

Wednesday, December 16, 2020



Securing Azure with

Azure Advisor, Security Center, Sentinel,
AAD Conditional Access, & Privileged
Identity Management

Greg White – Manager, Cloud Sales Engineering



Microsoft Azure



Productive



Hybrid



Intelligent



Trusted

Gain unmatched security with Azure

\$1B annual investment in cybersecurity

3500+ global security experts

Trillions of diverse signals for unique intelligence



Securing Azure resources is a shared responsibility between Microsoft and the customer

MICROSOFT'S COMMITMENT

Securing and managing the cloud foundation



Physical assets



Datacenter operations



Cloud infrastructure

Secure Foundation

Microsoft managed



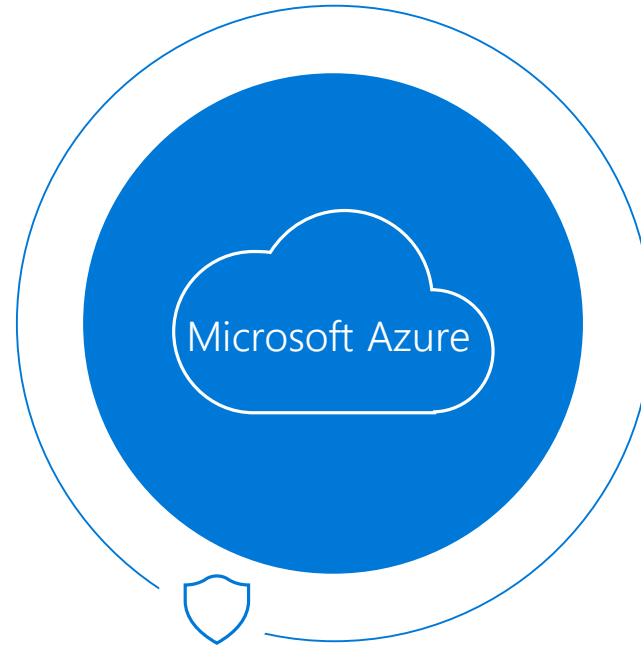
Physical assets



Datacenter operations

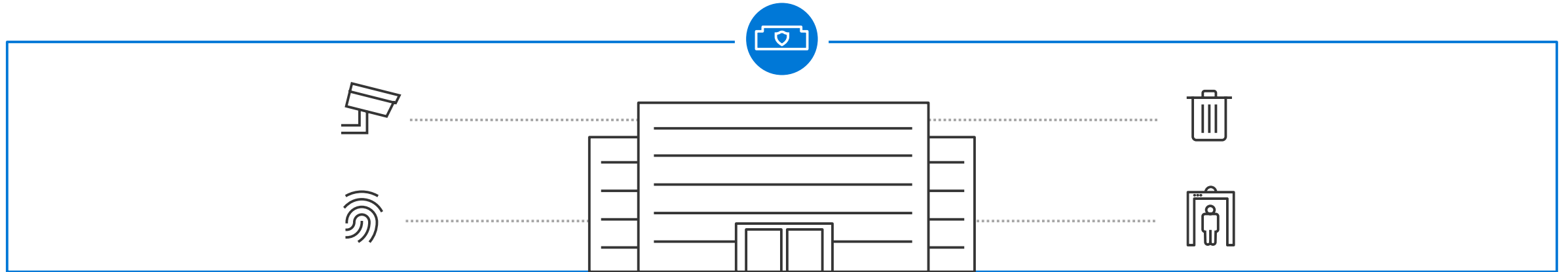


Cloud infrastructure



Secure foundation

Physical datacenter security



Global datacenters designed and operated by Microsoft

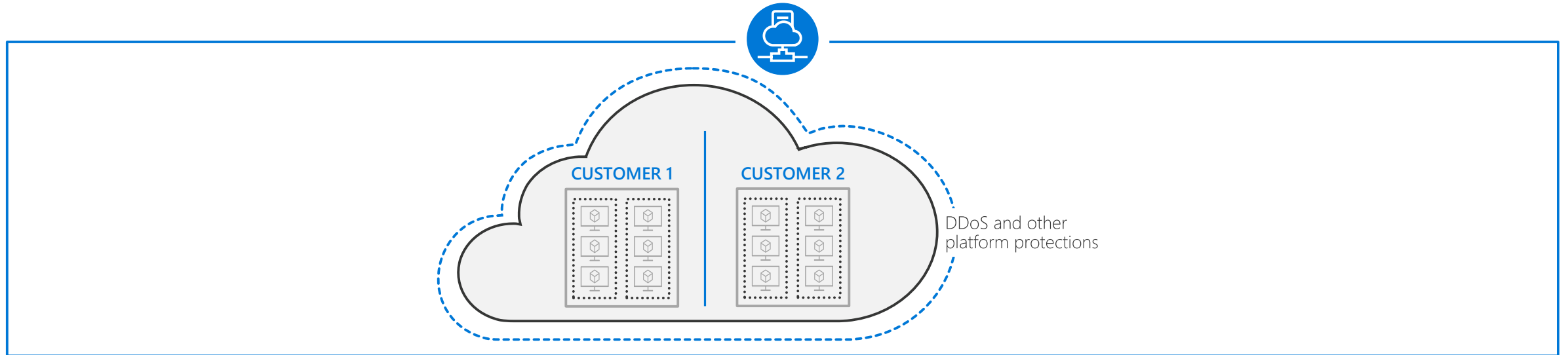
Protected by industry leading security systems

Extensive layers of protection

Helps reduce unauthorized physical access

Secure foundation

Azure infrastructure security



Securing customer data

Data, network segregation. Platform level protections like DDoS

Secure hardware

Custom-built hardware with integrated security and attestation

Continuous testing

War game exercises by Microsoft teams, continuous monitoring

Secure Foundation

Operational security



Restricted access for Microsoft administrators

Identity isolation and secure operator workstations

Grants least privilege required to complete task

Incident response

Multi-step incident response process

Focus on containment & recovery

3500+ security professionals

Working to harden, patch and protect the platform

24x7 monitoring for threats; assume breach drills

Securing Azure resources is a shared responsibility between Microsoft and the customer

MICROSOFT'S COMMITMENT

Securing and managing the cloud foundation



Physical assets



Datacenter operations



Cloud infrastructure

JOINT RESPONSIBILITY

Securing and managing your cloud resources



Virtual machines



Applications & workloads



Data

Common threats we see in the wild

VMs

- Brute force of open management ports
- Exploit through an unpatched vulnerability
- Run bitcoin mining on a compromised VM

Containers

- Exposed Kubernetes dashboards
- RBAC not configured in the cluster
- Insecure container/host configuration

App services

- Web shell deployment
- server-side request forgery (SSRF)
- Reconnaissance attempts

SQL Database

- SQL injection vulnerabilities and attacks
- Access by a remote threat actor
- Brute-force against SQL credentials

Storage account

- Use to propagate malware or load malicious images/packages
- Access by a remote threat actor
- Public access to storage accounts
- Harvest for reconnaissance or exfiltration of data

Key Vault

- Permissive policies grant access to unneeded resources
- Harvest for secrets

Azure Advisor

Your free, personalized guide to Azure best practices



Optimize resources for high availability, security, performance, and cost



Implement personalized recommendations with ease



Access best practice optimizations at no additional cost

Reliability

Increase availability of your business-critical apps

Security

Better protect your Azure resources from security threats

Performance

Boost the speed and responsiveness of your resources

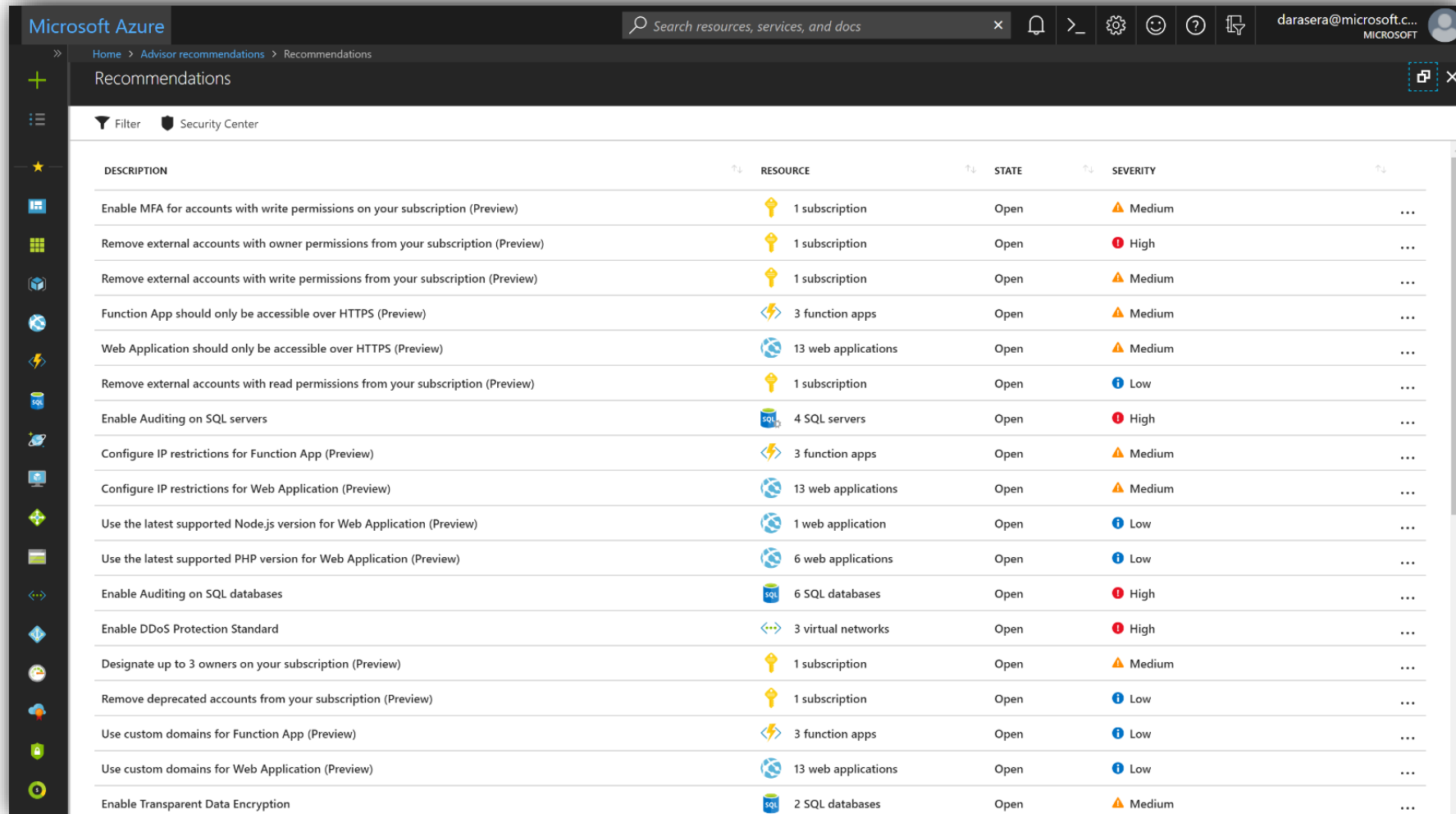
Cost

Maximize the return on your Azure investment

Built-in Controls

Azure Advisor

Security



Microsoft Azure

Search resources, services, and docs

darasera@microsoft.c... MICROSOFT

Home > Advisor recommendations > Recommendations

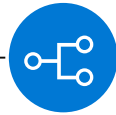
Recommendations

Filter Security Center

DESCRIPTION	RESOURCE	STATE	SEVERITY
Enable MFA for accounts with write permissions on your subscription (Preview)	1 subscription	Open	Medium
Remove external accounts with owner permissions from your subscription (Preview)	1 subscription	Open	High
Remove external accounts with write permissions from your subscription (Preview)	1 subscription	Open	Medium
Function App should only be accessible over HTTPS (Preview)	3 function apps	Open	Medium
Web Application should only be accessible over HTTPS (Preview)	13 web applications	Open	Medium
Remove external accounts with read permissions from your subscription (Preview)	1 subscription	Open	Low
Enable Auditing on SQL servers	4 SQL servers	Open	High
Configure IP restrictions for Function App (Preview)	3 function apps	Open	Medium
Configure IP restrictions for Web Application (Preview)	13 web applications	Open	Medium
Use the latest supported Node.js version for Web Application (Preview)	1 web application	Open	Low
Use the latest supported PHP version for Web Application (Preview)	6 web applications	Open	Low
Enable Auditing on SQL databases	6 SQL databases	Open	High
Enable DDoS Protection Standard	3 virtual networks	Open	High
Designate up to 3 owners on your subscription (Preview)	1 subscription	Open	Medium
Remove deprecated accounts from your subscription (Preview)	1 subscription	Open	Low
Use custom domains for Function App (Preview)	3 function apps	Open	Low
Use custom domains for Web Application (Preview)	13 web applications	Open	Low
Enable Transparent Data Encryption	2 SQL databases	Open	Medium

Built-in Controls

Simplify security with Azure services



Identity & access management

Data protection

Network security

Threat protection

Security management

Azure Active Directory

Encryption
(Disks, Storage, SQL)

VNET, VPN, NSG

Azure Security Center



Multi-Factor Authentication

Azure Key Vault

Application Gateway (WAF), Azure Firewall

Microsoft Antimalware for Azure

Azure Log Analytics

Role Based Access Control

Confidential Computing

DDoS Protection Standard

Azure Active Directory (Identity Protection)

ExpressRoute

+ Partner Solutions

Azure security center



Strengthen security posture

Cloud security posture management

Secure Score
Policies and compliance



Protect against threats

For servers

For cloud native workloads

For databases and storage

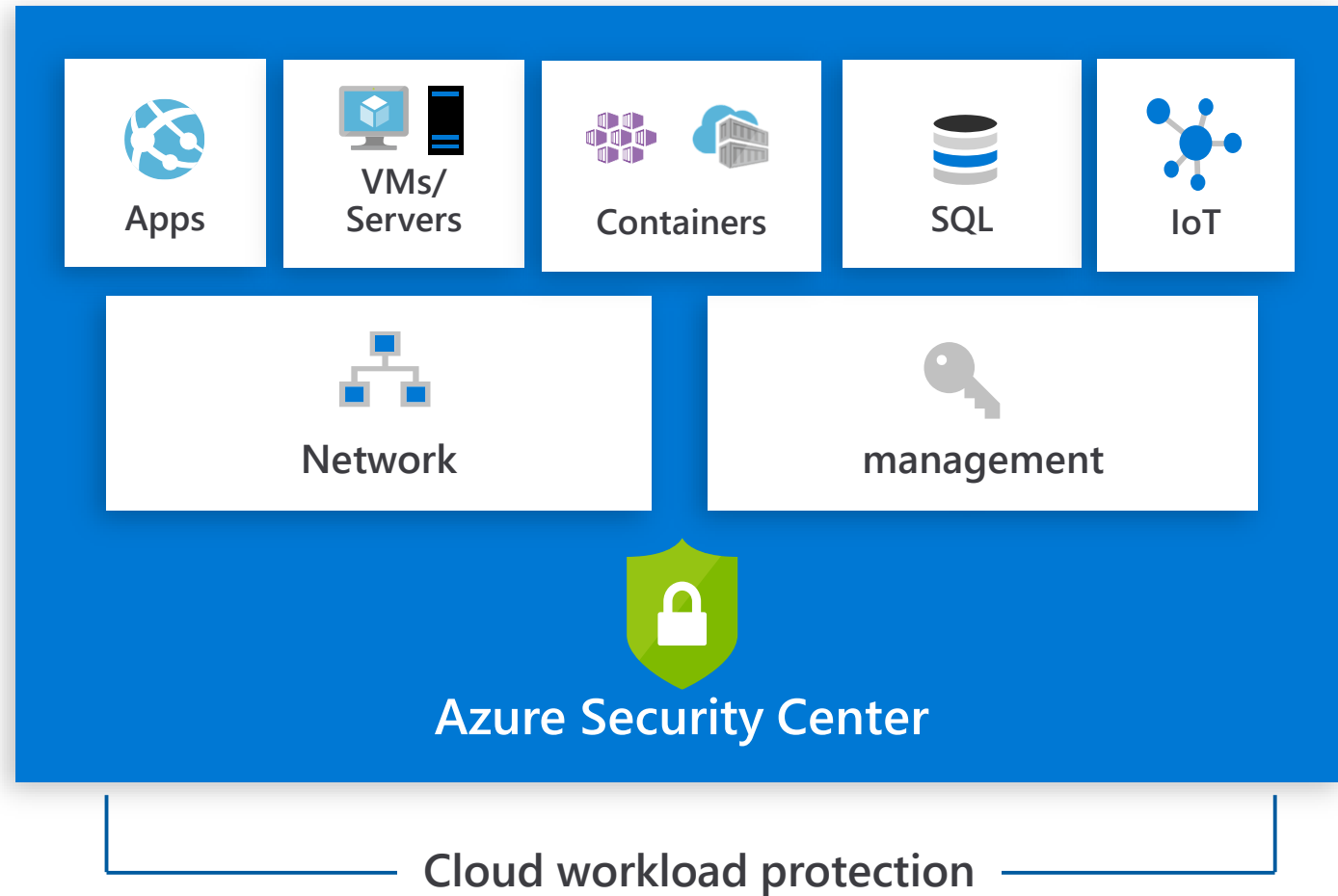


Get secure faster

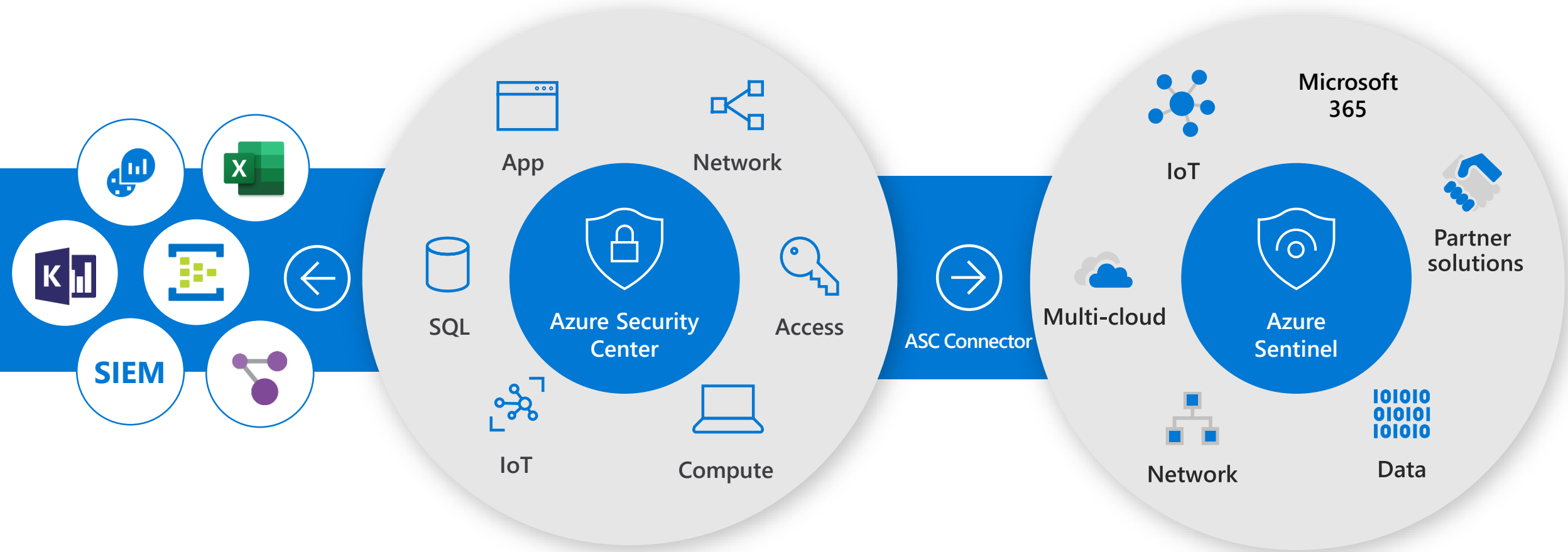
Protect your workloads from threats

Use industry's most extensive threat intelligence to gain deep insights

- Detect & block advanced malware and threats for Linux and Windows Servers on any cloud
- Protect cloud-native services from threats
- Protect data services against malicious attacks
- Protect your Azure IoT solutions with near real time monitoring
- Service layer detections: Azure network layer and Azure management layer (ARM)



Threat protection for cloud at scale: Export assessments and alerts for security roles



Azure Security Center
Cloud Workload Protection

Azure Sentinel
Cloud Native SIEM

Introducing Microsoft Azure Sentinel

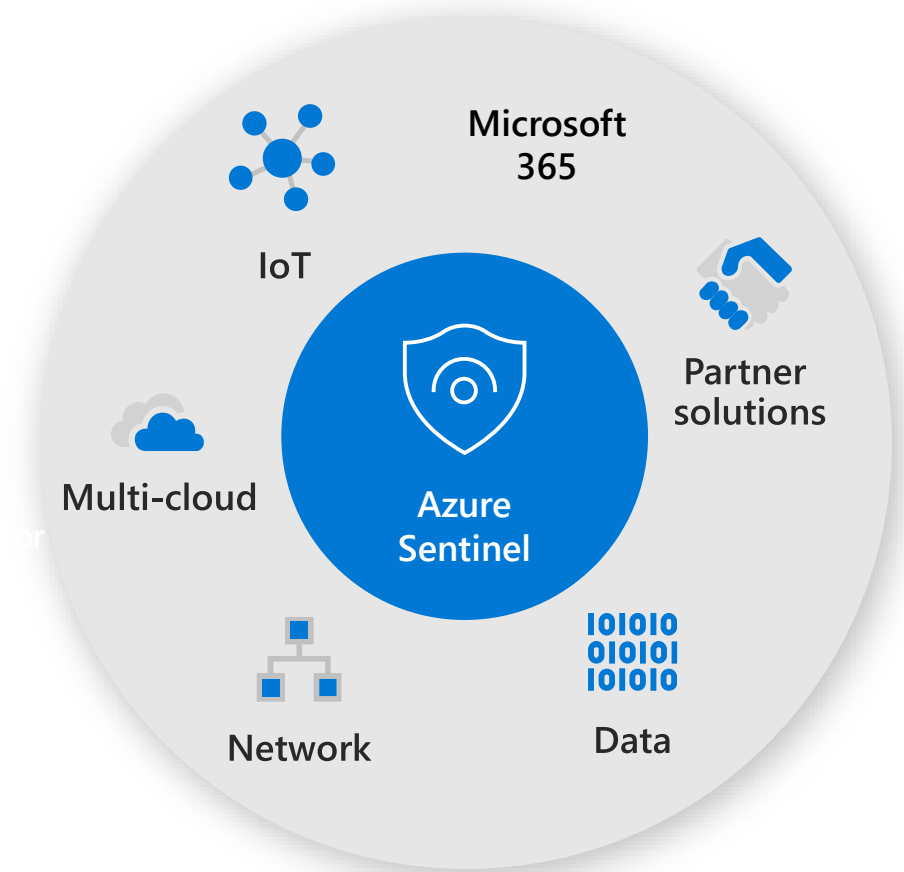
Cloud-native SIEM for intelligent security analytics for your entire enterprise

Near **Limitless** cloud speed and scale

Faster threat protection with **AI by your side**

Bring your **Office 365 data for Free**

Easy integration with your **existing tools**



Azure Sentinel
Cloud Native SIEM

Introducing Microsoft Azure Sentinel

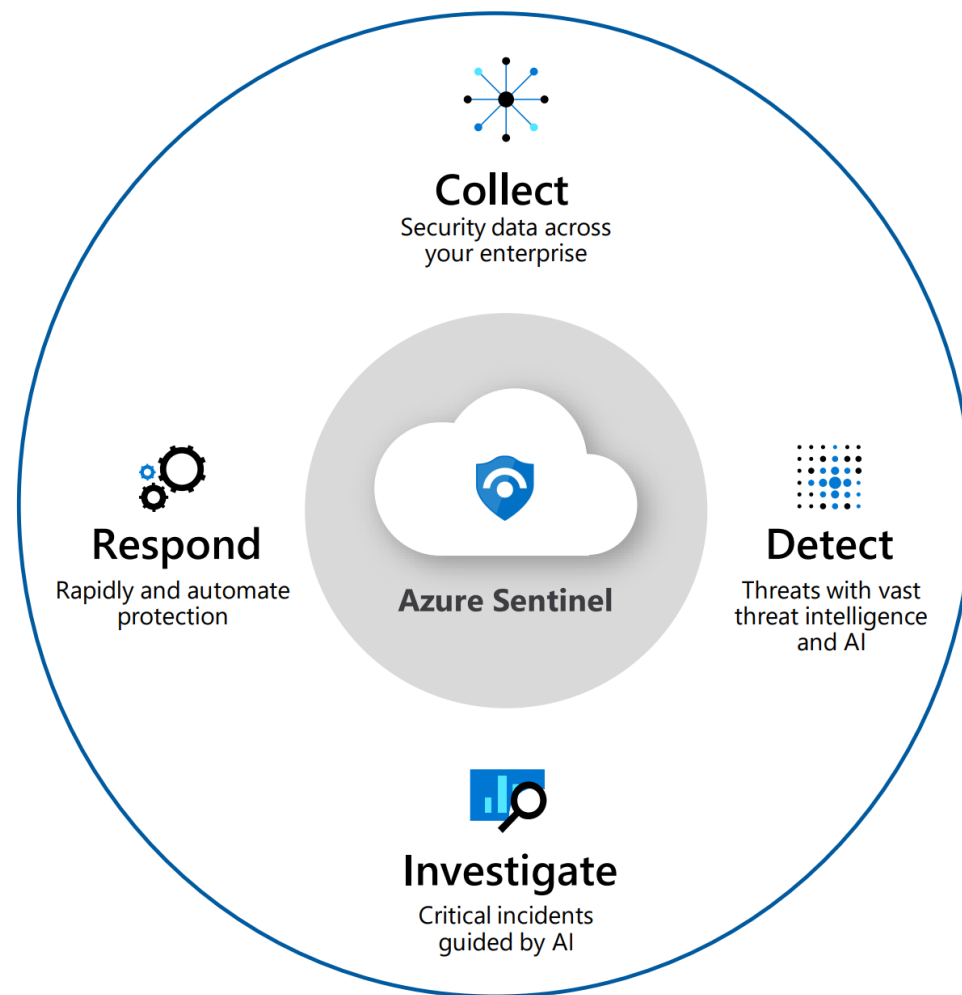
Cloud-native SIEM for intelligent security analytics for your entire enterprise

Near **Limitless** cloud speed and scale

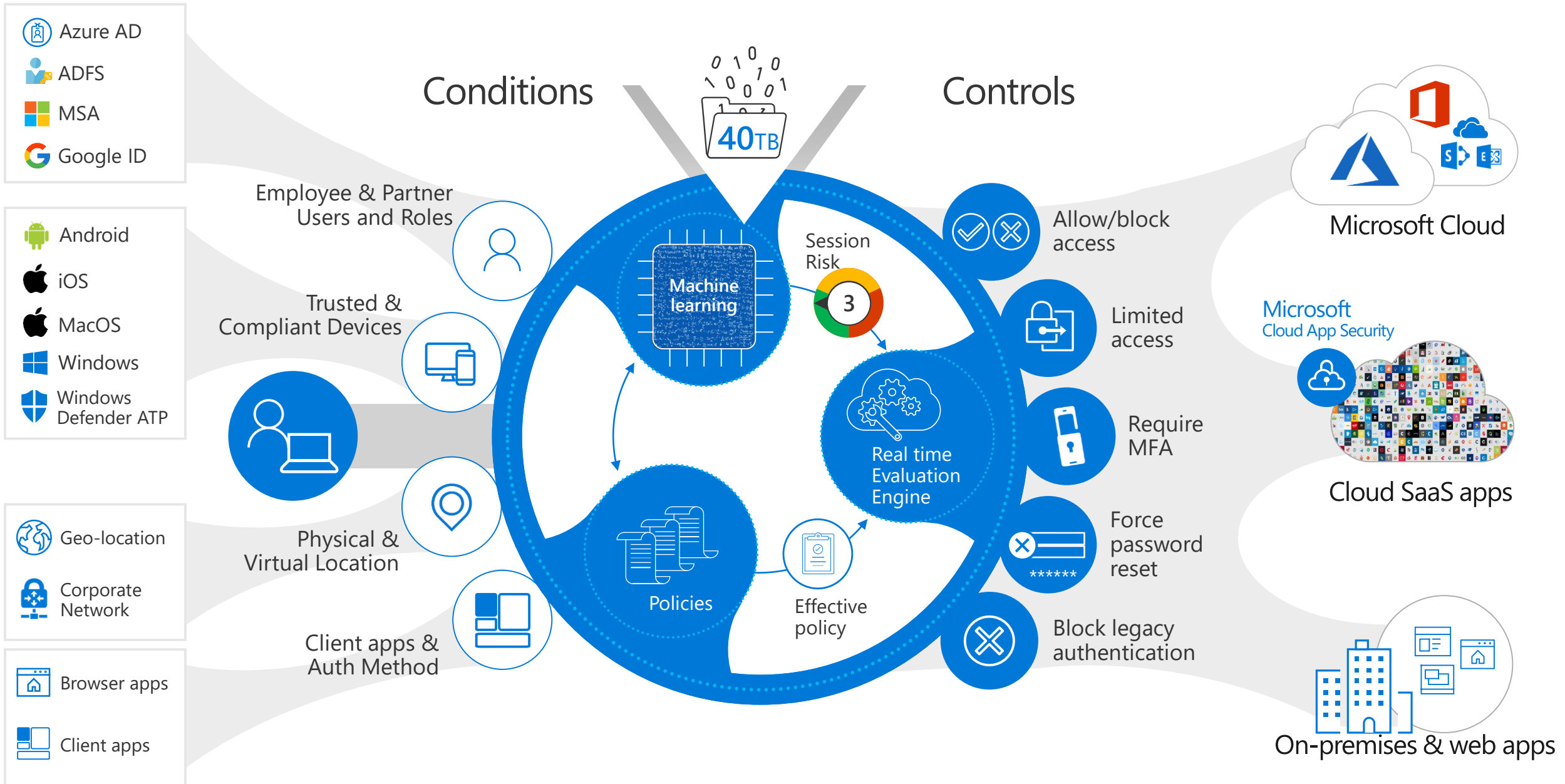
Faster threat protection with **AI by your side**

Bring your **Office 365 data for Free**

Easy integration with your **existing tools**



Azure AD Conditional Access

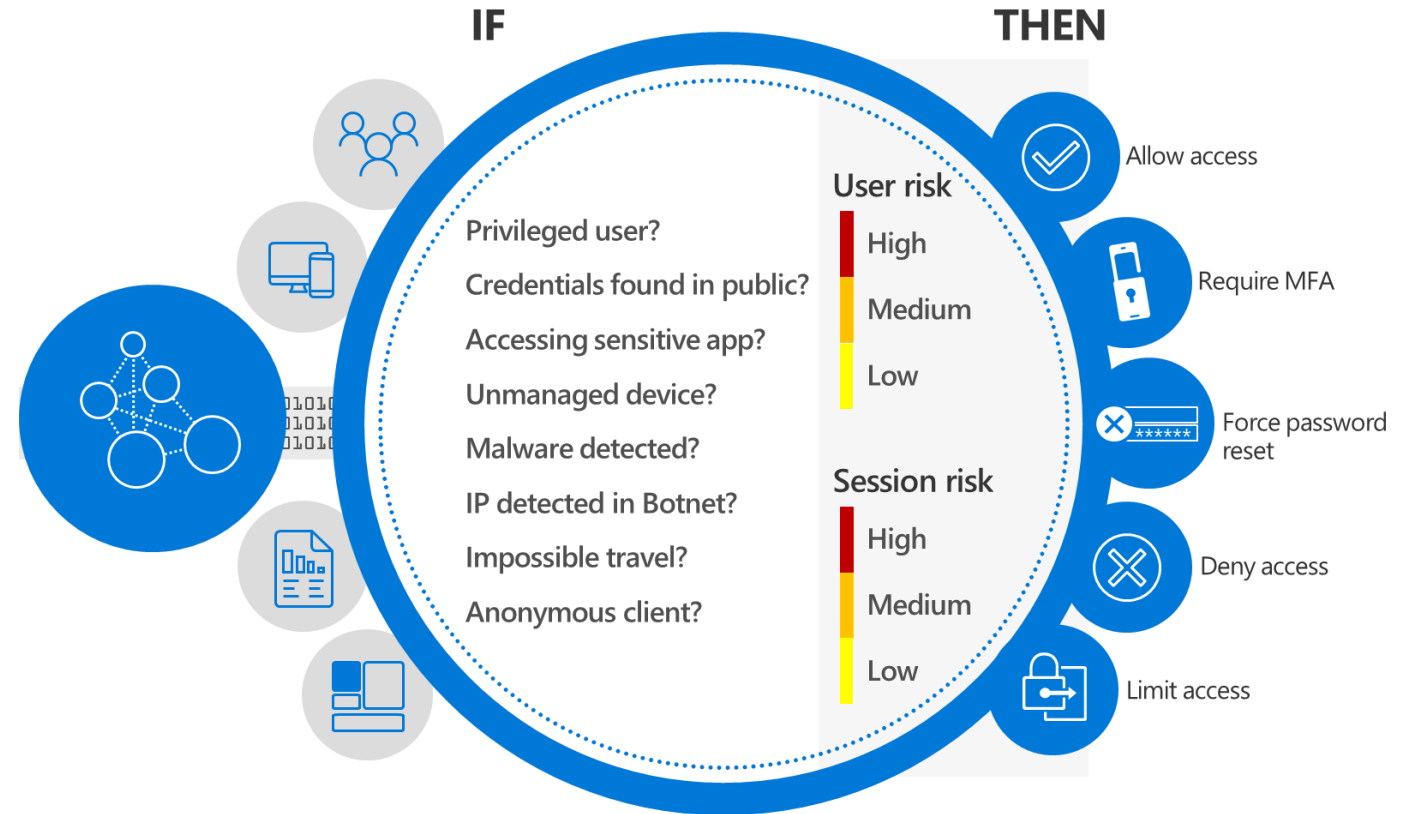


DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR USERS

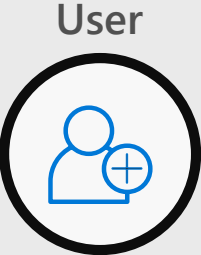
IDENTITY



USE **CONDITIONAL ACCESS** TO PROTECT YOUR ORGANIZATION AT THE FRONT DOOR



Conditional Access Example



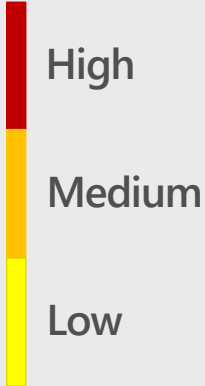
User

- ✓ Role: Sales Account Representative
- ✓ Group: London Users
- ✓ Device: Windows
- ✓ Config: Corp Proxy
- ✓ Location: London, UK
- ✓ Last Sign-in: 5 hrs ago



Device

- ✓ Health: Device Okay
- ✓ Client: Browser



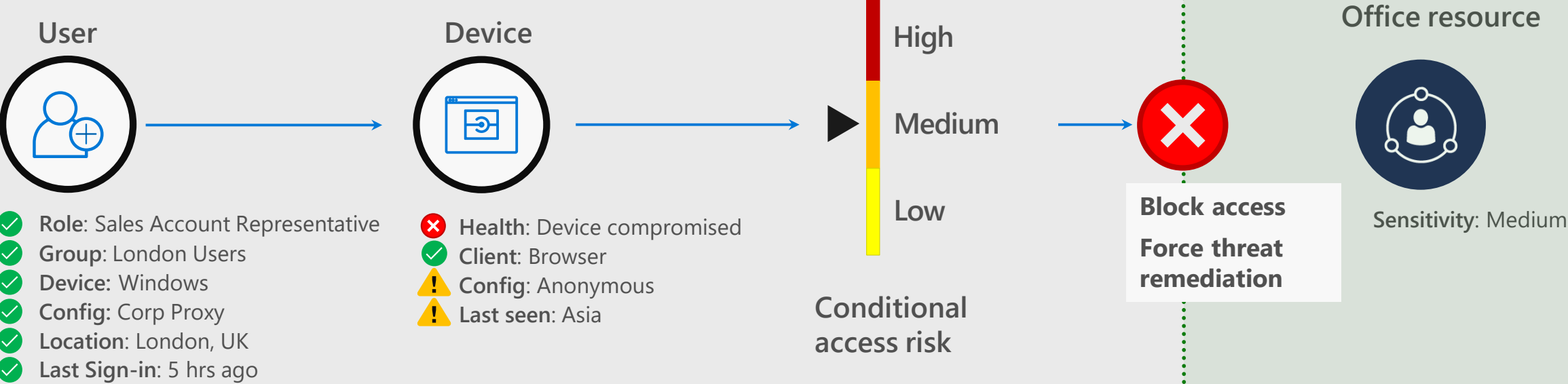
Conditional access risk



Office resource

Sensitivity: Medium

Conditional Access Example



- ✗ Malicious activity detected on device
- ⚠ Anonymous IP
- ⚠ Unfamiliar sign-in location for this user

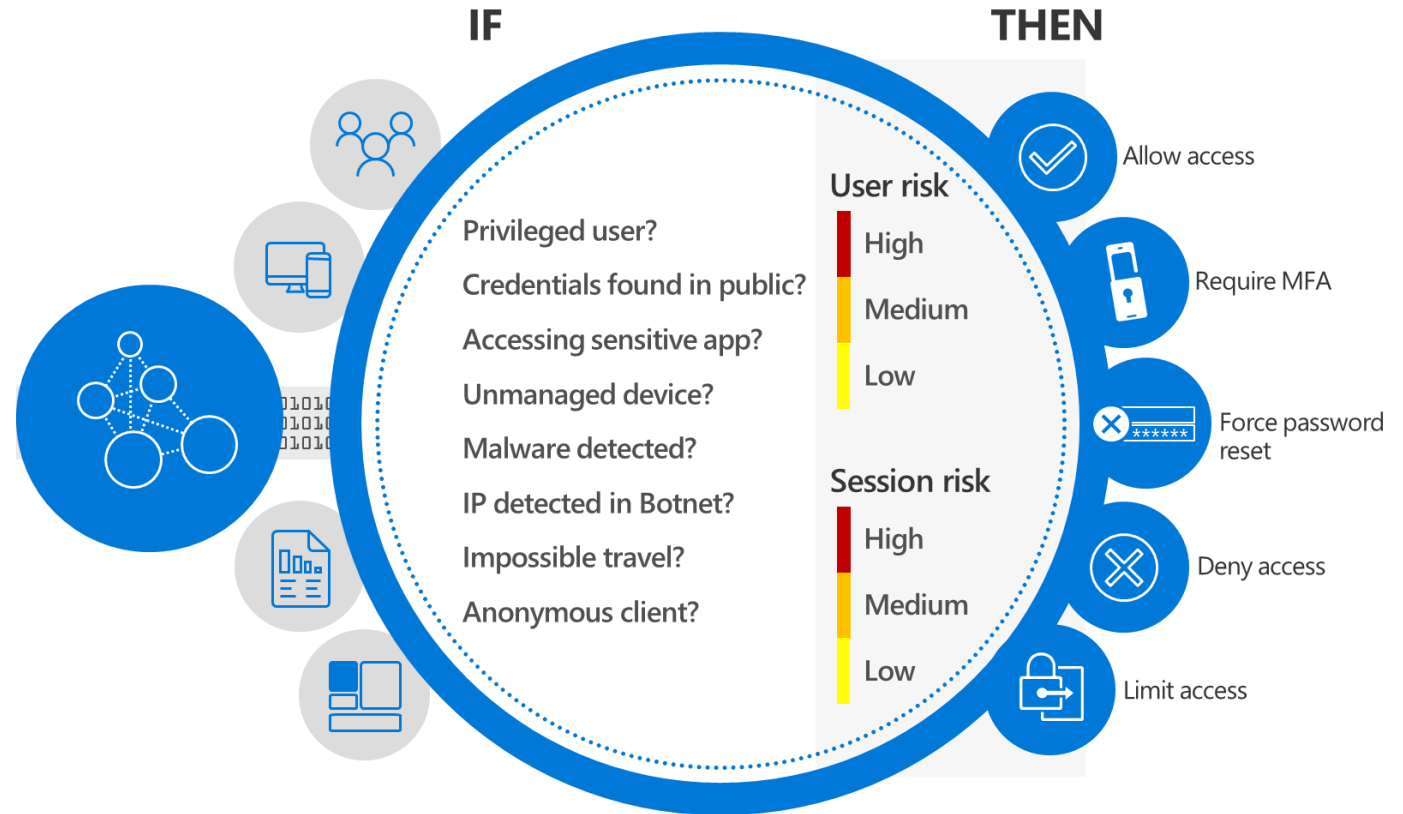
DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR USERS

IDENTITY



USE **CONDITIONAL ACCESS** TO PROTECT YOUR ORGANIZATION AT THE FRONT DOOR

CONTROL AND PROTECT **PRIVILEGED IDENTITIES**

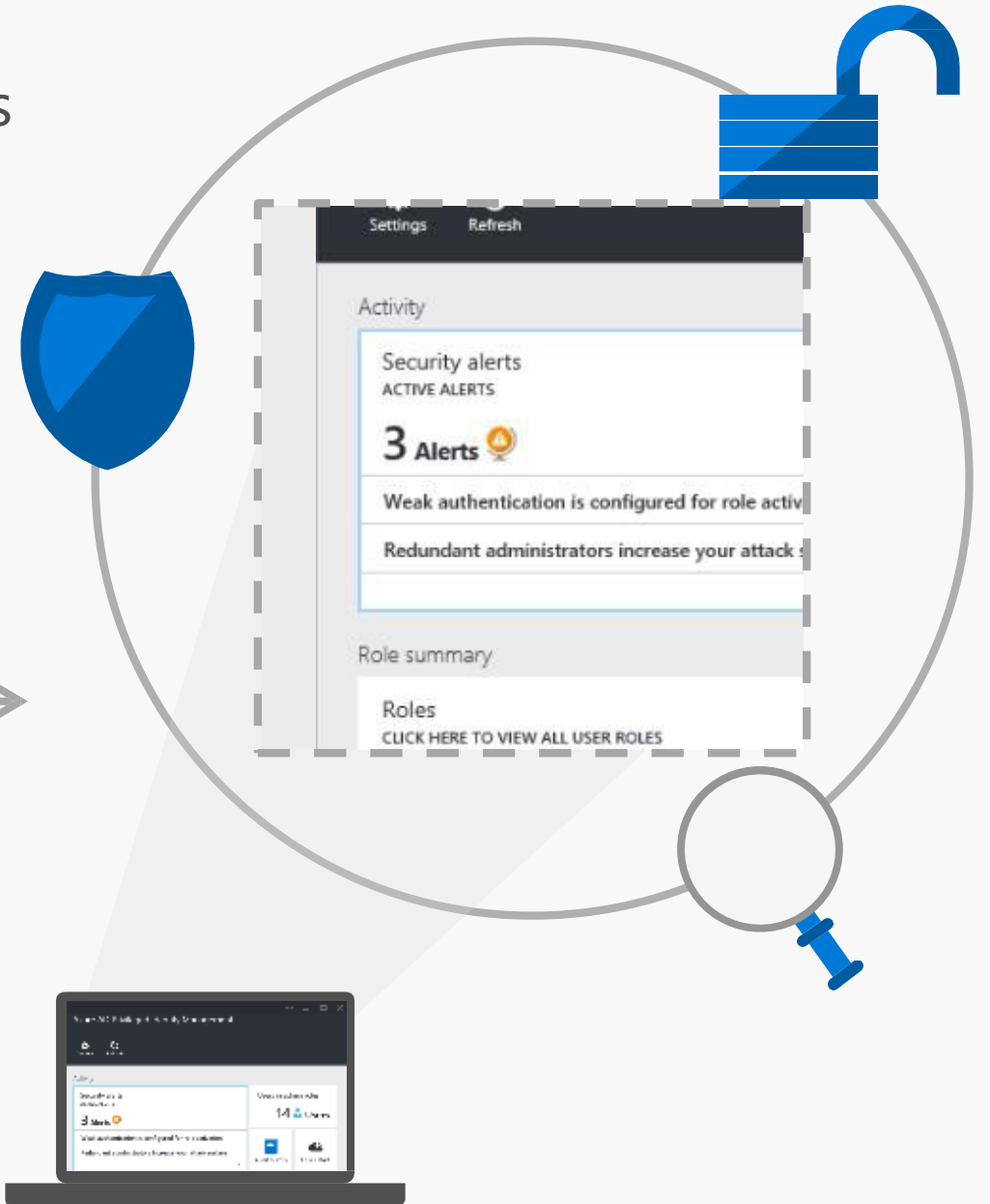


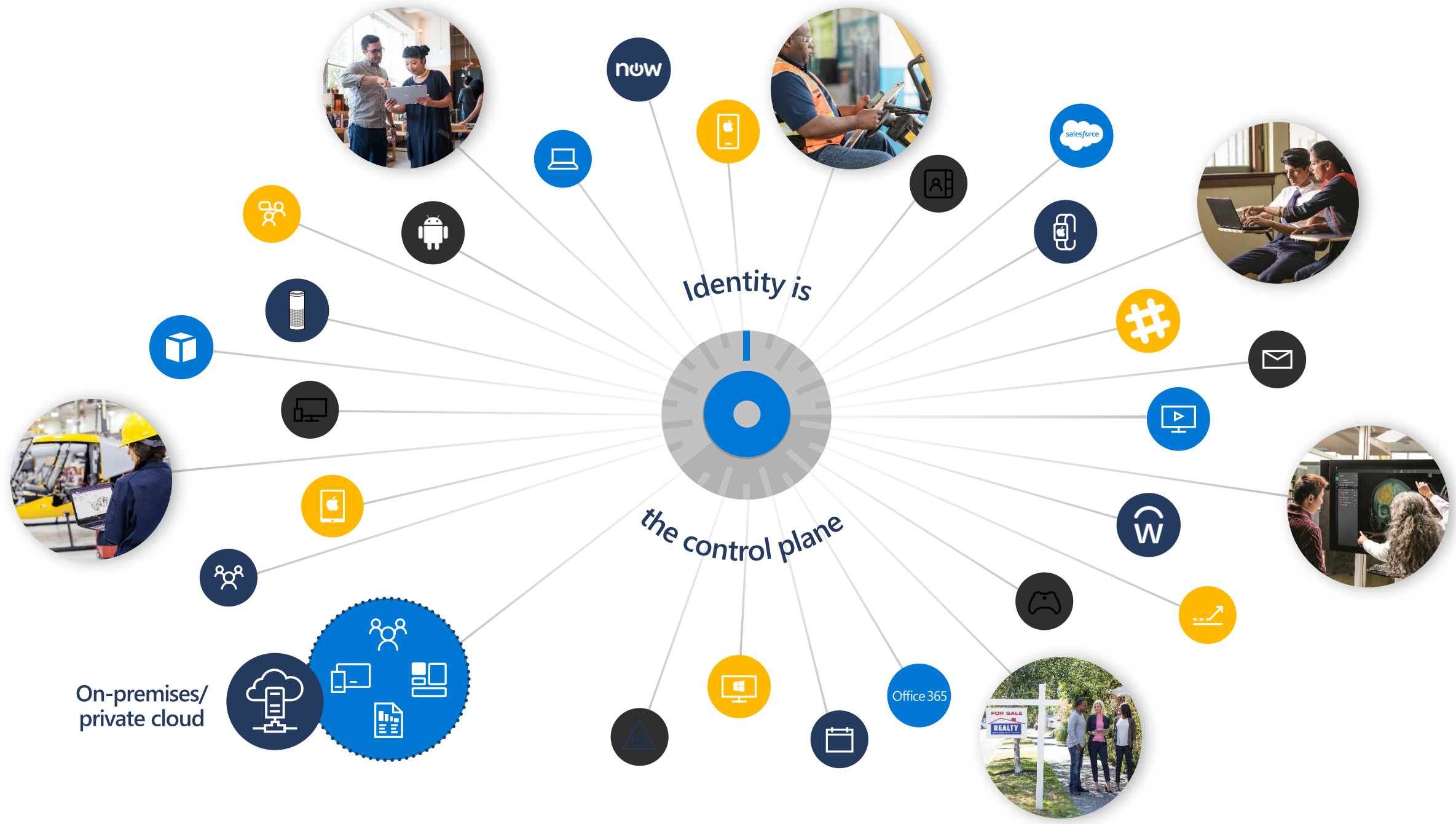
CONTROL AND PROTECT PRIVILEGED IDENTITIES

Discover, restrict, and monitor privileged identities

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

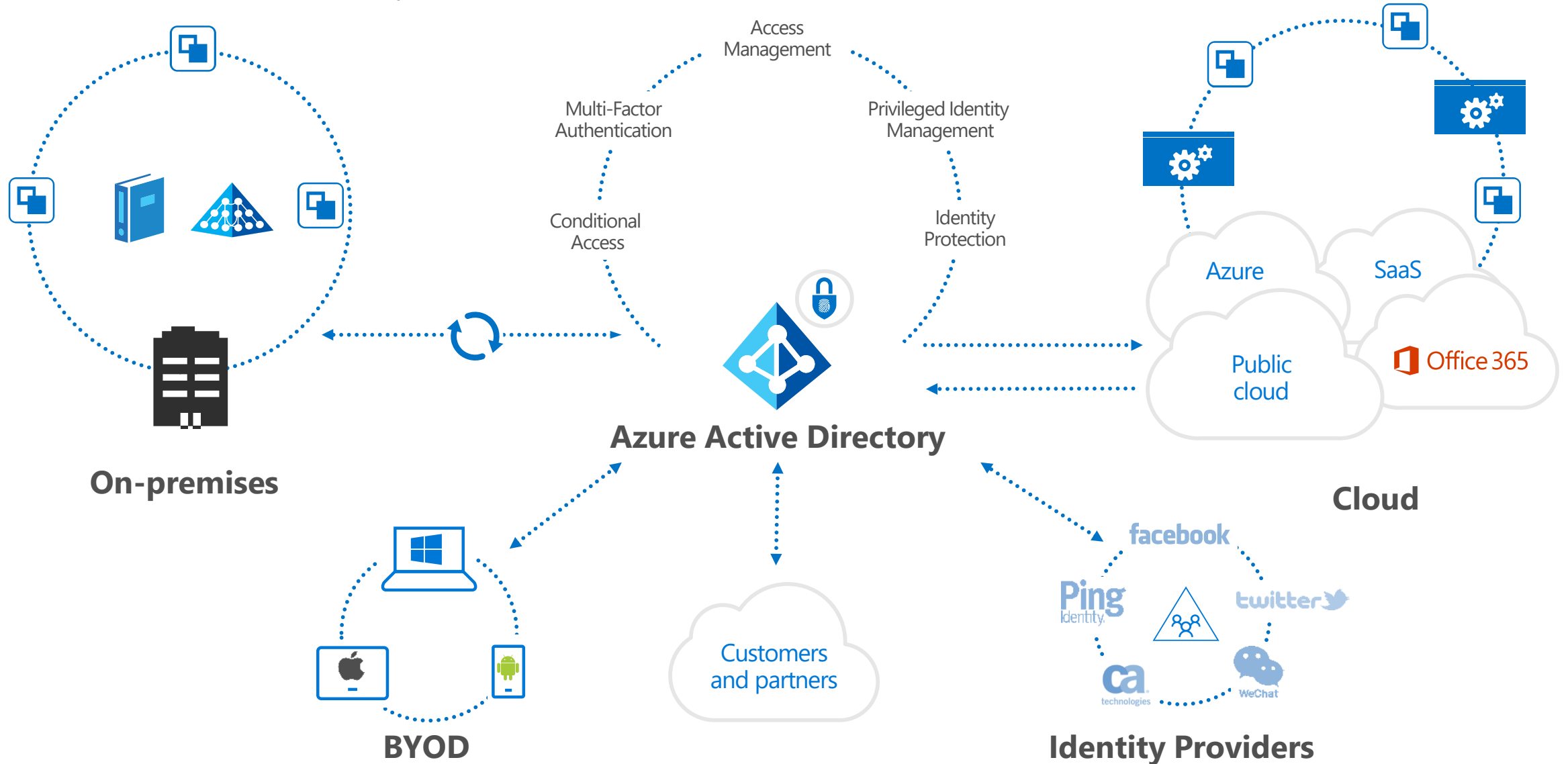
Use Alert, Audit Reports and Access Review





Identity is the Control Plane

of the modern cloud security architecture





Azure

Your vision. Your cloud.

