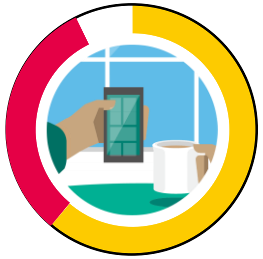
Microsoft 365 – k čemu to je?

Ondřej Výšek

MVP: Cloud & Data center management | MCT | MCP

vysek@kpcs.cz

World has changed (already)



66%

Millennials (93%)

of employees use personal devices for work purposes.*

>80%

of employees admit to using non-approved software-as-a-service (SaaS) applications in their jobs.**

>70%

percent of network intrusions exploited weak or stolen credentials.***

25%

of all software will be available on a SaaS delivery by 2020.****

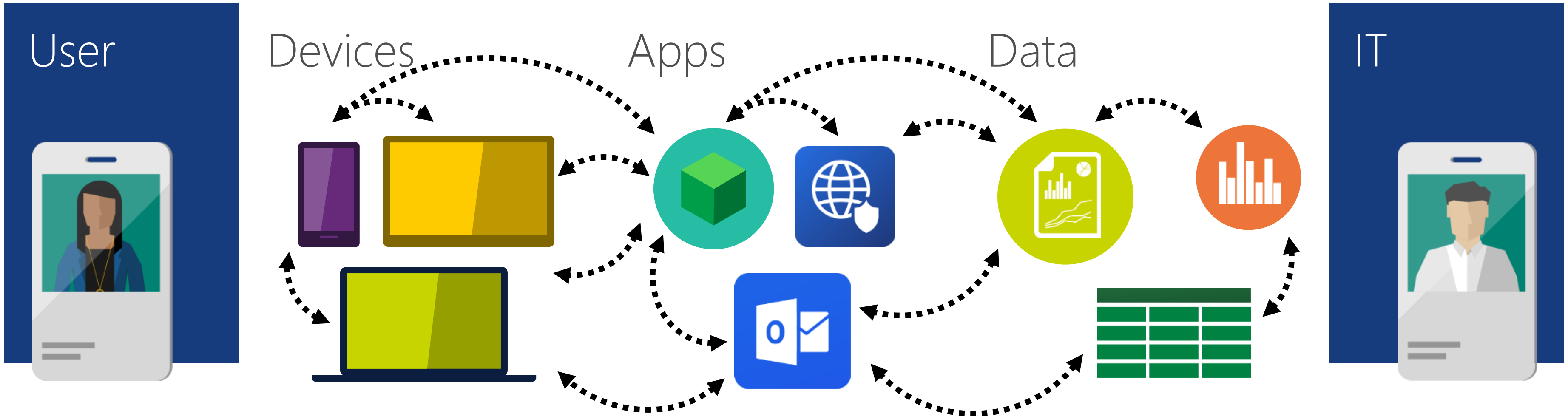
33%

Millennials (88%)

of employees that typically work on employer premises, also frequently work away from their desks.*****

*   Forrester Research: “BT Futures Report: Info workers will erase boundary between enterprise & consumer technologies,” Feb. 21, 2013
**   http://www.computing.co.uk/ctg/news/2321750/more-than-80-per-cent-of-employees-use-non-approved-saas-apps-report
*** Verizon 2013 data breach investigation report
****Forrester Application Adoption Trends: The Rise Of SaaS
*****CEB IT Impact Report: Five Key Findings on Driving Employee Productivity Q1 2014.

Why change? Do you recognize?



Microsoft 365

A complete, intelligent, secure solution to empower employees

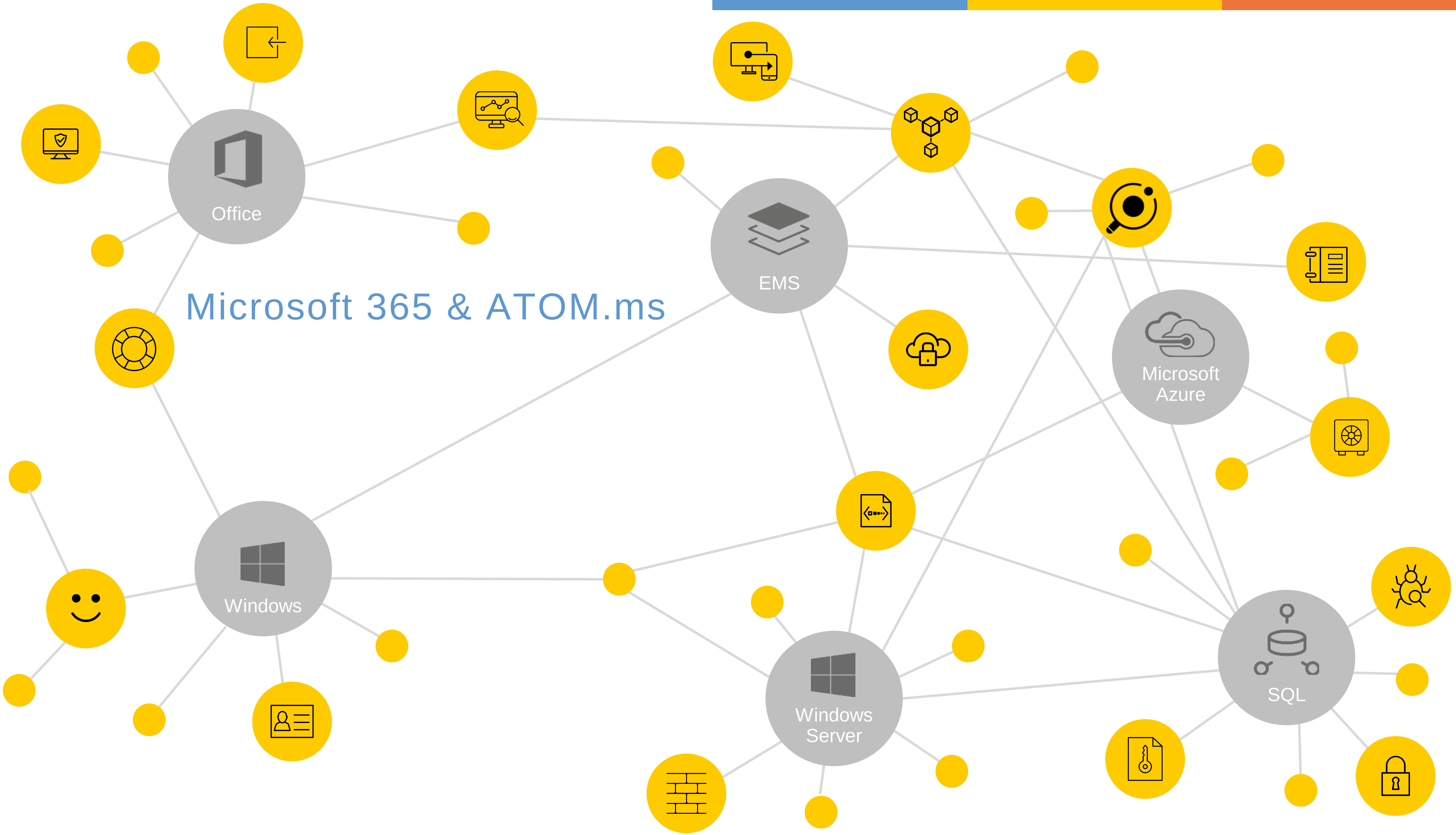
Unlocks creativity

Built for teamwork

Integrated for simplicity

Intelligent security

Microsoft 365 & ATOM.ms



True stories...

- Computer compromitted
- Password stolen from browser (Chrome)

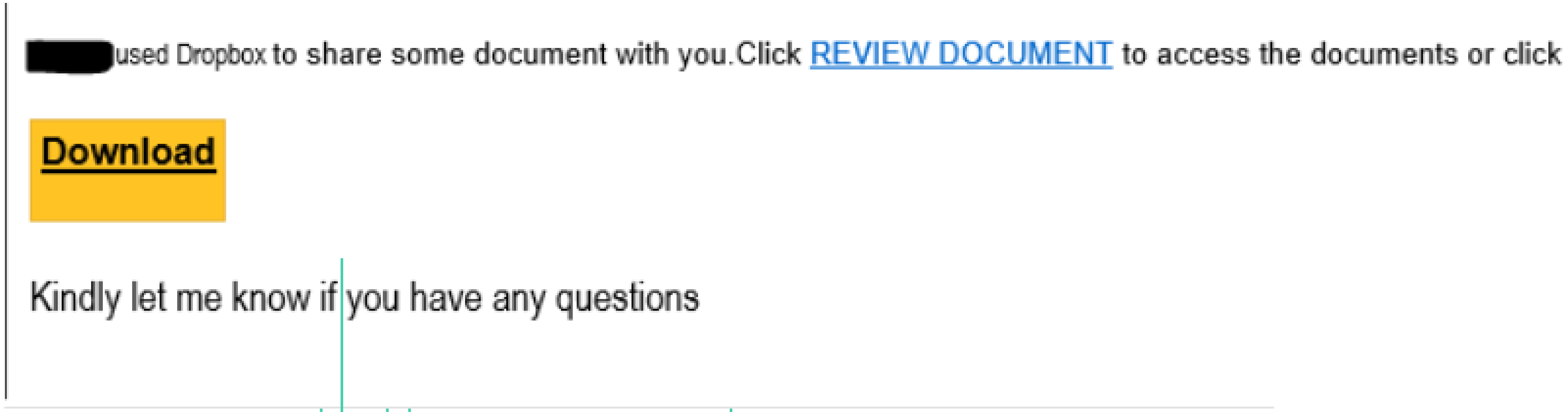
- Phishing e-mail to CEO from trusted user
- CEO device infected
- Malware installed

- Scan outlook and access gained
- Access to the Office 365 z NG
- Email move rule created

- Legitimate CFO request, handover to the CEO
- CEO approve payment
- Payment done

- Repeated request CFO, handover to the CEO
- CEO declines
- CEO has a suspicion

- Payment declined
- FBI investigation
- Forensic analysis



[redacted] used Dropbox to share some document with you.Click REVIEW DOCUMENT to access the documents or click

Download

Kindly let me know if you have any questions

Time: T+0

Time: T+8d

- Intune
  Conditional Access
  Windows 10 ATP

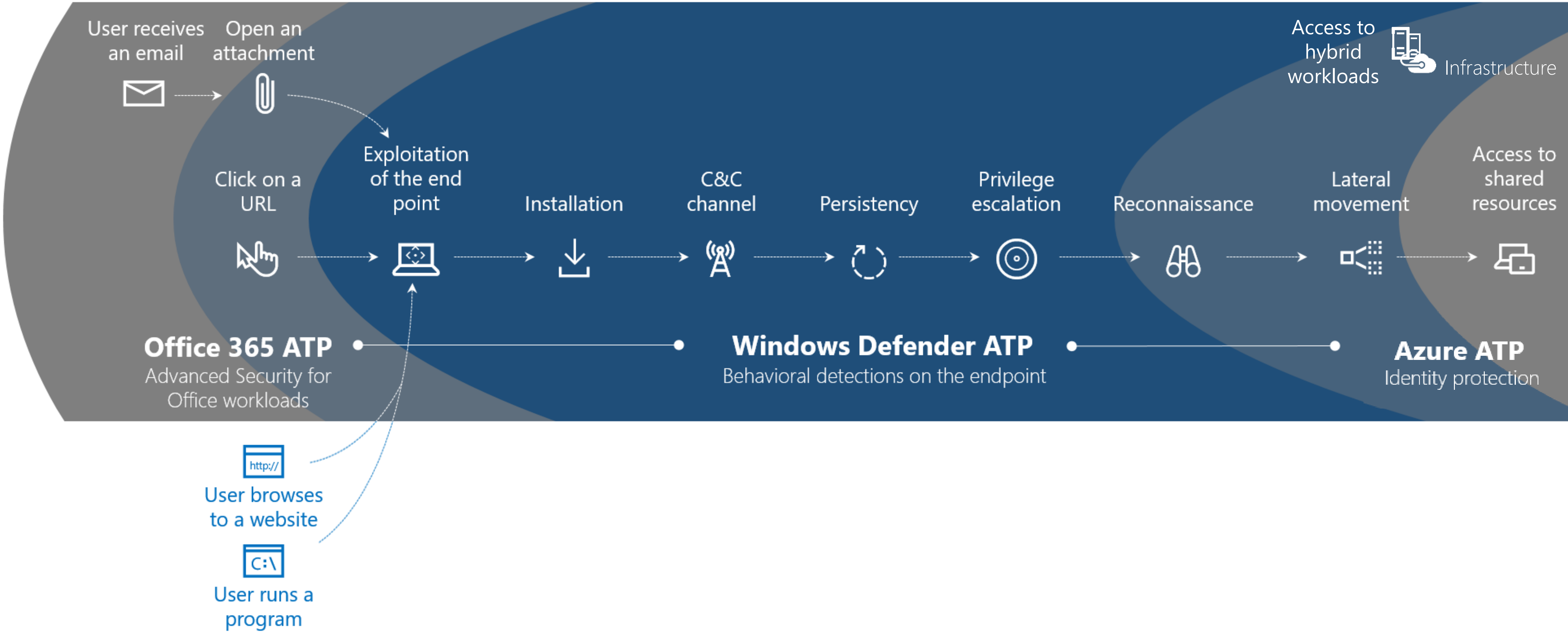
- ATOM security log detection
- ATOM app log detection
- Windows 10 ATP Process stolen
- Windows 10 ATP SandBox check

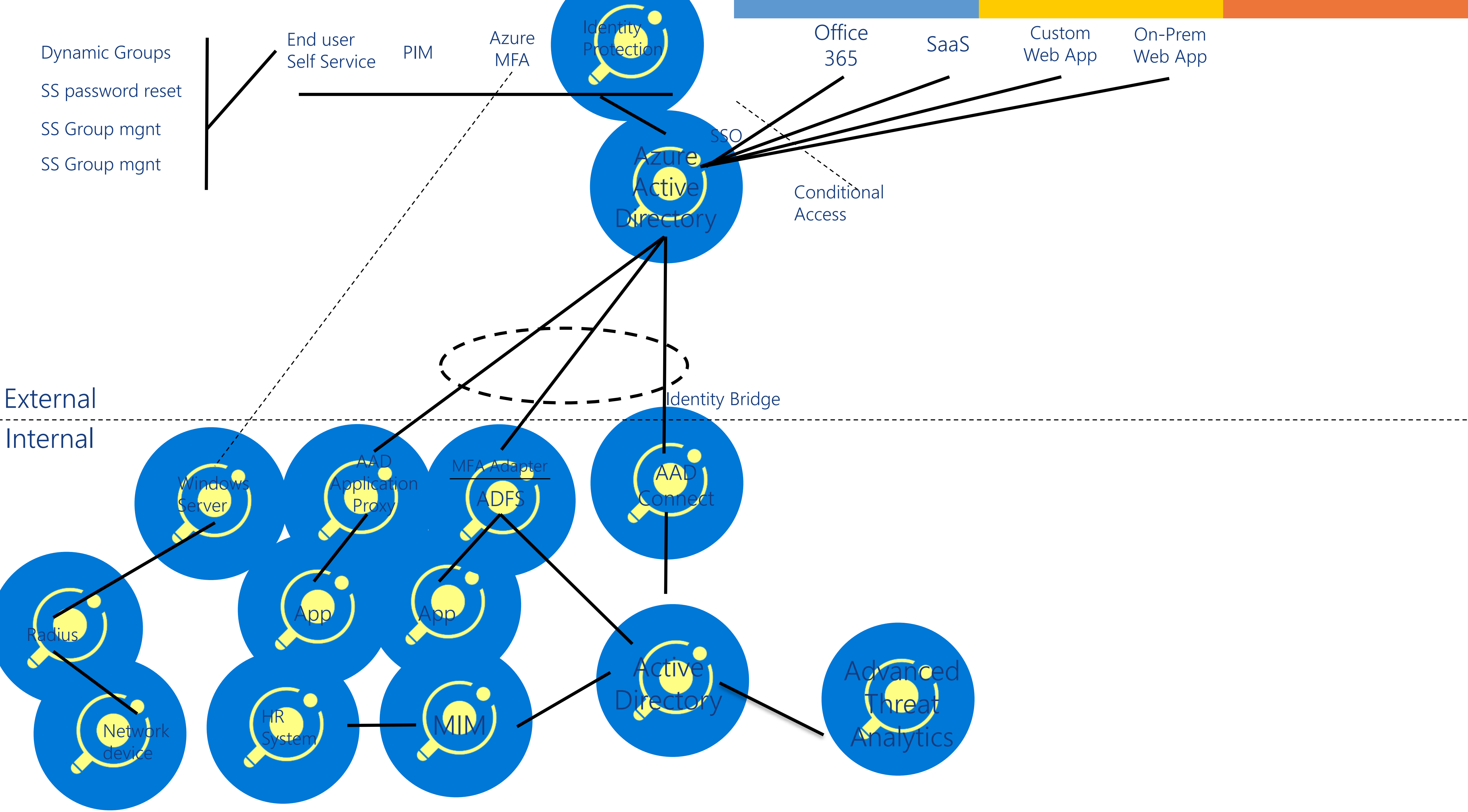
- AZURE AIP
- AZURE AIP
- ATOM security log detection
  Azure MFA
- Conditional Access
  Azure MFA
  ATOM AAD fraud detection

- AZURE AIP

- ATOM log trace

MAXIMIZE DETECTION COVERAGE THROUGHOUT THE ATTACK STAGES





Dynamic Groups

SS password reset

SS Group mgnt

SS Group mgnt

End user
Self Service

PIM

Azure
MFA

Identity
Protection

Office
365

SaaS

Custom
Web App

On-Prem
Web App

SSO

Azure
Active
Directory

Conditional
Access

Identity Bridge

External

Internal

Windows
Server

AAD
Application
Proxy

MFA Adapter

ADFS

AAD
Connect

Radius

App

App

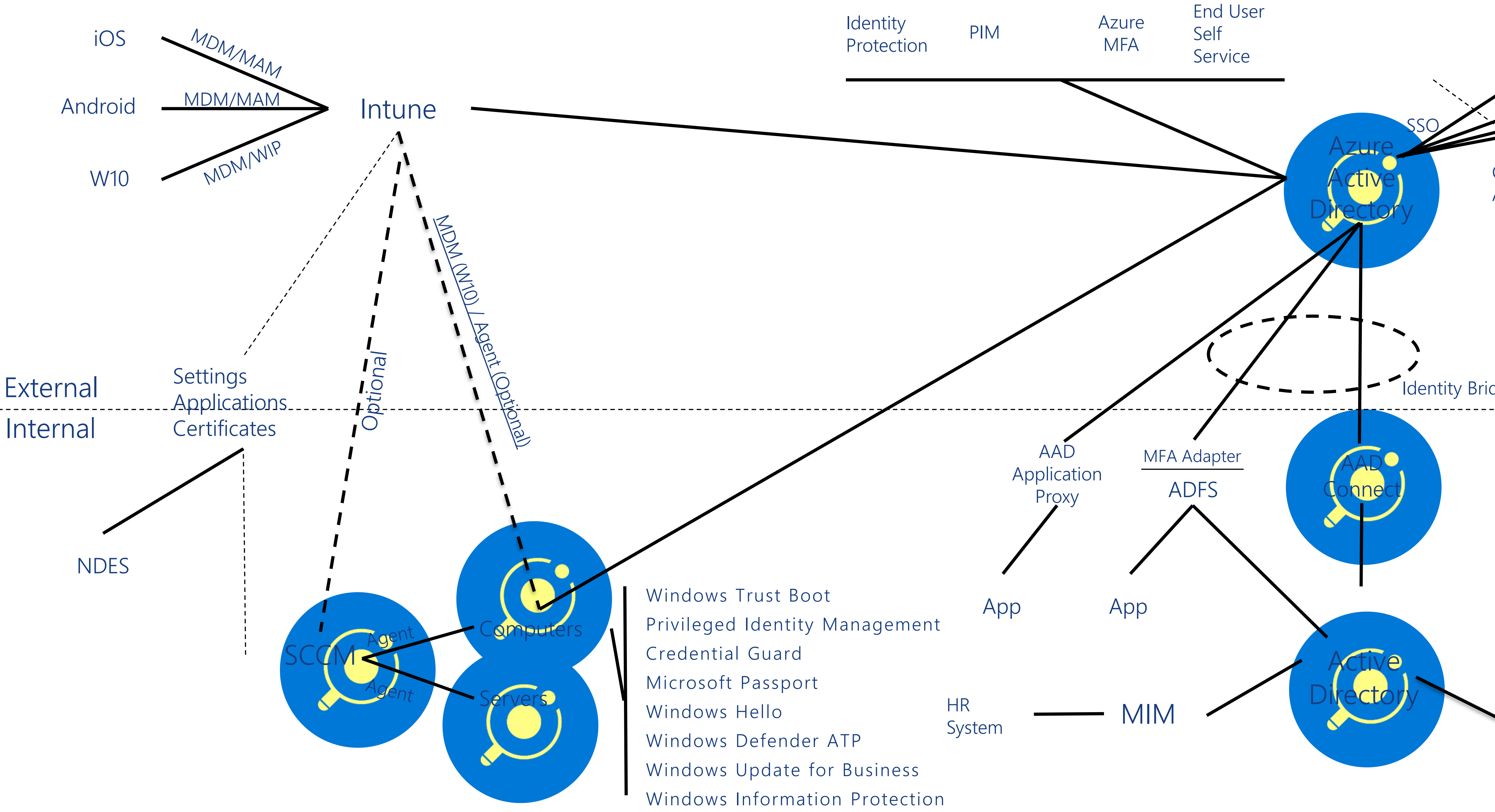
Network
device

HR
System

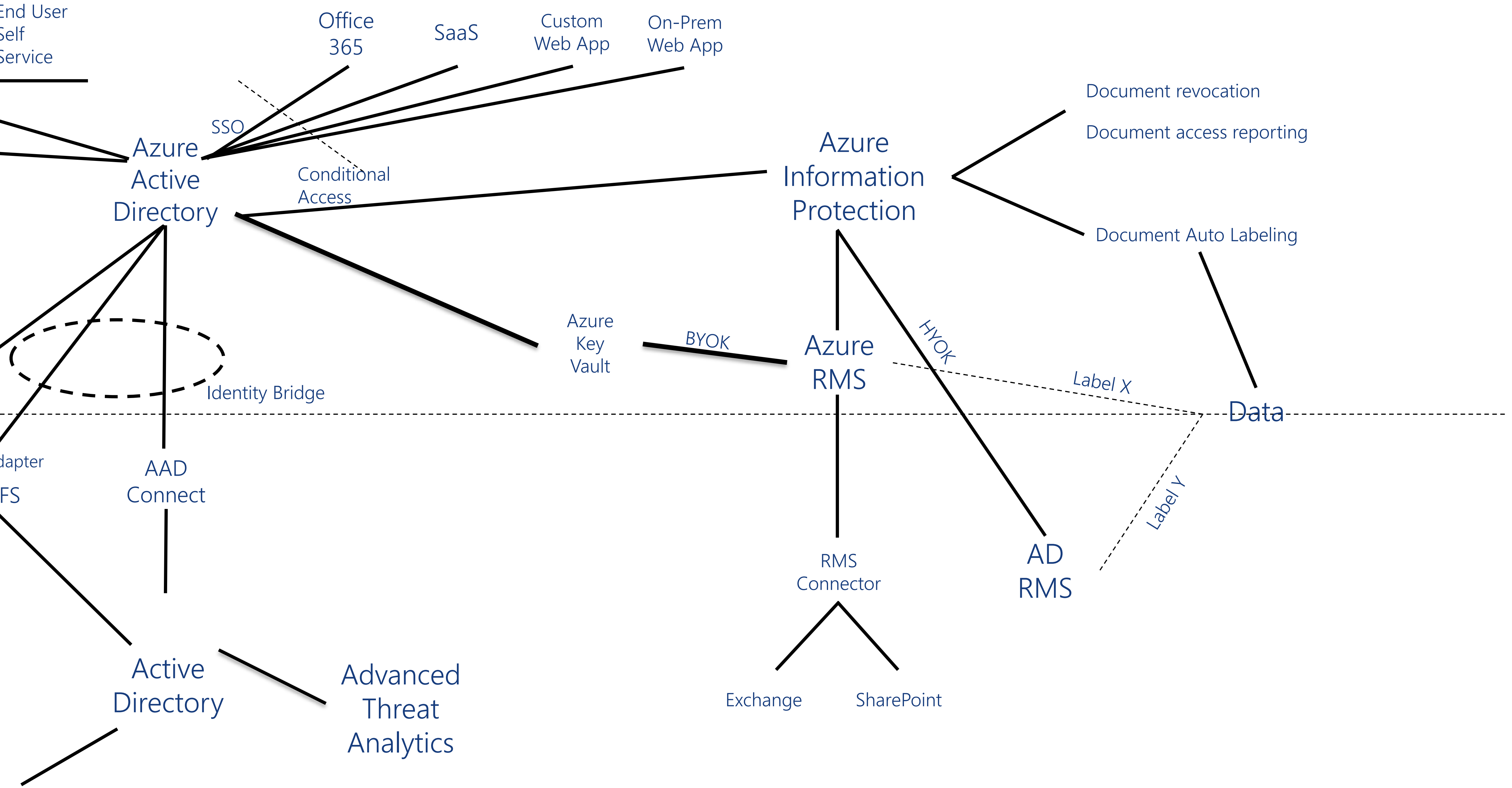
MIM

Active
Directory

Advanced
Threat
Analytics



Windows Trust Boot
Privileged Identity Management
Credential Guard
Microsoft Passport
Windows Hello
Windows Defender ATP
Windows Update for Business
Windows Information Protection



End User Self Service

Office 365

SaaS

Custom Web App

On-Prem Web App

SSO

Conditional Access

Azure Active Directory

Azure Information Protection

Document revocation

Document access reporting

Document Auto Labeling

Identity Bridge

Azure Key Vault

BYOK

Azure RMS

HYOK

Label X

Data

Label Y

dapter

FS

AAD Connect

RMS Connector

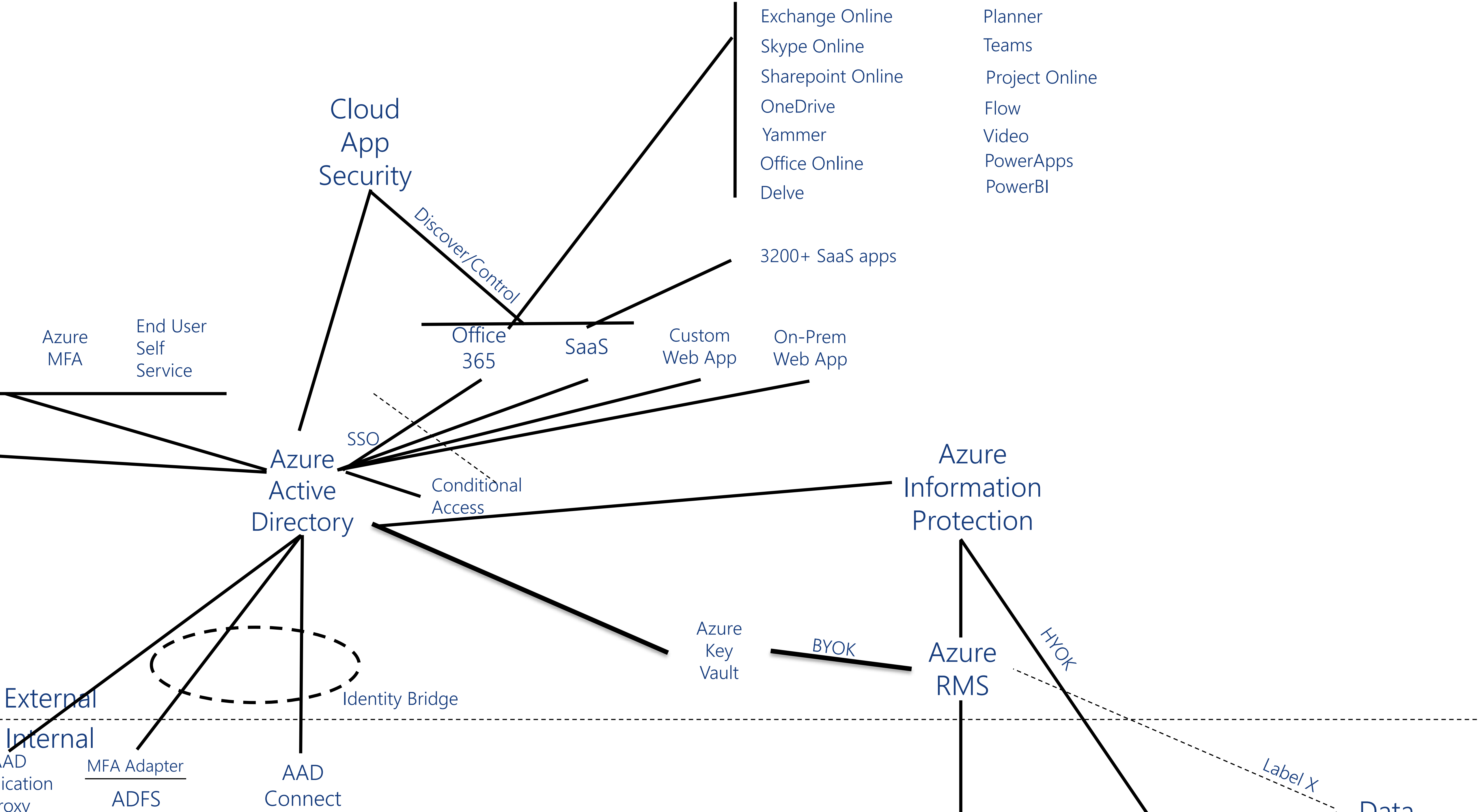
AD RMS

Exchange

SharePoint

Active Directory

Advanced Threat Analytics



Exchange Online

Skype Online

Sharepoint Online

OneDrive

Yammer

Office Online

Delve

Planner

Teams

Project Online

Flow

Video

PowerApps

PowerBI

Cloud App Security

Discover/Control

3200+ SaaS apps

Azure MFA

End User Self Service

Office 365

SaaS

Custom Web App

On-Prem Web App

SSO

Azure Active Directory

Conditional Access

Azure Information Protection

Azure Key Vault

BYOK

Azure RMS

HYOK

Identity Bridge

External

Internal

AD
ication
roxy

MFA Adapter

ADFS

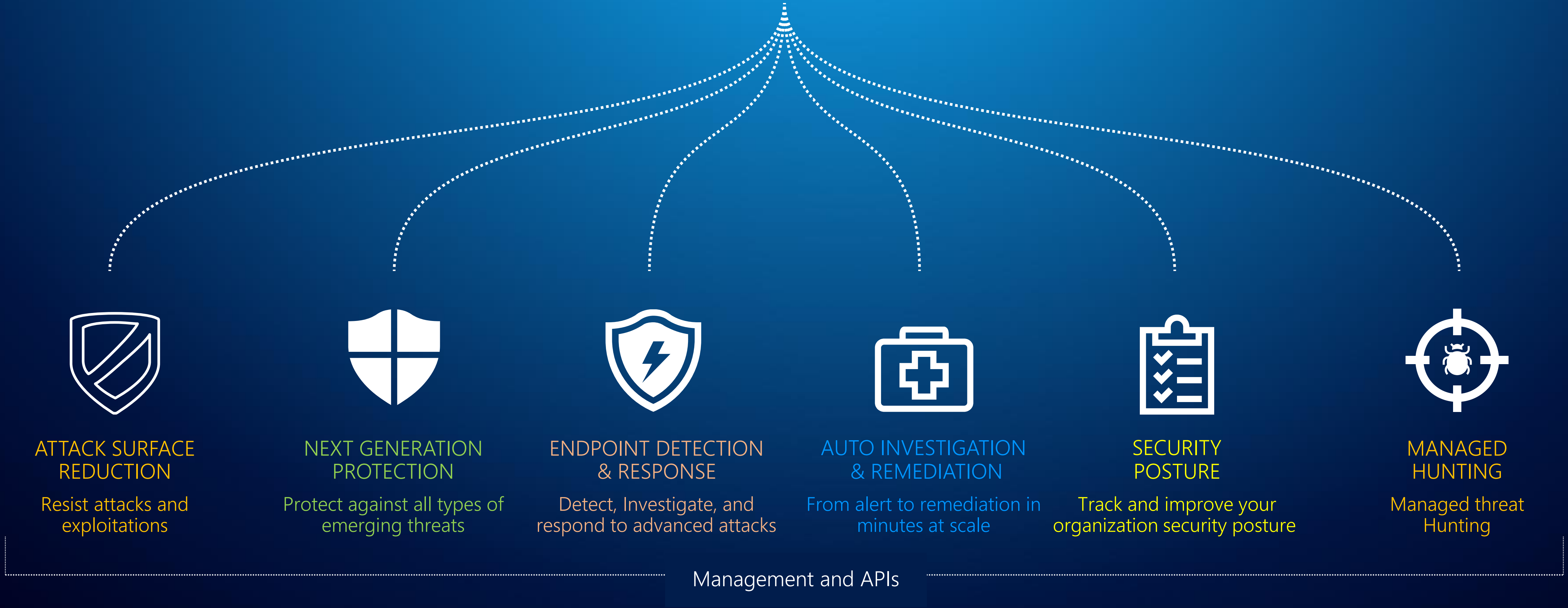
AAD Connect

Label X

Data

Windows Defender ATP

Built in. Cloud powered



ATTACK SURFACE REDUCTION

Resist attacks and exploitations

NEXT GENERATION PROTECTION

Protect against all types of emerging threats

ENDPOINT DETECTION & RESPONSE

Detect, Investigate, and respond to advanced attacks

AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale

SECURITY POSTURE

Track and improve your organization security posture

MANAGED HUNTING

Managed threat Hunting

Management and APIs

WINDOWS 10 END TO END PROTECTION

PRE-BREACH

POST-BREACH

OFF MACHINE

O365 Advanced Threat Protection

(Beyond standard E-mail filtering)

- Reducing email attack vector
- Advanced sandbox detonation
- Exploit mitigation
- Part of Office 365 E5 or Microsoft 365 E5 suites (add-on available)

Edge

(Browser)

- Browser hardening
- Reduce script based attack surface
- App container hardening with Application Guard
- Reputation based blocking for downloads (SmartScreen)

ON MACHINE

Windows Defender Exploit Guard

(Intrusion Prevention & Vulnerability Mitigation)

Attack Surface Reduction*

- Set of rules to reduce application attack surface

Controlled Folder Access*

- Protecting data against access by untrusted processes

Exploit Protection

- Mitigations against application vulnerability exploits

Network Protection*

- Blocking outbound calls to low rep sources

Device Integrity

(Secure boot processes)

- Secure Boot
- Trusted Boot
- Measured Boot
- Early Launch Anti Malware (ELAM)

Locked down device

(Hardened platform)

- Windows 10S
- Device Guard

System Guard

(Virtualization based security)

- Application isolation
- Credential isolation

Application Control

(Whitelist Executables)

- Only allowed apps can run
- Based on reputation list maintained by MS

Windows Defender Antivirus*

(Antimalware)

- Improved ML and heuristic protection
- Instantly protected with the cloud
- Enhanced Exploit Kit Detections
- Advanced anti-tampering

AntiMalware Scan Interface

(Script based attack detection)

- Improved detection for script based attacks
- AMSI for VBS/JS script runtime

Windows Defender Antivirus behavioral engine*

(Behavior Analysis)

- Enhanced behavioral and machine learning detection library
- Process tree visualizations
- Artifact searching capabilities
- Memory scanning capabilities

Windows Defender Advanced Threat Protection**

(Enterprise Detection and Response)

- Enhanced behavioral and machine learning detection library
- Process tree visualizations
- Artifact searching capabilities
- Machine Isolation and quarantine
- Part of Windows Enterprise E5 or corresponding M365 E5 suite
- Automatic investigation and remediation COMING SOON (Hexadite)

OFF MACHINE

OneDrive for Business

(Cloud Storage)

- Reliable versioned file storage in the cloud
- Point in time file recovery

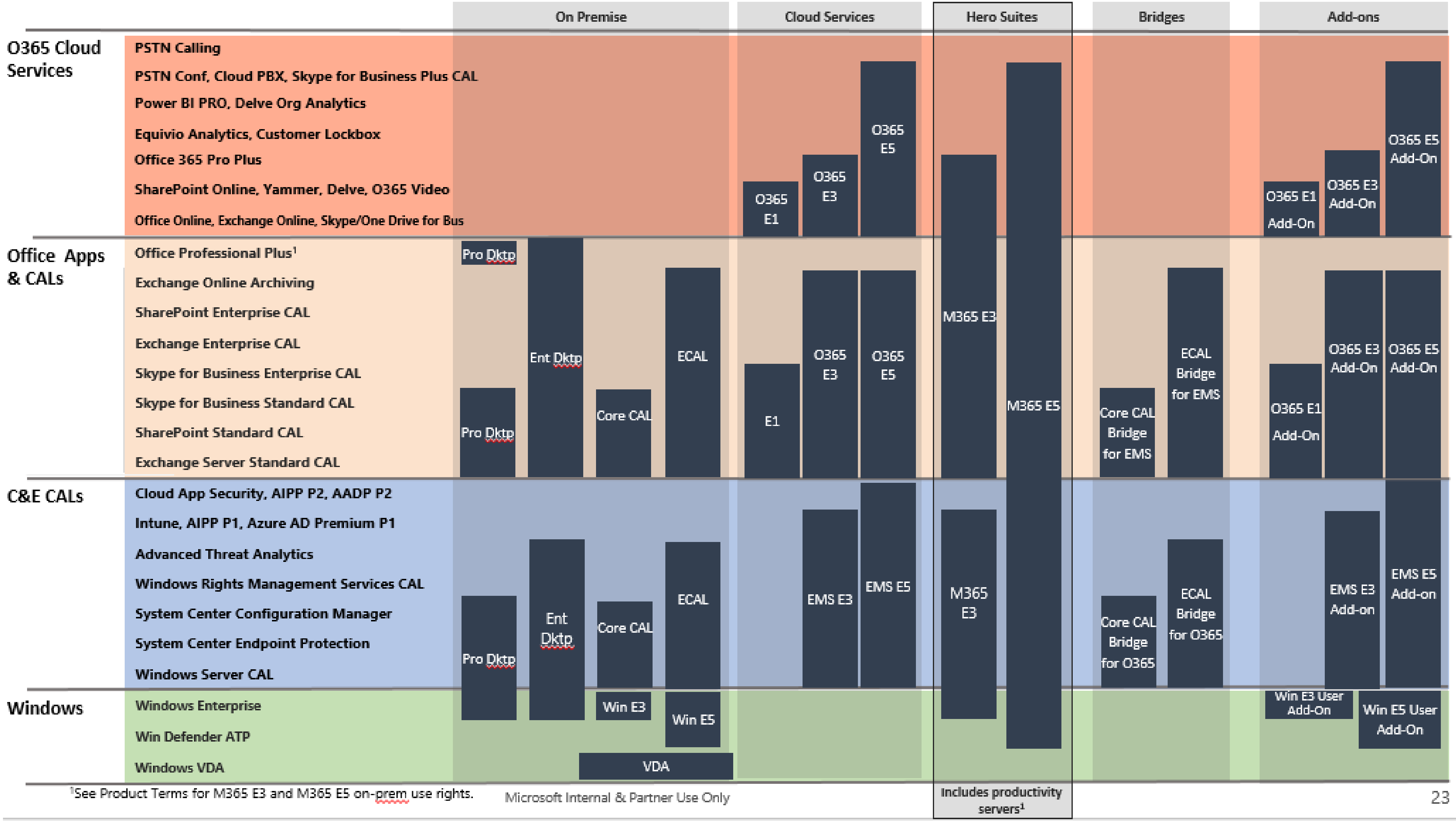
Office 365 TI & Windows Security Center

(Security Management)

- Investigate and respond to attacks by seeing activity, correlating signals and taking remediation actions

*requires Windows Defender Antivirus as the active/only antimalware solution

**can run side-by-side with any antimalware solution, no agent required



On Premise | Cloud Services | Hero Suites | Bridges | Add-ons

O365 Cloud Services

- PSTN Calling
- PSTN Conf, Cloud PBX, Skype for Business Plus CAL
- Power BI PRO, Delve Org Analytics
- Equivio Analytics, Customer Lockbox
- Office 365 Pro Plus
- SharePoint Online, Yammer, Delve, O365 Video
- Office Online, Exchange Online, Skype/One Drive for Bus

Office Apps & CALs

- Office Professional Plus[1]
- Exchange Online Archiving
- SharePoint Enterprise CAL
- Exchange Enterprise CAL
- Skype for Business Enterprise CAL
- Skype for Business Standard CAL
- SharePoint Standard CAL
- Exchange Server Standard CAL

C&E CALs

- Cloud App Security, AIPP P2, AADP P2
- Intune, AIPP P1, Azure AD Premium P1
- Advanced Threat Analytics
- Windows Rights Management Services CAL
- System Center Configuration Manager
- System Center Endpoint Protection
- Windows Server CAL

Windows

- Windows Enterprise
- Win Defender ATP
- Windows VDA

[1] See Product Terms for M365 E3 and M365 E5 on-prem use rights.

KPCS

ATOM

Ondrej Vysek | Microsoft MVP | vysek@kpcs.cz

DO IT MODERN (AND SECURE) WAY