CLOUD CAMP QUARTERLY

SECURING AND MONITORING YOUR AZURE AD IDENTITIES

BY THOMAS NAUNHEIM

APRIL 15TH 2021
BROUGHT TO YOU ONLINE

SPONSORED BY

THOMAS NAUNHEIM

Cloud Solutions Architect
Koblenz, Germany

@Thomas_Live

www.cloud-architekt.net

Azure Meetup BONN

MVP Microsoft® Most Valuable Professional

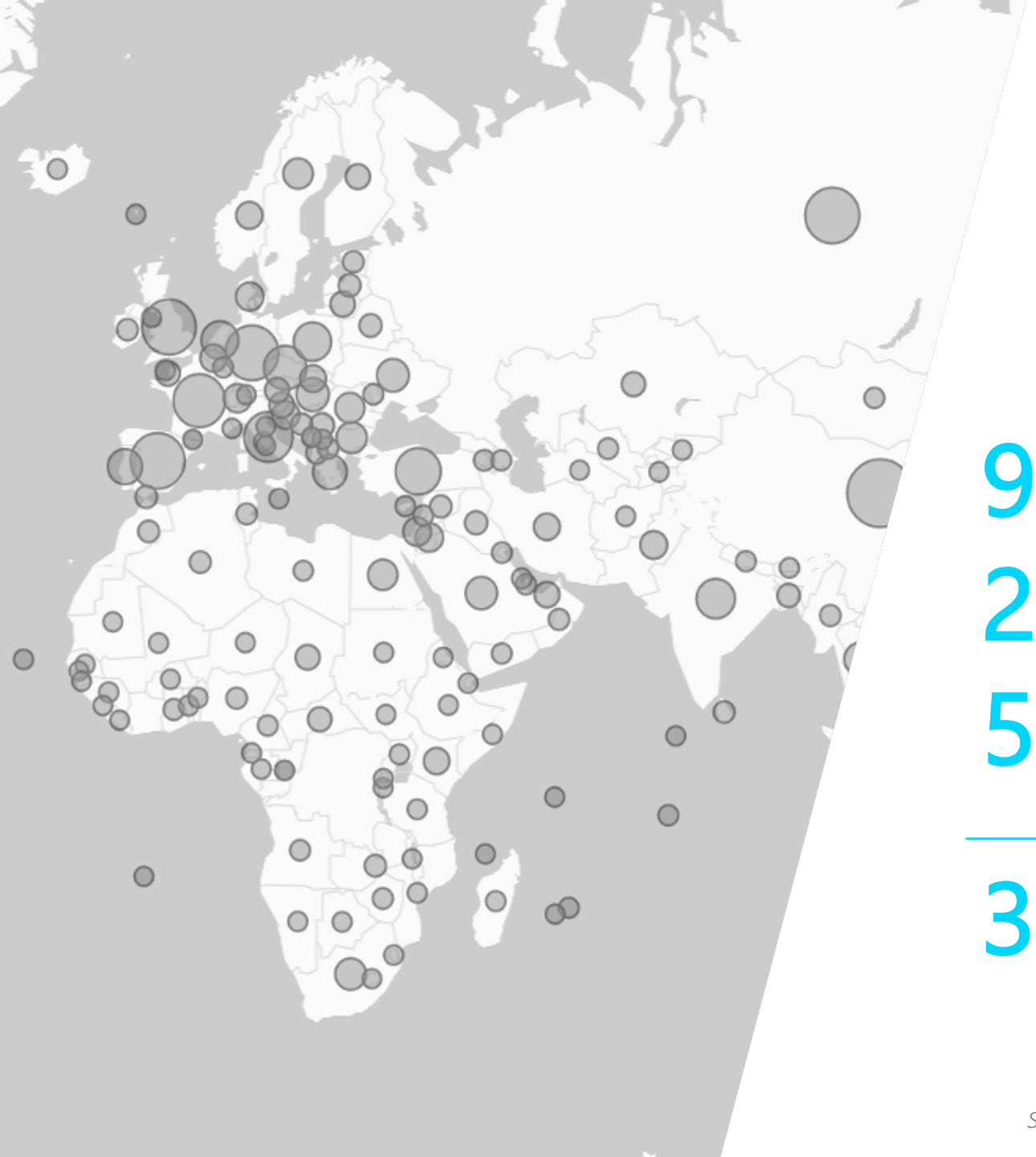
Microsoft Certified Azure Solutions Architect Expert

Most Valuable Mentor

IDENTITY IN TIMES OF COVID-19

SHIFT TO CLOUD AUTHENTICATION

Source: "Azure Active Directory: our vision and roadmap to help you secure remote access and boost employee productivity"



IDENTITY ATTACKS IN TIMES OF **COVID-19**

Attacks in August 2020:

9M high-risk enterprise sign-in attempts flagged

2M compromised accounts detected

5.8B attacker-driven sign-ins detected

300% increase in attacks over the past year

Source: "The science behind Azure Active Directory Identity Protection"

AGENDA

Strong Authentication

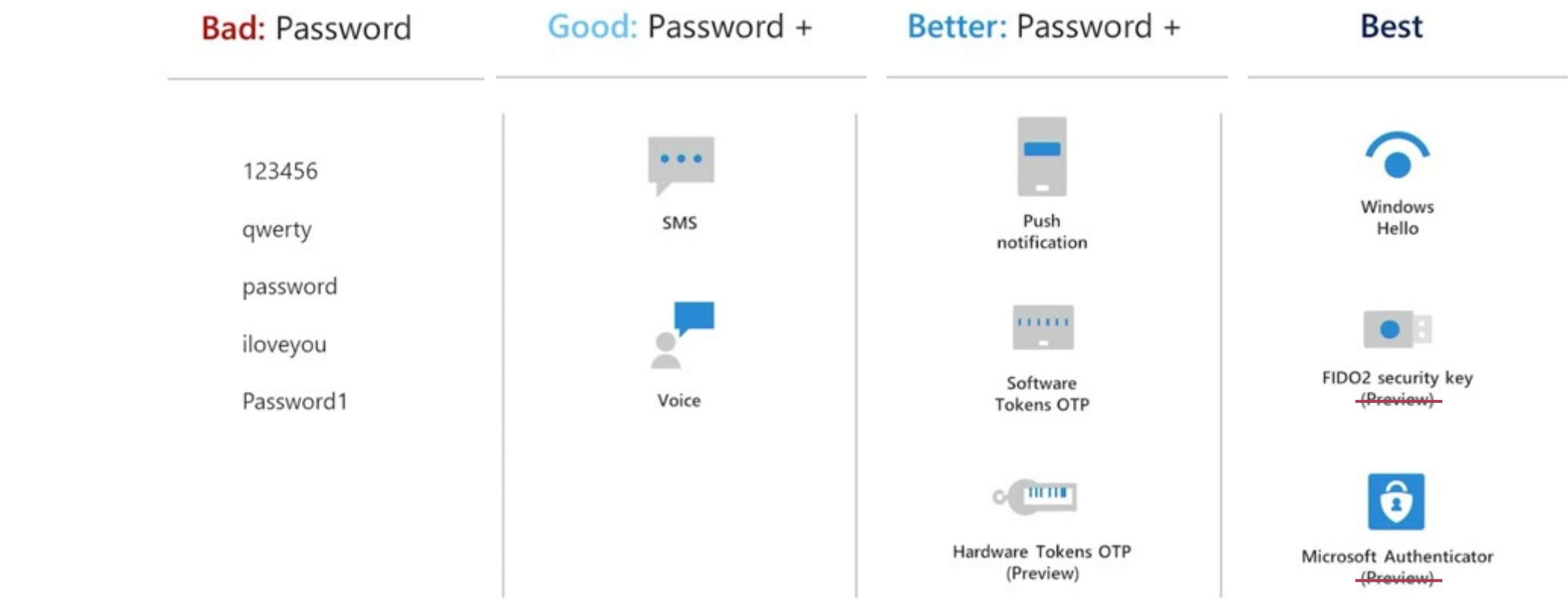
Reduced attack surface

Unified view of identity threats

STRONG AUTHENTICATION

PROTECTED IDENTITY

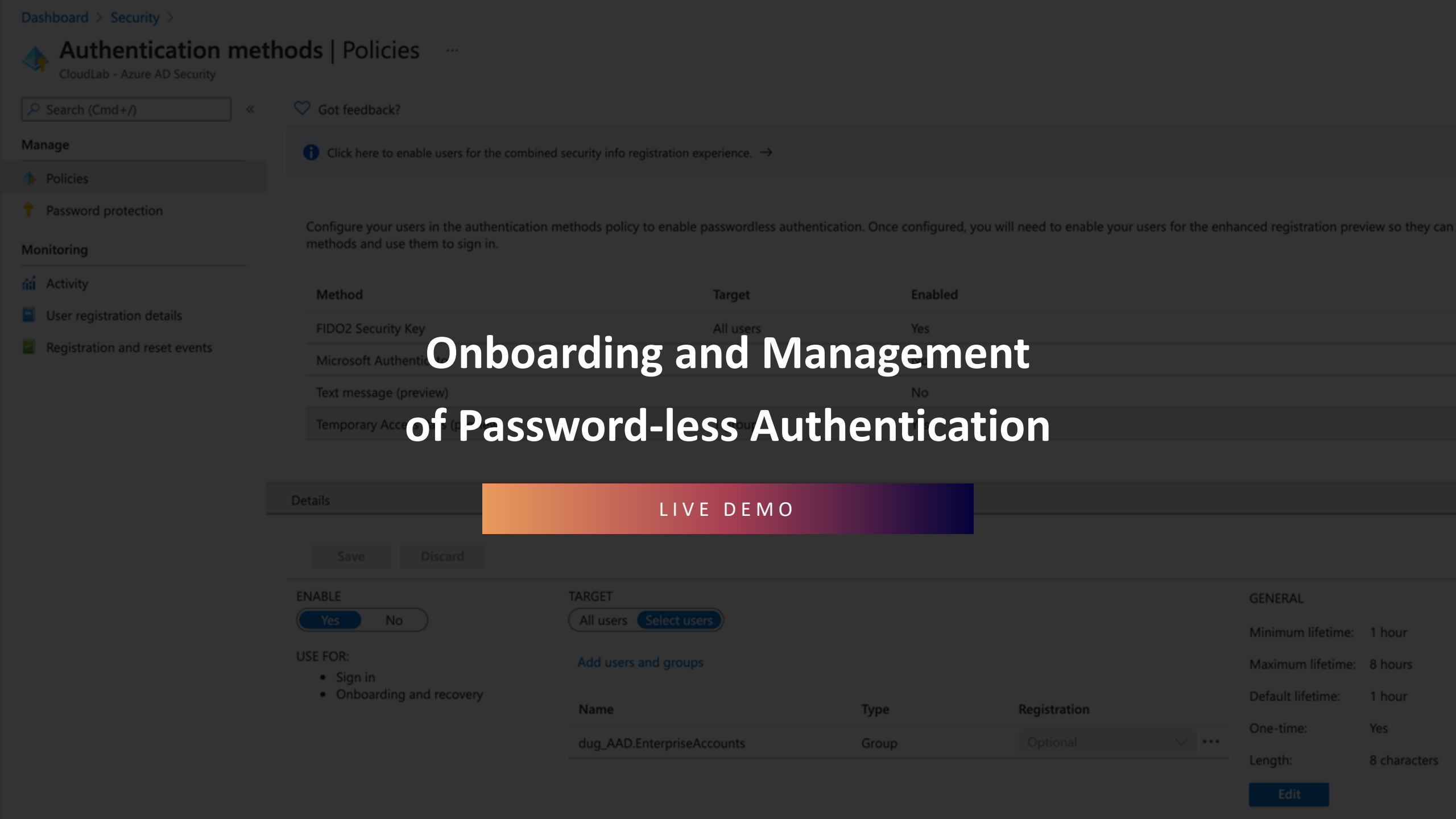
OVERVIEW OF AUTHENTICATION METHODS



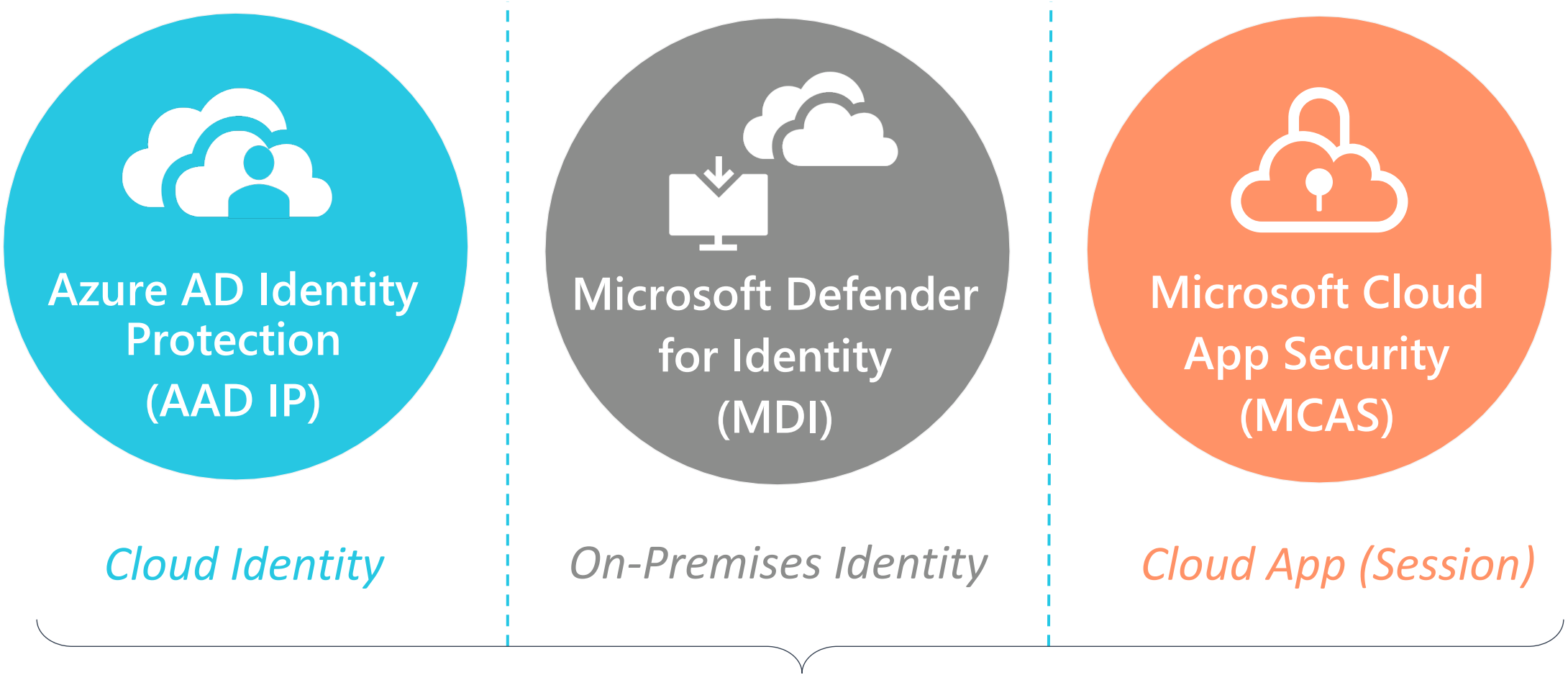
Increase Password Strength (AAD Password Protection) → Modernize password policy (e.g. expiration) → Enable Self-Service Password Reset (SSPR) → Reduce usage of passwords

Enroll User Registration of MFA methods → Require Azure MFA in case of risky sign-ins or access to sensitive app/data → Always MFA by Password-less incl. Device-based Identity

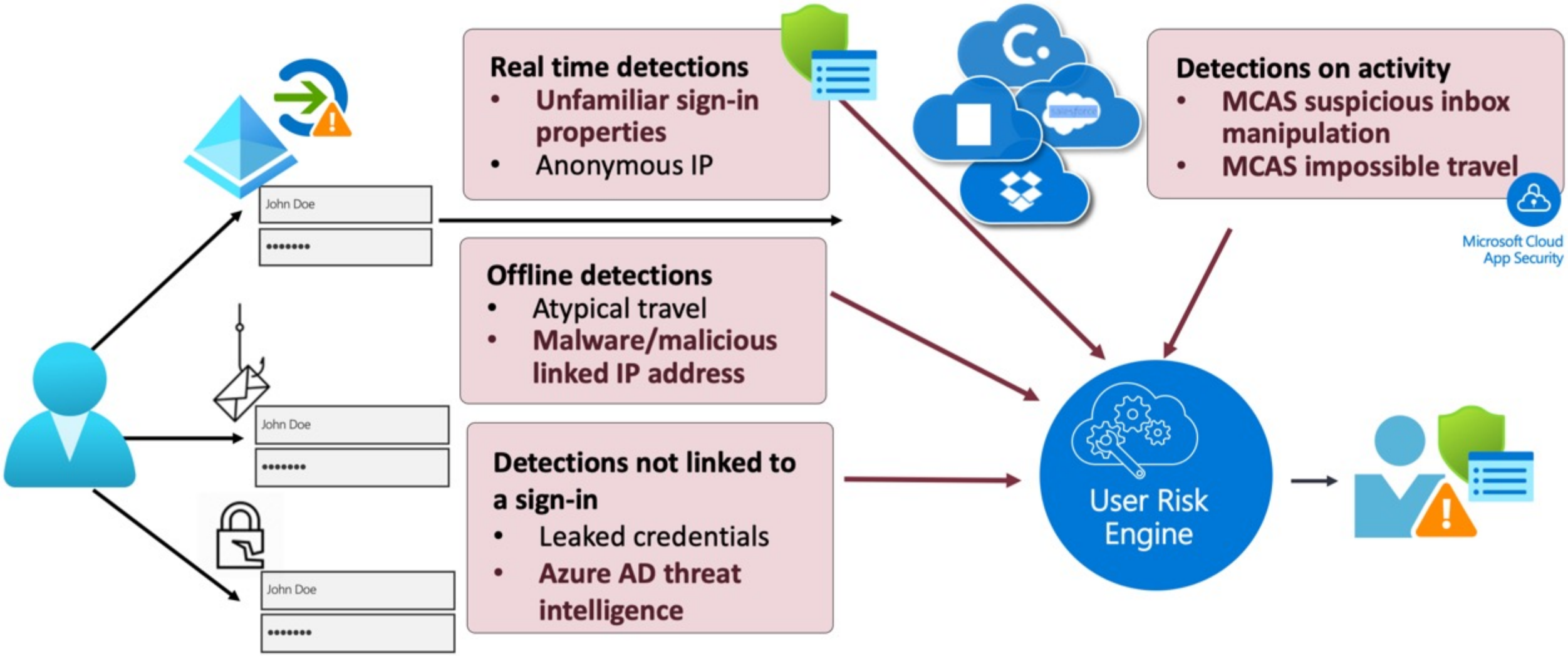
Image Source "Overview of Authentication Methods": Winning Azure Active Directory strategies for identity security and governance


Dashboard > Security >
Authentication methods | Policies
CloudLab - Azure AD Security
Search (Cmd+/)
Got feedback?
Manage
Policies
Password protection
Monitoring
Activity
User registration details
Registration and reset events
Click here to enable users for the combined security info registration experience.
Configure your users in the authentication methods policy to enable passwordless authentication. Once configured, you will need to enable your users for the enhanced registration preview so they can
methods and use them to sign in.
Method
Target
Enabled
FIDO2 Security Key
All users
Yes
Text message (preview)
No
Onboarding and Management
of Password-less Authentication
LIVE DEMO
Details
Save
Discard
ENABLE
Yes
No
TARGET
All users
Select users
USE FOR:
Sign in
Onboarding and recovery
Add users and groups
Name
Type
Registration
dug_AAD.EnterpriseAccounts
Group
Optional
GENERAL
Minimum lifetime:
1 hour
Maximum lifetime:
8 hours
Default lifetime:
1 hour
One-time:
Yes
Length:
8 characters
Edit

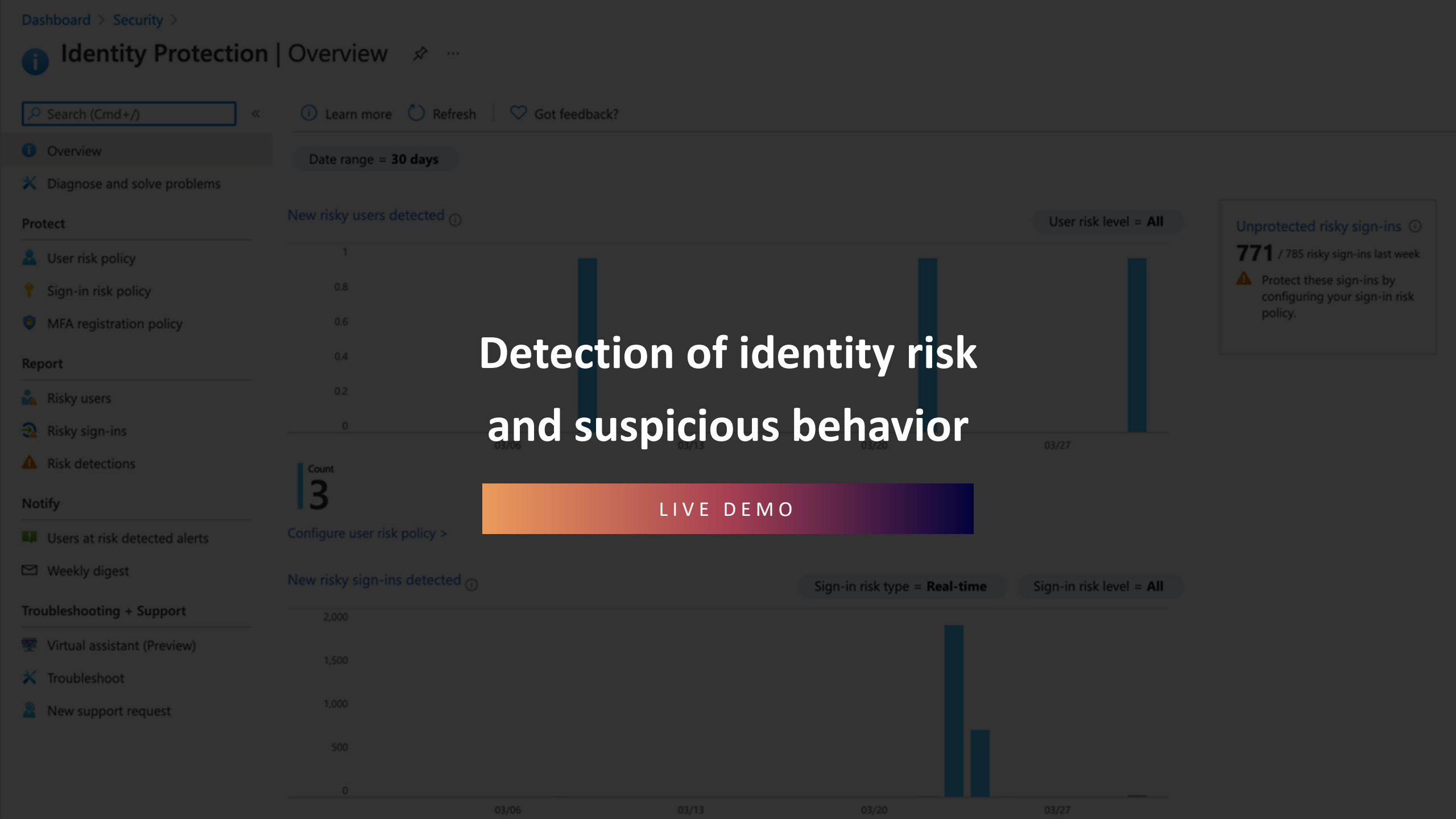
END-TO-END IDENTITY PROTECTION



IDENTITY PROTECTION



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



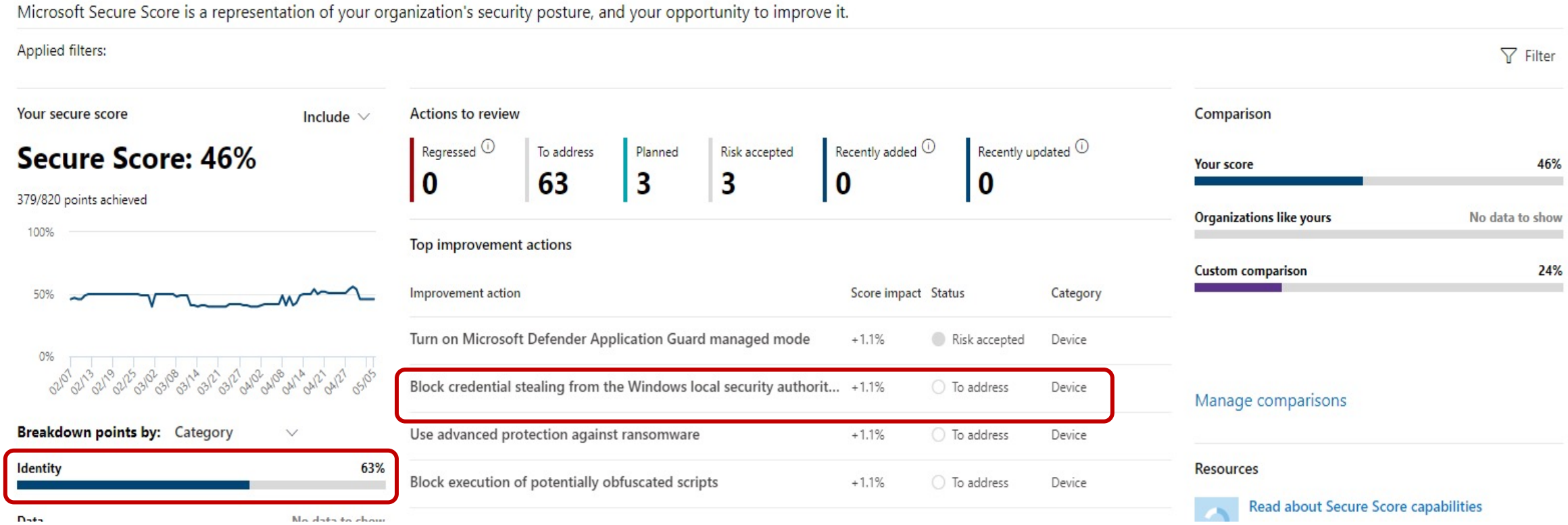
Detection of identity risk and suspicious behavior

LIVE DEMO

REDUCED ATTACK SURFACE

SECURITY POSTURE & CA POLICIES

MICROSOFT SECURE SCORE



Source: Microsoft (Overview "Microsoft Secure Score")

REDUCED ATTACK SURFACE

IDENTITY SECURE SCORE

Secure Score for Identity

43.99%

Last updated 3/28/2021, 1:00:00 AM
View your Microsoft Secure Score.

Comparison

CloudLab	43.99%
Industry average	0%
Typical 0-5 person company	12.99%

Change industry

Score history

7 days | 30 days | 60 days | 90

Improvement actions

Download | Columns

Name	Score Impact	User Impact
Disable Print spooler service on domain controllers	4.20%	Low
Install Defender for Identity Sensor on all Domain Controllers	3.36%	Low
Configure Microsoft Defender for Endpoint Integration	0.84%	Low
Configure VPN integration	0.84%	Low
Reduce lateral movement path risk to sensitive entities	4.20%	Low
Resolve unsecure account attributes	4.20%	Low
Stop clear text credentials exposure	4.20%	Low

Active Directory and On-Premises enviroment

Improvement action

Stop clear text credentials exposure

SCORE IMPACT
+4.20%

CURRENT SCORE
0

MAX SCORE
5

STATUS
To address

DESCRIPTION
Entities exposing credentials in clear text increase risk because unsecure traffic, such as LDAP simple-bind, is highly susceptible to interception. Attackers can then engage in malicious activities like stealing credentials. Through a security assessment, Azure Advanced Threat Protection detects credentials being exposed in clear text through network traffic and event monitoring.

USER IMPACT
Low

IMPLEMENTATION COST
Low

WHAT AM I ABOUT TO CHANGE?
In

HOW WILL IT AFFECT MY USERS?
Any user or application that relies on authentication in clear text will no longer be able to work.

Get Started

REDUCED ATTACK SURFACE

IDENTITY SECURE SCORE

Secure Score for Identity

43.99%

Last updated 3/28/2021, 1:00:00 AM
View your Microsoft Secure Score.

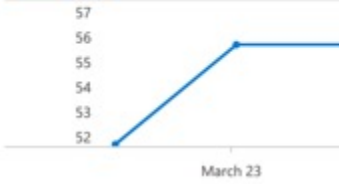
Comparison

CloudLab	43.99%
Industry average	0%
Typical 0-5 person company	12.99%

Change industry

Score history

7 days | 30 days | 60 days | 90 d



Improvement actions

Download | Columns

Name	Score Impact	User Impact	
Enable Password Hash Sync if hybrid	4.20%	Low	Prerequites and configuration of Identity Protection
Turn on user risk policy	5.88%	Moderate	
Turn on sign-in risk policy	5.88%	Moderate	
Enable self-service password reset	0.84%	Moderate	Modernized Password Policy
Do not expire passwords	6.72%	Moderate	
Do not allow users to grant consent to unmanaged applications	3.36%	Moderate	App Integration
Require MFA for administrative roles	8.40%	Low	Conditional Access and MFA Design
Ensure all users can complete multi-factor authentication for secure access	7.56%	High	
Enable policy to block legacy authentication	6.72%	Moderate	

Improvement action

Do not allow users to grant consent to unmanaged applications

SCORE IMPACT
+3.36%

CURRENT SCORE
4

MAX SCORE
4

STATUS
To address

DESCRIPTION
Tighten the security of your services by regulating the access of third-party integrated apps. Only allow access to necessary apps that support robust security controls. Third-party applications are not created by Microsoft, so there is a possibility they could be used for malicious purposes like exfiltrating data from your tenancy. Attackers can maintain persistent access to your services through these integrated apps, without relying on compromised accounts.

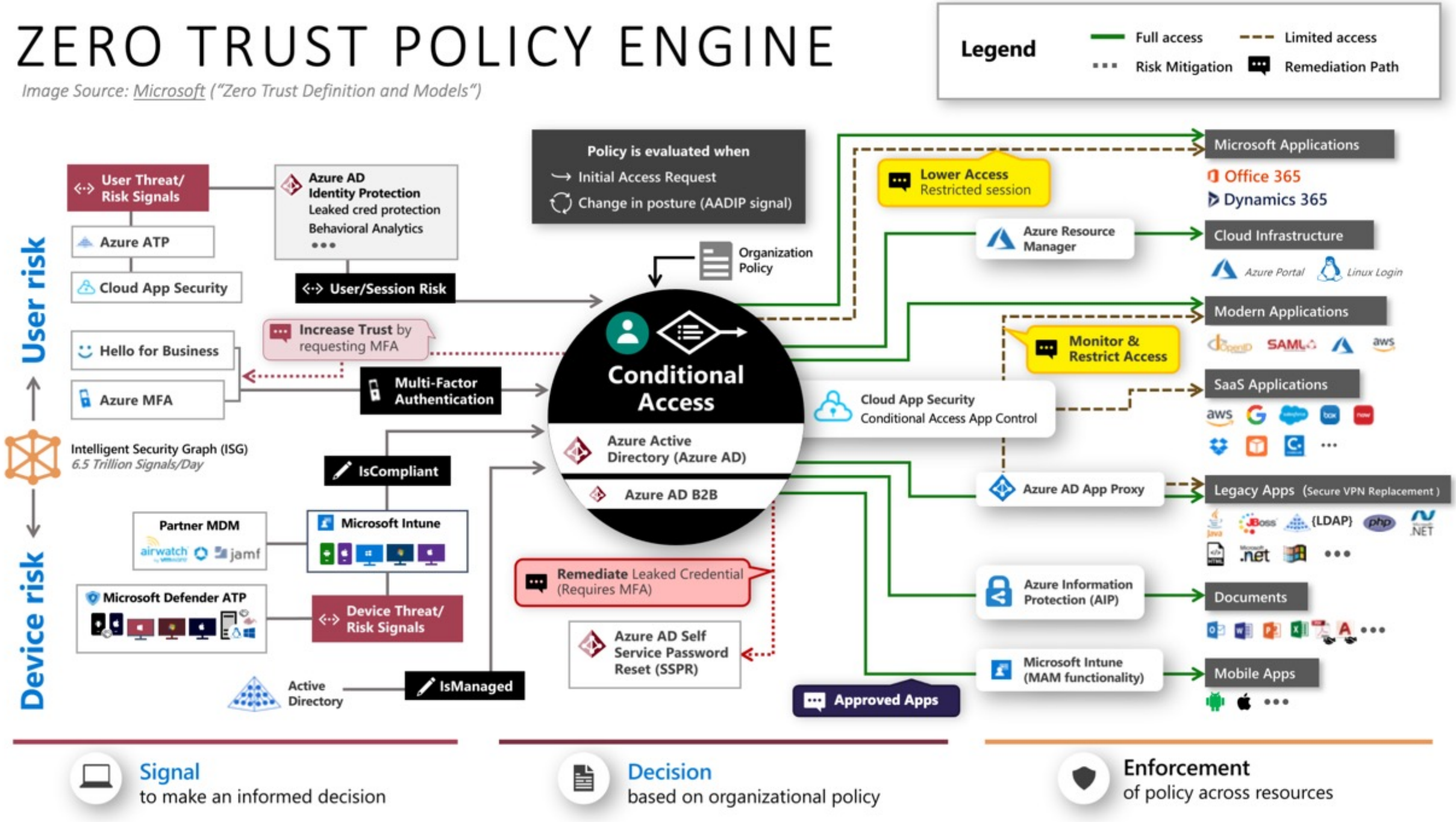
USER IMPACT
Moderate

IMPLEMENTATION COST
Low

WHAT AM I ABOUT TO CHANGE?
To prevent users in your organization from allowing third-party apps to access their Office 365 information, and require future consent operations to be performed by an administrator, go to the Azure Active Directory admin center > Enterprise applications > User settings > Enterprise applications. Set the toggle "Users

ZERO TRUST POLICY ENGINE

Image Source: Microsoft ("Zero Trust Definition and Models")

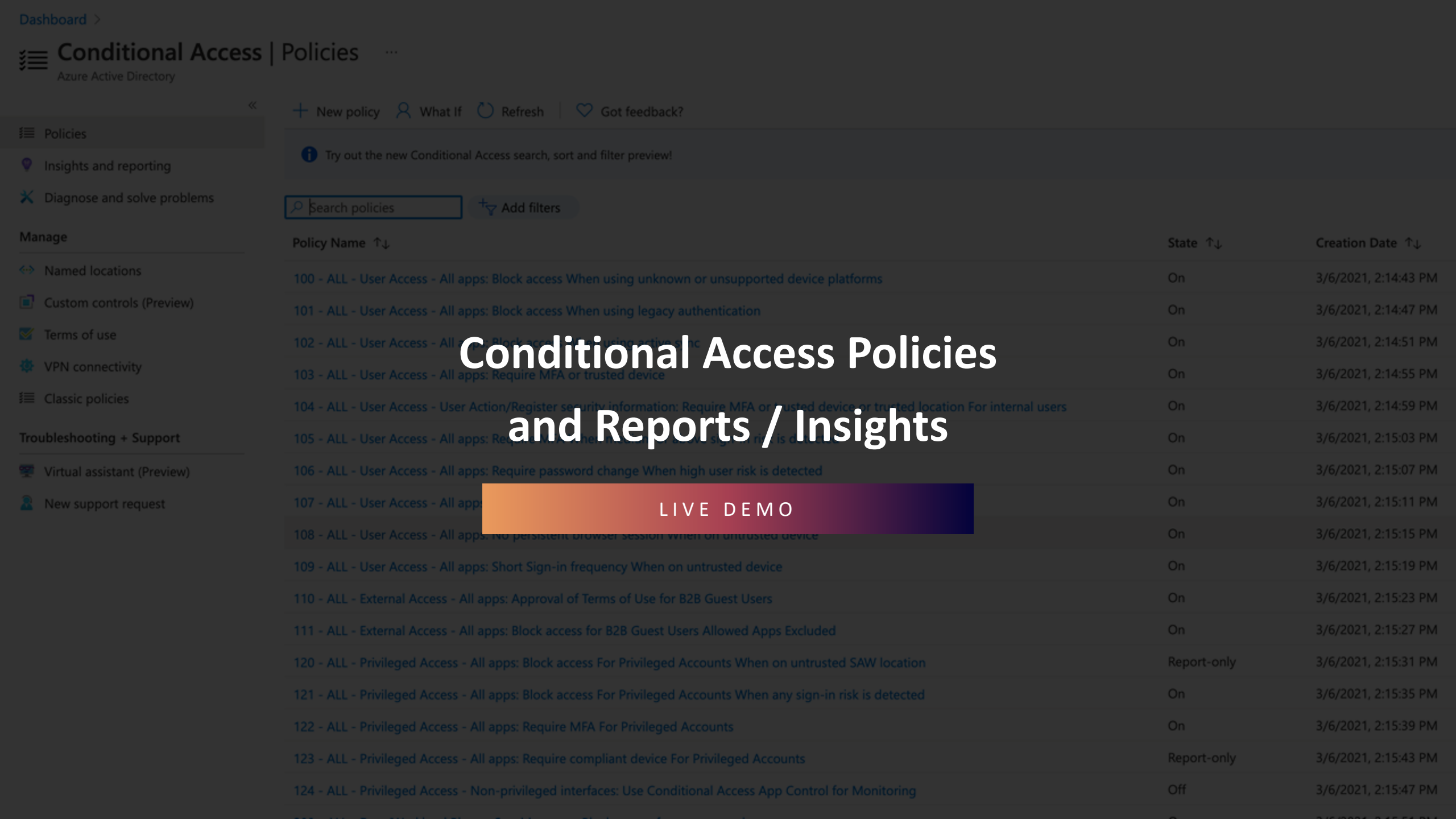


DESIGN YOUR CA POLICY BASELINE

Ensure to protect **every user and every app by baseline policy set**!

Consider your environment (types of apps, devices and authentication methods)!

Exclusions and lifecycle of **policies must be managed very carefully!**



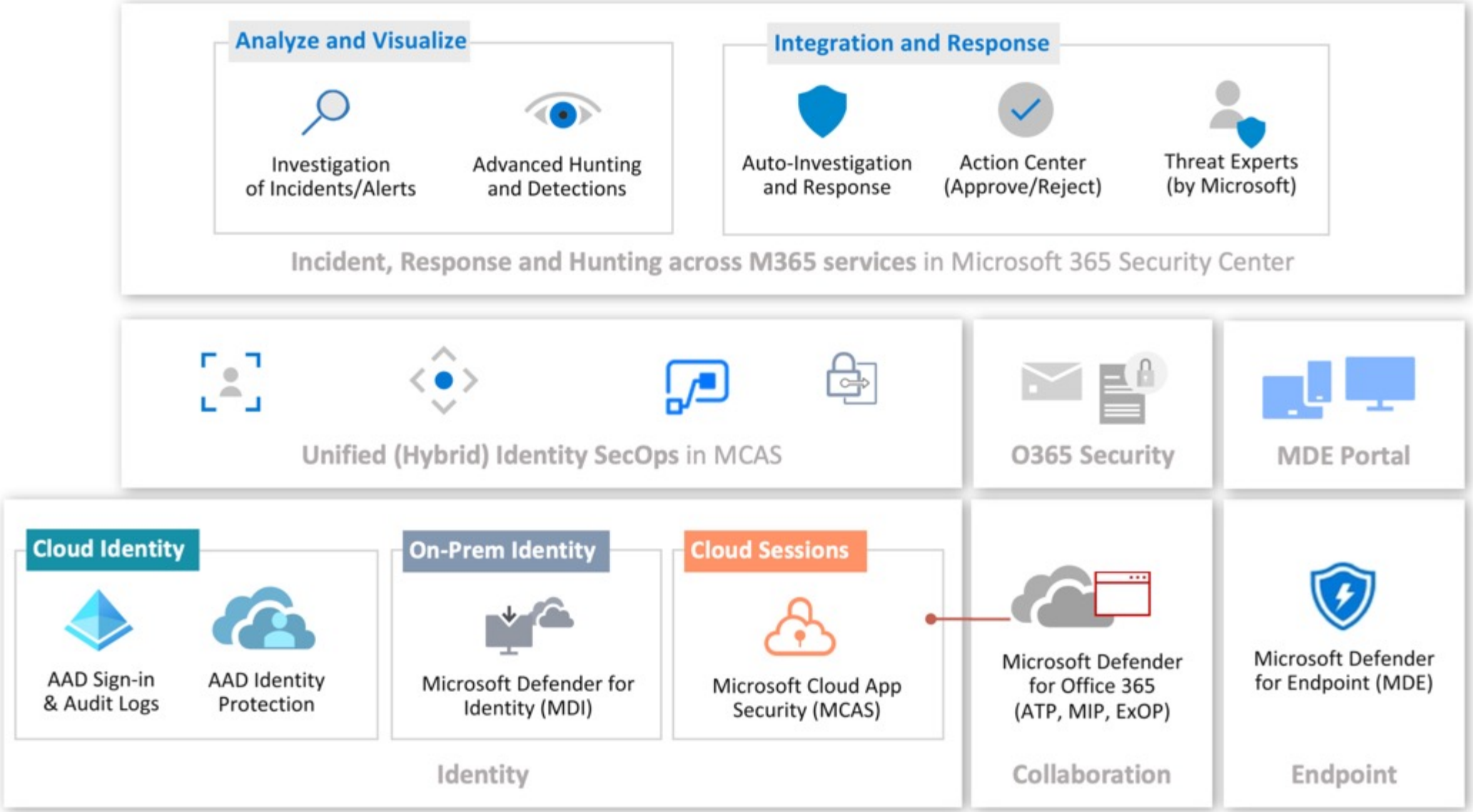
Conditional Access Policies and Reports / Insights

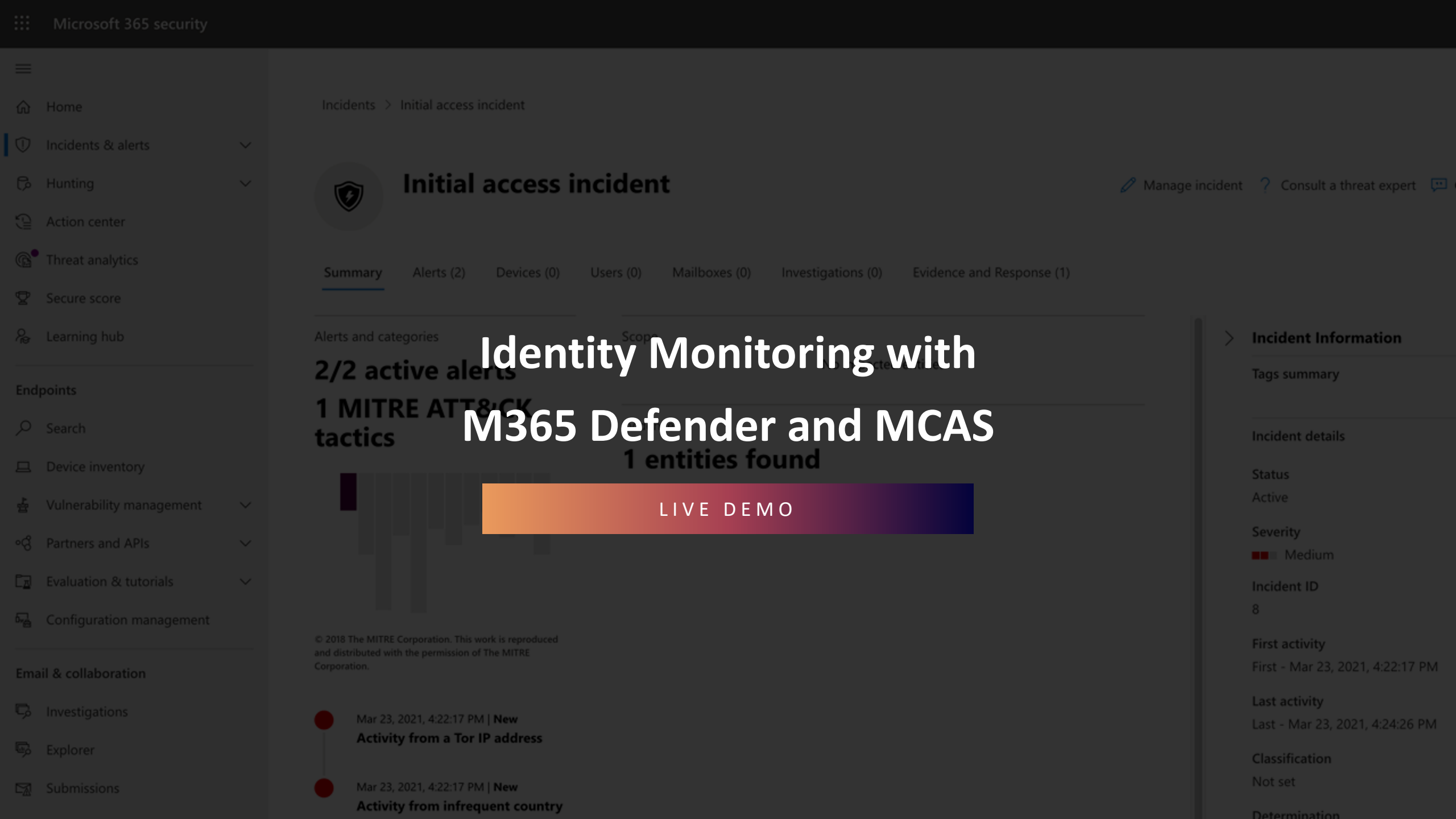
LIVE DEMO

UNIFIED VIEW OF IDENTITY THREAT

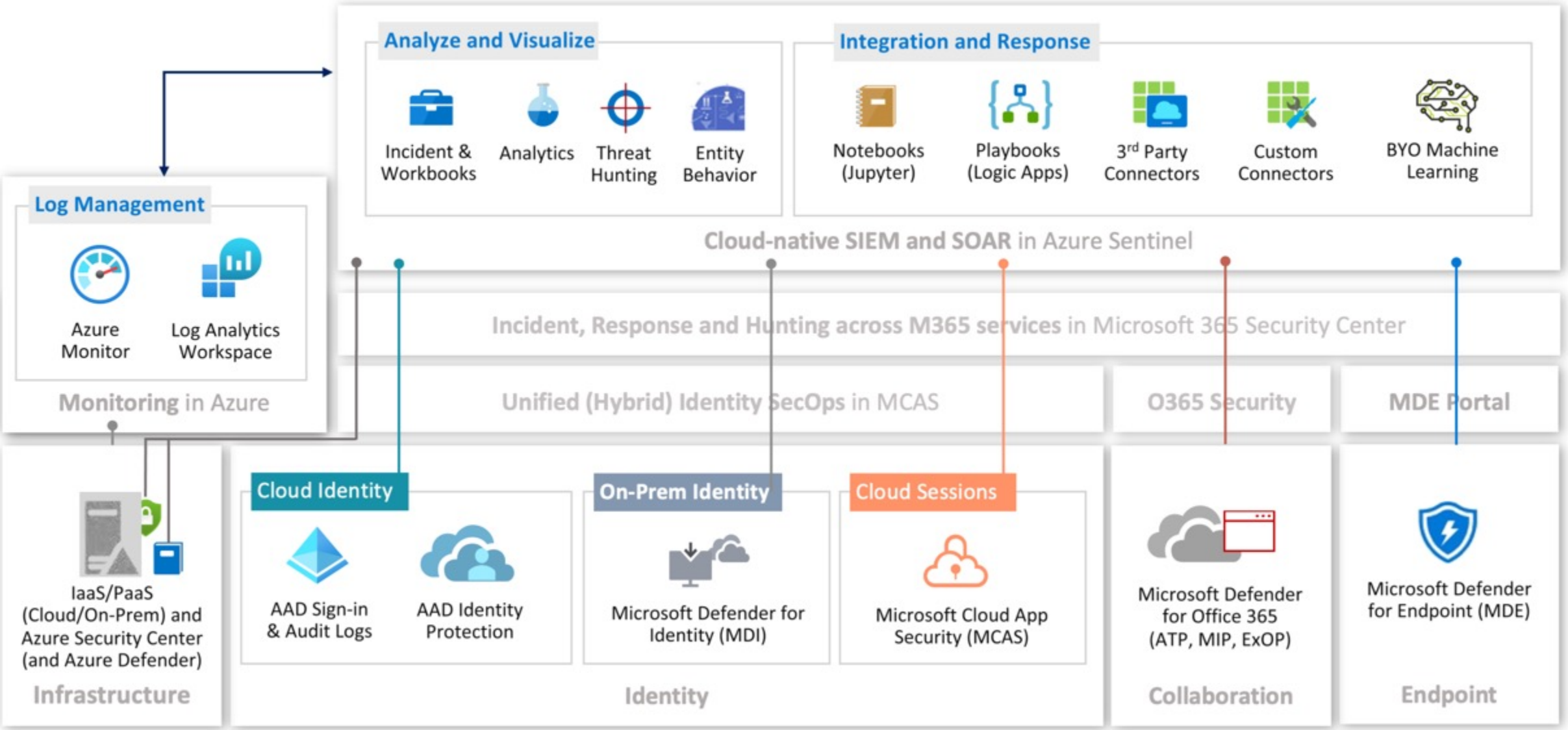
IDENTITY SECURITY MONITORING

IDENTITY SECURITY OPERATIONS

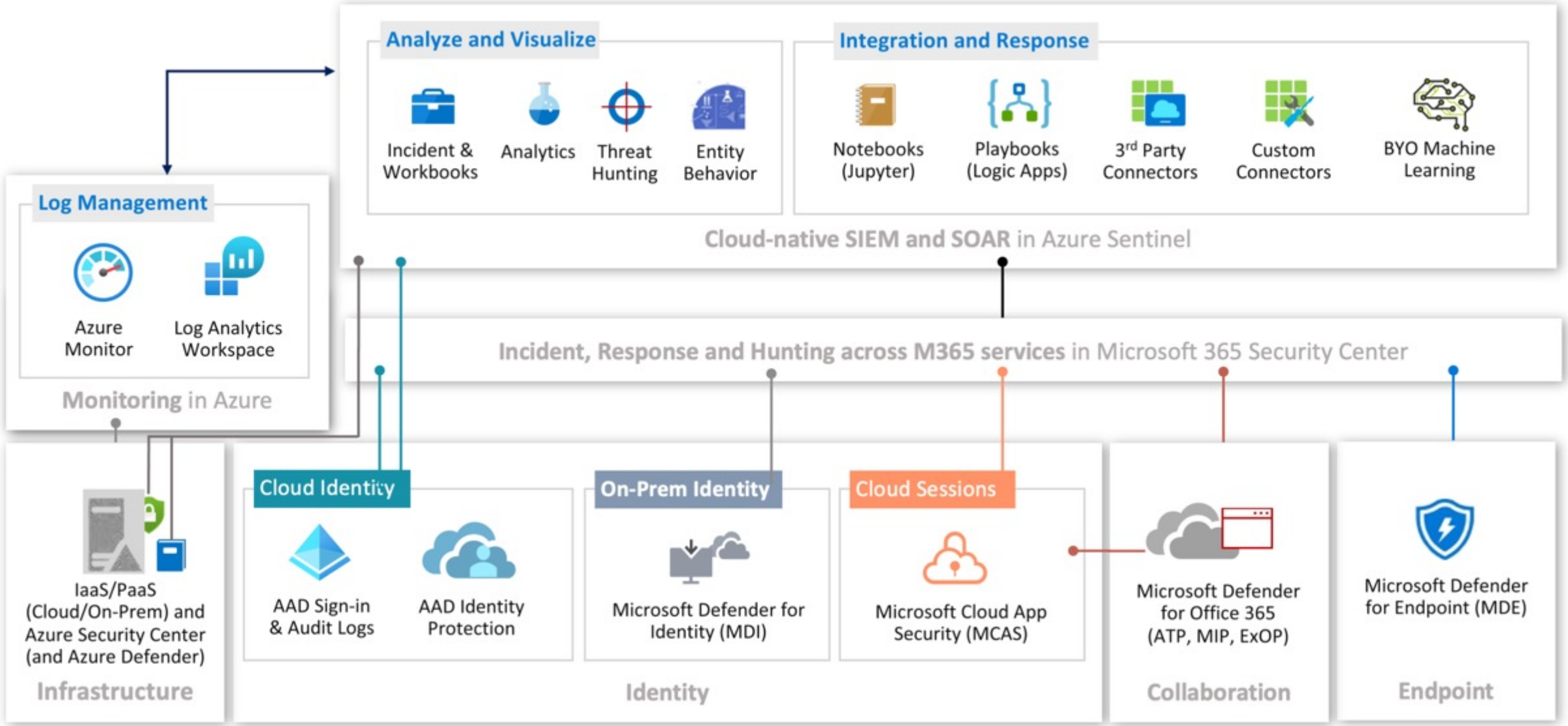


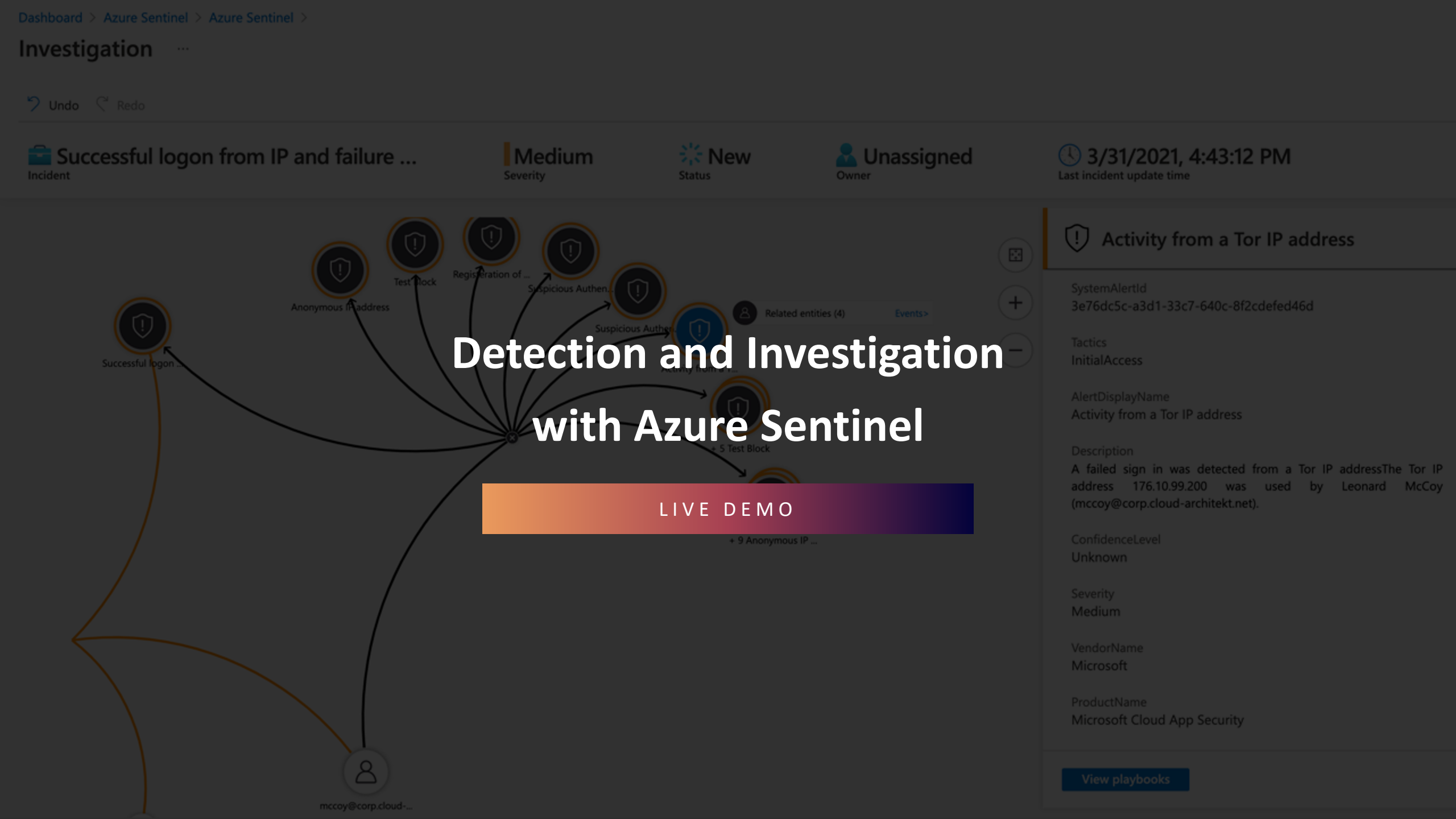

Microsoft 365 security
Home
Incidents & alerts
Hunting
Action center
Threat analytics
Secure score
Learning hub
Endpoints
Search
Device inventory
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management
Email & collaboration
Investigations
Explorer
Submissions
Incidents > Initial access incident
Initial access incident
Manage incident
Consult a threat expert
Summary
Alerts (2)
Devices (0)
Users (0)
Mailboxes (0)
Investigations (0)
Evidence and Response (1)
Alerts and categories
2/2 active alerts
1 MITRE ATT&CK tactics
1 entities found
© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
Mar 23, 2021, 4:22:17 PM | New
Activity from a Tor IP address
Mar 23, 2021, 4:22:17 PM | New
Activity from infrequent country
Incident Information
Tags summary
Incident details
Status
Active
Severity
Medium
Incident ID
8
First activity
First - Mar 23, 2021, 4:22:17 PM
Last activity
Last - Mar 23, 2021, 4:24:26 PM
Classification
Not set
Identity Monitoring with
M365 Defender and MCAS
LIVE DEMO

SECOPS WITH AZURE SENTINEL



AZURE SENTINEL & M365 DEFENDER





Detection and Investigation with Azure Sentinel

LIVE DEMO

THANK YOU

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net