PROACTIVE

PROACTIVE

Cloud Sikkerhed

Hvordan bygger vi en Zero Trust cloud?

Frederik Stengaard Hansen

ProActive A/S

Indhold

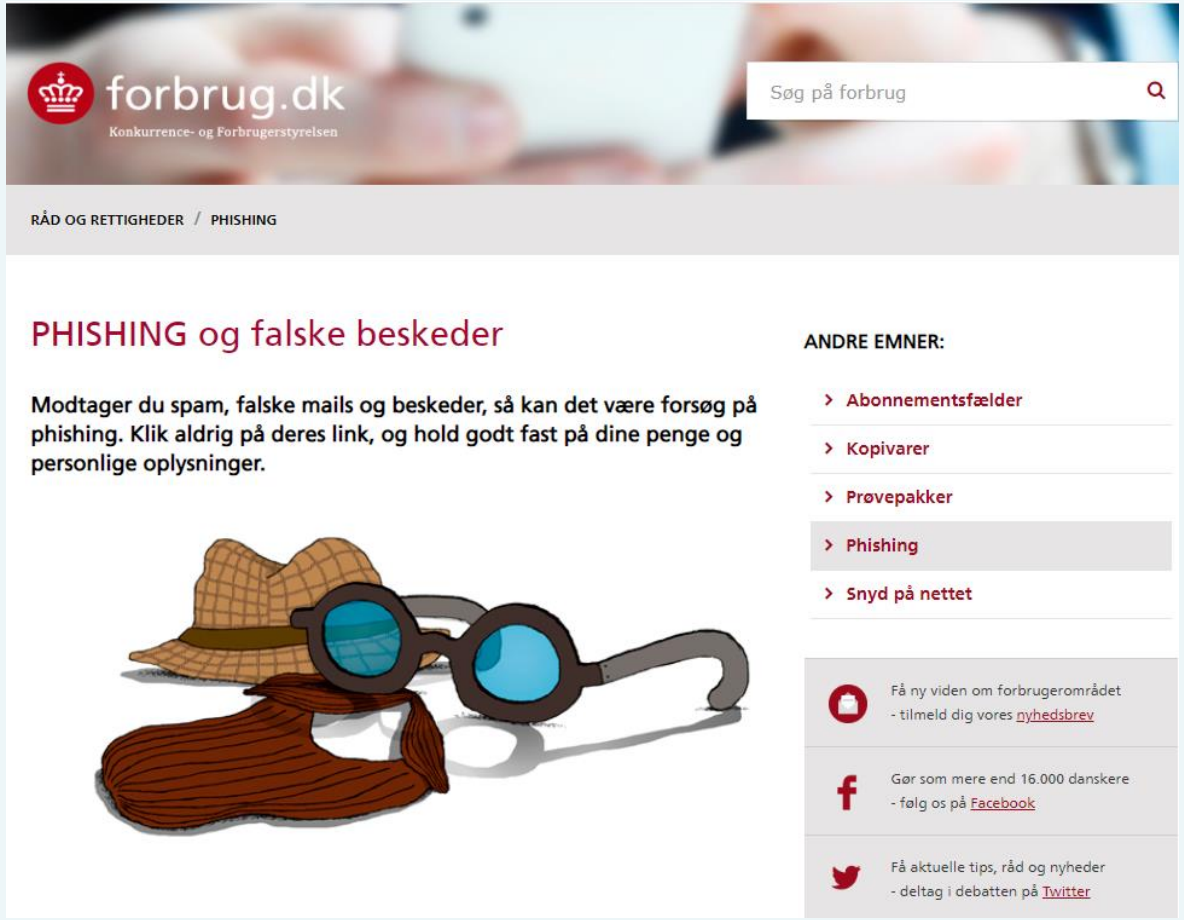
Når cloud applikationer, -services og -tjenester bliver tilgået fra interne og eksterne mobile enheder oplever vi et stigende behov for identitets- og adgangsstyring for at bevare sikkerheden på tværs af organisationen.

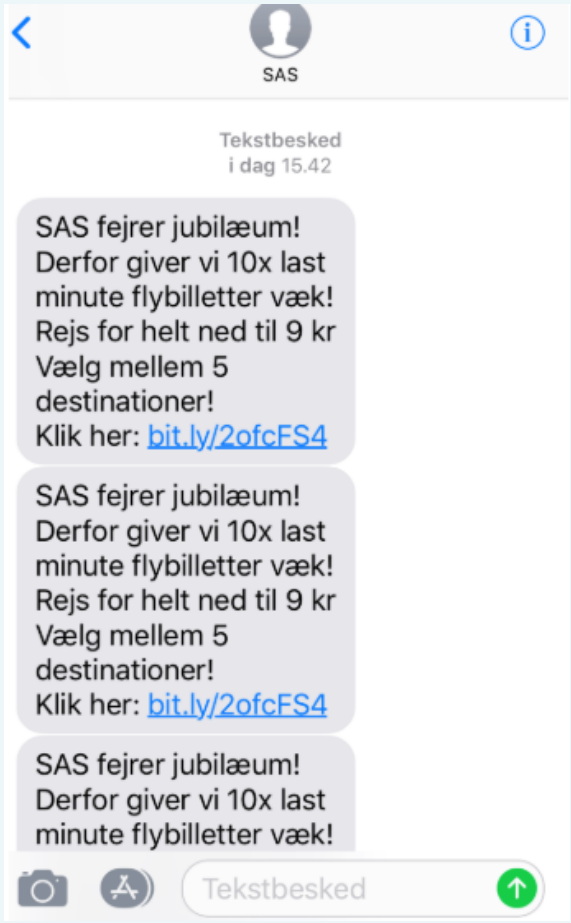
Virksomheder drukner i portaler og log filer, hvordan kan vi sikre at sikkerheds ressourcer kan arbejde mest hensigtsmæssigt.

Emner og spørgsmål vi vil forsøge at besvare

1. **Hvordan planlægger man sin cloud sikkerheds strategi**
2. **Hvordan kan man sikre sine brugere i cloud?**
3. **Hvordan beskytter man imod datalæk?**
4. **Hvordan overvåger man sine forskellige miljøer?**
5. **Hvor skal man starte?**

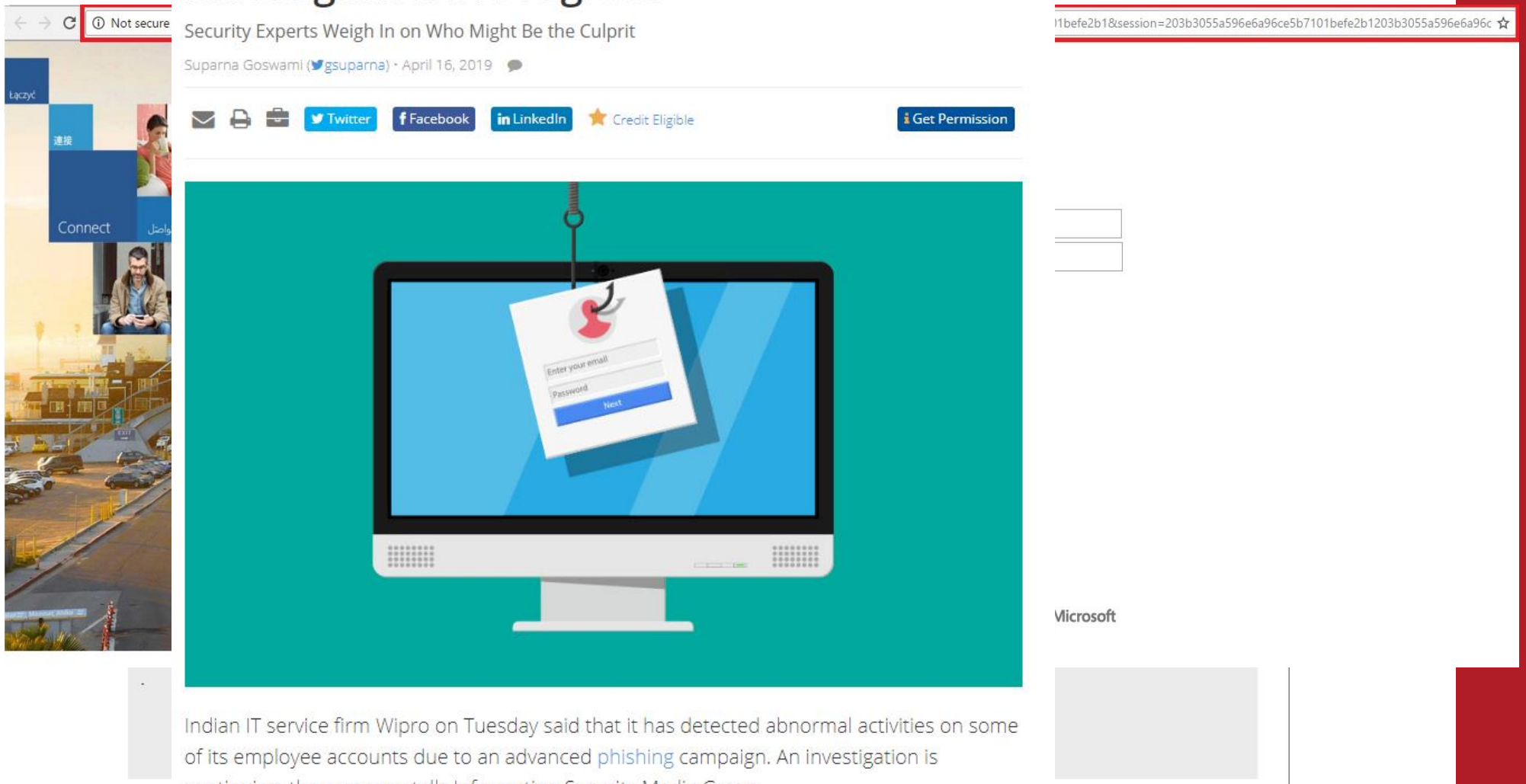
Hvorfor er det vigtigt at beskytte sine identiteter?





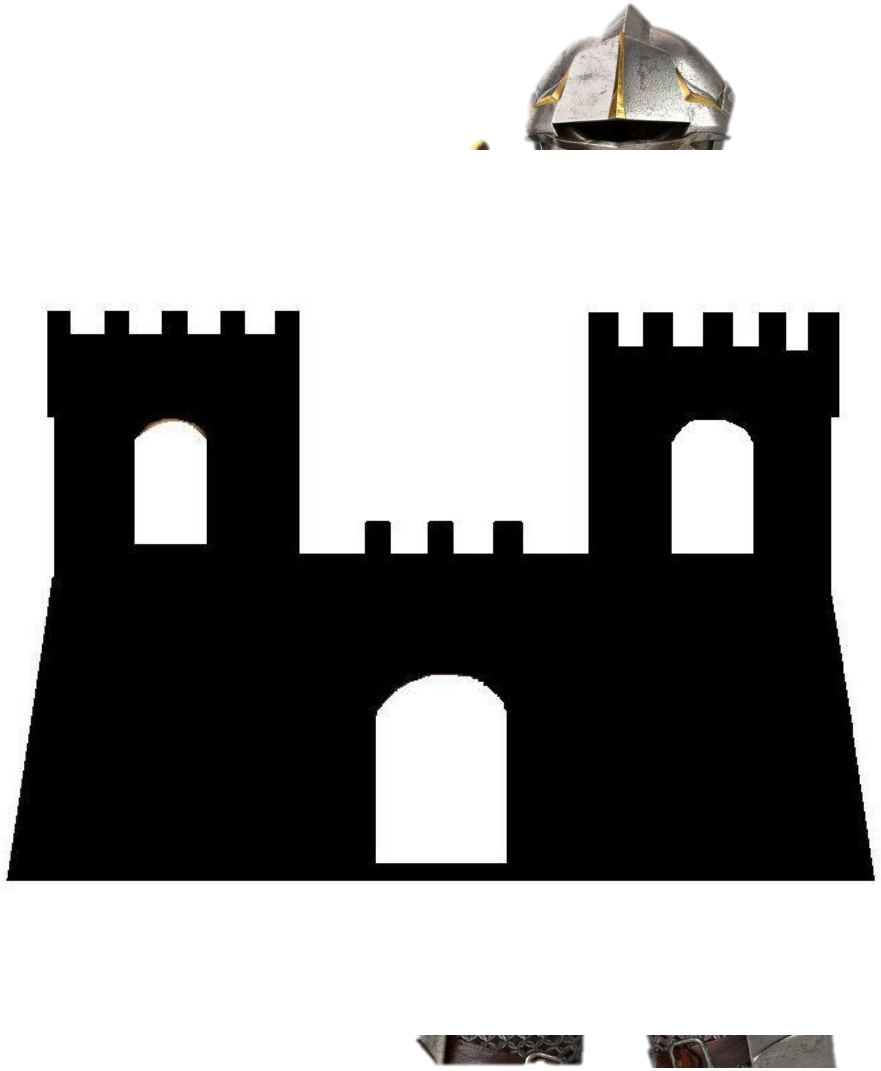
https://www.forbrug.dk/raad-og-rettigheder/snyd-og-bedrag/phishing/

Hvorfor er det vigtigt at beskytte sine identiteter?



https://www.forbrug.dk/raad-og-rettigheder/snyd-og-bedrag/phishing/

Hvad kan vi stole på udenfor borgens mure?

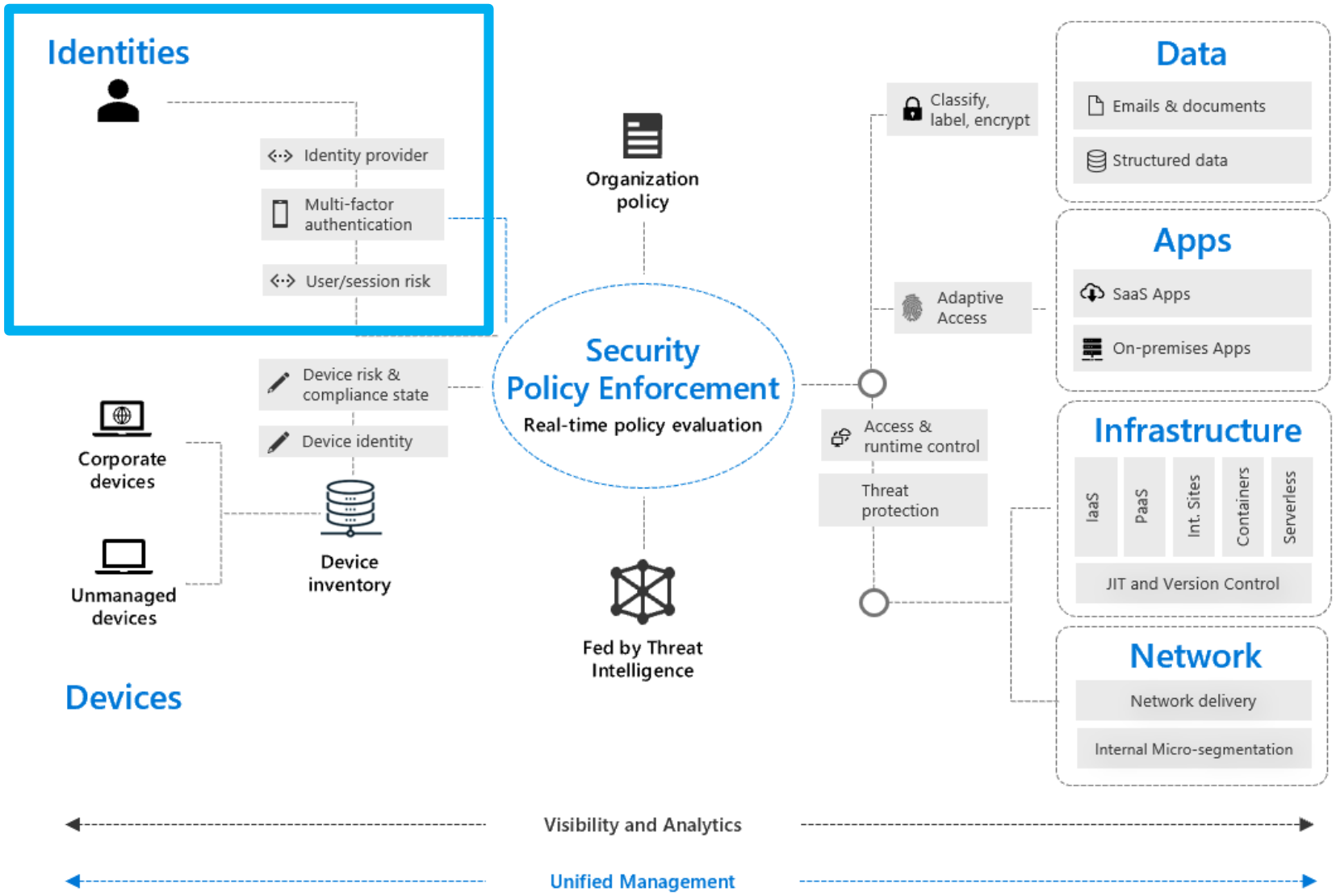


Zero Trust

Principper

- Bekræft Eksplicit
  - Brug alle tilgængelige data punkter I autentifikation
- Brug “Least Privilidged Access”
  - Begræns bruger roller, til der hvor det giver mening
- Antag at der er brud
  - Minimer spredning og sørg for at sessioner er krypterede

Zero Trust Architecture



https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft

A Password walks into a bar,

Bartender says, "haven't I seen you before ?"

Password says, “Probably, I just got dumped"

Passwords – Hvad skal vi med dem?

Password Best Practices

- Bloker for "Kendte Ord"
  - Vigtigt at have en løsning man kan tilpasse; "Dansk-IT", "Winter", "Sommer"
- Hvornår er et password komplekst?
  - "**wKERrBgQ#3*p**" vs "**HemmeligHelikopter7913**"
- Skal passwords udløbe?
  - Nej, de skal uddø.
- Overvåg proaktivt
  - Bloker for brugere I "pastebins", kræv altid MFA ved "Impossible travel"

Passwords – Hvad skal vi med dem?

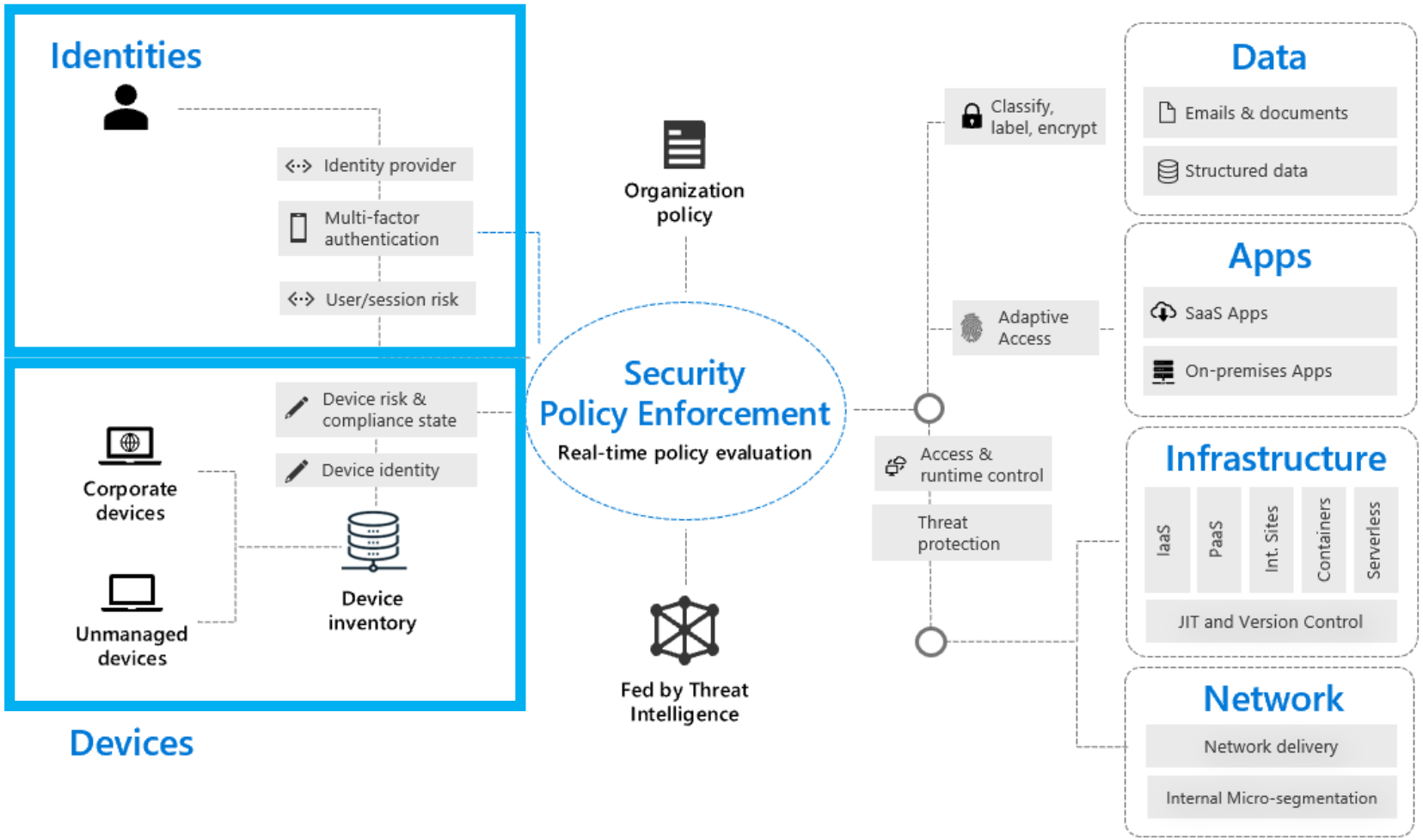
Fido 2

Passwords – Hvad skal vi med dem?

Fido 2 (Fast IDentity Online

- Standard-baseret Password-løs autentifikation
- WebAuthN og CTAP(Client To Authenticator Protocol)
  - Standarder der bruges bredt
- Public/Private Key Infrastruktur
  - Private keys opbevares sikkert på nøglen
- Lokal gestikulation (Biometri, PIN) er påkrævet
- Alt data er bundet til den enkelte nøgle

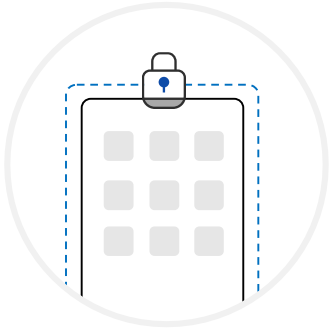
Zero Trust Architecture



Implementing Zero Trust for Mobile Devices

Mobile **Device** Management (MDM)

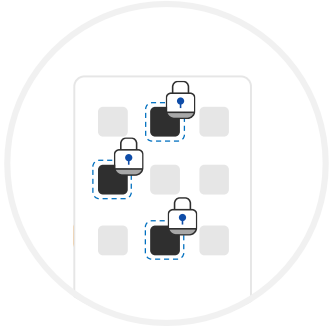
Conditional Access:
Restrict access to managed and compliant devices



- Enroll devices for management
- Provision settings, certs, profiles
- Report & measure device compliance
- Remove corporate data from devices

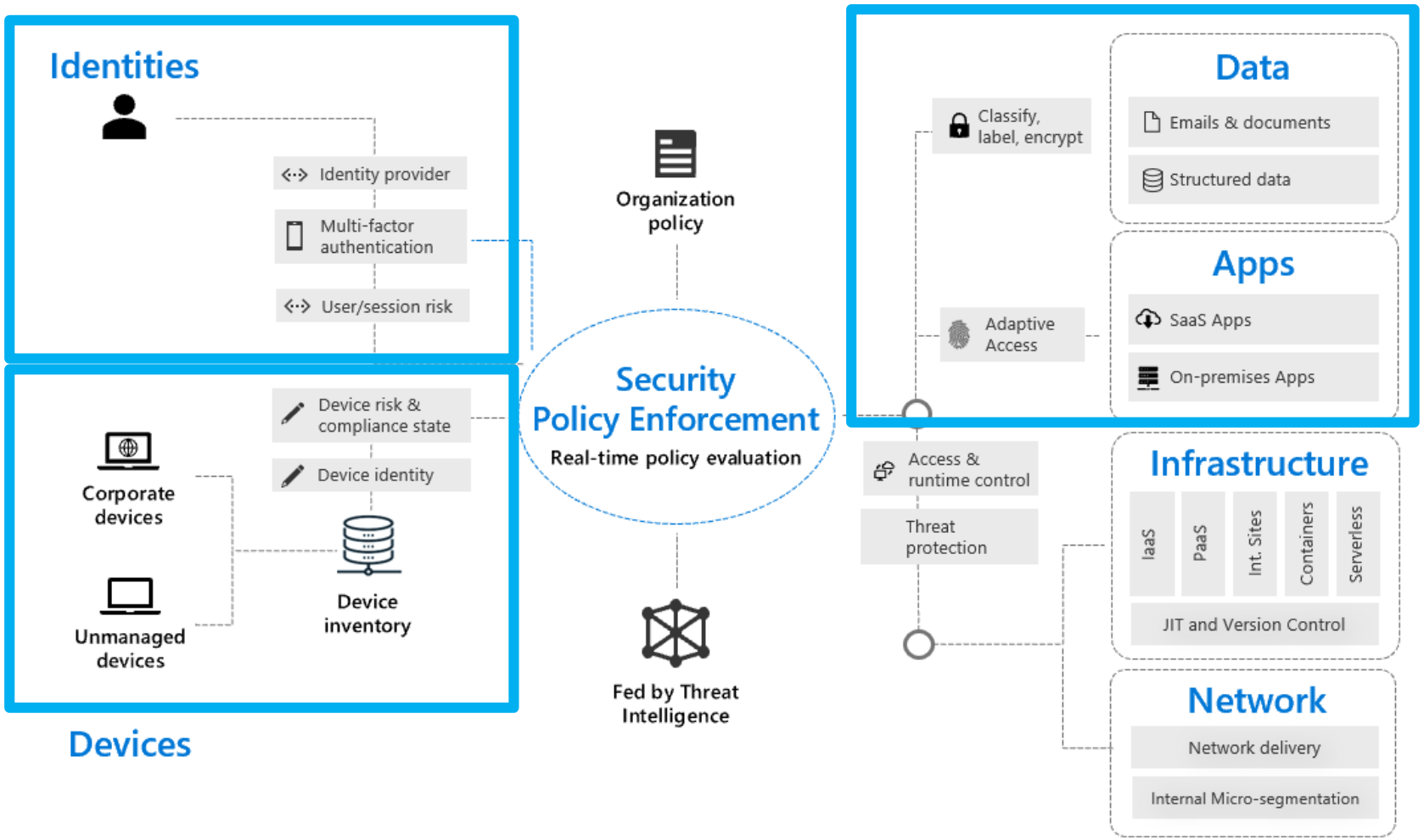
Mobile **Application** Management (MAM)

Conditional Access:
Restrict which apps can be used to access email or files



- Publish mobile apps to users
- Configure and update apps
- Report app inventory & usage
- Secure & remove corporate data within mobile apps

Zero Trust Architecture



Information Protection

Locate and classify information anywhere it lives

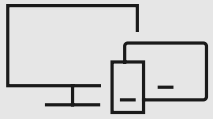
Discover & classify sensitive information

Apply protection based on policy

Monitor & remediate

Accelerate Compliance

Across



Devices

Apps

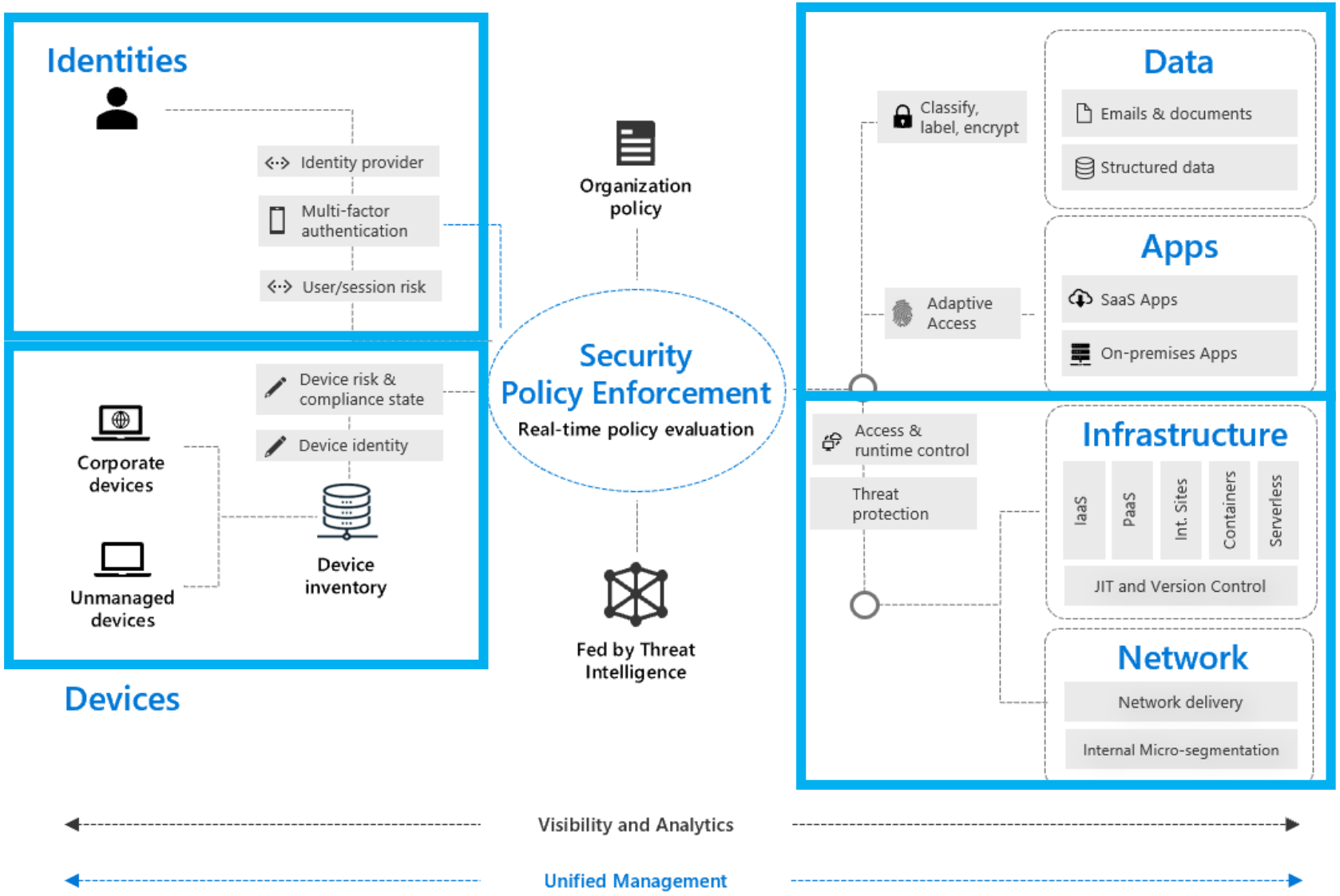
Cloud services

On-premises

Hvordan kan det se ud?

Restricted	• Highly-sensitive information
Confidential	• Sensitive information
Internal	• Non-sensitive information that is not released to public
Public	• Information has been approved for public access

Zero Trust Architecture



Hvordan beskytter man sine administratorer?

Privileged Identity Management

Just in Time Access

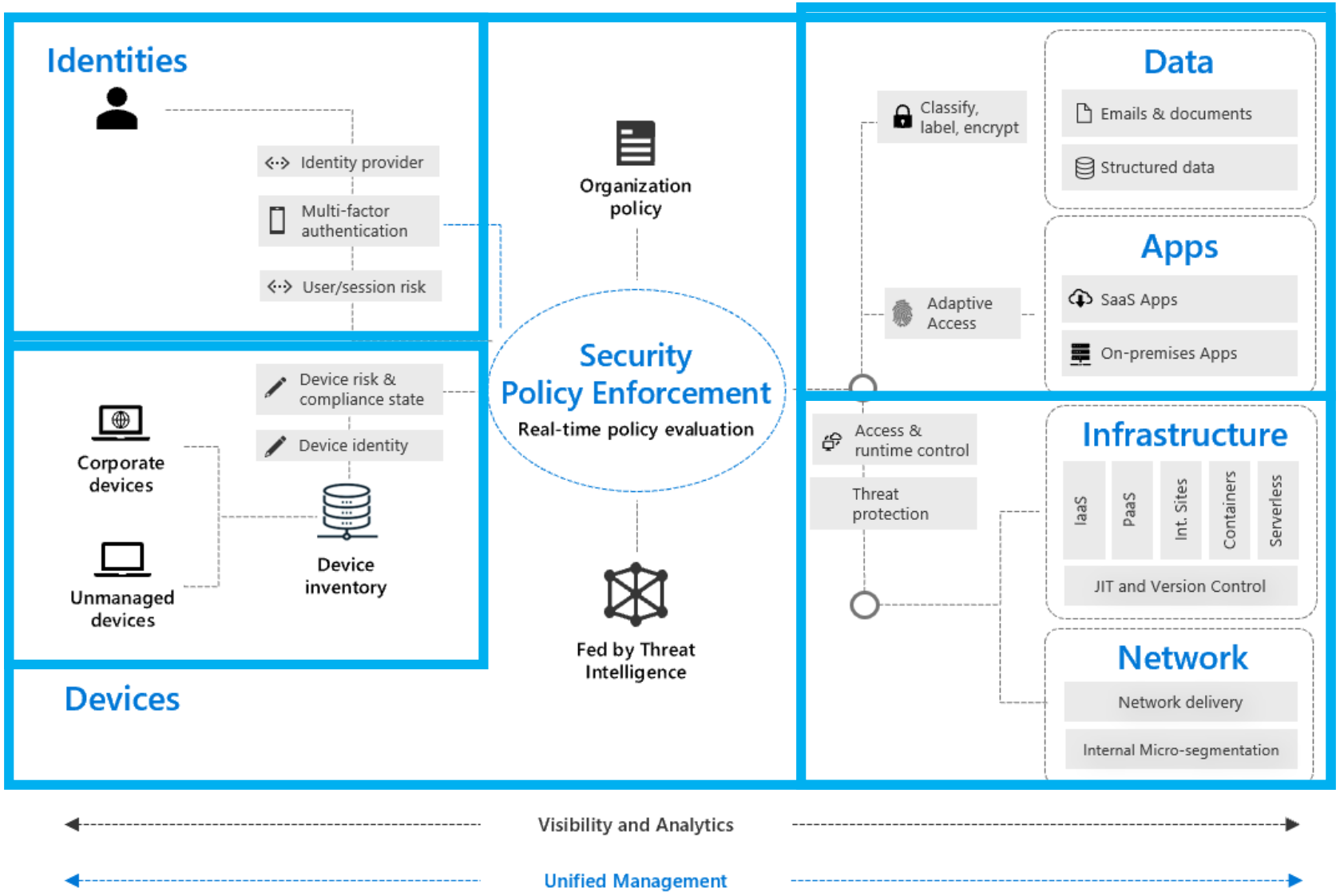
Just Enough Access

Privileged Admin Workflow

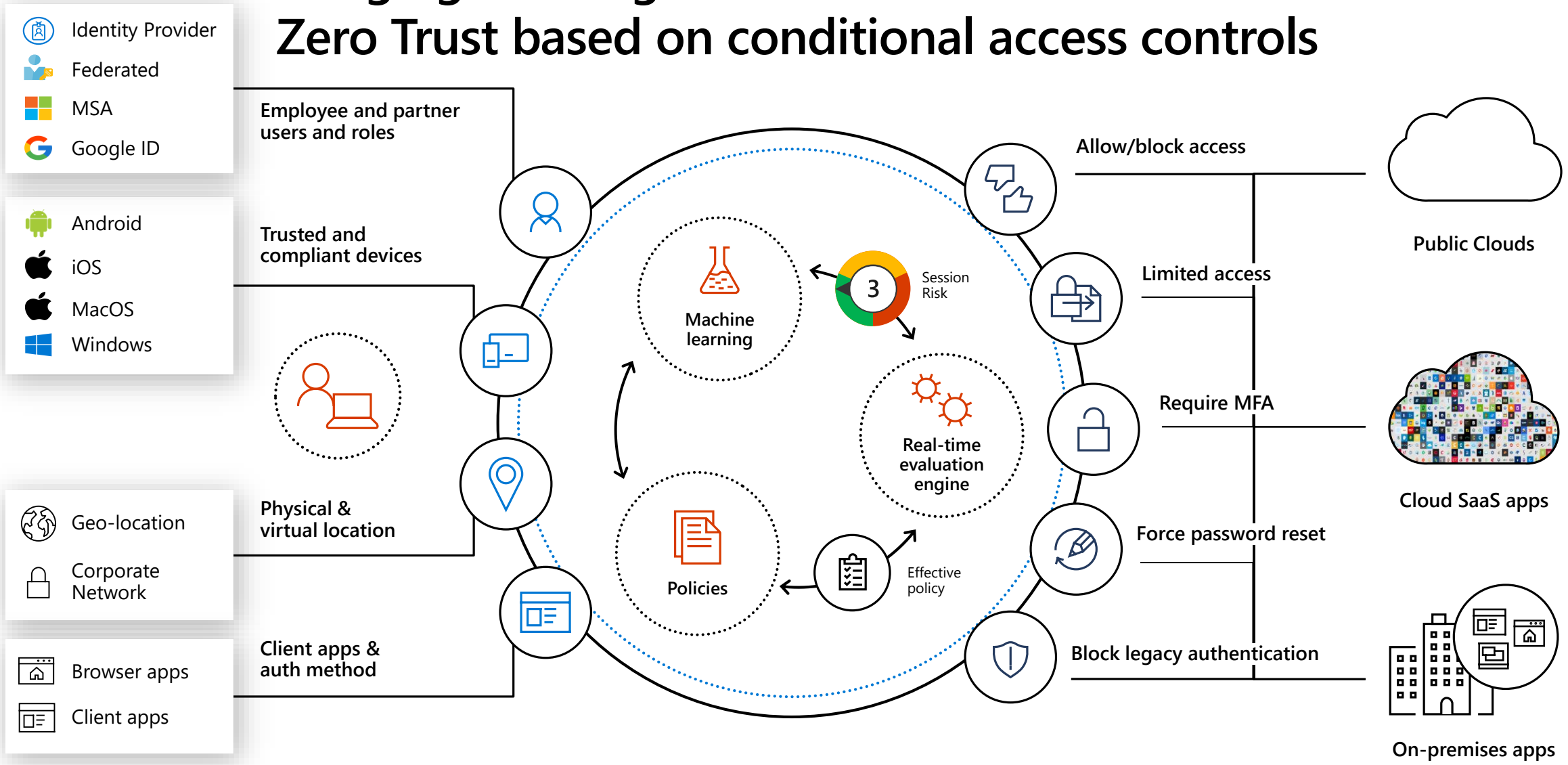
Audit-ready

Protect and control privileged access to your organization

Zero Trust Architecture



Bringing it all together:
Zero Trust based on conditional access controls



Conditions

Controls

Hvordan?

Hvor skal man starte?

Risk	Governance	Design
Bruger bliver kompromitteret	Brugere skal rammes af MFA fra ukendte lokationer	Conditional Access, Identity Protection & MFA
Bruger deler fortrolig data med eksterne	Proces for hvem der må deles med	DLP & Dataklassificering
Admin takeover	Begræns administrative roller.	Priviliged Identity Management & RBAC

?

Pause

Overvågning

Reaktiv eller Proaktiv?

- Har vi ressourcerne til at overvåge?
  - Forskellige løsninger = Forskellige dashboards
- Kan vi automatisere vores overvågning og investigations?
  - CASB, hvad, hvorfor & hvordan?
- Kan vi samle al information I ét system?
  - SIEM – Er det virkeligt så svært at komme i gang med?

Hvad skal vi holde øje med?

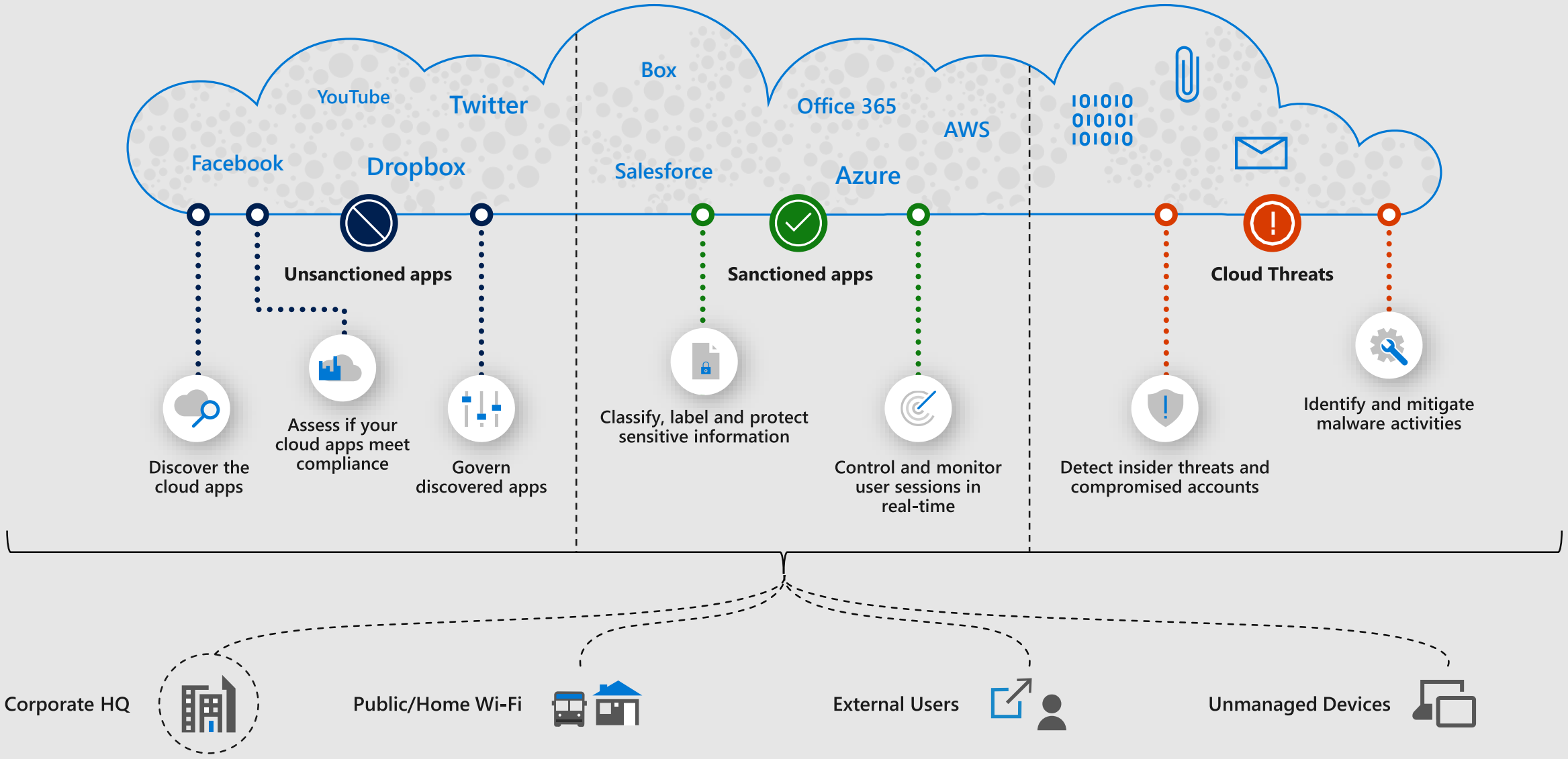
Name	Description
Anonymous IP address	Tor or anonymizer VPNs
Atypical travel	Travel distance > Travel time
Leaked credentials	Valid credentials compromised
Malware linked IP address	Botnet linked IP address
Unfamiliar sign-in properties	Periodicity based unfamiliar properties.
Unfamiliar sign-in properties	Multiple failed sign-ins in a short time period
Admin confirmed user compromised	Admin feedback
Malicious IP address	Valid creds, blocked IP (Sharkfin, etc.)
Impossible travel	Inter / intra session travel (MCAS)
Suspicious inbox manipulation rules	Mailbox manipulation (MCAS)

Proaktiv cloud

Cloud App Security Broker

- Synlighed
  - "Shadow IT" skal frem i lyset – Analyser firewall trafik
  - Hvad laver dine brugere? – Mistænkeligt adfærd
- Compliance
  - Hvor ligger min data?
  - Overholder 3. part vores krav?
- Sikkerhed
  - Forhindrer "risky" bruger adfærd
  - Beskyt data i din cloud – Hvad må gemmes og hvad må hives ud?

TOP CASB USE CASES



Proaktiv cloud

Security Information and Event Management

- Håndtering af logs
  - Central håndtering af log filer – Samt retention
- Korrelation
  - Alarm i system A, kan relateres med alarm i system B
- ”Master Dashboard”
  - Saml alle alarmer i et enkelt dashboard
- Analyser
  - Analyser incidents på tværs af systemer i en visning


Microsoft Azure
Search resources, services, and docs
admin@contoso.com
CONTOSO
Home > Azure Sentinel
Azure Sentinel - Overview
Search (Ctrl+/)
GENERAL
Overview
Logs
THREAT MANAGEMENT
Incidents
Dashboards
User analytics
Hunting
Notebooks
CONFIGURATION
Getting started
Data collection
Analytics
Playbooks
Community
Workspace
Last week (1/21/2018-1/27/2018)
8.2M 978.4K
EVENTS
39 6
ALERTS
18 4
INCIDENTS
INCIDENTS BY STATUS
NEW (7)
IN PROGRESS (4)
CLOSED (RESOLVED) (4)
CLOSED (DISSMISED) (3)
Events and alerts over time
ALERTS 89
CEF 315K
SECURITY EVENTS 121K
AZURE AD 110K
OTHERS (5) 106K
Potential malicious events
MALICIOUS IPS EVENTS 82K
OUTBOUND 4K
INBOUND 78K
Recent incidents
User logged in to critical assets 9 Alerts
Suspicious process execution after co... 9 Alerts
Computers with cleaned event logs 8 Alerts
Remote procedure call (RPC) attempts 8 Alerts
Most anomalous data sources
Azure AD
Office
SecurityEvents
Democratize ML for your SecOps
Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML
Learn more >

?

THINKING YOUR BUSINESS

T: +45 82 32 32 32
M: info@proactive.dk
W: www.proactive.dk

København
Rosenørns Allé 1
DK-1970 Frederiksberg C

Aarhus
Åbogade 15
DK-8200 Aarhus N

Odense
Egelundsvej 18
DK-5260 Odense

Aalborg
Stigsborgvej 60
9400 Nørresundby