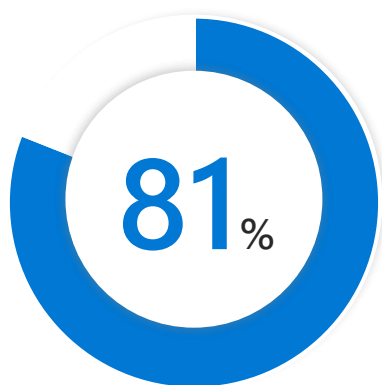


Secure access to your enterprise

Identity and access management



of hacking breaches leverage stolen or weak passwords.¹

It should be no surprise that identity-related cyberattacks are on the rise. The increase in worker mobility has eroded the traditional IT perimeter. That perimeter has been replaced with the user, front and center, and that perimeter goes wherever your users go.

With Microsoft 365, organizations can protect users' identities and control access to valuable resources based on their user risk level.

¹ Verizon. "Verizon Data Breach Investigations Report." July 2017.

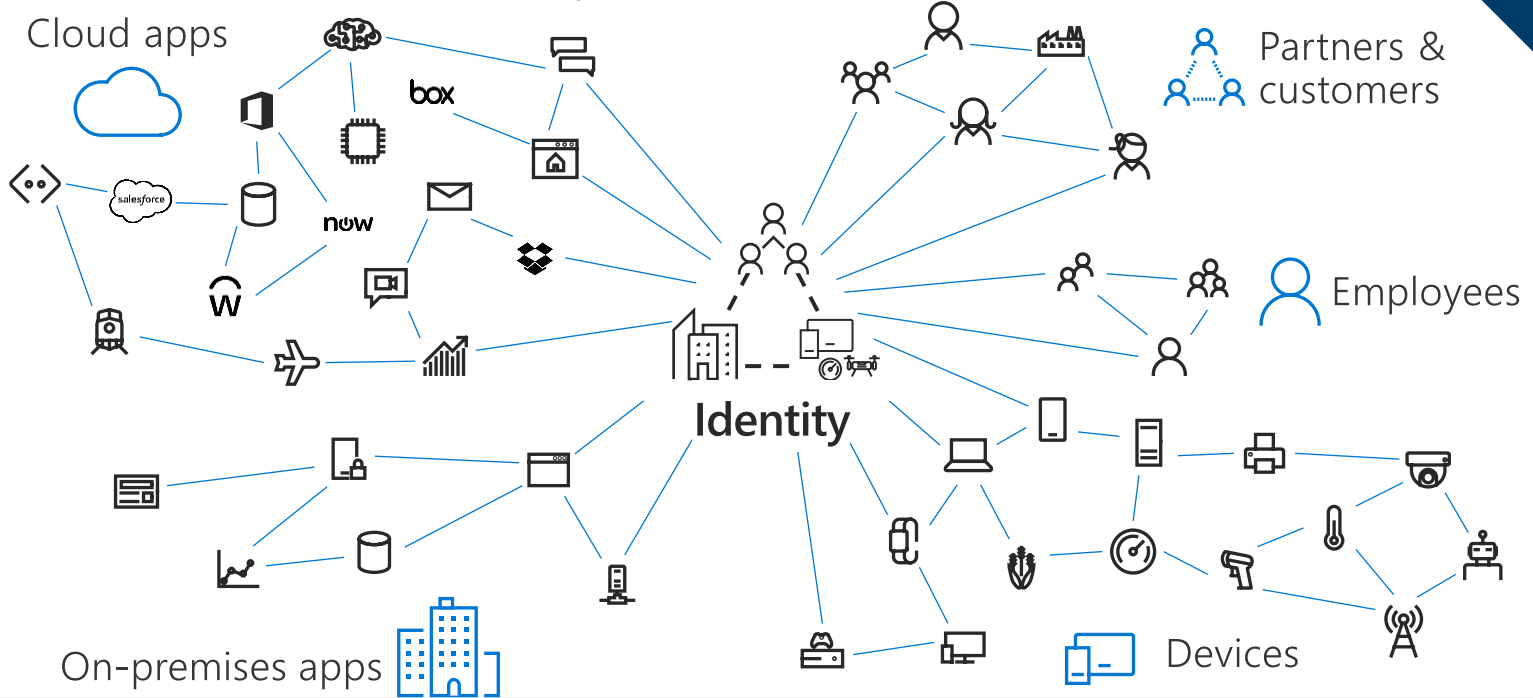


"With Azure Active Directory, we can set policies that treat employees outside the office more strictly than those inside it and that prompt for Multi-Factor Authentication on unmanaged devices or for certain applications. With Microsoft 365, we no longer have to choose between mobility and security—we have both."

Bryan Ackermann, Chief Information Officer, [Korn Ferry](#)

Secure access to your enterprise

Identity is the new control plane



Network walls have come down, but your security doesn't have to

Secure Authentication

Passwords are your **biggest vulnerability**, partly because they are the target of most attacks we see today. We are investing in the **next generation of authentication** solutions such as password-less authentication.

Conditional Access

Conditional access is an integrated capability across our security products that enables you to handle access scenarios using a **policy-based approach**.

Identity Protection

In this imperfect world where we sometimes rely on username and password, **keeping those credentials protected** once they're used is critical.

Get complete, intelligent enterprise security

See for yourself with a Security Workshop, or learn more at: microsoft.com/identity

