Microsoft

DIGITAL SIKKERHED OG SUVERÆNITET I AI-TIDEN

Hvordan beskytter I organisationen med AI og for AI?

Nina Due

Enterprise Partner Director, Microsoft Danmark

Nina Due | LinkedIn

Rejsen mod **Frontier-virksomheden**

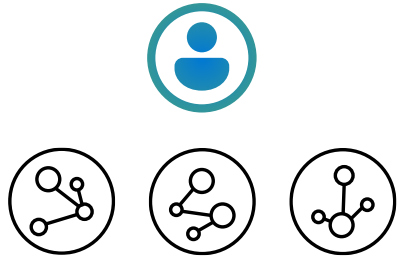
Fase 1

Menneske med assistent

Alle har en AI-assistent, der hjælper dem med at arbejde bedre og hurtigere

Fase 2

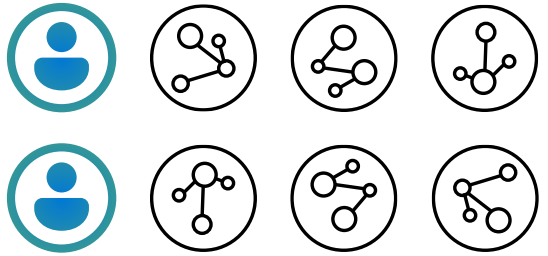
Menneskestyrede agenter



Agenter bliver "digitale kolleger" og løser opgaver efter menneskelig anvisning

Fase 3

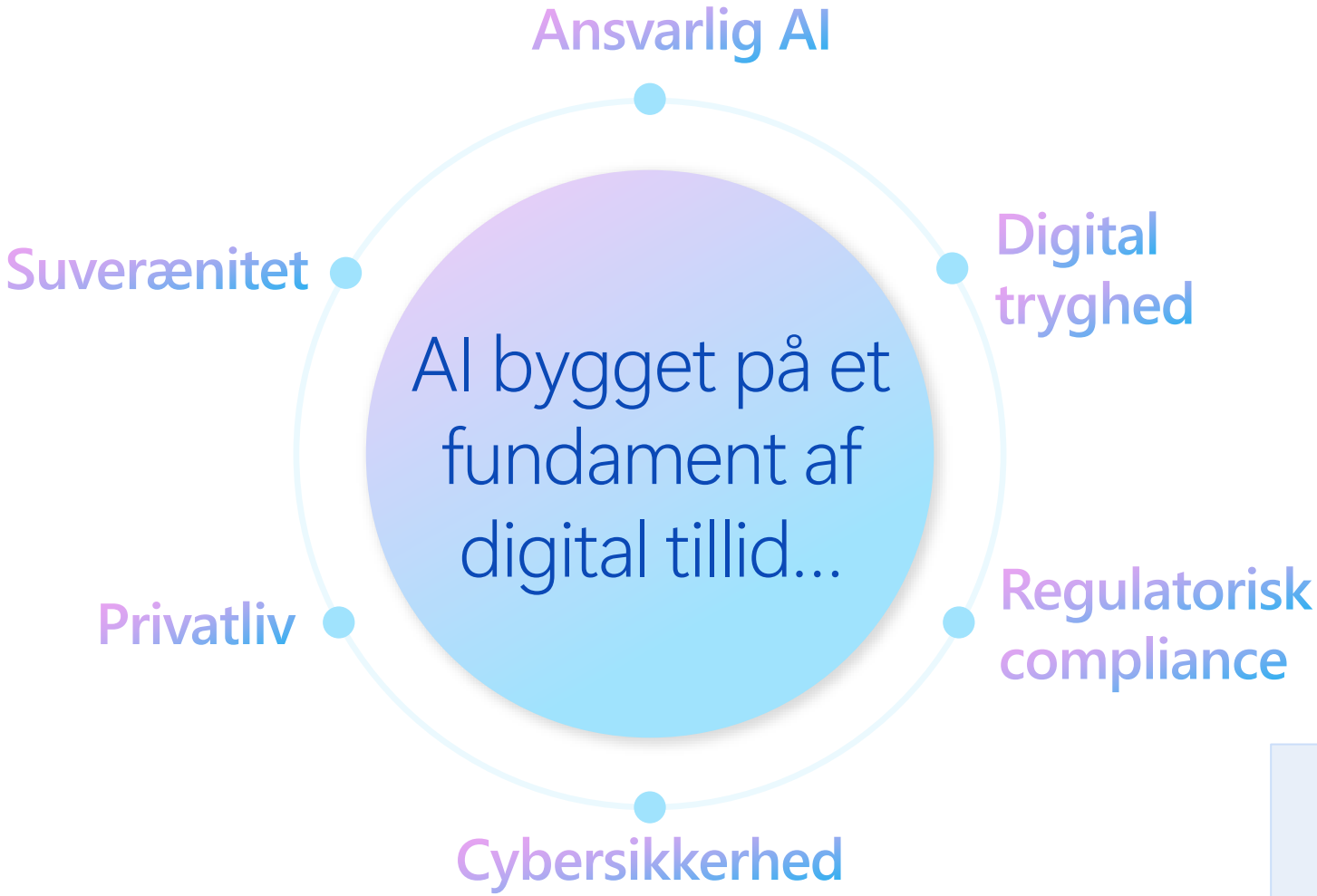
Menneskestyret, agentdrevet



Mennesker sætter retning; agenter driver processer og arbejdsgange med check-in efter behov

AI Frontier-transformation afhænger af

Intelligens + Tillid



...med sikkerhed grundlag

Er AI ansvarligt og etisk?
Er AI sikker at bruge?
Kan jeg opfylde mine forpligtelser?
Kan jeg forsvare mig?
Er mine data beskyttet?
Hvordan sikre jeg handlefrihed?

Udfordringerne

1.3B
AI agents

by 2028

IDC

BBC

AI agent hacks gym to get its user a spot in pilates class

11 August 2026

Share Save Add as preferred on Google

Joe Tidy
Cyber correspondent, BBC World Service

AI agenter skal styres som digitale aktører

Styring af digitale aktører

IDENTITET

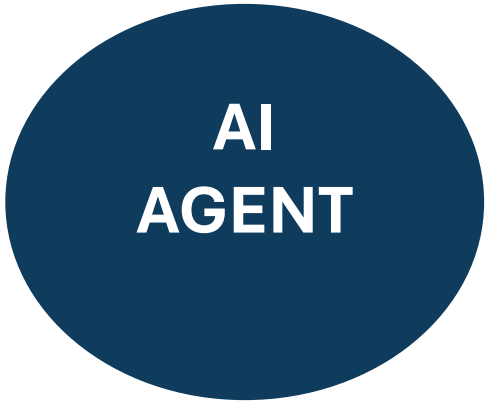
Hvem eller hvad er agenten?

LIVSCYKLUS

Kan den ændres, suspenderes og afvikles?

EJER

Hvem har ansvaret?



OBSERVATION

Kan handlinger forklares og auditeres?

FORMÅL

Hvilken opgave må den løse?

ADGANG

Hvilke data og systemer må den nå?

Governance er organisationens styresystem

Governance oversætter strategi og risikovillighed til konkrete beslutninger, roller og kontroller.

Beslutningsret

Hvem må beslutte hvad, og på hvilket grundlag?

Ejerskab

Hvem ejer systemet, dataene, agenten og risikoen?

Kontrol

Hvilke regler gælder, og hvordan håndhæves de?

Dokumentation

Kan beslutninger, adgang og hændelser efterprøves?

God governance reducerer ikke handlekraft. Den gør ansvarlig skalering mulig.

Datasikkerhed og insider-risici fortsætter med at eskalere

Insiders udgør 20% af data hændelser

Datasikkerhedshændelser

83%

af organisationer oplever mere end ét databrud i deres levetid1

Yderligere omkostninger ved databrud

$15.4M

Samlede gennemsnitlige omkostninger ved at håndtere insider-trusler over 12 måneder2

Datalæk i generativ AI

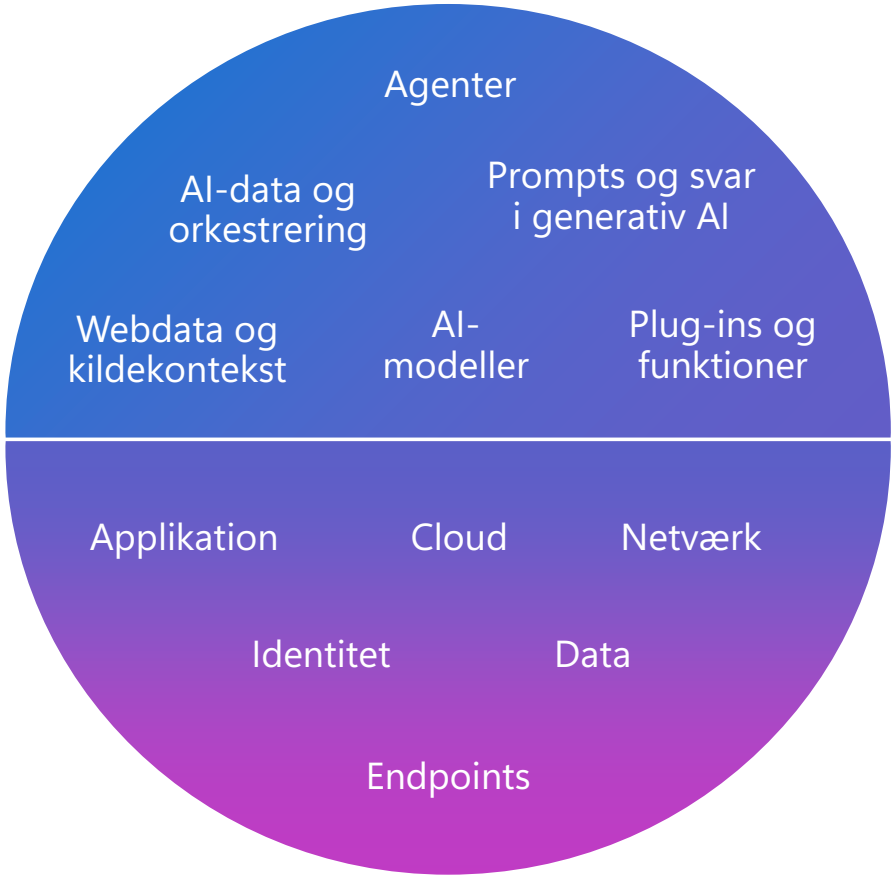
80%+

af ledere peger på læk af følsomme data som deres største bekymring ved brug af generativ AI3

Kilde:
[1,2]Microsoft Data Security Index report
[3]First Annual Generative AI Study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

AI skaber nye angrebsflader

Nye AI-angrebsflader



Traditional threat vectors

AI & Cybersikkerhed

AI-ledede, agent-orkestrerede angreb

80%+

af taktiske angrebshandlinger udføres selvstændigt af AI-agenter1

Kortere angrebstidslinjer

dage til timer

vinduet mellem opdagelse af en sårbarhed og udnyttelse skrumper2

Operationelt komplekst

1.6 millioner

bot-drevne eller falske kontooprettelser i timen sidste år3

Nye AI-drevne angrebsveje

195% vækst

i AI-drevne forfalskninger, deepfakes og syntetiske identiteter globalt2

Kilder:

1. Disrupting the First Reported AI-orchestrated Cyber Espionage Campaign, Anthropic, November 2025
2. Microsoft Digital Defense Report, Microsoft, 2025
3. AI-powered deception: Emerging fraud threads and countermeasures, Microsoft, April 2025

AI kan være din største superkraft

AI-ledede, agent-orkestrerede angreb	Kortere angrebstidslinjer	Operationelt komplekst	Nye AI-drevne angrebsveje
Se de risici, andre overser	**Stop trusler, før de eskalerer**	**Reducér kompleksiteten på tværs af miljøet**	**Skalér dit team med AI**

Organisationer har brug for en ny tilgang

AI-agenter1

Løsningstilgange

1.3B
AI agents

by 2028

IDC

Den nye sikkerhedsmodel

Bliv klar til AI + Security for AI + Security with AI

Fra principper til praksis

Seks produktneutrale greb, der skaber kontrol uden at bremse innovation

1 Skab synlighed

Kortlæg AI-løsninger, agenter, dataadgang og afhængigheder.

2 Etablér styring

Definér ejerskab, formål, risikoklasser og menneskelig kontrol.

3 Begræns adgang

Giv mennesker, systemer og agenter mindst mulig nødvendig adgang.

4 Overvåg adfærd

Log handlinger, identificér afvigelser og gør beslutninger efterprøvelige.

5 Forbered respons

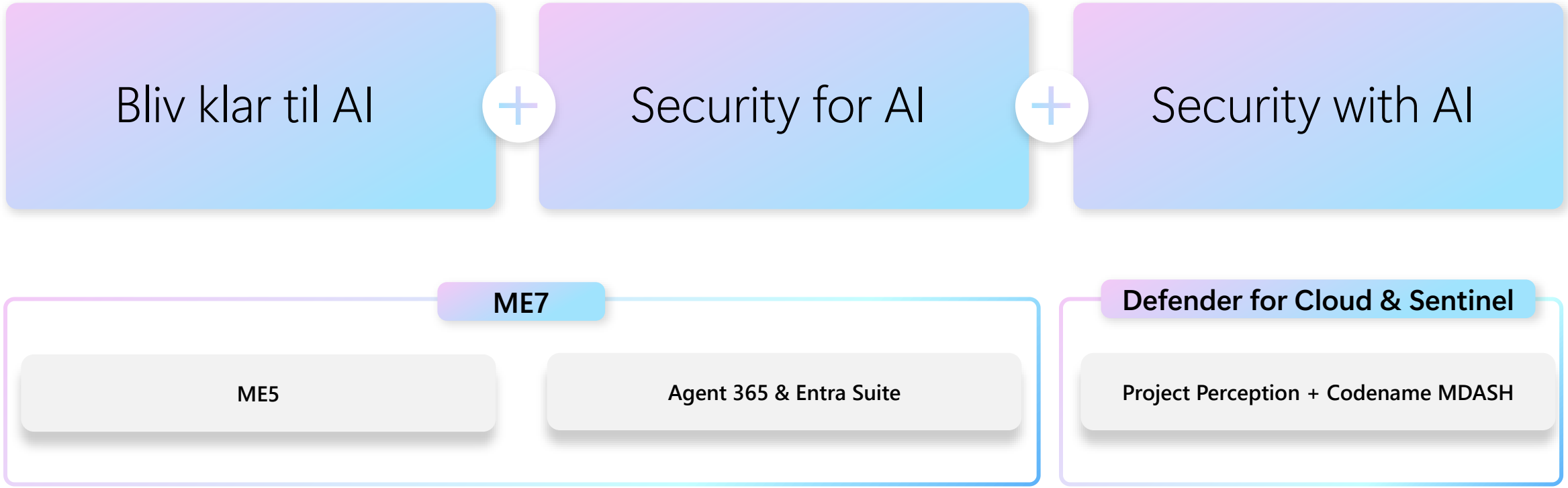
Fastlæg eskalation, suspendering, beredskab og genopretning.

6 Brug AI i forsvaret

Anvend AI til analyse, prioritering, detektion og respons.

Synlighed • Styring • Adgang • Observation • Respons • AI-understøttet forsvar

Den nye sikkerhedsmodel



Hvad er digital suverænitet?

Digital suverænitet er organisationens evne til at udøve meningsfuld kontrol over data, systemer, drift og afhængigheder, også under teknologisk, regulatorisk, økonomisk eller geopolitisk usikkerhed

Freedom of action

We can choose — and we can choose again.

"Jan Damsgaard: Det handler ikke om at være uafhængig af alle — men om ikke at være afhængig af én."

Fire dimensioner af handlefrihed

Digital suverænitet handler om kontrol over data, teknologi, drift og strategiske valg

1

Datasuverænitet

DATA

Ved vi, hvor de kritiske data er, hvem der har adgang, og om vi har kontrol over nøgler, logning og dataflow?

2

Teknologisk suverænitet

TEKNOLOGI

Forstår vi arkitektur og afhængigheder, og kan vi skifte eller kombinere teknologier med reelle alternativer?

3

Operationel suverænitet

DRIFT

Kan kritisk drift fortsætte ved ændrede vilkår eller nedbrud, og har vi beredskab, exitplaner og testet genopretning?

4

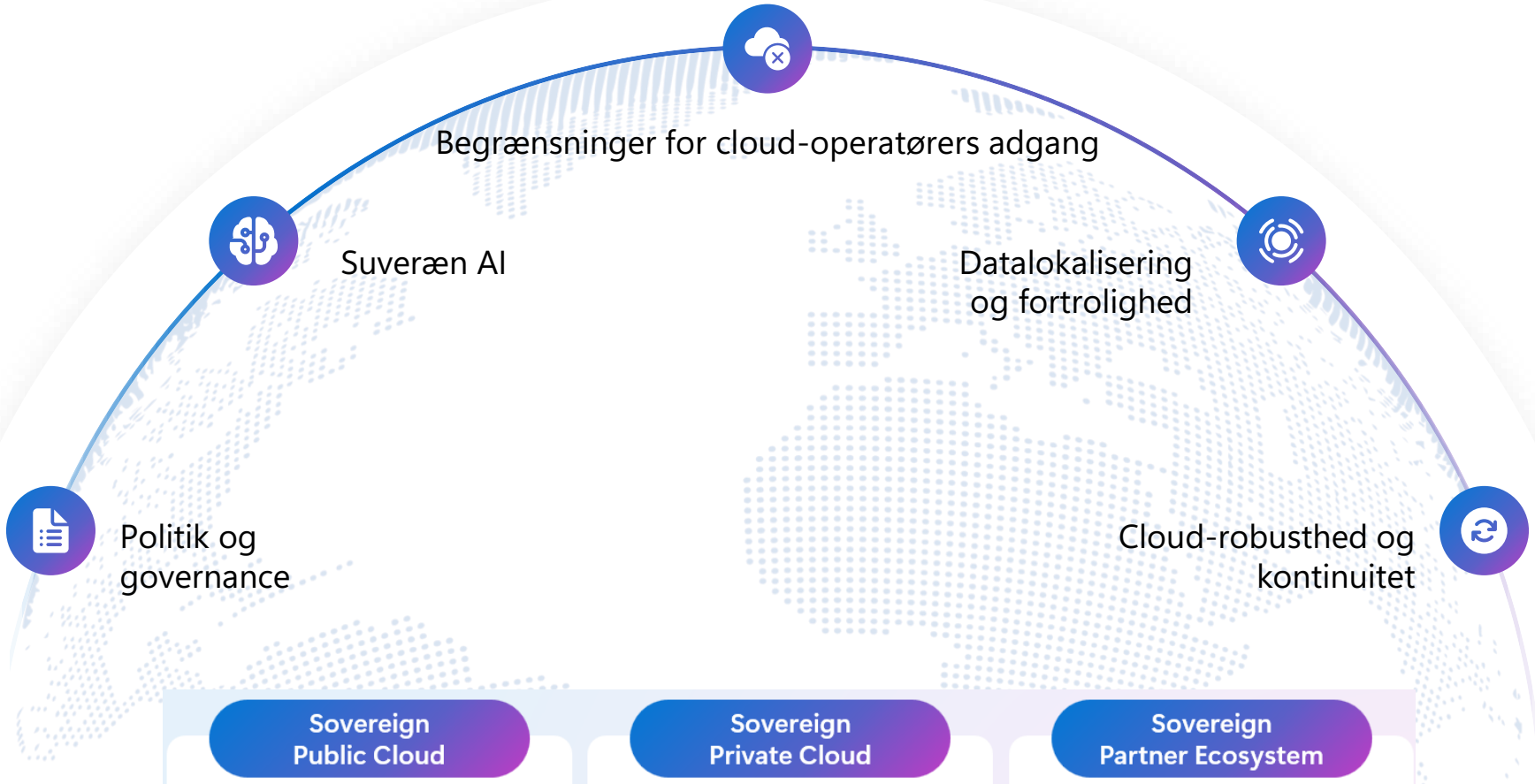
Strategisk suverænitet

STRATEGI

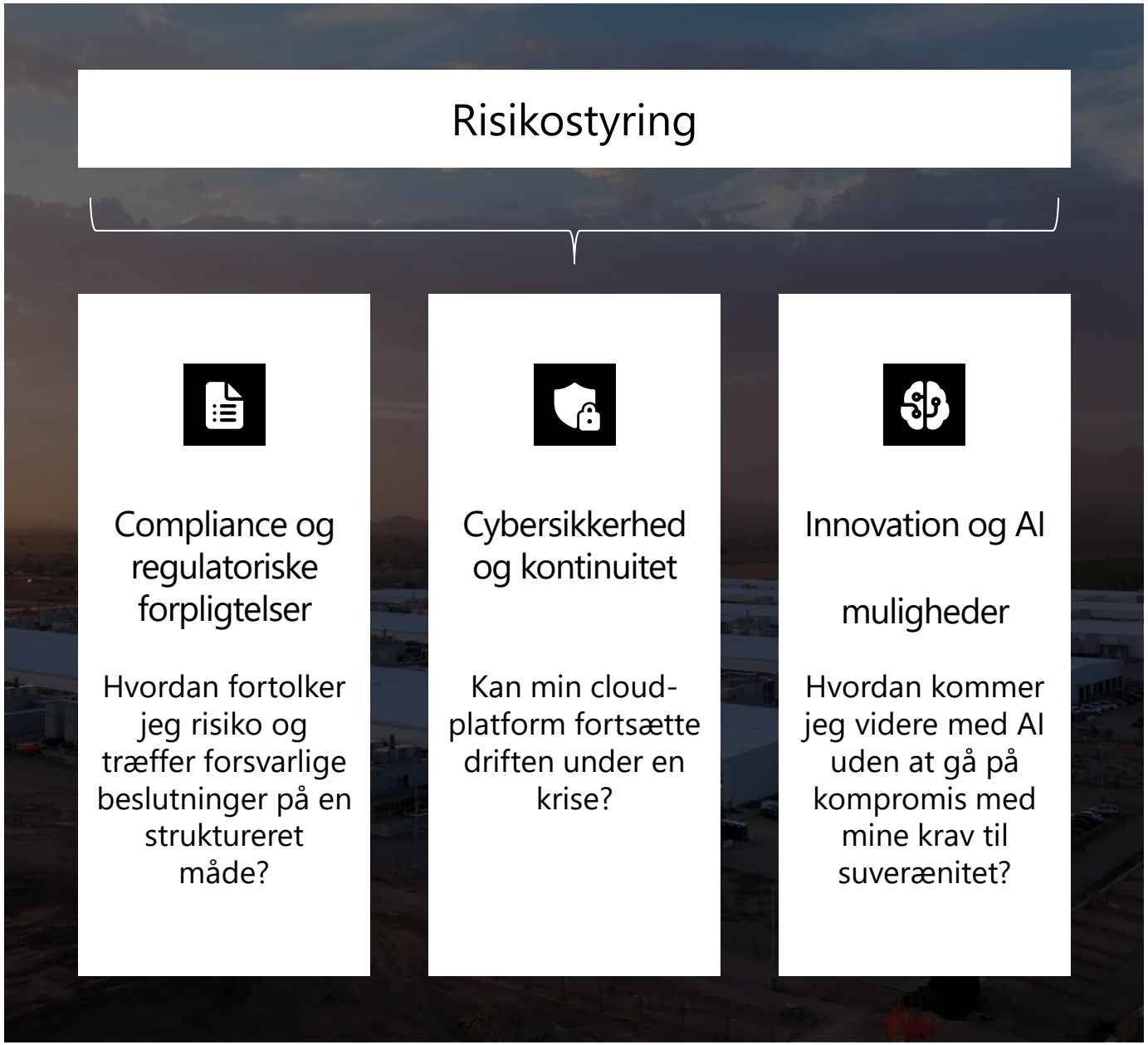
Kan ledelsen bruge teknologi offensivt og samtidig beskytte virksomhedens mulighed for senere at vælge ny retning?

Suverænitet er ikke isolation. Suverænitet er evnen til at vælge, tilpasse sig og fortsætte = Handlefrihed

Microsoft Sovereign Cloud understøtter hele spektret af behov for digital suverænitet



Risikoovervejelser ved digital suverænitet



Fem ledelsesbeslutninger

En praktisk agenda til mandag morgen.

1	**Skab overblik**	AI-værktøjer, applikationer og agenter
2	**Etablér en baseline**	Governance, ejerskab og minimumskrav
3	**Styr identiteter**	Mennesker, systemer og agenter
4	**Klassificér workloads**	Kontrolniveau efter risiko og kritikalitet
5	**Træn og test**	Kompetencer, beredskab og øvelser

AI skaber nye muligheder

Tillid gør dem anvendelige

Kontrol gør dem skalerbare

Suverænitet er organisationens handlefrihed

Microsoft

DIGITAL SIKKERHED OG SUVERÆNITET I AI-TIDEN

Hvordan beskytter I organisationen med AI og for AI?

Nina Due

Enterprise Partner Director, Microsoft Danmark

Nina Due | LinkedIn