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

#M365VM
M365VirtualMarathon.com

Brought to you by:
The Global Microsoft Community
Microsoft 365 COLLABORATION CONFERENCE

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”

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)

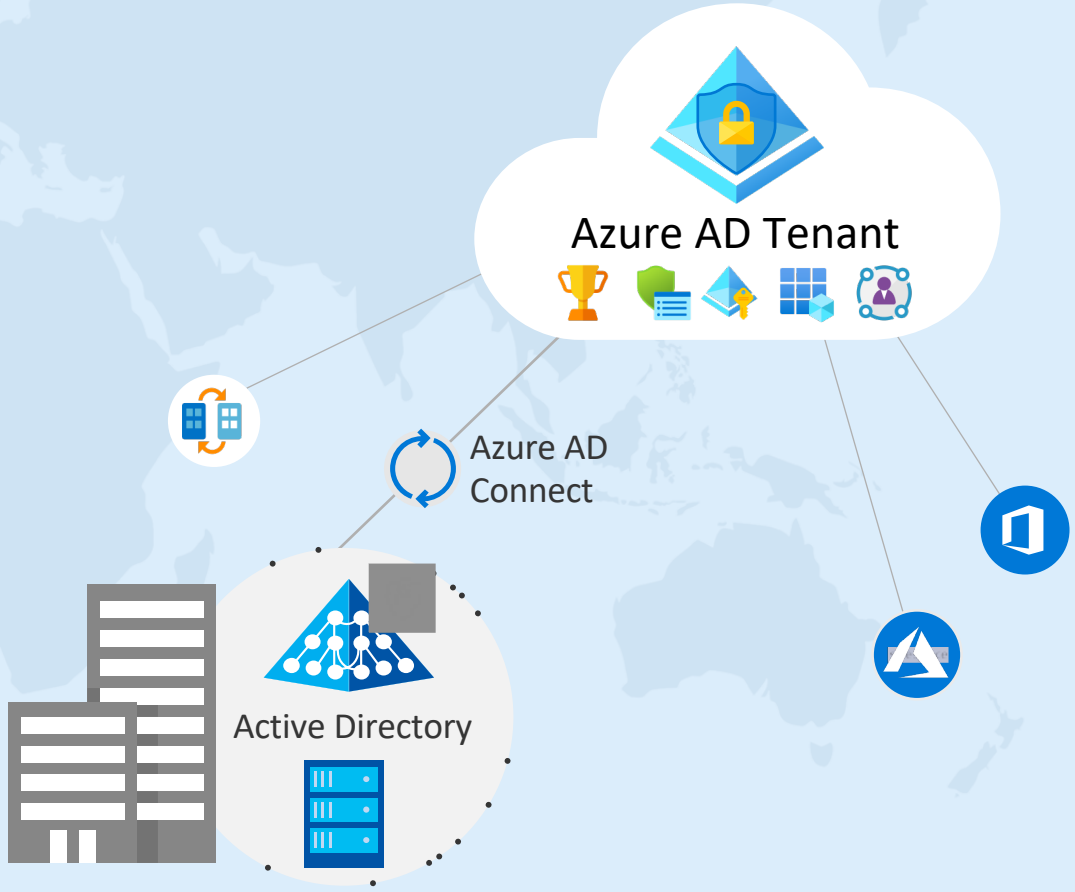
- Best practices and recommendations (Identity Secure Score)
- Default Security Settings vs. Common policies → CA Strategy

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

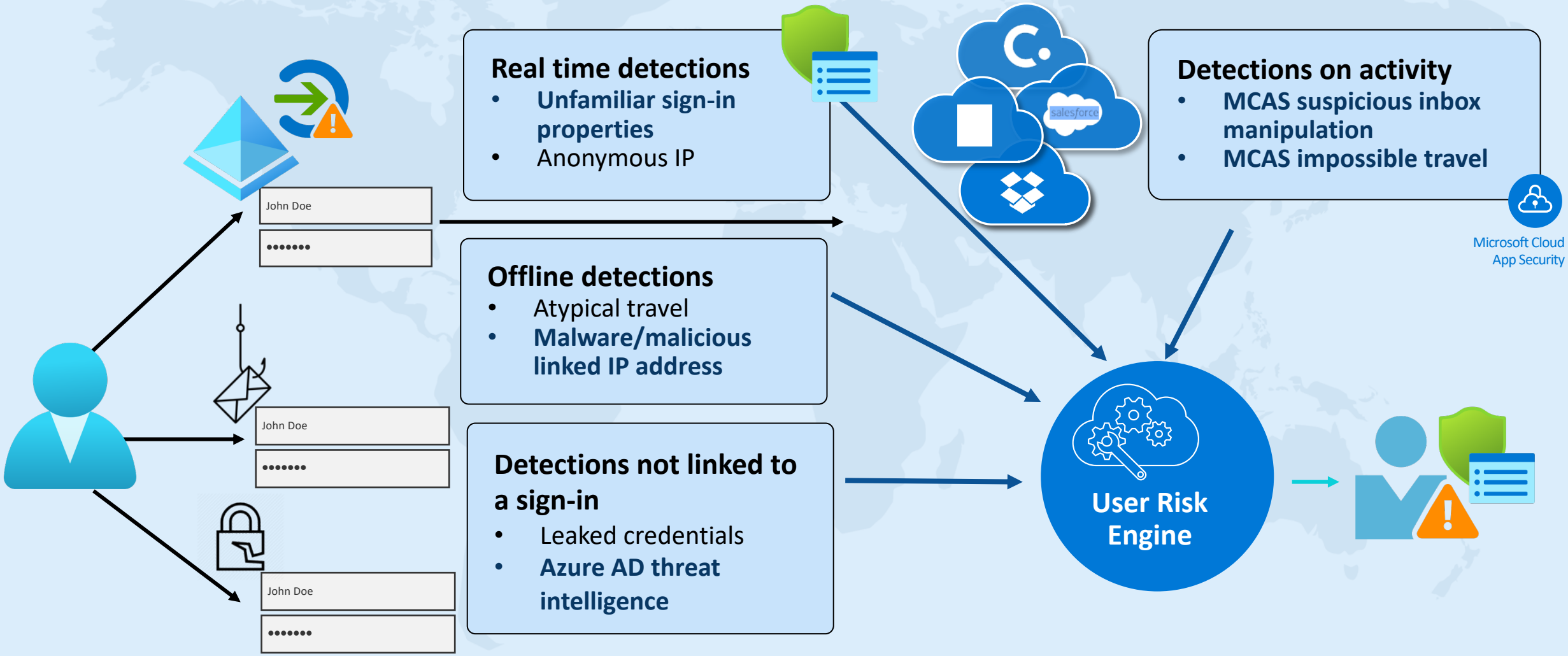
IDENTITY PROTECTION AND STRONG AUTHENTICATION

End-to-end Identity Protection

Aggregation + **U**ser and **E**ntity **B**ehavior **A**nalytics (UEBA)

IDENTITY PROTECTION AND STRONG AUTHENTICATION

Automate response with Identity Protection and MCAS signals



Source: Microsoft Ignite Session ("The science behind Azure Active Directory Identity Protection")

HANDS-ON:
Detect and response to identity risks

Brought to you by

Microsoft 365 COLLABORATION CONFERENCE

M365Conf.com | #M365CONF

IDENTITY PROTECTION AND STRONG AUTHENTICATION

Options of „Passwordless“ authentication

Image Source: Identity and access management best practices from around the world

REDUCED ATTACK SURFACE WITH CONDITIONAL ACCESS

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

REDUCED ATTTACK 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)

- **„Conditional Access as Code“** (Automation and policy sets by Alexander Filipin)

Source: Microsoft Docs („How To: Plan your Conditional Access deployment in Azure Active Directory“)

HANDS-ON:
Conditional Access Policies, Reports & Insights

Brought to you by

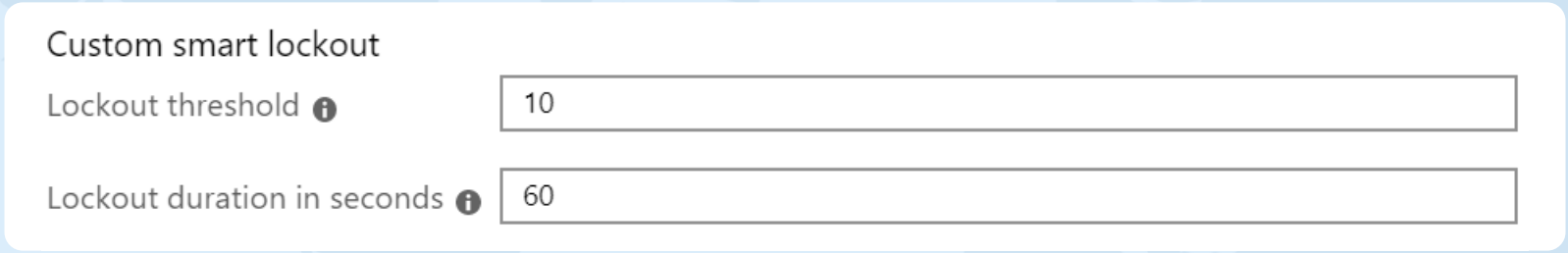
Microsoft 365 COLLABORATION CONFERENCE

M365Conf.com | #M365CONF

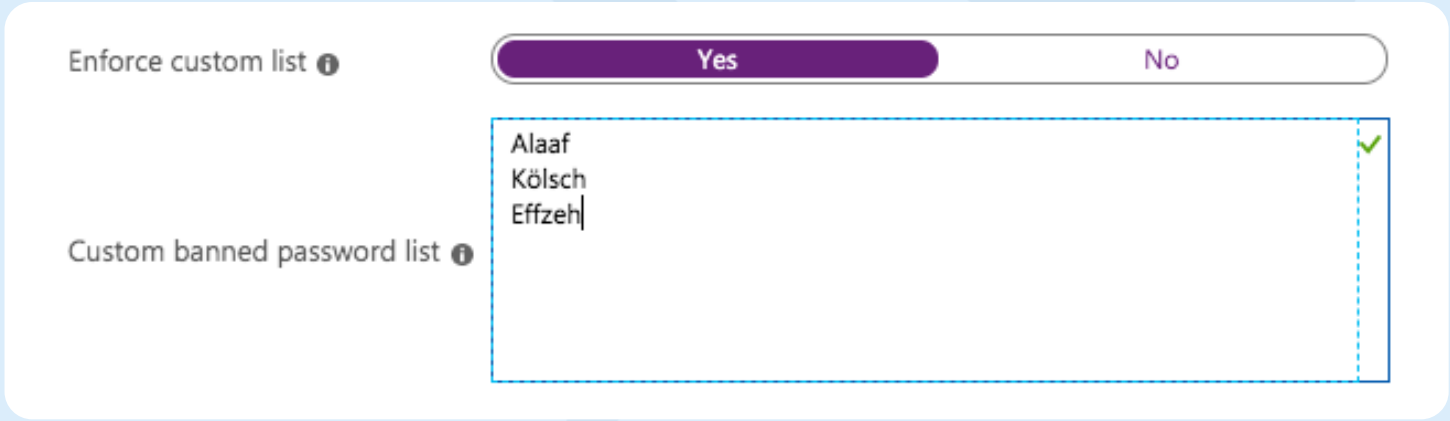
REDUCED ATTTACK SURFACE

Smart Lockout and Password Protection

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



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



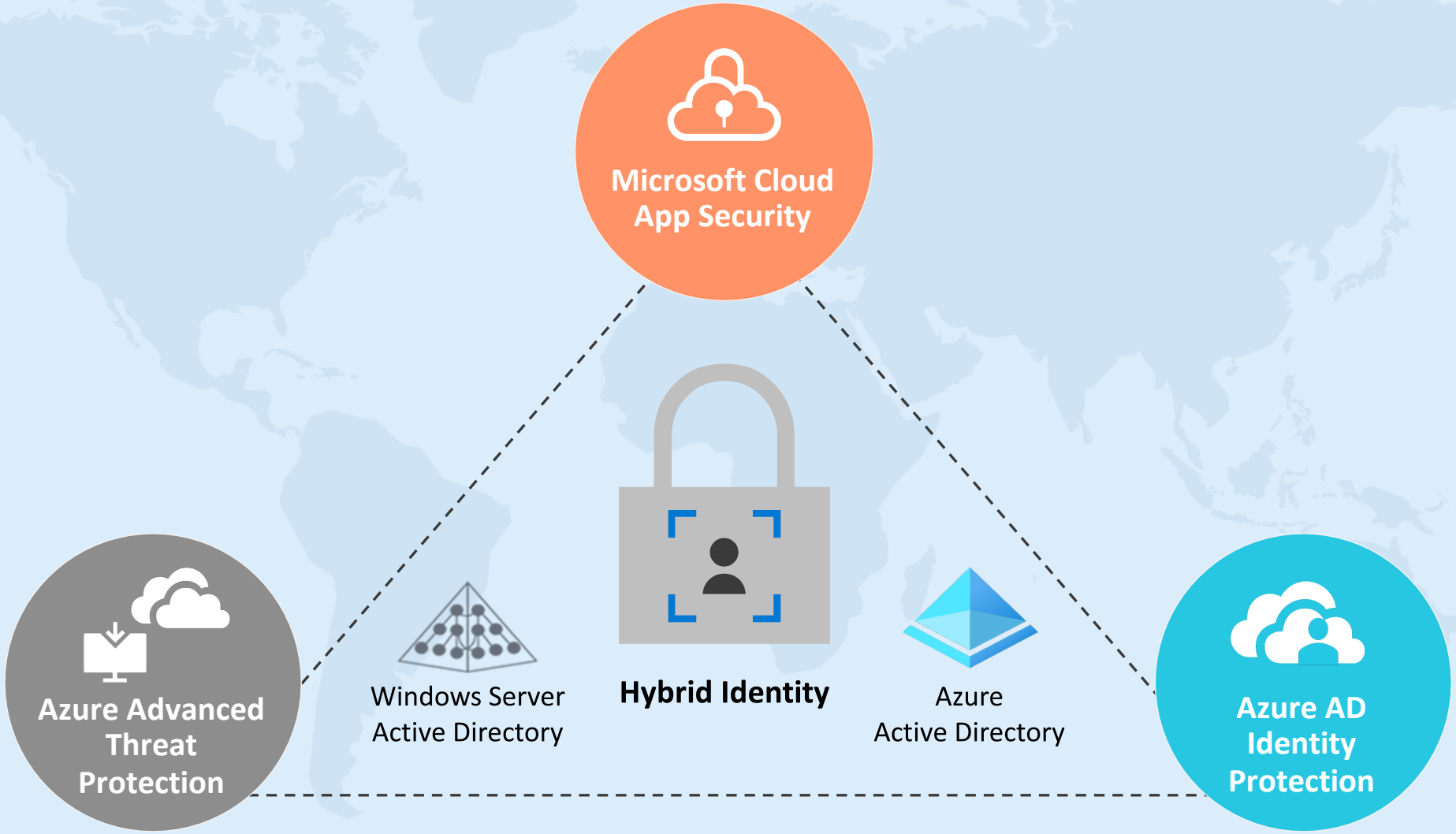
Source: Microsoft Docs ("Enforce Azure AD password protection for Windows Server Active Directory")

DETECTION AND INVESTIGATION OF IDENTITY THREATS

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

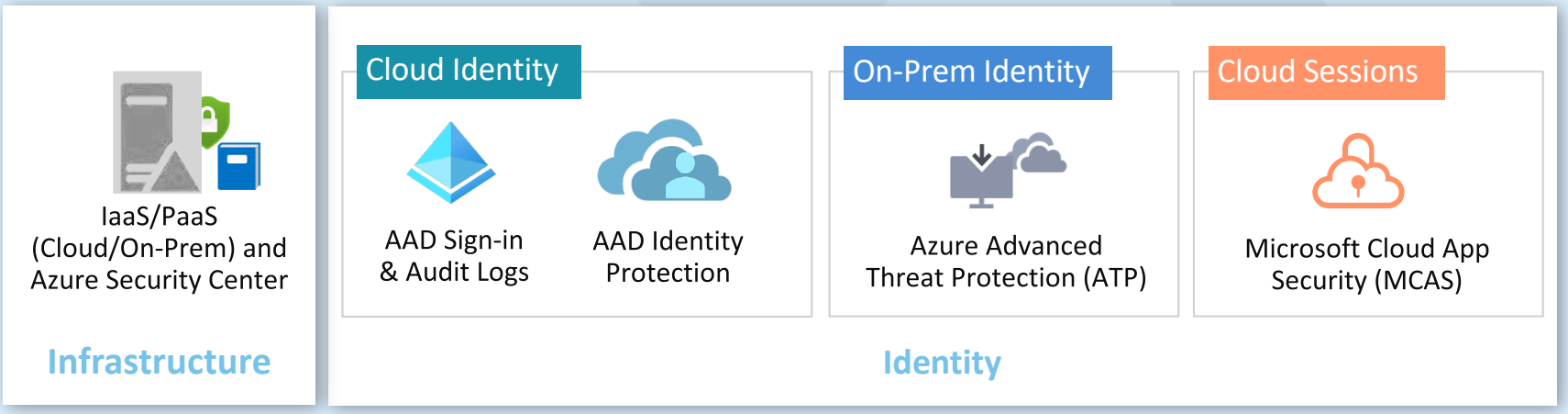
DETECTION AND INVESTIGATION OF IDENTITY THREATS

Identity Security Operations in (Microsoft) Hybrid Environment



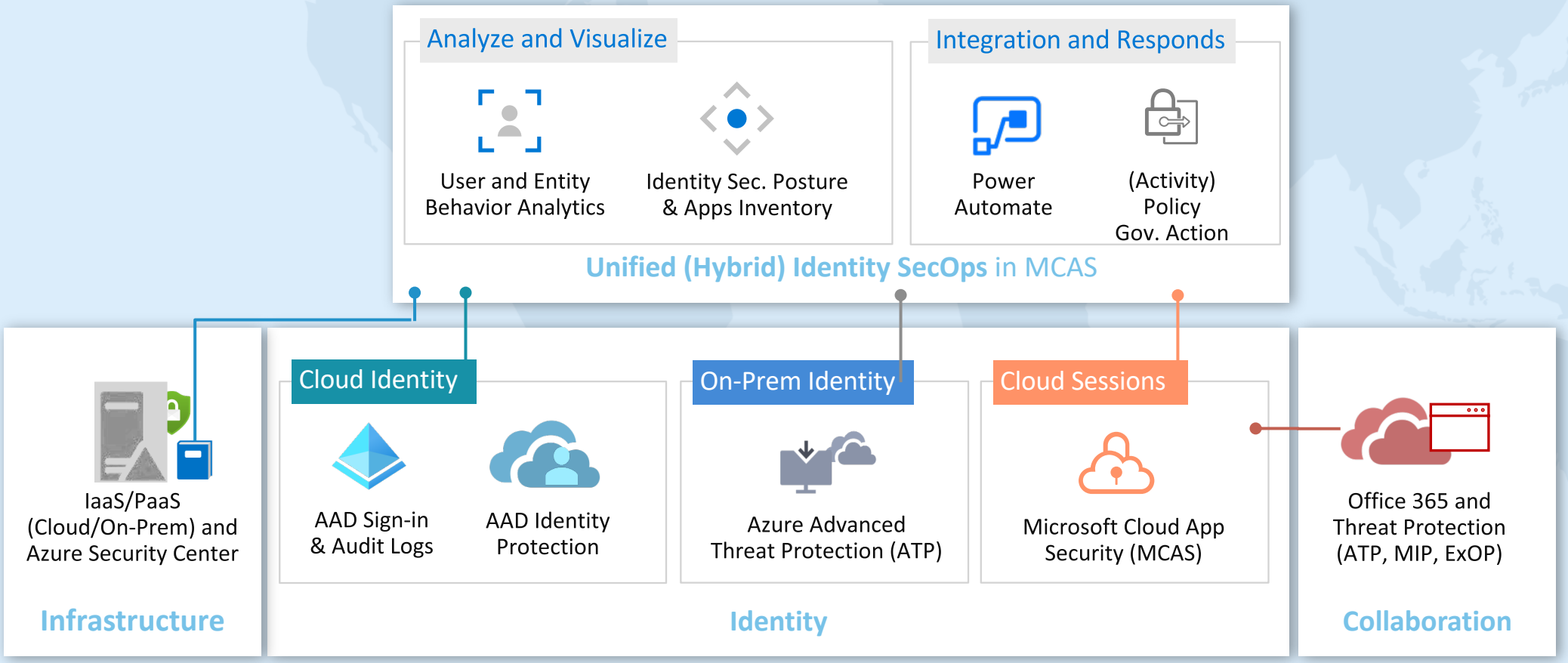
DETECTION AND INVESTIGATION OF IDENTITY THREATS

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



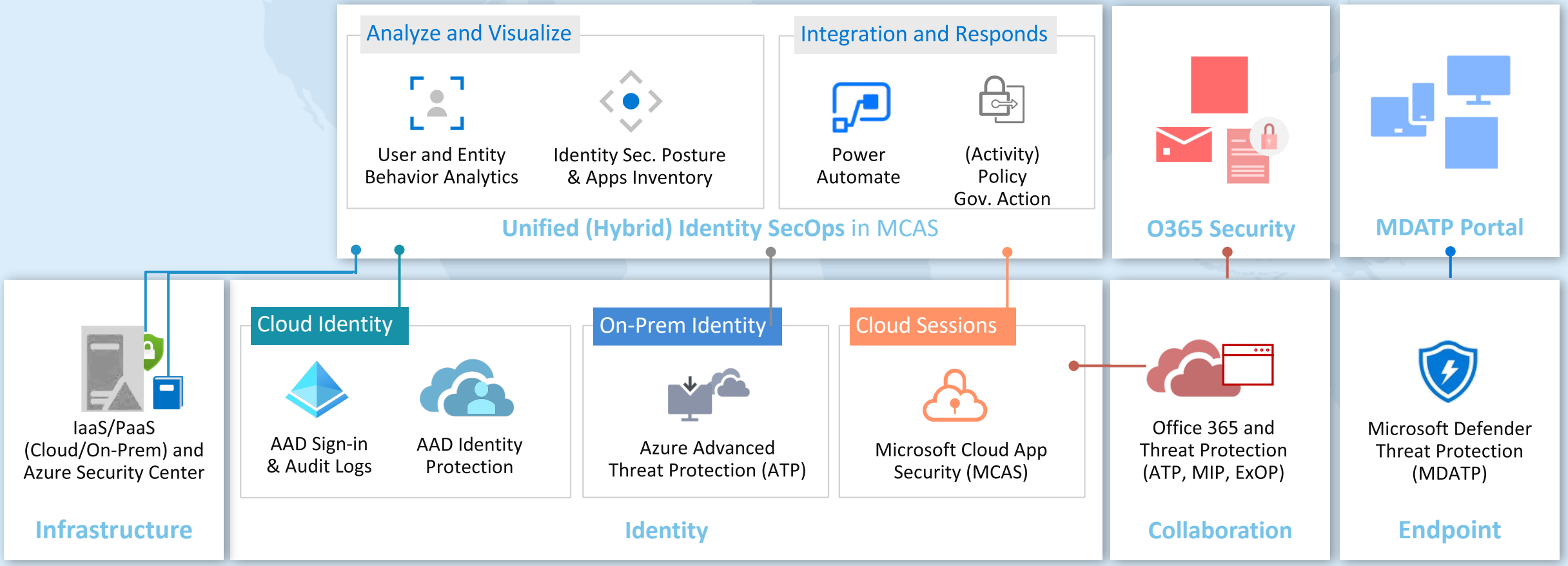
DETECTION AND INVESTIGATION OF IDENTITY THREATS

Microsoft Cloud App Security: Unified Identity SecOps



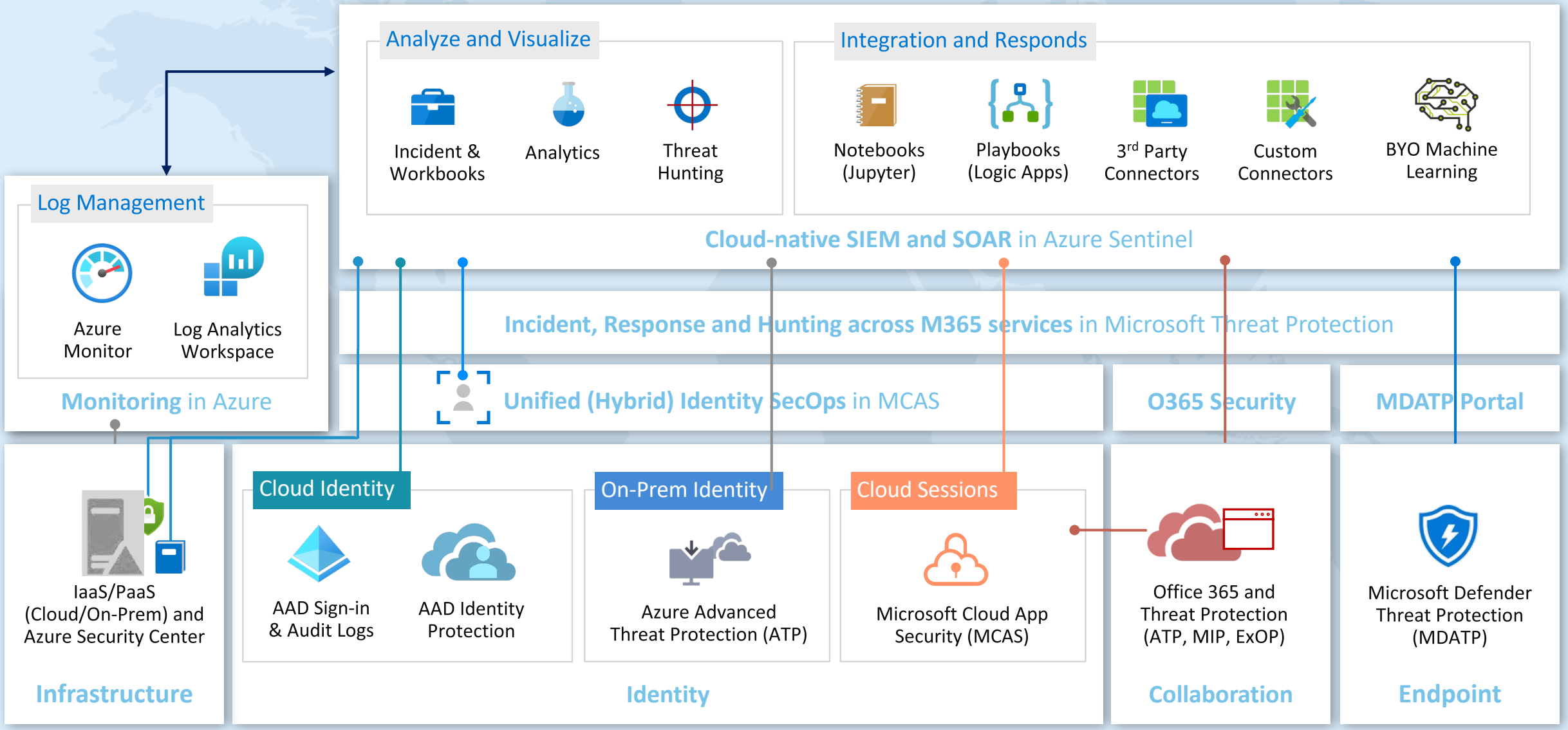
DETECTION AND INVESTIGATION OF IDENTITY THREATS

Unified Identity SecOps with MCAS, Microsoft and Office 365 ATP



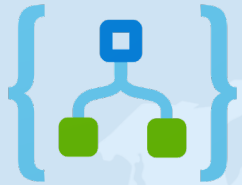
DETECTION AND INVESTIGATION OF IDENTITY THREATS

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-AADSignInSessions**
- Reset-AADUserPassword

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

INTERNATIONAL MEDICAL CORPS: 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

#M365VM
M365VirtualMarathon.com

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