Securing and monitoring Azure AD accounts

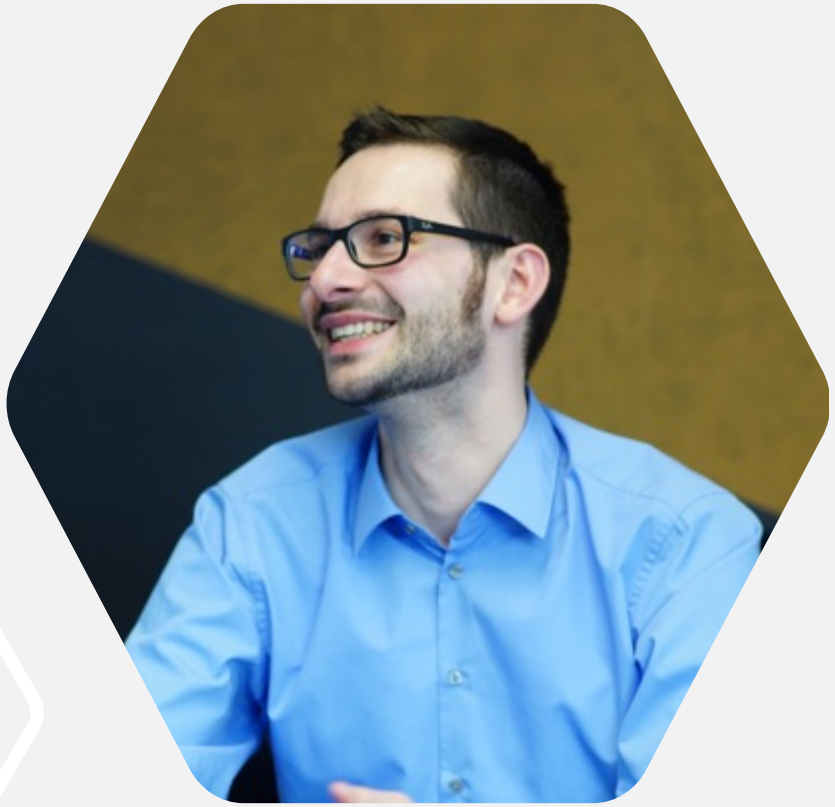
Thomas Naunheim

Azure Meetup Bonn, 20.08.2019

About Me

Thomas Naunheim

Cloud Engineer
Koblenz, Germany

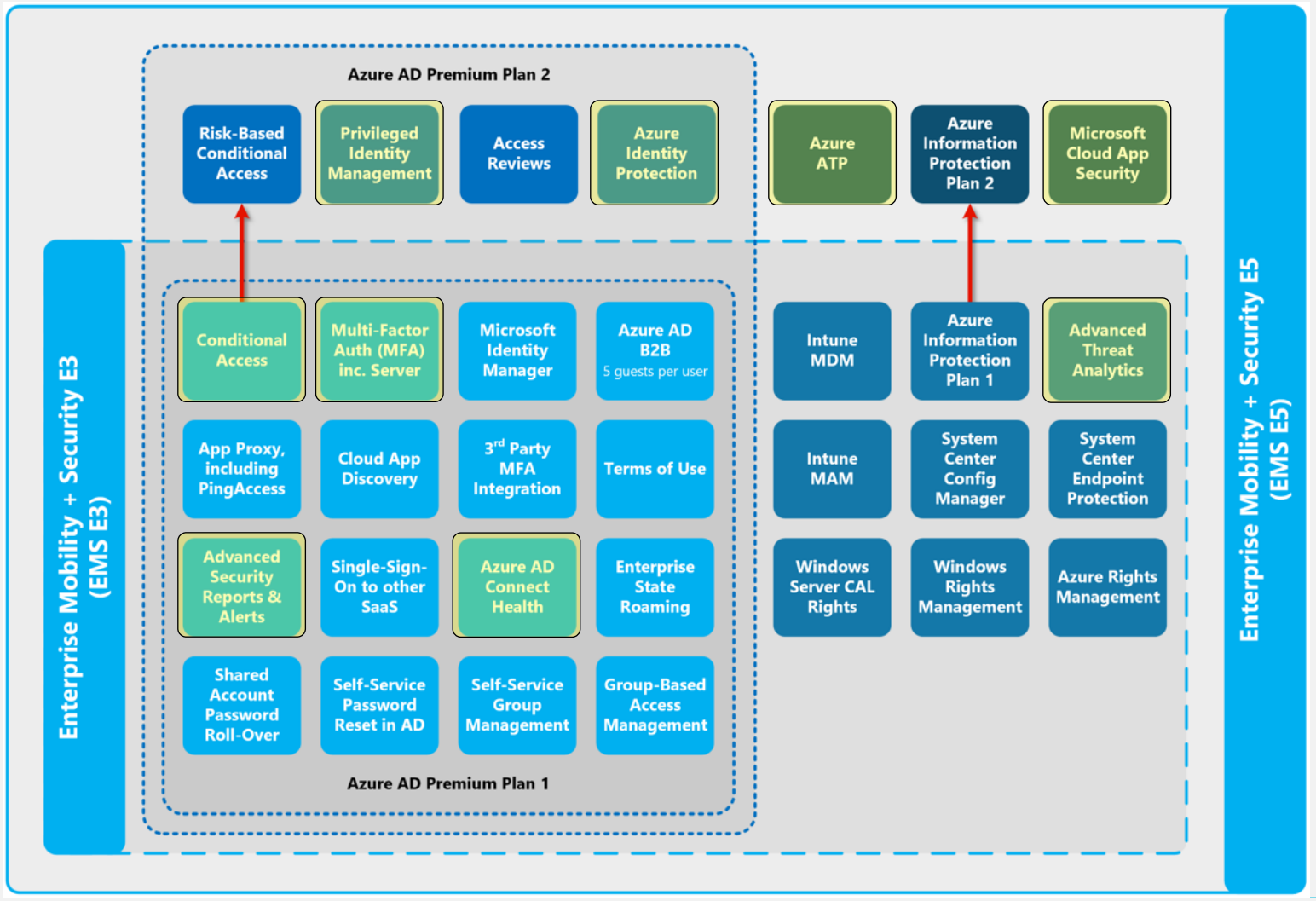


@Thomas_Live

Thomas@Naunheim.net

About Licensing...

...security costs money!



Source: https://github.com/AaronDinnage/Licensing/

Agenda

1. Zero Trust with „Conditional Access“
2. Advanced protection of identities and access
3. Privileged identity management
4. Auditing and monitoring

Microsoft's "Zero Trust" approach

never trust, always verify

Identity Protection

→ Strong identities with detection of user/sign-in risk

Endpoint Security

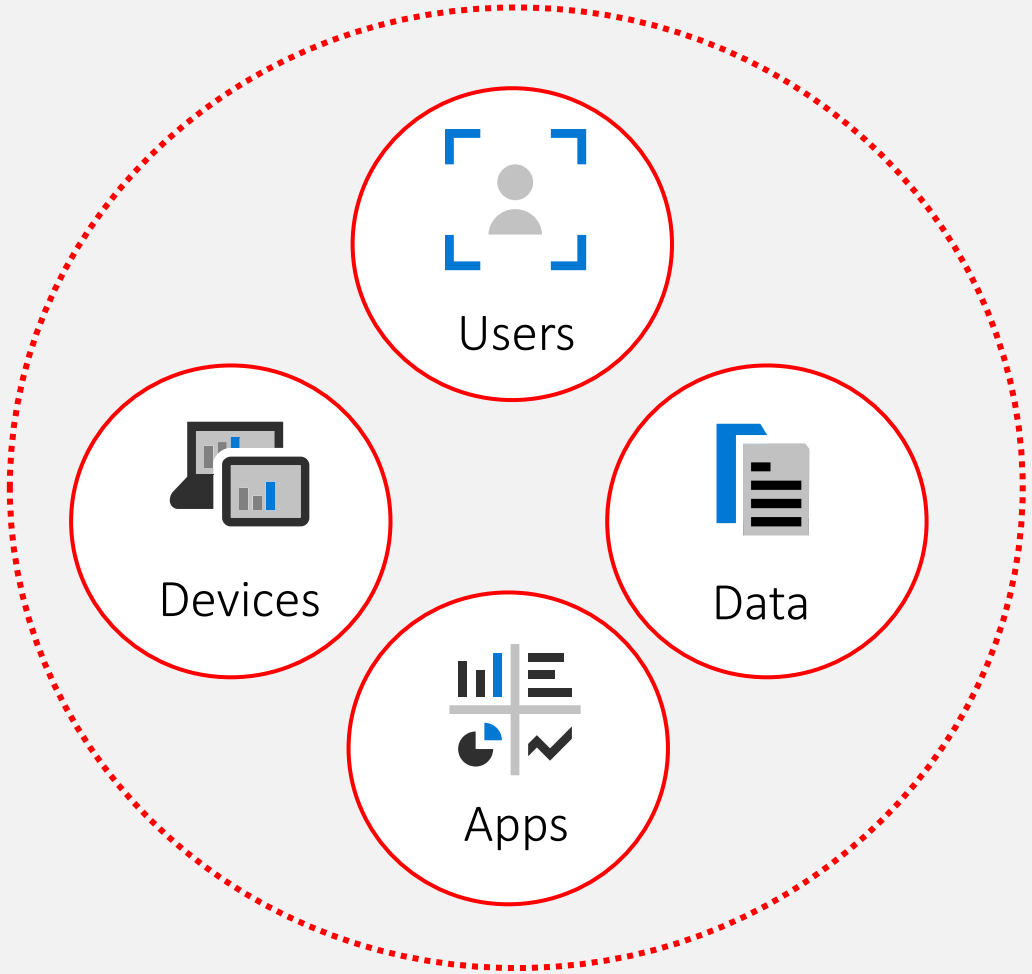
→ Enrolled devices (health and compliance status)

Information Protection

→ Policies based on classification/risk levels

(Cloud) App Security

→ Monitoring and controlling of apps and activities



Unpriviliged network
(outside traditional corporate network boundaries with VPN and firewalls)

Identity as a new perimeter
General considerations

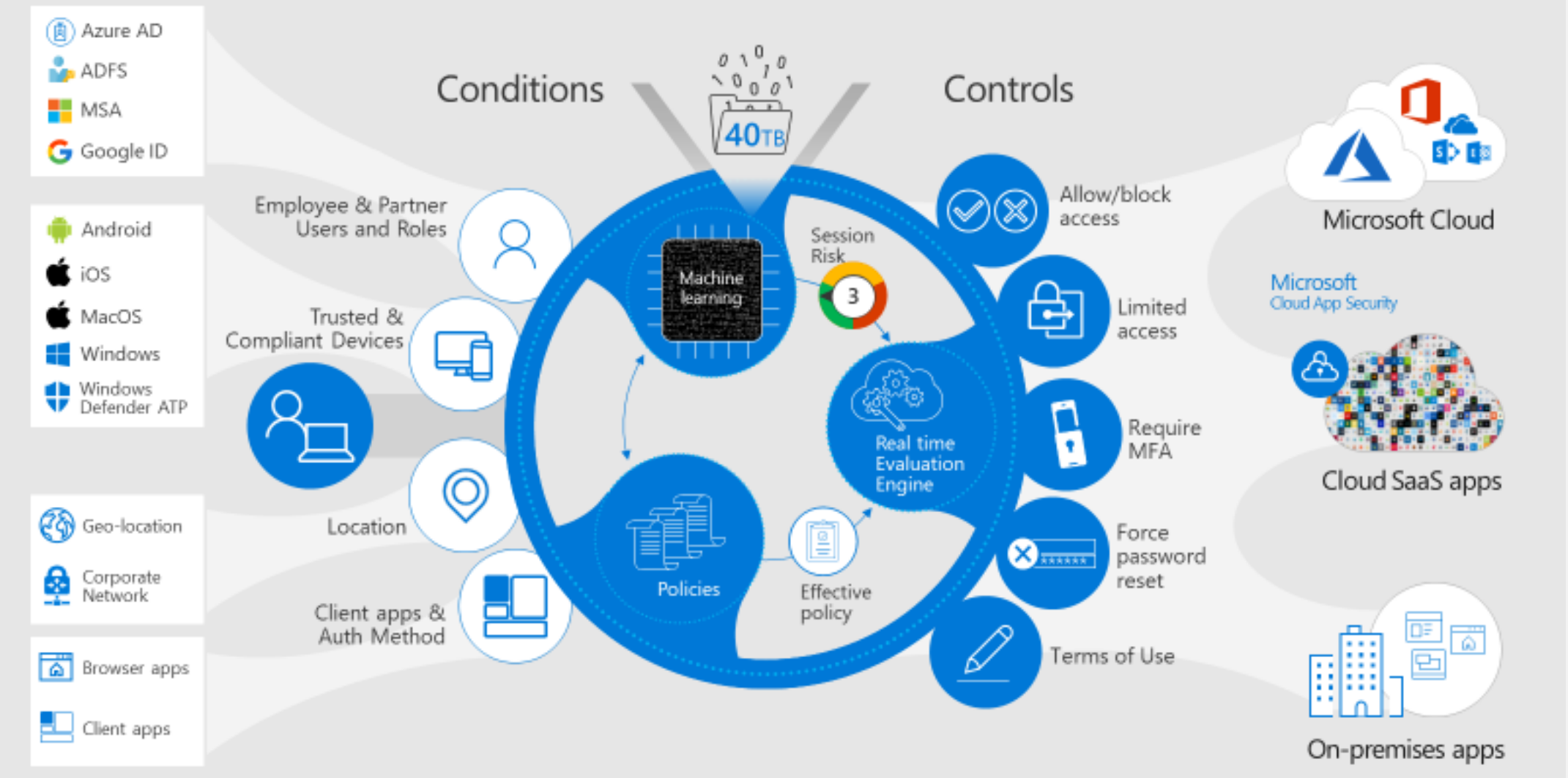
- Do not relay on your **existing security policies and network environments** (only)
  - Bypassing based on trusted network range
  - Block access from specific countries
  - Block unknown areas (mostly IPv6 addresses)

- **Configuring** named locations to reduce the amount of false-positive

- **Microsoft Security Intelligent (Graph)**
  Machine Learning and advanced AI = Security insights, risk score and alerts

„Zero Trust“ with Conditional Access

Zero Trust with „Conditional Access“



Source: https://www.microsoft.com/security/blog/2019/04/25/microsoft-threat-protection-april-update/

Zero Trust with „Conditional Access“

Design and Implementation of policies

- (Predefined) **Baseline** and (**custom**) standard **policies**
- Group by user-, (device) platform- or resource-related policies
- Define a standard **naming** convention for policies

  CA01 - Dynamics CRP: Require MFA for marketing When on external networks

<SN>-	<Cloud app>:	<Response>	For	<Principal>	When	<Conditions>

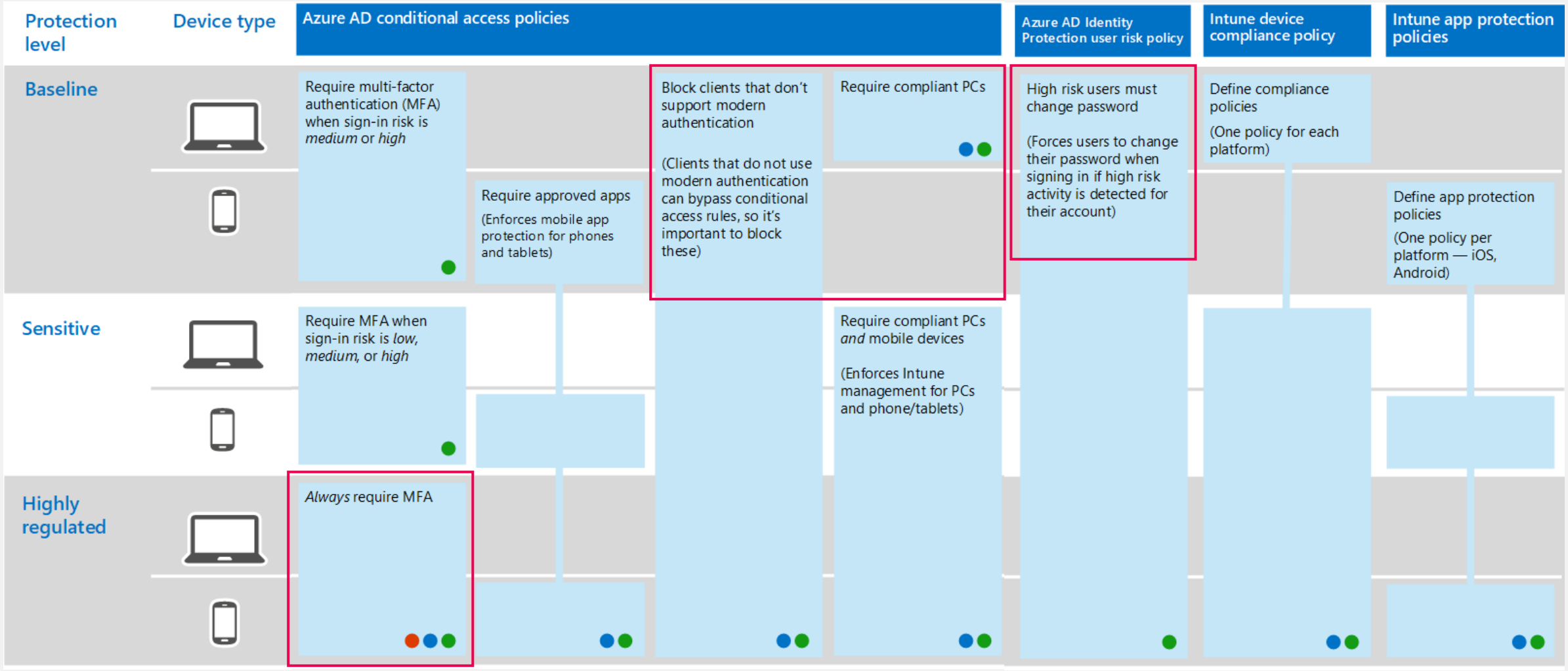
- **Draft policies** (when this happens → do this)

When this happens	Then do this

Source: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

Zero Trust with „Conditional Access“

Microsoft‘s “Golden“ Config (aka.ms/M365GoldenConfig)

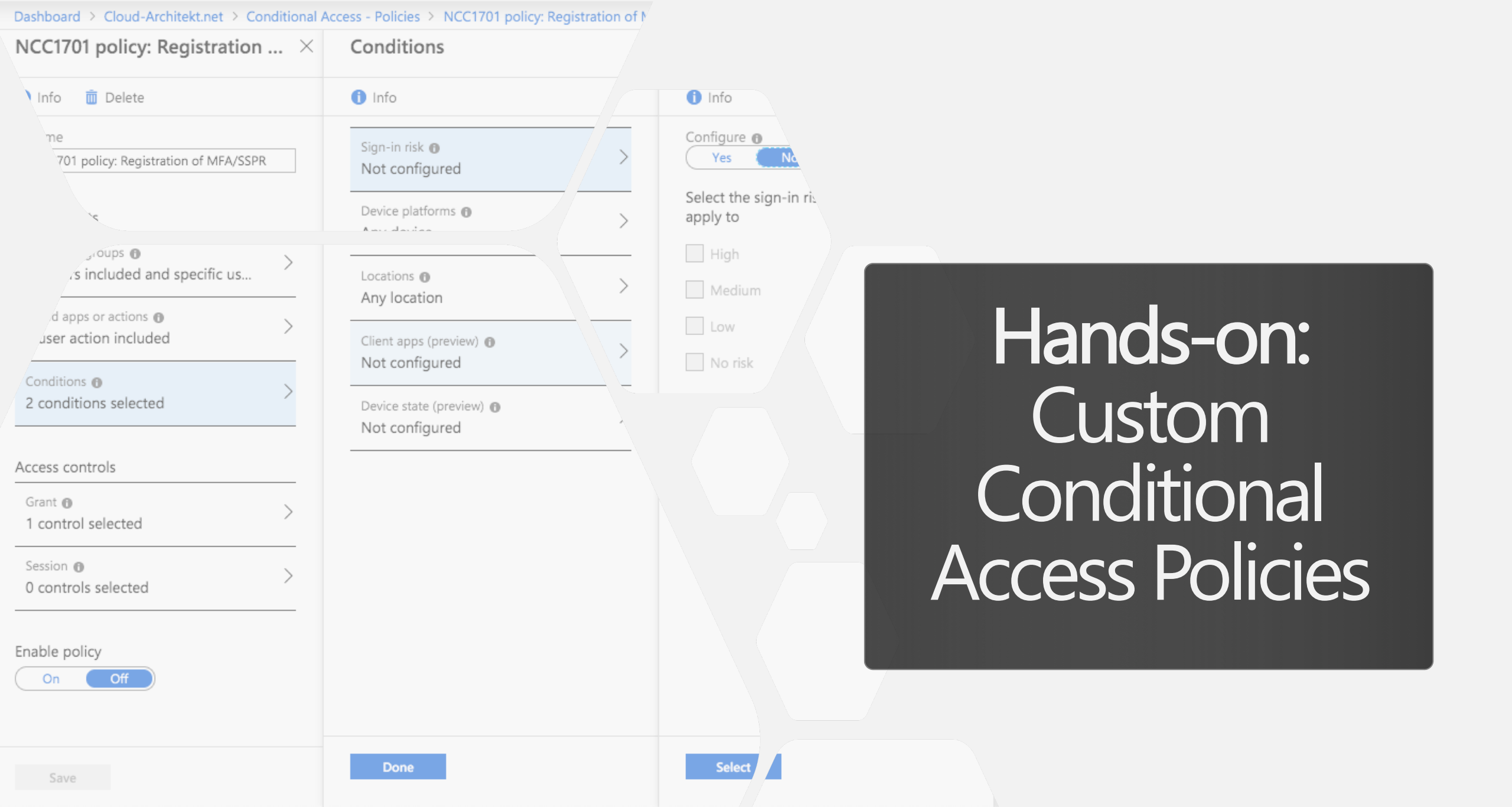


Source: https://docs.microsoft.com/en-us/microsoft-365/enterprise/identity-access-policies

Zero Trust with „Conditional Access“

Deployment and Management of policies

- Azure AD access reviews to **manage exclusions** from policies
- **Exclude emergency accounts** from every policy
- **Case of disruption or lockout: Contingency CA policy**
  (as part of resilient access control management strategy)
- **Automated documentation of Intune policies**
  (Intune Documentation by Thomas Kur)

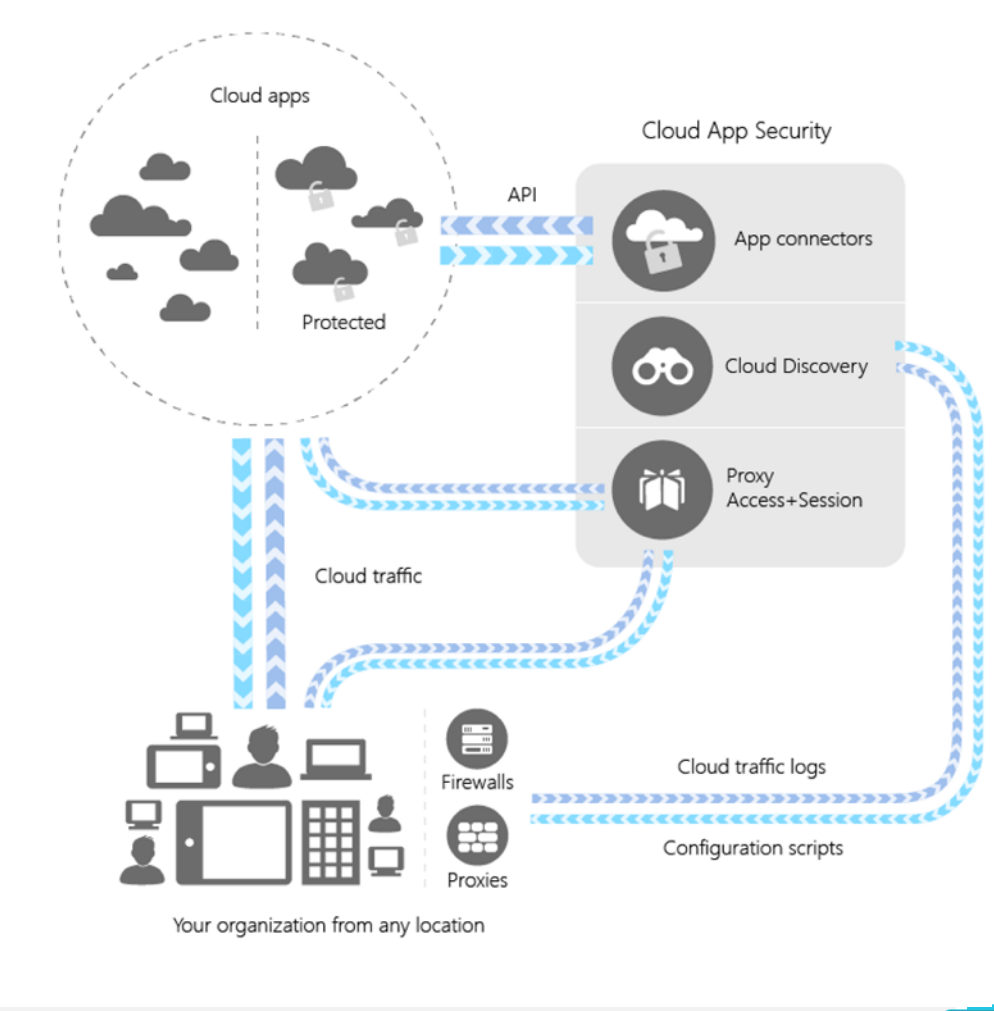


Hands-on: Custom Conditional Access Policies

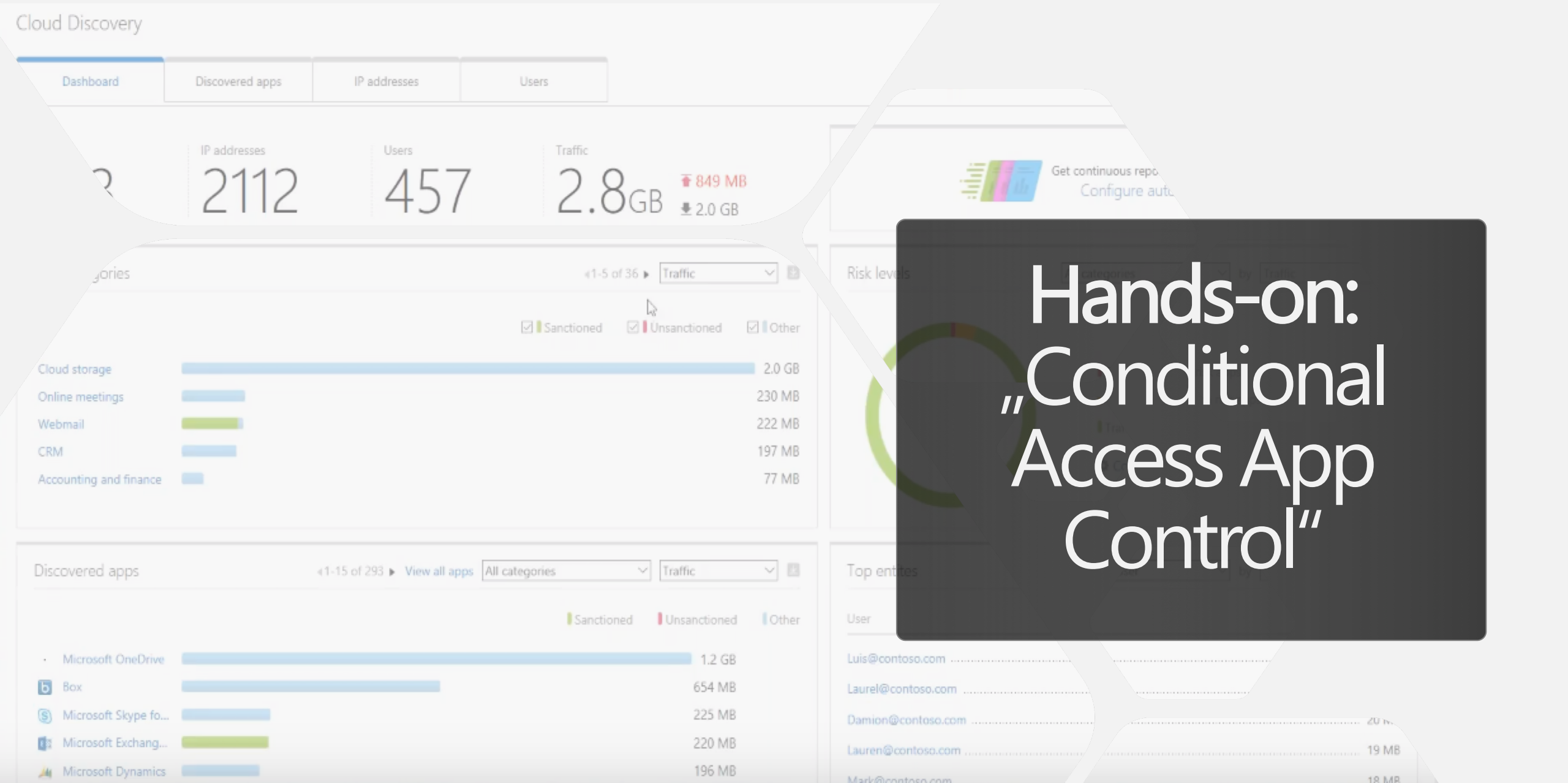
Zero Trust with „Microsoft Cloud App Security“

Detection across cloud apps and providers

- App connectors
  - Alerted on user or file behavior anomalies
  - Control data stored in (supported) cloud apps
- Cloud Discovery
  - Discover cloud apps based on traffic- and user data (from local network or MDATP as data source)
  - Evaluate risk of discovered apps
- Proxy Access + Conditional Access App Control
  - Sanctioning or blocking of (risky) apps/sessions
  - Real-time monitoring and control (AAD CA Integration)



Source: https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security


Cloud Discovery
Dashboard
Discovered apps
IP addresses
Users
IP addresses
2112
Users
457
Traffic
2.8GB
849 MB
2.0 GB
Traffic
Sanctioned
Unsanctioned
Other
Cloud storage
2.0 GB
Online meetings
230 MB
Webmail
222 MB
CRM
197 MB
Accounting and finance
77 MB
Risk levels
Discovered apps
View all apps
All categories
Traffic
Sanctioned
Unsanctioned
Other
Microsoft OneDrive
1.2 GB
Box
654 MB
Microsoft Skype fo...
225 MB
Microsoft Exchang...
220 MB
Microsoft Dynamics
196 MB
Top entities
User
Luis@contoso.com
Laurel@contoso.com
Damion@contoso.com
Lauren@contoso.com
19 MB
Hands-on:
„Conditional
Access App
Control“

Zero Trust with „Conditional Access“
Considerations of Conditional Access Policies

- Settings reference and support of policies
  - Device platform: Windows, iOS, macOS and Android devices
  - Browser support limitations: Device Compliance in Firefox, „In private“-browsing
- Applying policies to all users incudes:
  - On-Premises Directory Synchronization Service Account
  - B2B (Guest) → Covered home and targeted tenant policies
  - Does not apply to Windows client logon (PRT request)
- Order of appy: Assignments are logically ANDed, blocks always wins and controls enforced in specific order (Workflow Cheatsheet)
- Service dependencies of cloud apps (e.g. Microsoft Teams)
- New: MFA and SSPR registration with CA policies

Zero Trust with „Conditional Access“

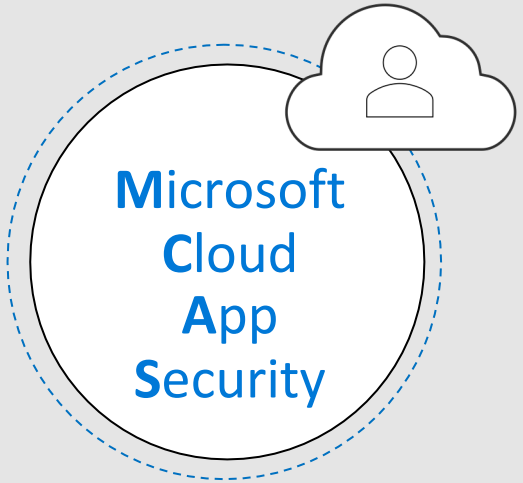
Support of 3rd party (security) solutions

- Users are redirected to a compatible service to satisfy further requirements outside of Azure Active Directory
- Configured as „custom control“ in Azure AD CA blade
- **MFA/User Risk:** PingID, DuoSecurity, …
- **Device Risk:** Lockout, Symantec Endpoint Protection,…
- **Device Compliance:** Jamf Pro, MobileIron
  (Integration of „Microsoft Intune Device Compliance Service“)
- **VPN Connectivity**: Azure AD-issued short-lived certificates for supported VPN solutions

Advanced protection of identities and access

Advanced protection of identities and access

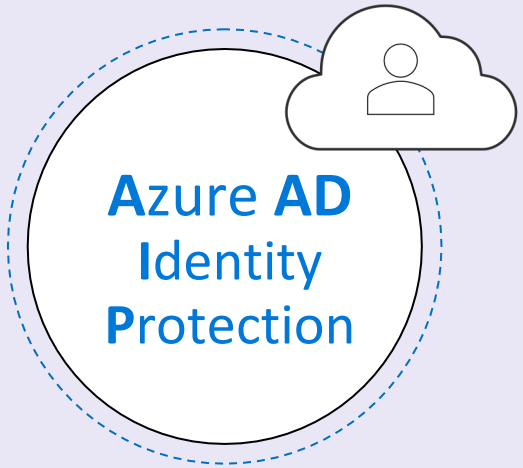
Investigation on cloud authentication, cloud apps and on-premises



Behavior across cloud apps

Activity from infrequent country

Data exfiltration to unsanctioned apps



Risky sign-ins & User Risk

Sign-ins from unfamiliar locations

-

Identity behavior on-premises

Suspicious VPN connection/sign-in

Data exfiltration over SMB

Source: Microsoft Ignite Session (https://mediusproduction.blob.core.windows.net/presentations/Ignite2018/BRK3117.pptx)

Advanced protection of identities and access

Automate response with risk-based conditional access policies

- Sign-In Risk
  - (Real-time or aggregated) Detections of the **probability a sign-in is compromised**
  - Various signals will be included and result will be sent to conditional access **(Session risk)**
  - Sample: Sign-in from Unfamiliar location
  - Automate response: Risk level „Medium and above“ → Allow access, Requried MFA

- User Risk
  - Detects the probability that a **user account has been compromised**
  - Analyzes each sign-in to detect suspicous and atypical user behaviour (collect data over time)
  - Sample: Leaked credential
  - Automate response: High Risk → Allow access, Force password change

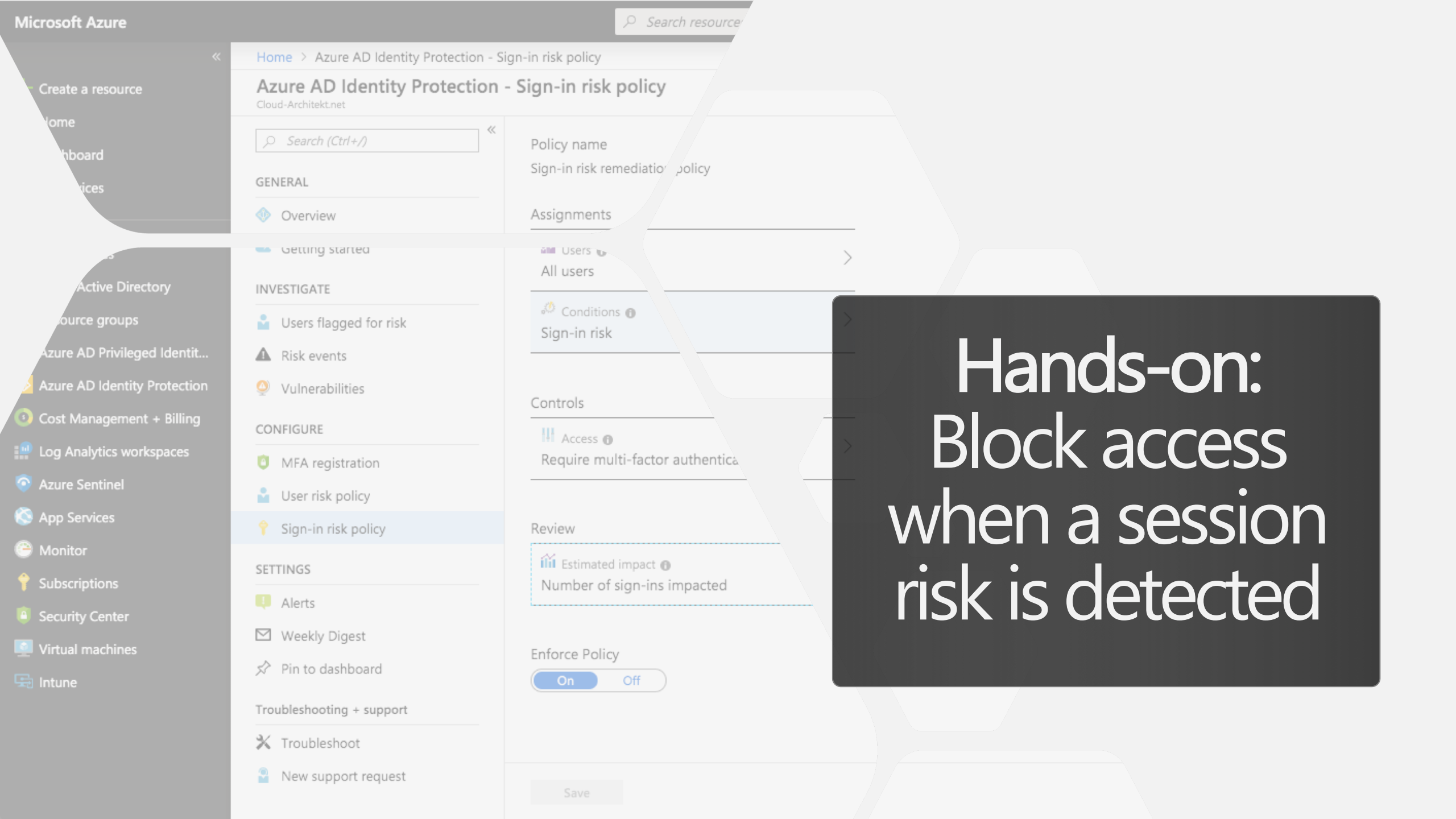
Advanced protection of identites and access

Risk events (Azure AD Identity Protection - Refreshed)

Risk event type	Description	Detection type
Atypical travel	Sign in from an atypical location based on the user's recent sign-ins.	Offline
Anonymous IP address	Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs).	Real-time
Unfamiliar sign-in properties*	Sign in with properties we've not seen recently for the given user.	Real-time
Malware linked IP address	Sign in from a malware linked IP address	Offline
Leaked Credentials	This risk event indicates that the user's valid credentials have been leaked	Offline

* Updated version of the Unfamiliar Sign-in Properties in August 2019.
increased number of signals (device identifiers, IP address, location, available browser sessions

Source: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-v2



Hands-on: Block access when a session risk is detected

Advanced protection of identities and access

Investigation on cloud authentication, cloud apps and on-premises

Behavior across cloud apps

Activity from infrequent country

Data exfiltration to unsanctioned apps

Risky sign-ins & User Risk

Sign-ins from unfamiliar locations

-

Identity behavior on-premises

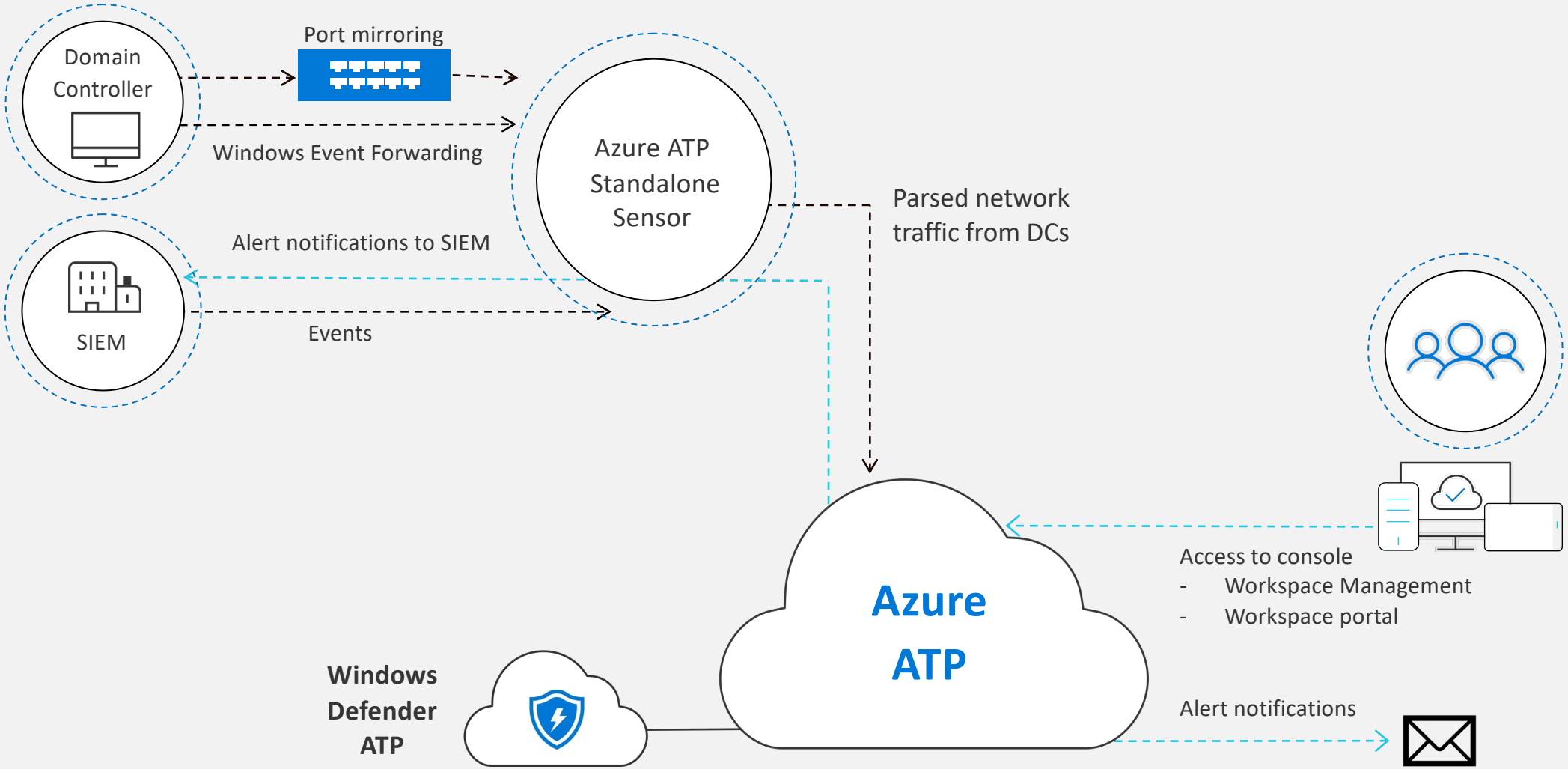
Suspicious VPN connection

Data exfiltration over SMB

Source: Microsoft Ignite Session (https://mediusproduction.blob.core.windows.net/presentations/Ignite2018/BRK3117.pptx)

Advanced protection of identities and access

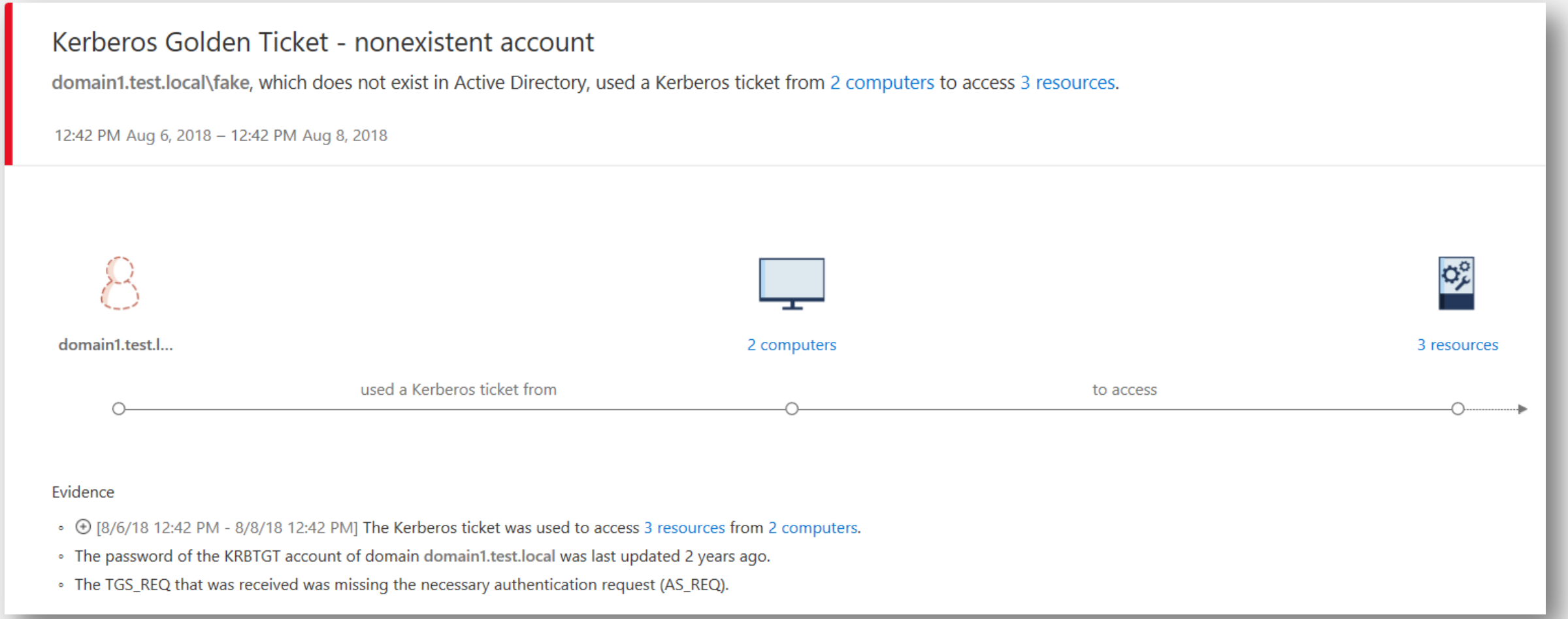
Protection of on-premises environment



Source: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-architecture

Advanced protection of identities and access

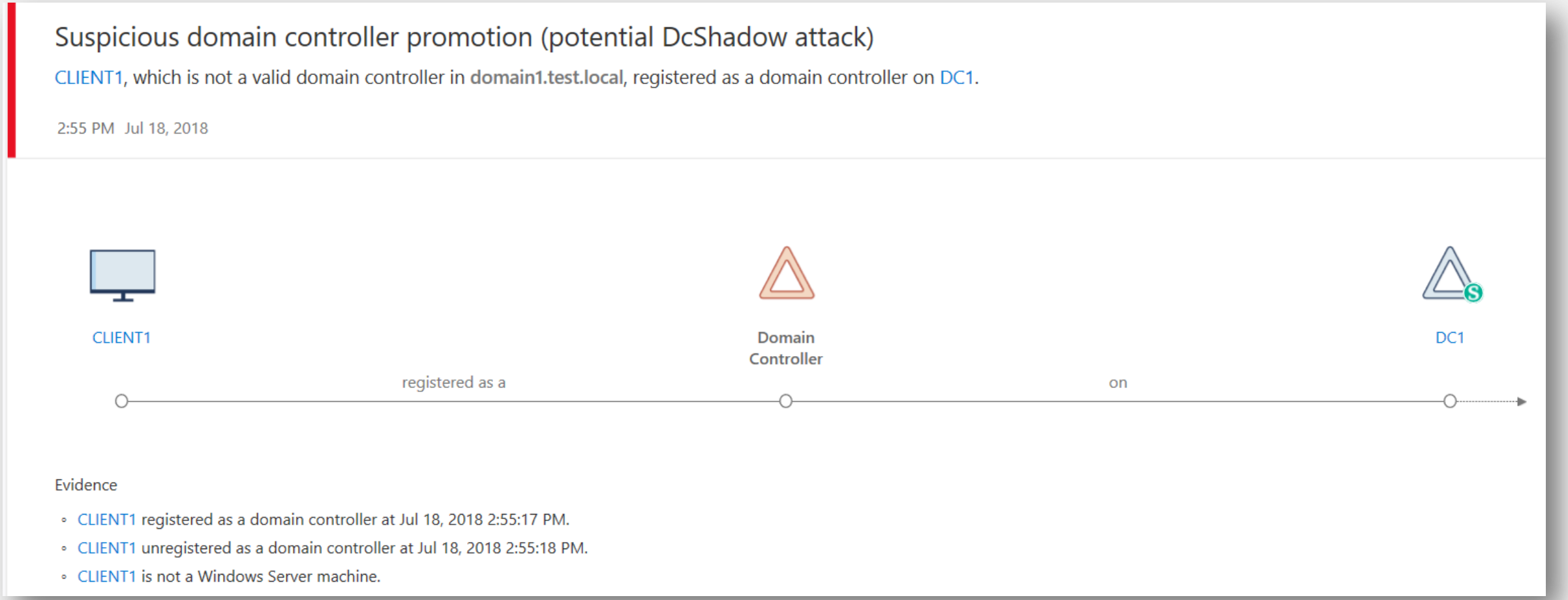
Protection of on-premises environment



Source: Microsoft Ignite Session (https://mediusproduction.blob.core.windows.net/presentations/Ignite2018/BRK3117.pptx)

Advanced protection of identities and access

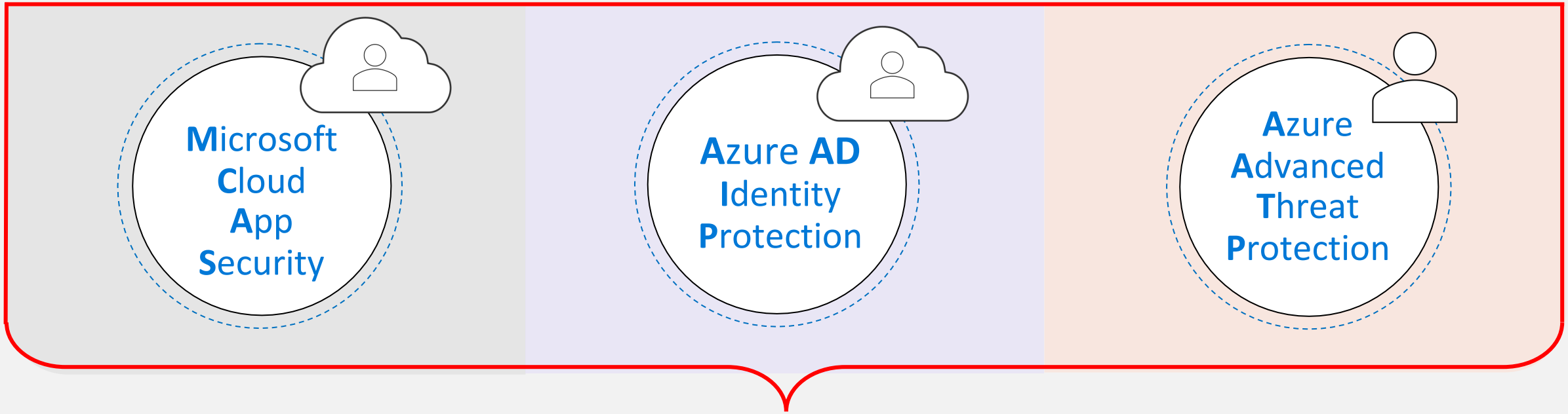
Protection of on-premises environment



Source: Microsoft Ignite Session (https://mediusproduction.blob.core.windows.net/presentations/Ignite2018/BRK3117.pptx)

Advanced protection of identities and access

Unified SecOps Investigation of hybrid environments



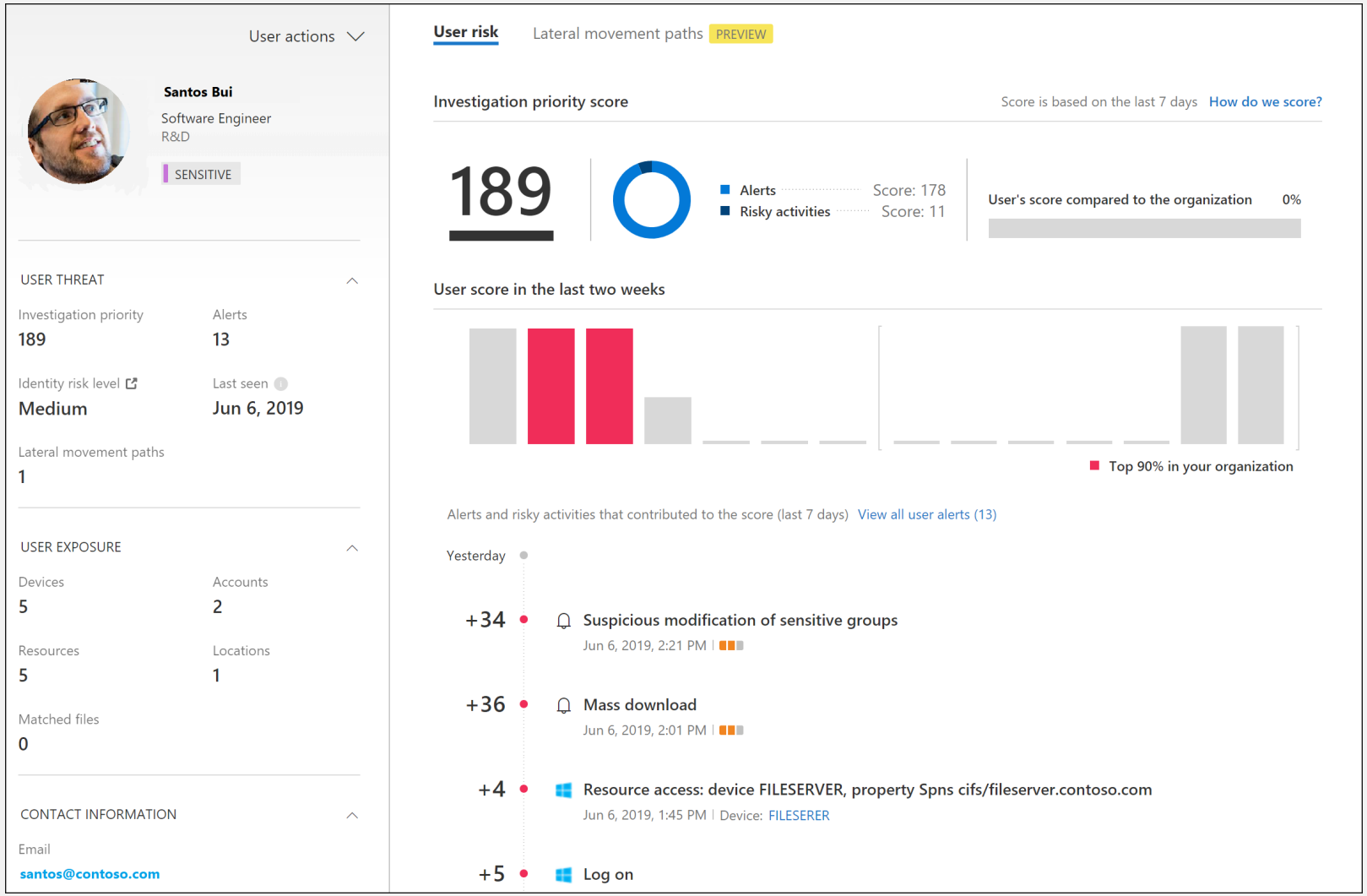
User and Entity Behavior Analytics (UEBA)

- Aggregated into users' „Investigation Priority score" built from evaluated data
- Unified portal for hunting and investigation in hybrid environments

Source: Microsoft Ignite Session (https://mediusproduction.blob.core.windows.net/presentations/Ignite2018/BRK3117.pptx)

Auditing and Monitoring of Azure Active Directory

Investigation Priority built on User and Entity Behavior Analytics



Source: https://docs.microsoft.com/en-us/cloud-app-security/tutorial-ueba

Advanced protection of identities and access
Smart Lockout

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

- AAD data center/regions tracks **lockout independently**
- (Un)familiar locations will be used for differentiation
  - Temporary lockout from (unfimiliar) locations (based on IP addresses)
- **Consideration** in hybrid environments **with PTA**:
  - **Lockout threshold** in Azure AD should be **less than in AD**
  - **Lockout duration** should be set **longer than AD reset**

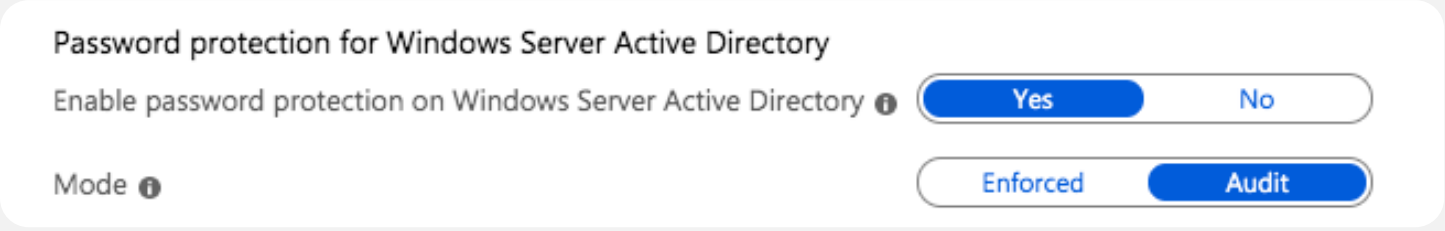
Source: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

Advanced protection of identities and access

Password Protection

- **Reset or change password checks** current version of „global **banned password list**“
- Based on **known bad patterns** (passw0rds and k3ywords)
- **Custom** banned password **list** (max. 1000 terms and 16 characters)

- On-premises integration with “**Azure AD Password Protection**“ (including monitoring)



Source: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

Privileged Identity Management (PIM)

Privileged Identity Management (PIM)

Foundation of securing privileged access

Isolated privileged identities

Issue managed and isolated administrator identity (“SC-Alt”), strong or password less authentication

Non-persistent access

Provide zero rights by default to administration accounts

Just-in-time (JIT) privileges based on a standardized RBAC model

Secure devices

Establish a separate device/workstation for administrative tasks

Various kinds of security levels and implementations

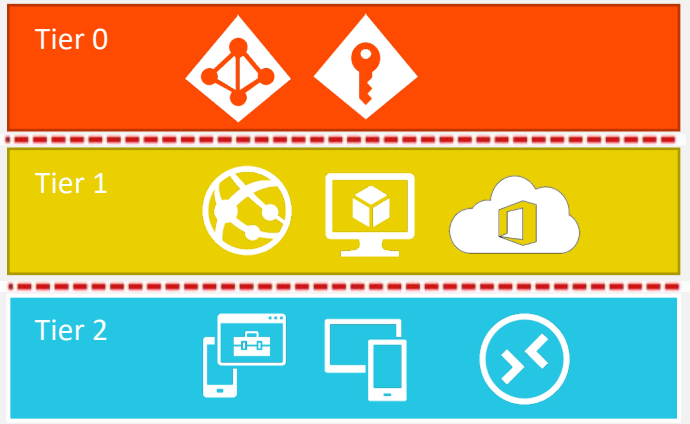
Source: https://www.microsoft.com/security/blog/2019/05/08/3-investments-improve-identity-management-microsoft/

Privileged Identity Management (PIM)

Design your Azure AD roles

Security isolation level of privileged identities

- Separate your work account and privileged account
- Do not sync on-premises accounts as cloud admin
- Tiering model of **E**nhanced **S**ecurity **A**dministrative **E**nvironment



Privileged Identity Management (PIM)

Design your Azure AD roles

Built-in Azure AD directory roles and limitations

- Azure AD Built-in Directory roles and least-privileged roles by task
- Custom directory roles → Available in public preview for “app registration”
- No support for security group assignment → “Under review” by AAD product group

“Red Tenant” / ESAE design approach in the cloud

- Securing privileged identities in an **isolated tenant**
  - Separated identity and device management
- **CSP scenarios** or very **high regulated organizations**
- **No hybrid identity** integration (AAD Connect)
- Access to managed tenants **via Guest assignment (B2B)**
- **Privileged resources only** (security groups, apps, network, devices,..)

Privileged Identity Management (PIM)
Considerations in RBAC Design

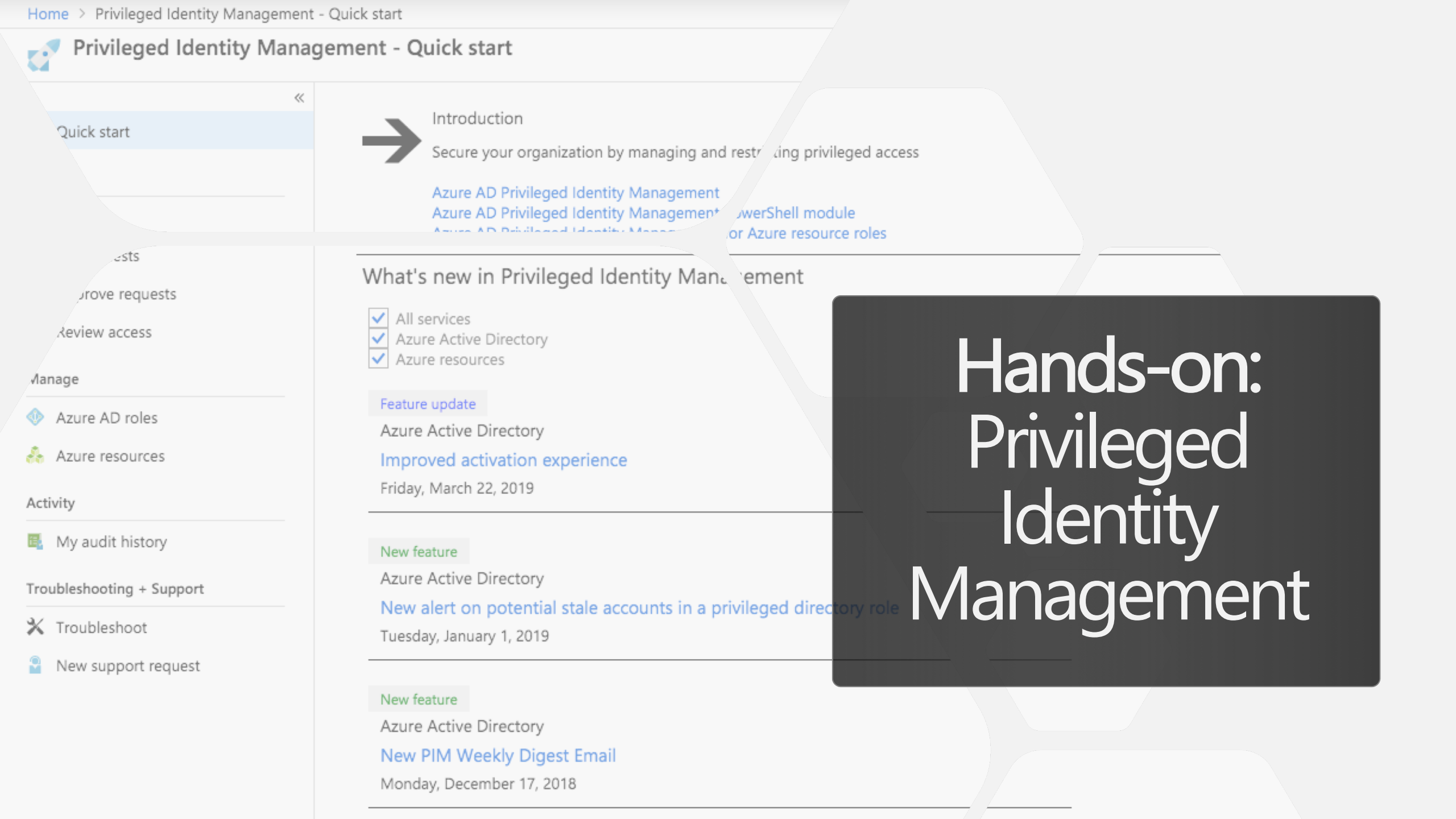
- Challenge to limit default directory roles / least privileges
  - Intune Service administrator has the permission to modify security groups
  - Exchange Online administrator are able to create security groups (undocumented)

- Additional administrative roles and assignments for Microsoft 365 services
  - RBAC in Intune, Microsoft Defender ATP, Windows Store for Business,…
  - No PIM management for these RBAC roles
  - Inheritance permission of Azure AD directory roles

- Cloud-only security groups for assignment to policies and Azure/AAD roles

- Permanent view-only permission (e.g. “Global Reader”)

- Inheritance permissions of Azure EA (Account Owner) and CSPs (delegated admins)


Home > Privileged Identity Management - Quick start
Privileged Identity Management - Quick start
Quick start
Introduction
Secure your organization by managing and restr ging privileged access
Azure AD Privileged Identity Management
Azure AD Privileged Identity Management owerShell module
or Azure resource roles
sts
rove requests
eview access
Manage
Azure AD roles
Azure resources
Activity
My audit history
Troubleshooting + Support
Troubleshoot
New support request
What's new in Privileged Identity Man ement
All services
Azure Active Directory
Azure resources
Feature update
Azure Active Directory
Improved activation experience
Friday, March 22, 2019
New feature
Azure Active Directory
New alert on potential stale accounts in a privileged directory role
Tuesday, January 1, 2019
New feature
Azure Active Directory
New PIM Weekly Digest Email
Monday, December 17, 2018
Hands-on: Privileged Identity Management

Privileged Identity Management (PIM)

Lower exposure of privileged accounts

- Process and requirements to activate roles
  - Limit risk time: Time-bound access to resources
  - Relation to change or incident: Approval and input text (Ticket number, activation reason)
  - Auditing and notifcation of privileged activities

Automation and integration of PIM

- PowerShell module and PIM App (PowerApps and Flow)

Notifications & eligible users

- Eligible users (such as Global Admins) not receiving notifcations

Privileged Identity Management (PIM)

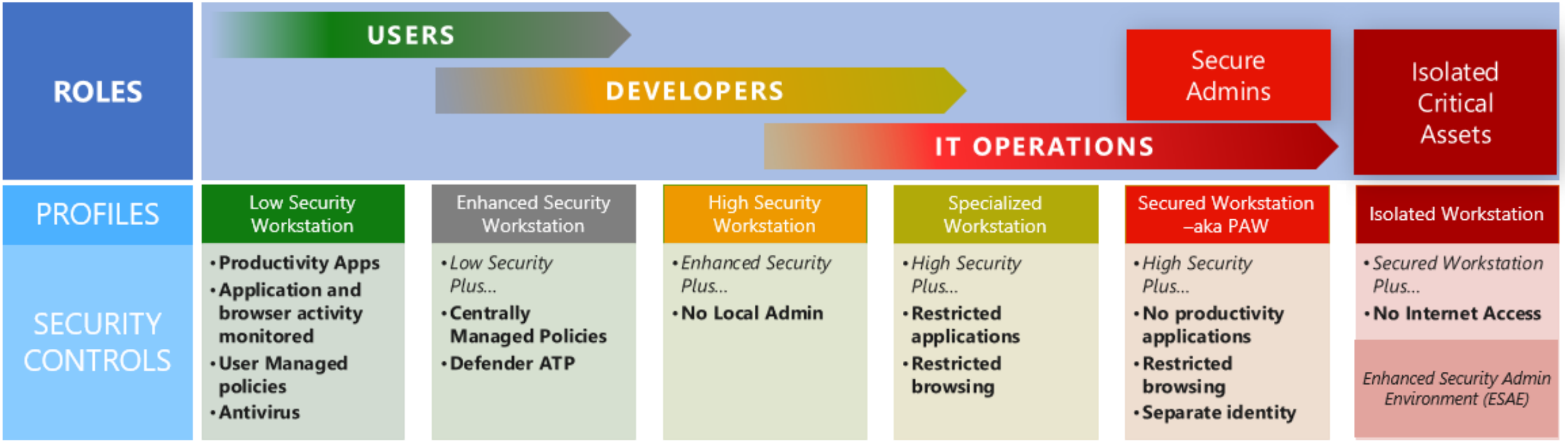
Access to Azure resources

- Browser (with different profiles)
  - Session token in various browser profiles
  - Accessible from loggedin user / no security by separate browser profiles
- RunAs (different users) or Jumpbox/Jumphost
  - Similiar to AD administration (back in the old days)
  - WHfB useable limited (→ only by „RunAs Administrator“)
  - Breach of „source-principal“ approach (“secure keyboard“)
- Privileged Admin Workstation (PAW)
  - Corporate PC as separated device or virtual machine (or WVD)
  - Isolated, hardenend and restricted usage of OS, apps and network

Privileged Identity Management (PIM)

Secure access to Azure (Roles and Security Levels)

- Understand secure, Azure-managed workstations

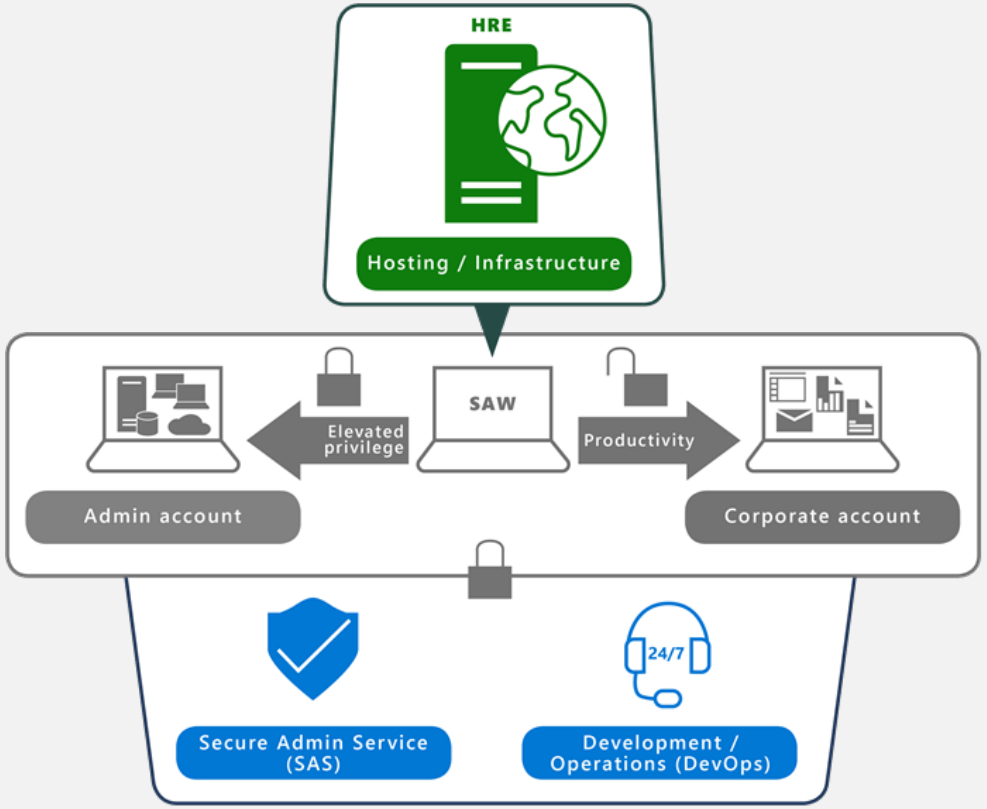


Source: https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-managed-workstation

Privileged Identity Management (PIM)

Secure access to Azure by Microsoft IT

- Secure Admin Workstation used for High Risk Environment at Microsoft



Microsoft's (IT) approach:

- Zero peristent admins
- 2FA and JIT
- Whitelisting and code integrity
- Password Vaulting
- Secure Supply Chain

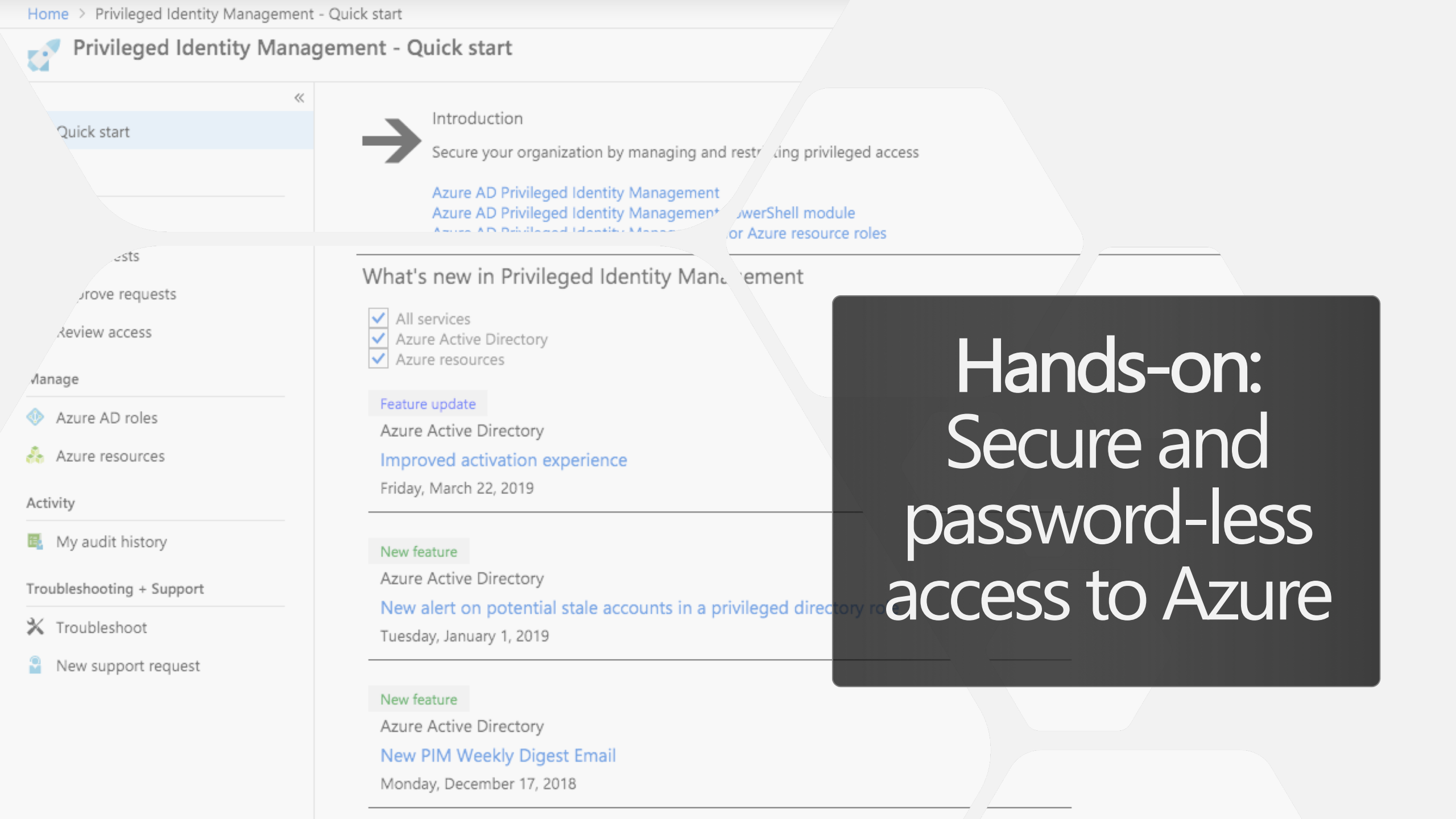
Source: https://www.microsoft.com/en-us/itshowcase/protecting-high-risk-environments-with-secure-admin-workstations
https://www.microsoft.com/en-us/itshowcase/improving-security-by-protecting-elevated-privilege-accounts-at-microsoft

Privileged Identity Management (PIM)

Secure access to Azure (Custom solution)

Hosting SAW VM

- **vShielded** and secured **Hyper-V VM**
- Secure Workstation configuration and policy baselines for Microsoft Intune and Windows 10 (latest build)
- Azure Portal „**Log me out when inactive**“ (Personal Setting or directory level timeout)
- **Reduced token life time and non-persistent session**
- **Reset of user profile** or VM (optional)
- Tenant restriction
- **URL auditing or blocking** to specified Azure resources (by Security Gateway or Broker solution)
- **Passwordless** authentication with Windows Hello- (or FIDO2-based) logon


Home > Privileged Identity Management - Quick start
Privileged Identity Management - Quick start
Quick start
Introduction
Secure your organization by managing and restr ging privileged access
Azure AD Privileged Identity Management
Azure AD Privileged Identity Managemen owerShell module
or Azure resource roles
sts
rove requests
eview access
Manage
Azure AD roles
Azure resources
Activity
My audit history
Troubleshooting + Support
Troubleshoot
New support request
What's new in Privileged Identity Mana ement
All services
Azure Active Directory
Azure resources
Feature update
Azure Active Directory
Improved activation experience
Friday, March 22, 2019
New feature
Azure Active Directory
New alert on potential stale accounts in a privileged directory ro
Tuesday, January 1, 2019
New feature
Azure Active Directory
New PIM Weekly Digest Email
Monday, December 17, 2018
Hands-on:
Secure and
password-less
access to Azure

Privileged Identity Management (PIM)
Lateral Movement

Discovery of Lateral Movement Paths (LMPs)

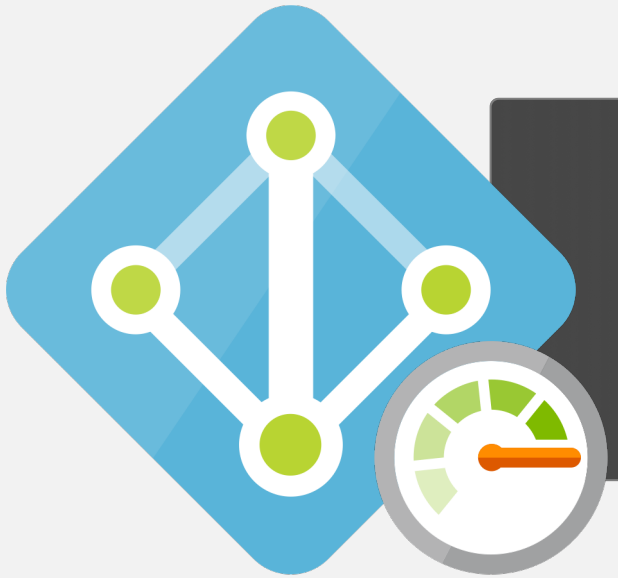
- Using Azure ATP to discover and analyze LMPs

Reduce attack surface of lateral movement

- Avoid usage of "Device administrator" or “Global administrator” for local helpdesk and troubleshooting

Management of (unique) local admin accounts of Azure AD clients

- Missing LAPS support or „Modern Management“-solution by Microsoft
- Custom or 3rd Party solutions:
  - Local Administrator Password Solution and RealmJoin (by Glueck & Kanja)
  - Serverless LAPS solution (Intune, Azure Functions and KeyVault) by John Seerden



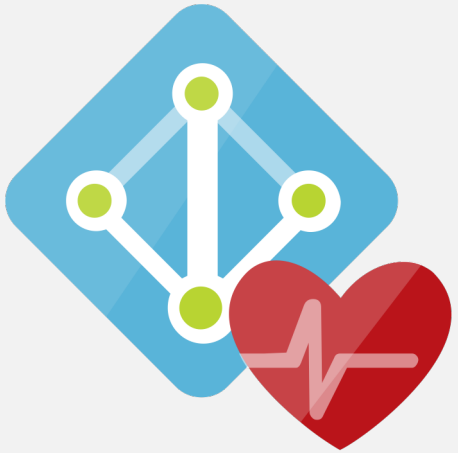
Auditing and Monitoring of Azure Active Directory

Auditing and Monitoring of Azure Active Directory

Azure Active Directory Connect Health

- Monitor your on-premises hybrid and synchronization services in Azure

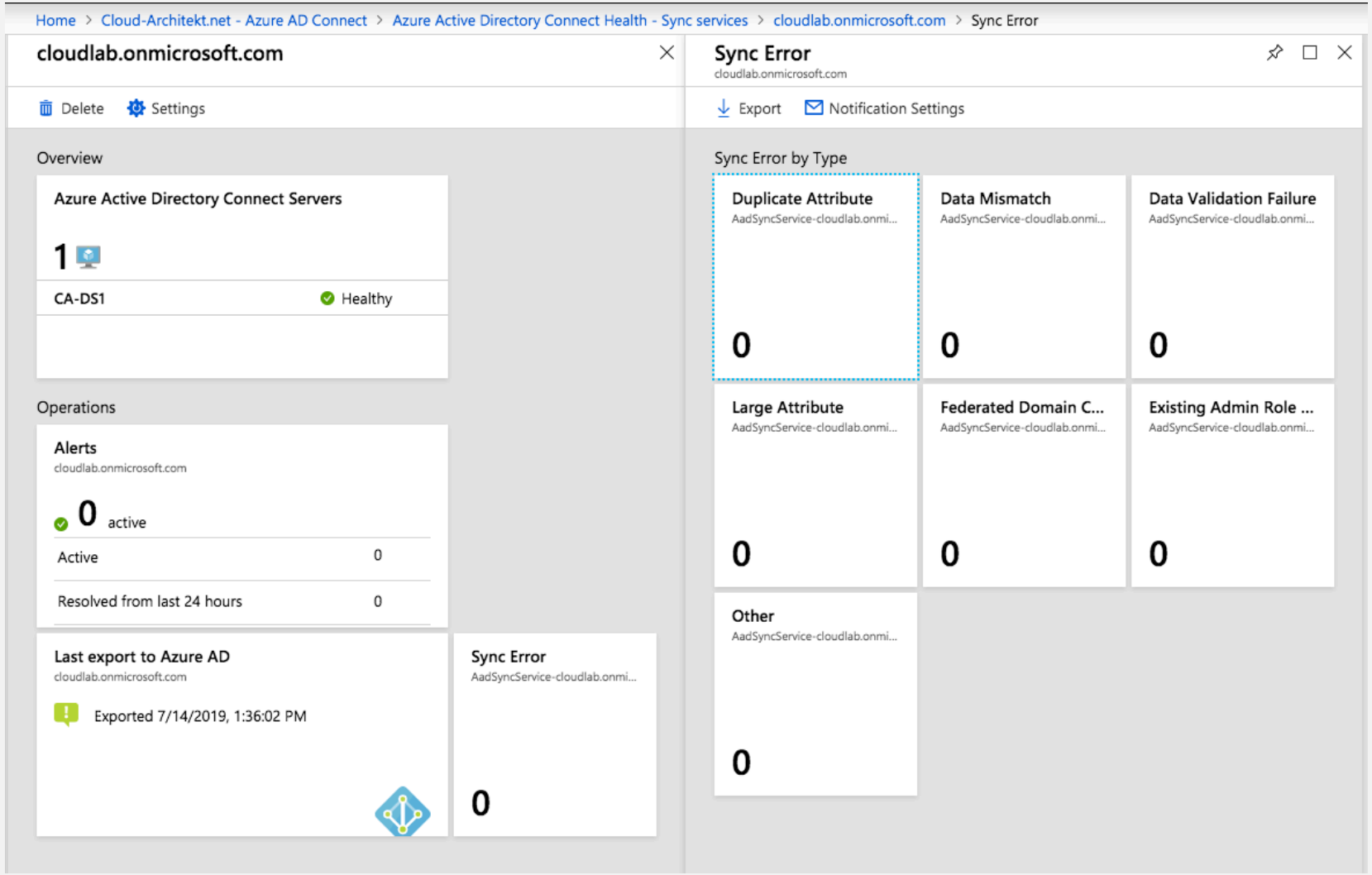
- **AAD Connect Health Agent must be configured on each targeted server:**
  - Outbound connectivity and disabled SSL inspection
  - Required to install „Health Agent for (AD DS) Domain Controllers“
  - Consideration: Azure AD Connect Health can not be configured on Server Core!



Source: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install

Auditing and Monitoring of Azure Active Directory

Azure Active Directory Connect Health



Auditing and Monitoring of Azure Active Directory

Service Health of Azure AD services

- **Create service health alerts**
  - Azure Active Directory
  - Multi-Factor Authentication
- **Status history & Root Cause Analysis (RCAs)**
  - Service outage history of the past 90 days only
- **What happens when Azure AD-related services fails?**
  - MFA major outtage in the past (November 2018, February 2019)
- Twitter @AzureSupport

Source: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install

Auditing and Monitoring of Azure Active Directory

Monitor your tenant-wide settings and app registration

- **Azure Identity Secure Score** (via Security Graph API)

- **MFA Authentication methode usage** (via Graph API)

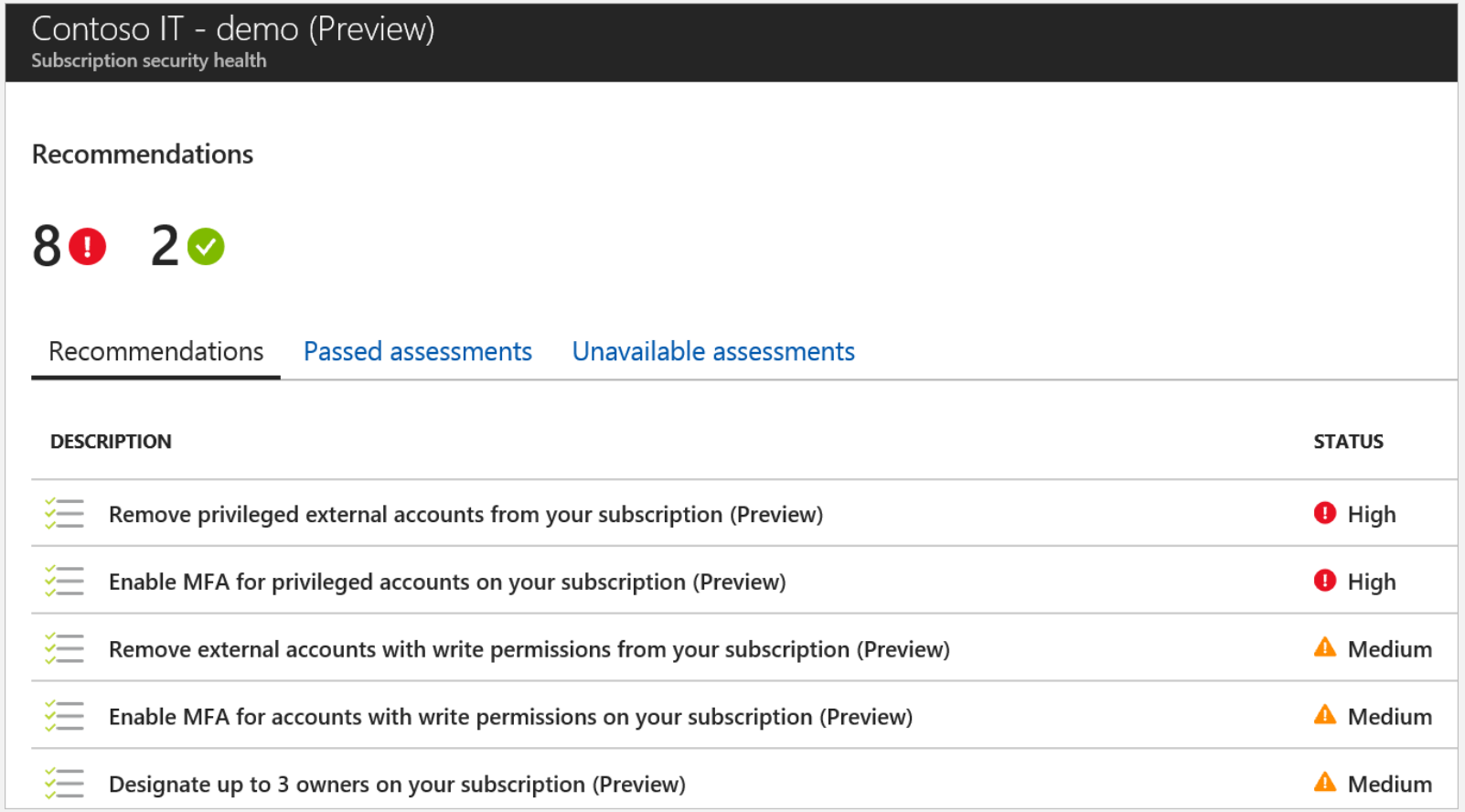
- **Assessment of application configuration**
  - Expired client secret of registered applications (AzureADAssessment)
  - OAuth2 admin and app consent delegation
    → Advanced lists of delegated and application permissions
    → Permission level, security breach and compliance reports with MCAS

Source: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install

Auditing and Monitoring of Azure Active Directory

Monitor IAM of Azure subscriptions and resources

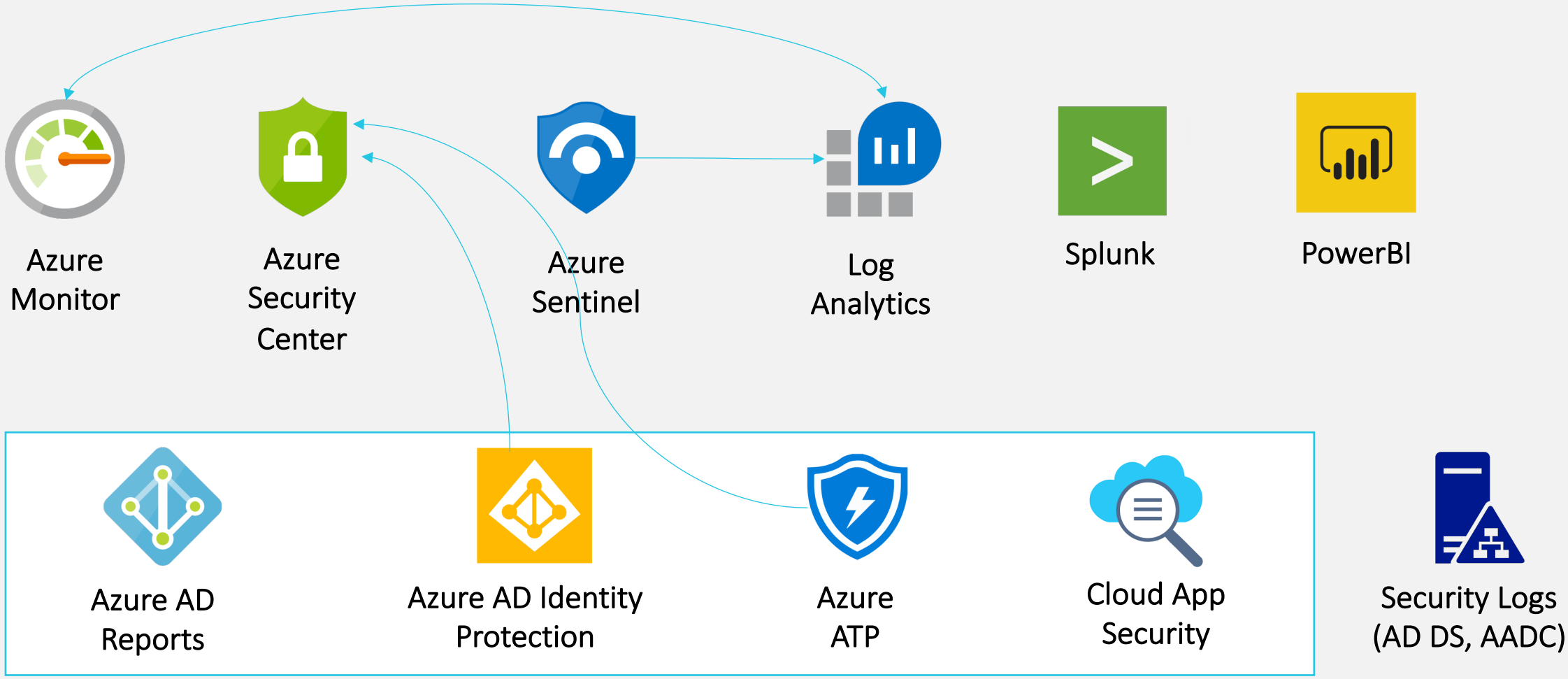
- Identity & Access recommendations in „Azure Security Center“



Source: https://docs.microsoft.com/de-de/azure/security-center/security-center-identity-access

Auditing and Monitoring of Azure Active Directory

Monitoring and Security solutions



Auditing and Monitoring of Azure Active Directory

Security events to take care on…

Microsoft‘s „Best practice“: Have a method to identify:

- ✓ *Attempts to sign in without being traced*
- ✓ *Brute force attacks against a particular account (high count of failed MFA challenges)*
- ✓ *Attempts to sign in from unfimiliar or multiple locations*
- ✓ *Sign-ins from infected devices or suspicious IP addresses*

Further examples of suspicious activies:

- *Modification of CA policies (and assigned security groups)*
- *Sign-ins of emergency accounts*
- *Modification of Directory roles (alerting covered by Azure AD PIM)*
- *Create service principals, modified app registration or admin/user consent*
- *Succesful authentication without the use of MFA or legacy authentication*
- *External forwarding or sharing of Exchange mailboxes*

Source: https://docs.microsoft.com/en-us/azure/security/azure-security-identity-management-best-practices

Auditing and Monitoring of Azure Active Directory

Activity Reports in Azure Active Directory

Sign-in Logs

- User sign-in to application with Success/Failure
- Details of client, MFA and session conditions

Audit Logs

- Activities to perform change of objects and resources in Core Directory and AAD-related components e.g. Conditional Access Policies, PIM,…
- Including self service activities by end-users

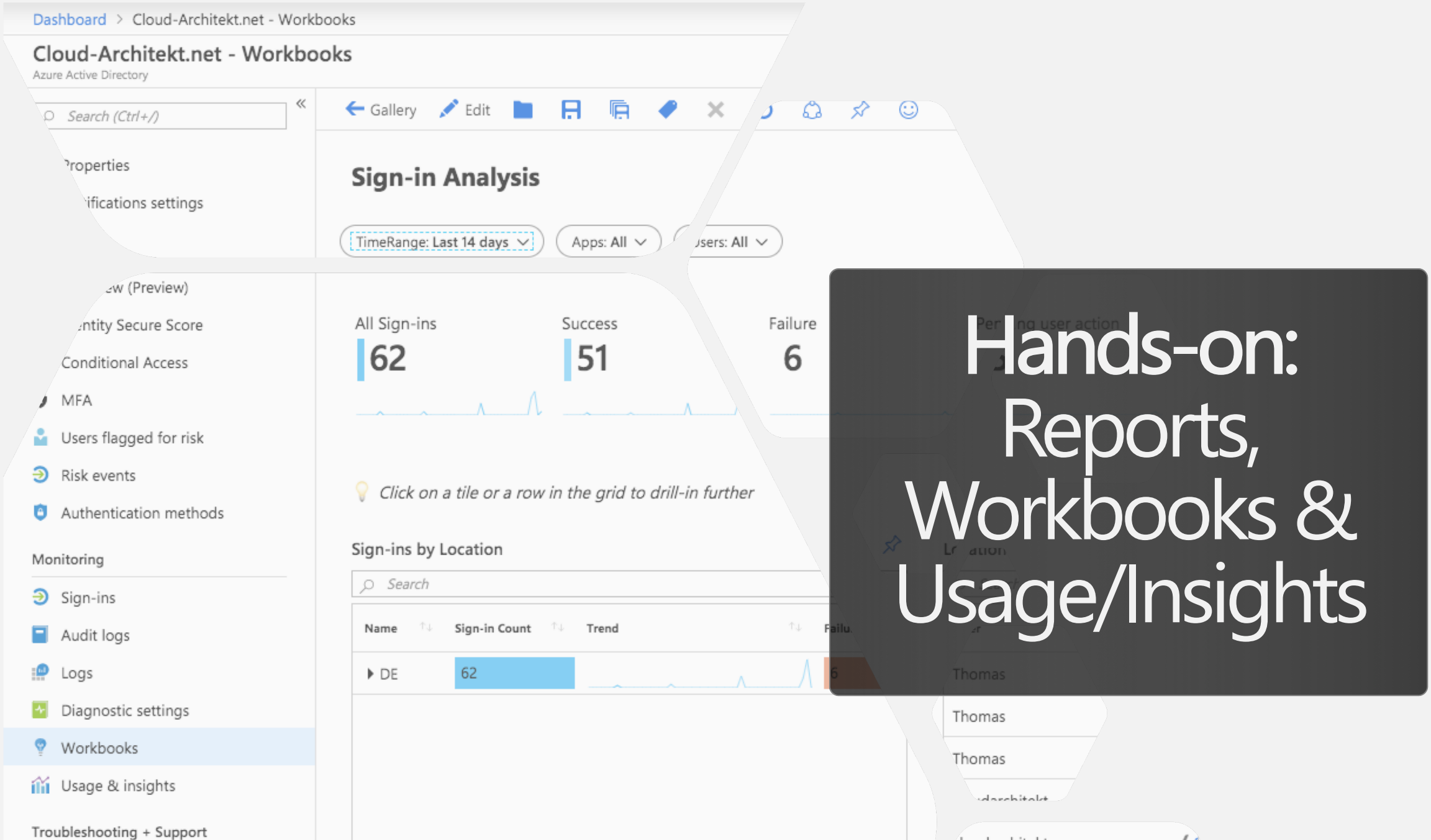
Security Logs

- Users flagged for risk, Risk events, Vulnerability

Usage and insights

- Reports of top used applications and top sign-in errors

Source: https://docs.microsoft.com/bs-latn-ba/azure/active-directory/reports-monitoring


Dashboard > Cloud-Architekt.net - Workbooks
Cloud-Architekt.net - Workbooks
Azure Active Directory
Search (Ctrl+/)
Properties
Gallery
Edit
Sign-in Analysis
TimeRange: Last 14 days
Apps: All
All Sign-ins
62
Success
51
Failure
6
Click on a tile or a row in the grid to drill-in further
Sign-ins by Location
Search
Name
Sign-in Count
Trend
DE
62
Conditional Access
MFA
Users flagged for risk
Risk events
Authentication methods
Monitoring
Sign-ins
Audit logs
Logs
Diagnostic settings
Workbooks
Usage & insights
Troubleshooting + Support
Thomas
Thomas
Thomas
Hands-on: Reports, Workbooks & Usage/Insights

Auditing and Monitoring of Azure Active Directory

Activity and security log considerations

- Name in reports are based on the object name at the time of the event/sign-in
- Only initial authentication is in the report (refresh token)
- Service principals are not covered by sign-in logs
- Non-Global Admins can access logs
  - Security Administrator & Reader
  - Reports Reader and Application Administrator
  - Global Reader ☺

Auditing and Monitoring of Azure Active Directory

Reporting latency and retention policies

Activity / Security Reports	Azure AD Free/Basic	Azure AD Premium P1/P2	Latency (Average)	Latency (Min-Max)
Audit logs	7 days	30 days	2-5 min.	15-60 min.
Sign-ins	N/A	30 days	2-5 min.	15-120 min.
Users at Risk	7 days	30 days (P2: 90 days)	15 min.	5-120 min.
Risky sign-ins	7 days	30 days (P2: 90 days)	15 min.	5-120 min.

→ Retain the **audit and sign-in activity data (based on your requirmenets)**

Source: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-latencies

Auditing and Monitoring of Azure Active Directory

Diagnostic Settings / Export Audit and Sign-In data

Archieve to a storage account

Retain the data for a long time, Retention policy (in days)

Stream to an event hub

Connecting 3rd party (SIEM) solutions, custom apps or automation/workflows

Send to Log Analytics

Advanced analytics, alerting and queries (by Kusto)

Consideration: Beware of the pipeline-process time from source to target resource by routing. Additional latency e.g. by storing data to Blob Storage, Event Hub or Log Analytics workspace.

Source: https://azure.microsoft.com/de-de/blog/azure-monitor-aad-activity-logs-using-diagnostic-settings/

Auditing and Monitoring of Azure Active Directory

Support of 3rd Party SIEM solutions

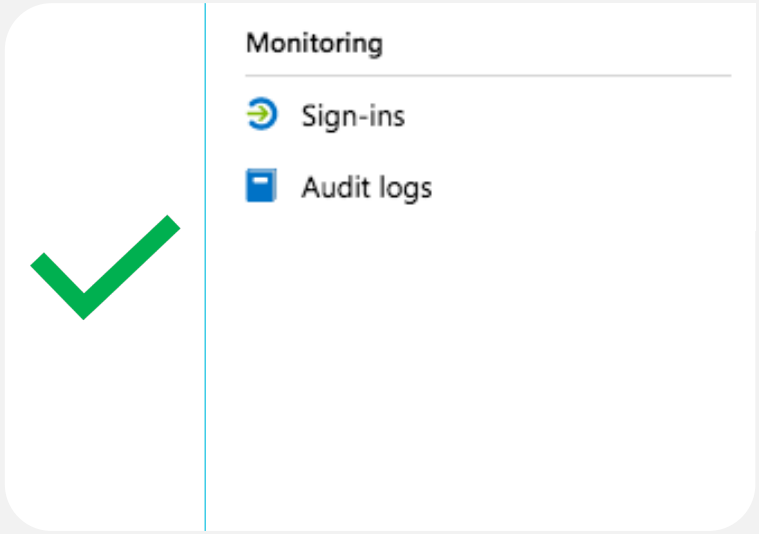
- Option 1: Microsoft Graph API and own scripts
  - Prerequiste: Call Graph API to access the data
    push it into the SIEM system using your own scripts

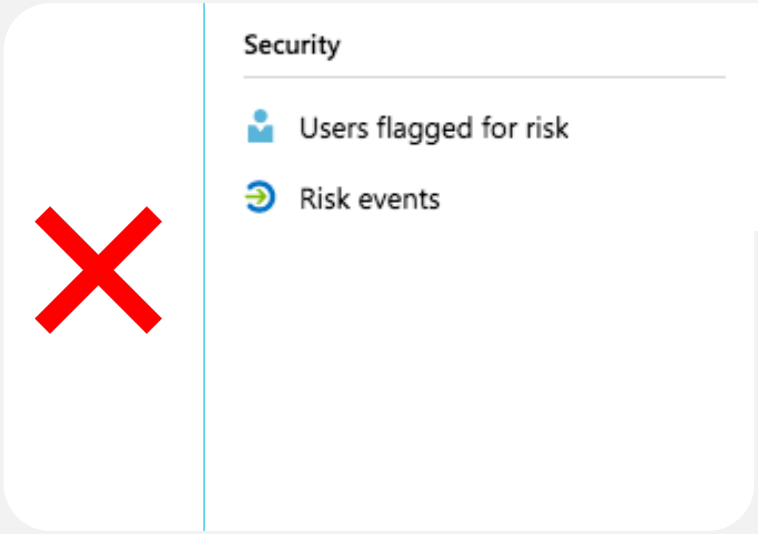
- Option 2: Azure Monitor and EventHub-Integration
  - Prerequiste: Azure Monitor to stream via EventHubs,
    configure SIEM connectors to source
    - Supported connectors by Splunk, QRader and Sumo (seamless integration)
    - Azure Function to foward Azure Monitor to Syslog
    - Event Hub Plug-in for ELK

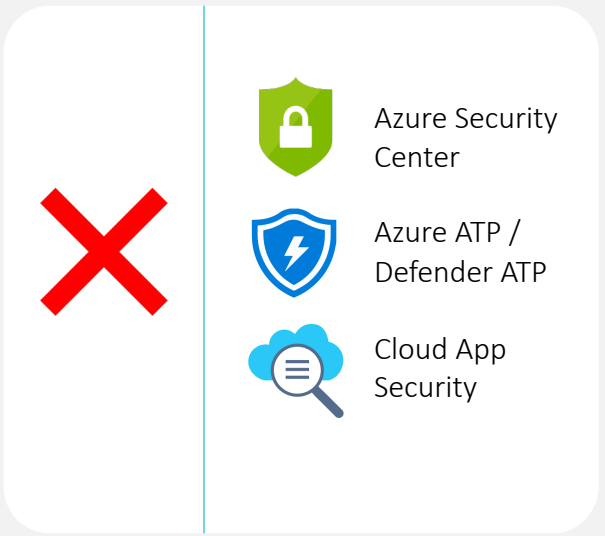
- Deprecated: AAD Log Integration tool

Auditing and Monitoring of Azure Active Directory

Checklist: Collect all Identity-related security logs to SIEM







Auditing and Monitoring of Azure Active Directory

Collecting Microsoft Security Graph API alerts with a SIEM

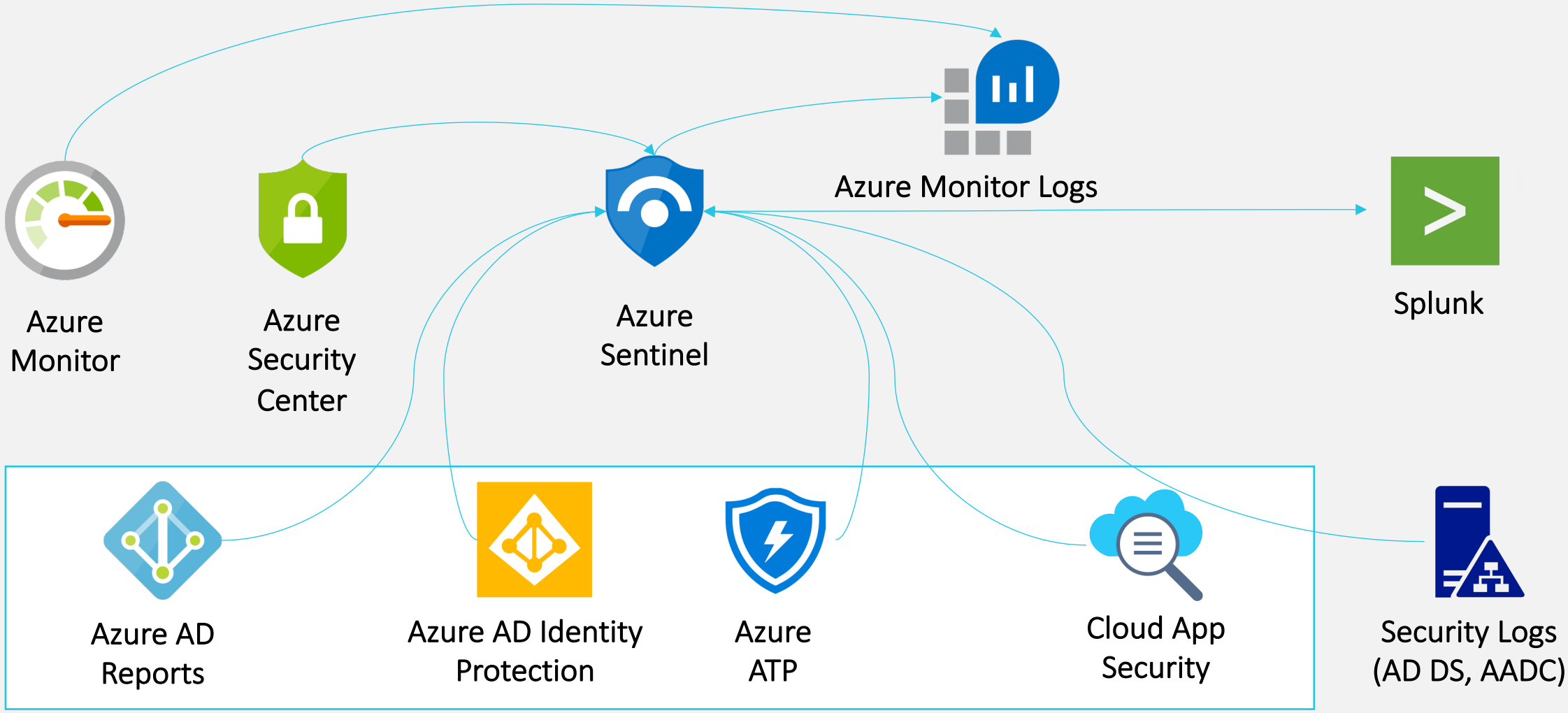
- Alerts from the following security providers are available via SIEM integration:
  - Azure Security Center
  - Azure Active Directory Identity Protection
  - Microsoft Cloud App Security
  - Azure Information Protection *(preview)*
  - Azure Advanced Threat Protection *(preview)*
  - Azure Sentinel *(preview)*

- Supported API Integration is currently available for Splunk and Qradar

- Graph Security API and Connectors to LogicApps, Flow and PowerApps

Auditing and Monitoring of Azure Active Directory

Monitoring and Security solutions



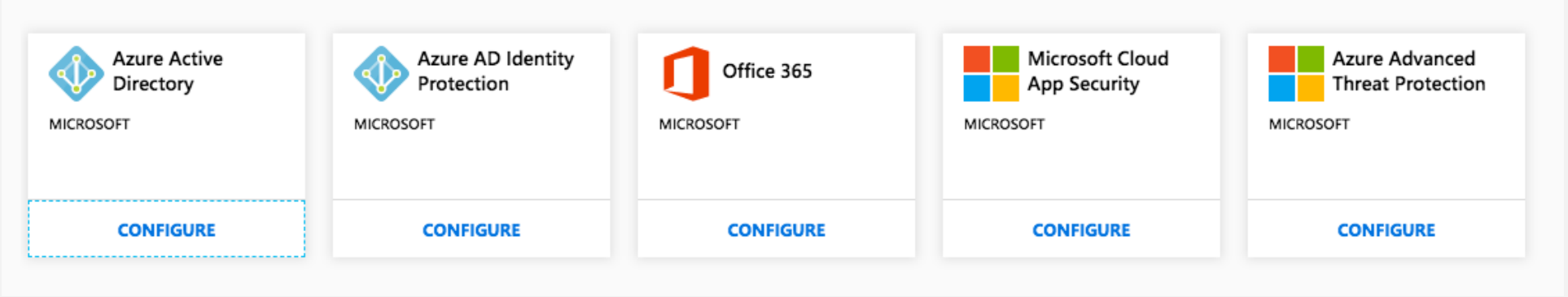
Auditing and Monitoring of Azure Active Directory

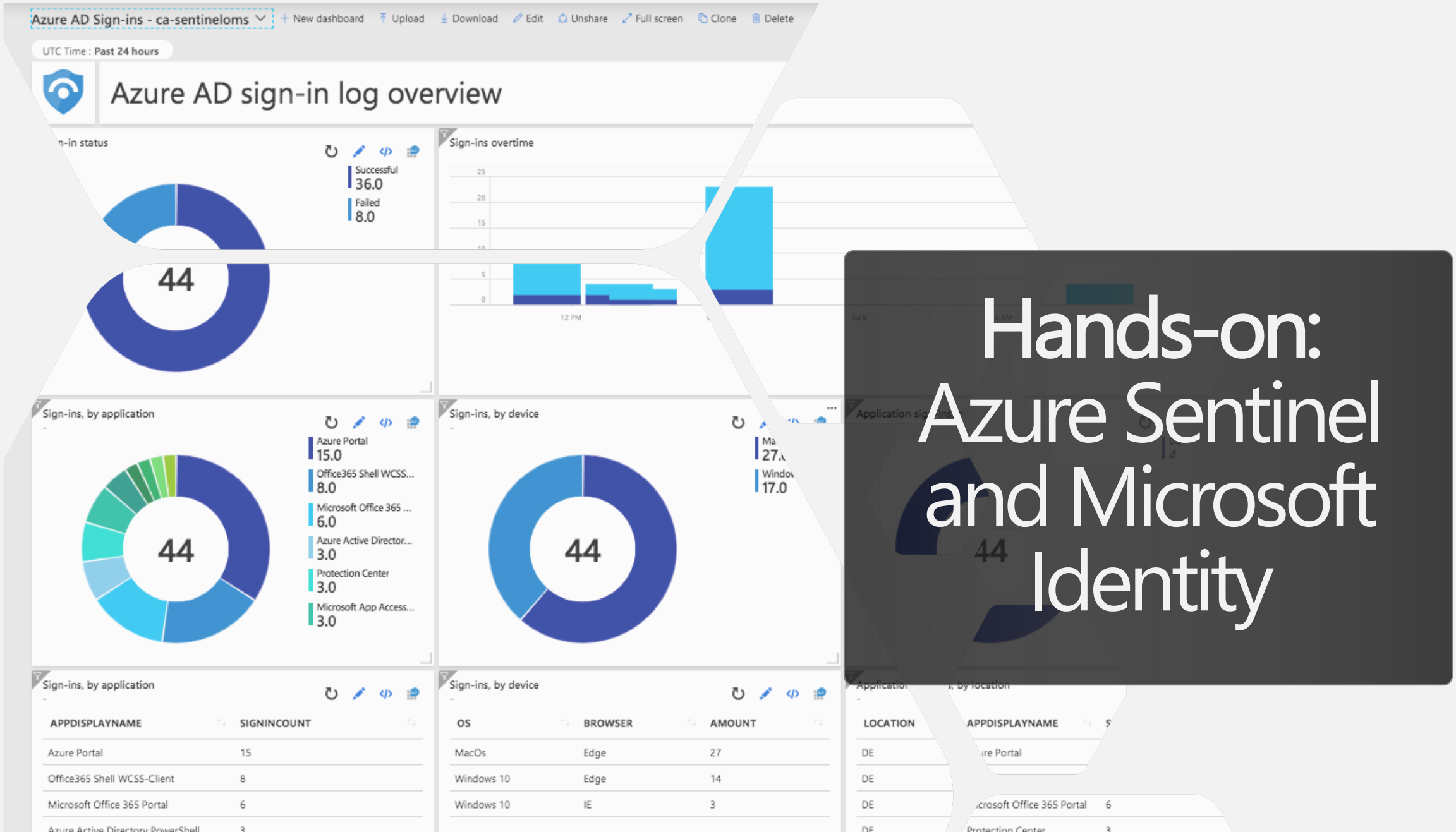
Azure Sentinel

- Advanced analytics, dashboards and huntings with Microsoft‘s Cloud „SIEM“ solution

- Build on Log Analytics Workspaces, Logic Apps,…
  - Create custom playbooks (e.g. Threat responding)

- Native „data connectors“ to gain insights and loggings

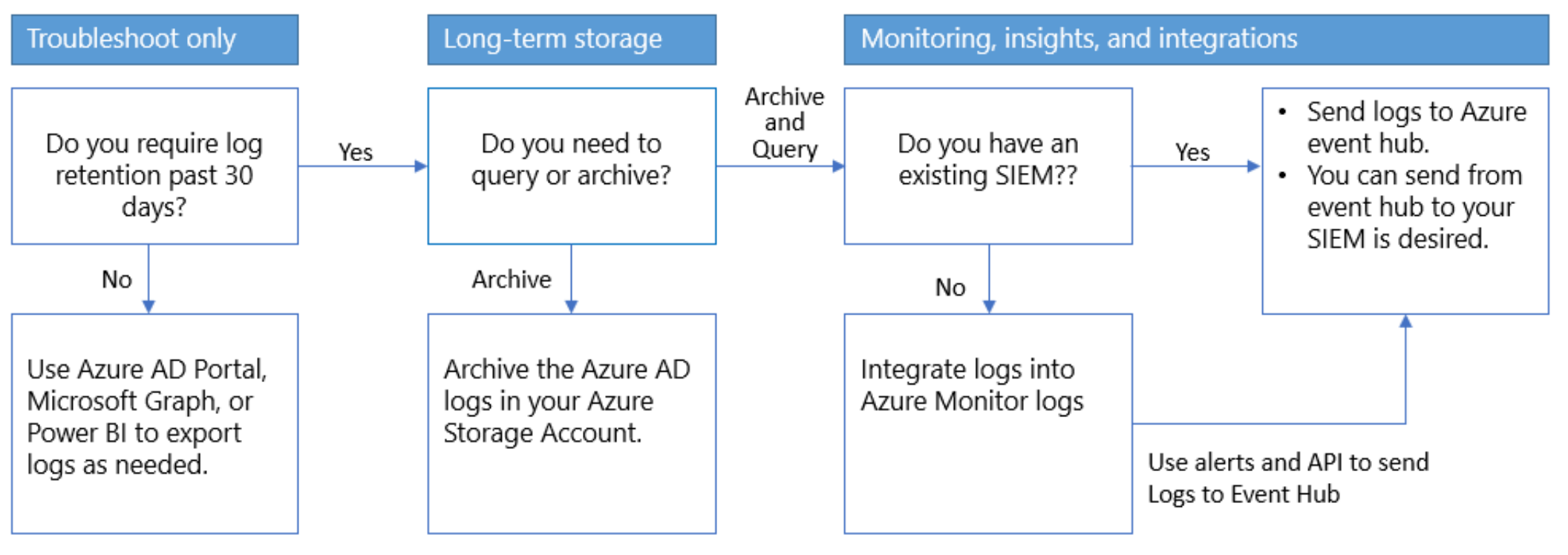



Azure AD Sign-ins - ca-sentineloms
New dashboard
Upload
Download
Edit
Unshare
Full screen
Clone
Delete
UTC Time : Past 24 hours
Azure AD sign-in log overview
Sign-ins overtime
Successful
36.0
Failed
8.0
44
Sign-ins, by application
Azure Portal
15.0
Office365 Shell WCSS...
8.0
Microsoft Office 365 ...
6.0
Azure Active Director...
3.0
Protection Center
3.0
Microsoft App Access...
3.0
Sign-ins, by device
17.0
APPDISPLAYNAME
SIGNINCOUNT
Azure Portal
15
Office365 Shell WCSS-Client
8
Microsoft Office 365 Portal
6
OS
BROWSER
AMOUNT
MacOs
Edge
27
Windows 10
Edge
14
Windows 10
IE
3
LOCATION
APPDISPLAYNAME
DE
DE
DE
6
Hands-on:
Azure Sentinel
and Microsoft
Identity

Auditing and Monitoring of Azure Active Directory

Choose a monitoring solution architecture

- Plan an Azure Active Directory reporting and monitoring deployment



Source: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/plan-monitoring-and-reporting

Thank You

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net