

MICROSOFT 365
Virtual **MARATHON**

May 27 & 28, 2020
36 hours / 2 days

MICROSOFT 365 VIRTUAL MARATHON

Securing and monitoring your Azure AD identities

THOMAS NAUNHEIM

@Thomas_Live

www.cloud-architekt.net



Brought to you by:
The Global Microsoft Community



M365VirtualMarathon.com | #M365VM

THANK YOU TO ALL OUR GENEROUS SPONSORS



PERFICIENT

 CoreView



 AvePoint®



 **affirma**

 **KWizCom**
Knowledge Worker Components

 **Valo**

 **SWOOP**
social network analytics

 **pointfire**

 **tyGraph**

**CIRRUS
SOFT** 



LET ME INTRODUCE MYSELF...

- Thomas Naunheim
- Cloud Engineer
- Koblenz, Germany
- Blogging on “www.cloud-architekt.net”
- Follow me on Twitter “[@Thomas_Live](https://twitter.com/Thomas_Live)”



Brought to you by



DAY 0: BEFORE SYNCHRONIZING IDENTITIES

Securing Hybrid Identity Environment

Hybrid Azure AD Security = Protect your AD and AAD

- Secured Active Directory environments
- Hybrid identity components on-premises like crown jewels

Tenant Hardening and CA Policies (right from the start)

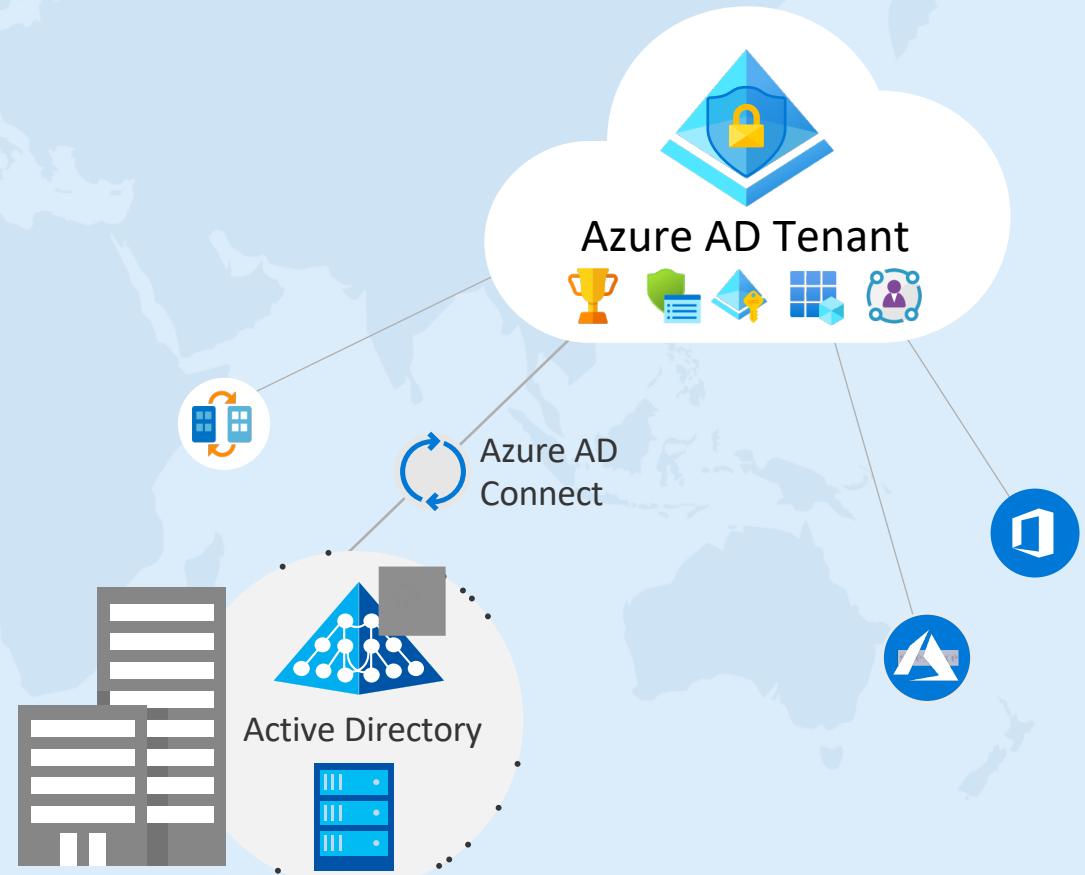
- Best practices and recommendations ([Identity Secure Score](#))
- [Default Security Settings](#) vs. [Common policies](#) → CA Strategy

Hybrid Identity Adoption Strategy

- Authentication options and existing (AD) security policies
- Scoped identity sync and write-back operations

Identity Compliance and Governance Strategy

- Governance and security of user self-services (e.g. SSPR)
- Securing [privilege access for cloud workloads](#)
- Implementation of (active) security monitoring system



SECURING AND MONITORING YOUR AZURE AD IDENTITIES

Protection of identities across platforms and perimeters



Identity Protection and
Strong Authentication



Reduced attack surface
with Conditional Access



Detection and investigation
of identity threats



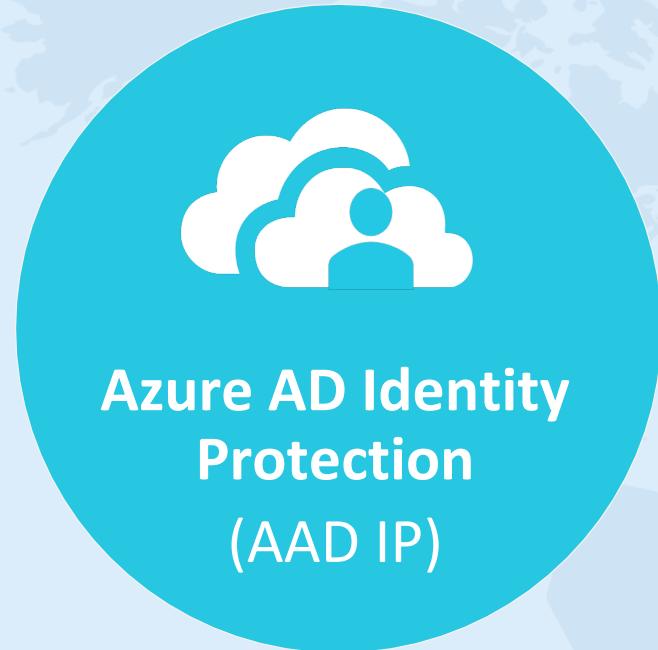
IDENTITY PROTECTION AND STRONG AUTHENTICATION



Brought to you by:
The Global Microsoft Community &
Microsoft 365
COLLABORATION
CONFERENCE
M365Conf.com | #M365CONF

IDENTITY PROTECTION AND STRONG AUTHENTICATION

End-to-end Identity Protection



Azure AD Identity
Protection
(AAD IP)

Cloud Identity



Azure Advanced
Threat Protection
(ATP)

On-Premises Identity



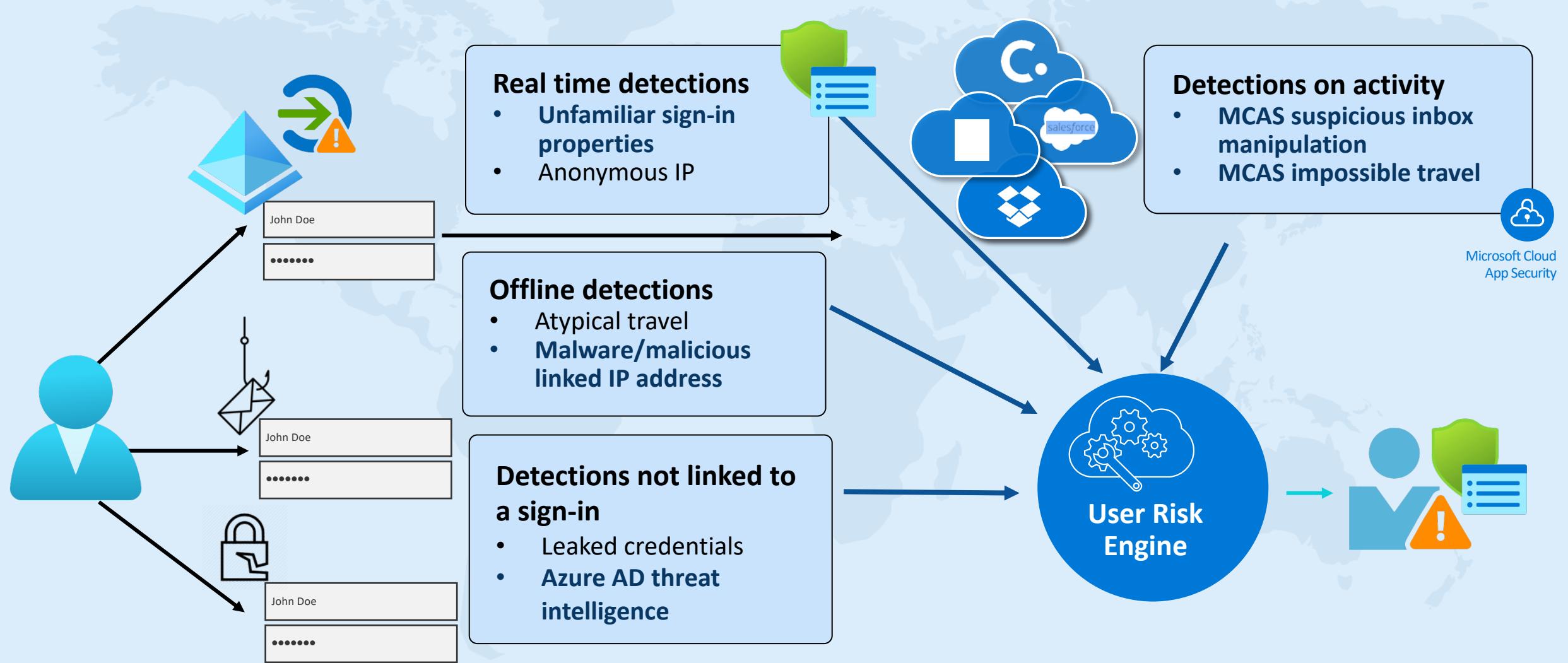
Microsoft Cloud
App Security
(MCAS)

Cloud App (Sessions)

Aggregation + User and Entity Behavior Analytics (UEBA)

IDENTITY PROTECTION AND STRONG AUTHENTICATION

Automate response with Identity Protection and MCAS signals





Identity Protection | Overview

Search (Cmd+/) «

Learn more Refresh Got feedback?

Overview

Protect

User risk policy

Sign-in risk policy

MFA registration policy

Report

Risky users

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Troubleshoot

New support request

Date range = 30 days

New risky users detected

Count

25.04.

10.05.

25.05.

09.06.

18.06.

25.06.

09.07.

18.07.

25.07.

09.08.

18.08.

25.08.

09.09.

18.09.

25.09.

09.10.

18.10.

25.10.

09.11.

18.11.

25.11.

09.12.

18.12.

25.12.

09.01.

18.01.

25.01.

09.02.

18.02.

25.02.

09.03.

18.03.

25.03.

09.04.

18.04.

25.04.

09.05.

18.05.

25.05.

09.06.

18.06.

25.06.

09.07.

18.07.

25.07.

09.08.

18.08.

25.08.

09.09.

18.09.

25.09.

09.10.

18.10.

25.10.

09.11.

18.11.

25.11.

09.12.

18.12.

25.12.

09.01.

18.01.

25.01.

09.02.

18.02.

25.02.

09.03.

18.03.

25.03.

09.04.

18.04.

25.04.

09.05.

18.05.

25.05.

09.06.

18.06.

25.06.

09.07.

18.07.

25.07.

09.08.

18.08.

25.08.

09.09.

18.09.

25.09.

09.10.

18.10.

25.10.

09.11.

18.11.

25.11.

09.12.

18.12.

25.12.

09.01.

18.01.

25.01.

09.02.

18.02.

25.02.

09.03.

18.03.

25.03.

09.04.

18.04.

25.04.

09.05.

18.05.

25.05.

09.06.

18.06.

25.06.

09.07.

18.07.

25.07.

09.08.

18.08.

25.08.

09.09.

18.09.

25.09.

09.10.

18.10.

25.10.

09.11.

18.11.

25.11.

09.12.

18.12.

25.12.

09.01.

18.01.

25.01.

09.02.

18.02.

25.02.

09.03.

18.03.

25.03.

09.04.

18.04.

25.04.

09.05.

18.05.

25.05.

09.06.

18.06.

25.06.

09.07.

18.07.

25.07.

09.08.

18.08.

25.08.

09.09.

18.09.

25.09.

09.10.

18.10.

25.10.

09.11.

18.11.

25.11.

09.12.

18.12.

25.12.

09.01.

18.01.

25.01.

09.02.

18.02.

25.02.

09.03.

18.03.

25.03.

09.04.

18.04.

25.04.

09.05.

18.05.

25.05.

09.06.

18.06.

25.06.

09.07.

18.07.

25.07.

09.08.

18.08.

25.08.

09.09.

18.09.

25.09.

09.10.

18.10.

25.10.

09.11.

18.11.

25.11.

09.12.

18.12.

25.12.

09.01.

18.01.

25.01.

09.02.

18.02.

25.02.

09.03.

18.03.

25.03.

09.04.

18.04.

25.04.

09.05.

18.05.

25.05.

09.06.

18.06.

25.06.

09.07.

18.07.

25.07.

09.08.

18.08.

25.08.

09.09.

18.09.

25.09.

09.10.

18.10.

25.10.

09.11.

18.11.

25.11.

09.12.

18.12.

25.12.

09.01.

18.01.

25.01.

09.02.

18.02.

25.02.

09.03.

18.03.

25.03.

09.04.

18.04.

2

IDENTITY PROTECTION AND STRONG AUTHENTICATION

Options of „Passwordless“ authentication





REDUCED ATTACK SURFACE WITH CONDITIONAL ACCESS



Brought to you by:
The Global Microsoft Community &
Microsoft 365
COLLABORATION
CONFERENCE
M365Conf.com | #M365CONF

REDUCED ATTACK SURFACE WITH CONDITIONAL ACCESS

Design and Implementation of policies

- Build strong baselines for users (hybrid, admins and guests) and apps
- Consider your environment (types of devices and level of protection needs)
- Define a standard **naming** convention for policies
 - CA01 - Dynamics CRP: Require MFA for marketing When on external networks
- Draft policies (when this happens → do this)
 - When this happens
 - Then do this
- „Conditional Access as Code“ (Automation and policy sets [by Alexander Filipin](#))

Search (Cmd+/)[Gallery](#) [Edit](#) [New](#) [Bell](#) [Help](#)

Breakdown per condition and sign-in status

Download results to Excel or open query in Log Analytics by clicking the icons in the upper right corner of each query.

Device State - Total

Unmanaged

Azure AD joined

Sign-in risk - Total

none

3

3

Device platform - Total

Windows 8

MacOs

Windows

1

1

3

1

Client app - Total

Mobile Apps and Desktop...

Browser

1

2

Duesseldorf

Dublin

Koblenz-Rauental

Amsterdam

Count

2

1

1

1

Brought to you by



Sign-in Details

To investigate sign-in details of a specific user, filter by username at the top of the workbook

User sign-in count - Total

Sign-in events - Total



Troubleshooting + Support

New support request

REDUCED ATTACK SURFACE

Smart Lockout and Password Protection

- Assists in locking out attackers to use **brute-force methods**:

Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

- Avoid creating **weak passwords** with global and custom banned password list

Enforce custom list ⓘ

Yes No

Custom banned password list ⓘ

Alaab
Kölsch
Effzeh



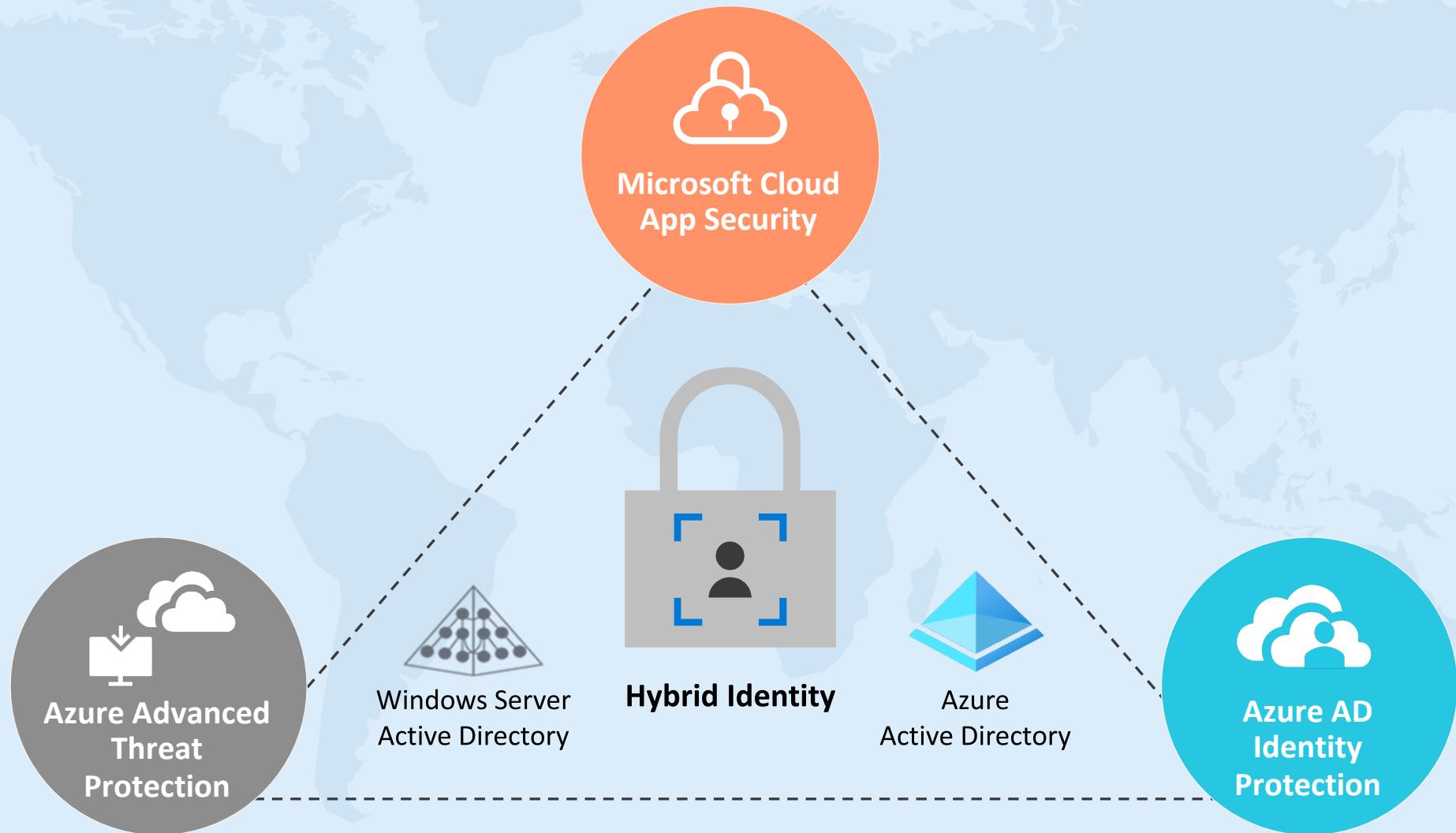
DETECTION AND INVESTIGATION OF IDENTITY THREATS



Brought to you by:
The Global Microsoft Community &
Microsoft 365
COLLABORATION
CONFERENCE
M365Conf.com | #M365CONF

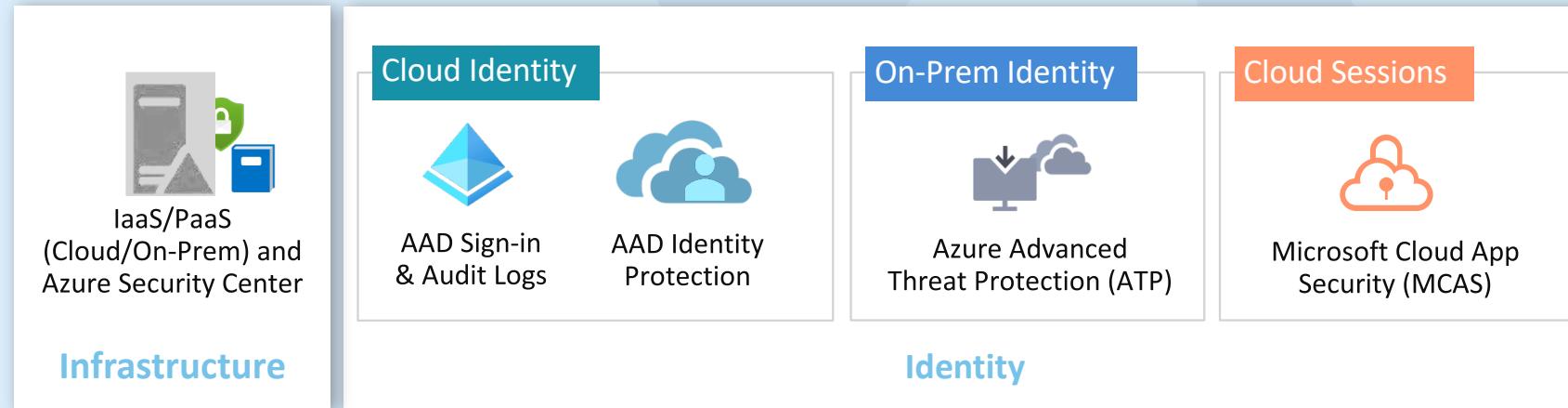
DETECTION AND INVESTIGATION OF IDENTITY THREATS

Identity Security Operations in (Microsoft) Hybrid Environment



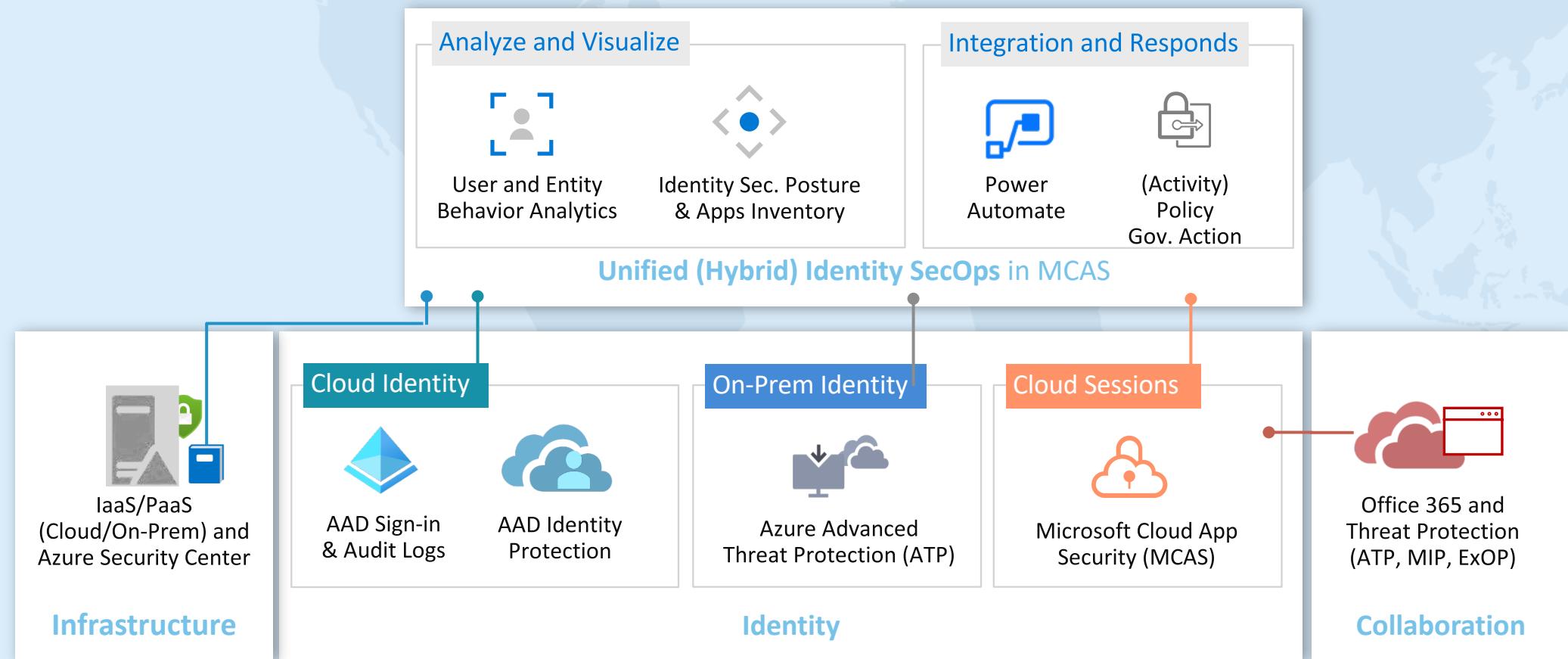
DETECTION AND INVESTIGATION OF IDENTITY THREATS

Azure Monitor: Logs of Azure AD and Azure services (IaaS/PaaS)



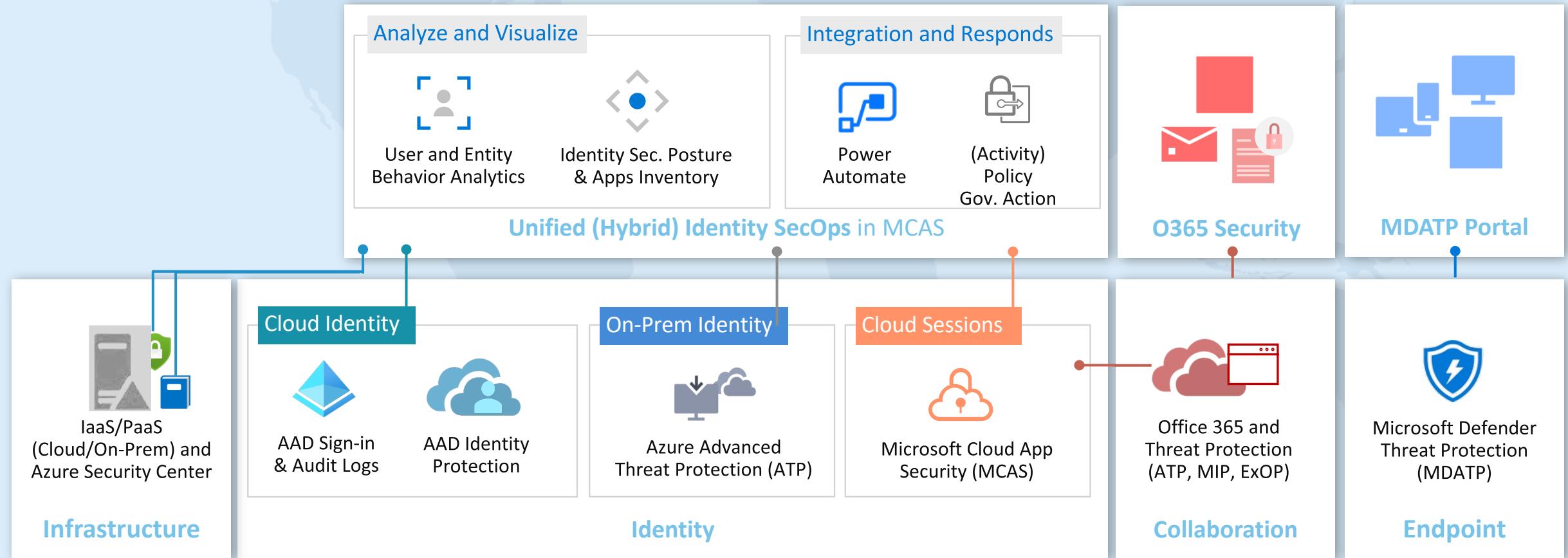
DETECTION AND INVESTIGATION OF IDENTITY THREATS

Microsoft Cloud App Security: Unified Identity SecOps



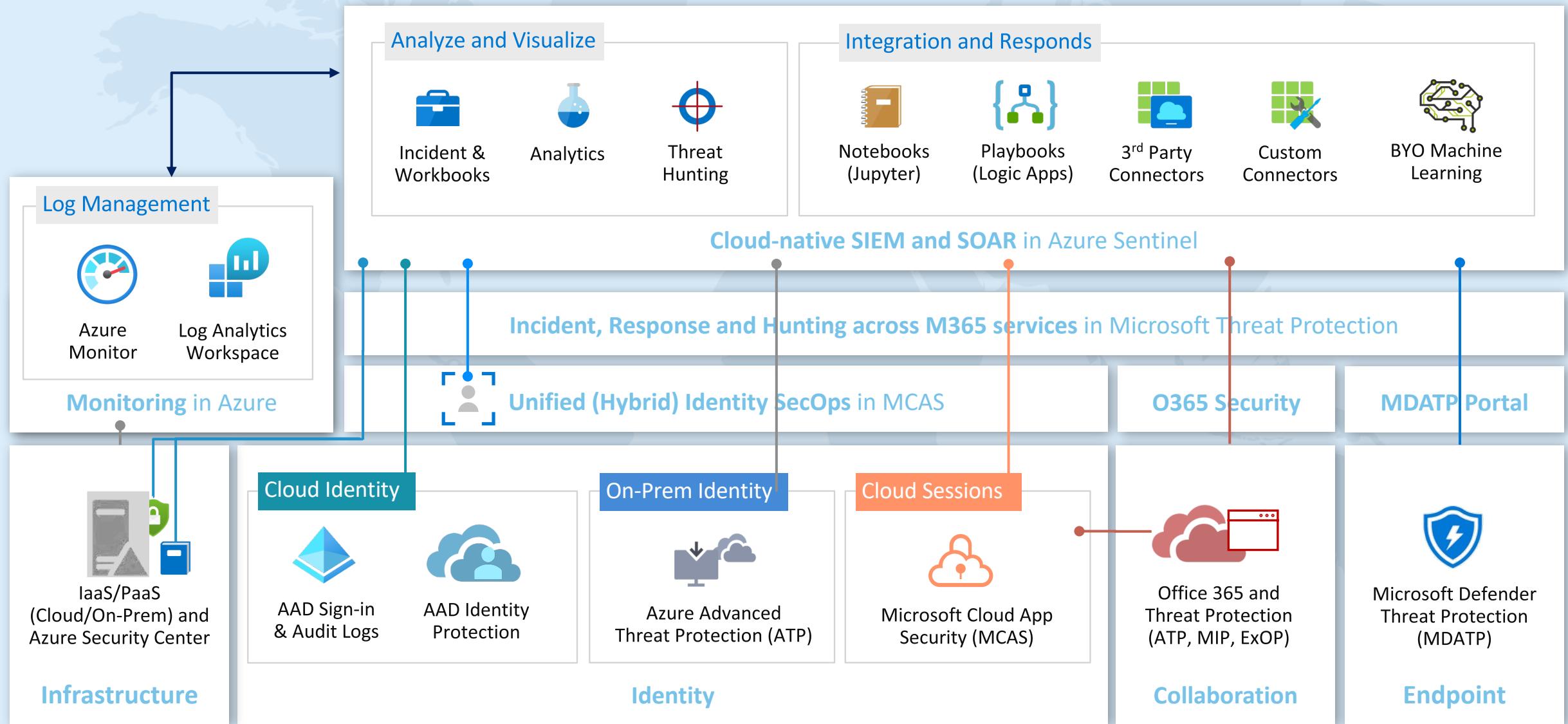
DETECTION AND INVESTIGATION OF IDENTITY THREATS

Unified Identity SecOps with MCAS, Microsoft and Office 365 ATP



DETECTION AND INVESTIGATION OF IDENTITY THREATS

Azure Sentinel: „Single pane of glass“



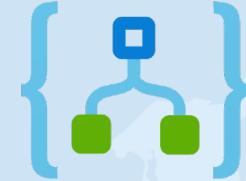
DETECTION AND INVESTIGATION OF IDENTITY THREATS

Hunting, Incidents and Automation in Azure Sentinel



Hunting

- Azure Active Directory signins from new locations
- ...



Analytics/Detections

- Cisco Firewall block but success logon to AAD
- ...

Response/Playbooks

- Block-AADUser
- Confirm-AADRiskyUser
- Isolate-MDATPMachine
- Revoke-AADSginSessions
- Reset-AADUserPassword

Investigation

Preview

Undo Redo

Suspected overpass-the-hash attack...

Incident

High Severity

New Status

Unassigned Owner

 4/19/2020, 10:43:52 AM
Last incident update time

Timeline

Antimalware Action Failed

4/19/2020, 10:32:45 AM

Microsoft Antimalware has encountered an error when taki...

Antimalware Action Failed

4/19/2020, 10:32:45 AM

Microsoft Antimalware has encountered an error when taki...

Suspected overpass-the-hash attack (Kerberos)

4/19/2020, 10:42:41 AM

ThomasSupport on cl2-vm successfully authenticated agai...

 HANdS-ON:
Azure Sentinel and
Identity Threats

Brought to you by

**Microsoft 365**
COLLABORATION
CONFERENCE

M365Conf.com | #M365CONF



ARE YOU READY FOR A RAFFLE? WE ARE GIVING AWAY 3 OCULUS QUEST ALL IN ONE!

- Visit the Vendors Booth, Sessions and Watch the Videos
- Submit Your Answers to Enter the Raffle
- You need at least 5 correct answers then submit for a chance to win one of 3

(One in each Americas, APAC, EMEA)



<https://bit.ly/m365raffle>



10% OF FUNDS FROM SPONSORS GO TO SUPPORT COMMUNITY RELIEF.

FOR MORE INFORMATION WRITE TO INFO@M365VIRTUALMARATHON.COM



CONSIDER DONATING TO THE FOLLOWING CHARITY RELIEF FUNDS:

UNITED WAY: [HTTPS://GIVE.UWKC.ORG/M365VM](https://give.uwkc.org/m365vm)

INTERNATIONAL MEDICAL CORPS: [HTTPS://BIT.LY/MEDICALCORPSFUND](https://bit.ly/MedicalCorpsFund)



MICROSOFT 365
Virtual **MARATHON**

Mark Your Calendars:

May 27 & 28, 2020
36 hours / 2 days



**SharePoint
CONFERENCE
& Microsoft 365**

March 23-25, 2021, MGM Grand Resort
Las Vegas, Nevada, USA

M365Conf.com
#M365CONF

The SharePoint Conference is now The Microsoft 365 Collaboration Conference



Brought to you by:
The Global Microsoft Community &
**Microsoft 365
COLLABORATION
CONFERENCE**
M365Conf.com | #M365CONF

THANK YOU FOR JOINING US!

DO YOU HAVE ANY QUESTIONS?



@Thomas_Live



www.cloud-architekt.net



Thomas@Naunheim.net



Brought to you by

**Microsoft 365**
COLLABORATION
CONFERENCE
M365Conf.com | #M365CONF