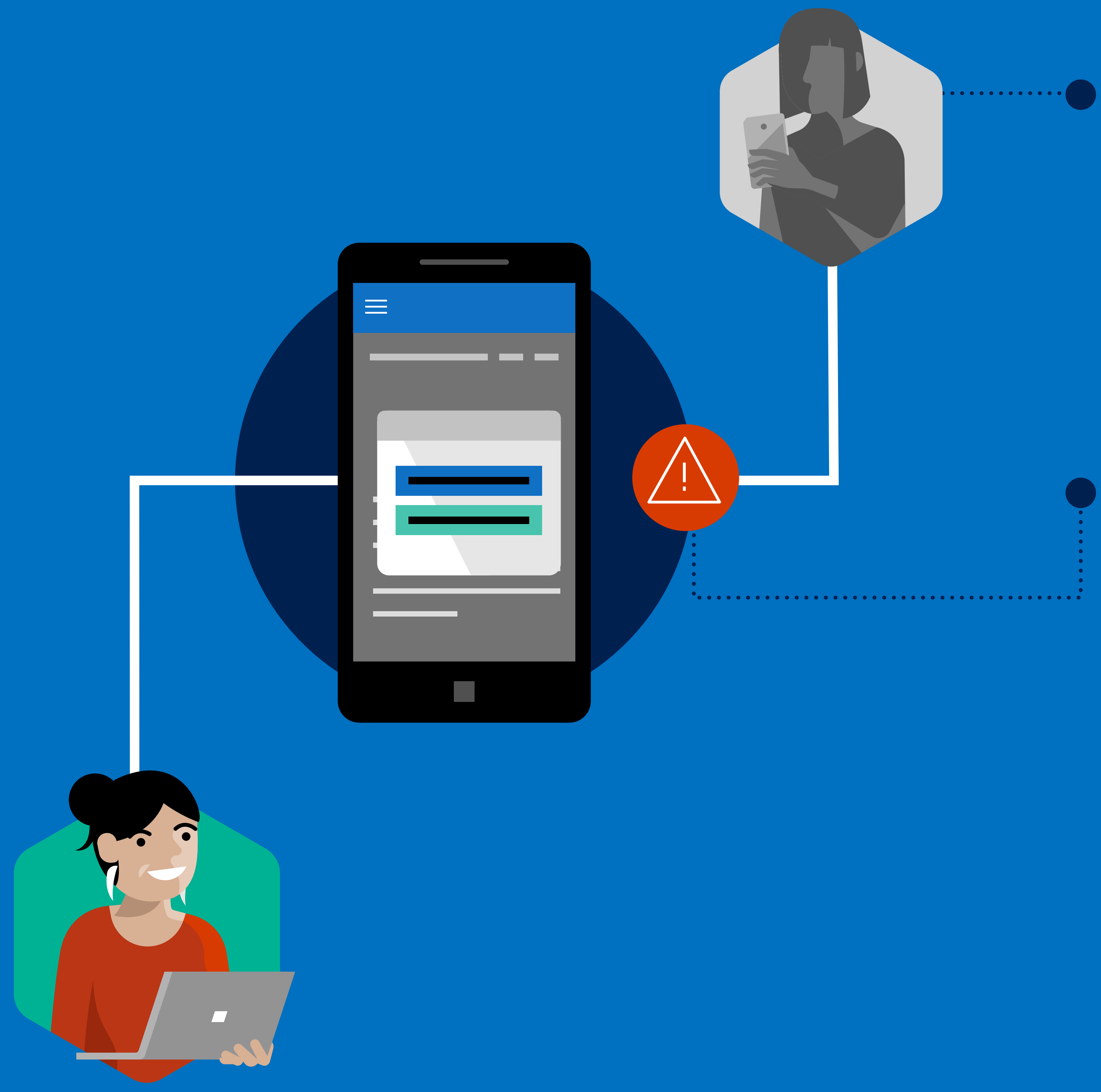
Our newest product for security operations staff, Azure Advanced Threat Protection is a **cloud-based security solution** that helps detect and investigate incidents and suspicious behavior by leveraging machine learning and threat intelligence signals across networks. **Learn more about Azure ATP.**

Microsoft

Proactive

Protect yourself against the latest advanced threats to your identities with Azure AD Identity Protection

Reactive



- An **unrelated, third-party site** has been **hacked and user credentials are exposed on the dark web** as in a typical Breach Replay attack. A bad actor attempts to log-in with the compromised credentials.
- Azure AD Identity Protection proactively **identifies that the login is from an unknown location that's possibly malicious,** assigns a high-risk level and is challenged for MFA which the hacker is not able to get through. However, when the real user logs in the next time and is similarly challenged with a **second factor authentication,** the user is able to authenticate and is then asked to reset the password thus ensuring that your organization is protected. Learn more about the types of risk events that Azure AD Identity Protection can detect.

Almost every week,

a new form of threat emerges, and a new modus operandi unveiled.

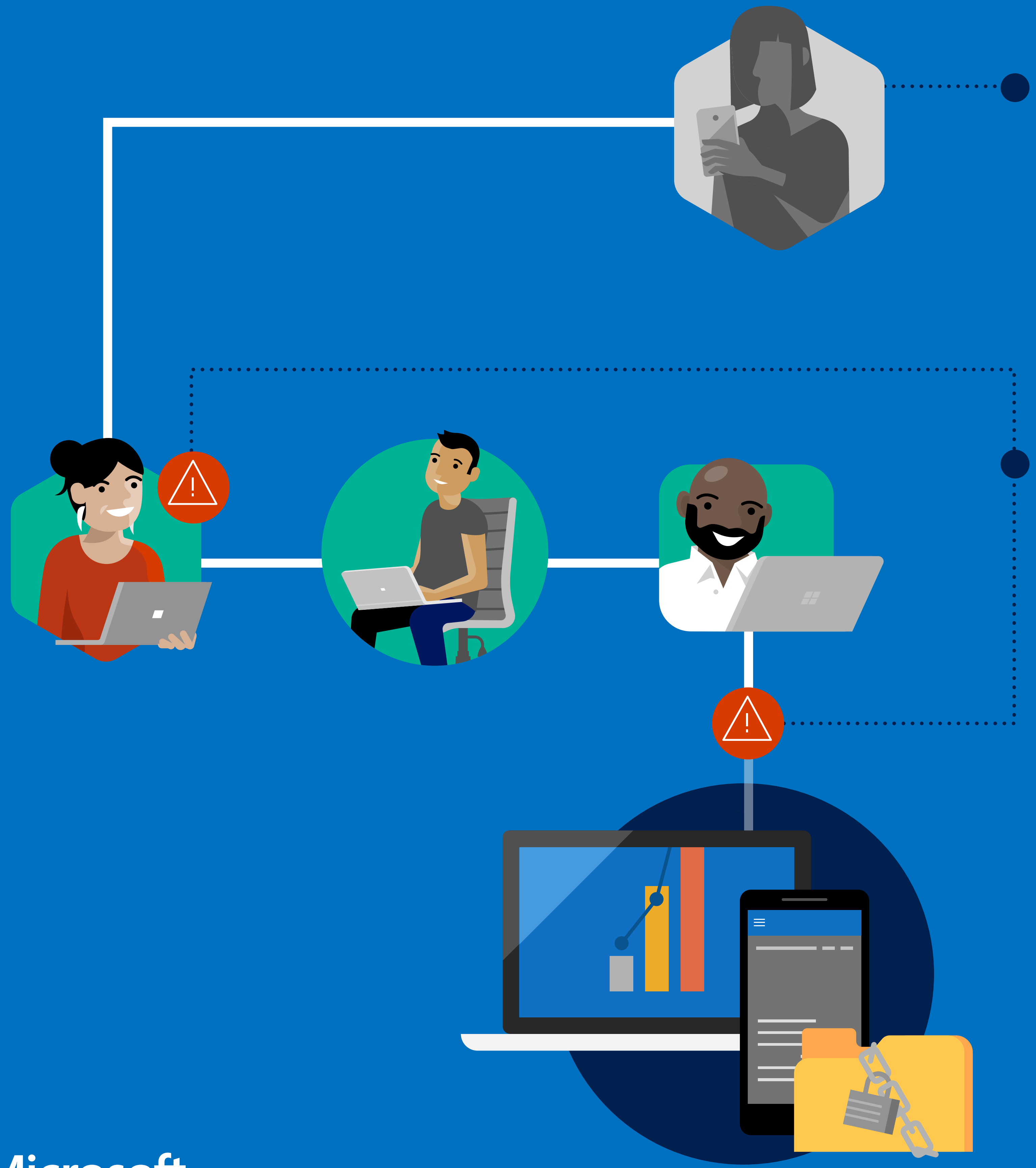
In today's times, the capability to digest this information actionably has gone beyond the ability of humans and so, within Azure AD Identity Protection, we have founded capability that takes advantage of Microsoft's decade-long experience of securing cloud identities with the latest machine learning technologies and a billion $ annual R&D investment to create a solution that enables IT admins to define actionable policies that **protects individual user identities to protect against account compromise in real-time.**

Microsoft

Proactive

Reactive

Respond to incidents with Azure Advanced Threat Protection



Attacker **compromises a user account** and attempts to **laterally move** through a network until they locate a privileged account to **gain greater access** to devices and sensitive data.

Azure Advanced Threat Protection **notifies you of compromised identities, and attacks in progress,** which enables you to take steps to mitigate damage, to data, and resources, from the intrusion. With Azure ATP's Windows Defender ATP integration **broadens incident response** allowing investigation into both compromised identities and devices.

In today's reality of sophisticated threats,

organizations know that even with the greatest of proactive measures in place, it is possible that a persistent hacker can still worm their way into your environment and the agenda now swiftly moves to being able to respond quickly.

Azure Advanced Threat Protection provides a **real-time view of attacks,** providing a detailed timeline showing **which users** have been compromised, **what techniques** are being used, and on **what devices.**

Microsoft