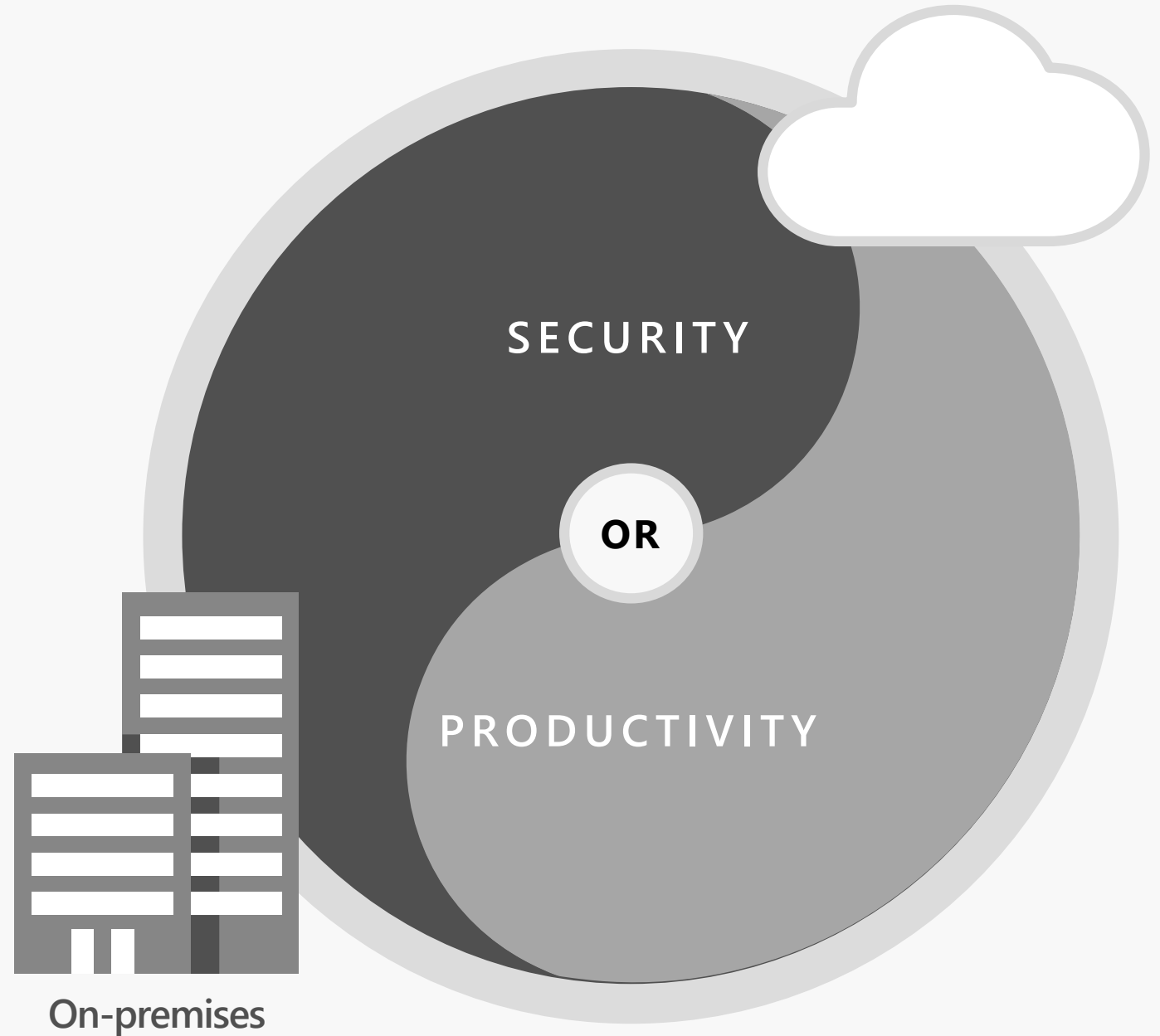


Identity & Access Management

THE PROBLEM:

HOW DO WE ENABLE
PRODUCTIVITY WITHOUT
**COMPROMISING
SECURITY?**



THE PROBLEM:

HOW DO WE ENABLE
PRODUCTIVITY WITHOUT
**COMPROMISING
SECURITY?**





OUR COMMITMENT TO **YOU**



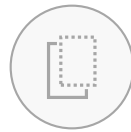
SECURITY



PRIVACY & CONTROL



COMPLIANCE



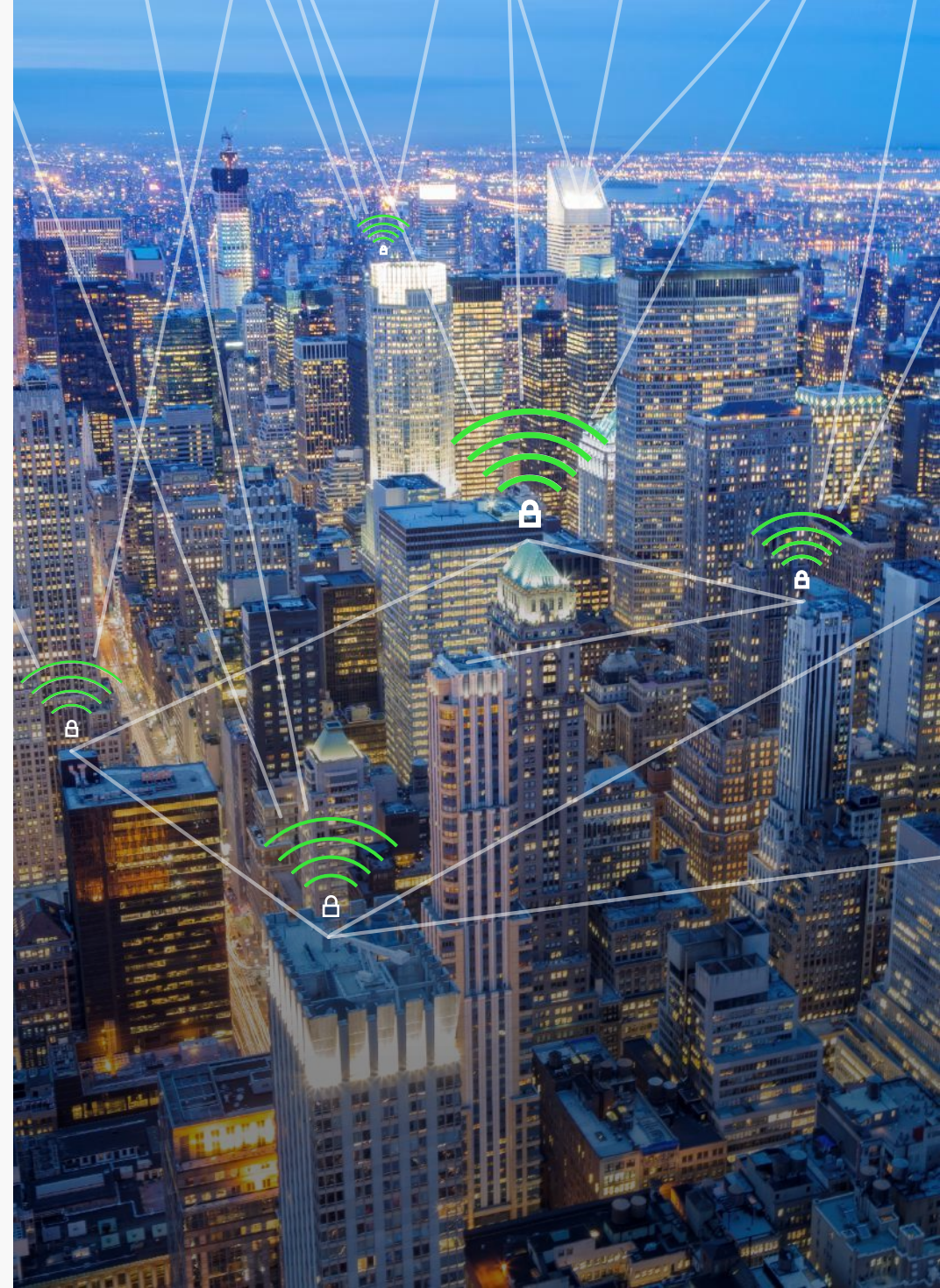
TRANSPARENCY



RELIABILITY

Microsoft Secure

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships



OUR **UNIQUE** APPROACH



PLATFORM

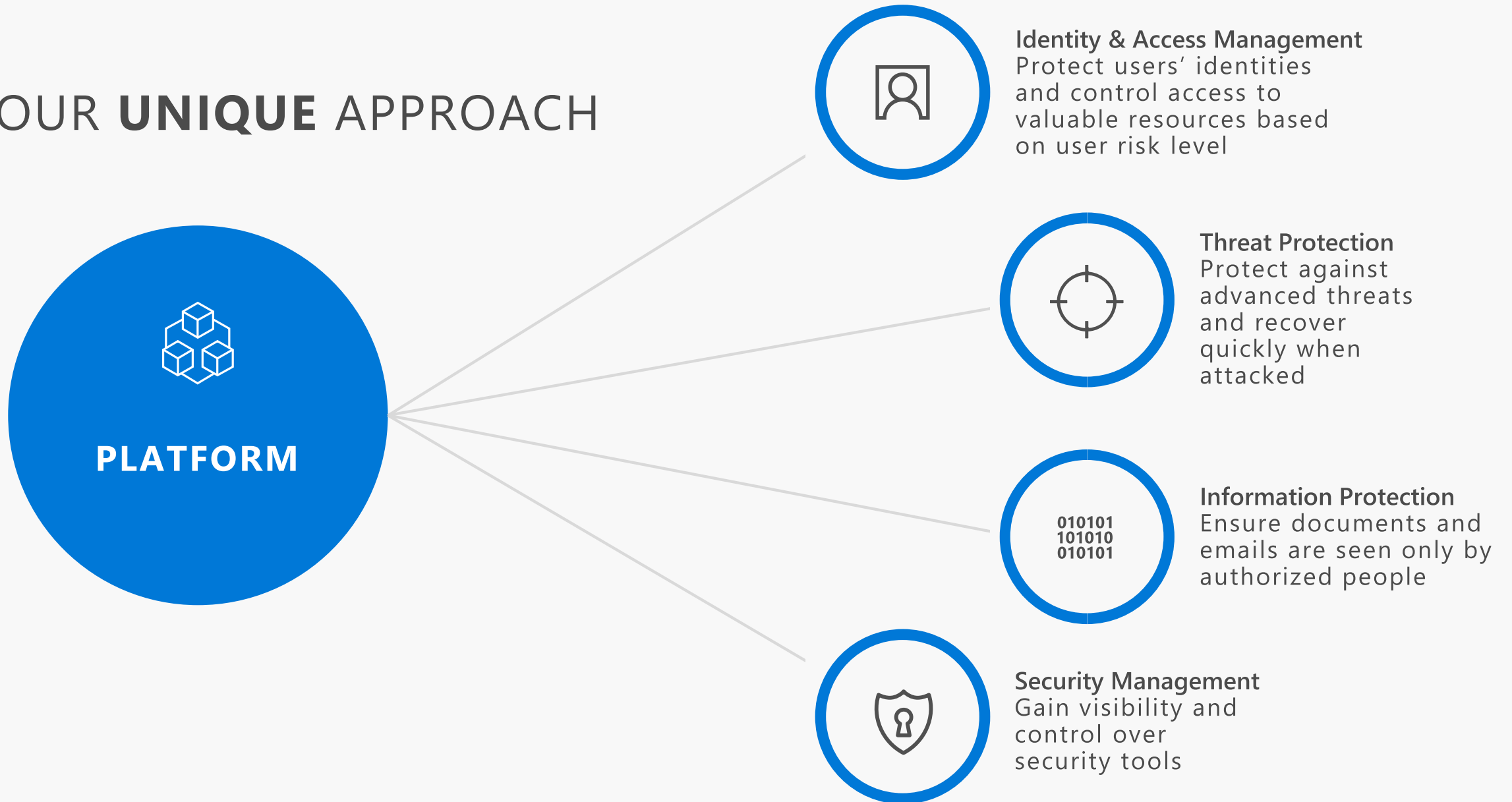


INTELLIGENCE



PARTNERS

OUR **UNIQUE** APPROACH





OUR SECURITY OFFERING

Identity & Access Management

Azure Active Directory
Conditional Access
Windows Hello
Windows Credential Guard

Threat Protection

Advanced Threat Analytics
Windows Defender Advanced Threat Protection
Office 365 Advanced Threat Protection
Office 365 Threat Intelligence

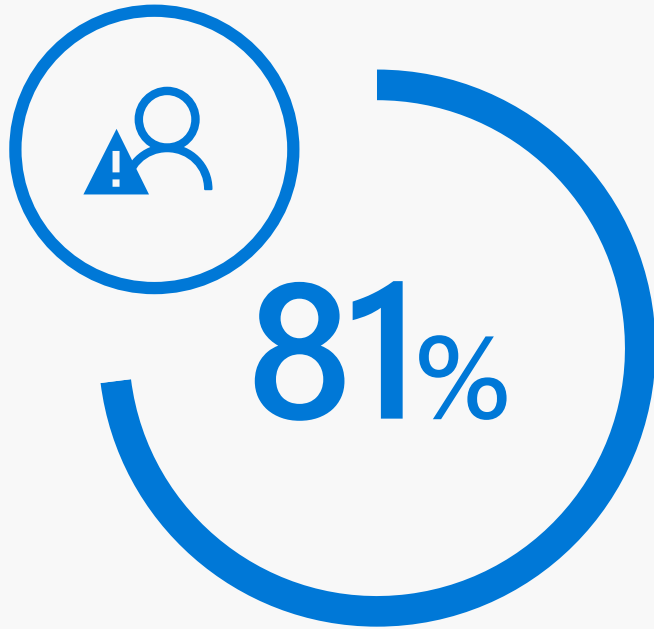
Information Protection

Azure Information Protection
Office 365 Data Loss Prevention
Windows Information Protection
Microsoft Cloud App Security
Office 365 Advanced Security Mgmt
Microsoft Intune

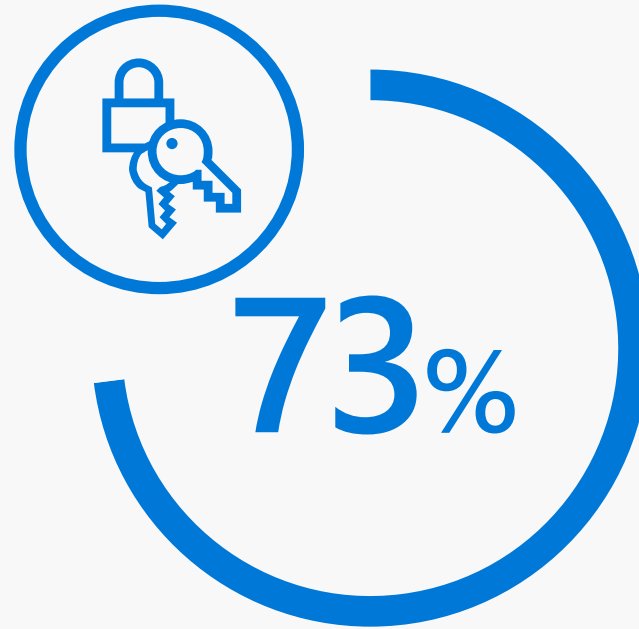
Security Management

Azure Security Center
Office 365 Security & Compliance Center
Windows Defender Security Center

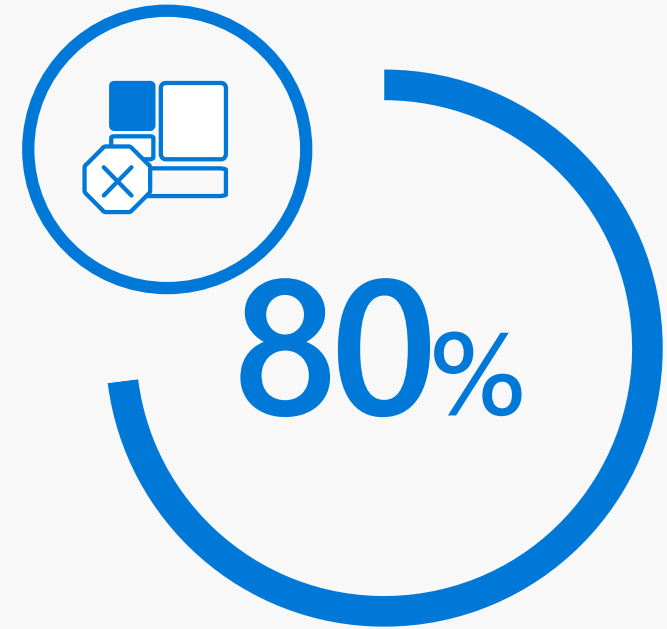
WHY **IDENTITY** IS IMPORTANT



of breaches are caused
by credential theft

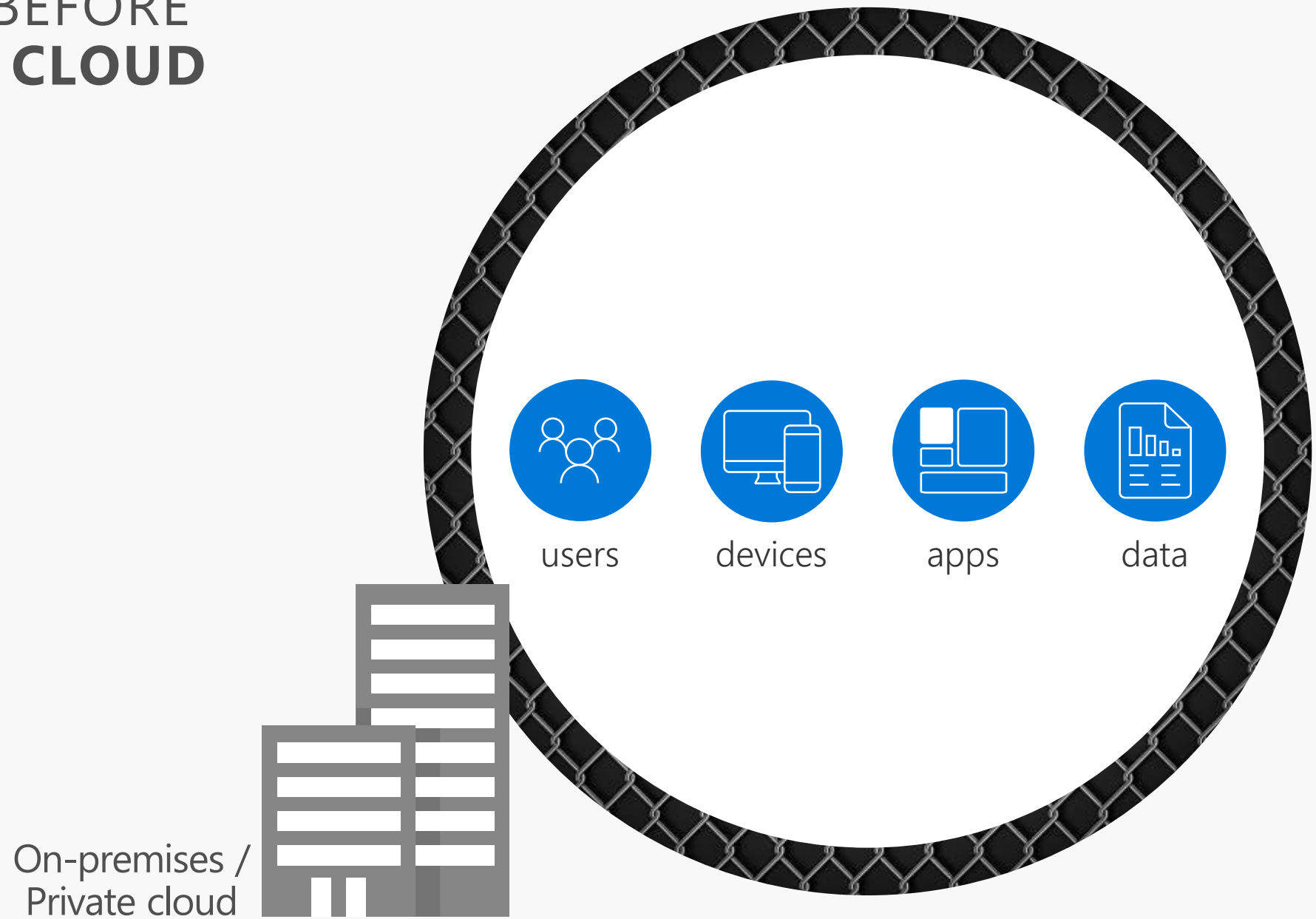


of passwords are
duplicates



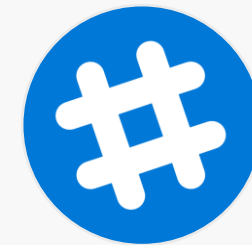
of employees use non-
approved apps for work

THE WORLD BEFORE **MOBILITY & CLOUD**



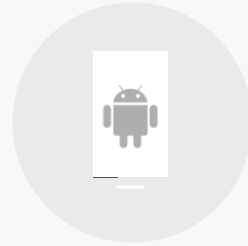


CLOUD APPS & SAAS SERVICES

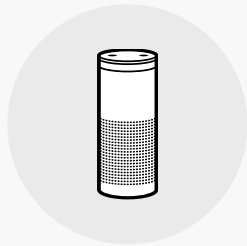


On-premises /
Private cloud





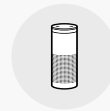
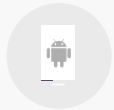
MOBILE AND PERSONAL DEVICES



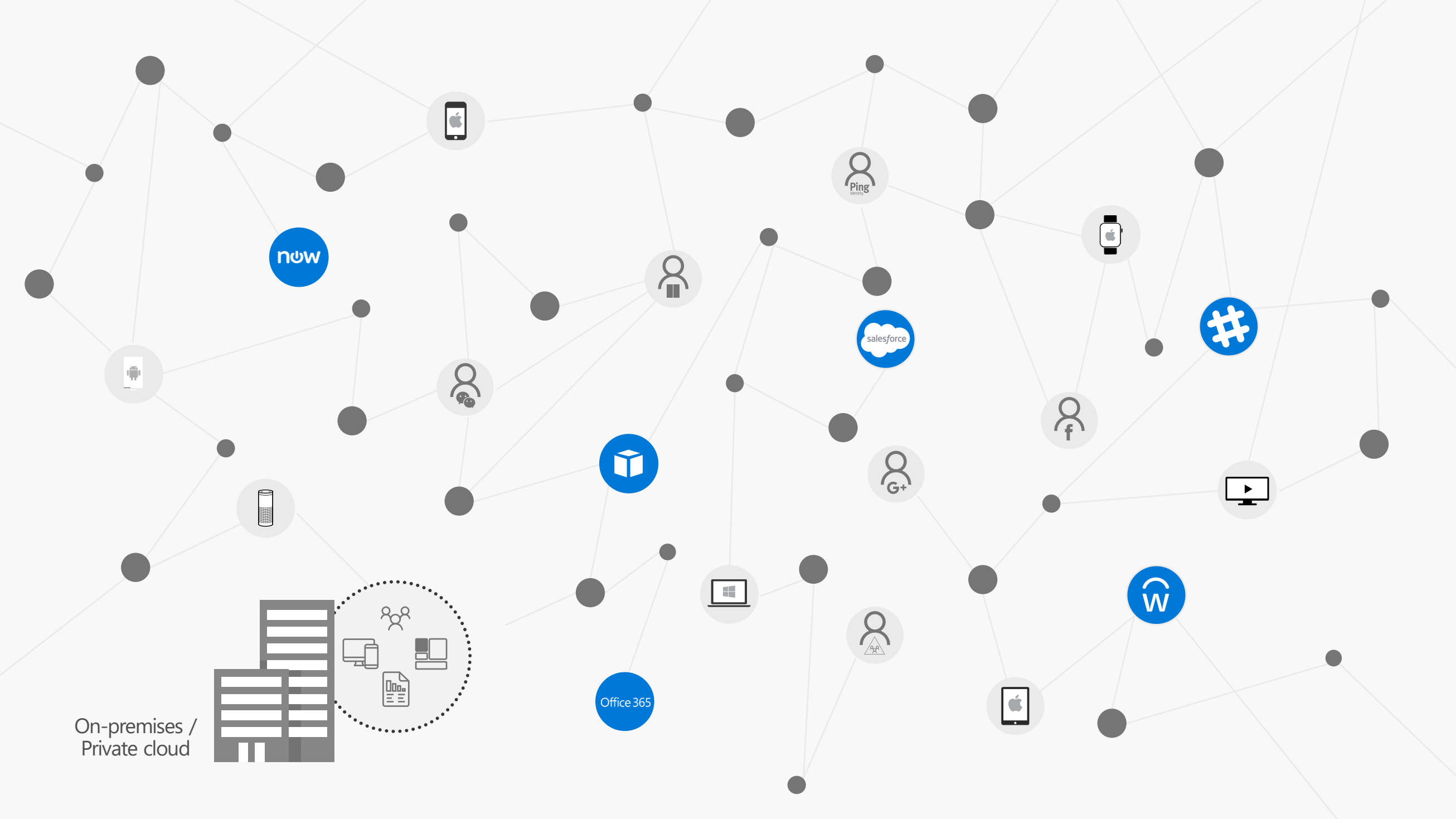
On-premises /
Private cloud

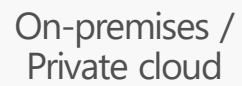


On-premises /
Private cloud



ORGANIZATION & SOCIAL IDENTITIES





IDENTITY & ACCESS MANAGEMENT

Prove users are authorized and secure before granting access to apps and data



Protect at the
front door



Simplify access to
devices and apps



Safeguard your
credentials

HOW MUCH **CONTROL** DO
YOU HAVE OVER **ACCESS**?



Who is accessing? What is their role?
Is the account compromised?



Where is the user based? From where is
the user signing in? Is the IP anonymous?



Which app is being accessed?
What is the business impact?



Is the device healthy? Is it managed?
Has it been in a botnet?

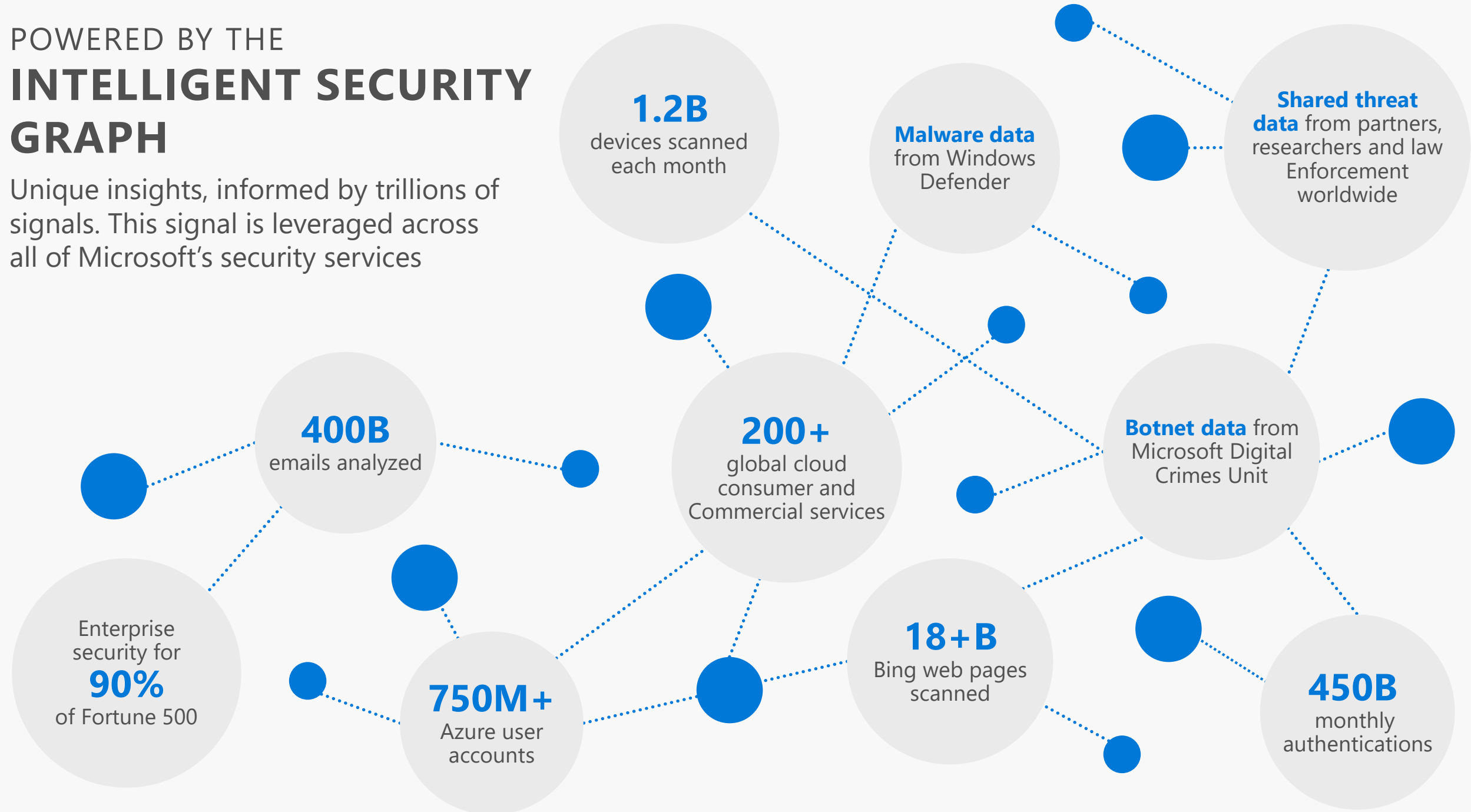


What data is being accessed?
Is it classified? Is it allowed off premises?

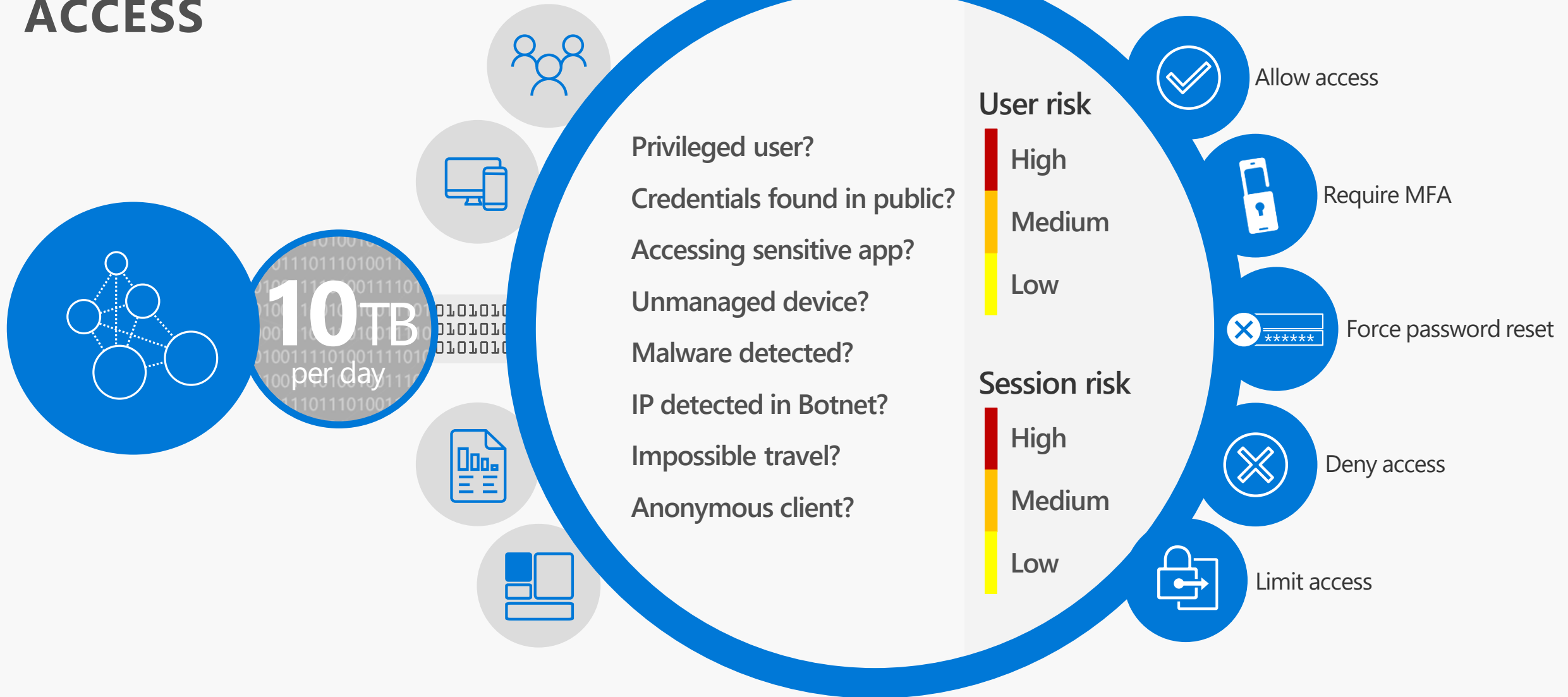


POWERED BY THE INTELLIGENT SECURITY GRAPH

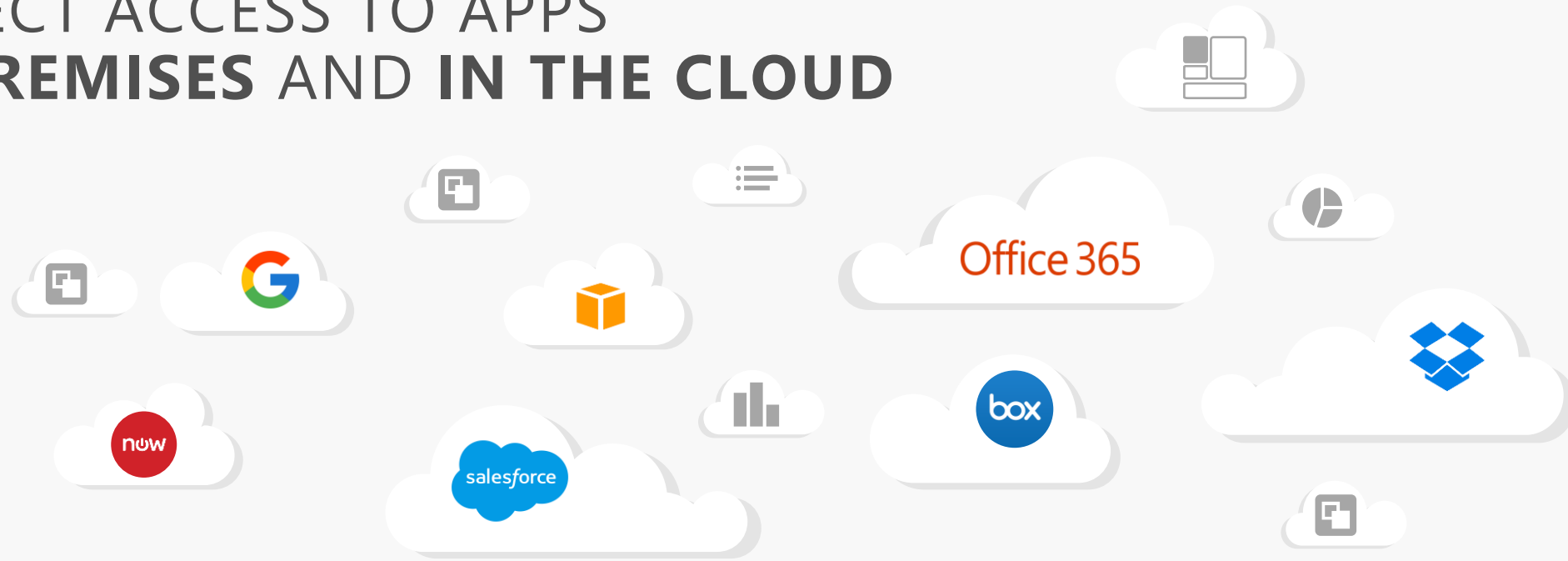
Unique insights, informed by trillions of signals. This signal is leveraged across all of Microsoft's security services



AZURE AD CONDITIONAL ACCESS



PROTECT ACCESS TO APPS **ON-PREMISES AND IN THE CLOUD**



ON-PREMISES

HOW CAN YOU SIMPLIFY
ACCESS TO **DEVICES & APPS?**



Do your users struggle to remember complex passwords?



Do they have to juggle multiple credentials?



Can you extend user identity for Office 365 or Windows to other apps?



Do you MFA every time you want to ensure secure access?



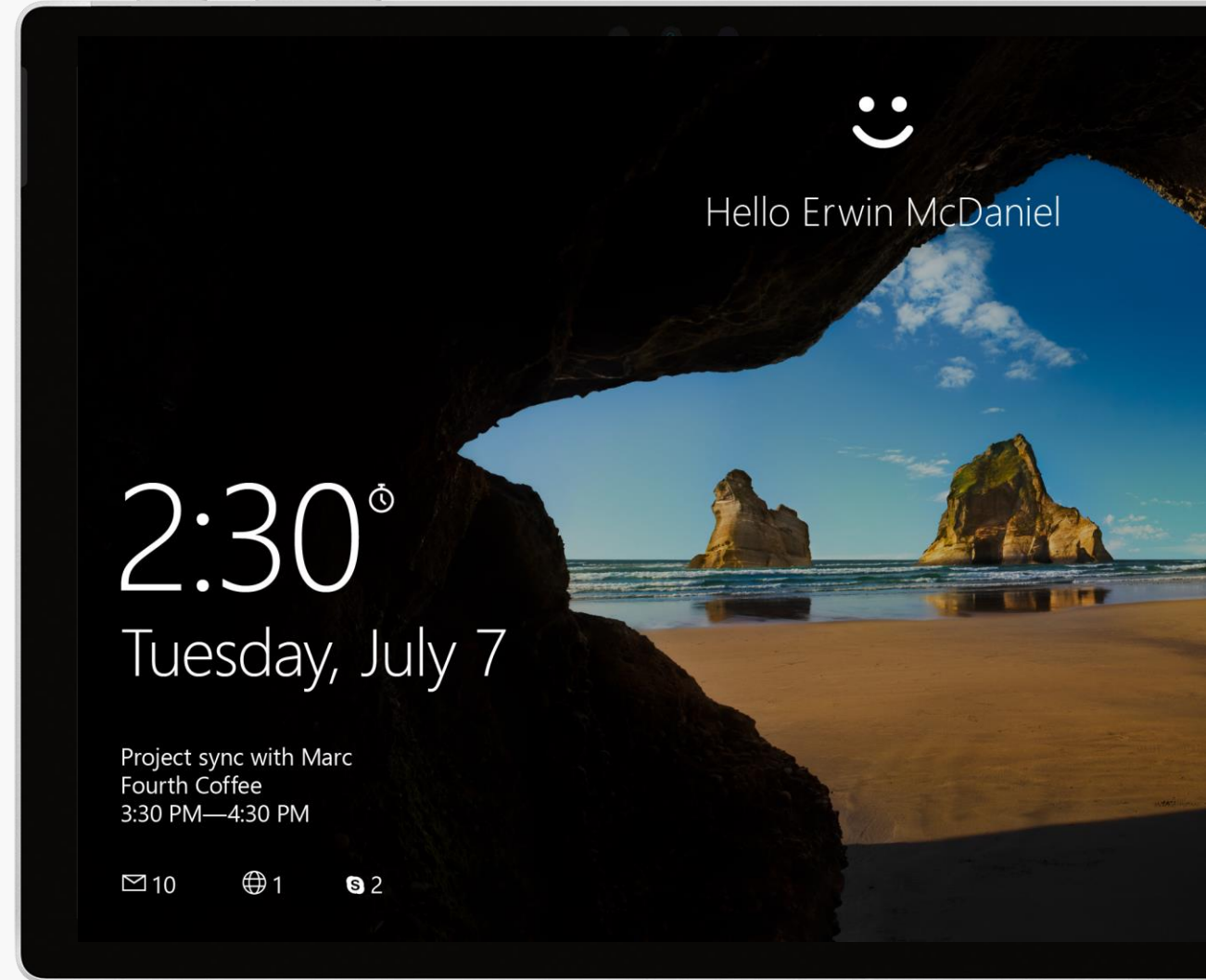
WINDOWS HELLO **FOR BUSINESS**

Passwordless strong authentication via multiple factors

- PC + PIN or Biometrics
- PC + Companion Device
- PC supported Biometrics: fingerprint & facial
- Companion Device can support other biometrics options (e.g.: EKG)

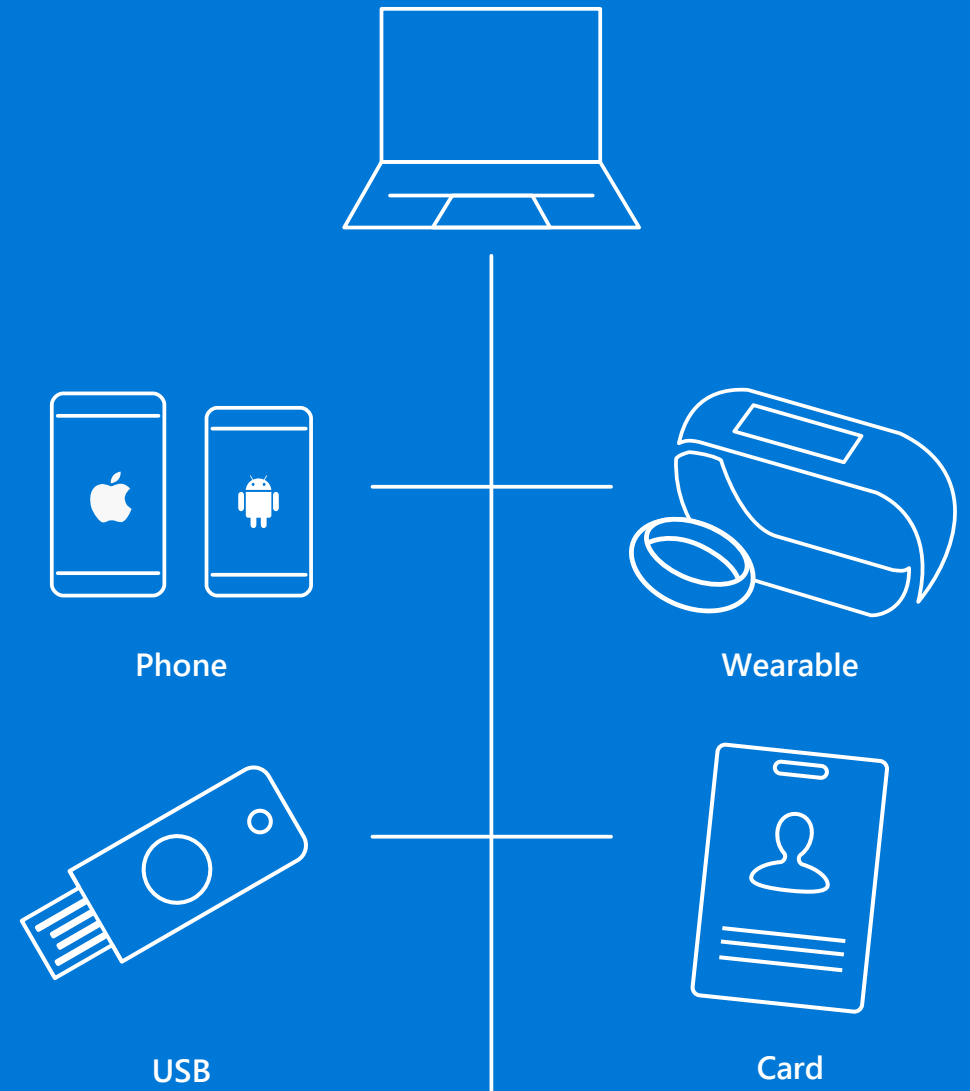
Supported on any Windows 10 device

>100 devices supporting biometrics



MAKING WINDOWS HELLO **WORK FOR EVERY ENVIRONMENT**

Windows Hello Companion Device Framework



WHAT IS FIDO?

Security on
premises and web

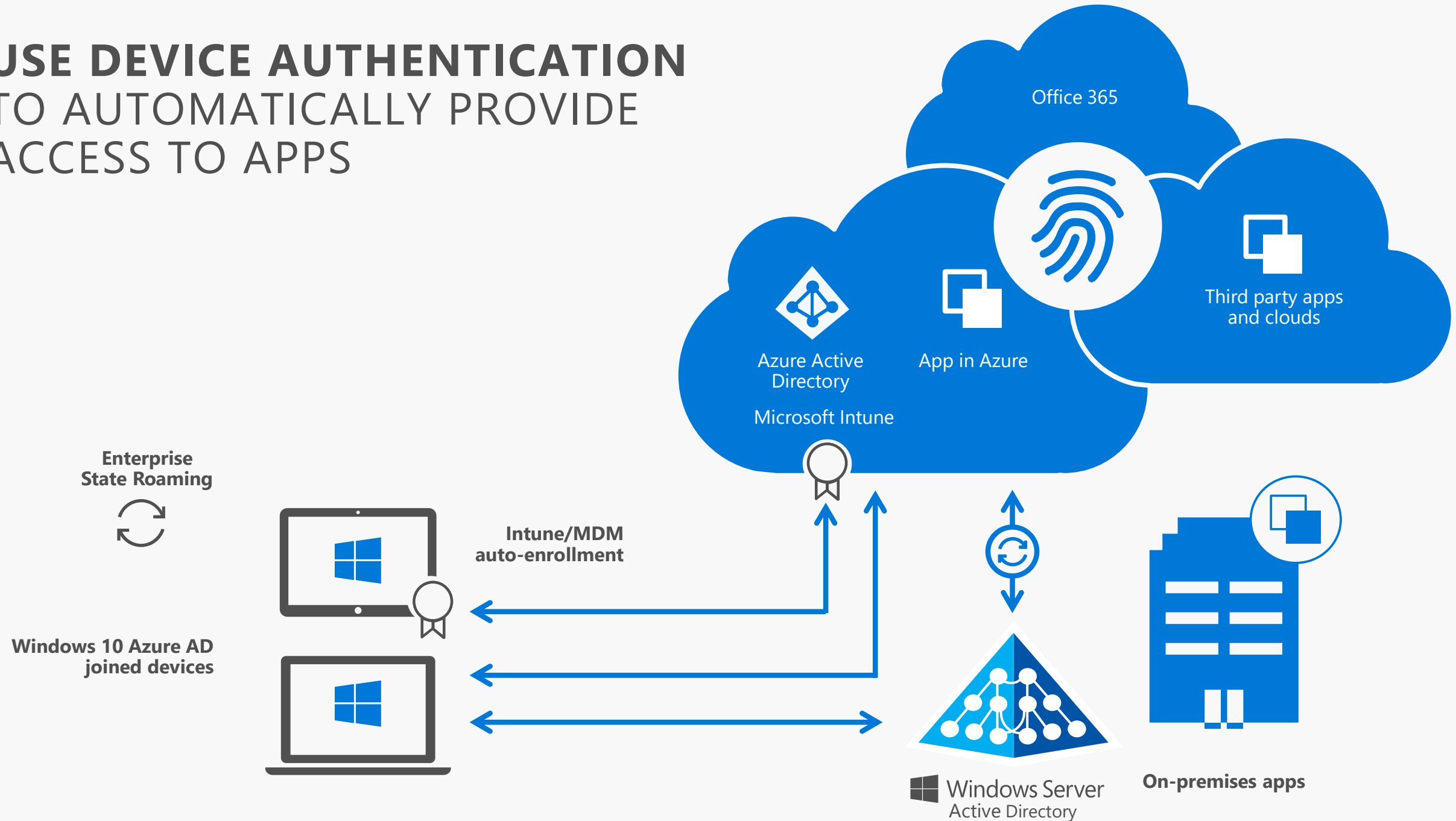
Secure mobile user
credentials

Secure
authentication

FIDO BOARD MEMBERS



USE DEVICE AUTHENTICATION TO AUTOMATICALLY PROVIDE ACCESS TO APPS



ACCESS ALL YOUR SAAS AND ON-PREMISES APPS

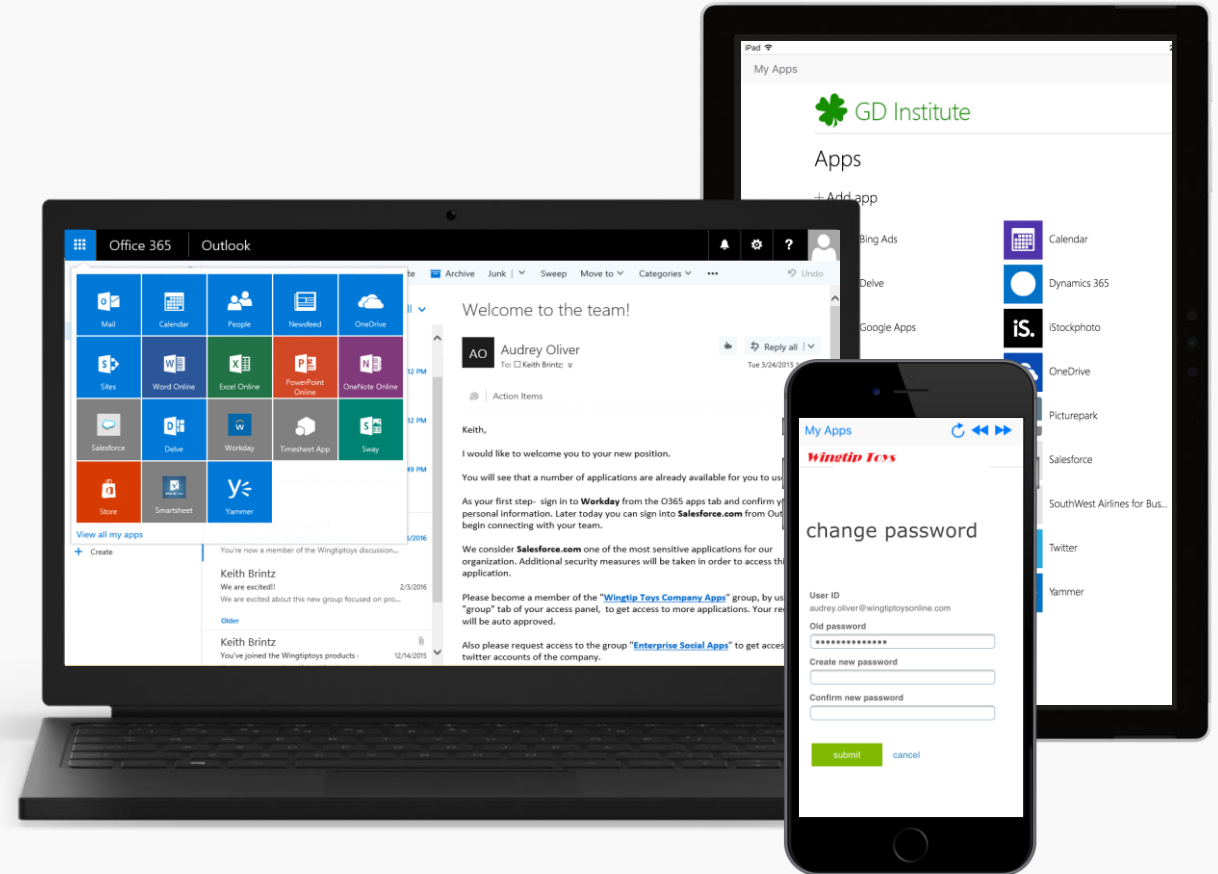
My apps portal

Integrated Office 365 app launching

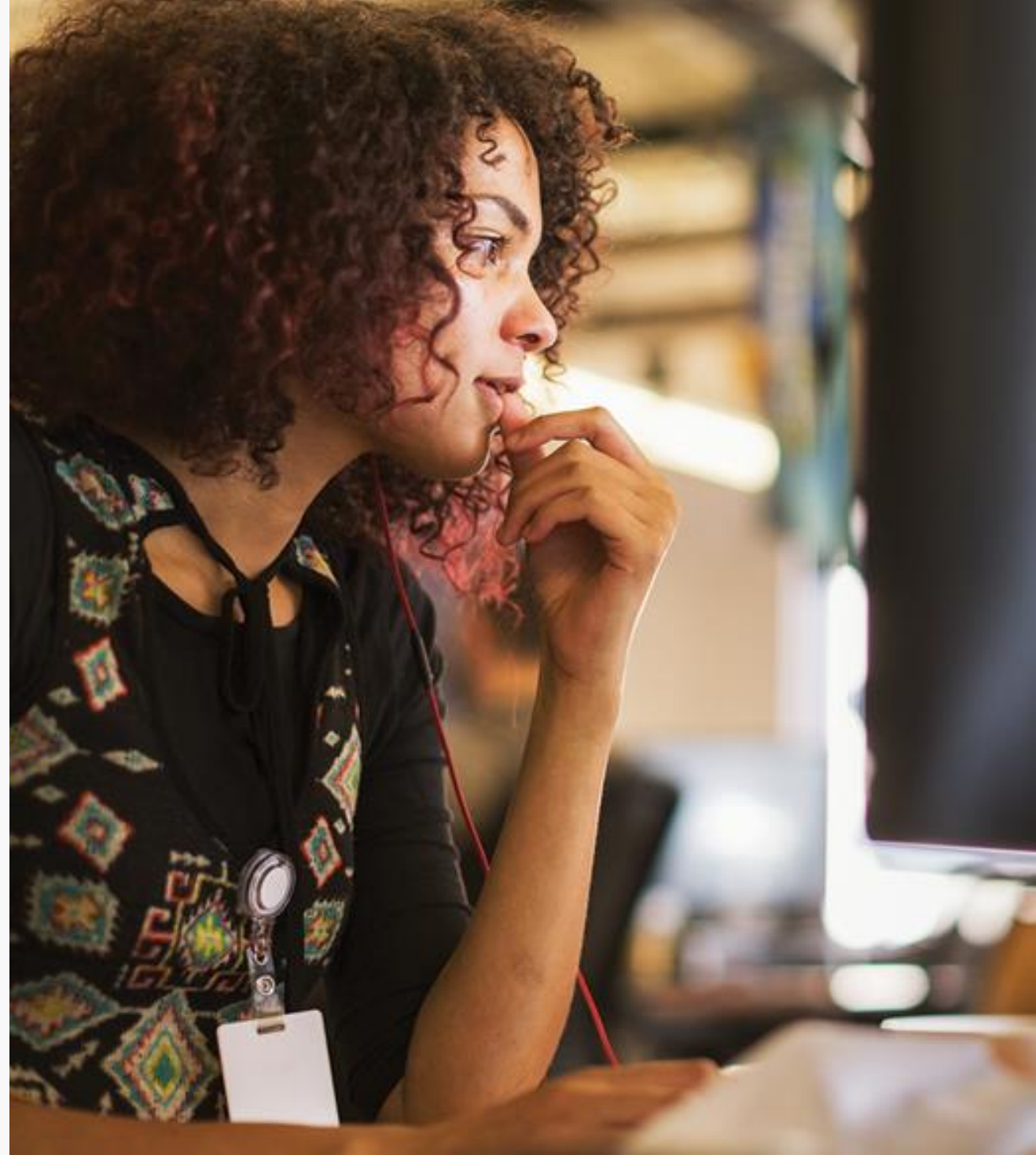
Manage your account, apps, and groups

Self-service password reset

Application access requests



HOW DO YOU PROTECT USER
& ADMINISTRATOR
CREDENTIALS?



Can you protect credentials against Pass-the-Hash and other similar classes of attacks?



Can you restrict and monitor the use of privileged credentials?



How are the credentials stored in your devices?

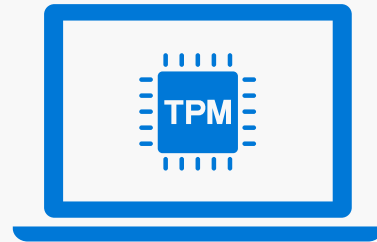


HOW HELLO PROTECTS CREDENTIALS



Strong authentication via multiple factors

- Uses two factors for authentication (e.g.: PC + PIN or Biometric)
- Asymmetrical Keys (i.e: Private/Public)



User credentials protected by hardware

- Hardware generated credential (keys)
- Credential isolated and protected by hardware

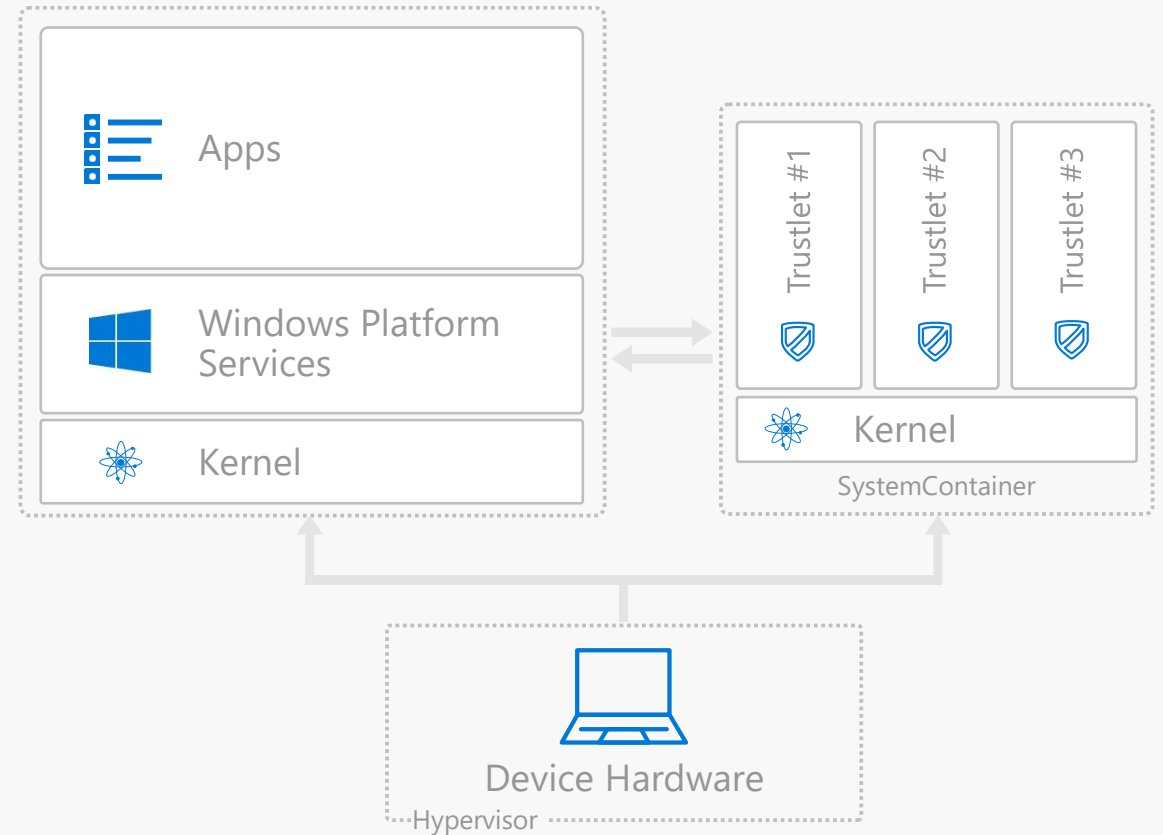


Secure biometrics

- Hardened biometric implementation in Windows & hardware
- Anti-spoofing and brute-force protection

HOW WINDOWS PROTECTS SINGLE SIGN-IN TOKENS

- #1 go-to attack for hackers: Pass the Hash
- Used in nearly every major breach for lateral movement
- Credential Guard uses Windows Defender System Guard to hardware isolate authentication and authentication data away from system
- Fundamentally breaks derived credential theft even when OS is fully compromised

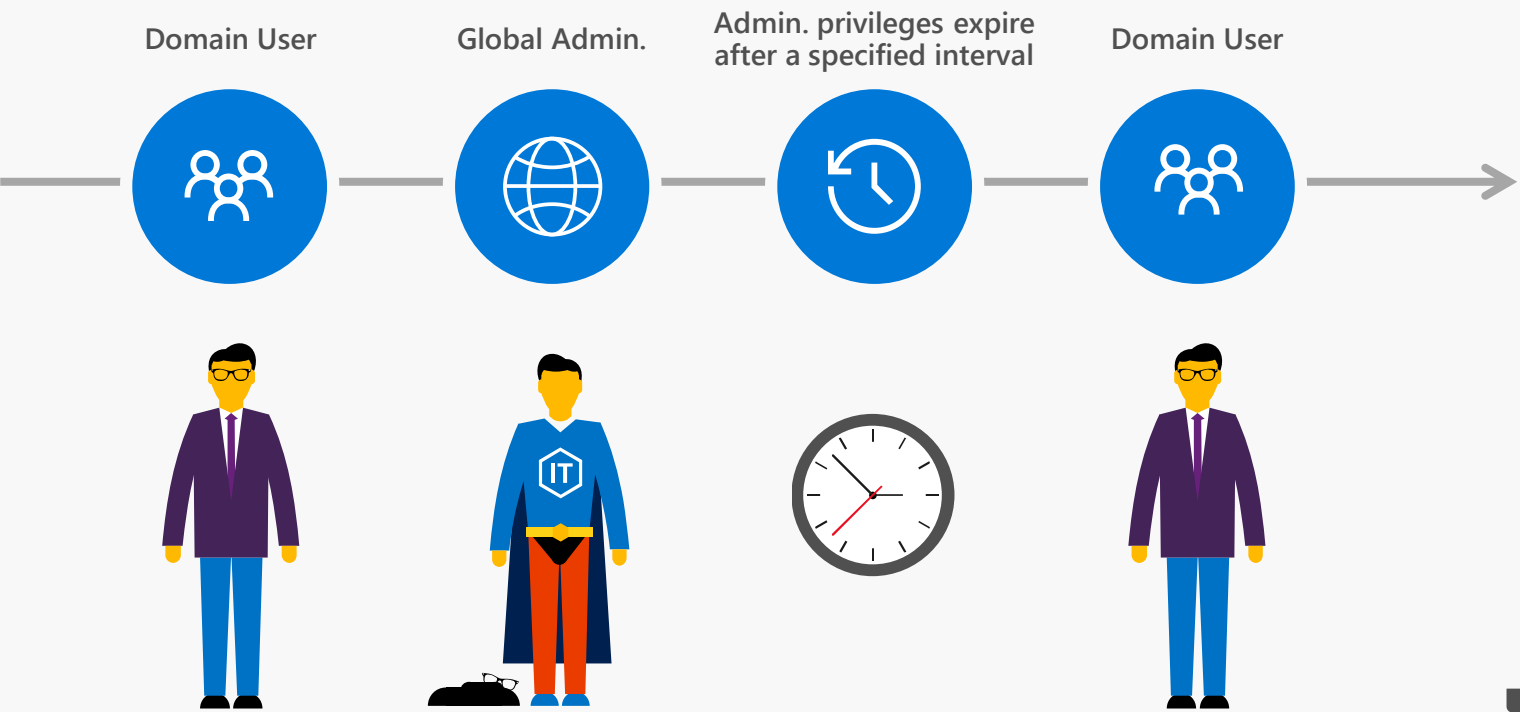


PROTECT PRIVILEGED IDENTITIES

Discover, restrict, and monitor privileged identities

Enforce on-demand, just-in-time administrative access when needed

Use Alert, Audit Reports and Access Review



GENERAL DATA PROTECTION REGULATION (GDPR)

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

HOW YOU GET STARTED:

1	Discover	Identify what personal data you have and where it resides
2	Manage	Govern how personal data is used and accessed
3	Protect	Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches
4	Report	Keep required documentation, manage data requests and breach notifications

“The breadth and scale of the Microsoft cloud was impressive. It had Office 365 on the desktop productivity side and Azure on the datacenter side. We could use Azure Active Directory Premium to provide single sign-on for all applications, from email to SAP, which would support our ‘invisible technology’ objective.”

RICHARD CAMMISH
CIO
Coats



COATS

A photograph of a Whole Foods Market produce section. The shelves are stocked with various fresh vegetables. At the top, there are bunches of bright orange carrots tied with purple bands. Below them, on the left, are several heads of green cabbage. In the center, there are two large bins of beets: one with dark purple beets and another with golden-yellow beets. To the right of the beets, there are more carrots. At the bottom of the frame, there are green Brussels sprouts. The Whole Foods Market logo is overlaid in the bottom left corner.

WHOLE FOODS MARKET

“Using the conditional access we check that specific conditions are met before authenticating a user and giving that person access to an application. Identity is the new firewall of the future. We can’t continue to use our old way of controlling application access, because business isn’t happening exclusively in our network anymore. With Azure Active Directory Premium, we can stay in control, no matter where our users roam.”

WILL LAMB

Infrastructure Coordinator
Whole Foods Market

“Security and data protection also improved with Windows 10. Device Guard and Credential Guard achieved the our objectives for securing devices, credentials, and data in a way that does not impact machine performance or end user productivity. Our end users are happy with the results.”

PAVAN AGRAWAL
Head of IT
WiPro





NEXT STEPS:

Learn more about Microsoft 365

<https://www.microsoft.com/en-us/microsoft-365/enterprise>

Try and evaluate Windows 10

www.Microsoft.com/windows10

Try and evaluate Microsoft Enterprise Mobility + Security

www.Microsoft.com/tryems

Try and evaluate Office 365

Office 365 E5 trial

Appendix

Introducing

Microsoft 365

A complete, intelligent solution to empower employees to be creative and work together, securely.

Office 365

Windows 10

Enterprise Mobility + Security



Microsoft 365

A complete, intelligent, secure solution to empower employees.



Unlocks
creativity



Built for
teamwork



Integrated
for simplicity



Intelligent
security





NEWSIGNATURE

“The key things that we're leveraging today are Azure Active Directory, Microsoft Intune, and Windows 10. It's really the intersection of those three products that allows us to be as effective as we possibly can be in this new world.”

“Our ability to have folks roam from one machine to the next, to the next is part of Azure AD. We wouldn't be able to do that as effectively if we were in that old mindset of having roaming profiles and folder redirection, and needing to connect back to an on-premises server to get your information.”

REED WIEDOWER
Chief Technology Officer
New Signature

One, integrated identity & access solution

	Simplify access	Verify users	Prevent ID Theft
User	 <ul style="list-style-type: none">✓ Windows Hello✓ SSO✓ MFA✓ SSPWR		<ul style="list-style-type: none">✓ Credential Guard
Admin	 <ul style="list-style-type: none">✓ Azure AD Join	<ul style="list-style-type: none">✓ MFA✓ SSPWR✓ Conditional Access	<ul style="list-style-type: none">✓ Privileged Mgmt