Microsoft

Microsoft CISO Workshop
3 - Identity and Access Management

Microsoft Cybersecurity Solutions Group

Microsoft CISO workshop

Your strategy

Lunch

Security management learnings and principles

Kickoff and introduction

Identity and access management

Threat protection

(A) Identify-Protect
(B) Detect-Respond-Recover

Information protection

Joint planning

TYPICAL STAKEHOLDERS

- Identity Security Architects
- Identity Architects
- Identity Operations Teams
- Collaboration/Productivity Lead

CISO WORKSHOP OBJECTIVE:
Learn how Microsoft can help you achieve your cybersecurity goals

Identity and Access Management

CONTEXT

HISTORY & USE CASES

TRENDS AND CHALLENGES

COST OF ATTACK

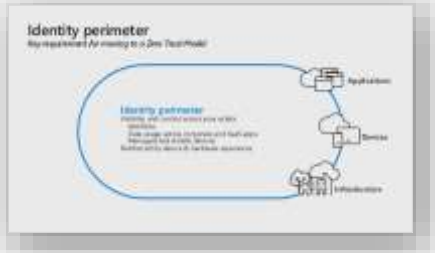
A COMPLETE STRATEGY

ACCOUNTS & PASSWORDS

ACCOUNT SECURITY

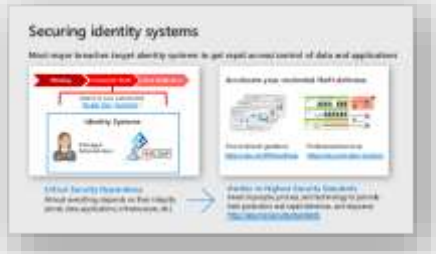
RETIRING PASSWORDS

IDENTITY PERIMETER



BUILDING AN IDENTITY PERIMETER

IDENTITY SYSTEMS



IDENTITY SYSTEM SECURITY

3RD PARTY ACCOUNT RISK

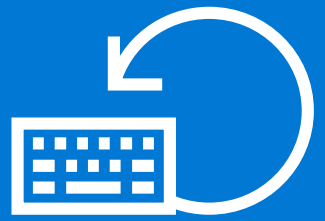
PARTNER ACCESS TO CORPORATE RESOURCES (B2B)

CUSTOMER IDENTITIES (B2C)

Evolution of IT, threats, and Microsoft Identity security

MICROSOFT IDENTITY APPROACH	Windows NT Domains	+ Enterprise Active Directory + Smartcard Authentication	+ Azure Active Directory + Passwordless Authentication + Hardware Credential Isolation
	Widespread Password Weakness and Re-use	**Credential Theft Attacks Mass Password Compromises**	
IDENTITY AND ACCESS TRENDS	Local Identities	Enterprise Single Sign On + 2 factor authentication	Hybrid and Federated Cloud Identity
INFORMATION TECHNOLOGY	 Mainframes + PCs	 + Datacenters + Mobile Devices	 + Cloud + Internet of Things (IoT)

Trends and challenges



Attackers using identity to bypass network controls

Phishing allow attackers to impersonate valid user Identities

Credential theft allows attackers to expand access by impersonating identities

Passwords aren't enough to protect identities

Single factor authentication (Passwords) without context isn't enough assurance

Attacks on credentials circumvent software assurances (without hardware isolation)

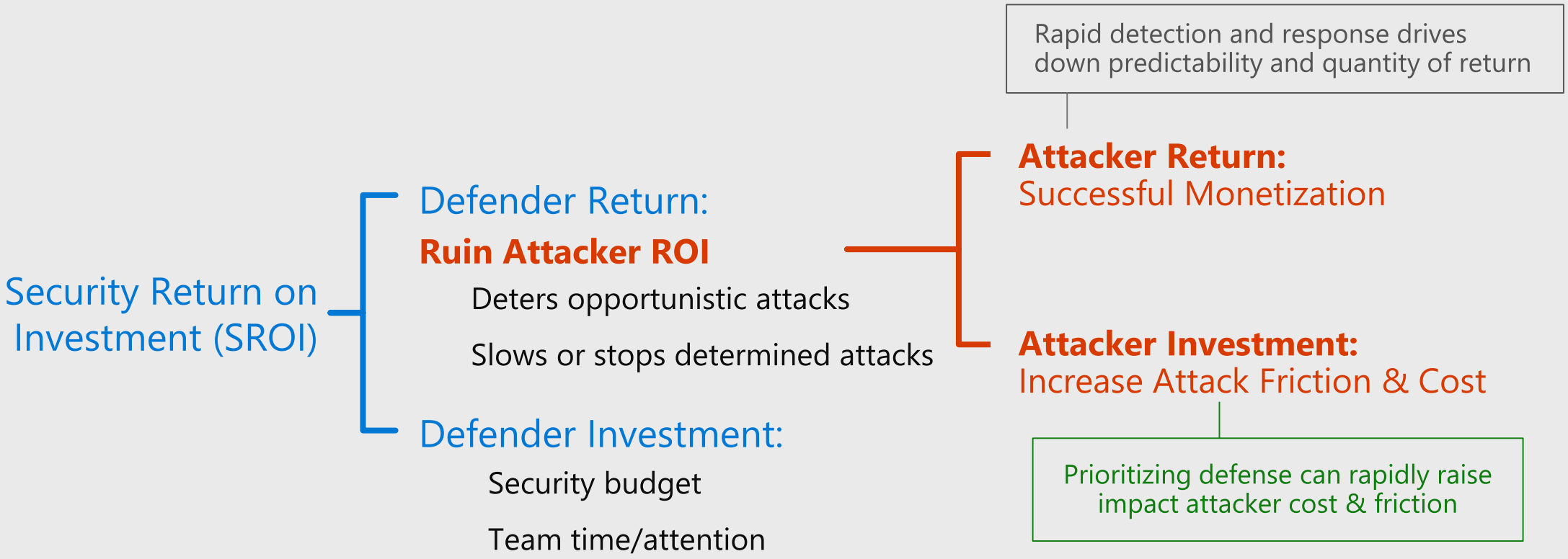
Identities being used outside network

Cloud, Mobile, and IoT assets are frequently beyond reach of enterprise firewalls

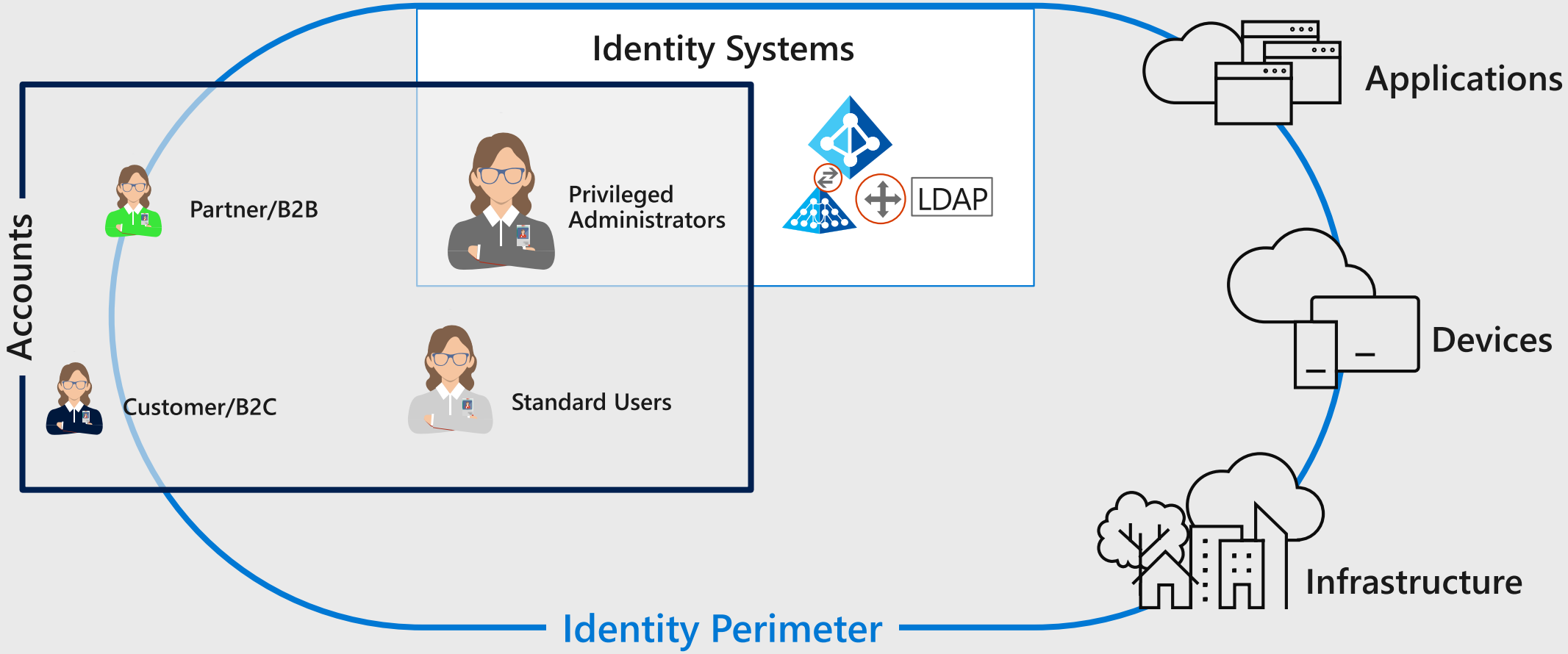
Identity and Access controls are inconsistent on different cloud services and devices

Disrupt Attacker ROI

Prioritize investments to maximize impact

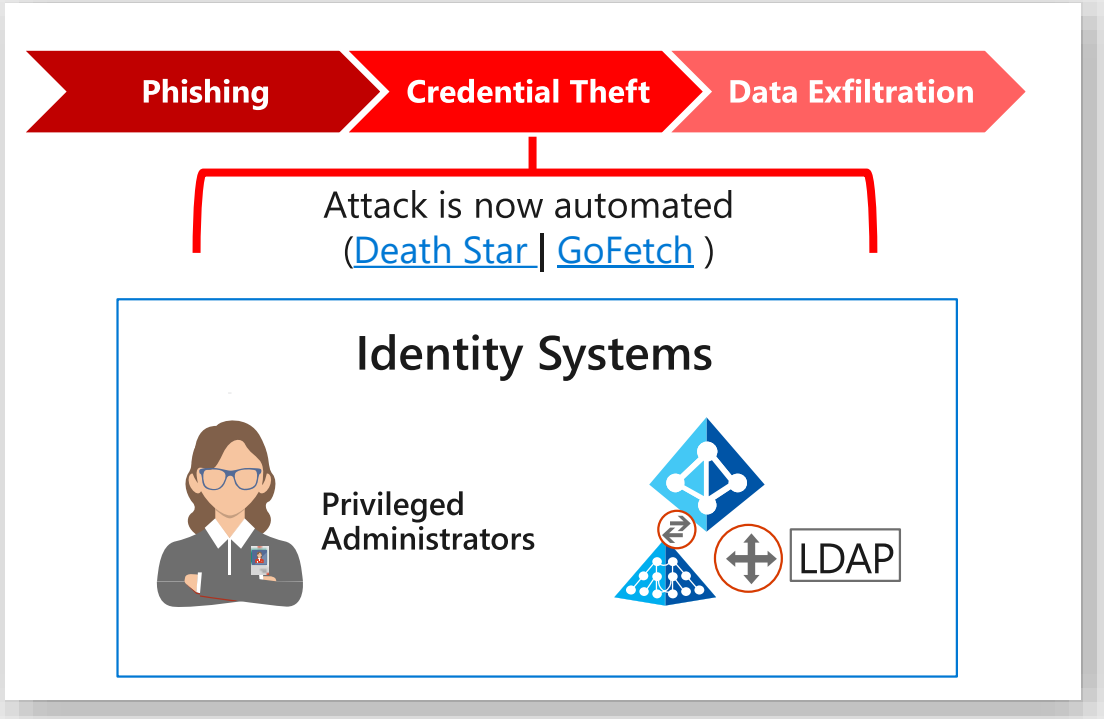


Identity and access management

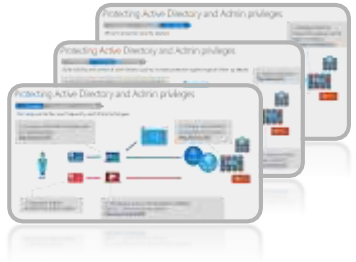


Securing identity systems

Most major breaches target identity systems to get rapid access/control of data and applications



Accelerate your credential theft defenses



Free technical guidance
http://aka.ms/SPAroadmap

Professional services
http://aka.ms/cyber-services

Critical Security Dependency

Almost everything depends on their integrity (email, data, applications, infrastructure, etc.)

Harden to Highest Security Standards

Invest in people, process, and technology to provide best protection and rapid detection, and response
http://aka.ms/securitystandards

Account security

Success factors to increase attack cost

Great experience

For **users, identity managers, and security**

Single Identity and Single Sign On (SSO)

Strong assurances

Additional Factors like biometrics and others

Increase context in authentication / authorization decisions

- **Time, date, geolocation**
- **Device integrity** and compliance
- **Known Bad** sources from threat intelligence

Behavior Analytics to understand normal profile *for that user/entity*

Hardware assurance for credentials stored on devices

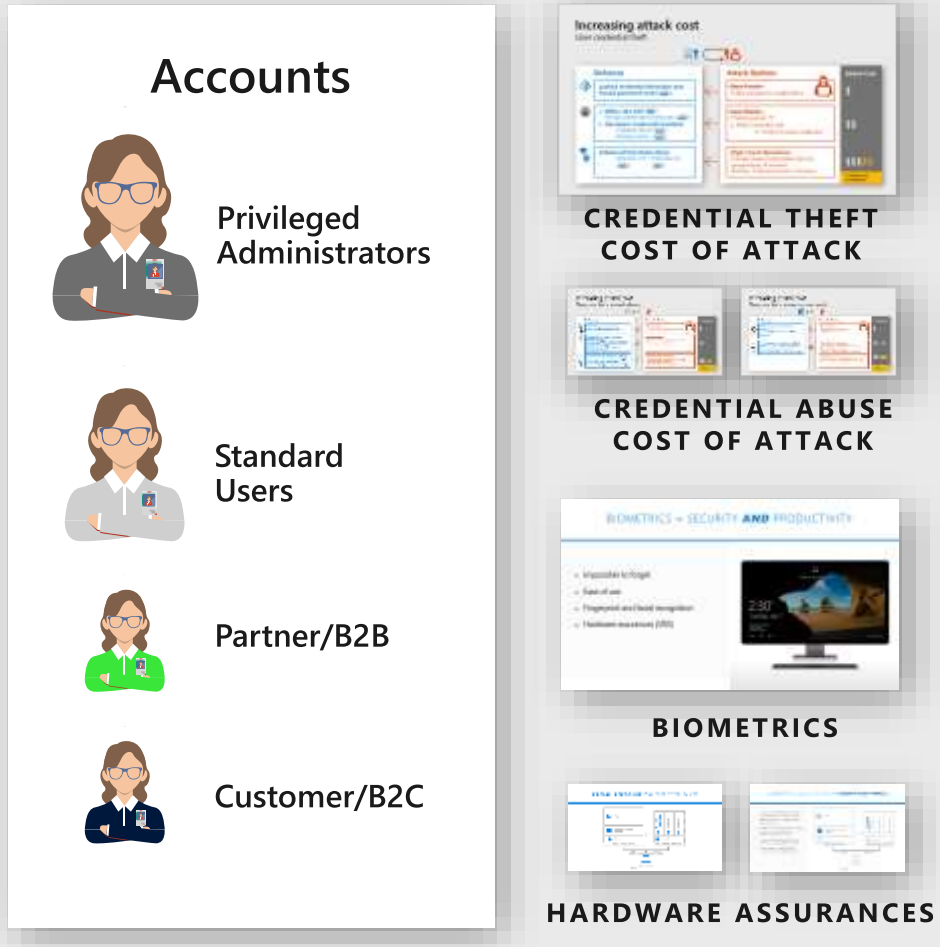
Flexible Access Levels

Allow for Low Risk

Increase Assurance (add MFA) based on risk factors

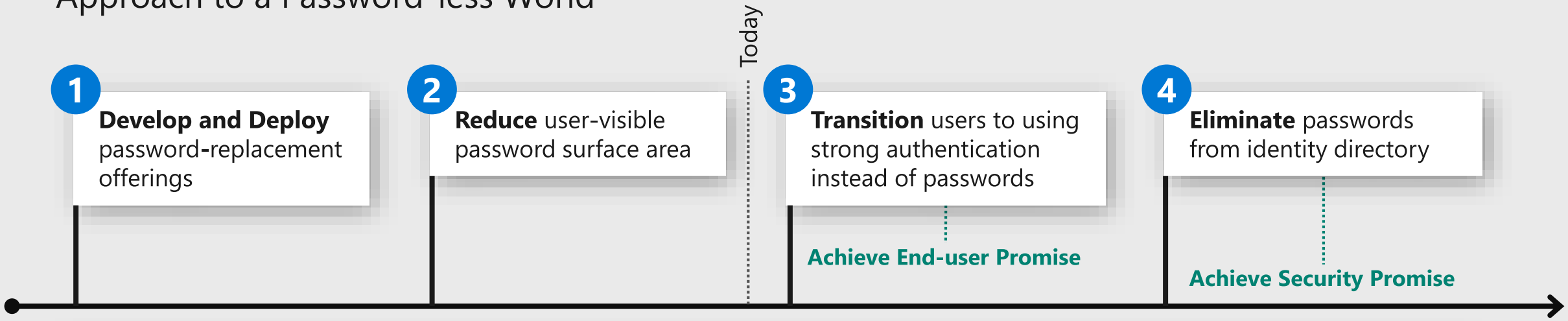
Decrease Access (Block download) based on risk factors

Force Remediation for high risks (compromised devices and accounts)



Eliminate Passwords through strong and multifactor authentication

Approach to a Password-less World



Windows Hello for Business
Available on all Windows 10 Machines today with improvements coming in RS4 and RS5

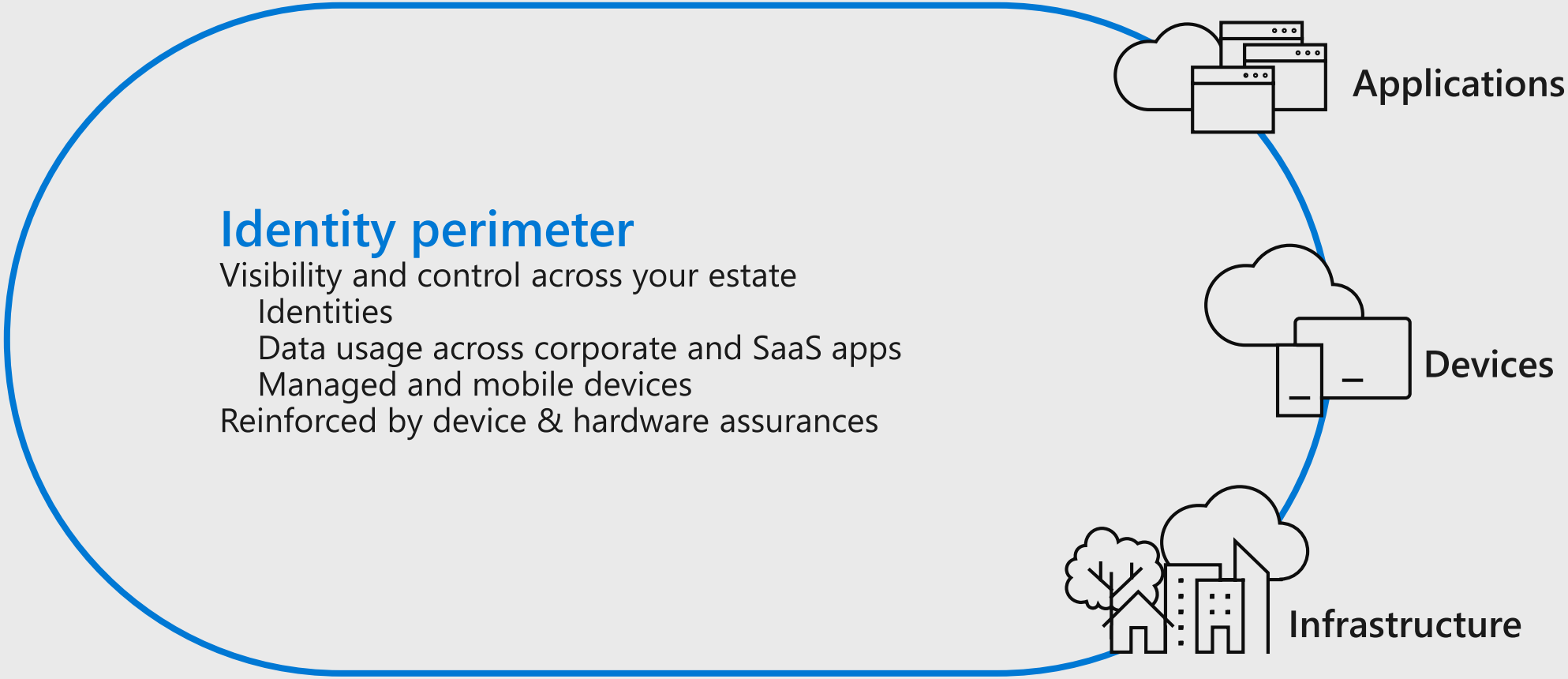
Microsoft Authenticator
Available today across all mobile platforms, integral in corporate bootstrapping of MFA

FIDO

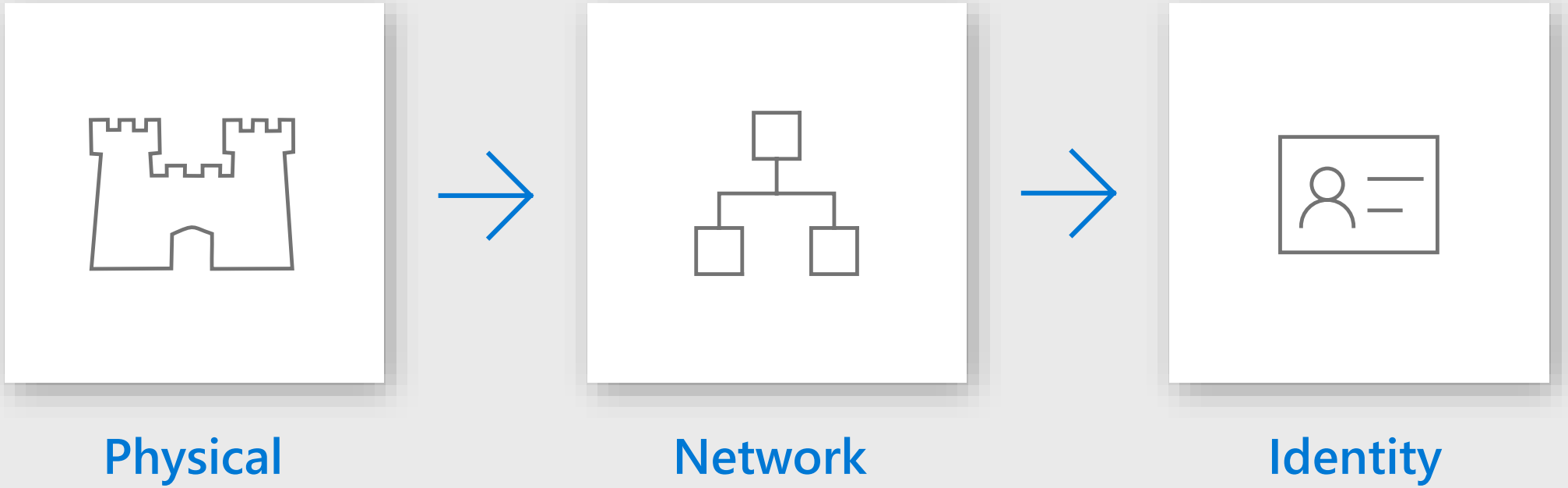
Microsoft + Third Party

Identity perimeter

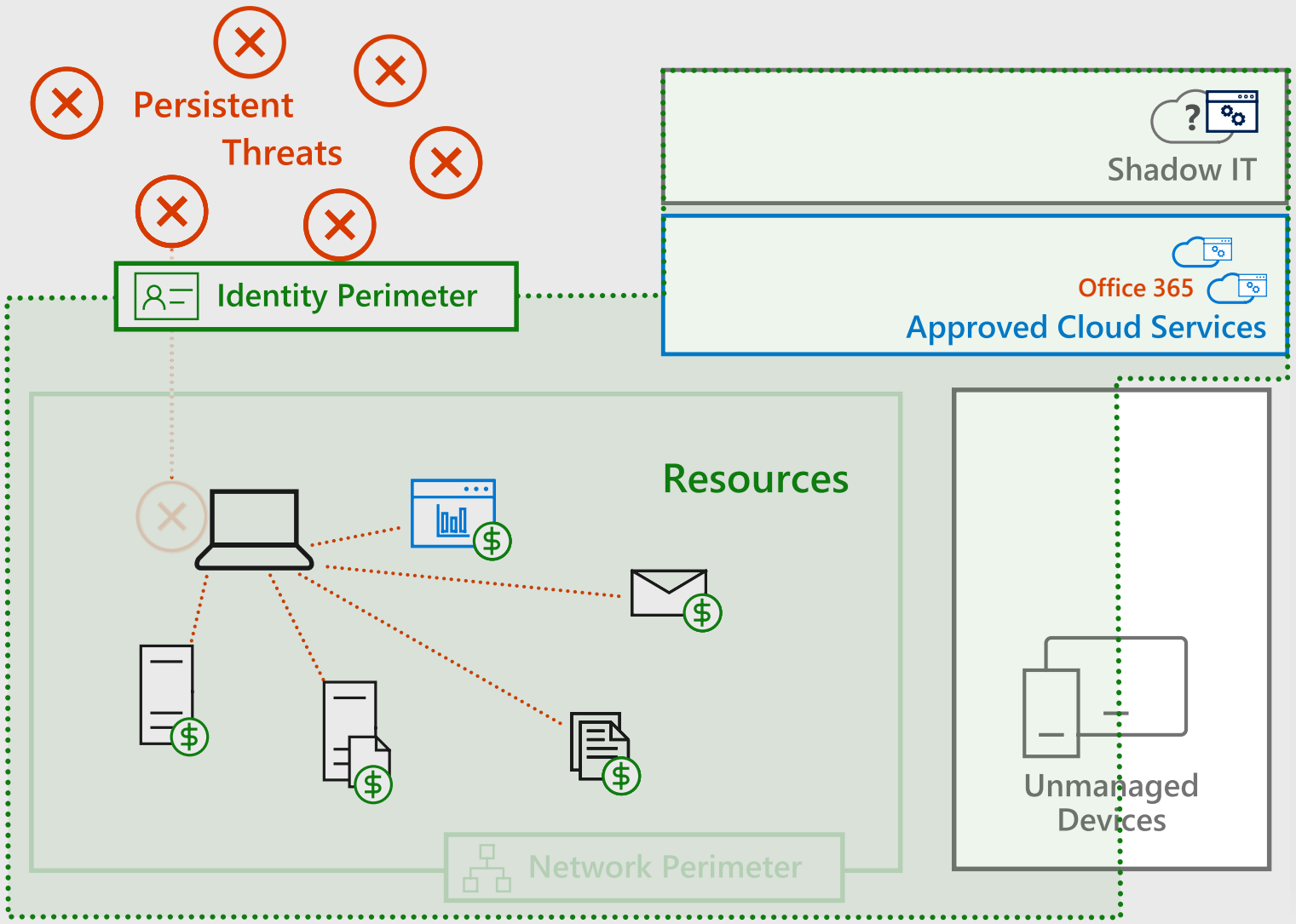
Key requirement for moving to a Zero Trust Model



Evolution of security perimeters



Modernizing the security perimeter



Network protects against classic attacks…

…but bypassed reliably with

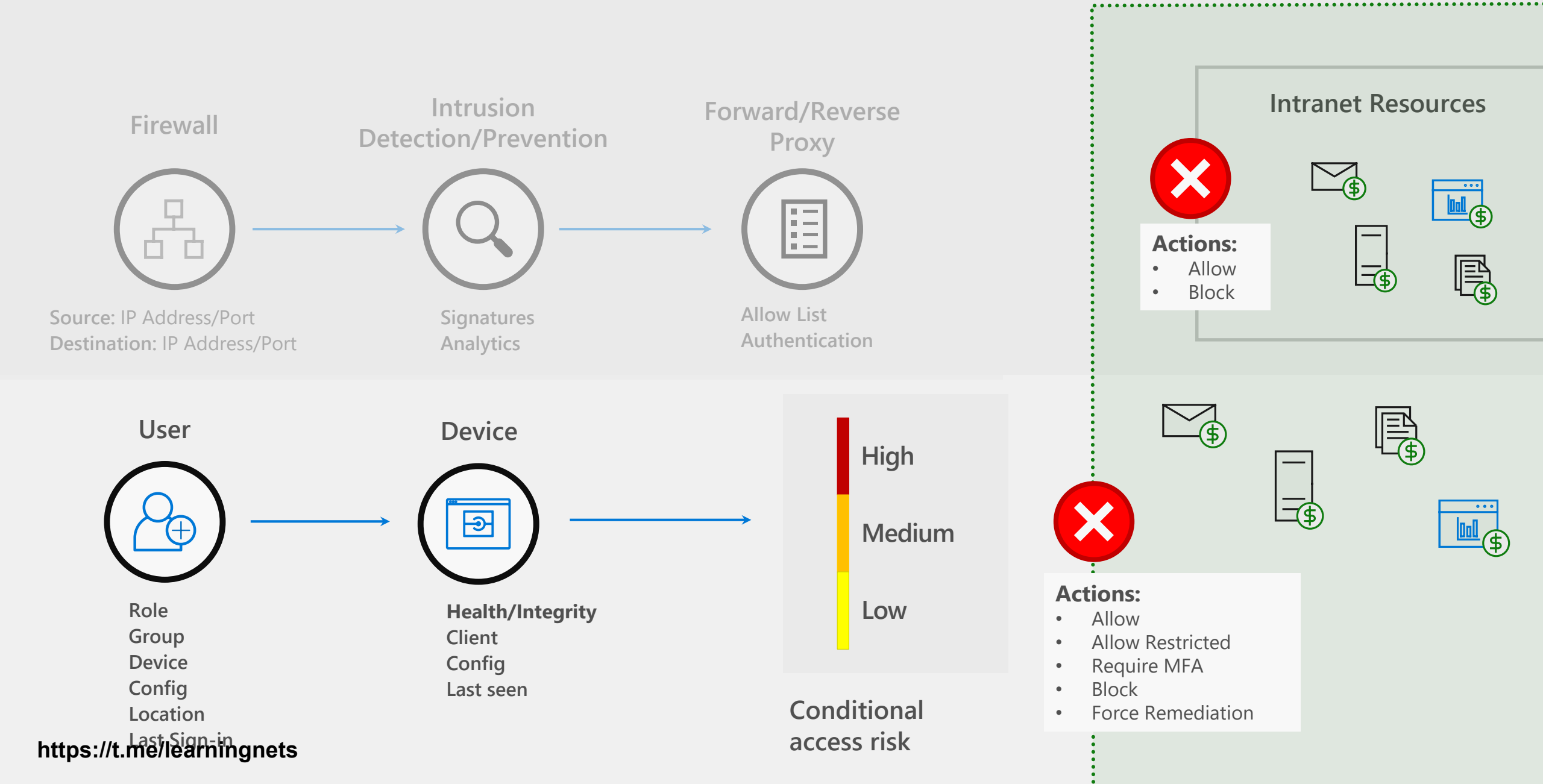
- Phishing
- Credential theft

\+ Data moving out of the network

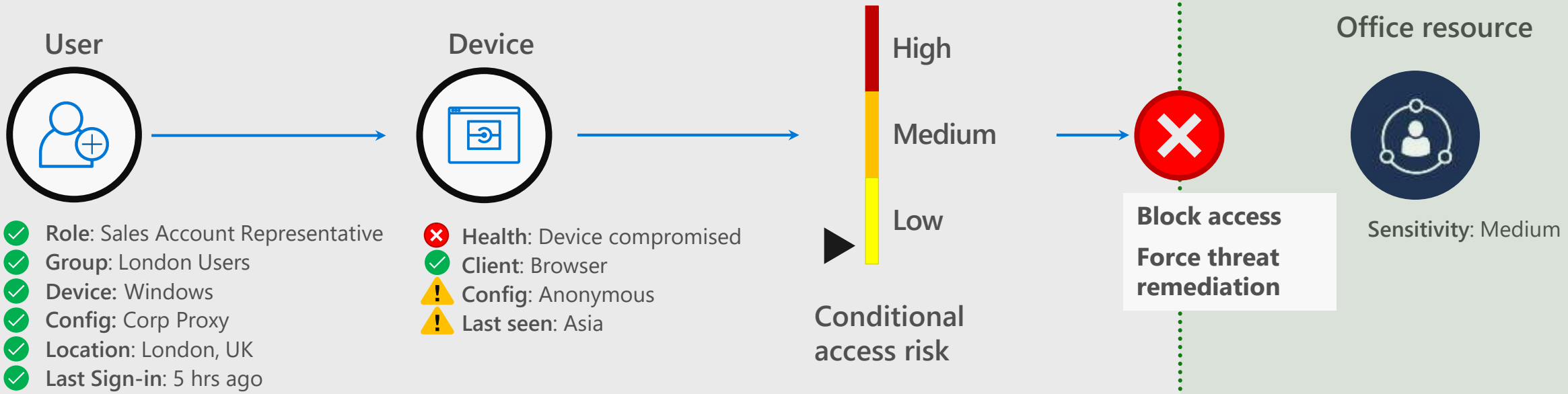
= Critical to build modern security perimeter based on Identity

- *Identity and Access Management* Strong Authentication + Monitoring and enforcement of policies
- *Strength from Hardware & Intelligence*– Auth & Access should consider device status, compromised credentials, & other threat intelligence

VISIBILITY AND CONTROL AT THE PERIMETER



Conditional Access Example



For insights into password spray and other modern attack patterns, see https://channel9.msdn.com/events/Ignite/Microsoft-Ignite-Orlando-2017/BRK3016

Malicious activity detected on device

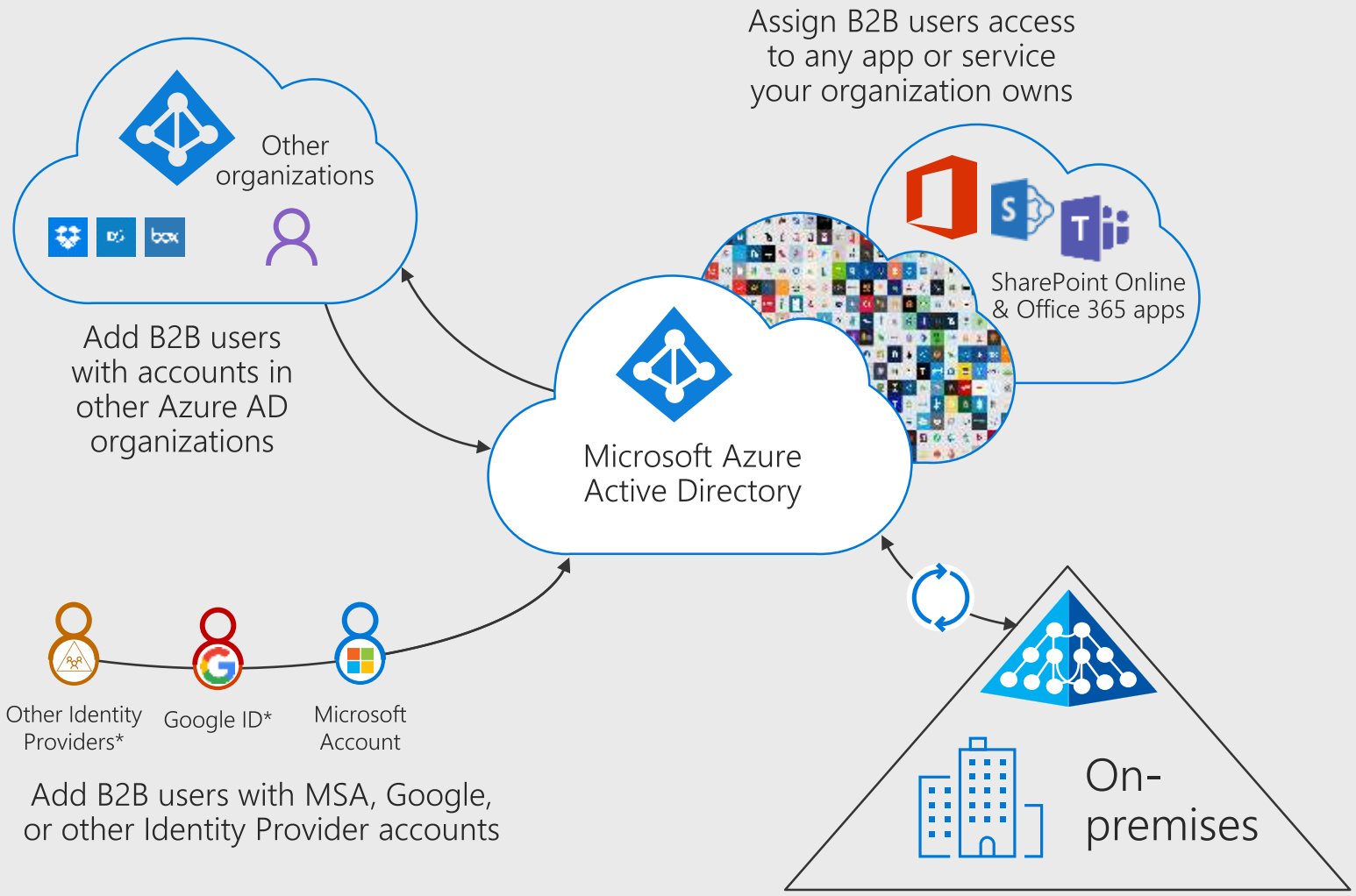
Anonymous IP

Unfamiliar sign-in location for this user

Identity and Access Management Use Cases

3 I need my customers and partners to access the apps they need from everywhere and collaborate seamlessly

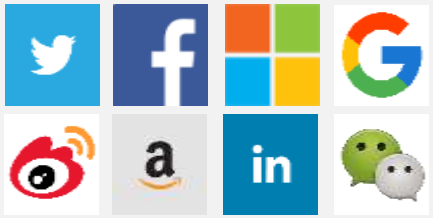
- Azure AD Connect
- B2B collaboration
- SSO to SaaS
- Self-Service capabilities
- Remote Access to on-premises apps
- Access Panel/MyApps
- Dynamic Groups
- Conditional Access
- Office 365 App Launcher
- Multi-Factor Authentication



Azure Active Directory B2C

Customers

Social IDs

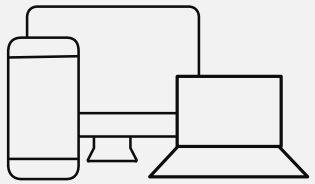


Business & Government IDs

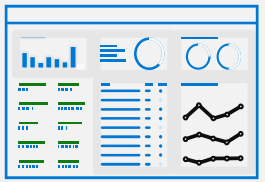
Azure AD B2C

- Securely authenticate customers with their preferred identity provider
- Provide branded registration and login experiences
- Capture login, preference, and conversion data for customers

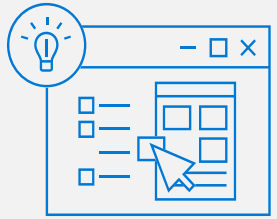
Business



Apps



Analytics



CRM and Marketing Automation

Identity and access management

Identity systems

Critical dependency for most or all security assurances

Harden to Highest security standards

Accounts

Great experience

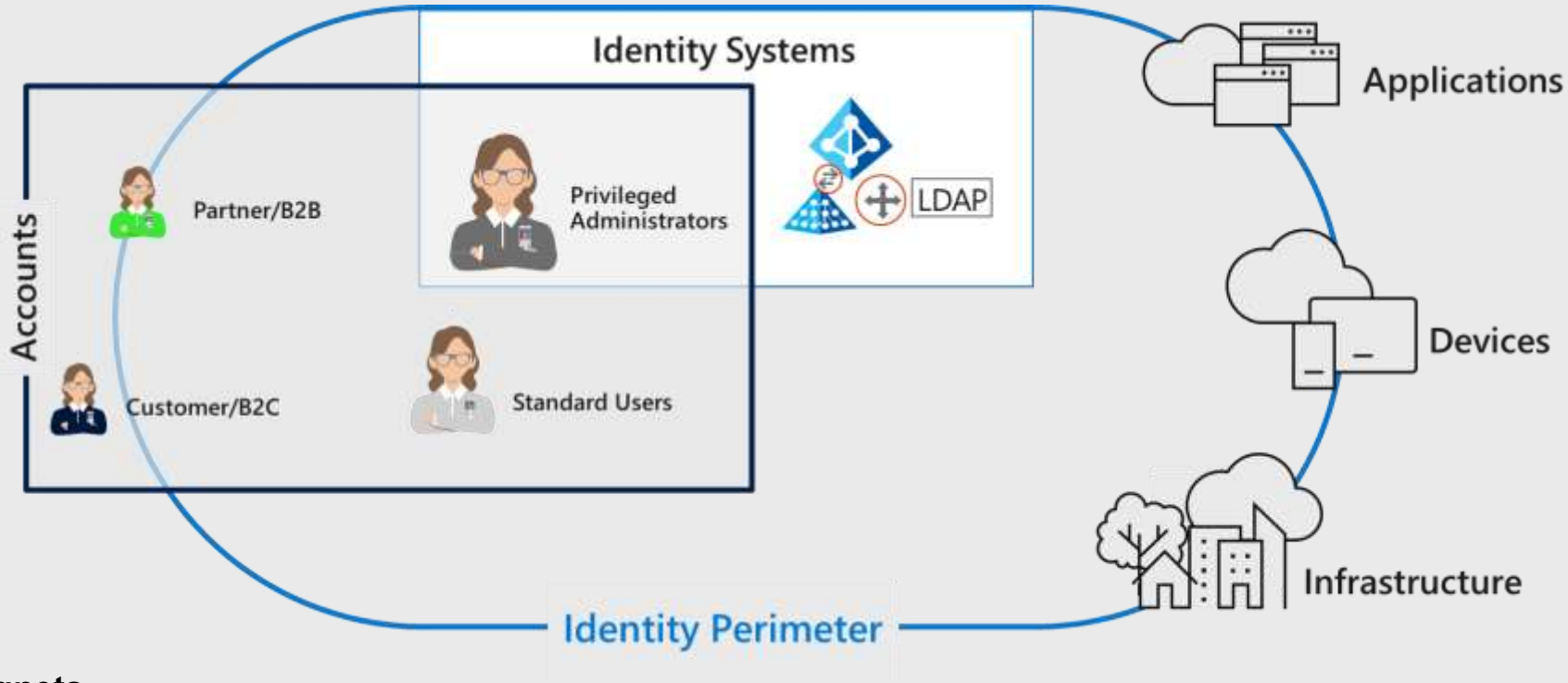
Strong assurances of identity

Policy control and response

Identity perimeter

Visibility and control across your estate

- Identities
- Sensitive data usage
- Corporate and SaaS applications
- Managed and mobile devices



Questions?

Microsoft

Reference

Additional Resources

- Azure AD and ADFS best practices
  - https://cloudblogs.microsoft.com/enterprisemobility/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/
- Microsoft Password Guidance
  - https://aka.ms/passwordguidance
- NIST Updated Password Guidance

- Ignite Session: Azure Active Directory risk-based identity protection
  - https://channel9.msdn.com/events/Ignite/Microsoft-Ignite-Orlando-2017/BRK3016