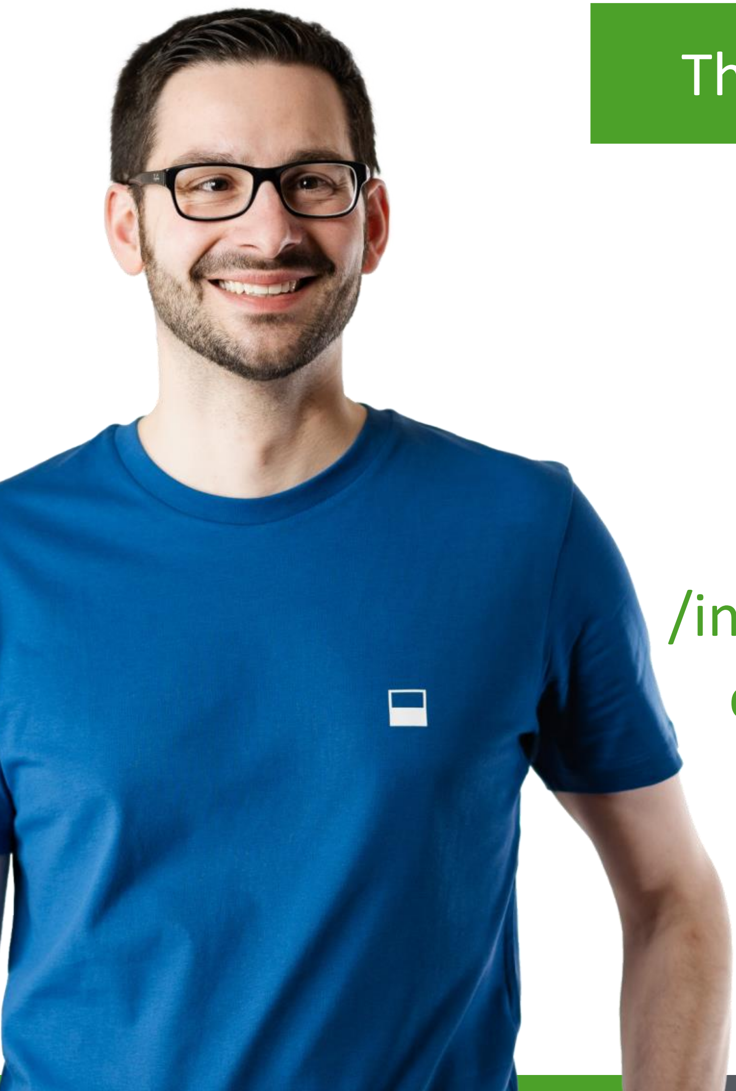
Zero Trust - Zero Gap? Spotlight on (new) uncovered aspects of your CA design

Christopher Brumm and Thomas Naunheim

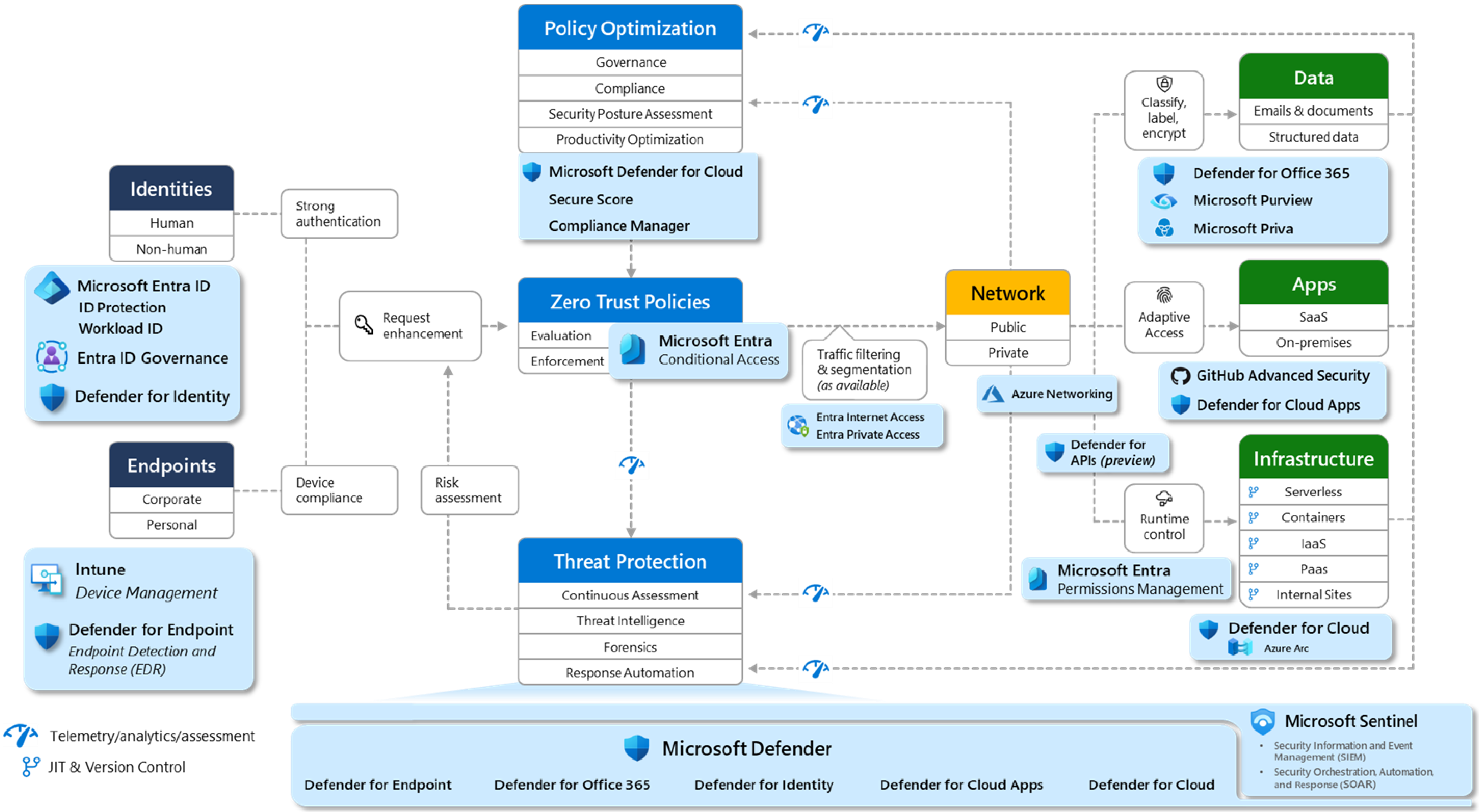
Workplace Ninja Summit 2024

About us...



Thomas Naunheim		Chris Brumm
old		very old
MVP		CISSP
Koblenz, Germany		Hamburg, Germany
left-handed		right-handed
@thomas_live	𝕏	@cbrhh
/in/thomasnaunheim	in	/in/christopherbrumm
cloud-architekt.net	🏠	chris-brumm.com

working at glueckkanja AG
as Cyber Security Architect
love (punk-rock) music and good wine



Policy Optimization
Governance
Compliance
Security Posture Assessment
Productivity Optimization

Microsoft Defender for Cloud
Secure Score
Compliance Manager

Identities
Human
Non-human

Microsoft Entra ID
ID Protection
Workload ID
Entra ID Governance
Defender for Identity

Strong authentication

Request enhancement

Zero Trust Policies
Evaluation
Enforcement

Microsoft Entra
Conditional Access

Traffic filtering & segmentation *(as available)*

Entra Internet Access
Entra Private Access

Network
Public
Private

Azure Networking

Classify, label, encrypt

Data
Emails & documents
Structured data

Defender for Office 365
Microsoft Purview
Microsoft Priva

Adaptive Access

Apps
SaaS
On-premises

GitHub Advanced Security
Defender for Cloud Apps

Defender for APIs *(preview)*

Runtime control

Infrastructure
Serverless
Containers
IaaS
Paas
Internal Sites

Microsoft Entra
Permissions Management

Defender for Cloud
Azure Arc

Endpoints
Corporate
Personal

Device compliance

Risk assessment

Intune
Device Management

Defender for Endpoint
Endpoint Detection and Response (EDR)

Threat Protection
Continuous Assessment
Threat Intelligence
Forensics
Response Automation

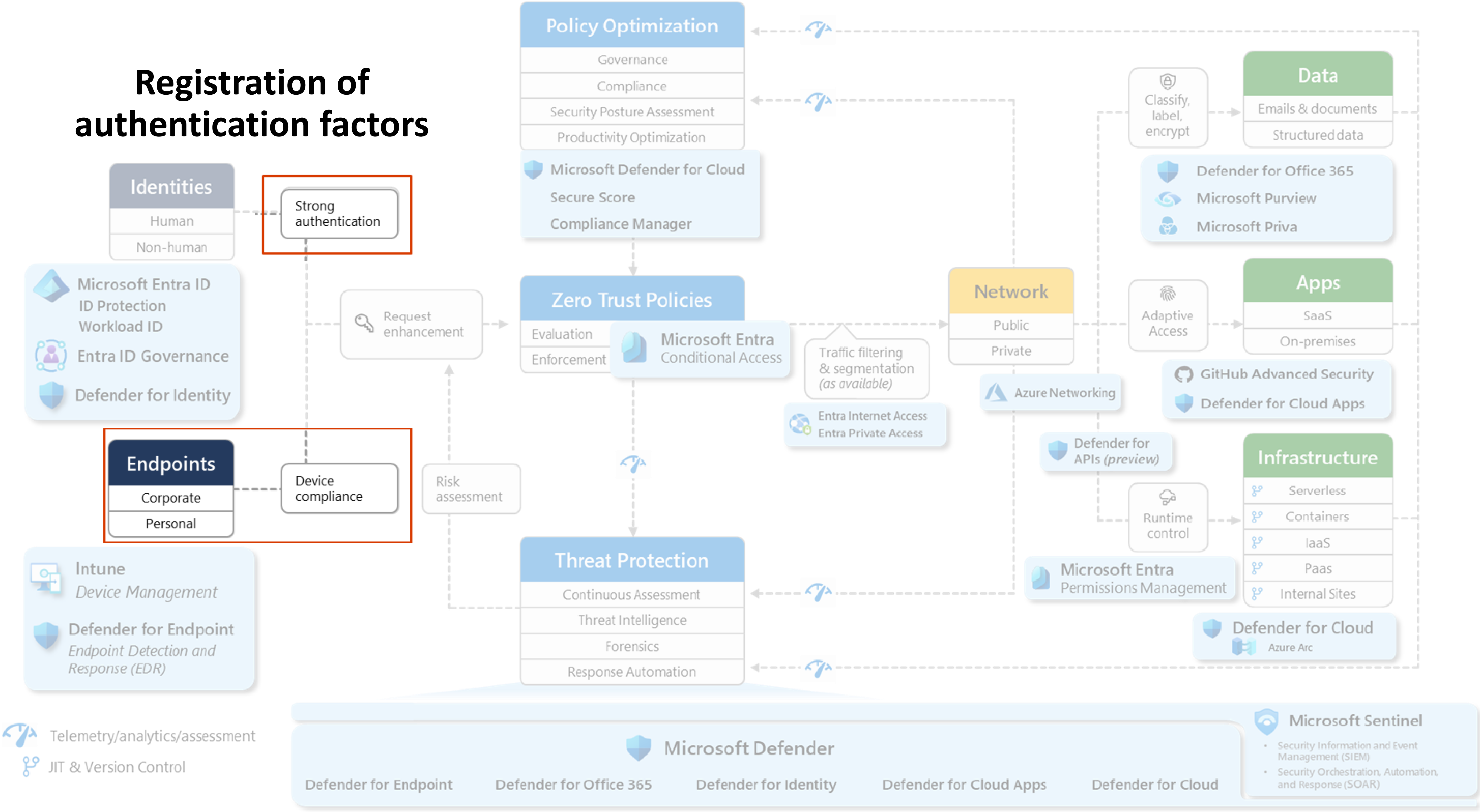
Telemetry/analytics/assessment
JIT & Version Control

Microsoft Defender
Defender for Endpoint
Defender for Office 365
Defender for Identity
Defender for Cloud Apps
Defender for Cloud

Microsoft Sentinel
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

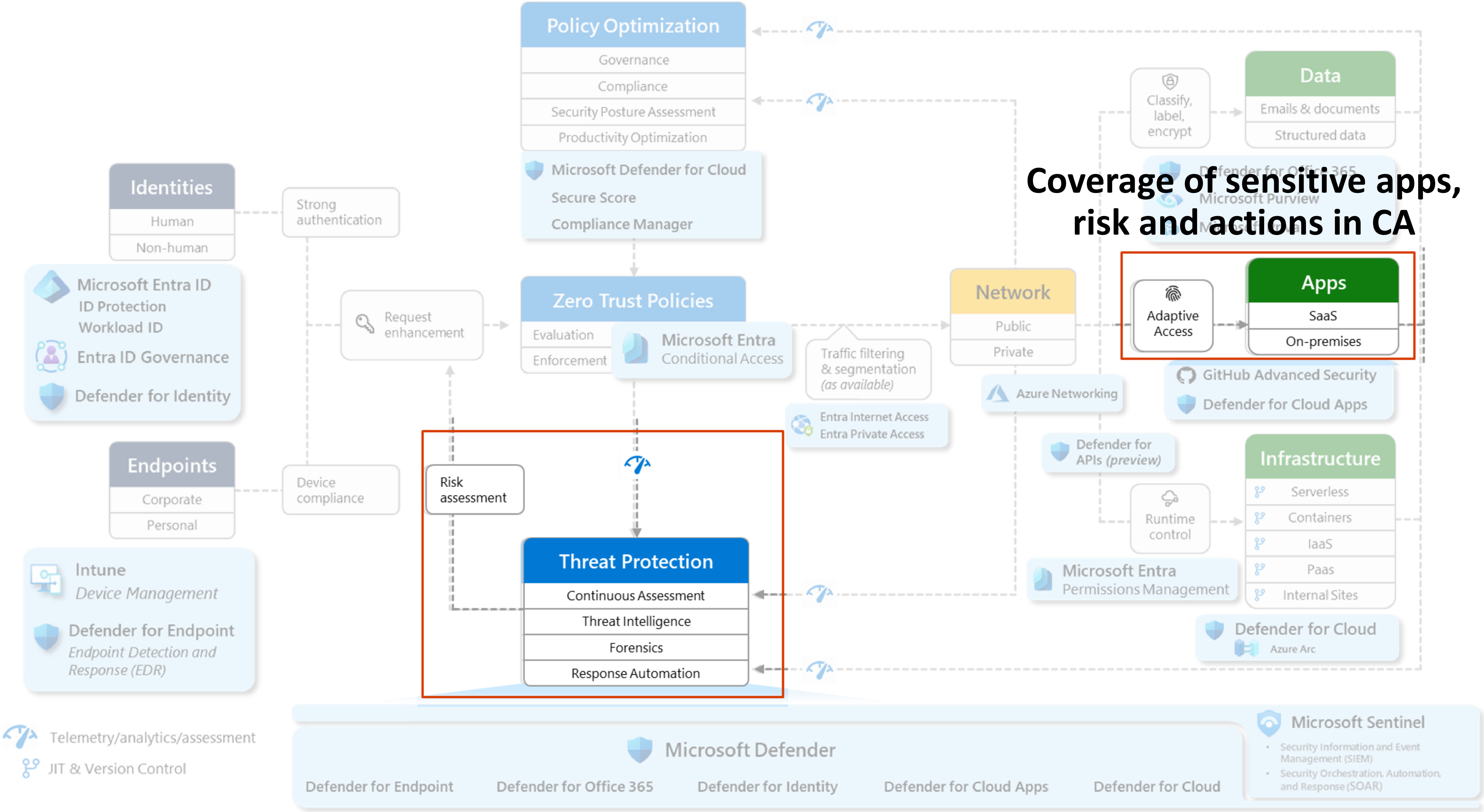
Source: Microsoft Cybersecurity Reference Architectures (MCRA) | Microsoft Learn

Registration of authentication factors



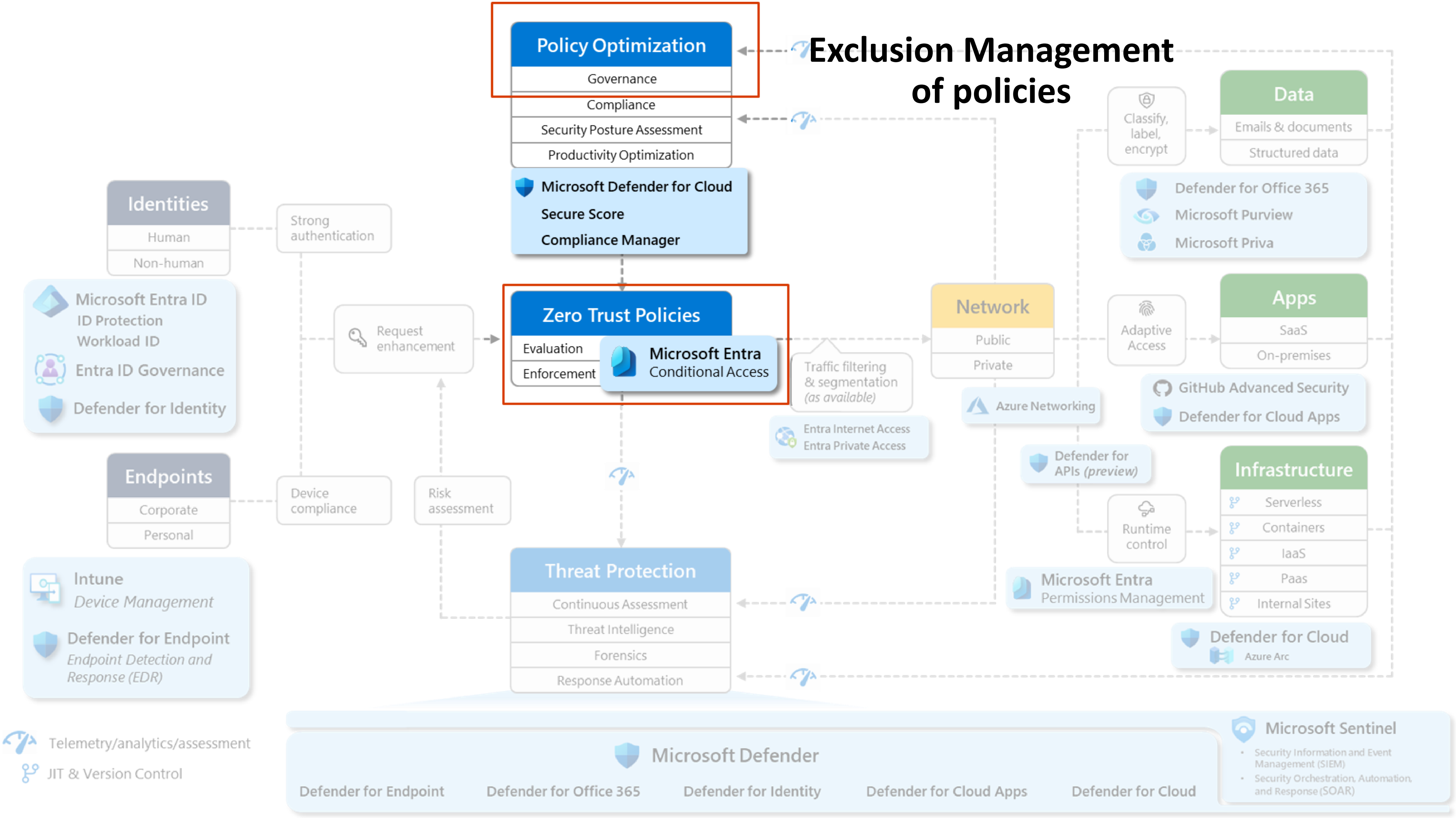
Source: Microsoft Cybersecurity Reference Architectures (MCRA) | Microsoft Learn

Coverage of sensitive apps, risk and actions in CA



Source: Microsoft Cybersecurity Reference Architectures (MCRA) | Microsoft Learn

Exclusion Management of policies



Policy Optimization

Governance

Compliance

Security Posture Assessment

Productivity Optimization

Microsoft Defender for Cloud

Secure Score

Compliance Manager

Identities

Human

Non-human

Strong authentication

Microsoft Entra ID

ID Protection

Workload ID

Entra ID Governance

Defender for Identity

Request enhancement

Zero Trust Policies

Evaluation

Enforcement

Microsoft Entra Conditional Access

Traffic filtering & segmentation *(as available)*

Entra Internet Access

Entra Private Access

Network

Public

Private

Azure Networking

Classify, label, encrypt

Data

Emails & documents

Structured data

Defender for Office 365

Microsoft Purview

Microsoft Priva

Adaptive Access

Apps

SaaS

On-premises

GitHub Advanced Security

Defender for Cloud Apps

Defender for APIs *(preview)*

Runtime control

Infrastructure

Serverless

Containers

IaaS

PaaS

Internal Sites

Microsoft Entra Permissions Management

Defender for Cloud

Azure Arc

Endpoints

Corporate

Personal

Device compliance

Risk assessment

Intune

Device Management

Defender for Endpoint

Endpoint Detection and Response (EDR)

Threat Protection

Continuous Assessment

Threat Intelligence

Forensics

Response Automation

Telemetry/analytics/assessment

JIT & Version Control

Microsoft Defender

Defender for Endpoint

Defender for Office 365

Defender for Identity

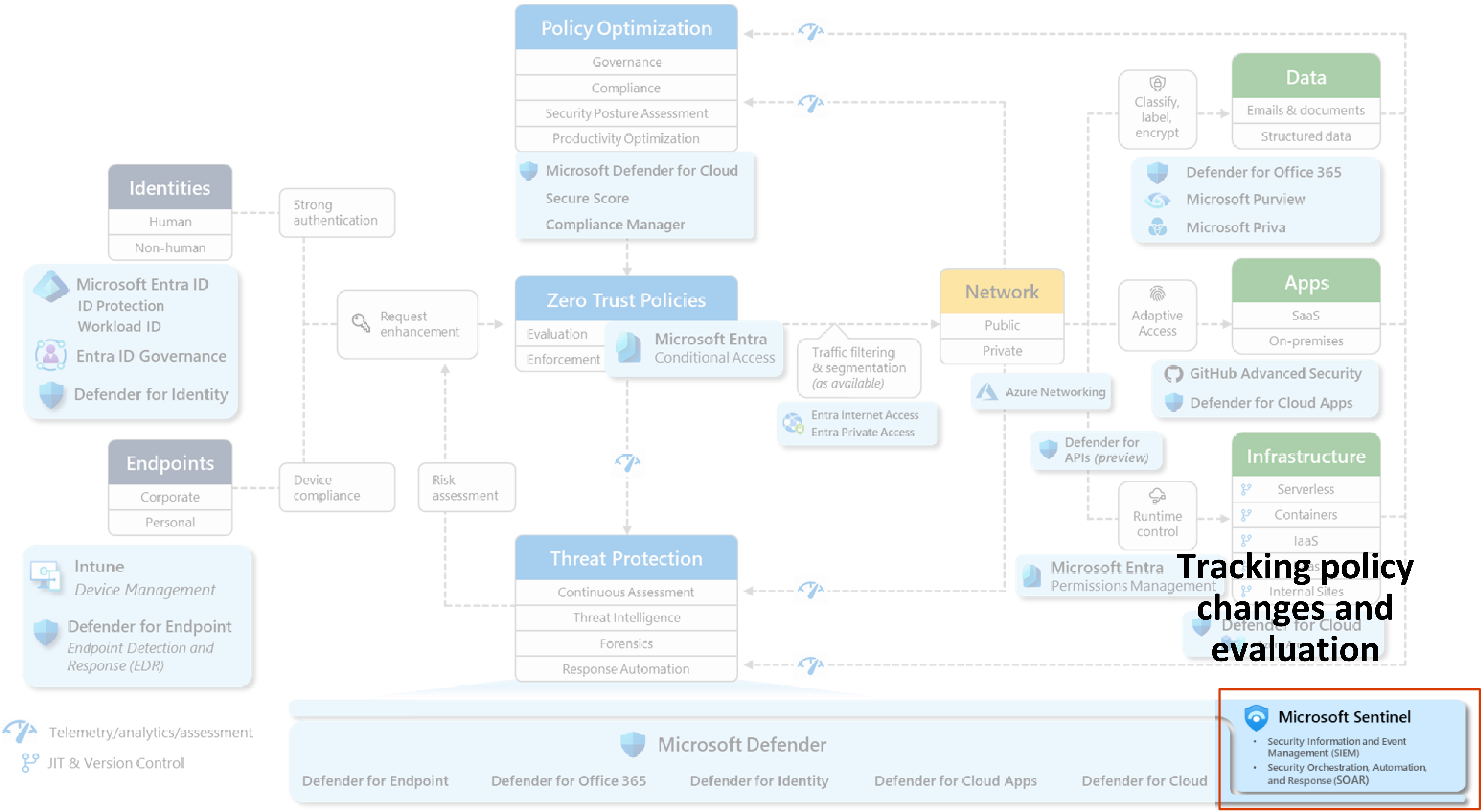
Defender for Cloud Apps

Defender for Cloud

Microsoft Sentinel

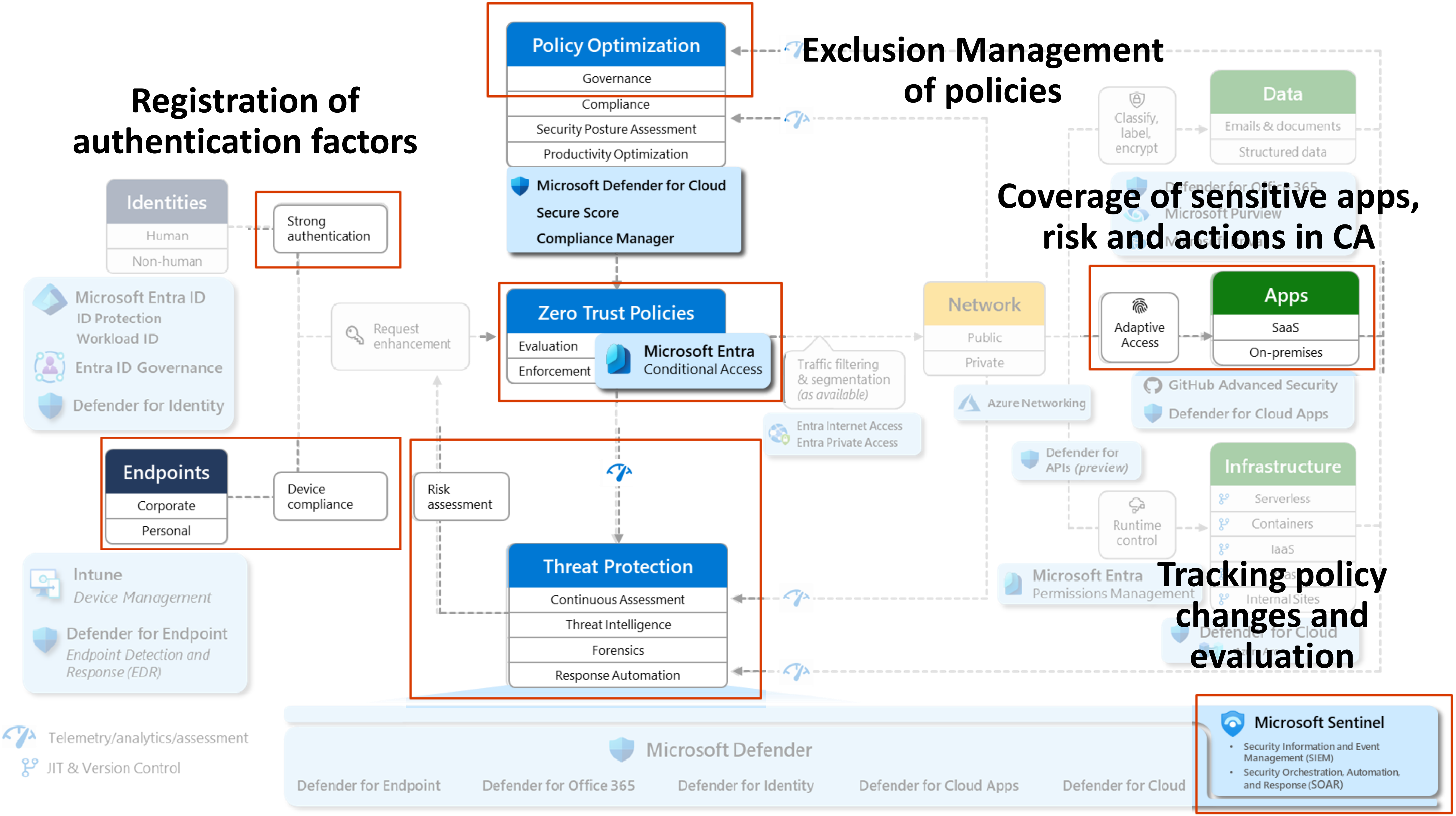
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

Source: Microsoft Cybersecurity Reference Architectures (MCRA) | Microsoft Learn



Tracking policy changes and evaluation

Source: Microsoft Cybersecurity Reference Architectures (MCRA) | Microsoft Learn



Exclusion Management of policies

Registration of authentication factors

Coverage of sensitive apps, risk and actions in CA

Tracking policy changes and evaluation

Policy Optimization
Governance
Compliance
Security Posture Assessment
Productivity Optimization

Microsoft Defender for Cloud
Secure Score
Compliance Manager

Identities
Human
Non-human

Strong authentication

Microsoft Entra ID
ID Protection
Workload ID
Entra ID Governance
Defender for Identity

Request enhancement

Zero Trust Policies
Evaluation
Enforcement
Microsoft Entra Conditional Access

Traffic filtering & segmentation *(as available)*

Entra Internet Access
Entra Private Access

Network
Public
Private

Azure Networking

Classify, label, encrypt

Data
Emails & documents
Structured data

Defender for Office 365
Microsoft Purview

Adaptive Access

Apps
SaaS
On-premises

GitHub Advanced Security
Defender for Cloud Apps

Defender for APIs *(preview)*

Endpoints
Corporate
Personal

Device compliance

Risk assessment

Infrastructure
Serverless
Containers
IaaS
Internal Sites

Runtime control

Microsoft Entra Permissions Management

Defender for Cloud

Intune
Device Management

Defender for Endpoint
Endpoint Detection and Response (EDR)

Threat Protection
Continuous Assessment
Threat Intelligence
Forensics
Response Automation

Telemetry/analytics/assessment
JIT & Version Control

Microsoft Defender
Defender for Endpoint
Defender for Office 365
Defender for Identity
Defender for Cloud Apps
Defender for Cloud

Microsoft Sentinel
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

Source: Microsoft Cybersecurity Reference Architectures (MCRA) | Microsoft Learn

AGENDA

- Registration of authentication factors
- Coverage of sensitive apps, risk and actions in CA
- Exclusion Management of policies
- Tracking policy changes and evaluation

Key takeaways:

- Do's and Don'ts in restricting authentication methods and flows by CA
- Attack paths and risks of weak operationalization of CA policies
- Importance of CAE and Session Management

Registration of authentication factors

Auth Factor Registration Maturity

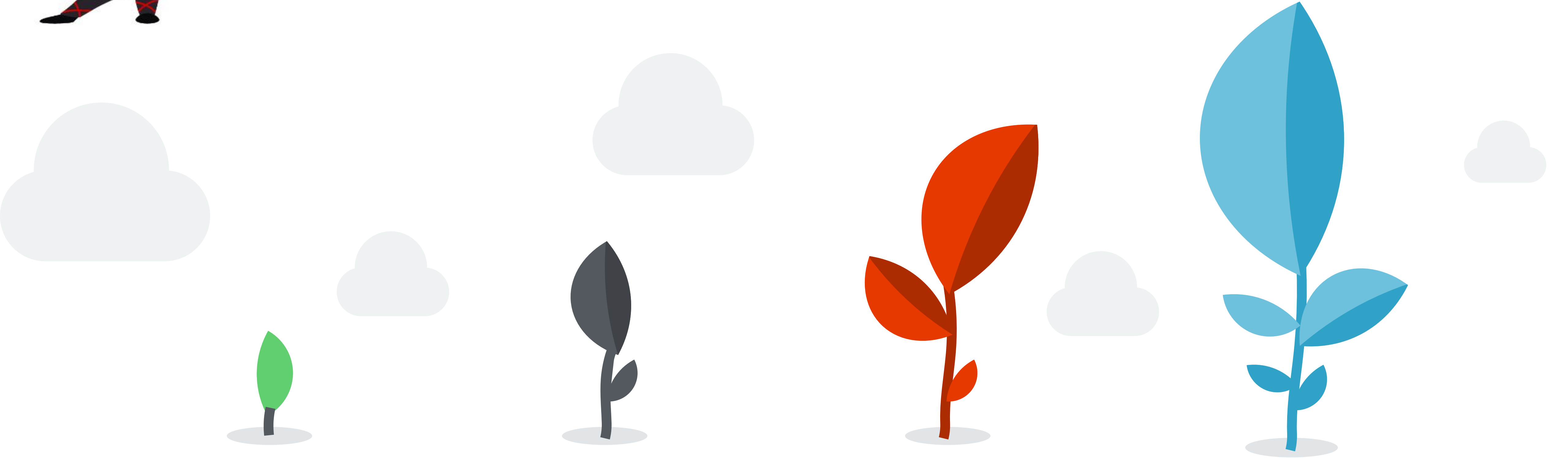
💻	Enforce MFA for Device Registration	Enforce MFA with SIF for Intune Enrollment	Block Personal Devices	Enforce TAP/FIDO2
🛡	Ask users to register MFA	Enforce MFA registration and usage	Restrict MFA registration to Trusted Devices / Locations	Make TAP a core part of your lifecycle processes

Demo: TAP Self-Service

Enable your users to request a Temporary Access Pass in a self-service portal

Coverage of sensitive apps, risk and actions in CA

Re-evaluation of Conditional Access



✓ Risk-based and User Action Policy

CAE for supported M365 apps and risk/critical events

Enforce Re-Auth by Risk Conditions or User Actions, Limited session lifetime

Require Re-Auth on sensitive app actions or context

Require Re-Authentication on sensitive cloud apps

CAE for location change by strictly enforcement

Demo: Sensitive Apps & Actions

Authentication context use cases and limitations

Acquired token and established sesssion from GSA client outside of compliant network

Exclusion Management of policies

Exclusion Management of User

Using ~~synced~~ cloud-only Security Groups for User Exclusion

Identity Governance Access Review of Exclusion Groups

Delegate management on exclusion group (on specific scope) to helpdesk or self-service (temporary)

Protecting security groups and manage exclusions with Entitlement Management

The Exclusion Management Dilemma

Role-Assignable Group

✅ Restrict group management to owner, Global and Priv Role Admin

✅ Can be managed by Entitlement management

‼️ Group member inherit the protection level of the group

Restricted Administrative Unit

✅ Restrict group management to dedicated role assignments

‼️ Can not be managed by Entitlement management

✅ No protection inheritance to the group members

Tracking policy changes and evaluation

Policy changes and monitoring

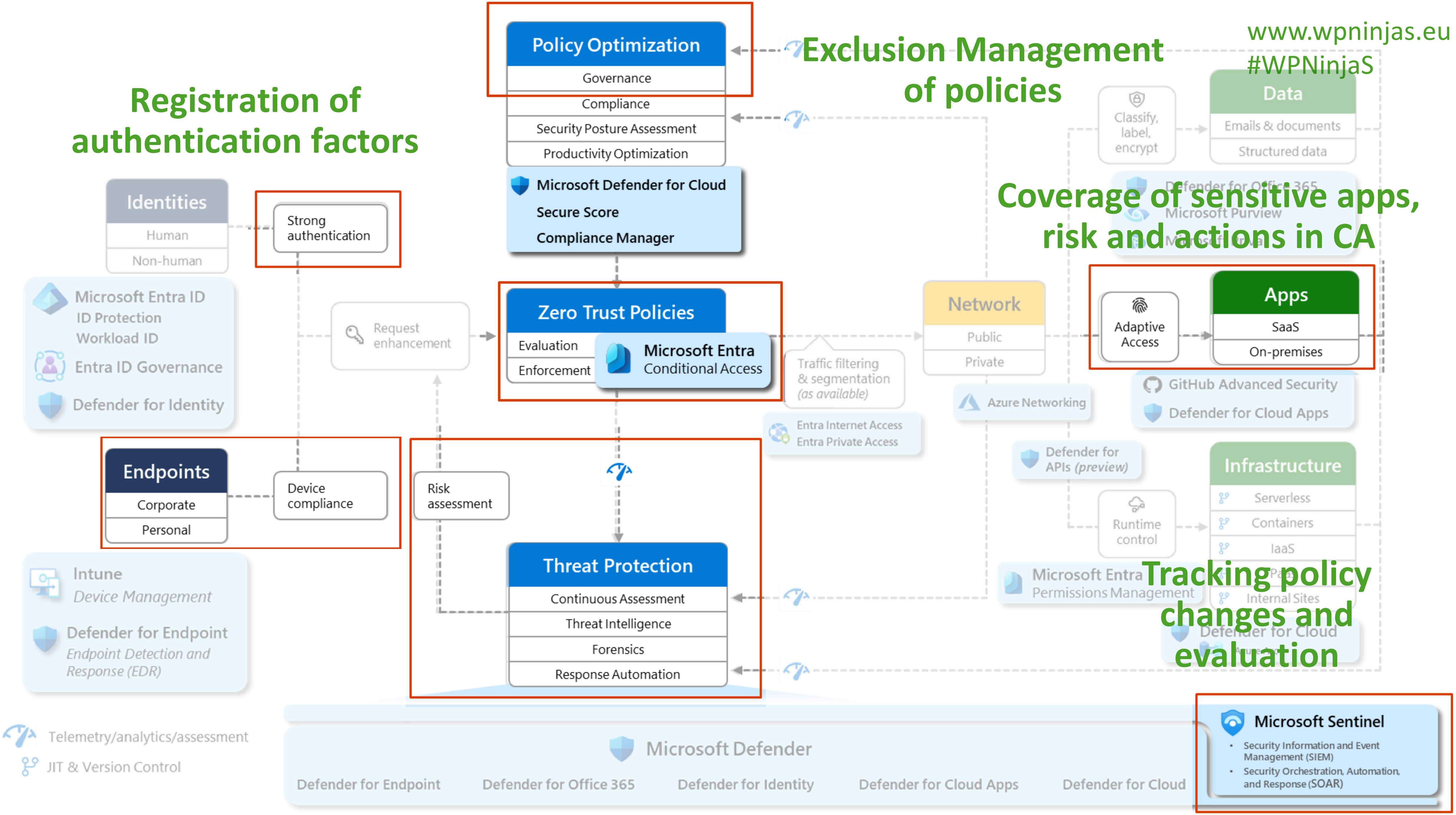
Enable sign-in logs and audit logs, using built-in workbooks (CA Insights)	Alert on policy change, comparison policy in Portal	Comparison of policy changes and effectiveness with community tools	Monitoring of CA effectiveness (e.g., Maester, KQL), alert on changes outside CI/CD
Manual modification of policy or using template	Duplicate and Import policy via portal	Export policies by using Graph API (e.g., EntraExporter)	“CA-as-Code” by using Terraform/Graph API

Demo: Advanced auditing & monitoring

Compare of policy change in UI portal

Community Workbooks for CA policy monitoring

Evaluation of Conditional Access configuration posture by Maester



Registration of authentication factors

Exclusion Management of policies

Coverage of sensitive apps, risk and actions in CA

Tracking policy changes and evaluation

Policy Optimization
- Governance
- Compliance
- Security Posture Assessment
- Productivity Optimization

Microsoft Defender for Cloud
Secure Score
Compliance Manager

Identities
- Human
- Non-human

Strong authentication

Microsoft Entra ID
ID Protection
Workload ID
Entra ID Governance
Defender for Identity

Request enhancement

Zero Trust Policies
- Evaluation
- Enforcement

Microsoft Entra Conditional Access

Traffic filtering & segmentation *(as available)*

Entra Internet Access
Entra Private Access

Network
- Public
- Private

Azure Networking

Defender for APIs *(preview)*

Classify, label, encrypt

Data
- Emails & documents
- Structured data

Defender for Office 365
Microsoft Purview
Microsoft Priva

Adaptive Access

Apps
- SaaS
- On-premises

GitHub Advanced Security
Defender for Cloud Apps

Endpoints
- Corporate
- Personal

Device compliance

Risk assessment

Intune
Device Management
Defender for Endpoint
Endpoint Detection and Response (EDR)

Threat Protection
- Continuous Assessment
- Threat Intelligence
- Forensics
- Response Automation

Runtime control

Infrastructure
- Serverless
- Containers
- IaaS
- PaaS
- Internal Sites

Microsoft Entra Permissions Management

Defender for Cloud

Telemetry/analytics/assessment
JIT & Version Control

Microsoft Defender
Defender for Endpoint
Defender for Office 365
Defender for Identity
Defender for Cloud Apps
Defender for Cloud

Microsoft Sentinel
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

Source: Microsoft Cybersecurity Reference Architectures (MCRA) | Microsoft Learn

Thank you Sponsors

www.wpninjas.eu
#WPNinjaS

Diamond Sponsor

Microsoft

Platinum Sponsors

2Pint

PATCH MY PC

RECAST SOFTWARE

glueck kanja

Gold Sponsors

nerdio

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

controlup

Rimo3

adaptiva™

Silver Sponsors

APENTO

UMB creating time®

EPIC FUSION
BRING IT ALL TOGETHER

water
IT Security & Defense

We love Feedback

https://wpninjas24.sched.com/

😀 Great Session!

😐 Okay Session!

🙁 Not so okay Session!