Get start with Identity Governance: Azure

Marius A. Skovli

Spirhed | marius.skovli@spirhed.com

MVP Dagen

Marius A. Skovli

Spirhed

Principal Consultant &
Microsoft MVP: Enterprise Mobility

marius.skovli@spirhed.com

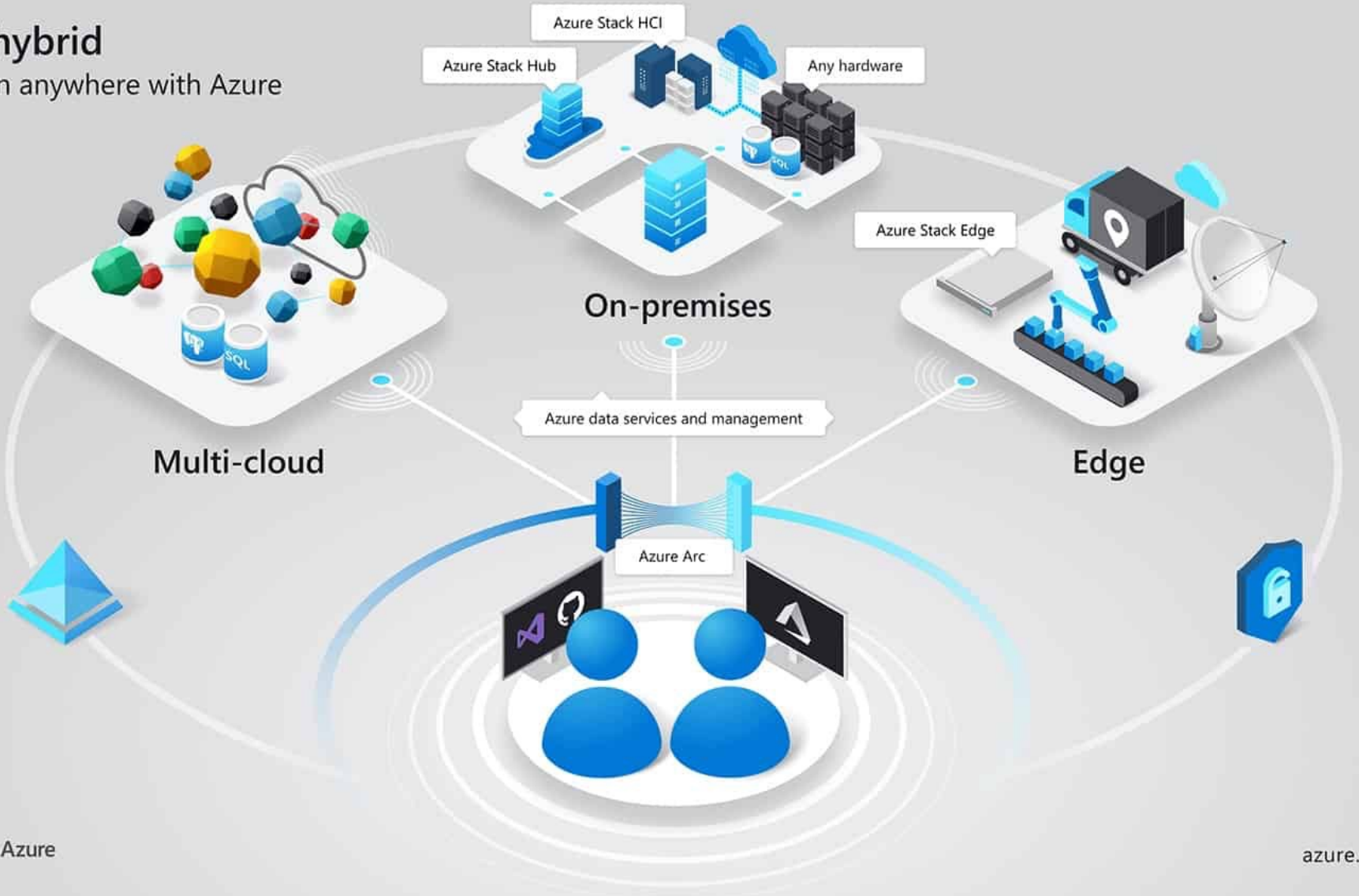
@MariusSkovli

MVP Microsoft Most Valuable Professional

Identity Governance enables security administrators to efficiently manage user identities and access across the enterprise

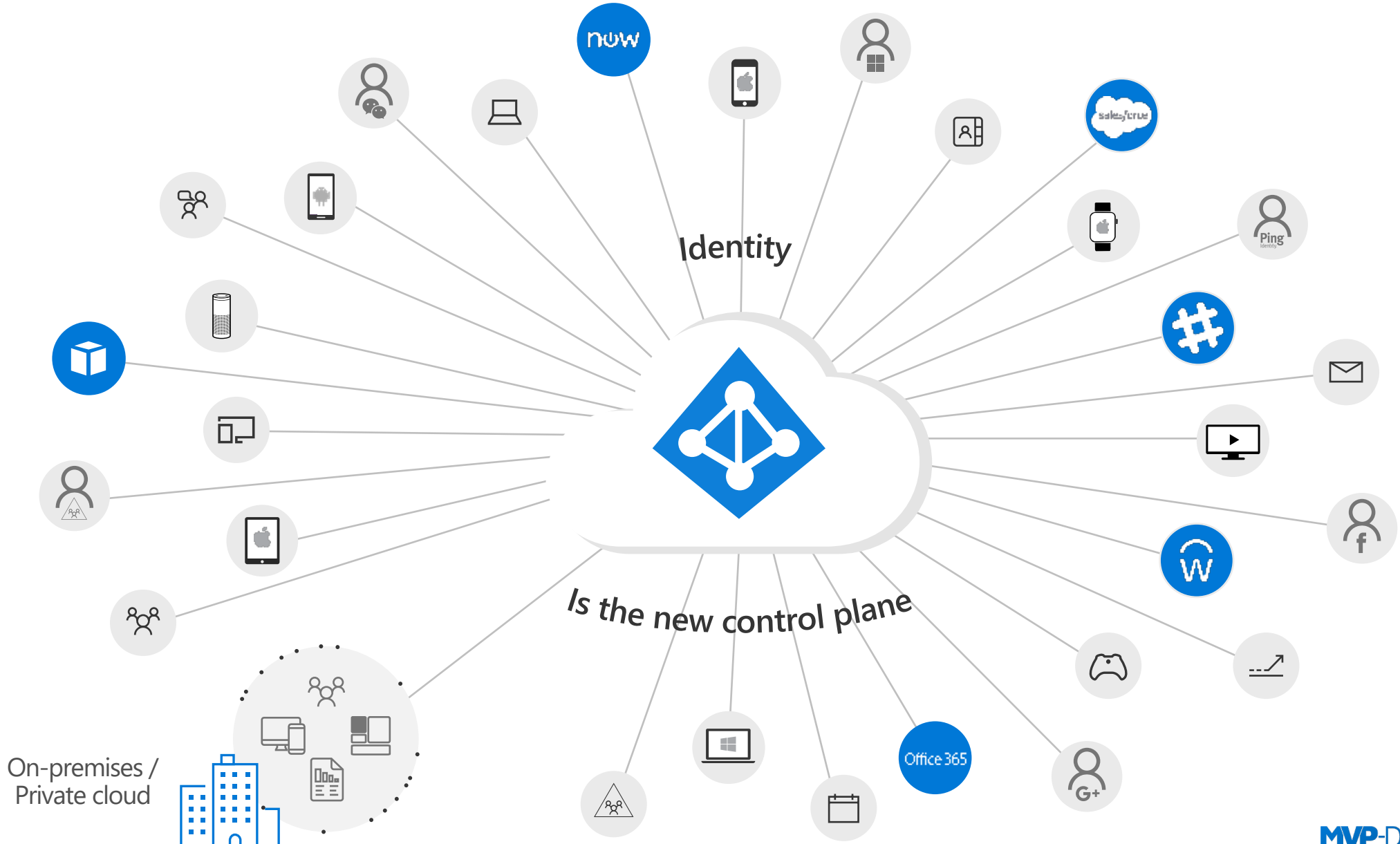
Azure hybrid

Innovation anywhere with Azure



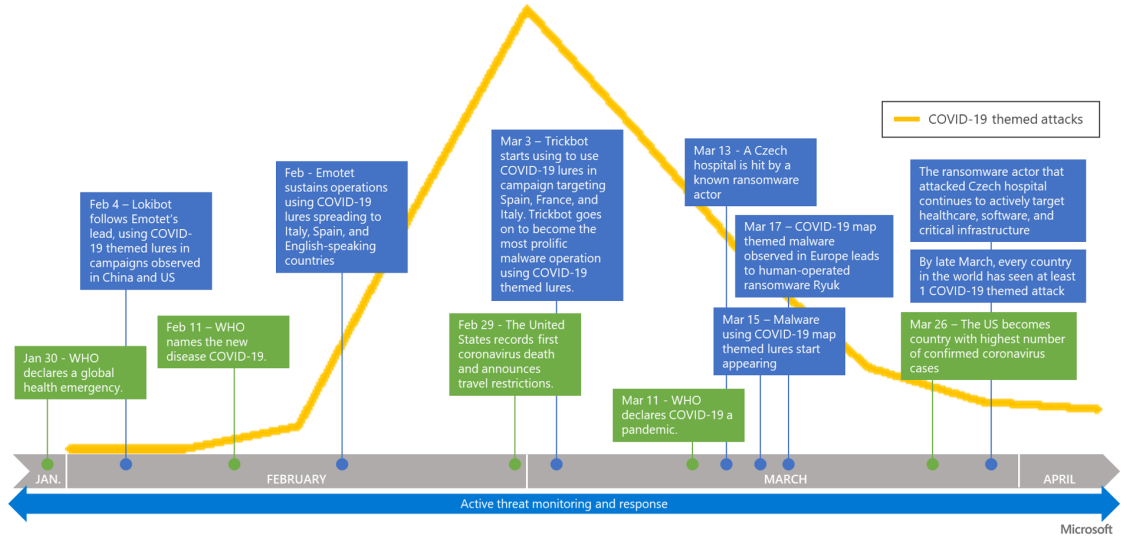
Microsoft Azure

azure.com/hybrid


Identity
Is the new control plane
On-premises /
Private cloud
Office 365
Ping

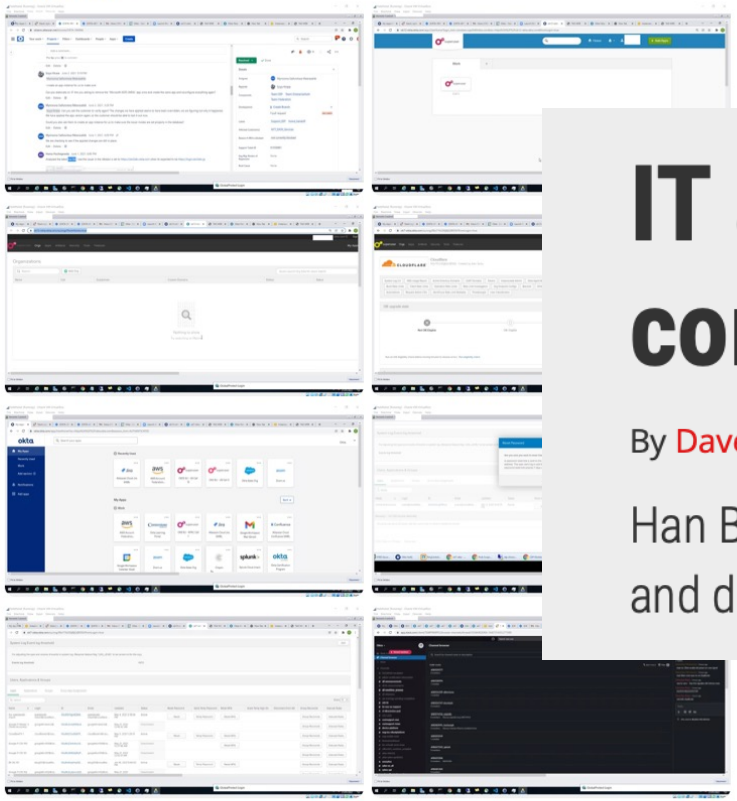
Threat landscape and trends (short)

- Cybercrime has increased by +600% due to the COVID-19 pandemic
- Shutdowns have permanently changed the way we run a business
- Patch Management has become a top priority for C-level
- Ransomware continues to be the number one threat
- Two-factor authentication no longer holds - multi-factor MFA authentication will continue to evolve
- We continue to be exploited when we are at our most vulnerable



MVP-Dagen

LAPSUS$



Just some photos from our access to Okta.c
Admin and various other systems.

For a service that powers authentication sys
of the largest corporations (and FEDRAMP a
think these security measures are pretty poo

(yes we know the URL has a email address. t
suspended - we dont care)

BEFORE PEOPLE START ASKING: WE DID NOT ACCESS/ STEAL ANY DATABASES FROM OKTA - our focus was ONLY on okta customers.

😏

IT admin gets 7 years for wiping his company's servers to prove a point

By Dave James published May 16, 2022

Han Bing allegedly felt undervalued after his security warnings were ignored, and decided to prove his point by trashing four financial servers.

Privileged Access Users Are a Target for Cybercriminals

Those who hold the key to data are prime targets. Cybercriminals will focus on certain roles and groups within an organisation to take advantage of their access rights. If a cybercriminal can get hold of those access rights, they can move around an organisation, entering sensitive areas of a network, undetected.

Who is accessing? What is their role?
Is the account compromised?

Where is the user based? From where is the user signing in? Is the IP anonymous?

Which app is being accessed?
What is the business impact?

Is the device healthy? Is it managed?
What is its exposure and attack surface?

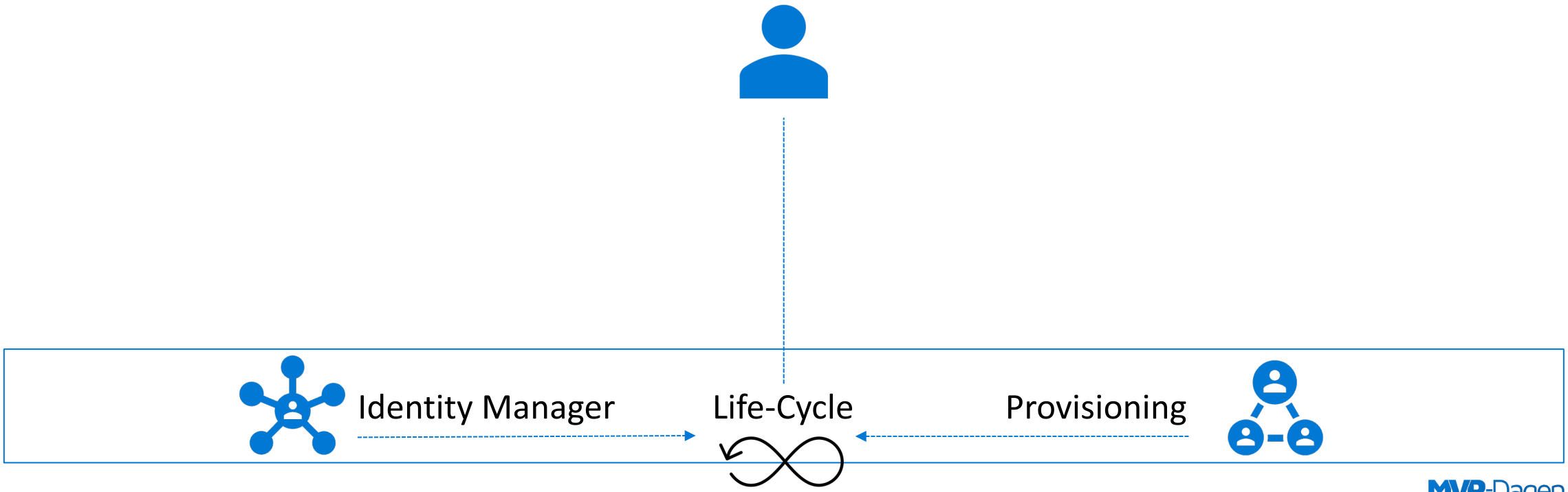
What data is being accessed?
Is it classified? Is it allowed off premises?

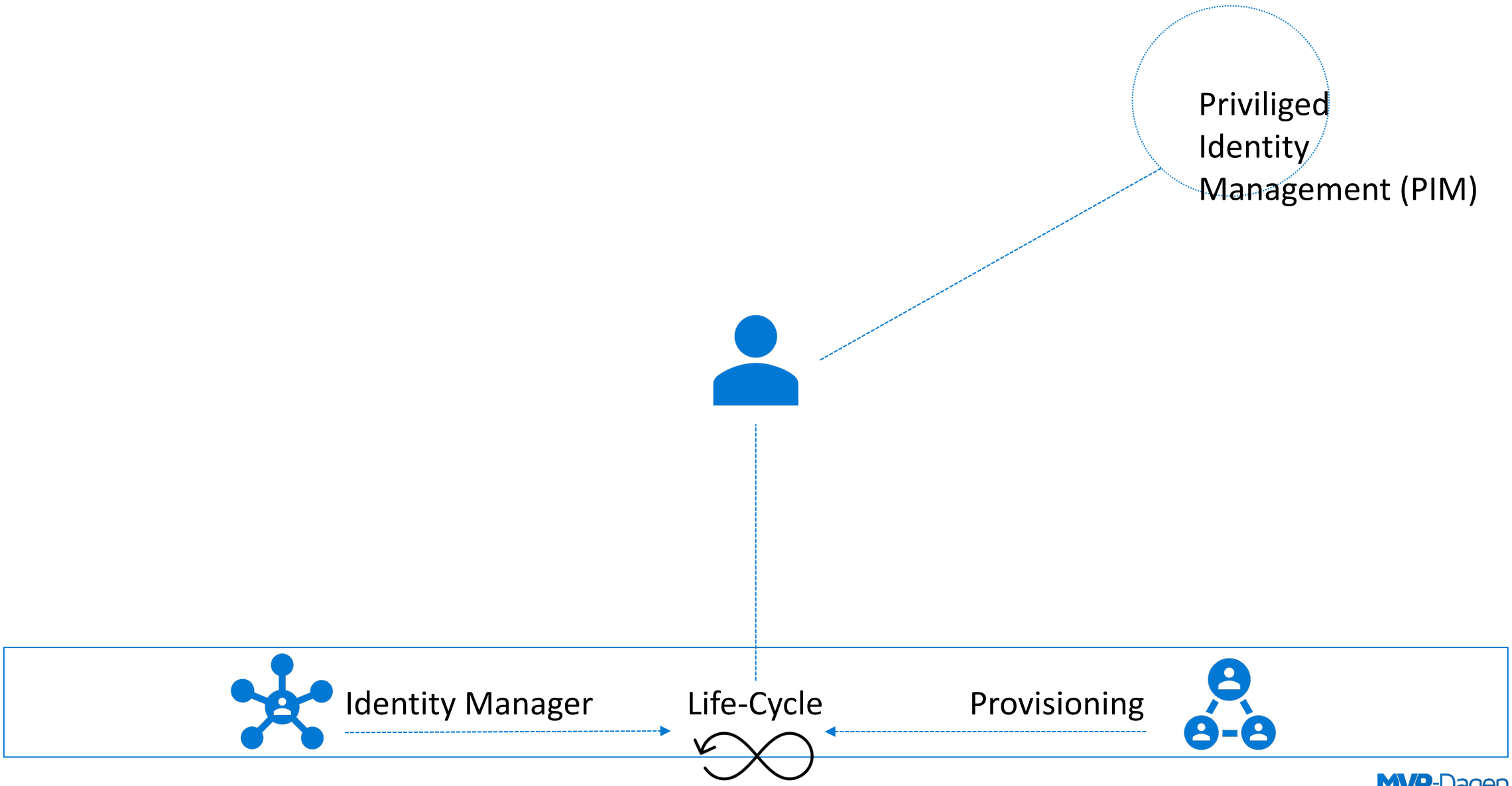
Oversight of Inactive identities and super identities?

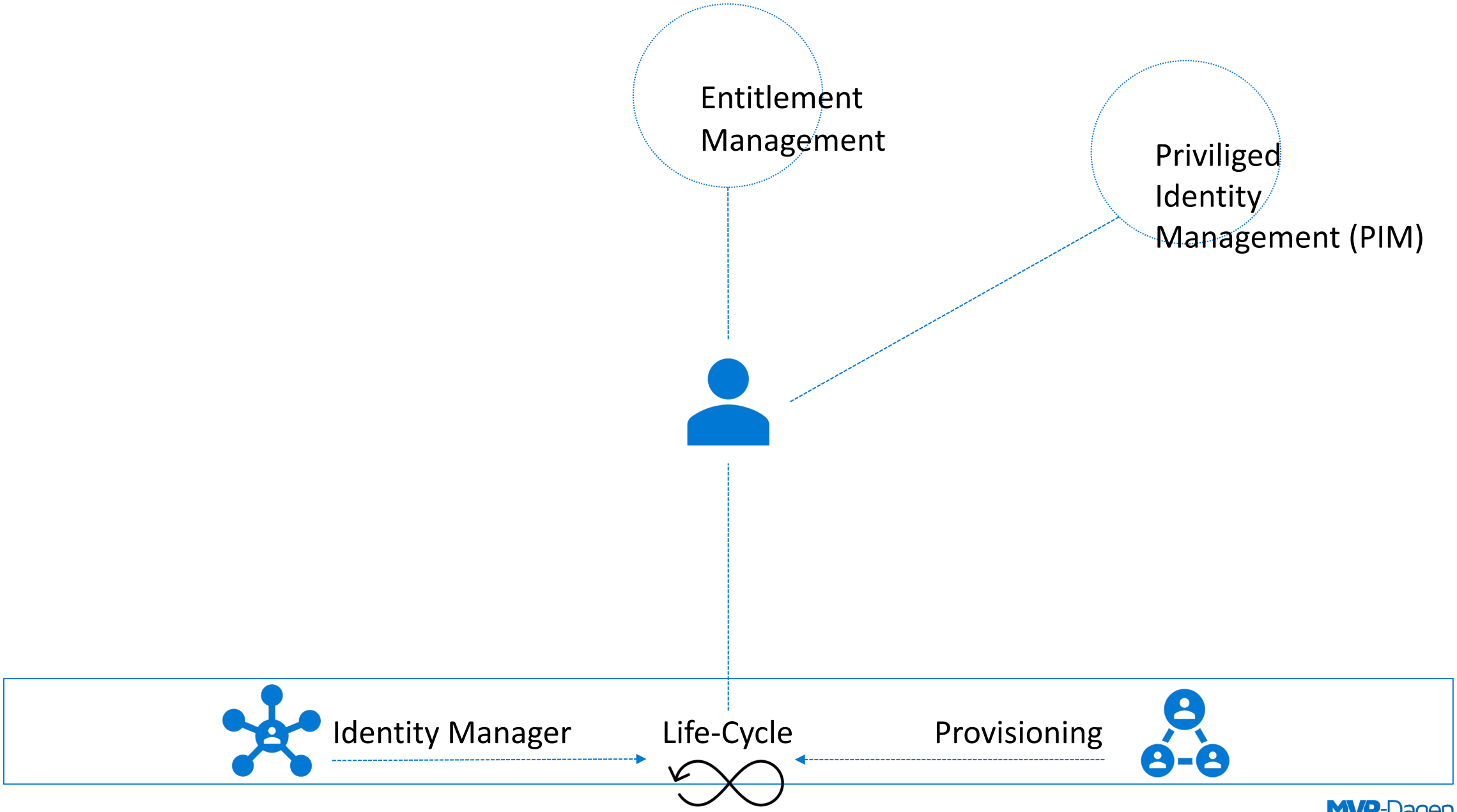
Identified Overpermissioned active identities?

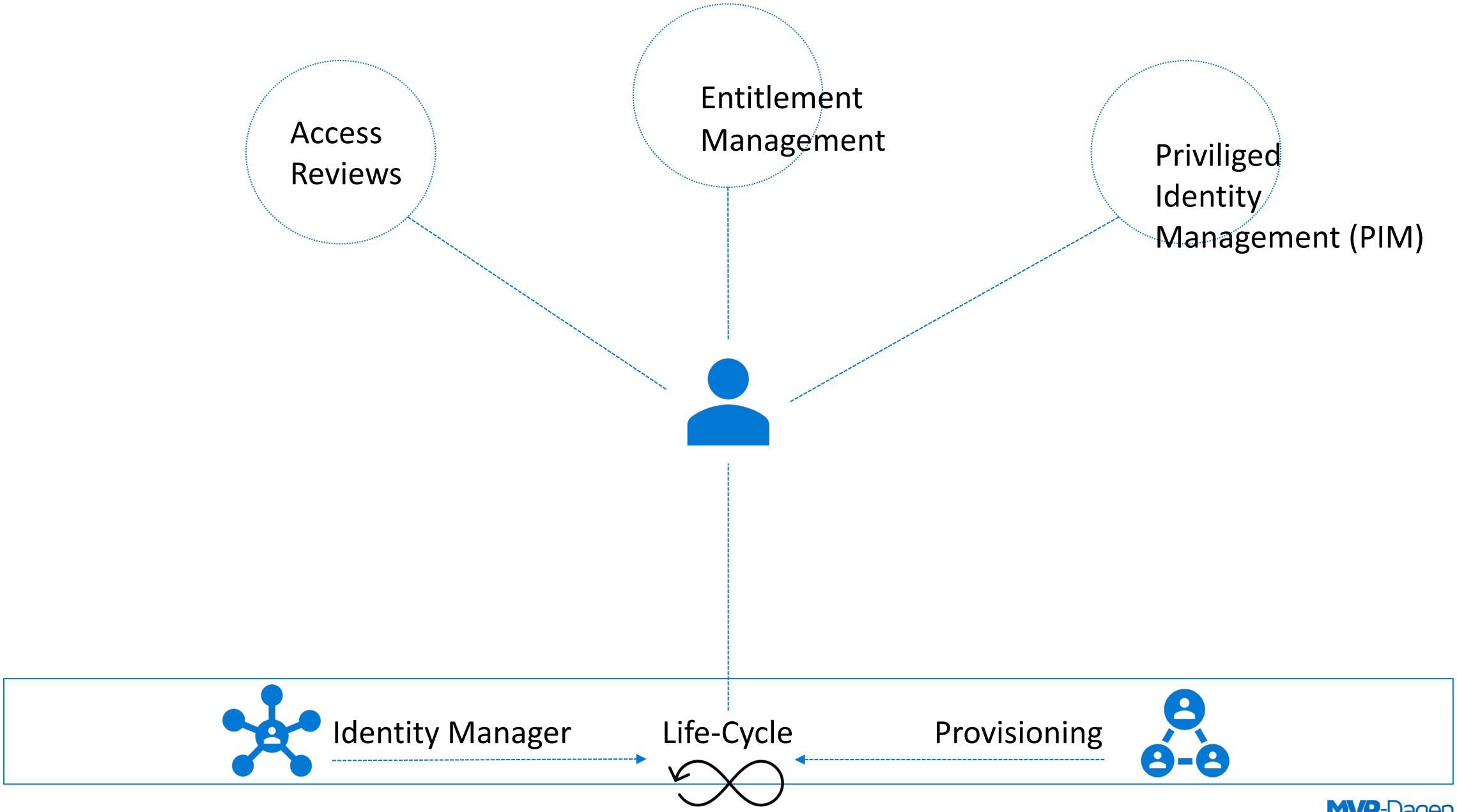
Are you able to visualize Cross-account access?

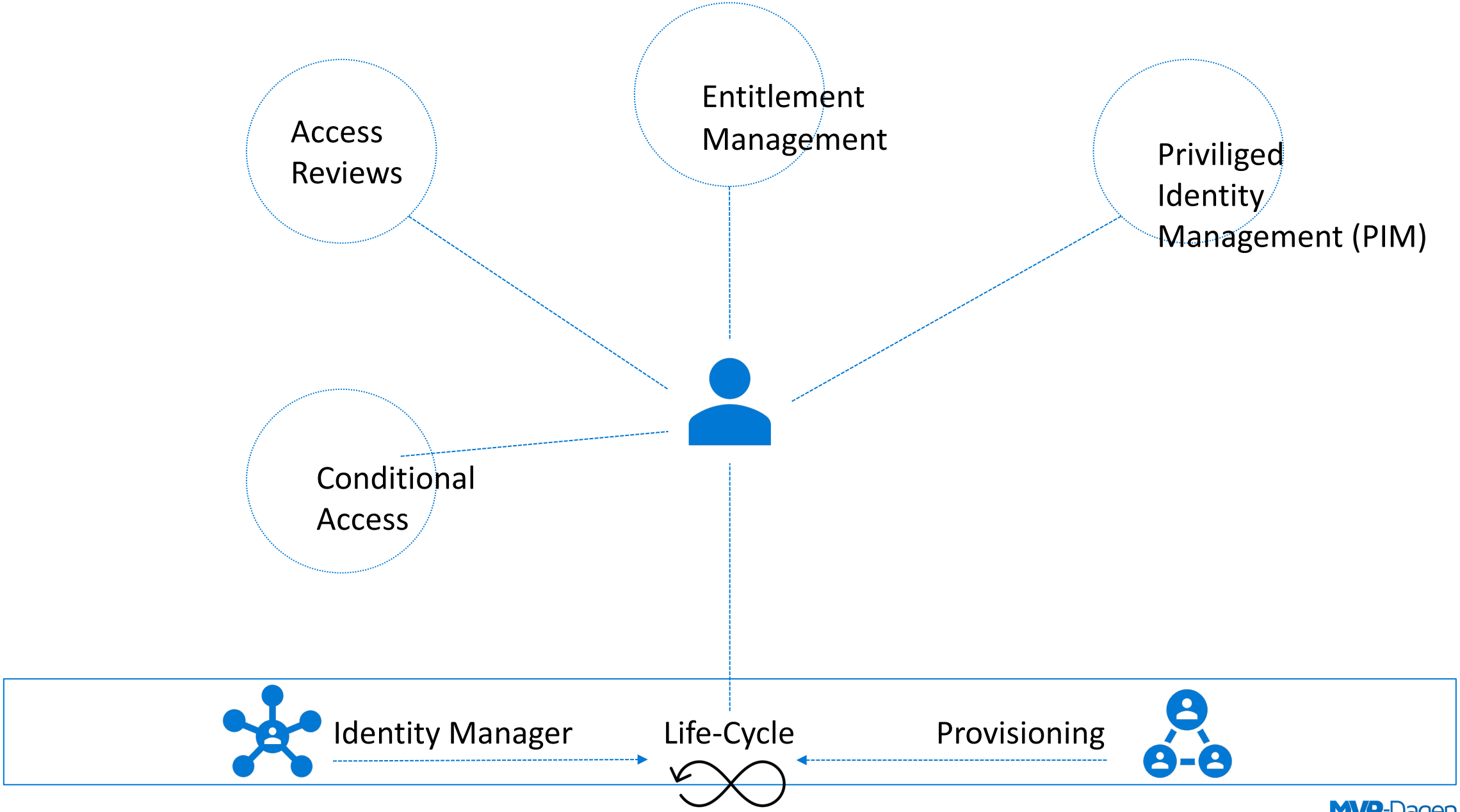
How do you detect anomalous behavior among workload identities?

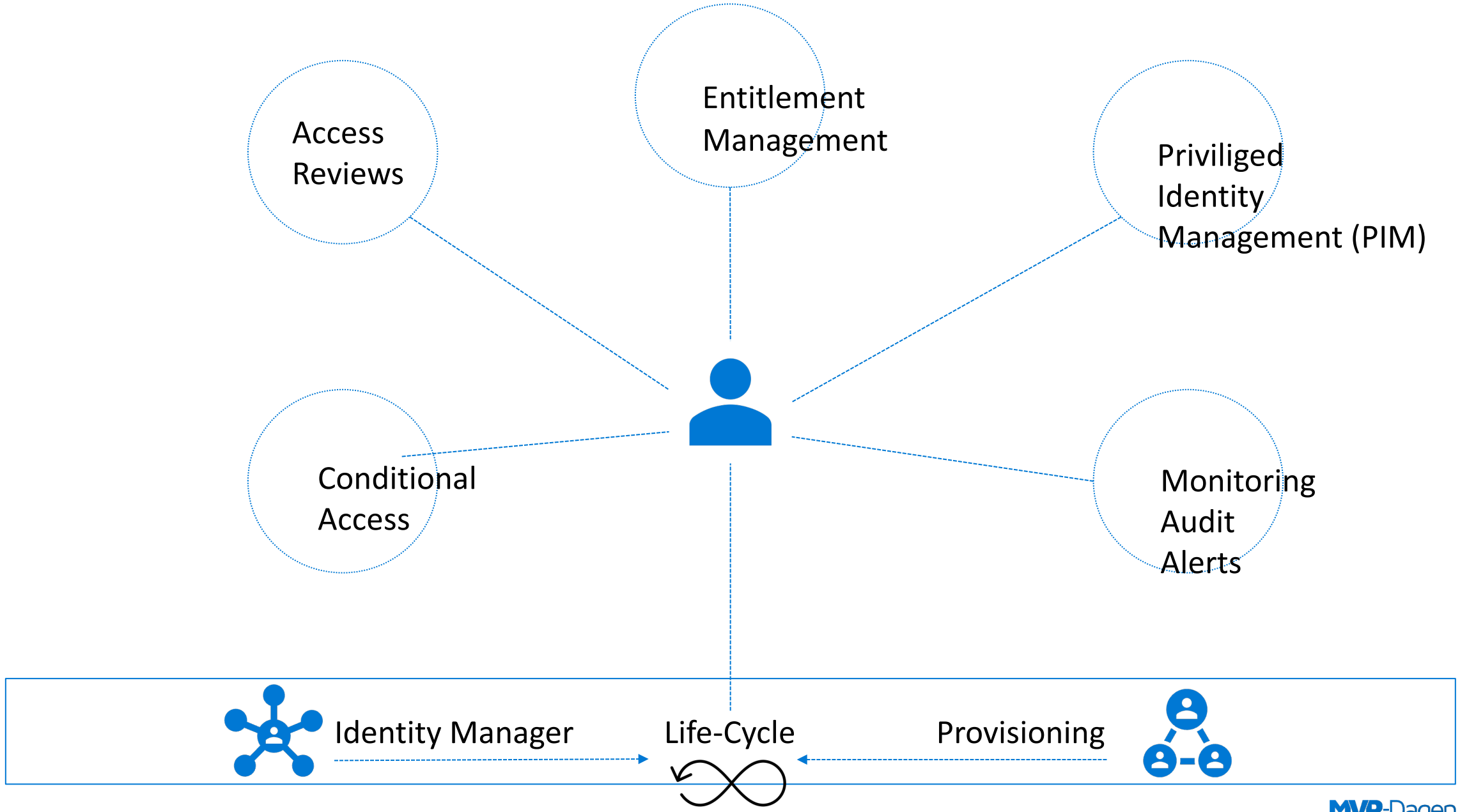

Identity Manager
Life-Cycle
Provisioning

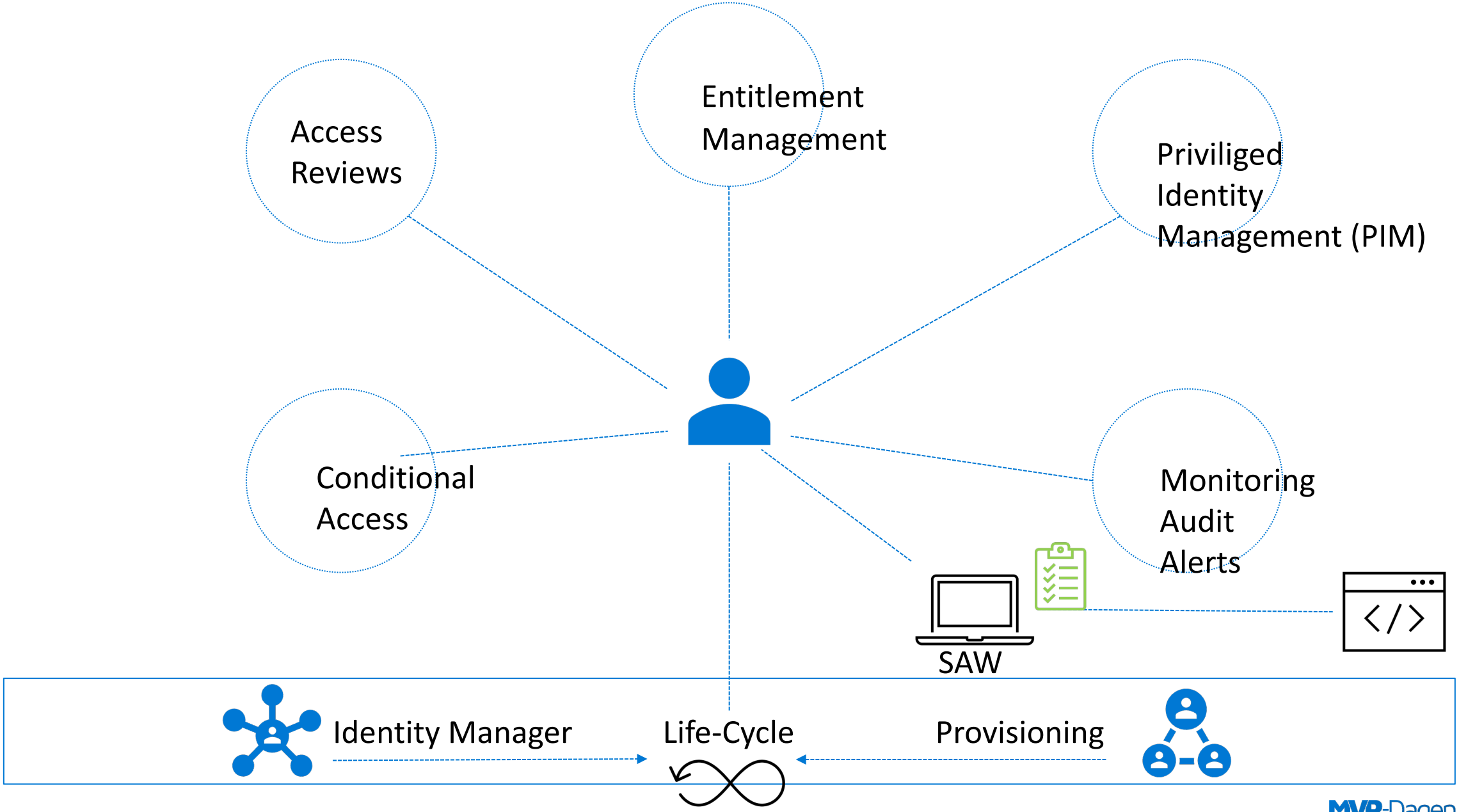

Priviliged
Identity
Management (PIM)
Identity Manager
Life-Cycle
Provisioning

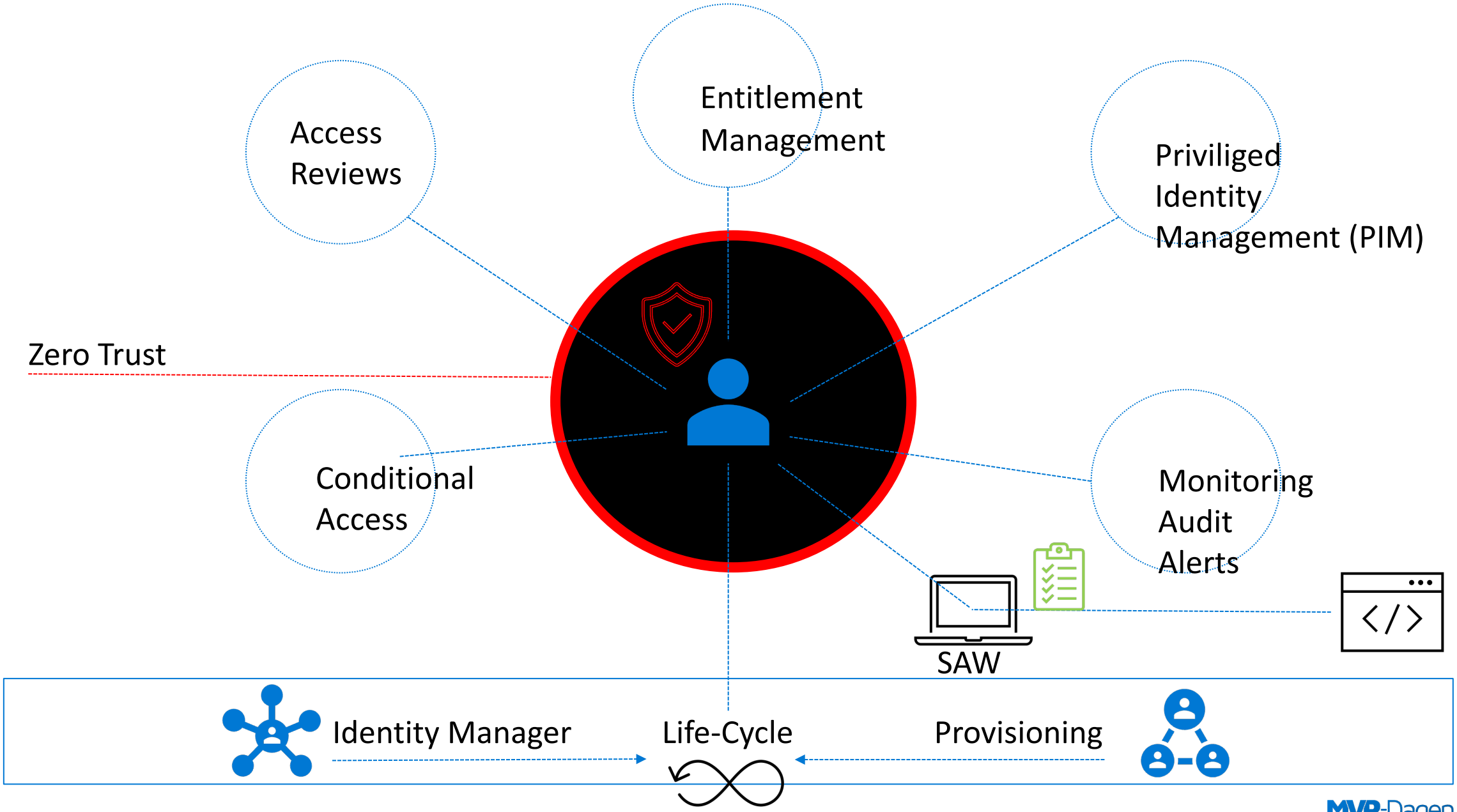

Entitlement Management
Priviliged Identity Management (PIM)
Identity Manager
Life-Cycle
Provisioning


Access Reviews
Entitlement Management
Priviliged Identity Management (PIM)
Identity Manager
Life-Cycle
Provisioning


Access Reviews
Entitlement Management
Priviliged Identity Management (PIM)
Conditional Access
Identity Manager
Life-Cycle
Provisioning

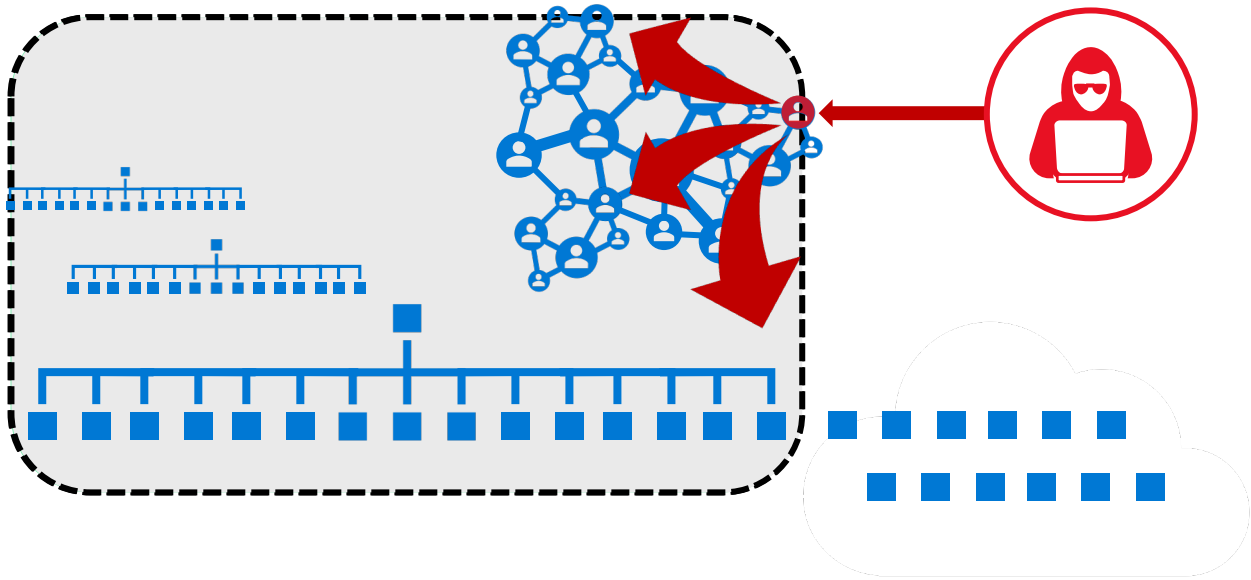

Access Reviews
Entitlement Management
Priviliged Identity Management (PIM)
Conditional Access
Monitoring Audit Alerts
Identity Manager
Life-Cycle
Provisioning


Access Reviews
Entitlement Management
Priviliged Identity Management (PIM)
Conditional Access
Monitoring Audit Alerts
SAW
Identity Manager
Life-Cycle
Provisioning


Access Reviews
Entitlement Management
Priviliged Identity Management (PIM)
Zero Trust
Conditional Access
Monitoring Audit Alerts
SAW
Identity Manager
Life-Cycle
Provisioning

Why are we having a Zero Trust conversation?

Access Control: Keep **Assets** away from **Attackers**



1. **IT Security is Complex**
   - Many Devices, Users, & Connections
2. **"Trusted network" security strategy**
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within network
3. **Assets increasingly leave network**
   - BYOD, WFH, Mobile, and SaaS
4. **Attackers shift to identity attacks**
   - Phishing and credential theft
   - Security teams often overwhelmed

Zero Trust Principals

Confirm explicitly

- Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification and irregularities.

Use least privileged access

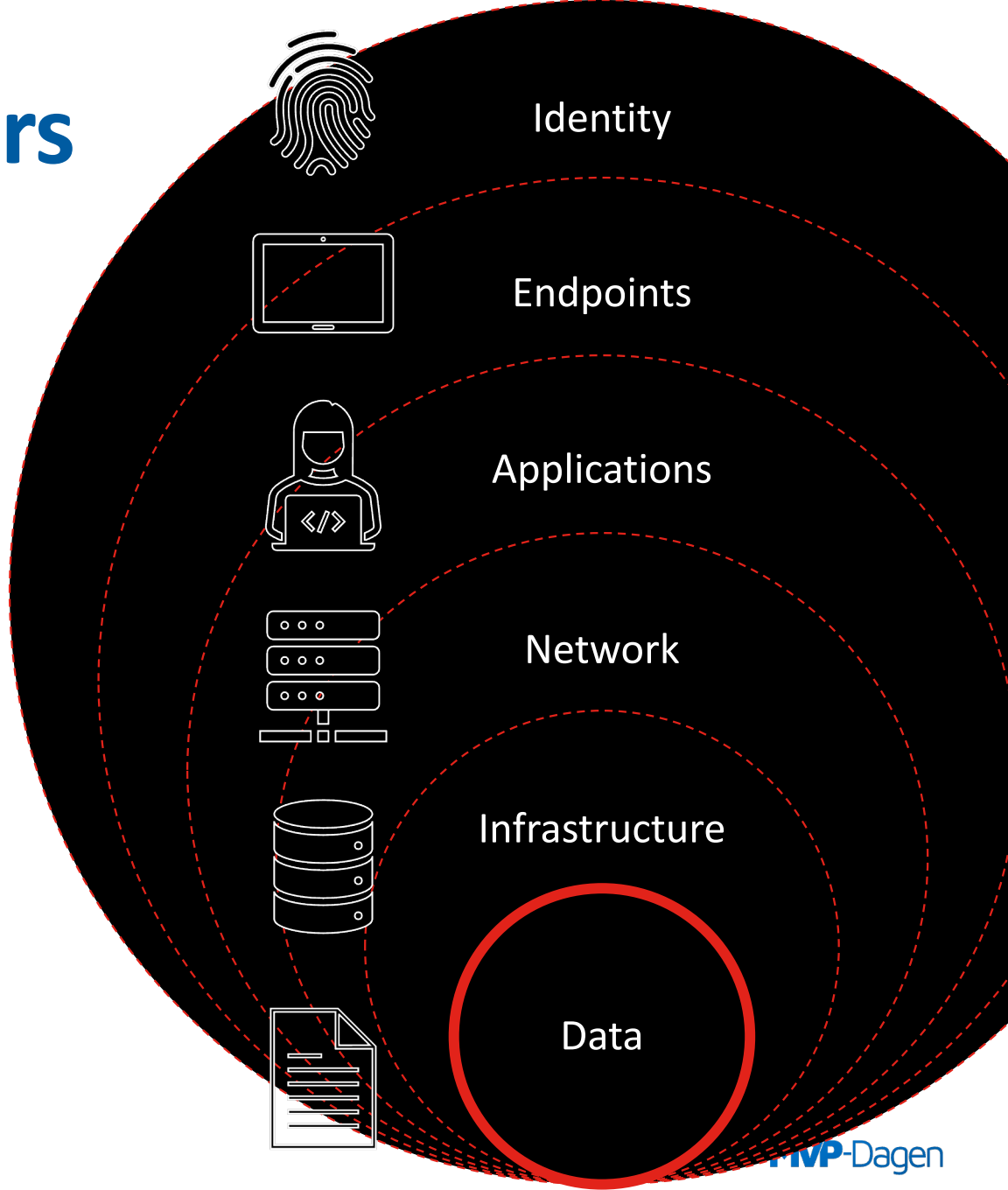
- Restrict user access with just-in-time and just-enough access (JIT / JEA), risk-based policy and data protection to ensure both data and productivity.

Assume breach

- Minimize exposure area and segment access. Verify end-to-end encryption and use analytics tools to gain visibility into the threat picture

Zero Trust security layers

- Confirm explicitly
- Use least privileged access
- Assume breach



Key Principles (assuming breach)

1. Manage privileged users

Ensure that privileged users have the appropriate roles and permissions at the right time **(NO WAY IN HELL YOU GET GA)**

2. Protect at the front door

Safeguard your resources at the front door with innovative and advanced risk-based conditional accesses

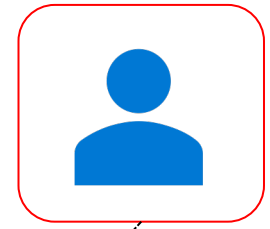
3. Protect your data against user mistakes

Gain deeper visibility into user, device and data activity

4. Detect attacks before they cause damage

Uncover suspicious activity and pinpoint threats with deep visibility and ongoing behavioral analytics.

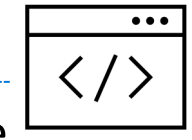
Example



.onmicrosoft.com
account

Roles:
Azure ARC Manager
Reader
Security Operator

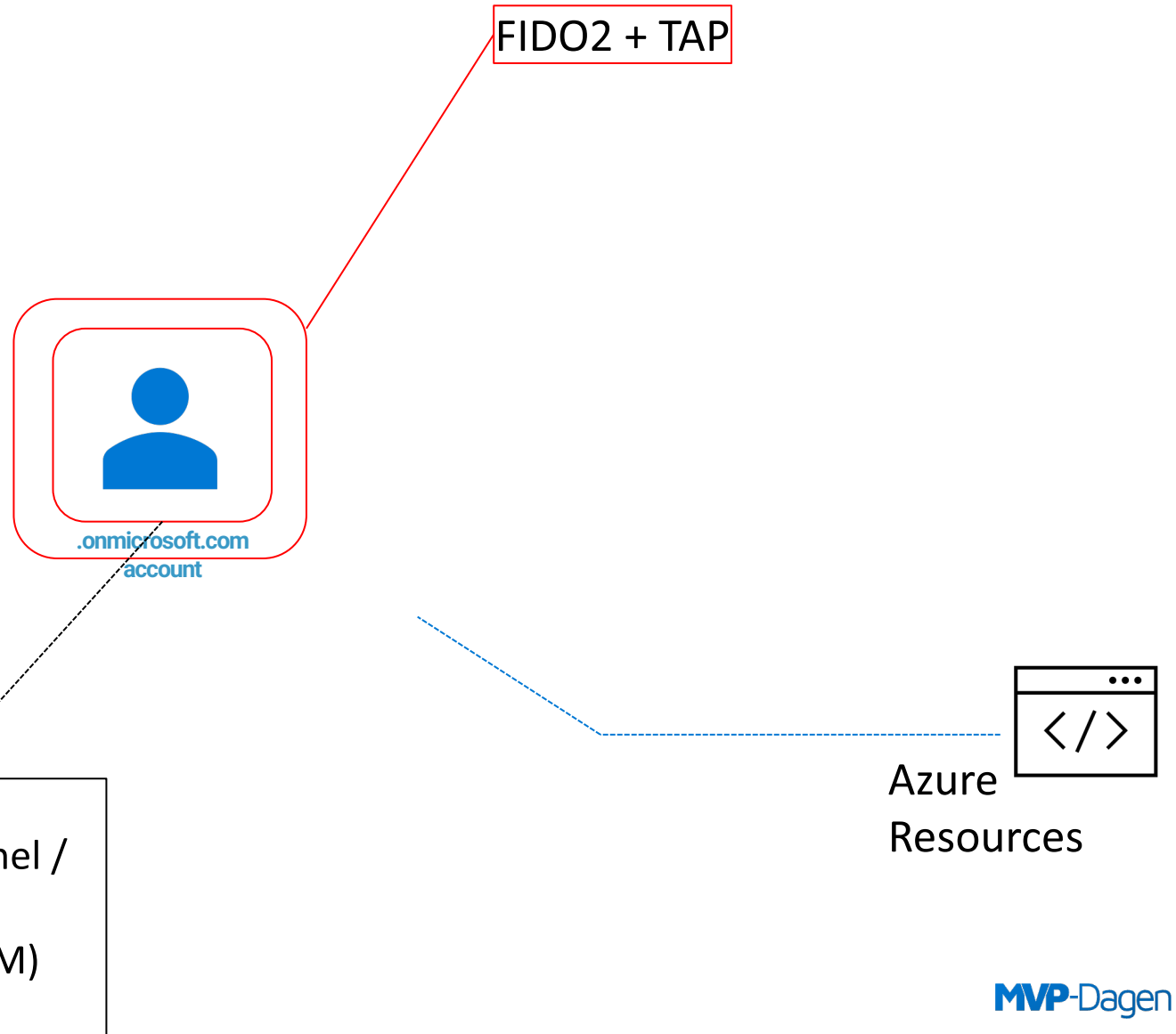
XDR
Azure Sentinel /
Monitor
(SIEM/CIEM)
Alerts



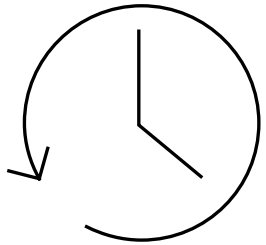
Azure
Resources

MVP-Dagen

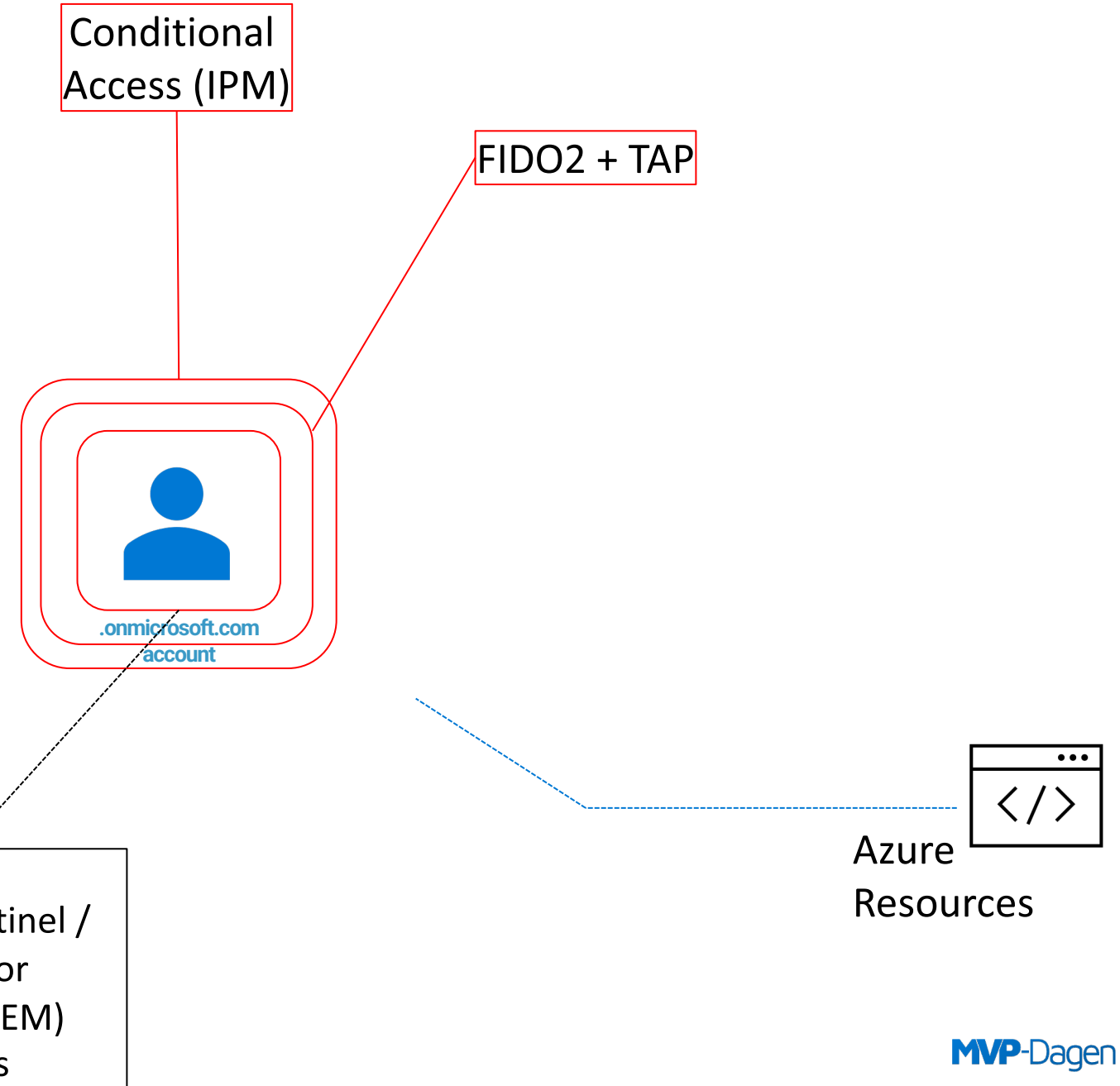
Example



Roles:
Azure ARC Manager
Reader
Security Operator
Contributor

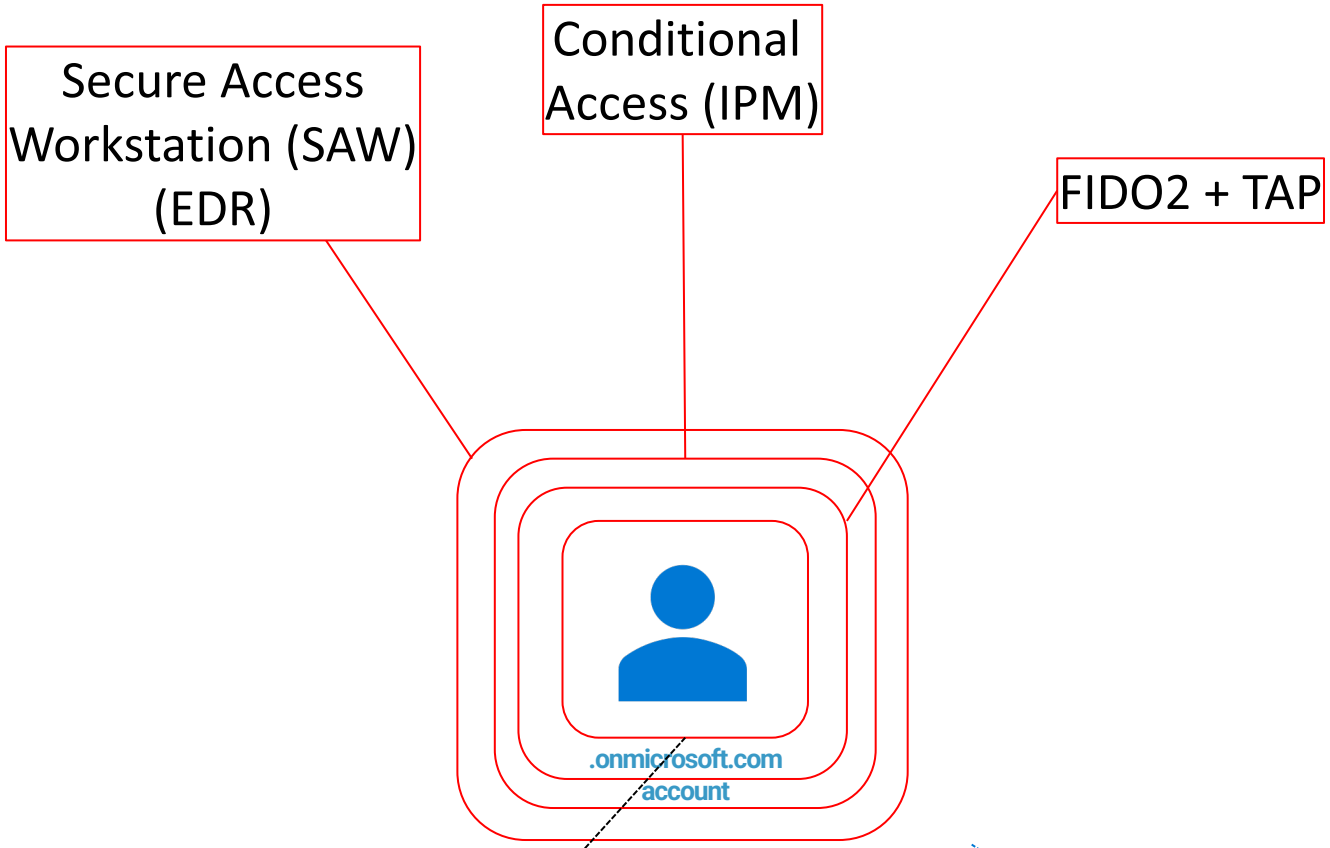


Example

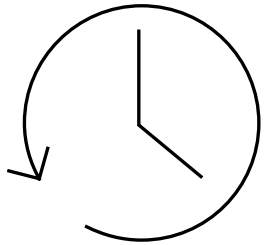


Roles:
Azure ARC Manager
Reader
Security Operator
Contributor

Example



Roles:
Azure ARC Manager
Reader
Security Operator
Contributor



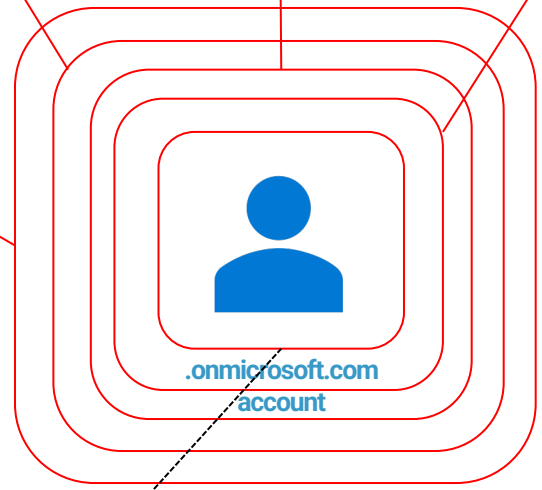
Example

Secure Access Workstation (SAW) (EDR)

Conditional Access (IPM)

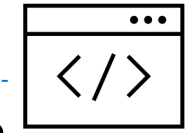
FIDO2 + TAP

Access Package (JiT) (Gate 1)



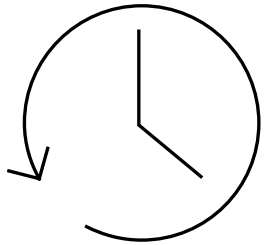
Roles:
Azure ARC Manager
Reader
Security Operator
Contributor

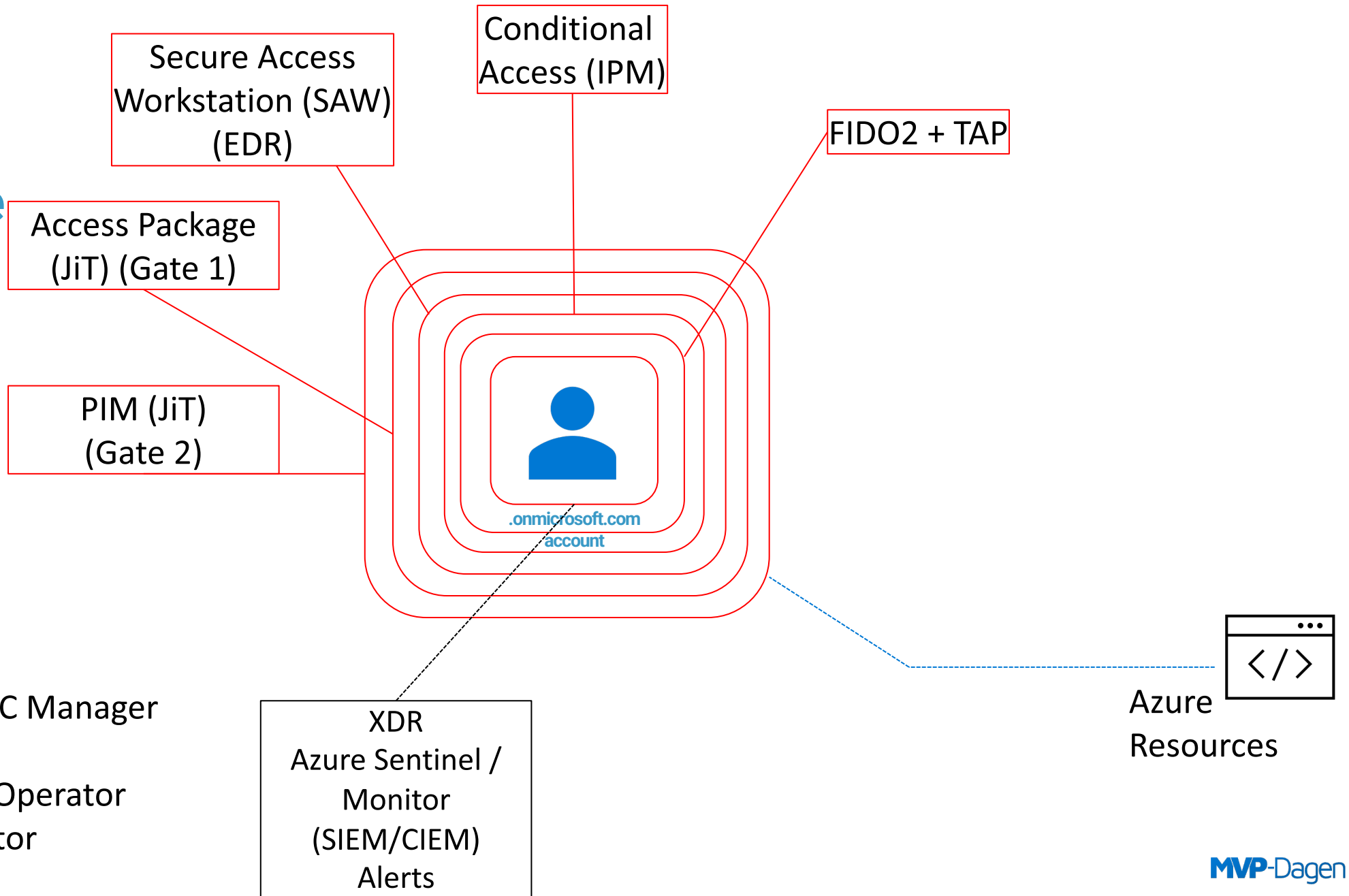
XDR
Azure Sentinel / Monitor
(SIEM/CIEM)
Alerts



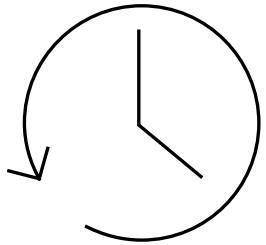
Azure Resources

Example





Roles:
Azure ARC Manager
Reader
Security Operator
Contributor



Example

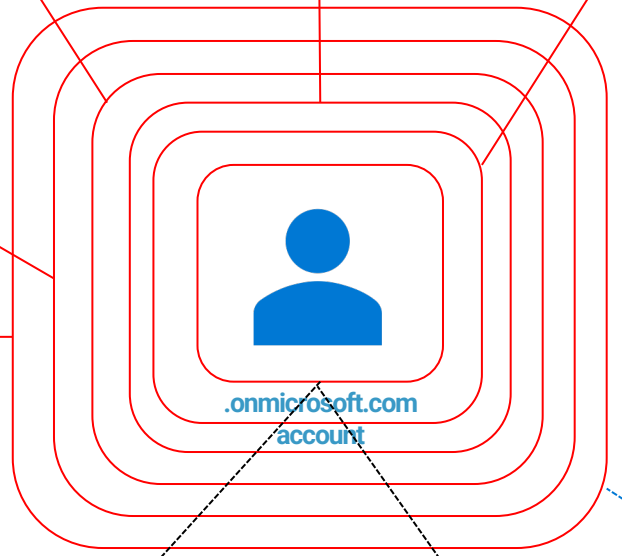
Secure Access Workstation (SAW) (EDR)

Conditional Access (IPM)

FIDO2 + TAP

Access Package (JiT) (Gate 1)

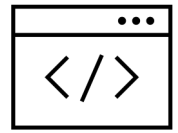
PIM (JiT) (Gate 2)



Roles:
Azure ARC Manager
Reader
Security Operator
Contributor

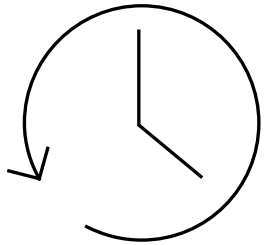
XDR
Azure Sentinel / Monitor
(SIEM/CIEM)
Alerts

Access Reviews



Azure Resources

MVP-Dagen



Example

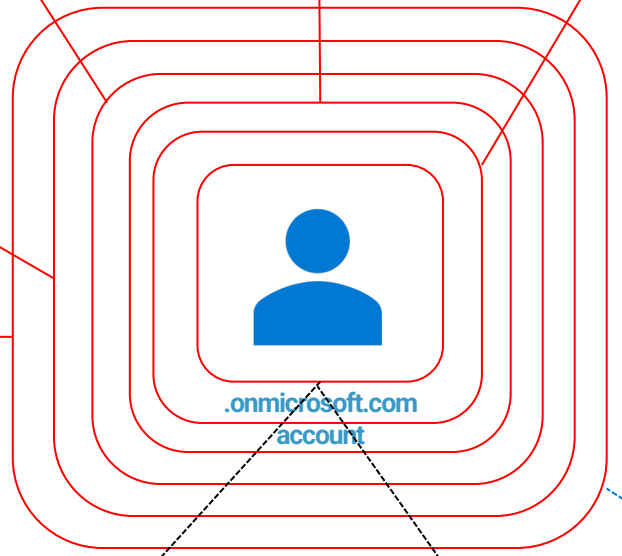
Secure Access Workstation (SAW) (EDR)

Conditional Access (IPM)

FIDO2 + TAP

Access Package (JiT) (Gate 1)

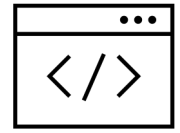
PIM (JiT) (Gate 2)



Roles:
Azure ARC Manager
Reader
Security Operator
Contributor

XDR
Azure Sentinel / Monitor
(SIEM/CIEM)
Alerts

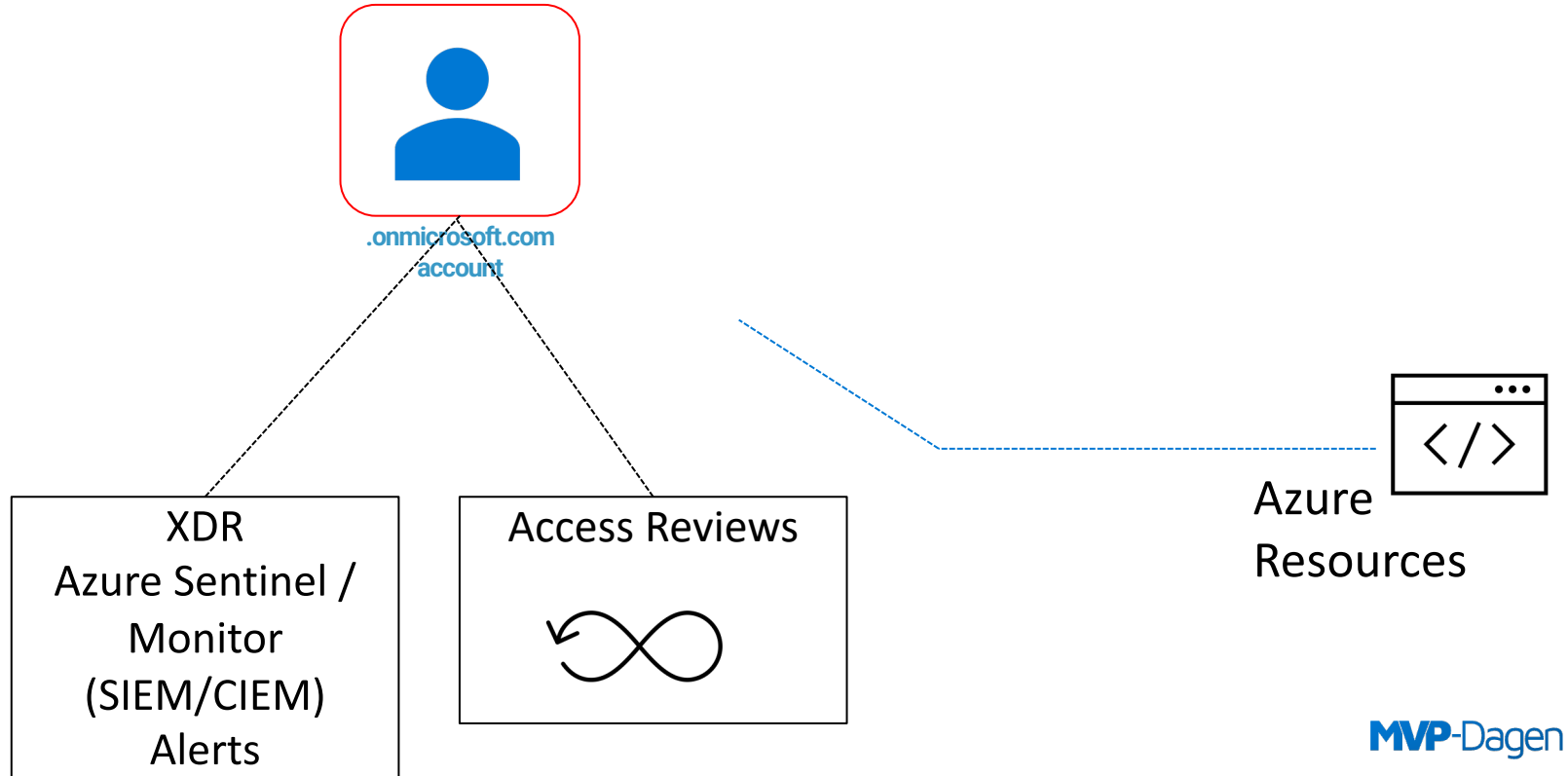
Access Reviews



Azure Resources

Example

Roles:
Azure ARC Manager
Reader
Security Operator
Contributor



DEMO

Entra Admin Center Lifecycle Workflows Permissions Management

Takk til våre sponsorer


Tusen takk!
MVP-Dagen