Wiki Webinar

by inetum realdolmen

Microsoft 365 Defender Threat Protection:

Een gedegen security-oplossing

Microsoft

Praktische afspraken

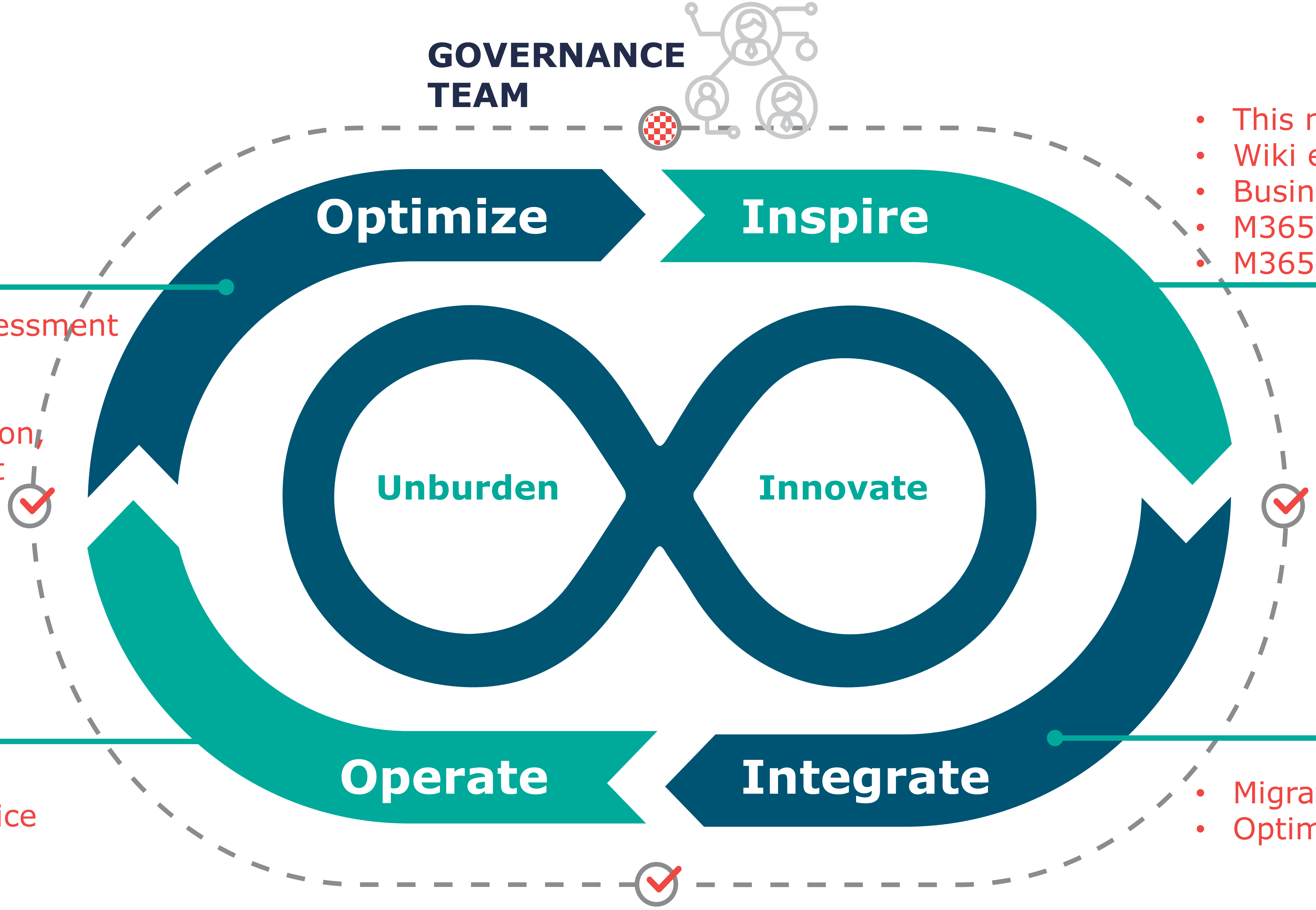
- Vragen via chat
- Iedereen op mute
- Q&A na de presentatie
- Evaluatie met link naar de slides worden na het event doorgestuurd

inetum

realdolmen

Positive digital flow

Zero Trust – Threat Protection



- This meeting
- Wiki events
- Business Productivity Roadmap
- M365 Roadmap
- M365 Jumpstart

- Security Priority Assessment
- Calling Assessment
- Proactive Services
- Training, user adoption, change management

- Managed Services
- Workplace as a Service

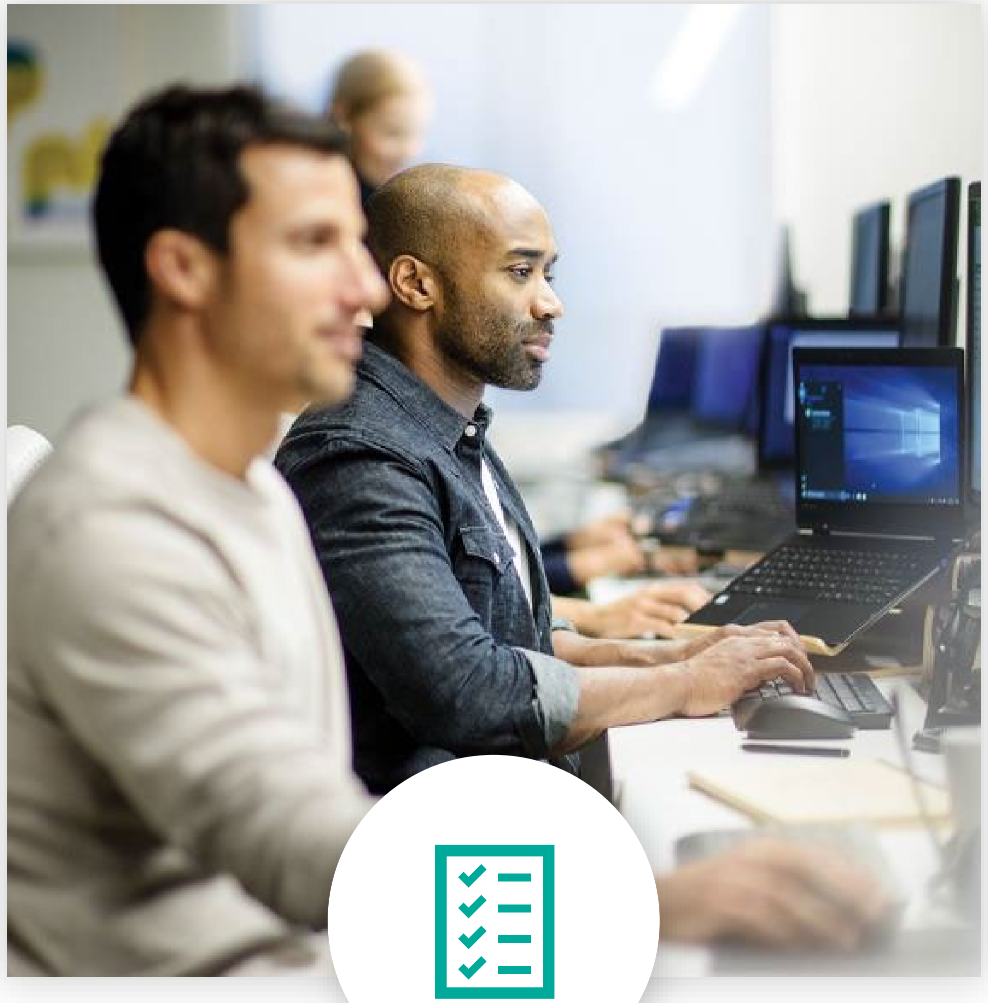
- Migration
- Optimization

Zero Trust Roadmap

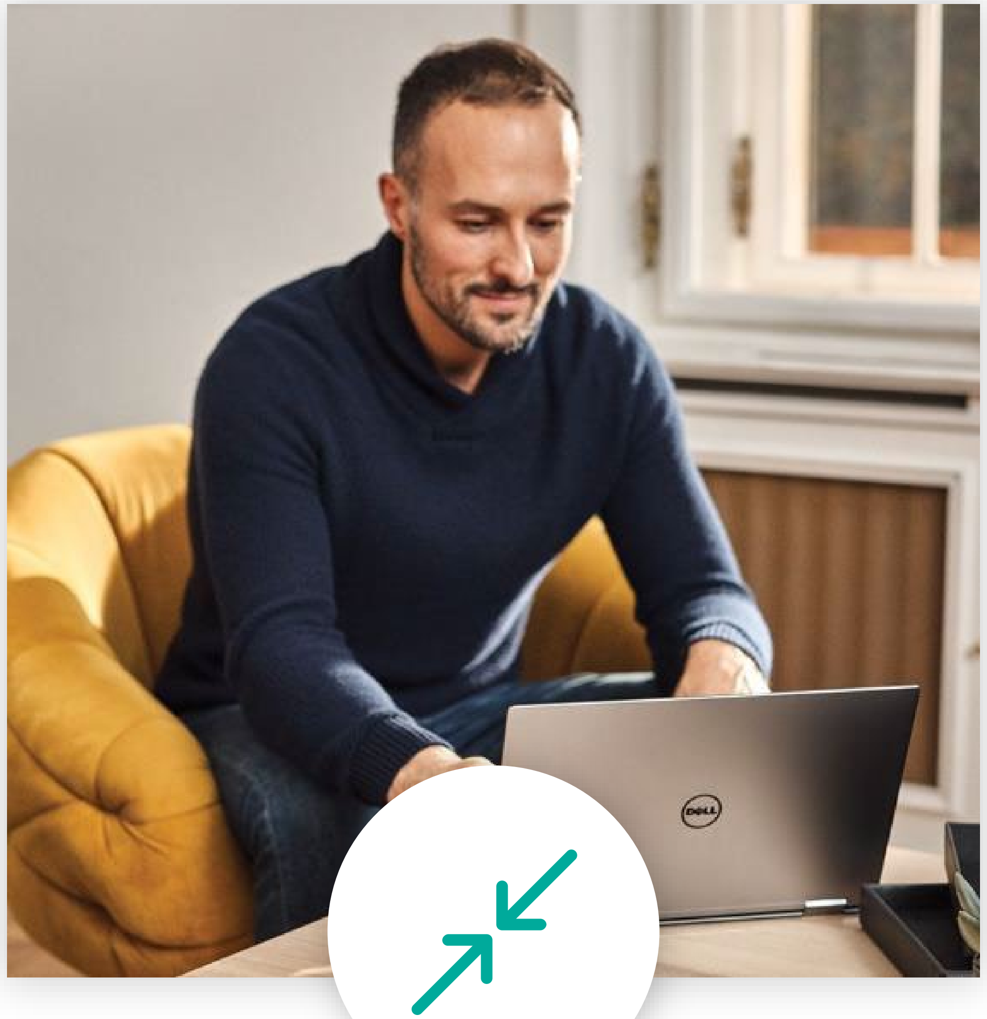
	Identities	Devices	Network & Infrastructure	Applications	Data
TRADITIONAL	No SSO between cloud and on-premises apps Visibility into identity risk is very limited	Devices are domain joined No overview and inventory of devices	Flat open network with unencrypted traffic Minimal threat protection	On-premises apps and no cloud apps No overview of shadow IT	Access is governed by perimeter Unencrypted and without classification
ADVANCED	Basic conditional access policies with basic MFA Cloud identity federation and visibility into identity risk	Devices are registered with a cloud identity provider DLP policies for BYOD	Basic network segmentation Cloud native filtering and threat protection	Apps configured with SSO + discover shadow IT Critical apps are monitored	Access is governed by classification Encrypted and classified via keywords
OPTIMAL	Password less authentication Phishing-proof MFA User behavior is analyzed in real time Enforce least privilege access	Endpoint threat protection is used to monitor device risk Access control is gated on device risk Continuous risk-based asset management	Micro segmentation ML-based threat protection and filtering All traffic is encrypted	Apps are available using least privilege access In-session monitoring and response Assess the security posture of cloud apps	Classification by AI DLP policies based on classification Access governed by cloud security policy engine

← Visibility, analytics, automation & governance →

A new reality needs new principles



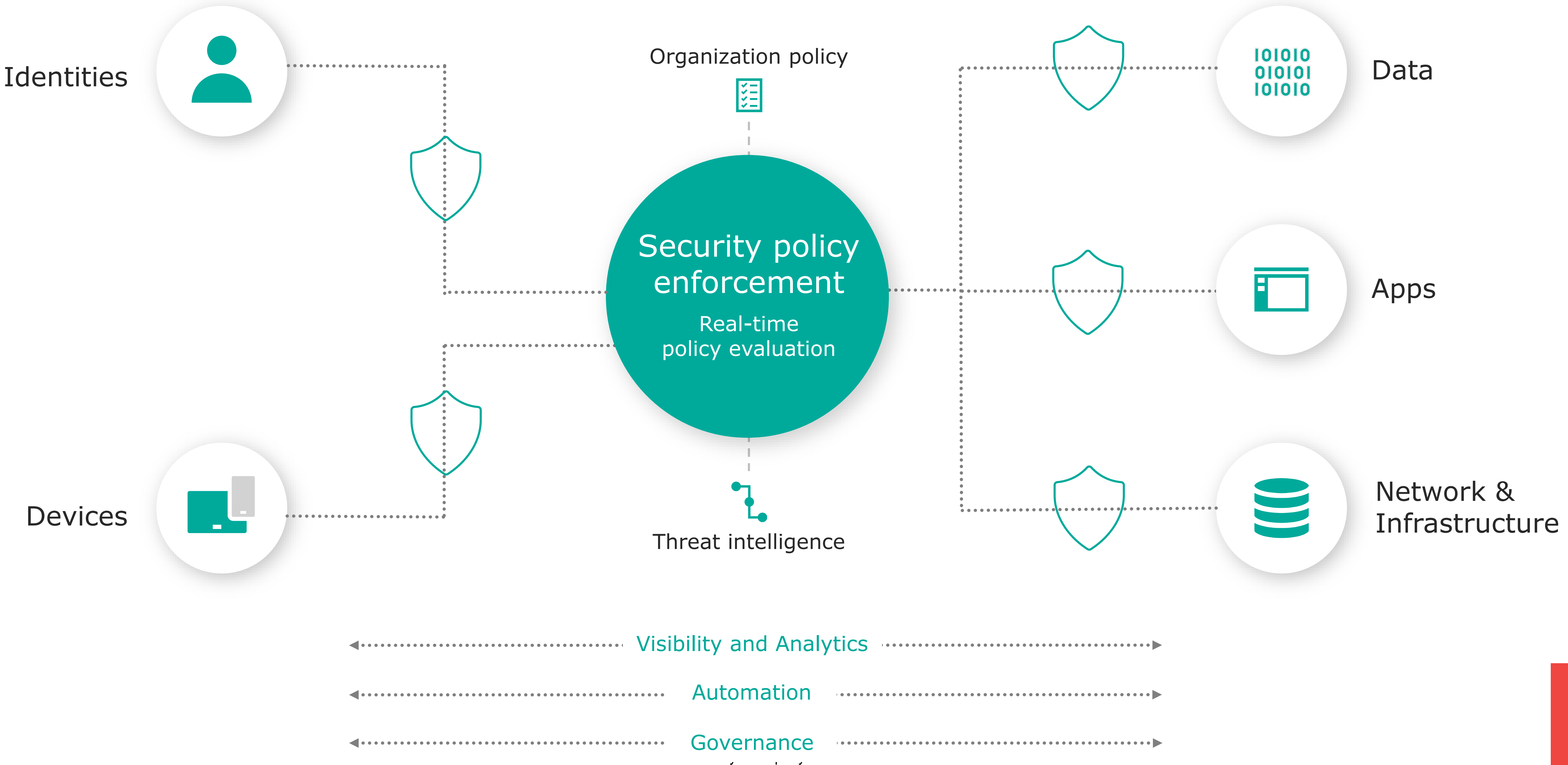
Verify explicitly



Use least privilege access

Assume breach

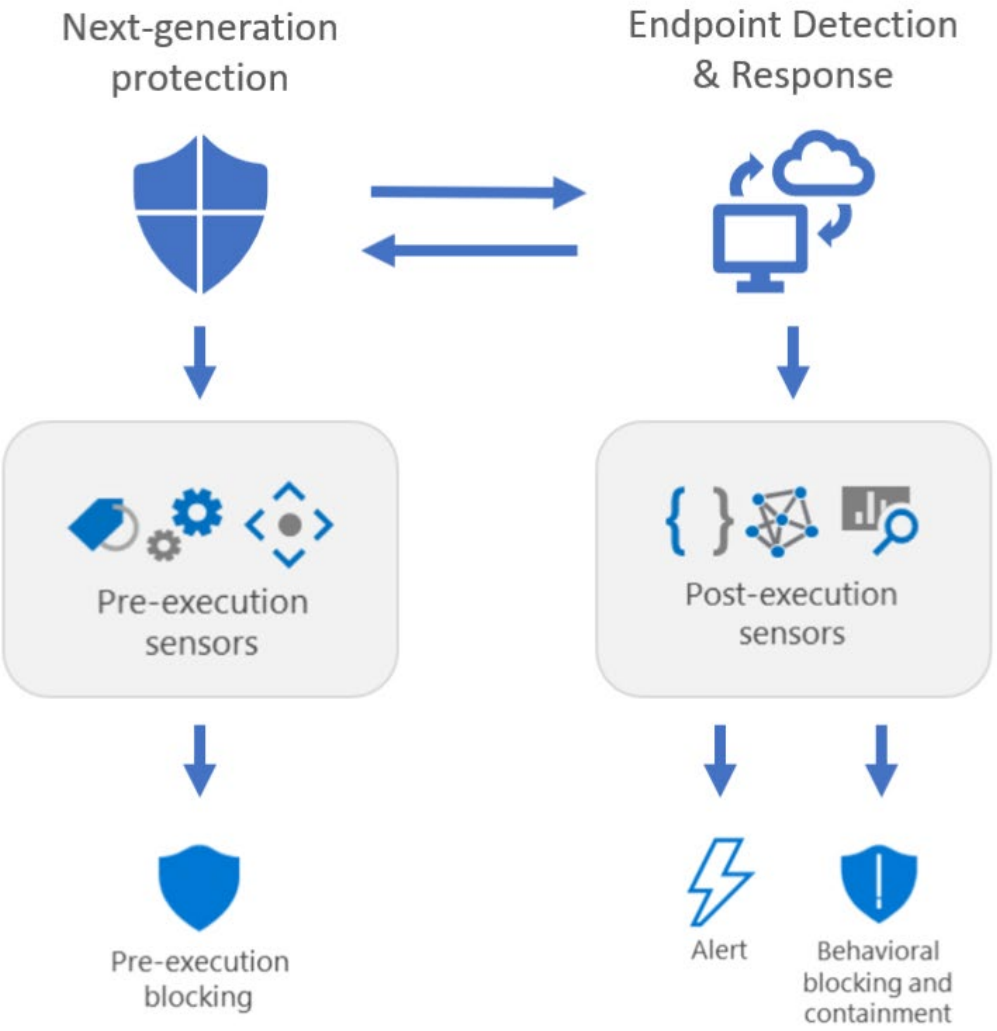
Zero Trust Architecture



Threat what? I have an Antivirus!

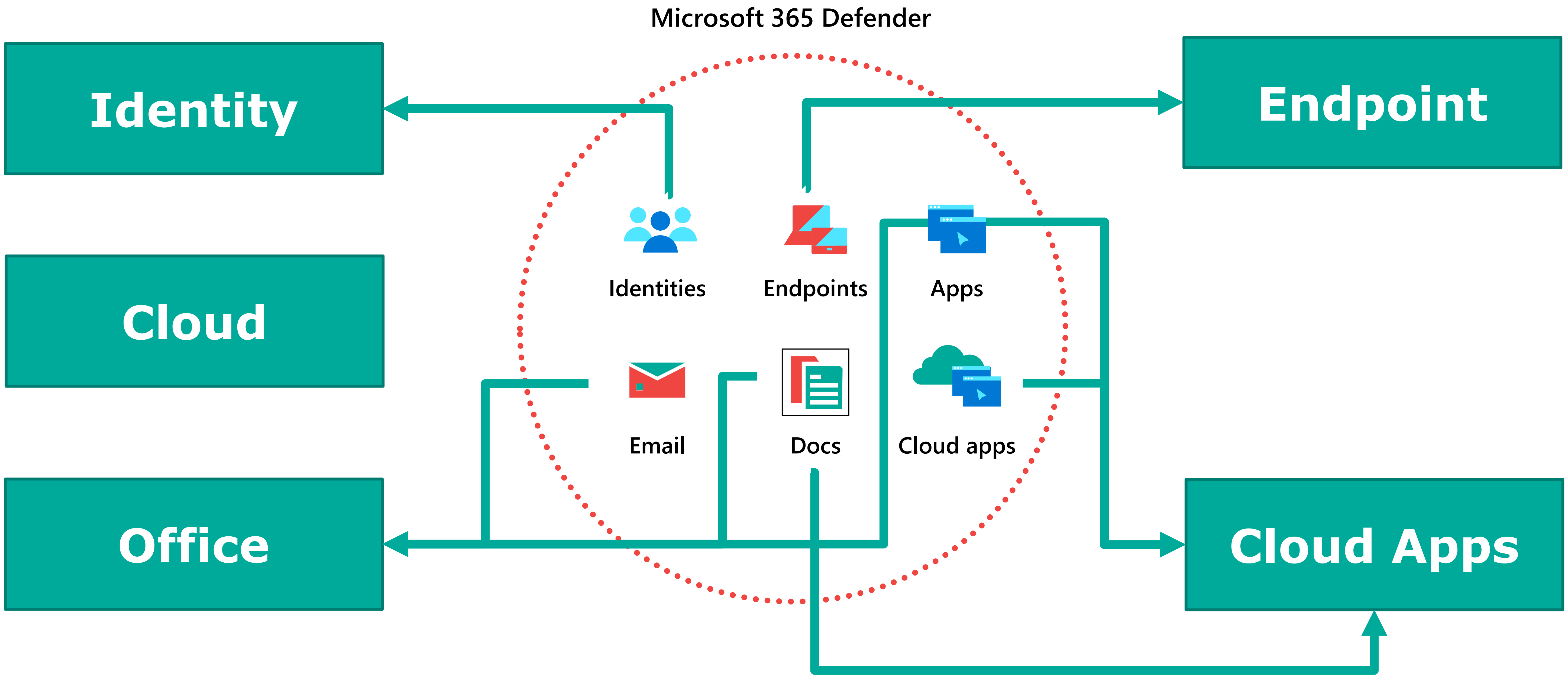
Anti Virus

Endpoint Detection and Response

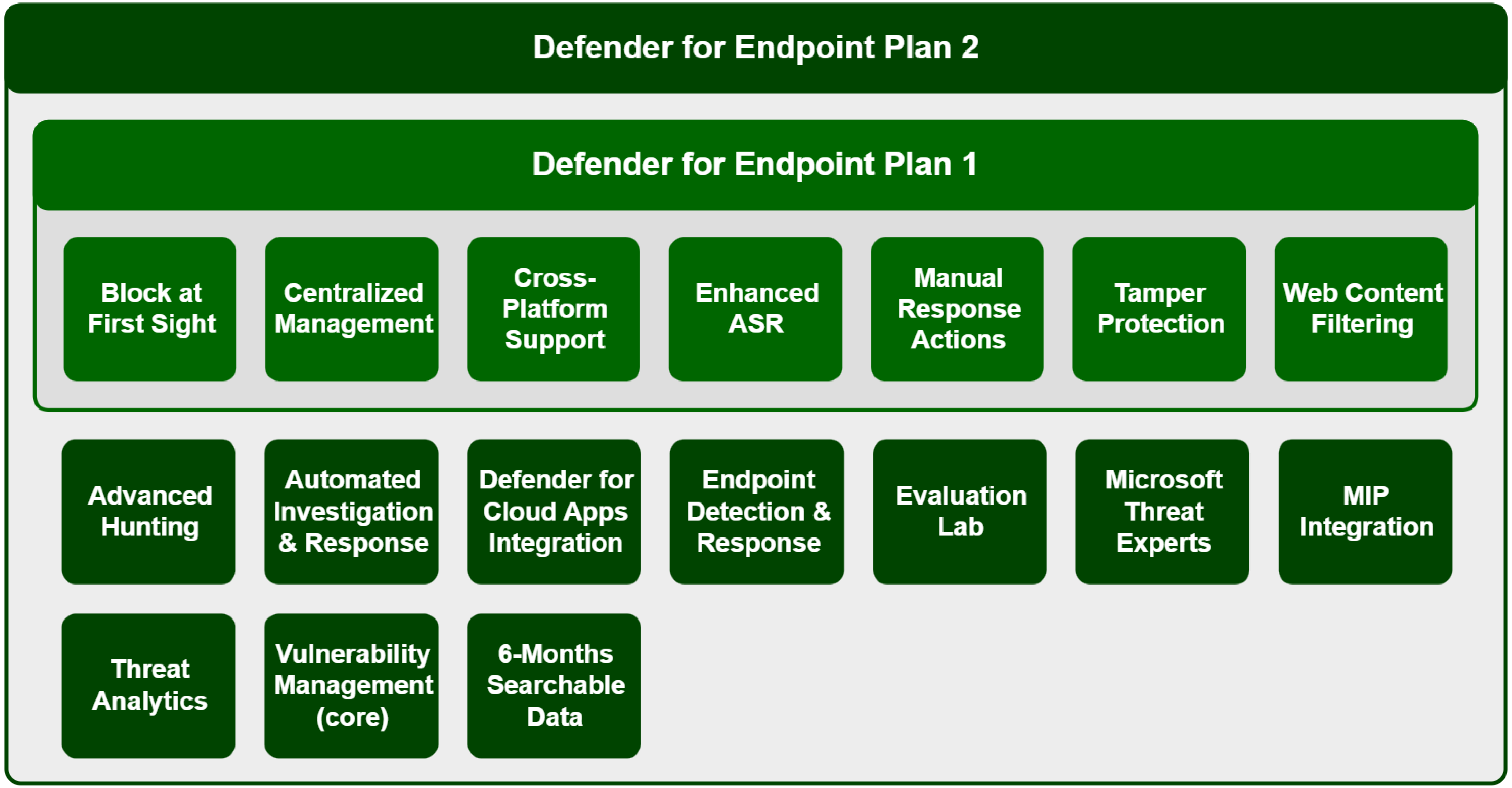

Next-generation protection
Endpoint Detection & Response
Pre-execution sensors
Post-execution sensors
Pre-execution blocking
Alert
Behavioral blocking and containment

Microsoft Defender for Endpoint

Microsoft Defender for…



Defender for Endpoint



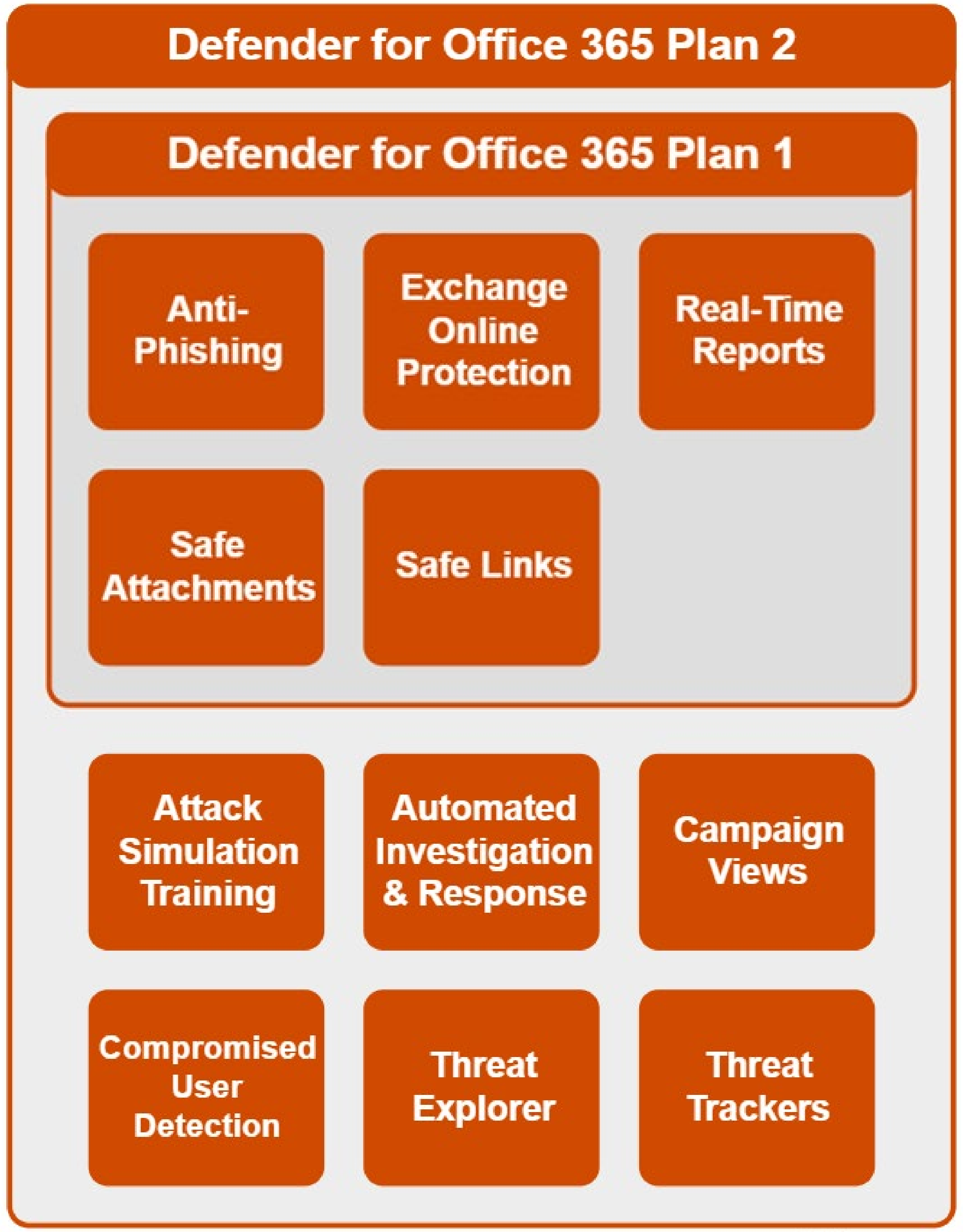
Defender for Endpoint Plan 2

Defender for Endpoint Plan 1

- Block at First Sight
- Centralized Management
- Cross-Platform Support
- Enhanced ASR
- Manual Response Actions
- Tamper Protection
- Web Content Filtering

- Advanced Hunting
- Automated Investigation & Response
- Defender for Cloud Apps Integration
- Endpoint Detection & Response
- Evaluation Lab
- Microsoft Threat Experts
- MIP Integration
- Threat Analytics
- Vulnerability Management (core)
- 6-Months Searchable Data

Defender for Office



Defender for Office 365 Plan 2

Defender for Office 365 Plan 1

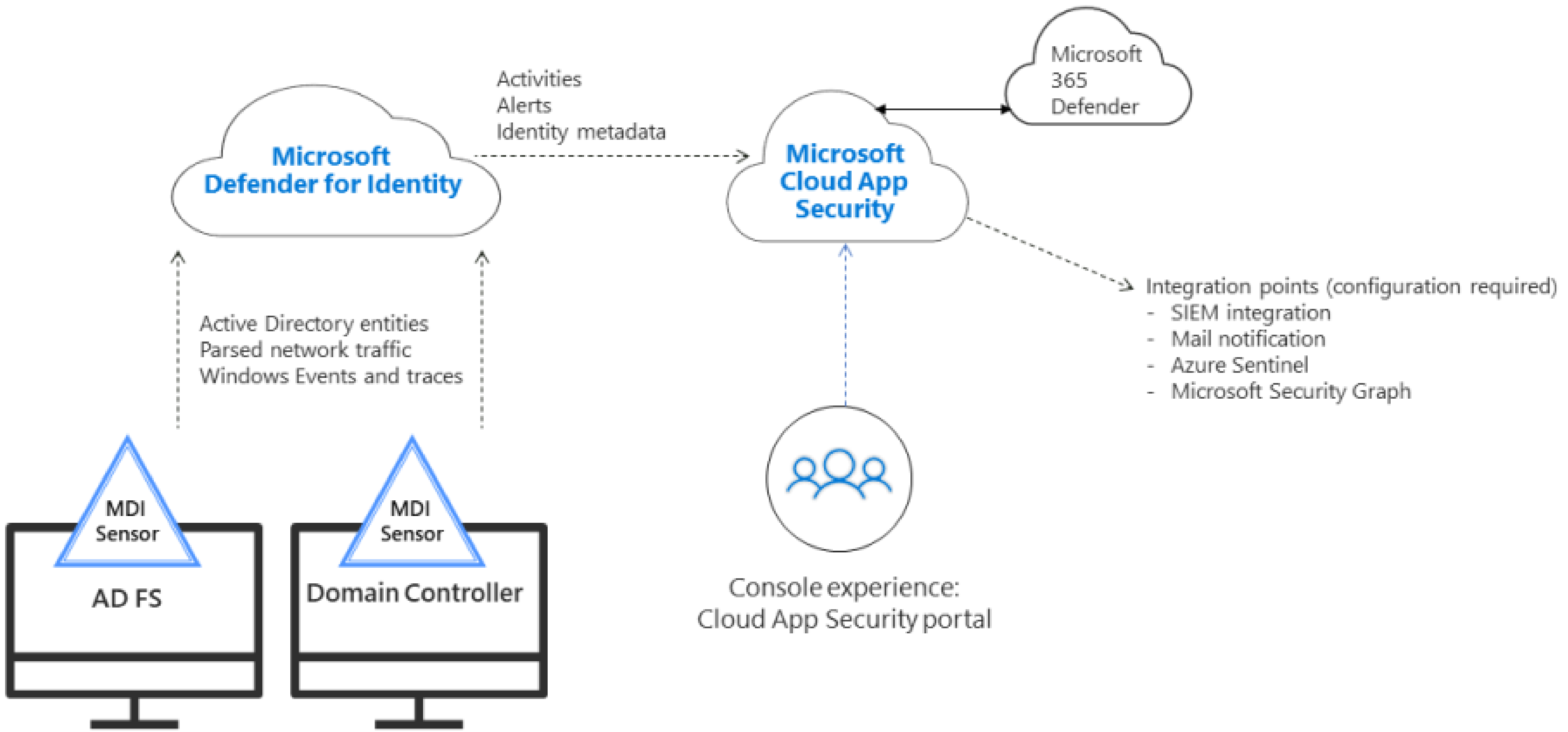
- Anti-Phishing
- Exchange Online Protection
- Real-Time Reports
- Safe Attachments
- Safe Links

- Attack Simulation Training
- Automated Investigation & Response
- Campaign Views
- Compromised User Detection
- Threat Explorer
- Threat Trackers

Defender for Identity

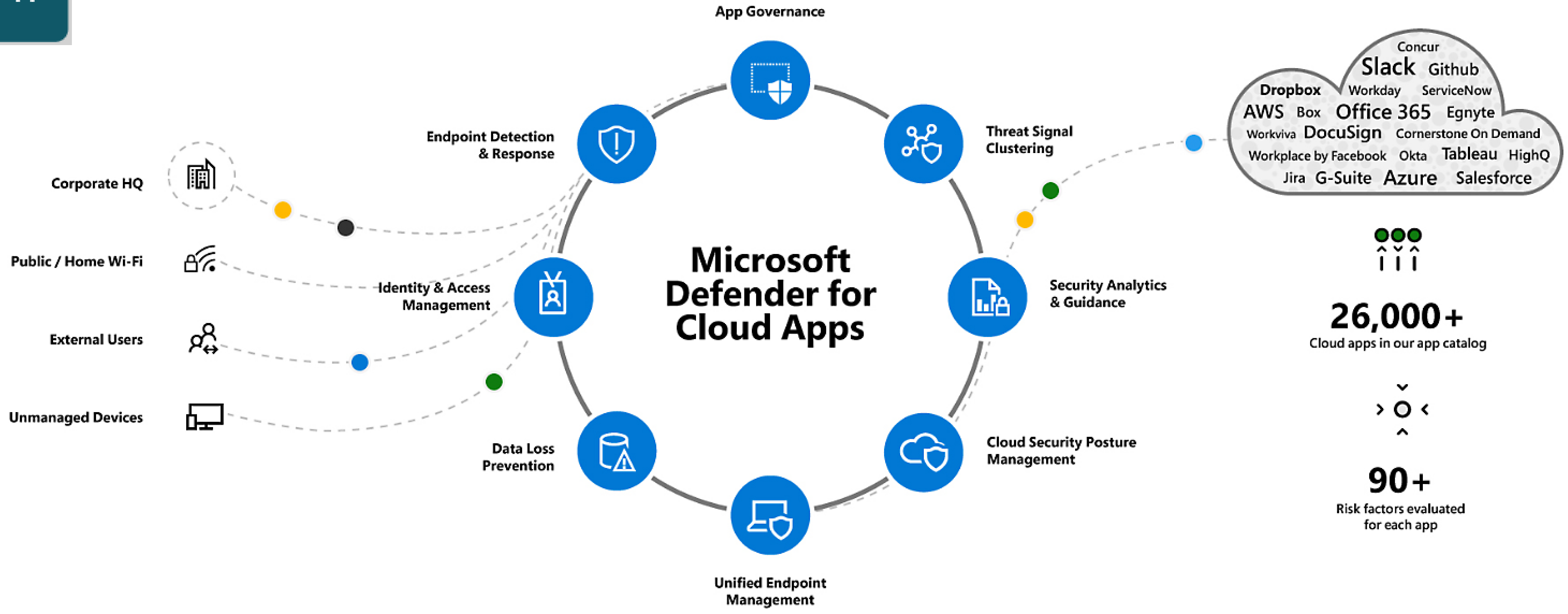
Defender for Identity

Microsoft Defender for Identity Architecture


Microsoft
365
Defender
Activities
Alerts
Identity metadata
Microsoft Defender for Identity
Microsoft Cloud App Security
Integration points (configuration required)
- SIEM integration
- Mail notification
- Azure Sentinel
- Microsoft Security Graph
Active Directory entities
Parsed network traffic
Windows Events and traces
MDI Sensor
AD FS
MDI Sensor
Domain Controller
Console experience:
Cloud App Security portal

Defender for Cloud apps

Defender for Cloud Apps



Corporate HQ

Public / Home Wi-Fi

External Users

Unmanaged Devices

App Governance

Endpoint Detection & Response

Threat Signal Clustering

Identity & Access Management

Microsoft Defender for Cloud Apps

Security Analytics & Guidance

Data Loss Prevention

Cloud Security Posture Management

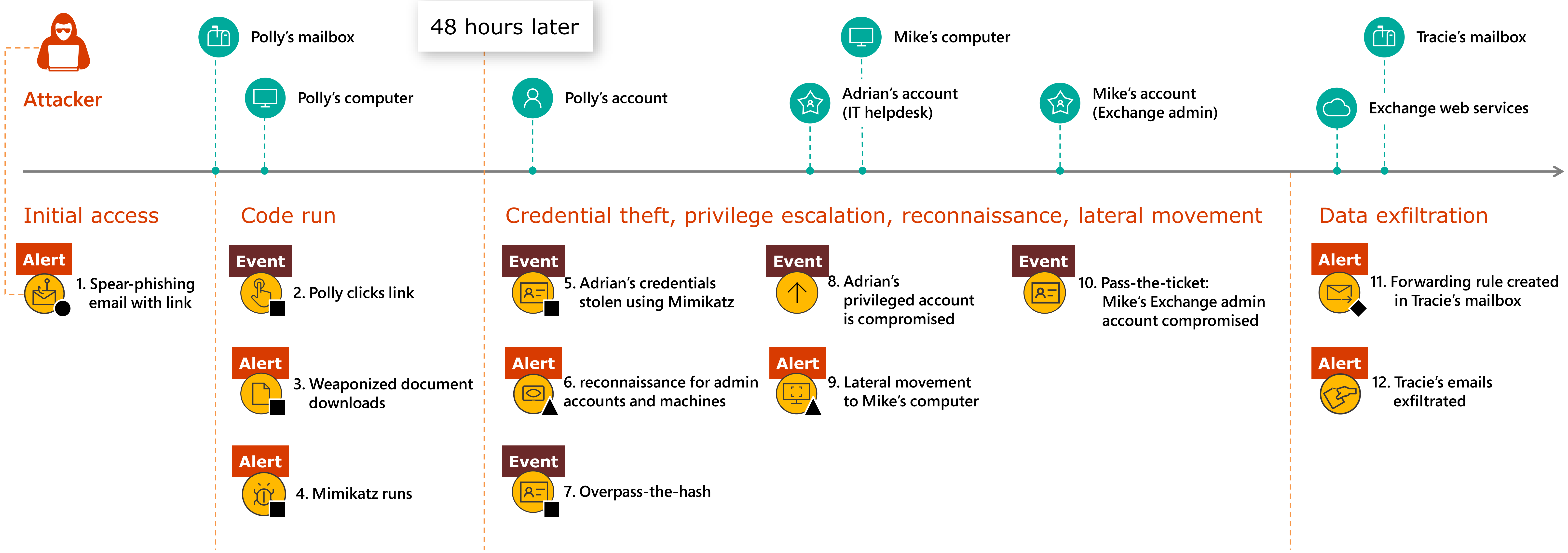
Unified Endpoint Management

Concur Slack Github Dropbox Workday ServiceNow AWS Box Office 365 Egnyte Workviva DocuSign Cornerstone On Demand Workplace by Facebook Okta Tableau HighQ Jira G-Suite Azure Salesforce

26,000+
Cloud apps in our app catalog

90+
Risk factors evaluated for each app

Why is it challenging?



48 hours later

Attacker

Polly's mailbox

Polly's computer

Polly's account

Adrian's account (IT helpdesk)

Mike's computer

Mike's account (Exchange admin)

Exchange web services

Tracie's mailbox

Initial access

Alert ●
1. Spear-phishing email with link

Code run

Event ■
2. Polly clicks link

Alert ■
3. Weaponized document downloads

Alert ■
4. Mimikatz runs

Credential theft, privilege escalation, reconnaissance, lateral movement

Event ■
5. Adrian's credentials stolen using Mimikatz

Alert ▲
6. reconnaissance for admin accounts and machines

Event ■
7. Overpass-the-hash

Event
8. Adrian's privileged account is compromised

Alert ▲
9. Lateral movement to Mike's computer

Event
10. Pass-the-ticket: Mike's Exchange admin account compromised

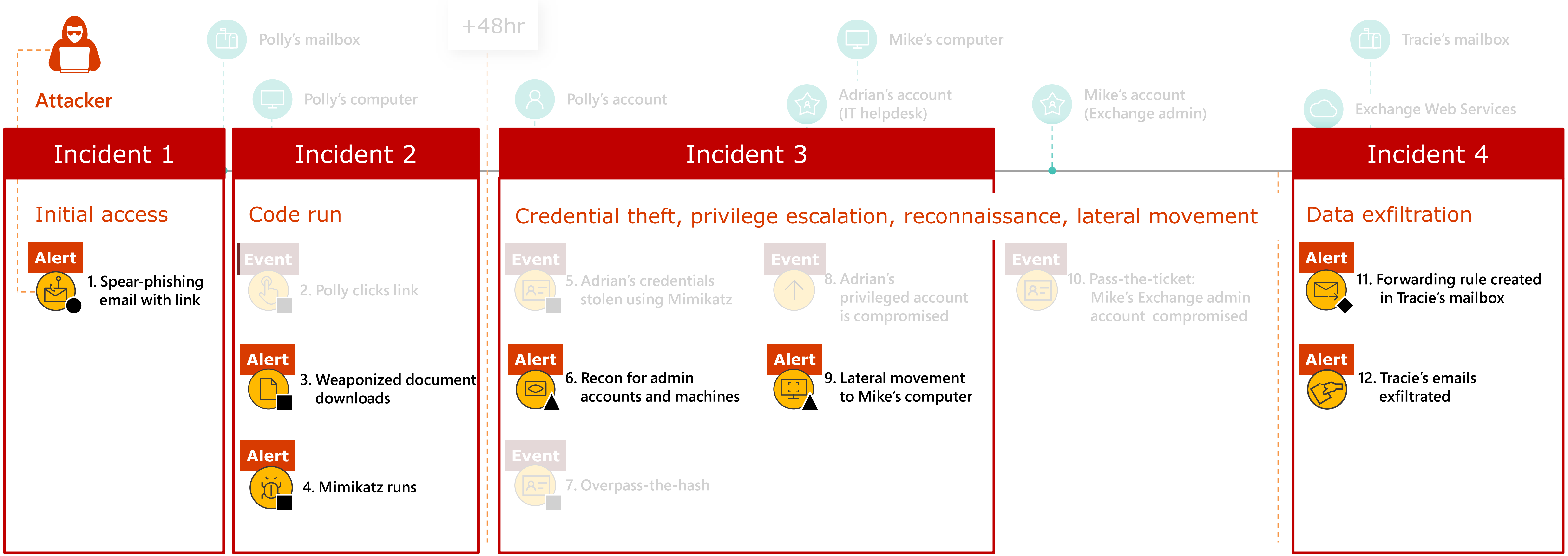
Data exfiltration

Alert ◆
11. Forwarding rule created in Tracie's mailbox

Alert
12. Tracie's emails exfiltrated

● Microsoft Defender for Office 365 ■ Microsoft Defender for Endpoint ▲ Microsoft Defender for Identity ◆ Microsoft Cloud Application Security

Why is it challenging – generic tools logic



Attacker

Polly's mailbox

Polly's computer

+48hr

Polly's account

Mike's computer

Adrian's account (IT helpdesk)

Mike's account (Exchange admin)

Tracie's mailbox

Exchange Web Services

Incident 1

Initial access

Alert ● 1. Spear-phishing email with link

Incident 2

Code run

Event ■ 2. Polly clicks link

Alert ■ 3. Weaponized document downloads

Alert ■ 4. Mimikatz runs

Incident 3

Credential theft, privilege escalation, reconnaissance, lateral movement

Event ■ 5. Adrian's credentials stolen using Mimikatz

Event 8. Adrian's privileged account is compromised

Event 10. Pass-the-ticket: Mike's Exchange admin account compromised

Alert ▲ 6. Recon for admin accounts and machines

Alert ▲ 9. Lateral movement to Mike's computer

Event ■ 7. Overpass-the-hash

Incident 4

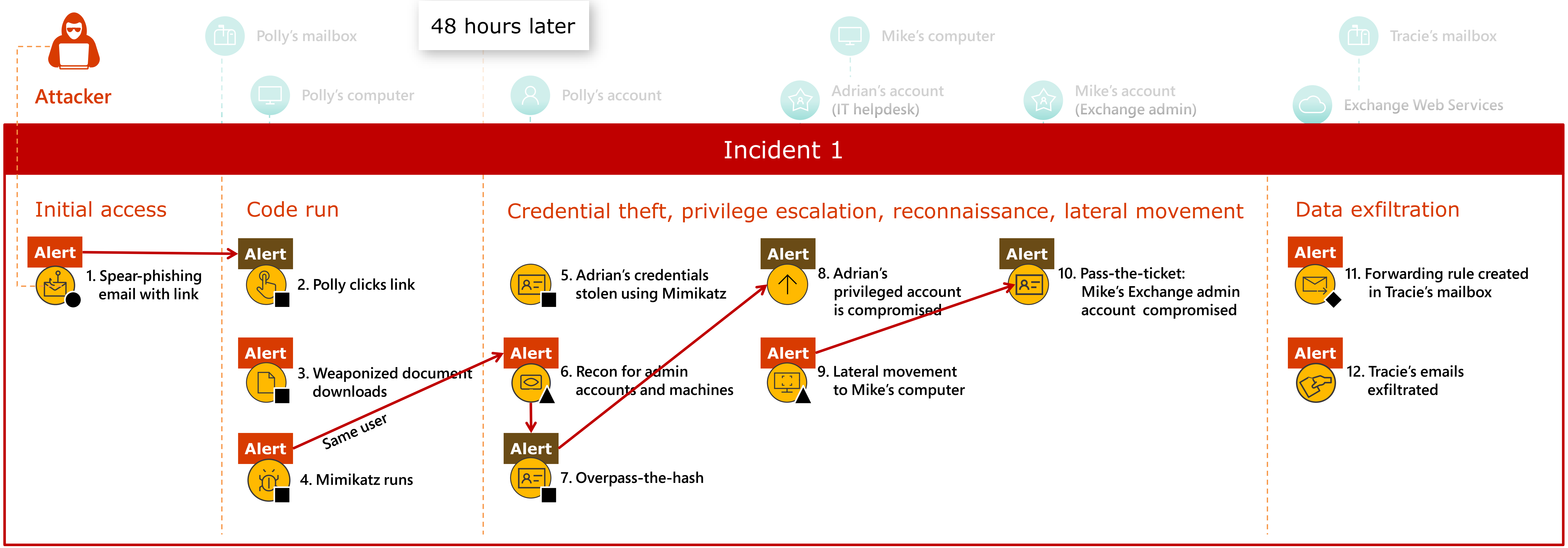
Data exfiltration

Alert ◆ 11. Forwarding rule created in Tracie's mailbox

Alert 12. Tracie's emails exfiltrated

● Microsoft Defender for Office 365 ■ Microsoft Defender for Endpoint ▲ Microsoft Defender for Identity ◆ Microsoft Cloud Application Security

Why is it challenging – with proper logic



Attacker

Polly's mailbox

Polly's computer

48 hours later

Polly's account

Mike's computer

Adrian's account (IT helpdesk)

Mike's account (Exchange admin)

Tracie's mailbox

Exchange Web Services

Incident 1

Initial access

Alert ● 1. Spear-phishing email with link

Code run

Alert ■ 2. Polly clicks link

Alert ■ 3. Weaponized document downloads

Alert ■ 4. Mimikatz runs

Same user

Credential theft, privilege escalation, reconnaissance, lateral movement

■ 5. Adrian's credentials stolen using Mimikatz

Alert ▲ 6. Recon for admin accounts and machines

Alert ■ 7. Overpass-the-hash

Alert 8. Adrian's privileged account is compromised

Alert ▲ 9. Lateral movement to Mike's computer

Alert 10. Pass-the-ticket: Mike's Exchange admin account compromised

Data exfiltration

Alert ◆ 11. Forwarding rule created in Tracie's mailbox

Alert 12. Tracie's emails exfiltrated

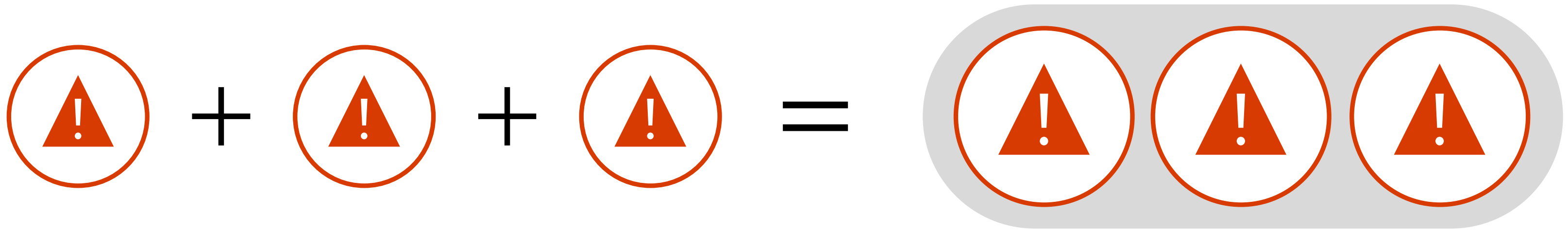
● Microsoft Defender for Office 365 ■ Microsoft Defender for Endpoint ▲ Microsoft Defender for Identity ◆ Microsoft Cloud Application Security

Microsoft 365 Defender incident analytics

More than simply combining alerts

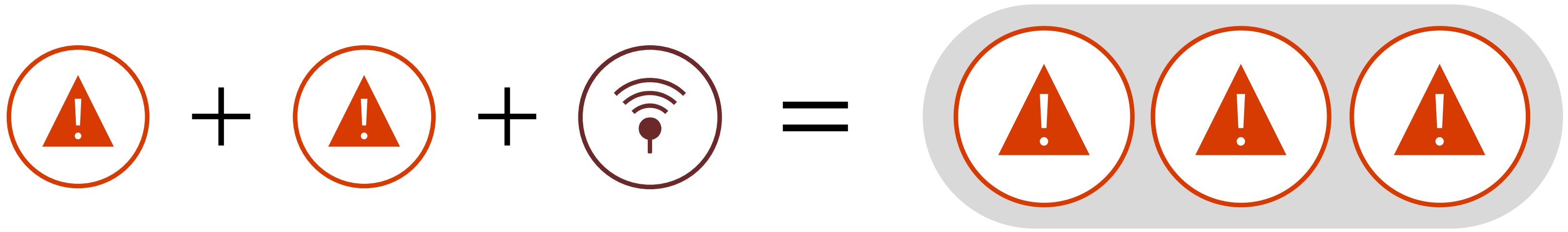
Alert→Alert

Analytic understanding of existing alerts across ATP products (both in-product and cross-product)



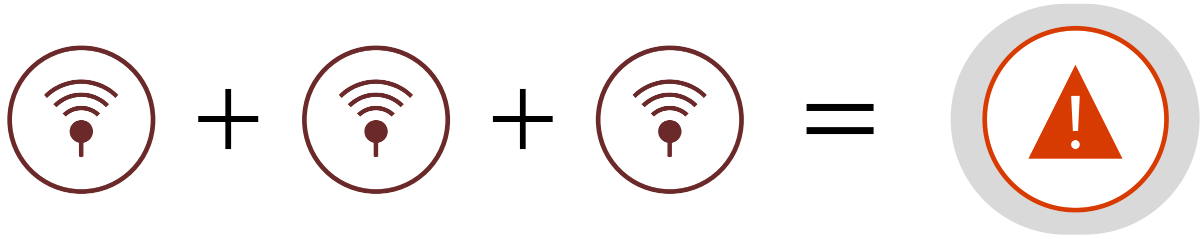
Alert→Event

Combining alerts raised by a product with relevant telemetry of another product, promoting events to alerts

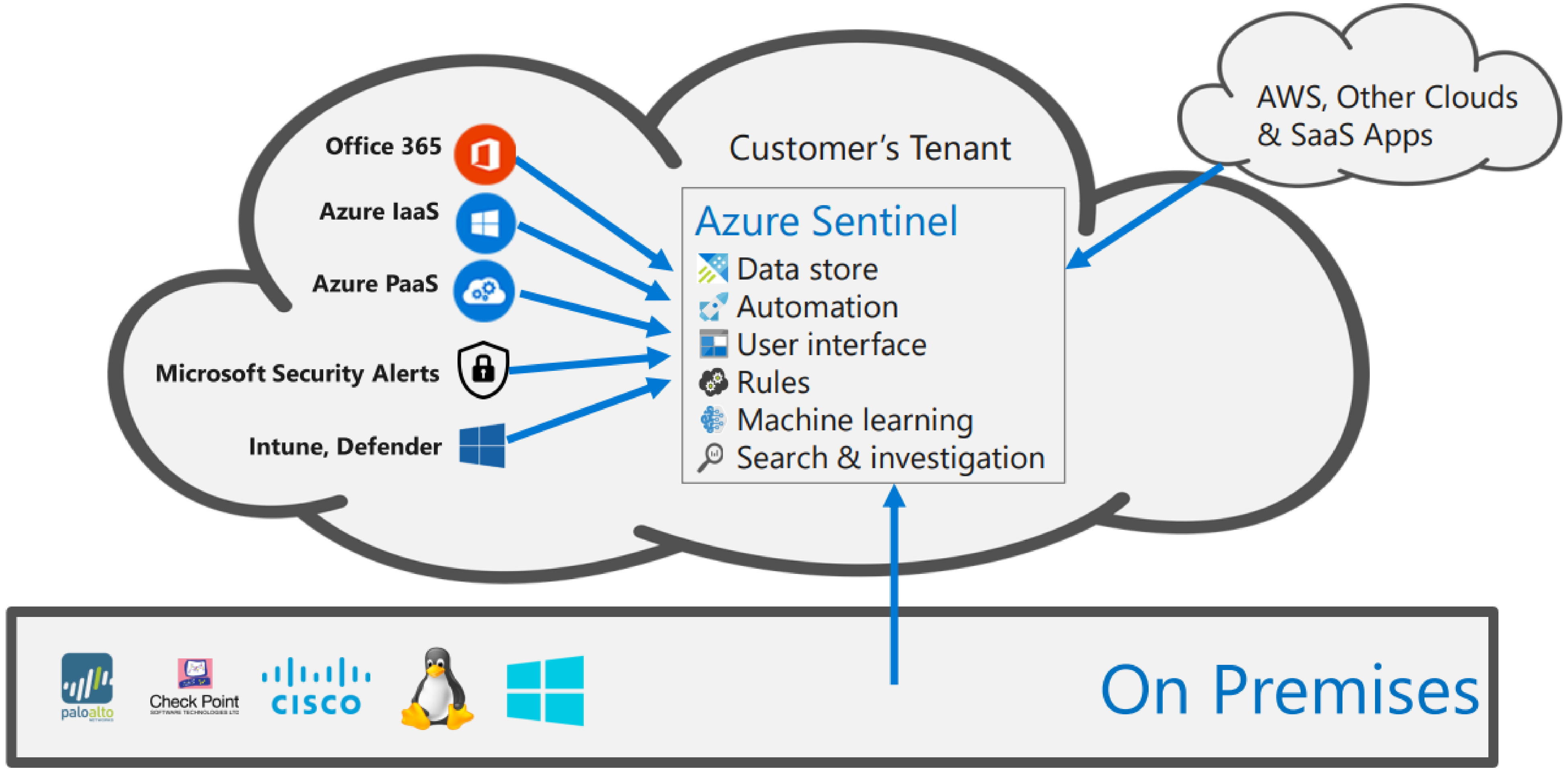


Event→Event

Weak signal combination generating new alerts when no individual product had enough confidence



LiveSOC.



3 | SOC MADRID
SOC SEVILLE
SOC BILBAO

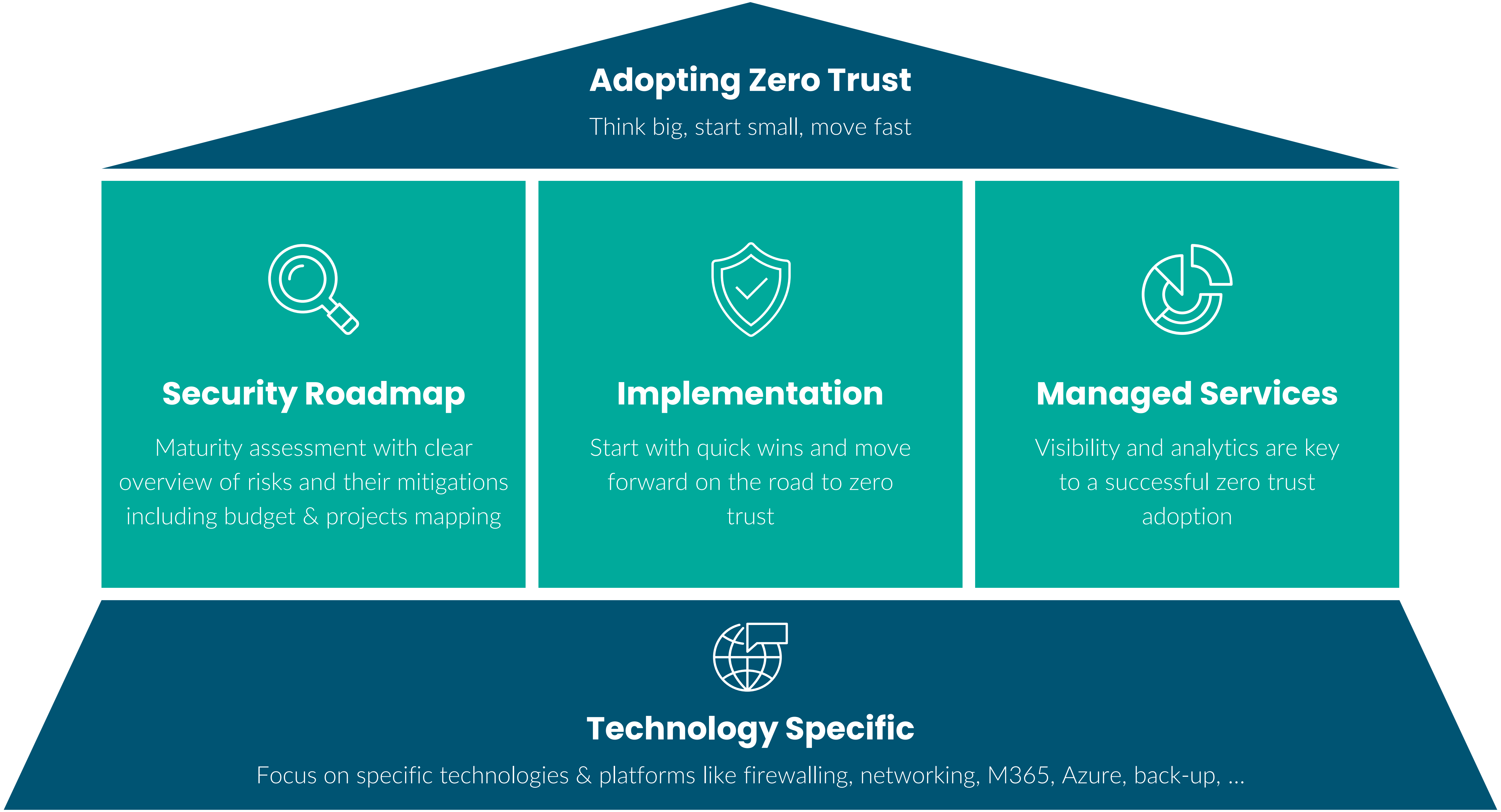
+85 PEOPLE (Spain)

BILBAO
MADRID
SEVILLE

inetum
realdolmen
Positive digital flow

Q&A

Security adoption



Adopting Zero Trust

Think big, start small, move fast

Security Roadmap

Maturity assessment with clear overview of risks and their mitigations including budget & projects mapping

Implementation

Start with quick wins and move forward on the road to zero trust

Managed Services

Visibility and analytics are key to a successful zero trust adoption

Technology Specific

Focus on specific technologies & platforms like firewalling, networking, M365, Azure, back-up, …

Toekomstige webinars rond Zero Trust

15/02 Aan de slag met big data? Beheer de overvloed aan data met Azure Purview

www.inetum-realdolmen.world/nl/events

Contacteer ons via:

- info@inetum-realdolmen.world
- Uw vertrouwde contactpersoon bij Inetum-Realdolmen
- Evaluatieformulier

Sensitivity: Company

inetum.
realdolmen
Positive digital flow

inetum.world

FRANCE | SPAIN | PORTUGAL | BELGIUM | SWITZERLAND | LUXEMBOURG | ENGLAND |
POLAND | ROMANIA | MOROCCO | TUNISIA | SENEGAL | CÔTE D'IVOIRE | ANGOLA |
CAMEROON | USA | BRAZIL | COLOMBIA | MEXICO | RP OF PANAMA | PERU | CHILI |
COSTA RICA | DOMINICAN REPUBLIC | ARGENTINA | SINGAPORE | UAE