Microsoft

Microsoft CISO Workshop
3 - Identity and Zero Trust User Access

Microsoft Cybersecurity Solutions Group

Video Presentation of this can be found at

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/ciso-workshop-module-3

Microsoft CISO workshop

Kickoff and introduction

Your strategy

Lunch

Security management learnings and principles

Identity and Zero Trust Architecture

Threat protection

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

Information protection

Joint planning

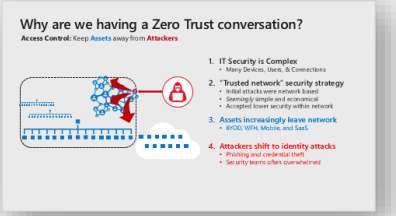
TYPICAL STAKEHOLDERS

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

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

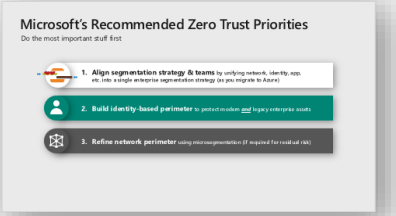
Identity and Zero Trust User Access

CONTEXT



IDENTITY & ZERO TRUST HISTORY

ZERO TRUST DEFINITION & MODELS

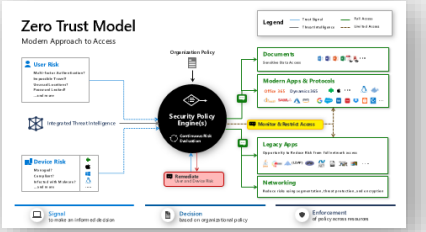


STRATEGY & PRIORITIES

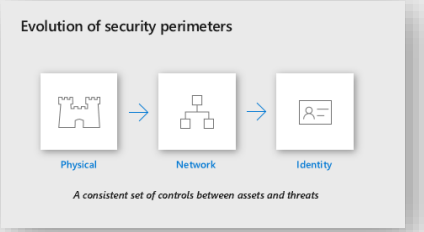
ACCOUNTS & PASSWORDLESS

ACCOUNT SECURITY & GOING PASSWORDLESS

ZERO TRUST ARCHITECTURE

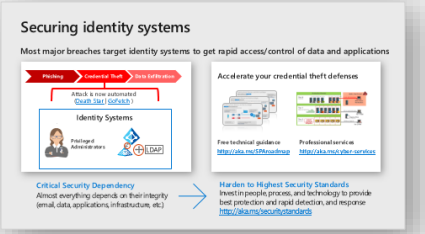


ZT ACCESS CONTROL REFERENCE ARCHITECTURE



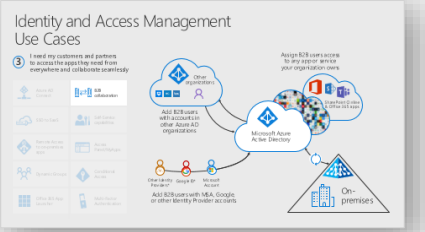
BUILDING AN IDENTITY PERIMETER

IDENTITY SYSTEMS

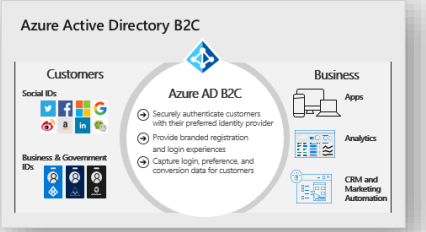


IDENTITY SYSTEM SECURITY

3RD PARTY ACCOUNT RISK



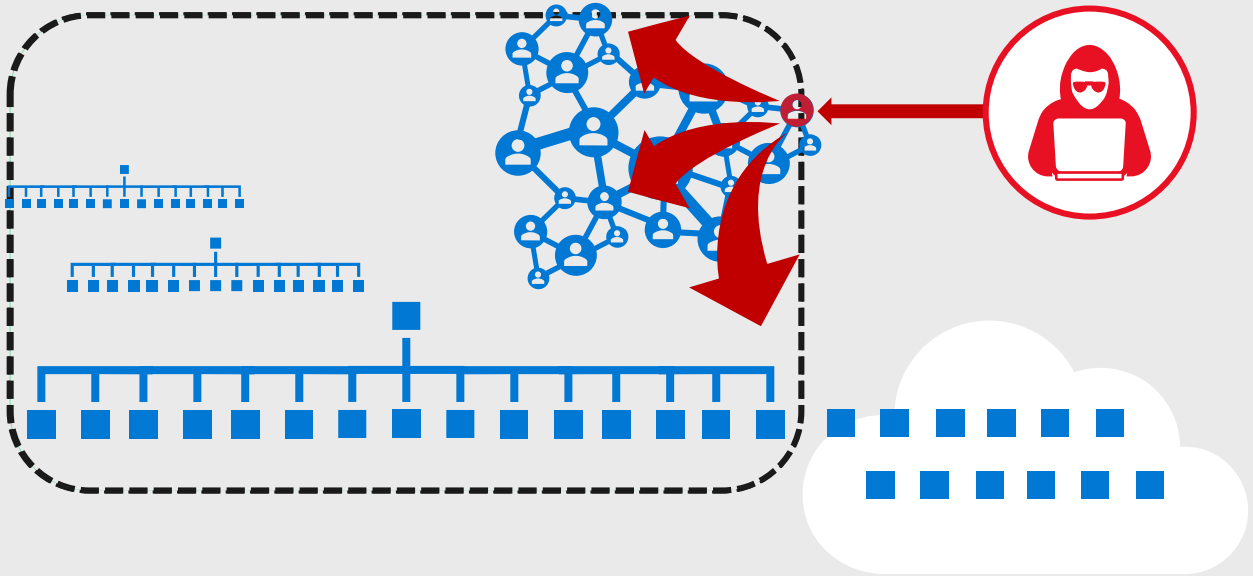
PARTNER ACCESS TO CORPORATE RESOURCES (B2B)



CUSTOMER IDENTITIES (B2C)

Why are we having a Zero Trust conversation?

Access Control: Keep **Assets** away from **Attackers**



1. **IT Security is Complex**
   - Many Devices, Users, & Connections
2. **"Trusted network" security strategy**
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within network
3. **Assets increasingly leave network**
   - BYOD, WFH, Mobile, and SaaS
4. **Attackers shift to identity attacks**
   - Phishing and credential theft
   - Security teams often overwhelmed

This “Zero Trust” idea has been evolving for a while

2004
Jericho Forum
Formally Established

~2004
Network Access
Control (NAC)
Architectures

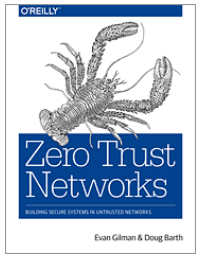
2010
Forrester coins
“Zero Trust” Term

2014
Microsoft Advocates
“Assume Breach”

2014
BeyondCorp
Published

2016
Conditional
Access Released

2017



Ongoing
Passwordless
Initiative

Slow mainstream adoption for both network identity models:

Network – Expensive and challenging to implement
Google’s BeyondTrust success is rarely replicated

Identity – Natural resistance to big changes
Security has a deep history/affinity with networking

Zero Trust Principles

Verify Explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, data classification, and anomalies.

Least Privilege

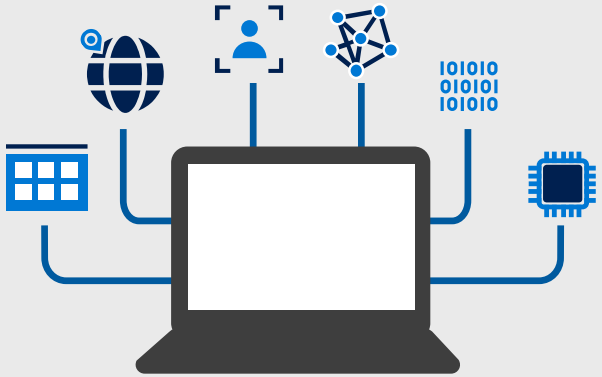
Minimize user access with Just-In-Time and Just-Enough Access (JIT/JEA), risk-based adaptive polices, and data protection which protects data and productivity.

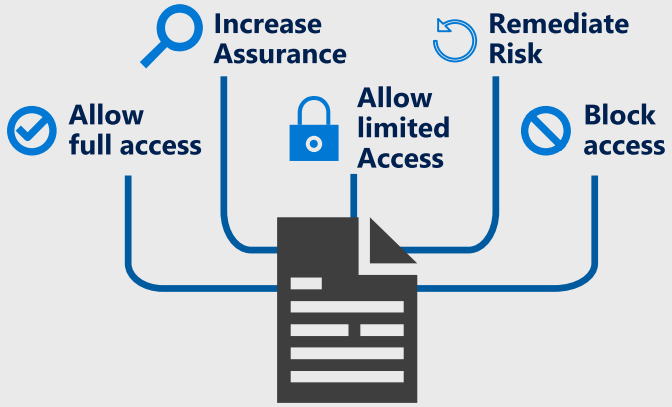
Assume Breach

Minimize scope of breach damage and prevent lateral movement by segmenting access via network, user, devices and application awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility and drive threat detection.

Zero Trust Access Control Strategy

Never Trust. Always verify.





Signal

to make an informed decision

Device Risk
- Device Management
- Threat Detection
- and more…

User Risk
- Multi-factor Authentication
- Behavior Analytics
- and more…

Decision

based on organization's policy

Apply to inbound requests

Re-evaluate during session

Enforcement

of policy across resources

Modern Applications
SaaS Applications
Legacy Applications
And more…

Zero Trust Access Control Paradigms

	Network	Identity
Control Plane	*Apply Zero Trust Policy to **network connections***	*Apply Zero Trust Policy to **access requests***
Industry Proponents	Network Security Vendors	Identity Vendors
Overall Effect	**Microsegmentation** enhances existing network perimeter by shrinking "trusted network" to each server / IP address.	**Dual Perimeter –** Adds an identity perimeter where "inside" is defined by authentication and authorization. *Coexists with network perimeter*
Applicability/Scope	**Limited to networks** controlled by customer. Doesn't protect modern SaaS and PaaS assets. *Microsegmentation approach varies by vendor*	**Applies to all assets –** • Natively protects modern cloud assets • Protects legacy intranet assets via proxy
Differentiation	**Scope of assets** where zero trust is enforced **Threat Intelligence** signal Integration	Integration of **Behavior Analytics (UEBA)** risk signal Use of **ML** across large datasets decisions
Common Components	Evaluate trust signals for Devices & User Identities with per application policy	

Microsoft focuses on protecting modern and legacy assets as well as integration of ML, UEBA, and massive diverse threat intelligence

Microsoft's Recommended Zero Trust Priorities

Do the most important stuff first

1. **Align segmentation strategy & teams** by unifying network, identity, app, etc. into a single enterprise segmentation strategy (as you migrate to Azure)

2. **Build identity-based perimeter** to protect modern ***and*** legacy enterprise assets

3. **Refine network perimeter** using microsegmentation (if required for residual risk)

Integrating Zero Trust with Strategic Initiatives

Closely related to other initiatives

Zero Trust Identity Architecture
Establish Identity Perimeter with Conditional Access to Resources

SOC Modernization
Shift Tooling and Processes to Endpoint, Identity, and Application Layers

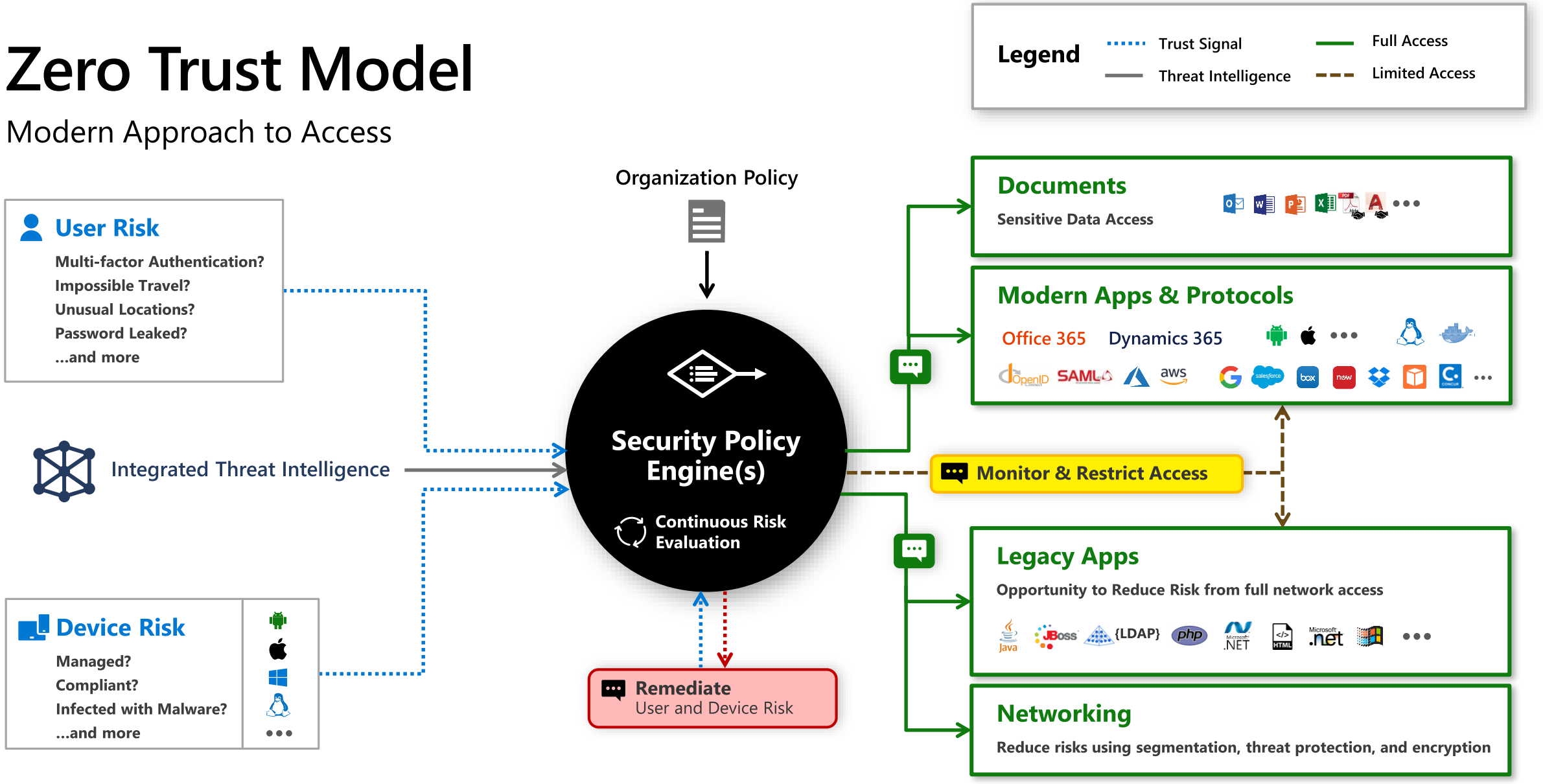
Secure Administration
Infrastructure/Datacenter access for admins

Network Transformation
- *Internet-only clients / Firewalls for Datacenters onl*
- *Evaluate Microsegmentation*

Resource Modernization
Enable ZT Access to Legacy Apps

Zero Trust Model

Modern Approach to Access



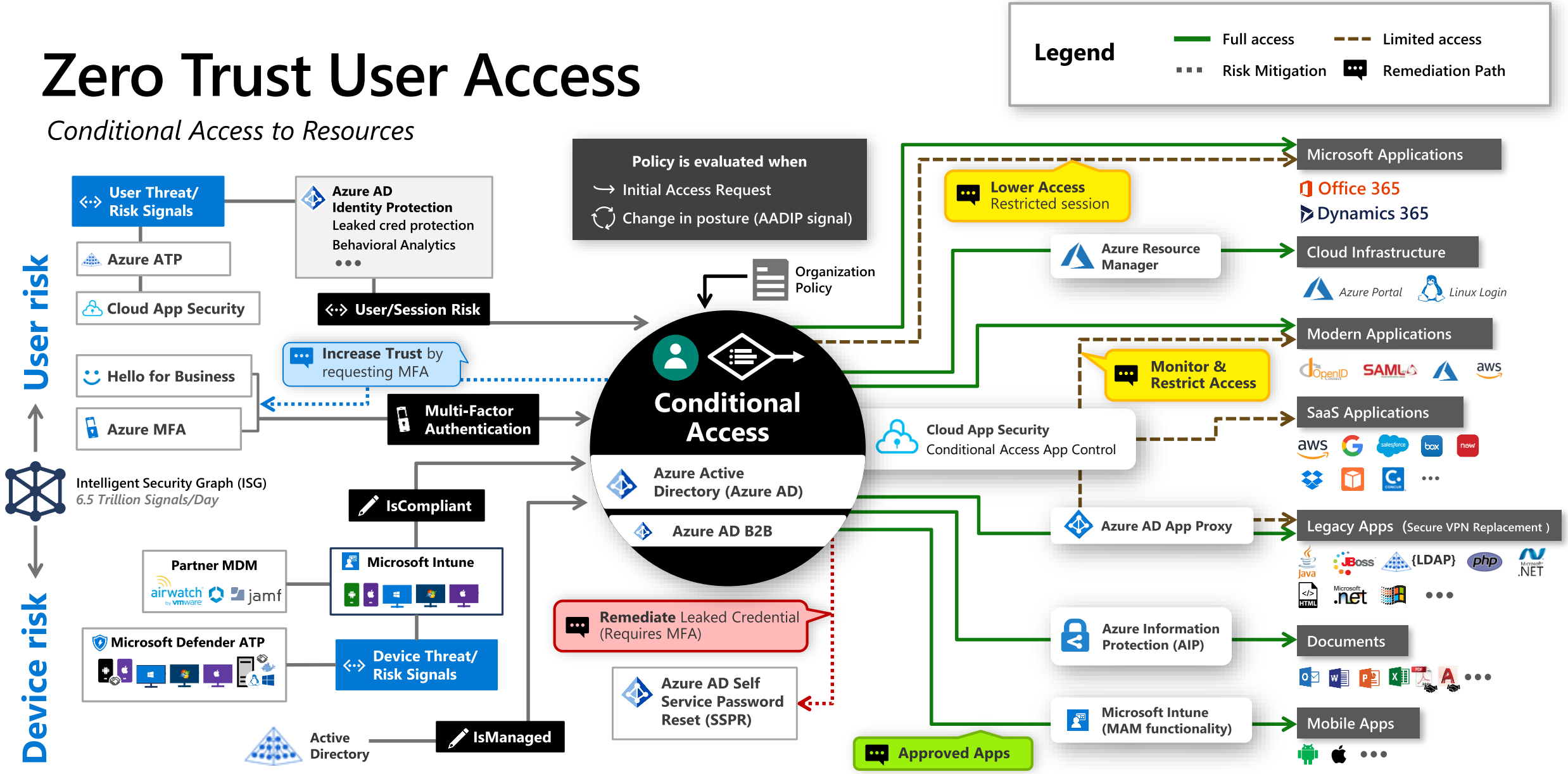
Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

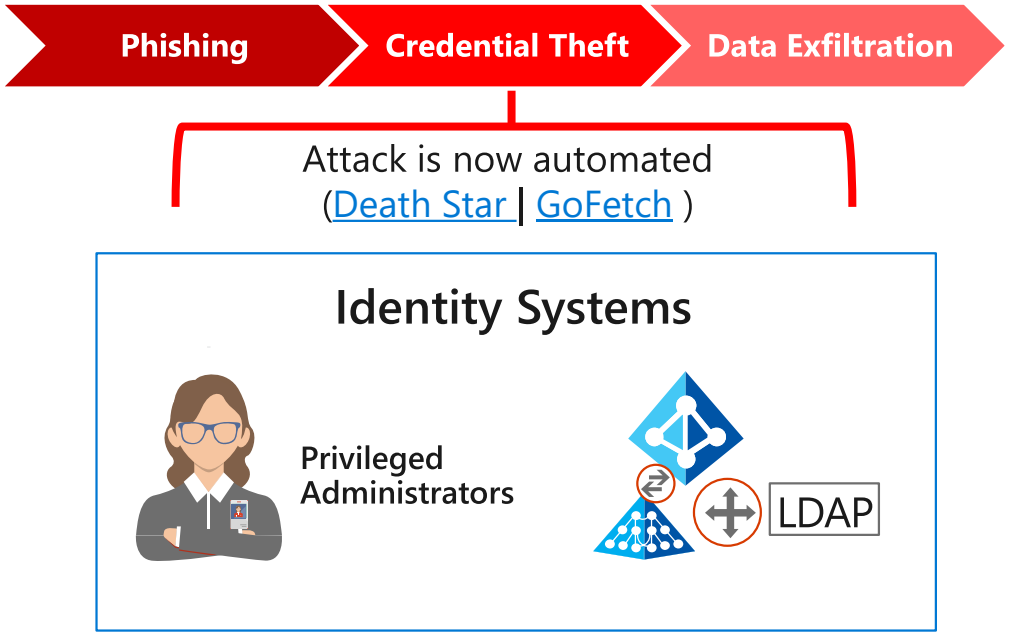
Zero Trust User Access

Conditional Access to Resources

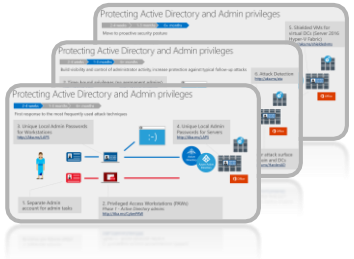


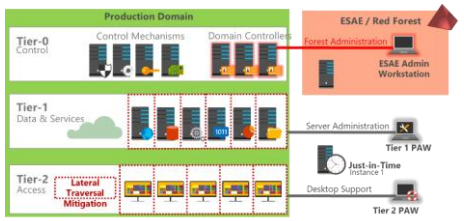
Securing identity systems

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)

Accounts

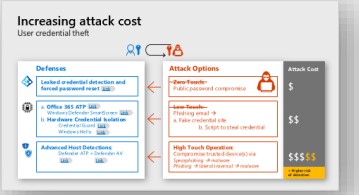
Privileged Administrators

Standard Users

Partner/B2B

Customer/B2C

COST OF ATTACK



CREDENTIAL THEFT COST OF ATTACK

CREDENTIAL ABUSE COST OF ATTACK

BIOMETRICS

HARDWARE ASSURANCES

Eliminate Passwords through strong and multifactor authentication

Approach to a Password-less World

Today

1. **Develop and Deploy** password-replacement offerings
2. **Reduce** user-visible password surface area
3. **Transition** users to using strong authentication instead of passwords
4. **Eliminate** passwords from identity directory

Achieve End-user Promise

Achieve Security Promise

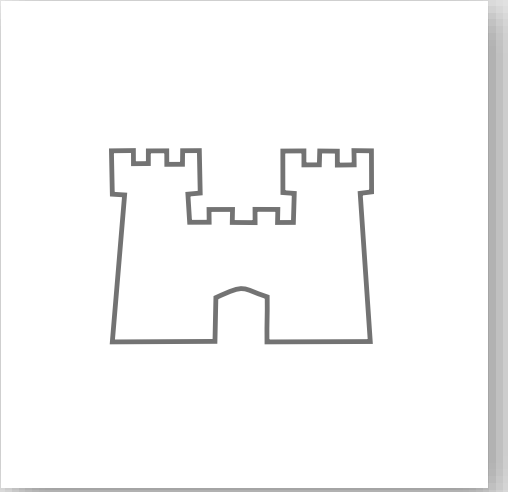
Windows Hello for Business
Available on all Windows 10 Machines today with improvements coming in RS4 and RS5

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

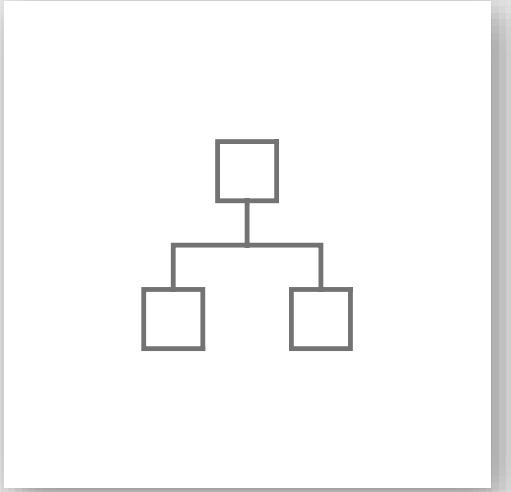
FIDO

Microsoft + Third Party

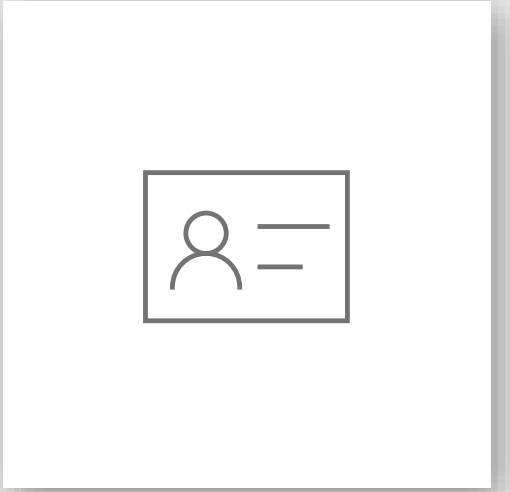
Evolution of security perimeters



Physical



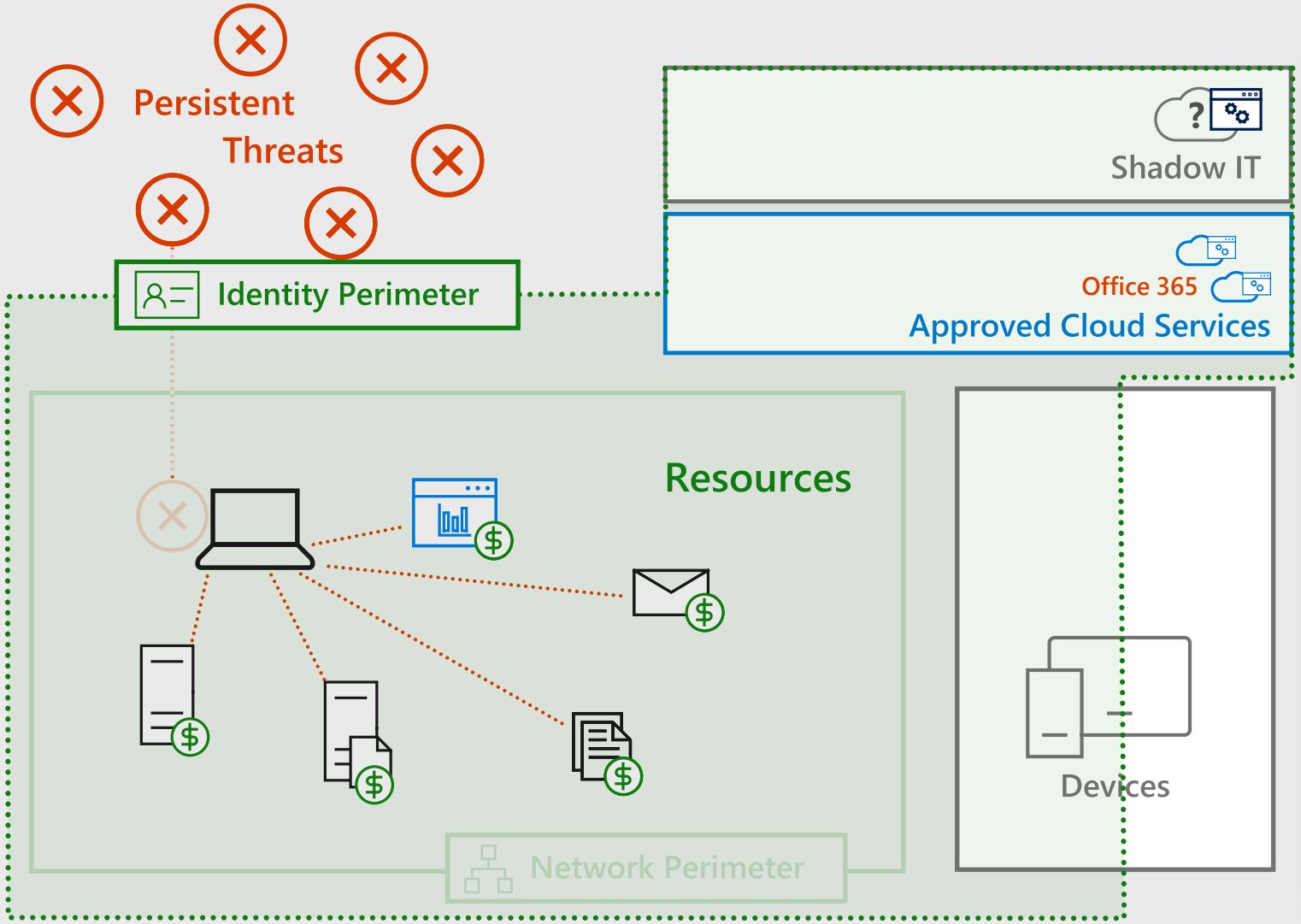
Network



Identity

A consistent set of controls between assets and threats

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

Firewall

Source: IP Address/Port
Destination: IP Address/Port

Intrusion Detection/Prevention

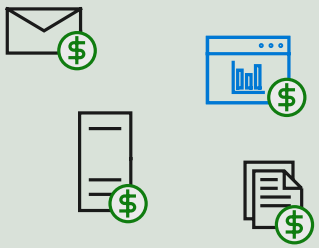
Signatures
Analytics

Forward/Reverse Proxy

Allow List
Authentication

Intranet Resources

Actions:
- Allow
- Block

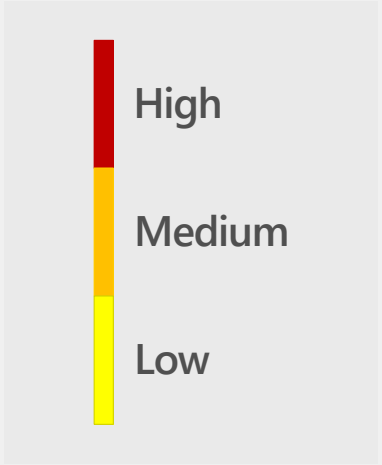


User

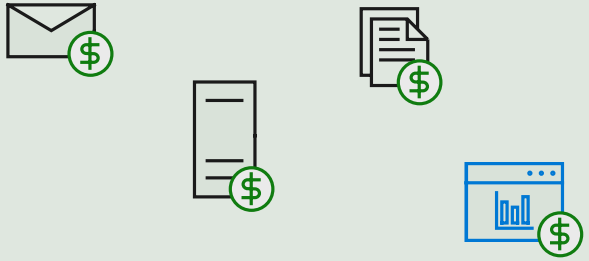
Role
Group
Device
Config
Location
Last Sign-in

Device

Health/Integrity
Client
Config
Last seen

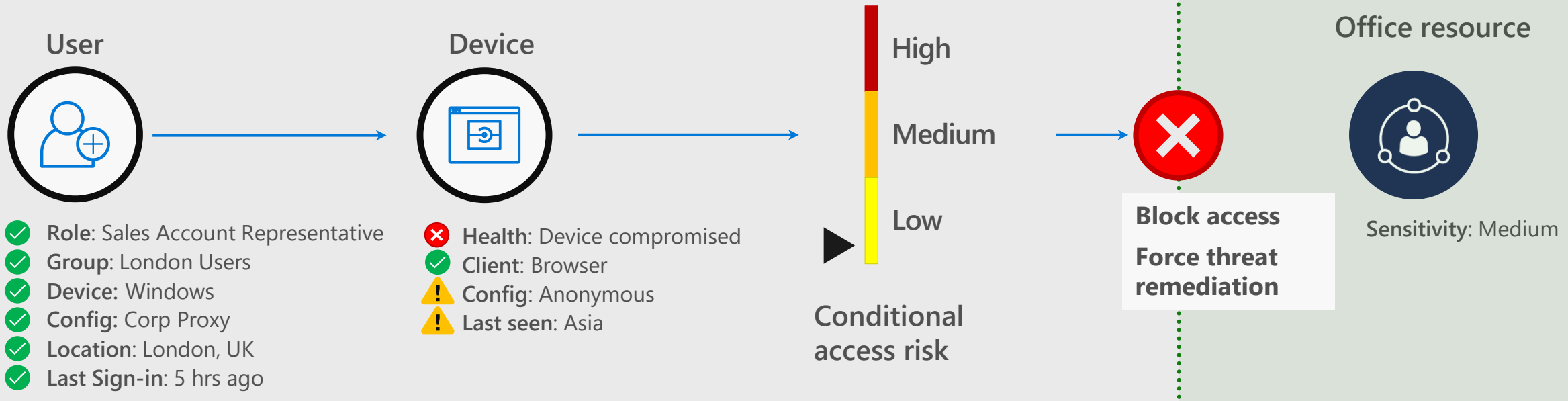


Conditional access risk



Actions:
- Allow
- Allow Restricted
- Require MFA
- Block
- Force Remediation

Conditional Access Example



For insights into password spray and other modern attack patterns, see

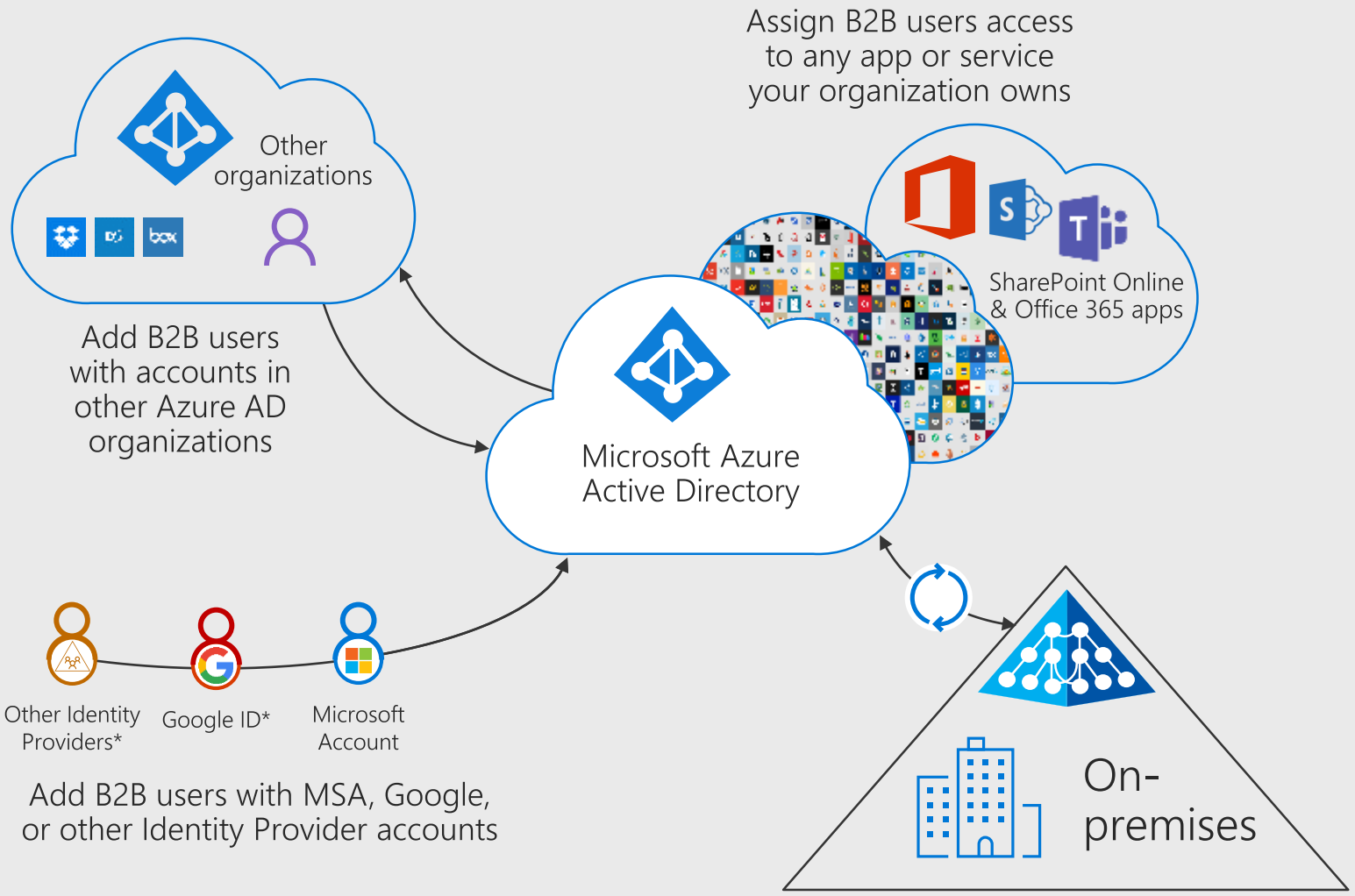
[Your Pa$$word doesn't matter]

- 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

Questions?

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

Disrupt Attacker ROI

Prioritize investments to maximize impact

Security Return on Investment (SROI)

Defender Return:

Ruin Attacker ROI

Deters opportunistic attacks

Slows or stops determined attacks

Defender Investment:

Security budget

Team time/attention

Attacker Return:
Successful Monetization

Rapid detection and response drives down predictability and quantity of return

Attacker Investment:
Increase Attack Friction & Cost

Prioritizing defense can rapidly raise impact attacker cost & friction