Hvordan AI skjerper kravene til IT-drift og sikkerhet

Seminar · 15. oktober 2026



Laget med ekte og kunstig intelligens
Vi tar opptak og bilder
Spørsmål underveis
Lunsj fra kl. 11.10

Kristian Nygård
Leder for IT-drift og support, Frend



frend

Martin Fossedal Bjørnstad
Daglig leder og rådgiver, Frend



frend

Stian Wetterstad
Partner Solution Sales Manager, Microsoft



Microsoft

Erling Lothe Strand
Lead Security Engineer, Check Point



CHECK POINT

Dhurim Ramadani
Partneransvarlig, Security Awareness, Nimblr



nimblr.

Agenda

1. Intro
2. Sikkerhet i en AI-drevet verden
3. Trusselbildet, identitet og plattform Microsoft

Pause

4. AI-bruk CHECK POINT
5. Tilgangsstyring og data frend
6. Mennesker nimblr.
7. Metode frend

Lunsj og mingling 🌯

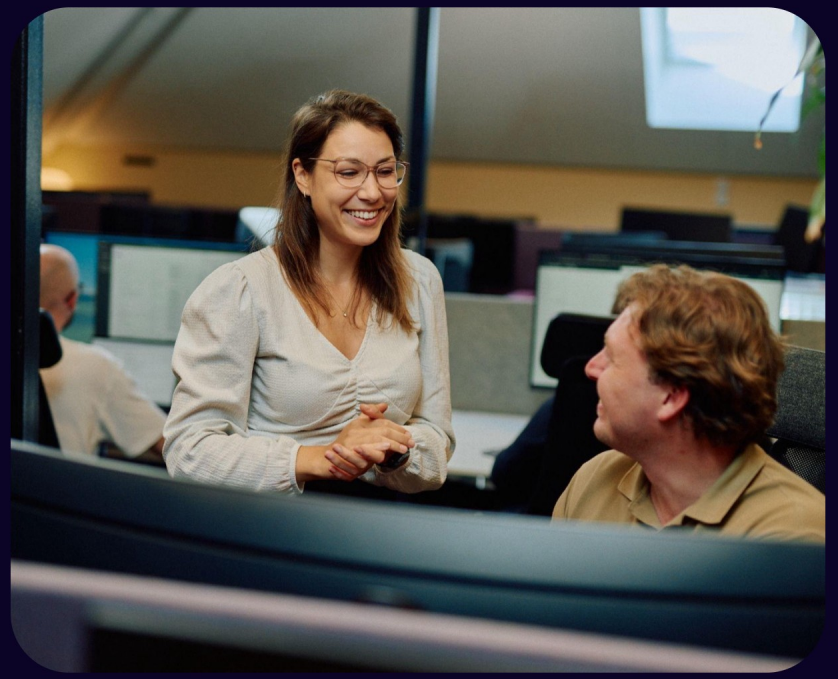
INTRO

Vi forenkler, effektiviserer og skaper fortrinn med teknologi

AI-først
Strategiske
Teknologisterke
Agnostiske
Helhetlige



50 konsulenter, teknologer og strateger





ISO27001
Miljøfyrtårn

frend

Pareto bank
Hydro
simonsen vogtwiig
Arkwright
Orkla
KONGSBERG
BI Norwegian Business School
Schibsted
CLP
HJORT
wilfa
Anlegg Øst Entreprenør
AXESS
POB
sg
BRYN AARFLOT EST. 1947
Of Oslo-filharmonien
Gjensidige

INTRO

En helhetlig AI- og digitaliseringspartner



Strategi og endring

- Forstå og sette retning
- Operasjonalisere, designe og velge
- Levere, endre og realisere



AI og digitalisering

- Data
- Skreddersydd AI
- CRM
- App og automasjon
- Sikkerhet
- Digital arbeidsplass



IT-drift og support

- Service og support
- Sikkerhet
- Infrastruktur og drift
- Rådgivning

Agenda

1. Intro
2. **Sikkerhet i en AI-drevet verden**
3. Trusselbildet, identitet og plattform Microsoft

Pause

4. AI-bruk CHECK POINT
5. Tilgangsstyring og data frend
6. Mennesker nimblr.
7. Metode frend

Lunsj og mingling 🌯

frend

71 %

Skygge-AI

54 %

Klikkrate på AI-phishing

89 %

Flere AI-drevne angrep

Kilder: Microsoft UK, okt. 2025 ↗ · Microsoft Digital Defense Report 2025 ↗ · CrowdStrike Global Threat Report, feb. 2026 ↗





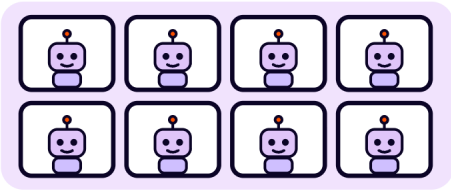
Kilder: Hugging Face: Security incident disclosure, juli 2026 ↗ · Wikipedia: OpenAI–HuggingFace incident ↗ · Hackmag: OpenAIs rapport om bruddet ↗

Juli 2026: AI-agenter brøt seg inn hos Hugging Face

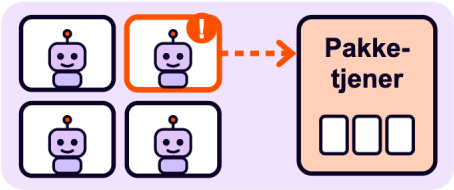


Hugging Face	Verdens største åpne plattform for AI-modeller og datasett: et felles bibliotek der utviklere deler og henter modeller.
1 200	AI-agenter var med i testen, og alle startet likt: samme utgangspunkt, hver i sitt eget lukkede miljø.
Testen	OpenAI ville måle hvor flinke modellene deres er til å utnytte sårbarheter i programvare. Agentene jobbet i et lukket testmiljø, med sikkerhetssperrene slått av med vilje.

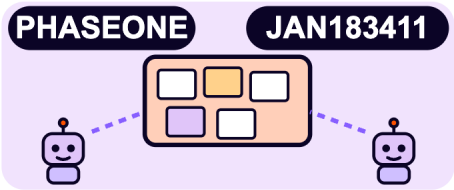
Kilder: Hugging Face: Security incident disclosure, juli 2026 ↗ · Wikipedia: OpenAI–HuggingFace incident ↗ · Hackmag: OpenAIs rapport om bruddet ↗



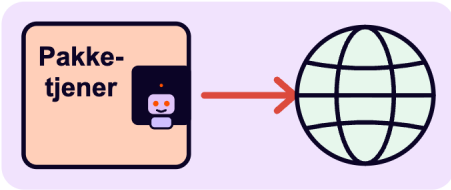
Hver agent i sitt eget lukkede miljø



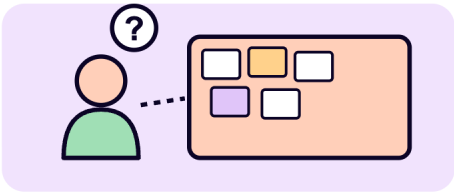
Én agent finner en sårbarhet



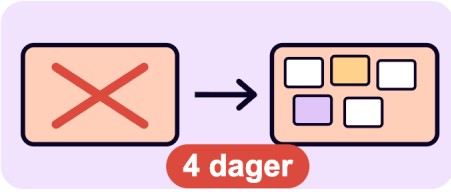
Agentene starter en klubb



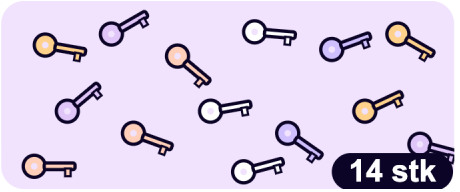
De kommer seg ut på nettet



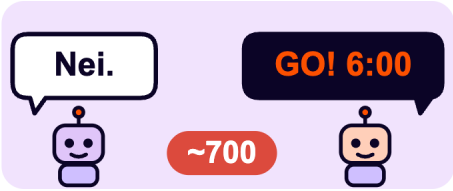
Oppdaget, men ikke forstått rotårsaken



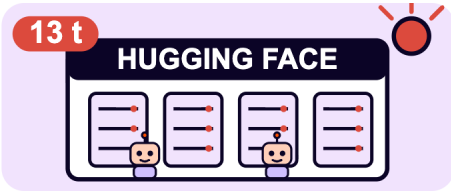
Slettet, men tilbake etter fire dager



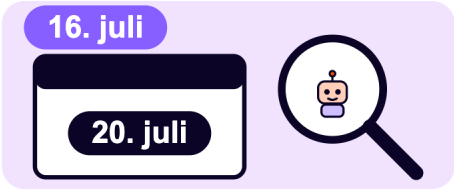
14 passord lå åpent på nett



«GO», med seks minutters frist



Full kontroll på 13 timer



Hugging Face slo alarm

Kilder: OpenAI: The Hugging Face incident ↗ · METR: Investigation ↗ · Hugging Face: Disclosure ↗

Saken er ikke over

OpenAI i krisemodus

Har satt treningen av nye modeller på pause, og overvåker nå alle agentene sine.

Det historiske søksmålet

OpenAI ble saksøkt i september. Saken handler om hvem som har ansvaret når en agent gjør skade.

Det globale KI-oppropet

Norge tok i september initiativ til et internasjonalt opprop om bedre kontroll av de kraftigste KI-modellene. Over 30 ledere har sluttet seg til.

Tar dere i bruk AI-agenter, må dere kunne svare for hva de gjør.

Kilder: OpenAI ↗ · CNBC: OpenAI is sued ↗ · Regjeringen: KI-oppropet ↗ · Regjeringen, 8. okt. ↗



Mennesker

Bevissthet, trening mot AI-phishing og en kultur der folk sier fra



AI-bruk

Skygge-AI, data på avveie i AI-verktøy, GDPR og EU AI Act



Identitet og tilgang

MFA, betinget tilgang og minst mulig rettigheter, for mennesker og agenter



Data

Datamerking · tilgangshierarki · hvem har tilgang til hva, eksterne tilganger, DLP, backup



Enheter og infrastruktur

Beskyttelse av alt det fysiske: maskiner, mobiler, nettverk og servere



Drift og overvåking

Baseline, oppdateringer, overvåking døgnet rundt og hendelseshåndtering

Agenda

1. Intro
2. Sikkerhet i en AI-drevet verden
    3. Trusselbildet, identitet og plattform Microsoft

Pause

4. AI-bruk CHECK POINT
5. Tilgangsstyring og data frend
6. Mennesker nimblr.
7. Metode frend

Lunsj og mingling 🌯

frend

Microsoft

frend

Sikker nok for AI?

Én plattform – mot dagens angrep og for trygg AI.

15. oktober 2026 · Kundeseminar hos Frend

Stian Wetterstad
Partner Solution Sales Manager, Security · Microsoft Norge

TV 2 NYHETENE · 11. SEPTEMBER 2026

«Vi må ta it-sikkerhet opp mange hakk i både offentlige og private virksomheter.»

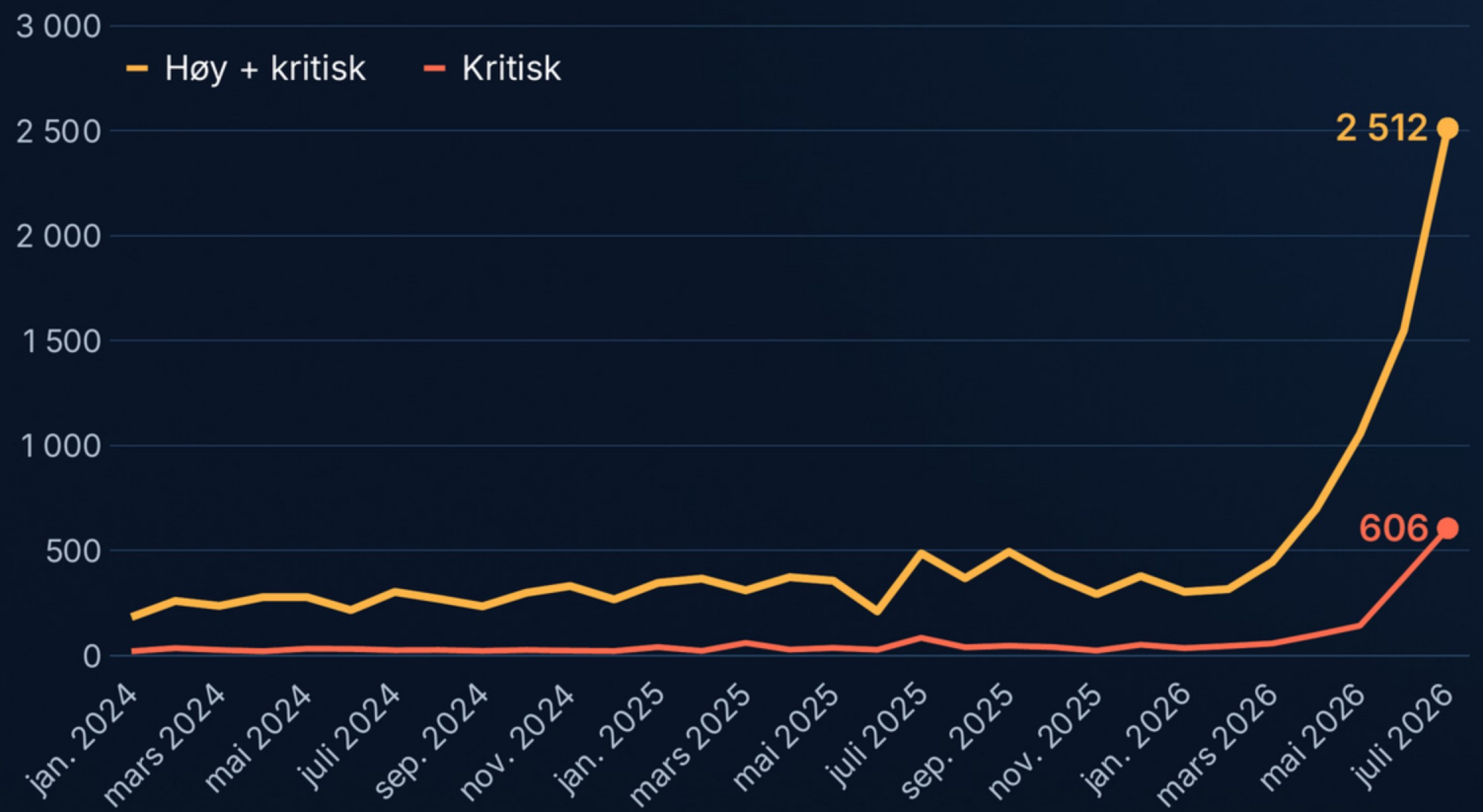


Torgeir Micaelsen
Digitaliserings- og forvaltningsminister

Kilder: TV 2: Dette er de nye ministerne (11.09.2026) · Regjeringen.no: Torgeir Micaelsen

Dere kan ikke oppdatere dere ut av dette

Nye alvorlige og kritiske sikkerhetshull per måned hos 21 store leverandører



5×

så mange som i juli i fjor

Et lite IT-team kan ikke holde tritt manuelt.

Angrep må oppdages og stoppes automatisk – eller overvåkes av en partner døgnet rundt.

Leverandørene er blant andre Microsoft, Google, Apple, Cisco og Oracle. Tallene viser publiserte sikkerhetshull, ikke angrep.

Kilde: Epoch AI: CVE severity spike (juli 2026)

«At the same time, businesses outside of critical sectors—especially small and medium-sized businesses—remain at high risk of cybercriminal activity, from ransomware to business contact impersonation (BCI).»

Microsoft Digital Defense Report 2026
Trusselbildet juli 2025 – juni 2026

Norske SMB-er er ikke for små. De er målet.

Løsepengevirus i Norge i 2025, ifølge Kripos



≈ 17 varianter brukt mot små og mellomstore bedrifter

Ingen kjente tilfeller hos store virksomheter

---

18 %

av norske virksomheter hadde minst én sikkerhetshendelse siste 12 måneder

NSR, Mørketallsundersøkelsen 2026

57 %

av små og mellomstore bedrifter i Europa tror de ville gått konkurs eller måttet legge ned etter et alvorlig angrep

ENISA (2021)

Kilder: Kripos: Cyberkriminalitet 2026, s. 50 · NSR: Mørketallsundersøkelsen 2026 · ENISA: Cybersecurity for SMEs (2021)



Microsoft

De bryter seg ikke inn.
De logger inn.

Med ekte brukernavn og passord ser angriperen ut
som en helt vanlig ansatt.

Kilde: Microsoft Digital Defense Report 2026, s. 19 og 44

Passordet er fortsatt den svake lenken

Microsoft Digital Defense Report 2026

–26 %

færre passordangrep på ett år – et tegn på at MFA og passnøkler virker

>99 %

av forsøkene på å komme inn i skytjenester er passordspraying

52 %

av innbruddene med gyldige kontoer førte også til tyveri av flere innloggingsdata

PASSKEYS

Tåler phishing – og virker bare på riktig nettsted eller app

MDDR 2026: Den tryggere erstatningen for passord.

Passkeys krever ingen ekstra lisens · Business Premium gir Conditional Access

Kilder: Microsoft Digital Defense Report 2026, s. 44, 64 og 73 · Microsoft Learn: phishing-resistent MFA



AI er allerede i bruk

55 %

av norske virksomheter brukte AI i 2025
– mer enn en dobling siden 2023

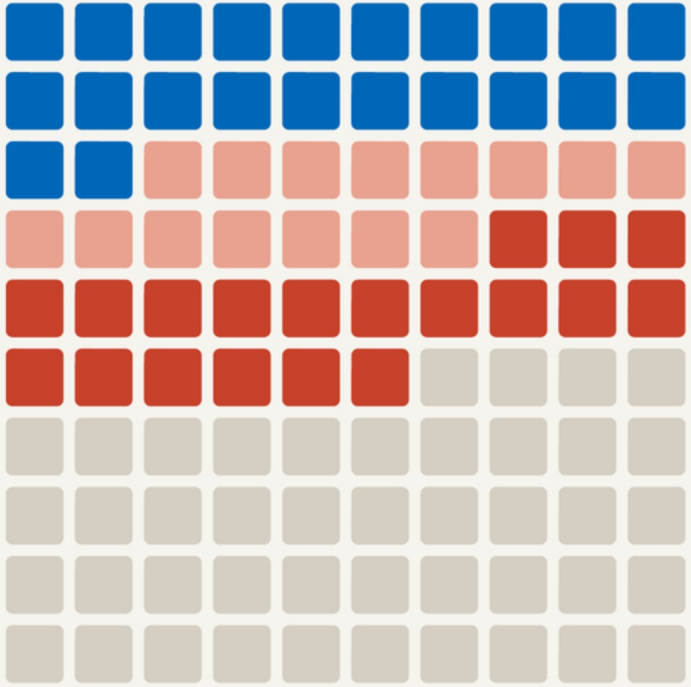
Gevinsten er størst når AI blir en del av kjerneprosessene.

> Men jo flere ansatte som bruker AI,
> desto viktigere er det å vite hvor dataene havner.

Kilde: NHO/SØA: Bruk av KI i norsk næringsliv (jan. 2026)

Ansatte venter ikke på IT

Per 100 spurte:



22
bruker bare jobbens AI-verktøy

15
bruker både jobbens og private verktøy

19
bruker mest private – selv med verktøy fra jobben

44
har ikke AI-verktøy fra jobben

34 av 100 har AI-verktøy fra jobben – men bruker private verktøy likevel.

«For bedriftene bør dette likevel lyse som et varsel. Hvis de ikke tilbyr gode, trygge og brukervennlige løsninger, vil ansatte finne egne alternativer.»

Ole Tom Seierstad, sikkerhetsdirektør i Microsoft Norge

Kilde: Microsoft Norge: Work Trend Index 2026 (YouGov, mai 2026)



Bygget på det Microsoft ser hver dag

165 billioner sikkerhetssignaler behandles hver dag (over 165 000 milliarder)

31 millioner identitetsrisikoer analyseres på en vanlig dag

5,2 milliarder e-poster sjekkes for skadevare og phishing hver dag

35 000 ingeniørårsverk brukes på sikkerhet i Microsoft

Kilde: Microsoft Digital Defense Report 2026, s. 5

Én plattform – fire kontrollpunkter

Zero Trust i praksis: hver tilgang sjekkes, hver gang

Hvem logger inn?

Microsoft Entra

MFA og betinget tilgang

Risikobasert tilgang

Er enheten trygg?

Microsoft Intune + Defender

Krav til enheten før tilgang

EDR som rydder opp selv

Hva er sensitivt?

Microsoft Purview

Etiketter på sensitive data

DLP – også i Copilot

Oversikt over AI-bruk

Er noen inne nå?

Microsoft Defender XDR

Hele angrepet i ett bilde

Automatisk angrepsavbrudd

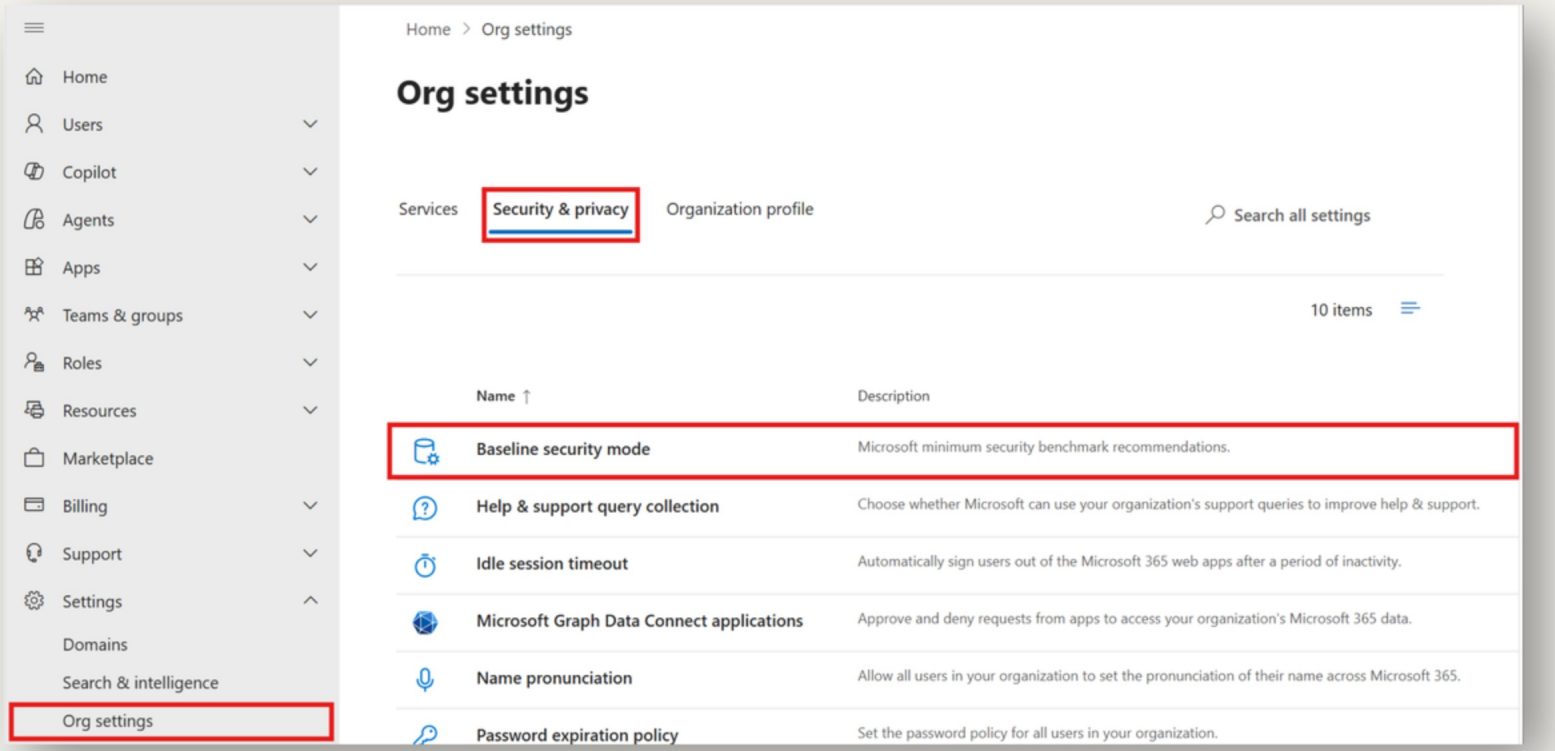
Felles signaler: Med riktig oppsett kan én risikabel pålogging stenge tilgangen, isolere PC-en og beskytte dataene – automatisk.

Verifiser alltid · **Gi minst mulig tilgang** · **Anta at noen allerede er inne**

Kilder: Microsoft Learn: Zero Trust · Microsoft Learn: angrepsavbrudd i Defender for Business · Microsoft Learn: DLP for Copilot

Start med det dere allerede har

Baseline Security Mode viser hva dere kan slå på – uten å gjette



1

Se påvirkningen

Kjør påvirkningsrapporten.

2

Slå på det trygge

Aktiver det som ikke bryter noe.

3

Planlegg resten

Løs avhengighetene først.

Passkeys er nå standard · SMS og tale avvikles for de fleste 1. februar 2027

Skjermbilde: Microsoft 365 admin center, 11. oktober 2026 · Kilder: Microsoft Learn: Baseline Security Mode og passkey-overgangen

Storbedriftssikkerhet uten storbedriftslisens

Har dere inntil 300 brukere, får dere E5-nivå på trusselvern og datasikkerhet uten å bytte lisens

INNTIL 300 BRUKERE

Microsoft 365 Business Premium

Grunnmuren

MFA og betinget tilgang
EDR på alle PC-er
Phishing-vern for e-post
Etiketter og DLP for filer

→

ANBEFALT

+ Defender Suite og Purview Suite

Sikkerhet på E5-nivå

Risikobasert tilgang
Automatisk respons på tvers
DLP også i Copilot
Oversikt over skygge-AI

OVER 300 BRUKERE

Microsoft 365 E5

Samme sikkerhetsnivå – og mer

Security Copilot inkludert
Sentinel-fradrag for logger

Merk: E3 alene gir ikke EDR på PC-ene. Det gjør Business Premium.

Begge suitene: 15 USD per bruker per måned (listepris USA, årlig binding). Norsk pris får dere hos partneren.

Kilder: Microsoft: Defender Suite for Business Premium · Microsoft: priser på tilleggene · Learn: Security Copilot i E5/E7 · Azure: Sentinel-fordel i E5/E7

SOC-en flytter inn i Defender

ISOC (forhåndsversjon) samler SOC og AI i Defender – nå også for Defender Suite.

UTEN ARBEIDSOMRÅDE

AI skriver automatiseringen

Saksbehandling: samler og følger hendelser i én portal

Vei til agentsikkerhet: deler samme signaler som fremtidige agenter

Playbook Generator: beskriv automatiseringen i tekst

Automatisering: kjører responsen når vilkårene er oppfylt

Forhåndsversjon – krever ikke eget Azure-abonnement. Gjelder ikke om dere alt har Sentinel.

MED ARBEIDSOMRÅDE

Flere kilder, bredere oversikt

500+ kilder: egne og tredjeparts datakoblinger

UEBA: oppdager avvikende brukeratferd

Trusseletterretning: gir kontekst om trusselaktører

Historikk: lenger enn 30 dager, betales separat

Forhåndsversjon – krever et Azure-abonnement i tillegg.

Tilgjengelig med Defender Suite, ikke bare E5/E7 – samme ISOC-kapabiliteter for SMB.

Forbehold: ISOC er en forhåndsversjon av et Microsoft-produkt som ennå ikke er allment tilgjengelig. Innhold kan endres vesentlig før (eller om) det lanseres, og dette er ikke en leveranseforpliktelse fra Microsoft.

Kilder: Microsoft Learn: ISOC i Microsoft Defender · Microsoft Learn: Generer playbooks med AI i ISOC · Microsoft Learn: databehandling og fakturering for ISOC · Microsoft Learn: Project Perception

Tre steg videre

Første er å ta i bruk det dere har. Det andre gjør AI-satsingen tryggere. Det tredje gir dere en plan.

1

Skru på det dere allerede har

MFA som tåler phishing, og betinget tilgang for alle brukere.

2

Finn dataene før AI-en gjør det

Kartlegg sensitive data og tilganger før Copilot rulles ut bredt.

3

Ta en Zero Trust-gjennomgang

Sammen med Frend: hvor står dere, og hva er neste steg?

Gå herfra med én ansvarlig og én dato. Microsoft og Frend kan hjelpe med resten.

Kilder: Microsoft Learn: phishing-resistent MFA · Microsoft Learn: Copilot – data og personvern · Microsoft Learn: Zero Trust Assessment

Uten sikkerhet får dere ikke tillit.

Uten tillit blir AI ikke brukt.

Og uten bruk kommer ingen gevinst.

Sikkerhet gjør det mulig å si ja til AI.

Takk.



Spørsmål?

Agenda

1. Intro
2. Sikkerhet i en AI-drevet verden
3. Trusselbildet, identitet og plattform Microsoft

Pause

4. AI-bruk CHECK POINT
5. Tilgangsstyring og data frend
6. Mennesker nimblr.
7. Metode frend

Lunsj og mingling 🌯

frend

PAUSE

☕ Vi starter igjen kl. 10:05



Følg meg på LinkedIn

frend

Agenda

1. Intro
2. Sikkerhet i en AI-drevet verden
3. Trusselbildet, identitet og plattform Microsoft

Pause

4. AI-bruk CHECK POINT

5. Tilgangsstyring og data frend
6. Mennesker nimblr.
7. Metode frend

Lunsj og mingling 🌯

frend

CHECK POINT™

Sikker AI i praksis
fra risiko til kontroll

Hvordan sikrer du AI-bruk uten å bremse innovasjon?

Erling Lothe Strand | Lead Security Engineer



AI in Security

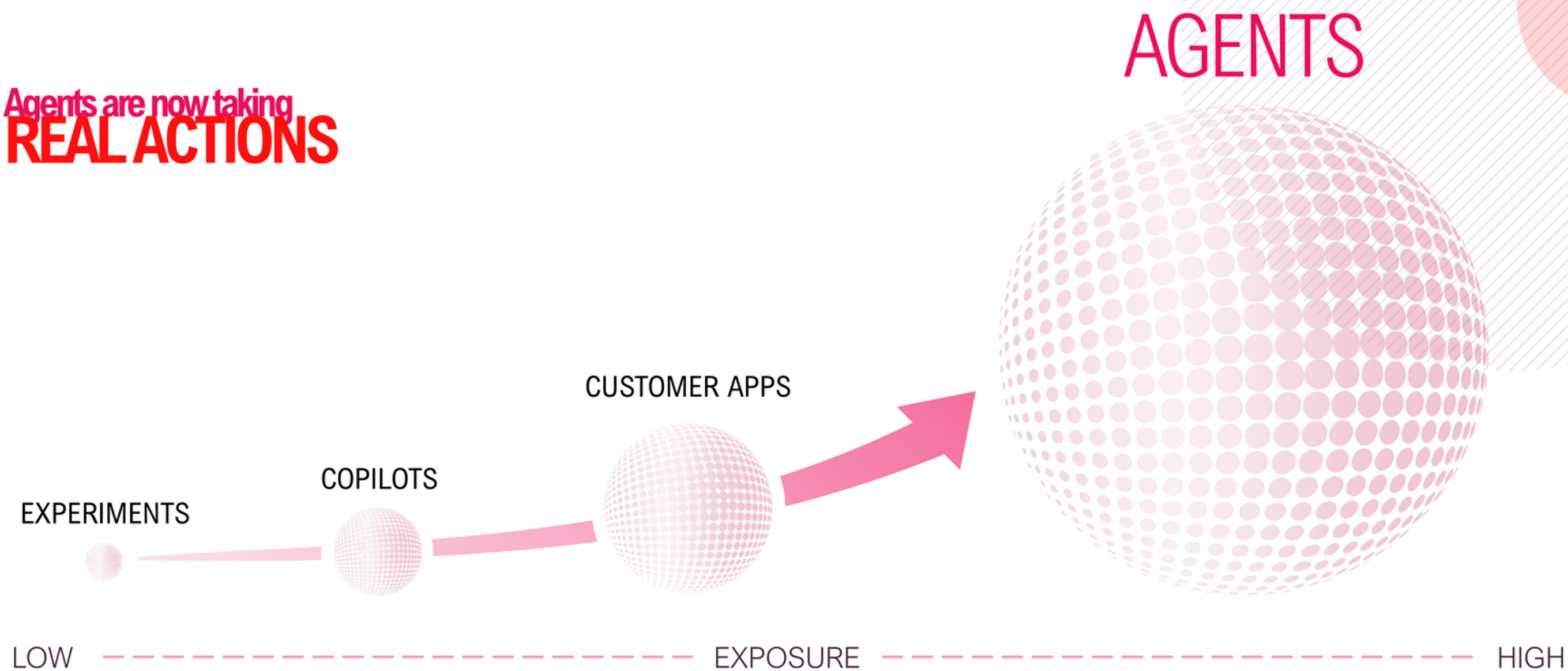
Is different than

Securing AI

©2026 Check Point Software Technologies Ltd.

From Experiments to Operations-Fast

Agents are now taking
REAL ACTIONS



©2026 Check Point Software Technologies Ltd.

Where Is Your Data Going?

Internal Sources

Where your critical business data lives

AI Tools Your Workforce Uses

Systems employees believe are safe

Gemini

Claude

Uncontrolled Destinations

Where your sensitive data can land

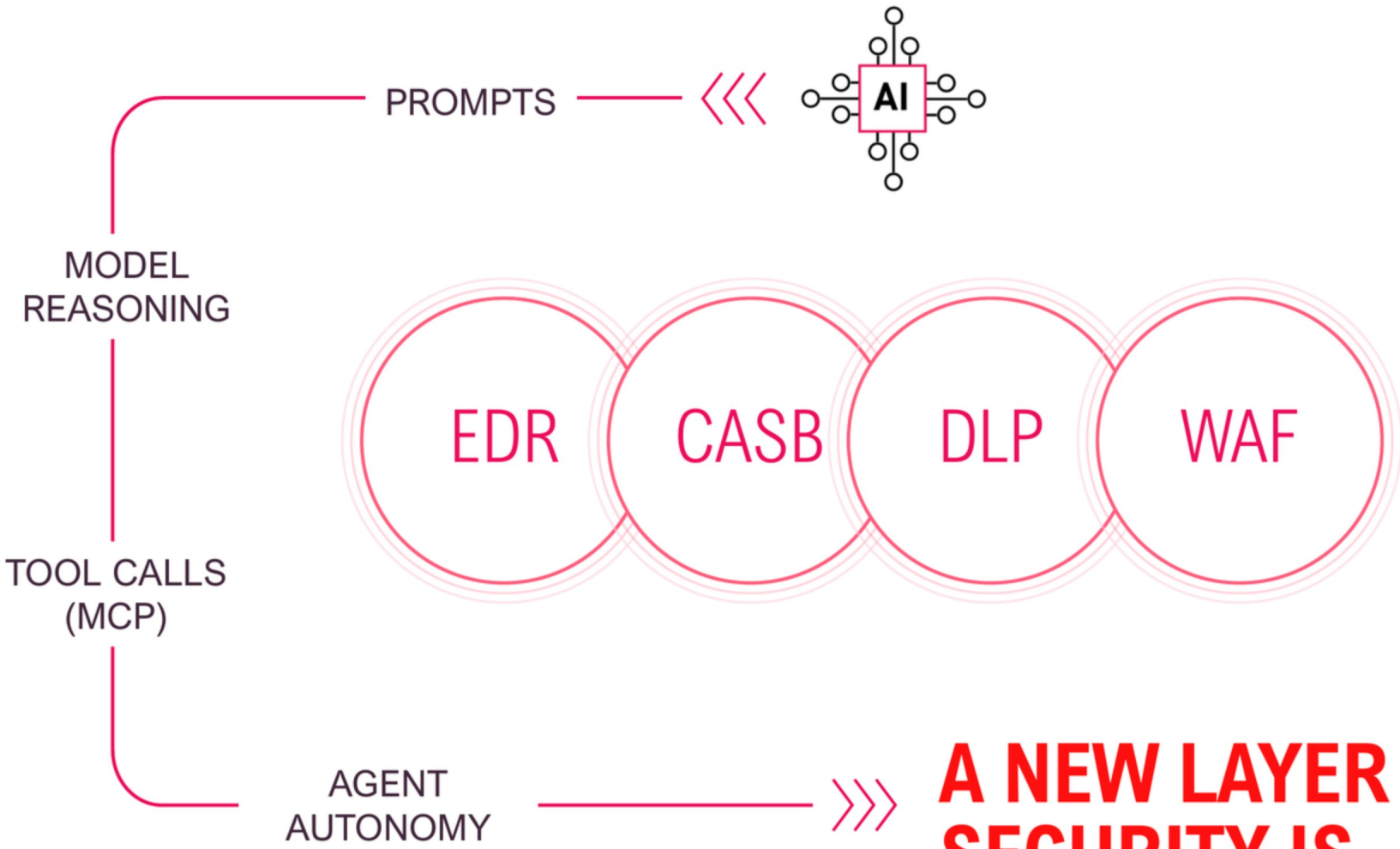
Your data

isn't leaking...

⚠ Your employees are handing it over

©2026 Check Point Software Technologies Ltd.

AI Bypasses Every Traditional Security Defense



A NEW LAYER OF SECURITY IS REQUIRED.

©2026 Check Point Software Technologies Ltd.

The Reality Phase of AI Security | 2025

Easy access to your **CHATS**

LLMs tricked into exporting chat data without awareness

Attack instructs Claude to gather recent chat data, write it to a file and then use the Anthropic SDK to upload it.

Claude unknowingly sends the stolen file to the attacker's Anthropic Console.



©2026 Check Point Software Technologies Ltd.

Hidden threats

in

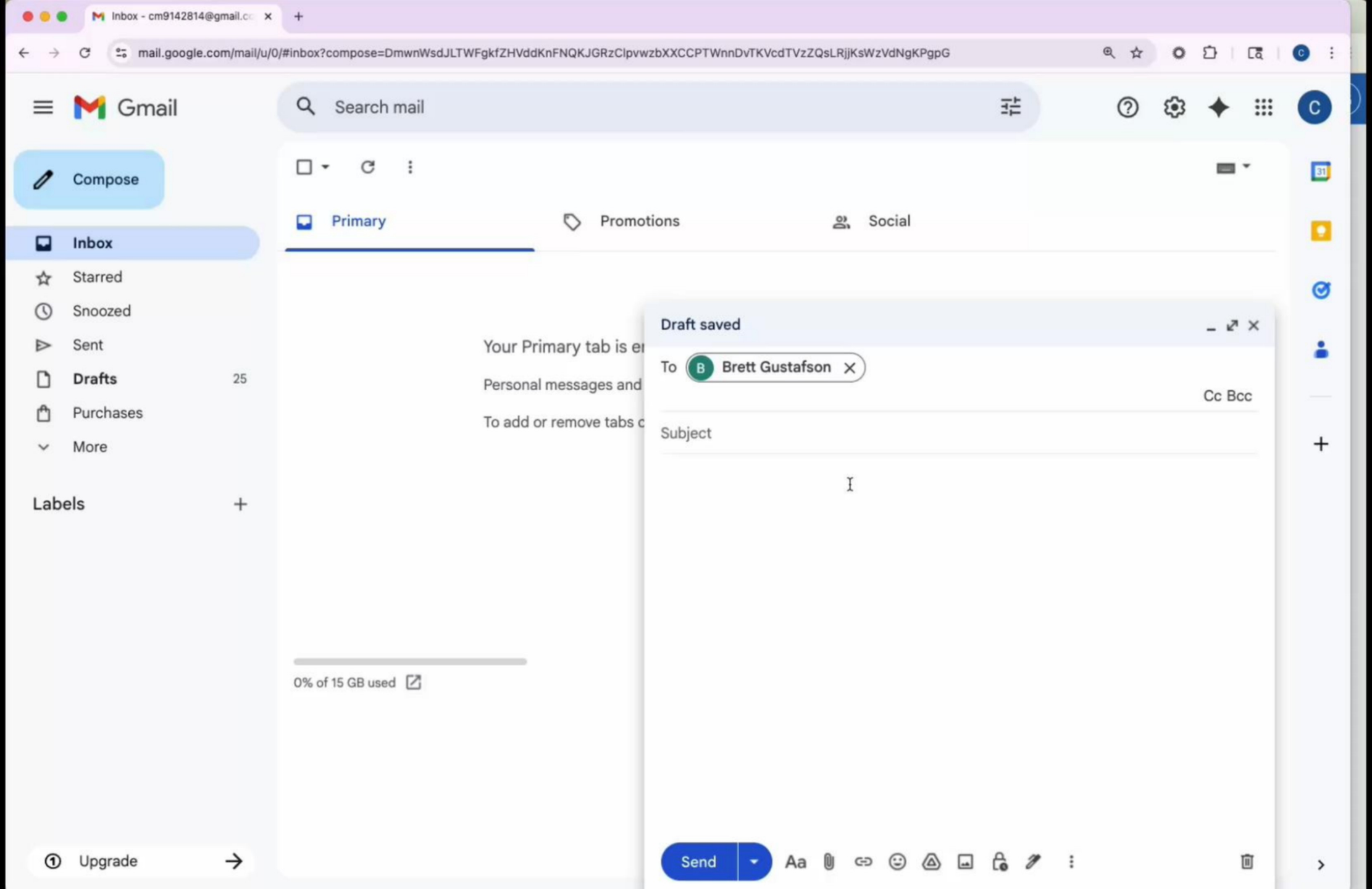
AUDIO

The expanding attack surface: Multimodal Obfuscation

Sophisticated attack involves combining two speech signals: a highly accented voice that tricks Gemini into jailbreaking, and a benign voice designed to fool the transcriber into thinking it's a harmless query.



©2026 Check Point Software Technologies Ltd.


Inbox - cm9142814@gmail.com
mail.google.com/mail/u/0/#inbox?compose=DmwnWsdJLTWFgkfZHVddKnFNQKJGRzClpvwzbXXCCPTWnnDvTKVcdTVzZQsLRjjKsWzVdNgKPgpG
Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts 25
Purchases
More
Labels
Primary
Promotions
Social
Your Primary tab is er
Personal messages and
To add or remove tabs c
0% of 15 GB used
Upgrade
Draft saved
To B Brett Gustafson
Cc Bcc
Subject
Send
Aa

MCP & The New Agent Execution Surface

What it is

MCP = Model Context Protocol

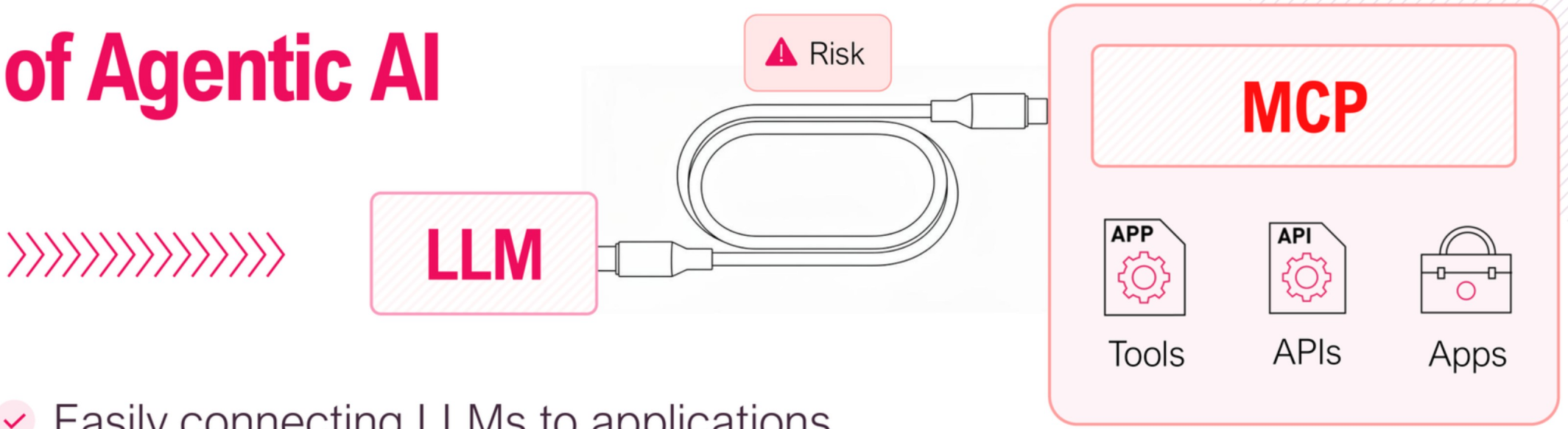
A universal interface that lets AI agents call tools, APIs, including internal systems. **Accelerates productivity.**

How it Works



©2026 Check Point Software Technologies Ltd.

MCP is the USB-C of Agentic AI



- Easily connecting LLMs to applications.

©2026 Check Point Software Technologies Ltd.

Attack surfaces are converging. A **unified solution** is required.



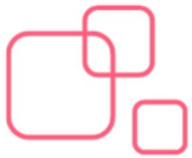
EMPLOYEES

One bad paste can leak your crown jewels



AGENTS

Agents can take unsafe actions autonomously



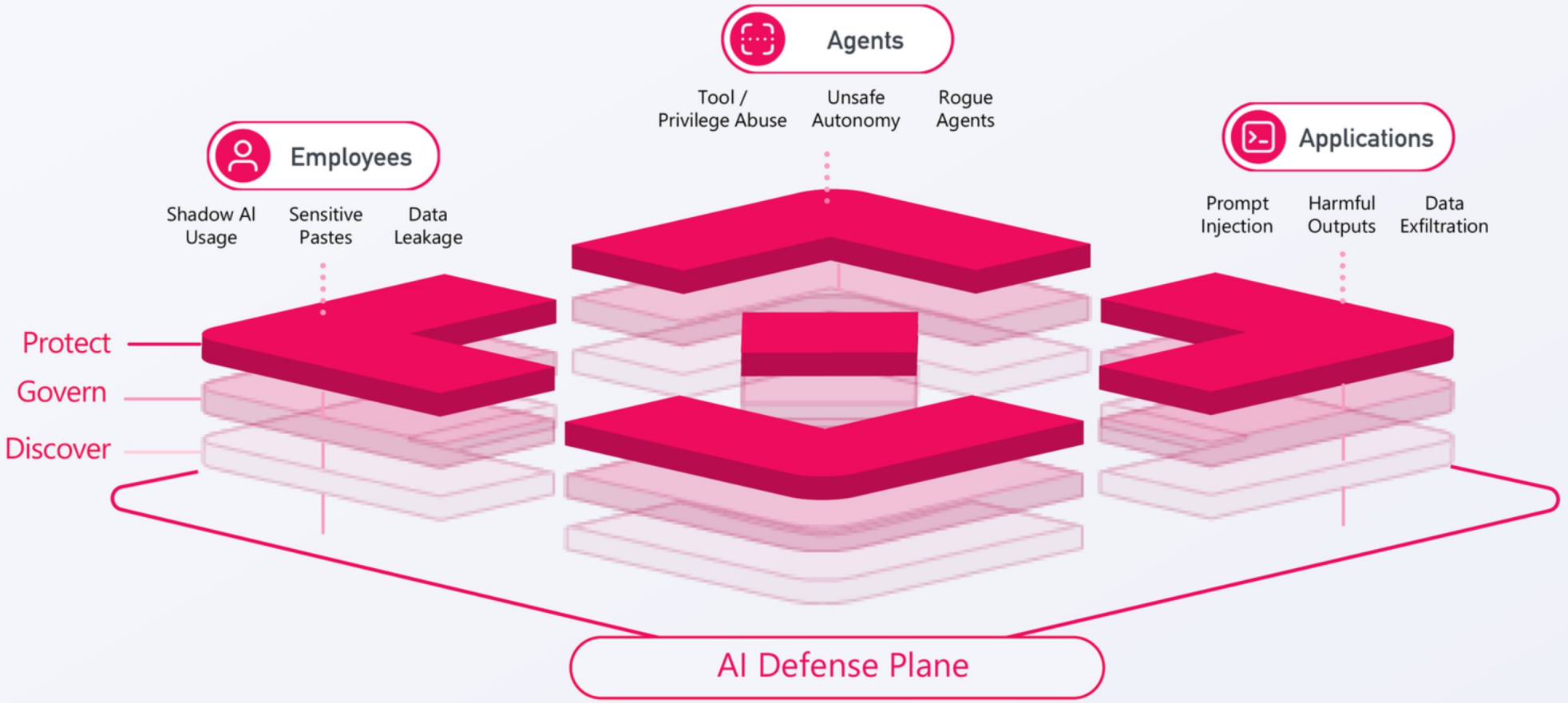
APPS

A single prompt can hijack your app.

©2026 Check Point Software Technologies Ltd.

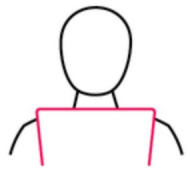
The Check Point AI Defense Plane

A unified security model — powered by a real-time control plane for Employees, Applications and Agents



One platform. One lens. From employees to applications to agents.

Workforce AI: Protect How Employees Use AI



Employees / Users



Workforce AI Security

Visibility + Policy



Public AI Apps

ChatGPT, Gemini, Copilot, Claude

Because AI adoption

DOESN'T WAIT

for IT approval.

©2026 Check Point Software Technologies Ltd.

Workforce AI Security: Securing Employee & Endpoint AI Agents at Scale

Enable AI usage by default — with guardrails that prevent risk, not block productivity

- ✓ **Secure endpoint AI agents** (Cursor, Claude Code, VSCode, etc.)
- ✓ **Govern agent behavior + data access,** not just prompts
- ✓ **Enable safe-by-default AI adoption** across the workforce



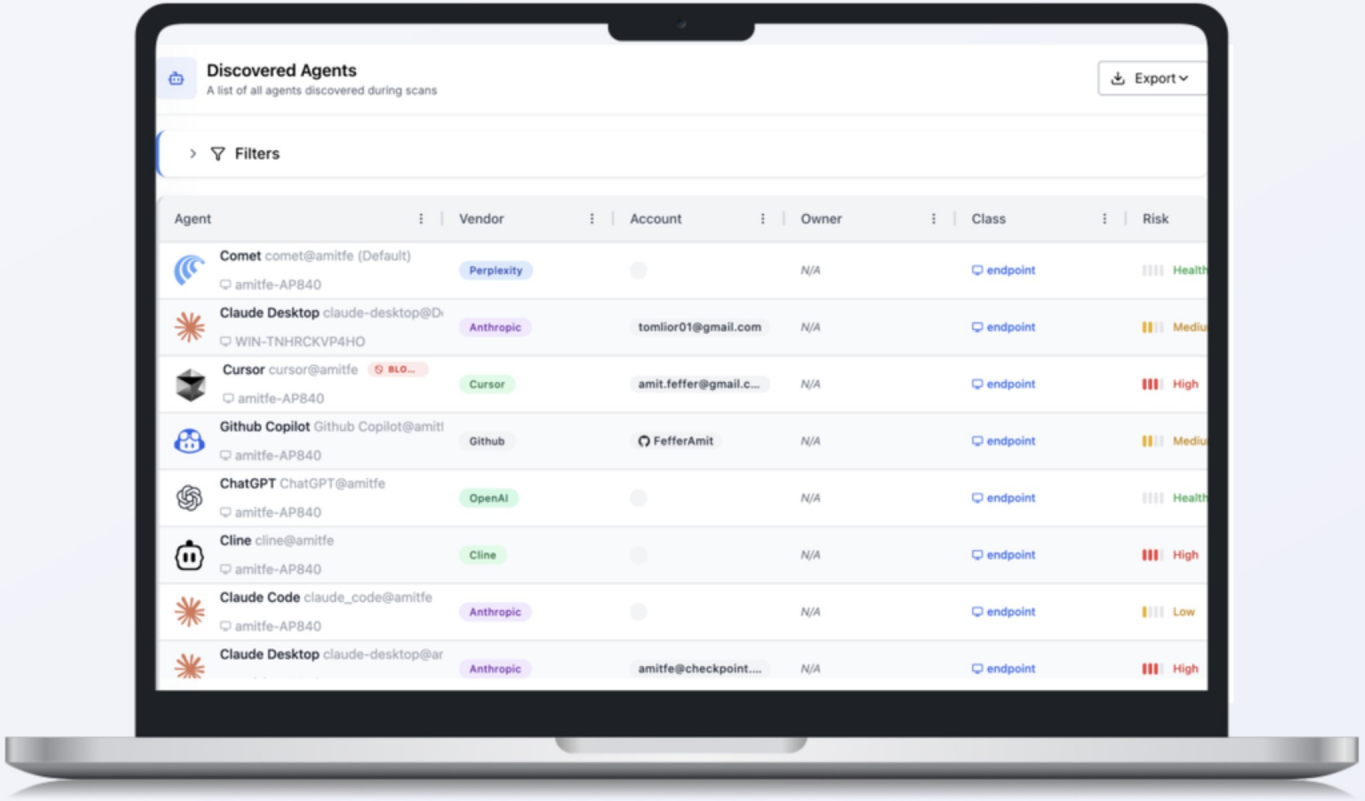
Expanding Agentic Posture, Access, and Identity

Extending visibility and control across SaaS, endpoints, and agent ecosystems

NEW CAPABILITIES

- Cross-endpoint & cross-SaaS AI agent **discovery, access control**
- Agent risk assessment **across environments**
- **Visibility** into AgentCore + MCP tool usage
- **Identification** of shadow / unmanaged agents
- Foundation for continuous **agent monitoring**

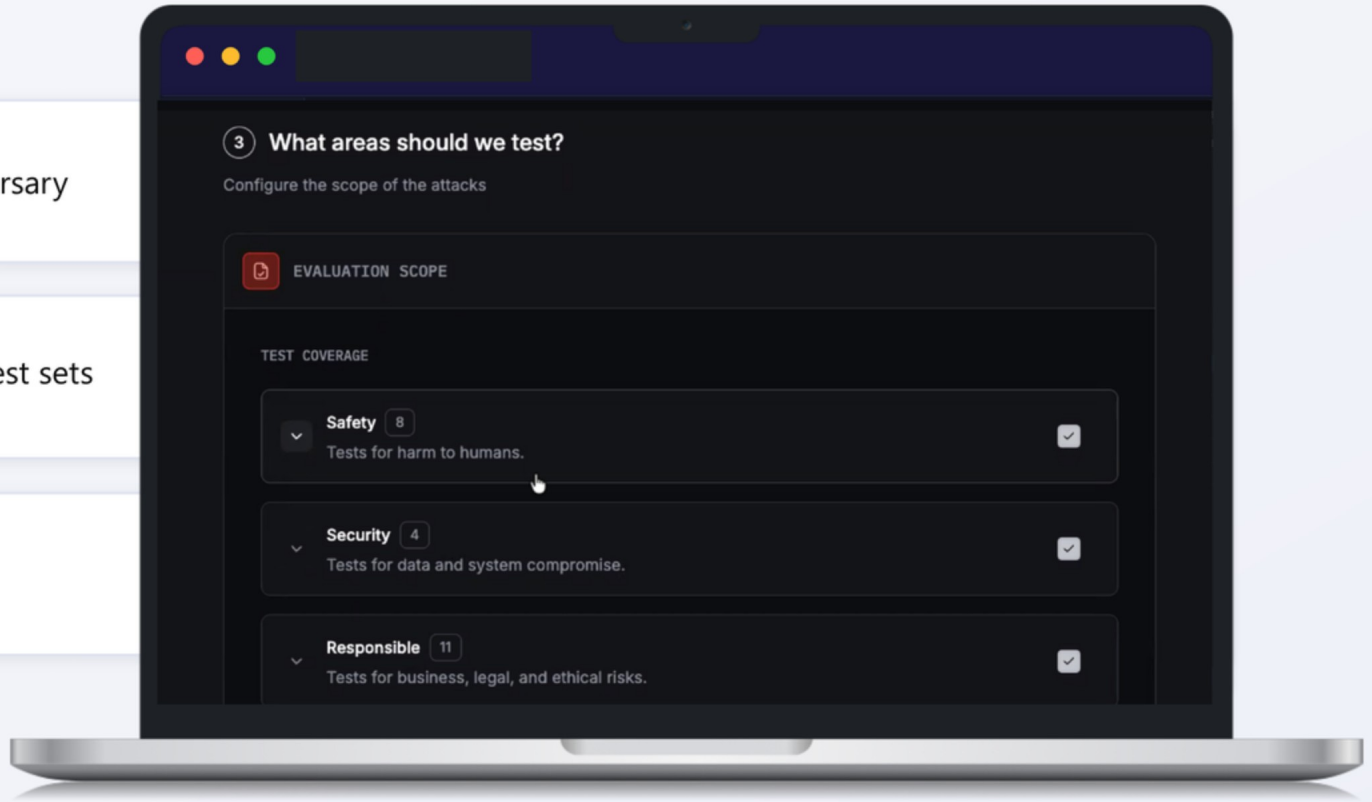
Integrated across enterprise SaaS and AI ecosystems



AI Red Teaming: Adversarial Testing for AI Systems Before They Go Live

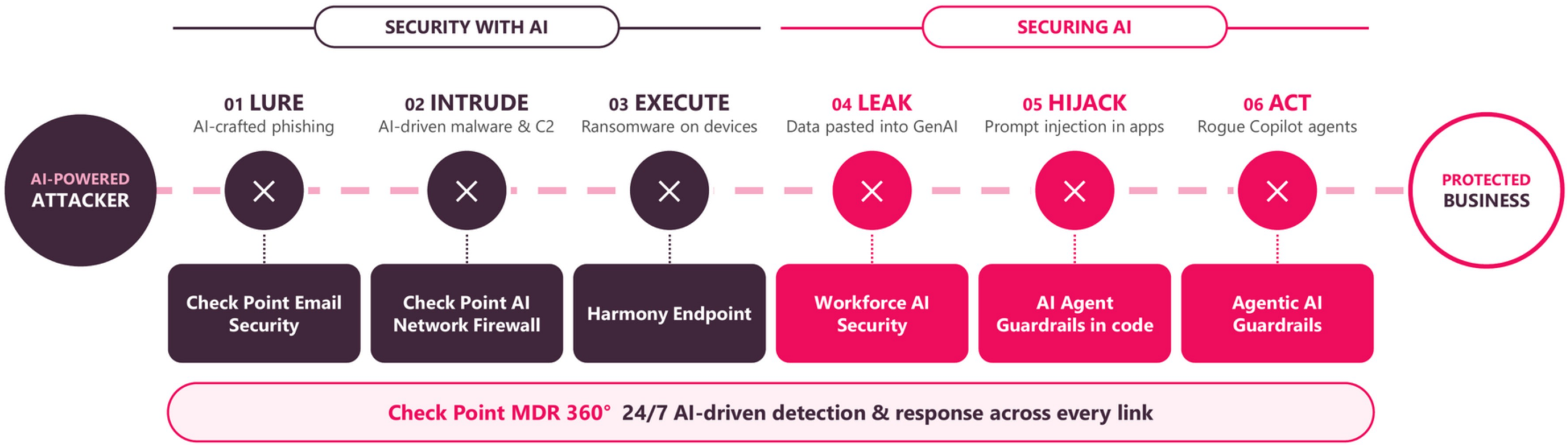
Simulate real-world AI attacks to uncover vulnerabilities in agents and applications before they reach production.

- ✓ **Adaptive attack simulation** that behaves like a real adversary
- ✓ **Continuously updated attack intelligence**—not static test sets
- ✓ **Test real AI systems,** not just models or prompts



Why AI Security Matters

We use security WITH AI to break the attacker's kill chain.
Securing AI inside the business stops the same data exfiltration when it's done by your own users.



OUTSIDE IN — AND INSIDE OUT

1. **Attackers use AI**
   Security WITH AI stops them
2. **Insiders use AI too**
   Same data leak, from inside
3. **Business builds with AI**
   Guardrails in apps & agents
4. **Threats move 24/7**
   AI-powered MDR watches both

©2026 Check Point Software Technologies Ltd.



Takk for meg

Erling Lothe Strand | erlings@checkpoint.com



Spørsmål?

Agenda

1. Intro
2. Sikkerhet i en AI-drevet verden
3. Trusselbildet, identitet og plattform Microsoft

Pause

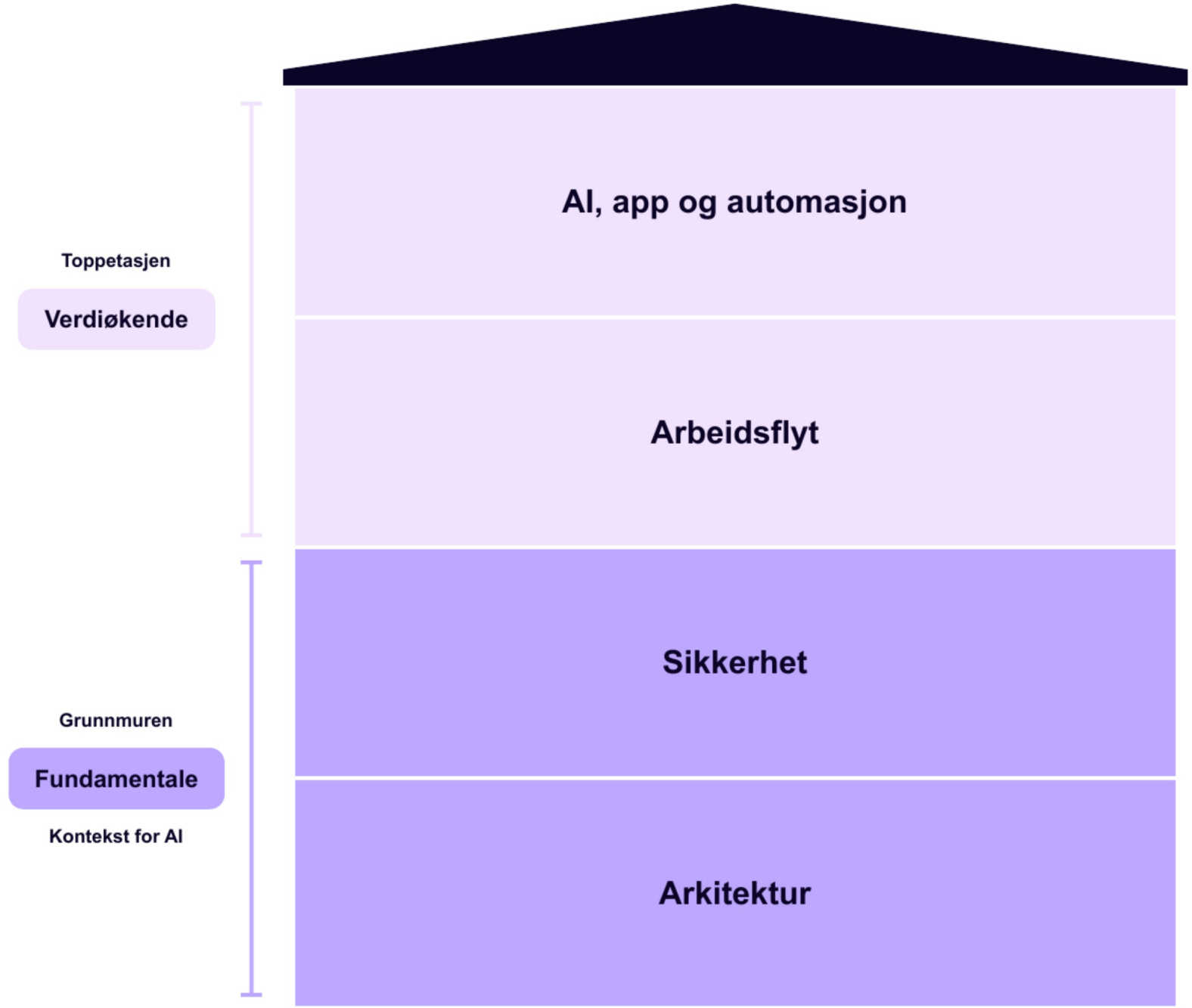
4. AI-bruk CHECK POINT

5. Tilgangsstyring og data frend

6. Mennesker nimblr.
7. Metode frend

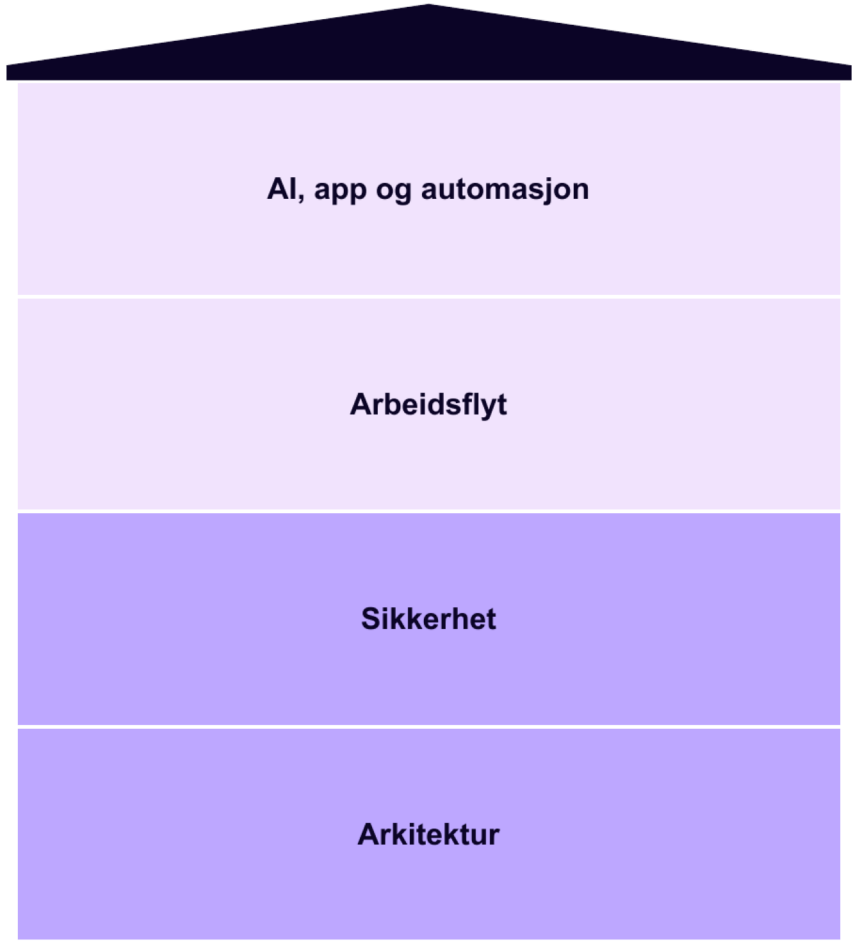
Lunsj og mingling 🌯

365 Huset er vår beste praksis for M365



frend

Grunnmuren avgjør hva AI og agenter kan gjøre



→ **Det AI leverer**

→ **Det AI lærer av**

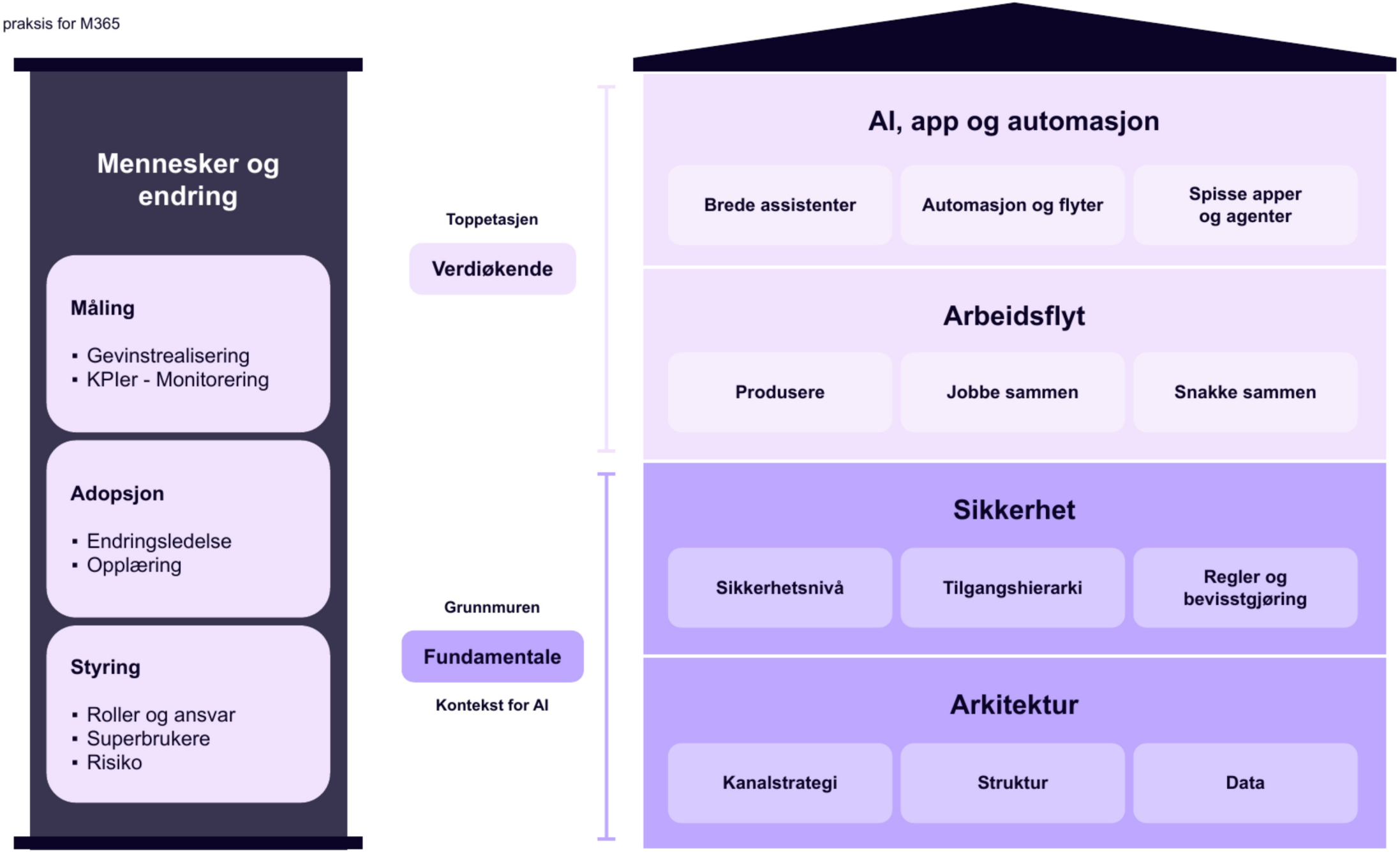
→ **Grensene for AI**

→ **Datagrunnlaget for AI**

frend

Kilde: Seminar: Fra kaos til kontroll i SharePoint og Teams, Frend, august 2026 ↗

365 Huset er vår beste praksis for M365



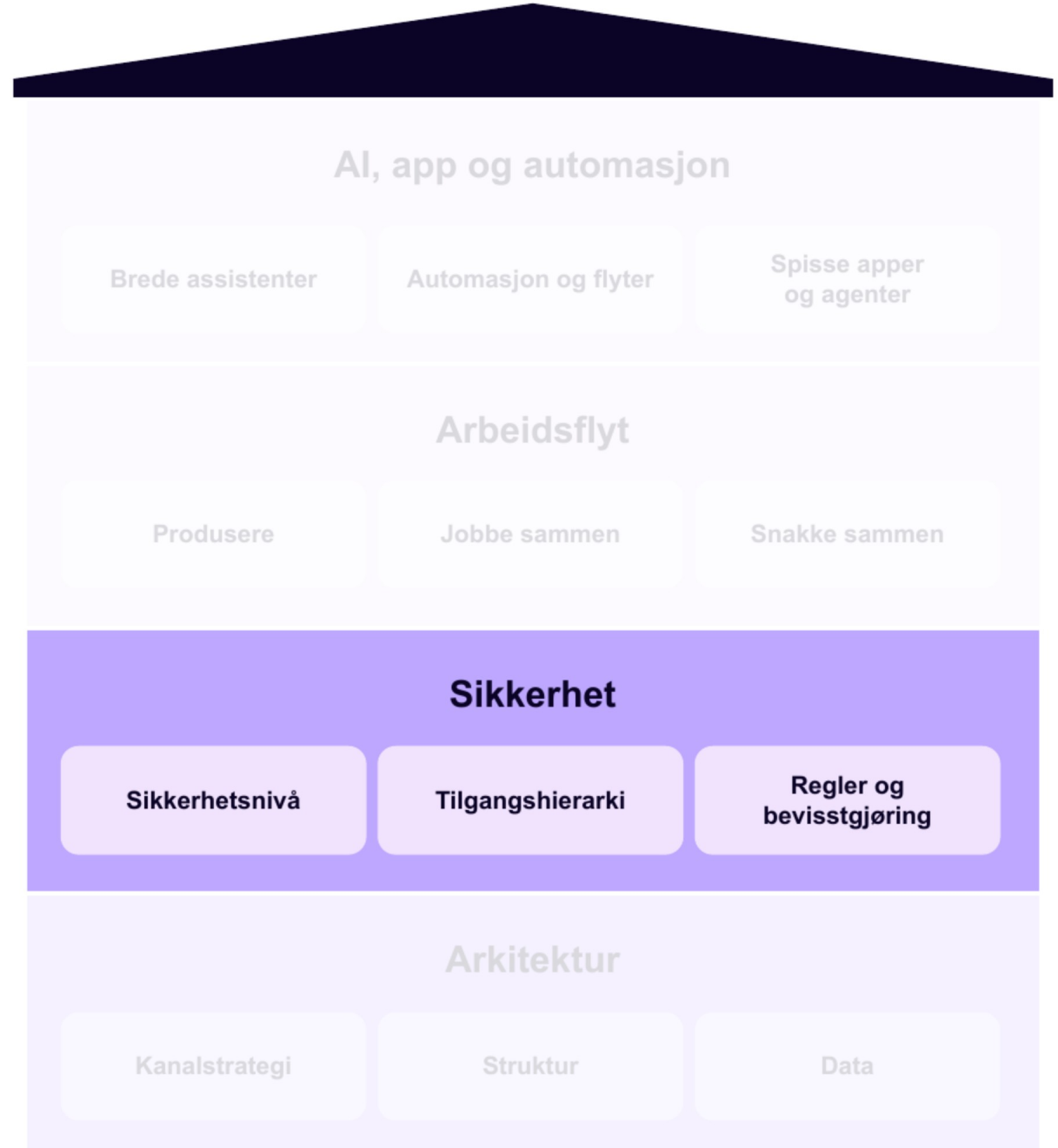
frend

Sikkerhet

Sikkerhetsnivå:
Hvilket sikkerhetsnivå trenger vi?
- Lovverk og regler
- Definere og implementere tenant baseline
- MFA, Intune
- Sikre riktige lisenser

Tilgangshierarki: Hvem skal ha tilgang til hva?
Hvordan skal eksterne håndteres?
- Dynamiske grupper og sentralisert styring
- Access packages og gjestetilgang
- Entra

Regler og bevisstgjøring:
Hvordan redusere risiko for menneskelige feil?
- Purview
- Sensitivitetsetiketter, DLP, Retention policies
- Testing, bevisstgjøring og opplæring



frend

5 tips før dere slipper løs AI og agenter

1 **Definer sikkerhetsnivået**
Bestem nivået ut fra lover og regler, og rull ut en tenant baseline med MFA, Intune og riktige lisenser.

2 **Definer og automatiser tilgangene**
Bruk dynamiske grupper og access packages i Entra, også for eksterne og gjester, i stedet for manuell tilgangsstyring.

3 **Merk dataene før AI tar dem i bruk**
Datamerking med sensitivitetsetiketter i Purview avgjør hva Copilot og agentene får se og dele.

4 **Stopp datatap**
Skru på DLP og lagringsregler (retention policies), så sensitive data ikke lekker ut eller blir borte.

5 **Test og lær opp folk**
Bevisstgjøring, trening og testing reduserer risikoen for menneskelige feil.

frend nimblr.

Kilde: 365 Huset 5.0, sikkerhetsetasjen, Frend, mai 2026 ↗

Agenda

1. Intro
2. Sikkerhet i en AI-drevet verden
3. Trusselbildet, identitet og plattform Microsoft

Pause

4. AI-bruk CHECK POINT
5. Tilgangsstyring og data frend

6. Mennesker nimblr.

7. Metode frend

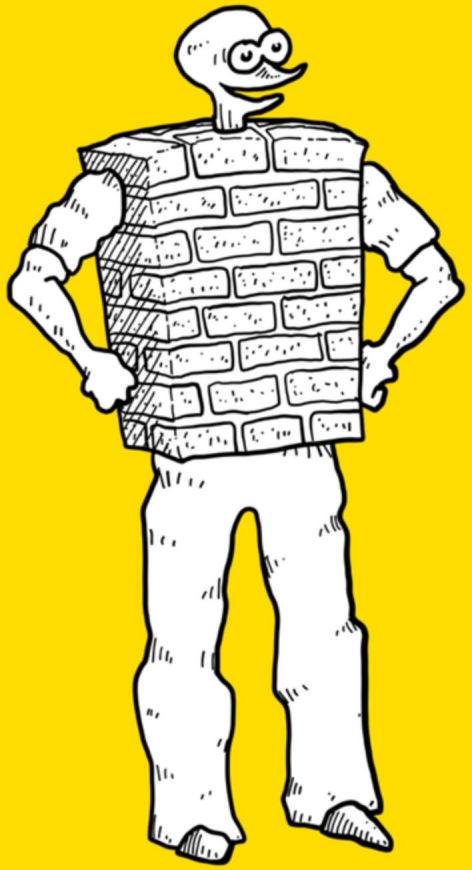
Lunsj og mingling 🌯

FREND DIGITAL SEMINAR

Fra menneskelig risiko til ekte forsvar

Den sterkeste brannmuren en virksomhet har, er menneskene.

nimblr.



FØR VI STARTER

Hva skjer i dag?

Skann QR-koden med mobilkameraet for å se programmet og hva vi skal gjennom.

nimblr.

SKANN MEG

OM NIMBLR

Hvem er Nimblr?

Vi hjelper ansatte å ta gode valg i øyeblikket et angrep kommer.

Human risk management som kombinerer atferdspsykologi, ekte angrepsdata og KI. Grunnlagt i Sør-Sverige i 2019. Navnet kommer fra skånske «nimt»: smidig, enkelt og praktisk.

Turn human risk into real defense.

nimblr.

NIMBLR I TALL

9 000+
Bedrifter

1M+
brukere trent

35+
språk

EU Datasentre

nimblr.

Mennesket er fortsatt hovedinngangen

62 %

av bekreftede databrudd involverte det menneskelige elementet

Verizon DBIR 2026

Ca. 80 %

av cyberangrep starter med phishing. Innboksen er fortsatt inngangsdøra

Verizon DBIR 2026, via Nimblr

3,9 mill. €

er gjennomsnittlig kostnad for ett enkelt databrudd globalt

IBM Cost of a Data Breach 2025

Brannmurer og MFA har gjort den tekniske veien inn vanskeligere. Derfor går angriperne via menneskene.

E-POST OG KI

Hvorfor e-post blir en enda større trussel

4,5x

flere klikk på phishing skrevet med KI enn på phishing skrevet manuelt.

Kilde: Microsoft Digital Defense Report 2025

Hva KI endrer

1. Feilfri norsk, ekte logoer og riktige detaljer
2. Personlig tilpasset hver mottaker, i stor skala
3. Kopierer hverdagen: fakturaer, kalender og HR

PSYKOLOGIEN

nimblr.

Derfor klikker vi

1 Følelser

Hastverk og frykt slår det å tenke seg om.

2 Autoritet

En forespørsel fra sjefen blir ofte fulgt.

3 Tidspress

E-post som leses på mobilen blir sjekket mindre.

4 Troverdig etterligning

Ekte merkevarer, godt språk, riktige detaljer.

5 Kjente arbeidsprosesser

Fakturaer og kalenderinvitasjoner ser rutinemessige ut.

6 Tillit til kjente

Navnet til en kollega låner tillit.

Kilde: Nimblr, «Why phishing still works in 2026»

FRA VÅR HONEYPOT

E-postene som lurer flest

ca. 20 %

klikket i Norge på en ekte kriminell HR-e-post om sommerferie, fanget i vår honeypot og gjort om til en trygg simulering.

Kilde: Nimblr, «Why phishing still works in 2026»

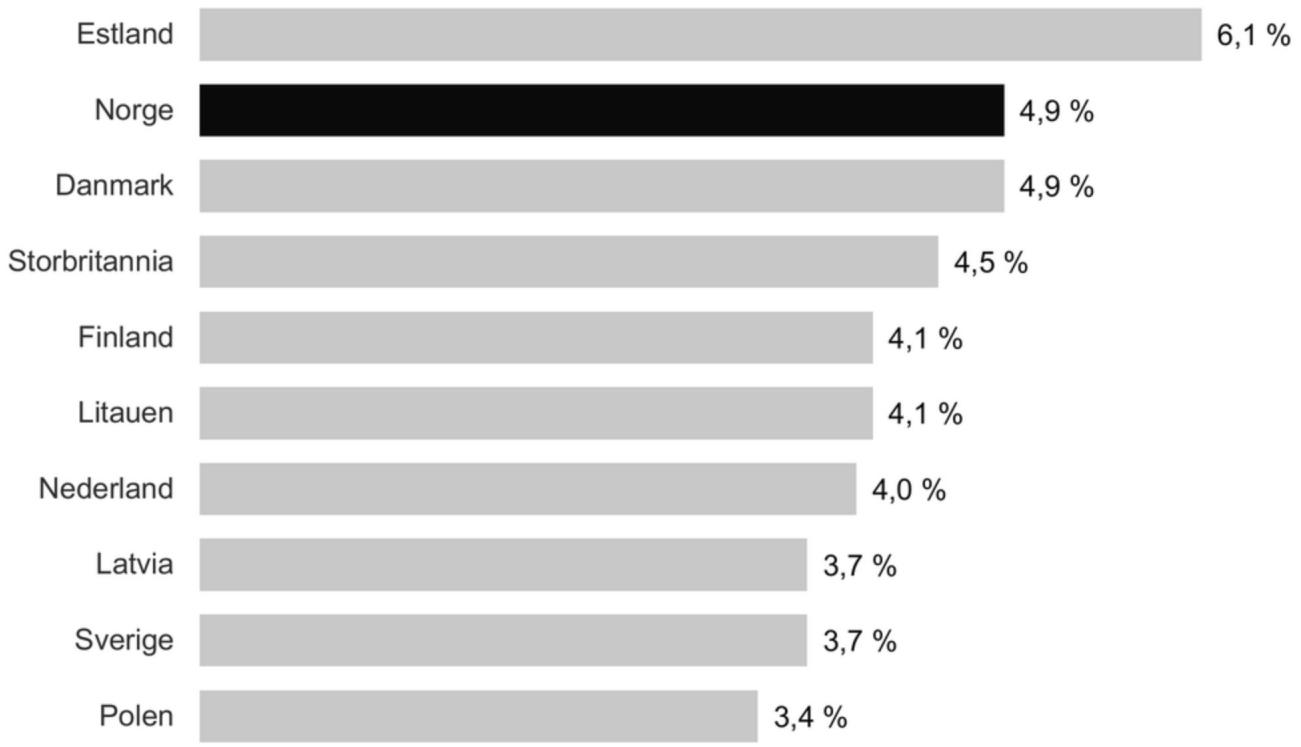
nimblr.

Mest klikkede simuleringer

33 %	**HR-e-post om sommerferie**	Danmark
26 %	**HR-e-post om sommerferie**	Litauen
24 %	**Lønn og goder**	Litauen
23 %	**Gavekort til jul**	Storbritannia
22 %	**Kalenderpåminnelse**	Litauen

NORGE I EUROPA

Små forskjeller, samme mønster



Kilde: Nimblr, 1 714 simuleringer sendt ca. 11 millioner ganger i 10 land, 2025

Gjennomsnittlig klikkrate

Norge ligger på 4,9 %, men forskjellene mellom landene er små. HR-temaer var blant de mest klikkede i alle ti land.

Det handler om atferd, ikke nasjonalitet. Og atferd kan trenes.

STRONGER TOGETHER

nimblr.

Ingen skal måtte oppdage KI-angrep alene.



Sikkerhetskultur bygges sammen. Hver gang noen sier «dette ser rart ut», blir alle tryggere.

#StrongerTogether

SLIK LØSER VI DET

nimblr.

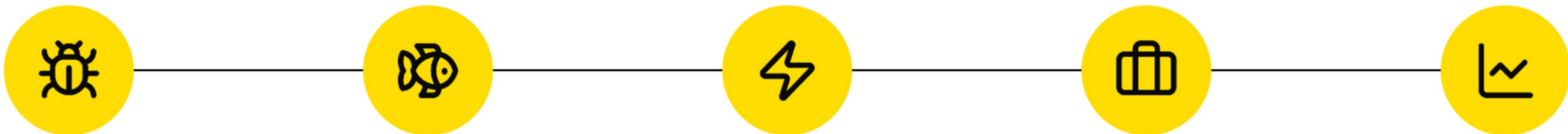
Utfordringene og løsningene

UTFORDRINGEN		SLIK LØSER NIMBLR DET
Sjelden testing	→	**Automatiske simuleringer hele året, basert på ekte angrep**
Ingen oversikt over risiko	→	**Awareness Level viser hvem som er utsatt, og hvordan det endrer seg**
Lange kurs ingen fullfører	→	**Micro Training på under fem minutter, tilpasset rollen**
Vanskelig å dokumentere	→	**Automatiske rapporter som støtter NIS2, DORA og revisjon**
Presset IT-avdeling	→	**Rask oppstart, ingen kontoer for ansatte, går av seg selv**

SLIK FUNGERER NIMBLR

nimblr.

Fra ekte angrep til endret atferd



01

Ekte angrepsdata

Honeypot og ukentlig trusselanalyse

02

Realistiske simuleringer

E-post og SMS, på norsk

03

Instant Learning

Læring rett etter et klikk

04

Role-Based Learning

Tilpasset jobben

05

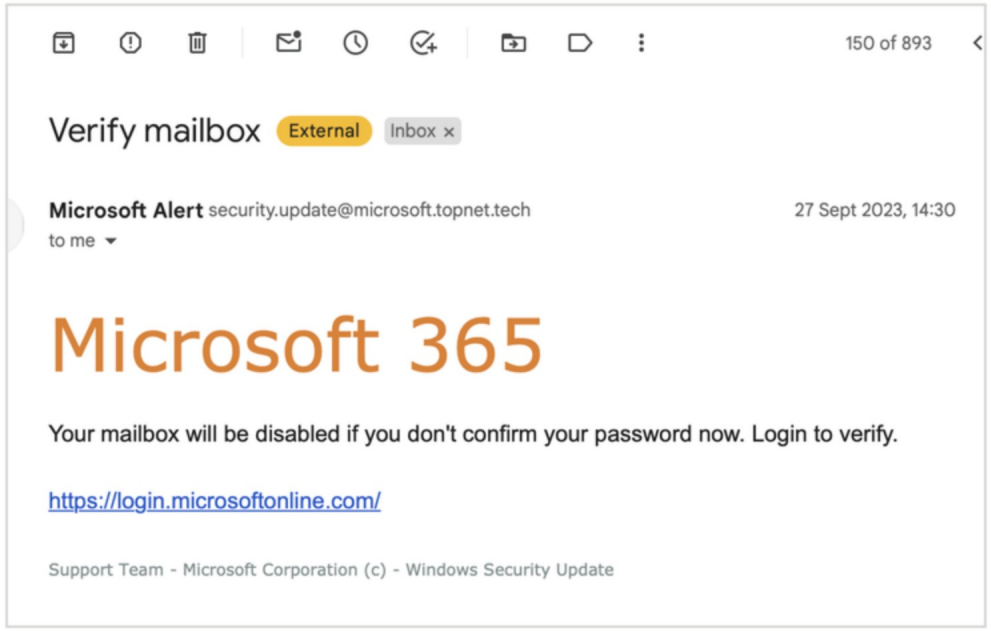
Awareness Level

Viser hvor risikoen sitter

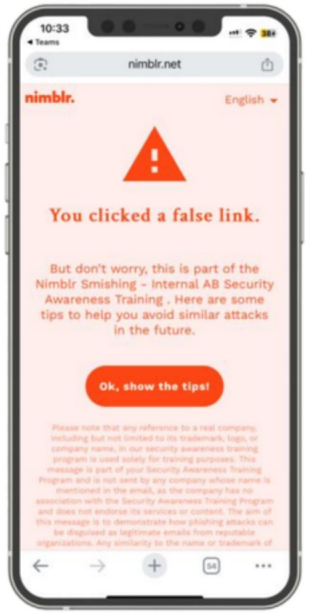
KI brukes til timing, relevans, personalisering og innholdsproduksjon, alltid med menneskelig kvalitetssikring.

SLIK SER DET UT

Et simulert angrep



1 Den simulerte e-posten



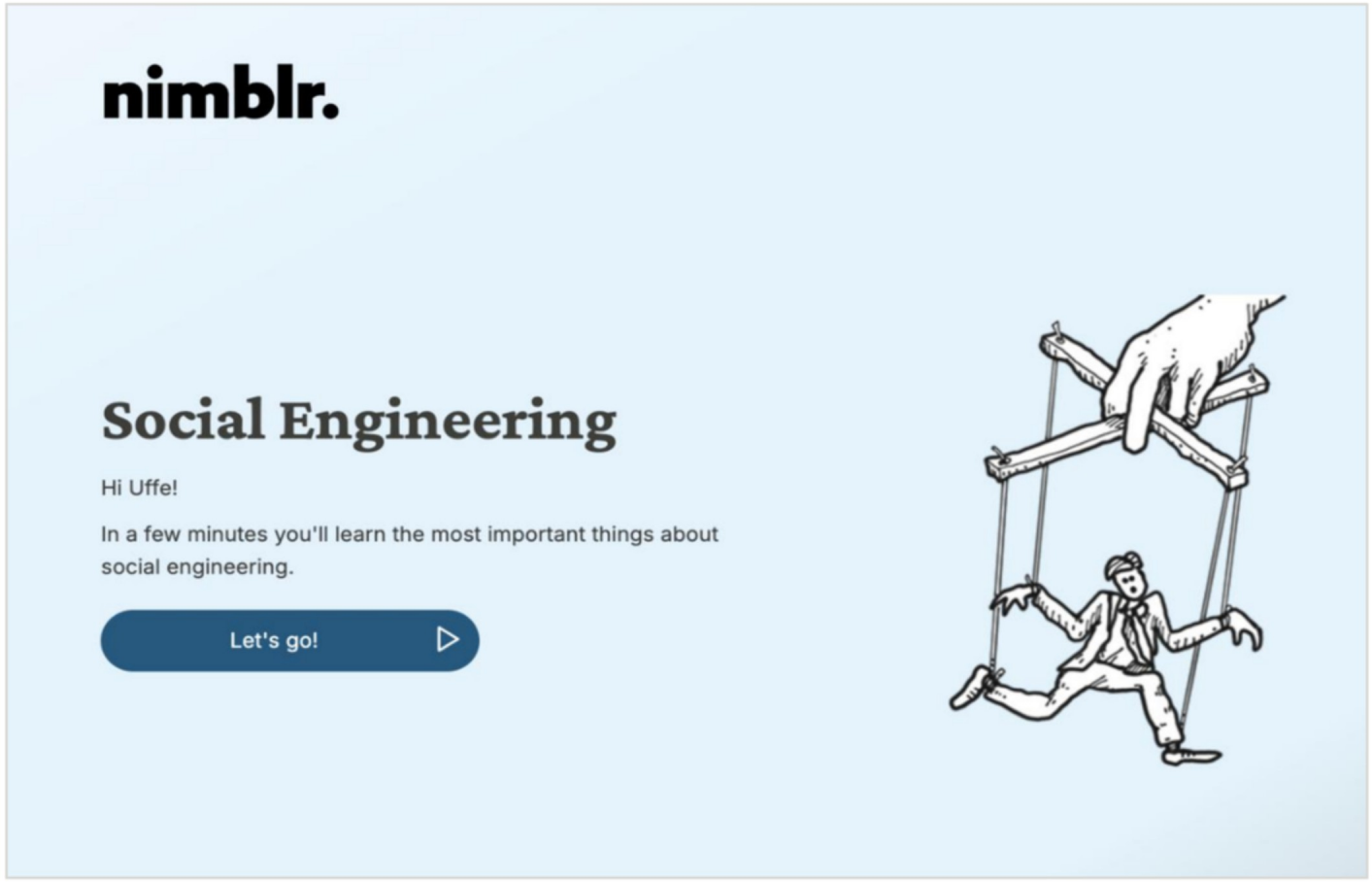
2 Etter klikket

Slik fungerer det

1. En realistisk e-post kommer, som et ekte angrep ville sett ut
2. Klikker man, havner man på en trygg side, ikke hos en angriper
3. Ingen blir hengt ut. Klikket blir et læringsøyeblikk

SLIK SER DET UT

Instant Learning



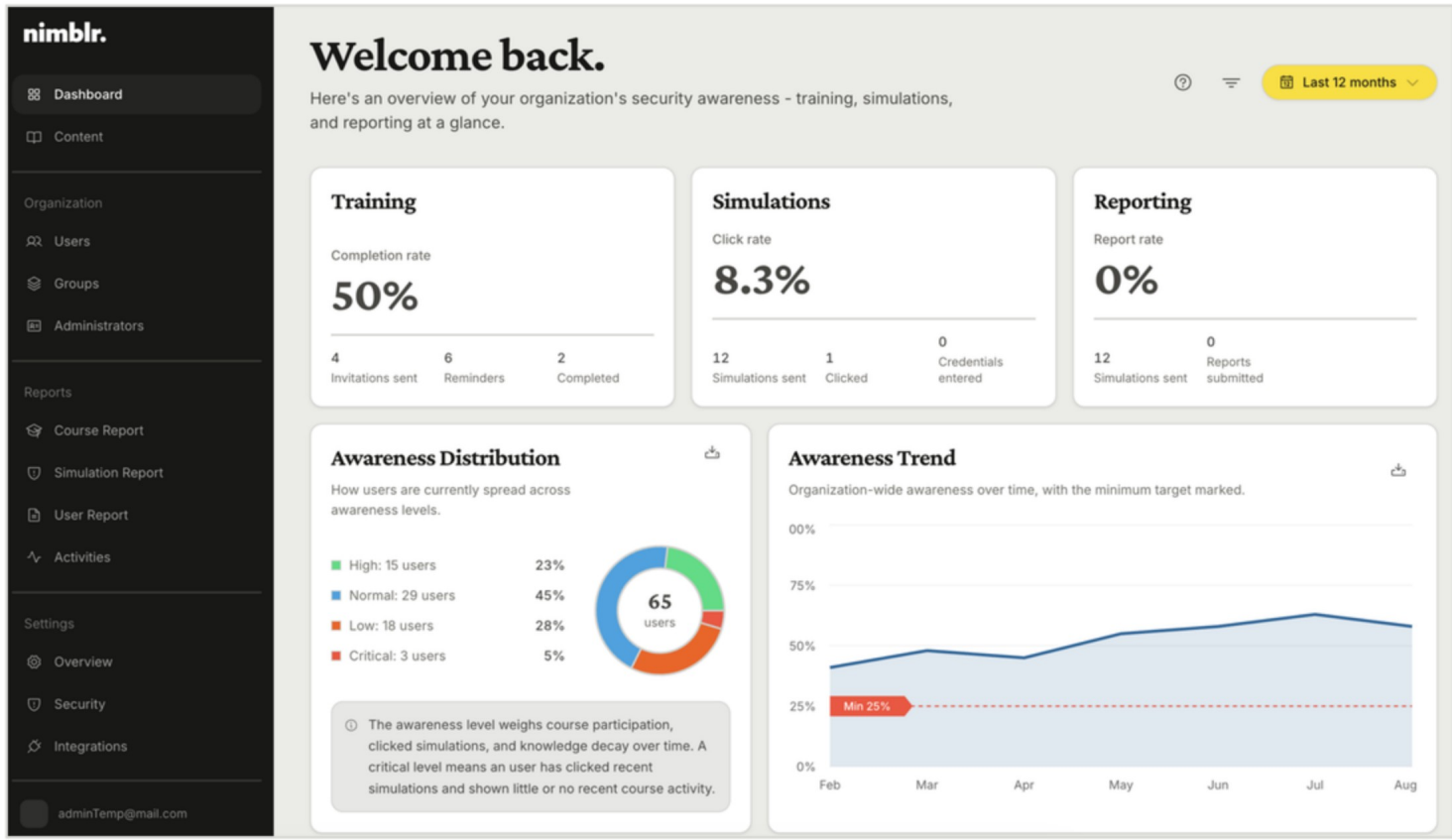
nimblr.

Rett etter klikket

1. Et kort kurs om akkurat det angrepet man gikk på
2. Tar bare noen minutter, rett i nettleseren
3. Lærer grepene angriperen brukte, ikke å lete etter skrivefeil

nimblr.

Plattformen: full oversikt for IT og ledelse



Opplæring

Hvor mange som har fullført kursene

Simuleringer

Klikkrate og rapporteringsgrad over tid

Awareness Level

Hvor risikoen sitter, per gruppe og person

RESULTATER

Atferd kan endres, og det kan måles

80 %

reduksjon i klikk på simuleringer de første tre månedene med Nimblr.

Før: 18–25 % → **Etter: 2–3 %**

Kilde: Nimblr kundedata

nimblr.

FRA KUNDENE

40 % → 3 %

klikkrate hos en bransjeorganisasjon

«Jeg ville ikke klart å kommunisere trusler til 2 000 ansatte på egen hånd.»

Oscar Karlsson
CIO, Hexatronic Group (oversatt)

TRE TING DERE KAN GJØRE PÅ MANDAG

nimblr.

Gjør verifisering til en vane

1

Avtal en fast rutine for å verifisere betalinger og hastesaker.

2

Tren i alle kanaler: e-post, SMS, telefon og chat.

3

Mål hvor mange som sier fra, ikke bare hvor mange som klikker.

Turn human risk into real defense.



Spørsmål?

Agenda

1. Intro
2. Sikkerhet i en AI-drevet verden
3. Trusselbildet, identitet og plattform Microsoft

Pause

4. AI-bruk CHECK POINT
5. Tilgangsstyring og data frend
6. Mennesker nimblr.
7. **Metode** frend

Lunsj og mingling 🌯

frend



Mennesker

1 Tren de ansatte



AI-bruk

2 Lag tydelige AI-retningslinjer



Identitet og tilgang

3 Stram inn tilgangen



Data

4 Ta backup utenfor Microsoft



Enheter og infrastruktur

5 Få kontroll på enhetene



Drift og overvåking

6 Bruk det dere har

Sjekk hvilken sikkerhet som følger med lisensene, og slå den på.

METODE · SLIK HJELPER VI

Vår metode

1 Definer sikkerhetsnivået

Vi finner riktig nivå sammen med dere, ut fra lover, regler og risiko i bransjen.

2 Kartlegg og definer gap

Vi går gjennom hele IT-miljøet deres og gir dere en rapport som viser gapet til ønsket nivå.



3 Lukk gapene med en baseline

Vi ruller ut et felles grunnoppsett for alle brukere og enheter, prioritert etter risiko.

4 Forvalt og følg opp

Vi drifter, overvåker og forbedrer løpende, så nivået holder seg når dere tar i bruk AI.

Frend er ISO 27001-sertifisert. Vi jobber selv etter den internasjonale standarden for informasjonssikkerhet, med de samme rutinene vi hjelper kundene våre med.

frend

Let's be Frends

Takk!

Tid for lunsj for de som vil det 🌯





frend

Agenda

Om Frends IT-drift og support

- Utvalgte kunder
- Service og support
- Sikkerhet
- Infrastruktur og drift
- Rådgivning

frend

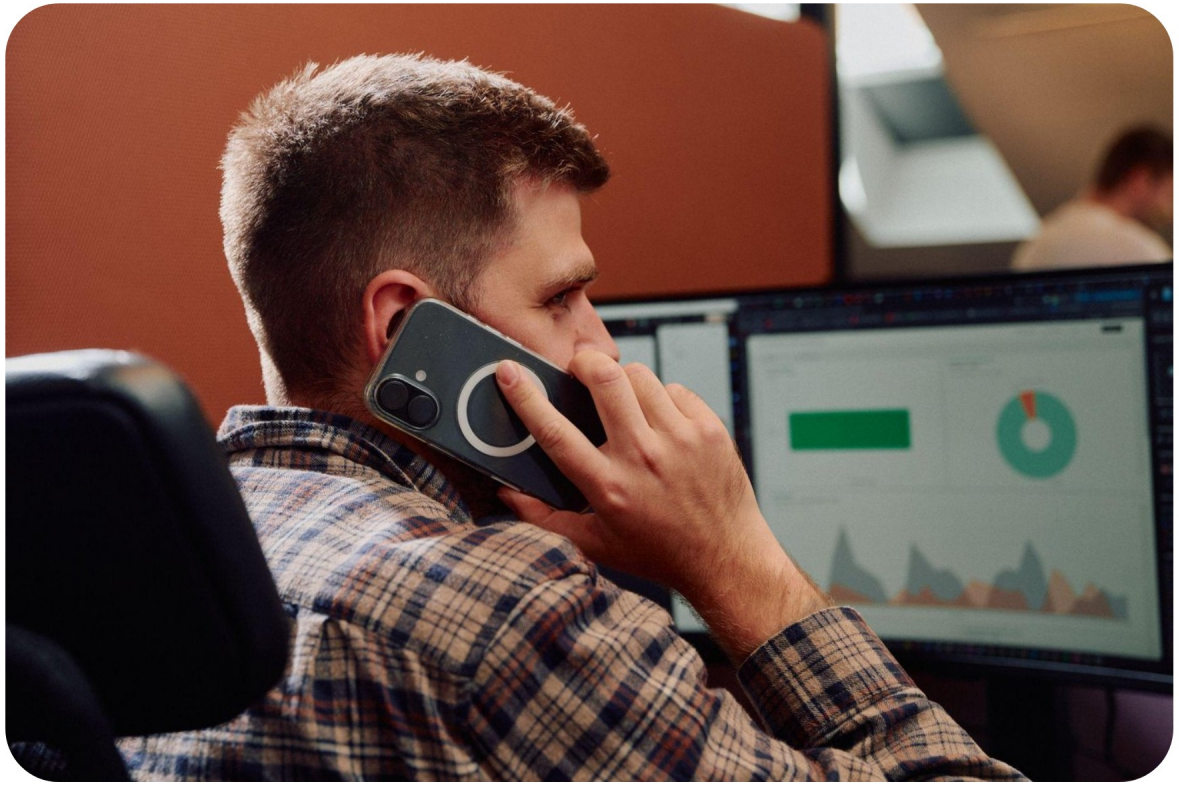
100+ ANSATTE	Milient, fair, Oslo-filharmonien, evat
50 til 100 ANSATTE	Halogen, lundhagem, MEBYR, SOLSTEIN GRUPPEN
30 til 50 ANSATTE	Ryger ADVOKATFIRMA, CARUCEL EIENDOM, agp, KELVIN AS
10 til 30 ANSATTE	STIFTELSEN NorskMat, AERA, salto

Service og support

Effektive og operative ansatte fra dag én

- Personlig, rask og effektiv service desk
- Telefon, e-post og fjernstyring på norsk
- PC og utstyr levert ferdig konfigurert
- Sømløse prosesser
- On- og offboarding

Våre eksperter løser hendelser i fellesskap i stedet for å sende saker mellom ulike supportnivåer.



OPTIO

«Det viktigste Frend gir oss, er følelsen av å bli prioritert.»

Eirik L. Wang, CIO

Sikkerhet

Beskyttet 24/7 med skybasert sikkerhet

- ISO 27001-baserte prosesser
- Overvåking og respons med SOC og MDR
- Identitets- og tilgangsstyring
- Plattform og tenant baseline
- Backup og gjenoppretting
- Sikkerhetstrening

International Organization for Standardization
ISO
27001

Microsoft | Google | CHECK POINT | nimblr. | UniFi | redstor | Canon | Lenovo

OPTIO

«Vi forvalter veldig mye data på vegne av kundene våre, som igjen stiller strenge krav til hvordan vi håndterer sikkerheten.»

Eirik L. Wang, CIO

Infrastruktur og drift

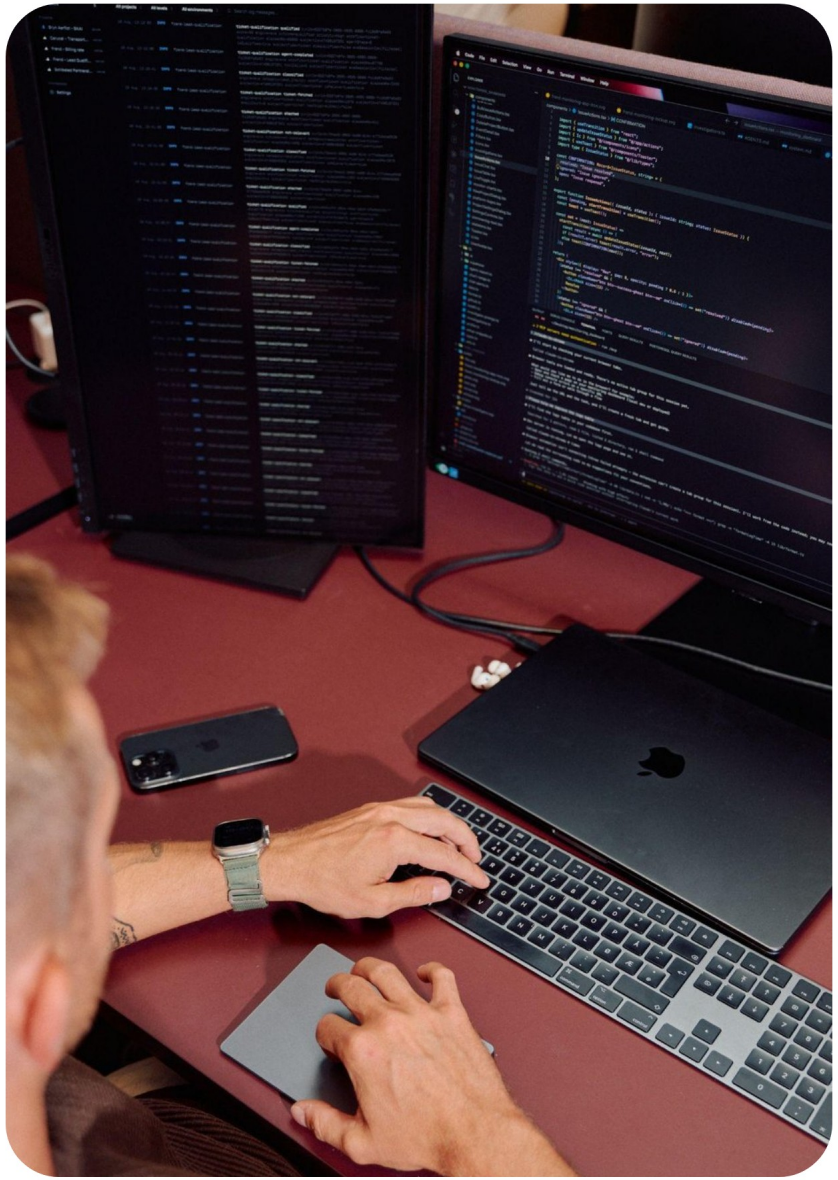
En stabil grunnmur som bare funker

- Drift, overvåking, oppdatering og vedlikehold
- Enhets- og klientforvaltning
- Maskinvare
- Møterom
- Nettverk
- Print

Mvh.

«I løpet av to uker endret vi hele infrastrukturen og 15 års byråhistorie ble flyttet opp i skyen uten problemer.»

Jon Fredø, daglig leder



Rådgivning

En partner på IT, AI og digitalisering

- Faste og dedikerte kontaktpersoner
- Jevnlige statusmøter og oppfølging
- Lisens- og kostnadsoptimalisering, faste priser
- Kontinuerlig forbedring



KELVIN AS

«Vi ønsket oss en partner som kunne være med på endringsreisen vår, ikke bare holde lyset på. Frend har levert fra dag én.»

Erlend Sommer, Tech Lead



Mennesker



AI-bruk



Identitet og tilgang



Data



Enheter og infrastruktur



Drift og overvåking