aitrainer.dk

AI-agenter anno 2026

Ét ord, fire vidt forskellige værktøjer. Et deep dive i OpenClaw, Claude Cowork, Perplexity Computer / Research og Hermes Agent.

DEEP DIVE · MAJ 2026 · PRO, KONTRA OG USE CASES

Stefano Vincenti er GenAI-strateg og -arkitekt med 25 år i IT og digital transformation. Han hjælper nordiske ledelsesteams med at gå fra AI-nysgerrighed til konkret implementering: med governance, fart og reel forretningsværdi.

Læs hele serien | **Tilmeld nyhedsbrevet**

bottellme.com · tryzone.dk · aitrainer.dk

INDHOLDSFORTEGNELSE

Ti korte afsnit. Spring til det, du har brug for. Eller læs det hele på ti minutter.

■ 1. OM DENNE GUIDE

Jeg har besluttet at lave et deep dive i fire værktøjer, som folk lige nu alle sammen kalder „AI-agent“. De løser vidt forskellige problemer.

Ingen af dem er plug-and-play til tung enterprise-compliance endnu. Nogle, især Claude Cowork på Team og Enterprise, er allerede enterprise-rettede med admin-kontroller og audit/logging, men kræver stadig konkret vurdering af data, integrationer, retention, logging og governance. De er alle lovende, og de giver et tidligt blik på det, der er på vej. Derfor er det værd at forstå dem nu.

For hvert værktøj får du det samme: hvad det er, hvad der taler for, hvad der taler imod, og hvad det er bedst til. Og vigtigst af alt: en ærlig markering af, hvad jeg har kørt hands-on, og hvad jeg stadig er ved at teste.

✓ TESTET HANDS-ON	Jeg har selv kørt værktøjet og taler ud fra erfaring. Gælder OpenClaw, Cowork og Perplexity.
UNDER TEST	Installeret, og jeg er i gang med at teste den. Vurderingen er foreløbig. Det gælder Hermes.

ØJEBLIKSBILLEDE

Feltet her flytter sig hurtigt. Det her er, hvad jeg ved i maj 2026. Tjek altid de aktuelle vilkår, priser og sikkerhedsmeldinger, før du beslutter dig.

■ 2. DEN DYRE FEJL

Den dyreste fejl, jeg ser: at bruge de her værktøjer i den forkerte sammenhæng.

Lad mig sige det klart. De fire værktøjer i denne guide er agentiske frameworks i tidlig modenhed. De er til små, modige startups og freelancere, og til teams der kan bevæge sig hurtigt, leve med skarpe kanter og selv tage ansvaret. Får du en agent op at køre i denne uge, vinder du tid og indsigt, før de fleste andre.

Til en stor organisation med tunge krav til compliance, sporbarhed og databehandling skal valget tages med konkret vurdering. Claude Cowork på Team eller Enterprise kan være en mulighed for interne opgaver, men kræver et review af data, integrationer og governance. Microsoft Copilot Cowork er den anden vej værd at holde øje med (mere på side 7).

■ 3. TO AKSER: KONTROL OG MODENHED

To akser sorterer de fire værktøjer og gør det til en bevidst beslutning frem for en mavefornemmelse.

Kontrol: ejer du stacken, eller låner du leverandørens rails?

OpenClaw og Hermes lader dig eje stacken: de kører på din egen maskine eller server, under din kontrol. Cowork og Perplexity kører på leverandørens rails, omend Perplexity er et hybridt local/cloud-flow med adgang til lokale filer. Det er nemmere at komme i gang med, men du accepterer leverandørens rammer.

Modenhed: hvor klar er værktøjet til reel brug?

Modenhed handler ikke kun om kernefunktionen. Et værktøj kan være stærkt og alligevel umodent, hvis sikkerheden ikke følger med. Et stort angrebsareal trækker modenheden ned, uanset hvor godt værktøjet ellers leverer.

MERE MODEN · KLAR TIL REEL BRUG

Claude Cowork Modent freelance- og team-produkt. Relativt kontrolleret og sandboxet som standard, men ikke risikofrit: prompt injection og data-exfiltration er stadig relevante risici.	**Perplexity** Modent research-flow. Hovedforbeholdet er dataresidens og modelbehandling for følsomme EU-data.
Hermes Designet med flere sandboxing-mekanismer tæt på kernen. Nyere, men med sikkerhed i fokus.	**OpenClaw** Kraftfuld og alsidig. Men højt sikkerhedsarbejde og stort angrebsareal, der kræver et isoleret miljø.

GRØNNERE · STØRRE FORBEHOLD

Leverandørens rails | kører i skyen

Du ejer stacken | lokalt / egen server

KAPACITET ER IKKE MODENHED

OpenClaw er kraftfuld, og jeg kører den dagligt. Men kapacitet er ikke det samme som modenhed. Sikkerhedssituationen trækker den ned: et stort angrebsareal vejer tungere end rå styrke. Hermes er nyere, men bygget med mere sandboxing, og vil sandsynligvis ligge højere end OpenClaw, når den er moden.

■ 4. OVERBLIK: DE FIRE VÆRKTØJER

Det vigtigste om hvert værktøj på ét sted. De fulde profiler følger på de næste sider.

OpenClaw

✓ Testet dagligt

KORT FORTALT
Kraftfuld, alsidig lokal agent på din egen maskine.

BEDST TIL
Teknisk stærke brugere, der vil eje stacken.

STYRKE
Kan en masse. Min daglige driver til research og nyheder.

FORBEHOLD
Højt sikkerhedsarbejde og stort angrebsareal. Kræver et isoleret miljø.

Claude Cowork

✓ Testet dagligt

KORT FORTALT
Modent agent-produkt i skyen, fra freelance til Enterprise.

BEDST TIL
Teams der hurtigt vil give en agent — efter konkret compliance-vurdering ved Enterprise.

STYRKE
Letteste vej ind. Spørger om lov, sandboxet, men ikke risikofrit.

FORBEHOLD
Stadig prompt injection / exfiltration-risici. Konkret review nødvendigt ved følsomme data.

Perplexity

✓ Testet hands-on

KORT FORTALT
Hybridt research-flow: lokale filer + cloud-orkestrering.

BEDST TIL
Research, der skal blive til dokumenter og slides.

STYRKE
Det bedste research-flow, jeg har set.

FORBEHOLD
Dataresidens og modelbehandling kræver vurdering for følsomme EU-data.

Hermes Agent

Under test

KORT FORTALT
Open-source agent, du selv driver lokalt eller på en server.

BEDST TIL
At eje stacken med flere sandboxing-mekanismer end OpenClaw.

STYRKE
Open-source, persistent memory, designet med mere sandboxing tæt på kernen.

FORBEHOLD
Ung. Min vurdering er foreløbig.

HVAD DER VÆLTER ET PROJEKT

Kig især på forbeholdene. Det er ikke styrkerne, der vælter et agent-projekt. Det er forbeholdene, du ikke fik taget stilling til i tide.

■ 5. OPENCLAW

✓ TESTET HANDS-ON, DAGLIGT

Hvad det er

En lokal AI-agent, der kører på din egen maskine. Den er kraftfuld og alsidig: jeg bruger den selv dagligt til research og nyheder, ikke kun til kode. Det er et af 2026's mest hypede agent-projekter, og med god grund, den leverer. Men det kræver tekniske hænder at sætte op og holde sikkert, og hypen overdøver en alvorlig sikkerhedssamtale.

DET TALER FOR	DET TALER IMOD
+ Kraftfuld og alsidig. Min daglige driver til research og nyheder.	– Højt sikkerhedsarbejde: flere høj-risiko CVE'er og mange advisories.
+ Du ejer stacken: kører lokalt, under din kontrol.	– Stort angrebsareal. Kræver et isoleret miljø, ikke din normale arbejdsmaskine.
+ Moden i kernefunktionen, den leverer.	– Microsoft meldte 19. februar 2026 ud, at OpenClaw ikke bør køre på almindelige private eller enterprise-workstations.
+ Stort økosystem og hurtige iterationer.	– Kræver tekniske hænder at sætte op og drifte sikkert.

Bedst til

Teknisk stærke brugere, der vil eje stacken og kan afsætte et isoleret miljø til den. Den kan en masse, men det er ikke et værktøj, du slår løs på maskinen med dine mails og kundedata.

SÅDAN KØRER JEG DEN SELV

Fire agenter på en gammel gamer-PC, trigget af et cron-job. Hver morgen kl. 7:30 leverer de tre nyhedshistorier i min Telegram, mens jeg sover.

Orkestratoren (StefOpenClawAI) styrer det hele og reviewer som sidste kvalitetsport. **Researcheren** scanner nettet for AI-nyheder. **Validatoren** er skeptikeren der smider det tynde ud. **Copywriteren** skriver de tre bedste historier op i min stemme.

Det der virker er kedeligt: rolleseparation, orkestrator som kvalitetsport, en indbygget skeptiker. Stabilitet er sværere end variation, og det er stabilitet der skaber værdi i drift.

SIKKERHEDSSTATUS · PR. MAJ 2026

Cyera Research afdækkede i april 2026 fire chainable sårbarheder under navnet „Claw Chain“ (CVE-2026-44112, 44113, 44115 og 44118). De er lukket i version 2026.4.22, og projektet patcher aktivt.

Men nye huller dukker op løbende. Adskillige hundrede sikkerhedsadvarsler og CVE’er er registreret, og den største risiko ligger i selve designet: en autonom agent med dine nøgler, der kører kode og henter skills udefra. Det patcher man ikke væk.

Kører du OpenClaw, så hold den på nyeste version og i et isoleret miljø. Microsofts anbefaling fra 19. februar 2026 står stadig.

*Vil du dykke ned i hvordan jeg bygger og driver min agent-sværm, så læs nummer 1 i serien: **AI-agenter i praksis** på stefanovincenti.substack.com.*

■ 6. CLAUDE COWORK

✓ TESTET HANDS-ON, DAGLIGT

Hvad det er

Den letteste vej til at give ikke-tekniske medarbejdere en rigtig AI-agent, ikke bare et chatvindue. Et modent produkt i freelance- og team-skala, og med Team og Enterprise-planer er det også enterprise-rettet med admin-kontroller og audit-logging. Den spørger om lov, før den rører noget nyt, og kører i et lokalt sandboxet miljø.

DET TALER FOR	DET TALER IMOD
+ Den absolut nemmeste vej ind for ikke-tekniske brugere.	– Låst til Claude/Anthropic-økosystemet.
+ Sandboxet og spørger om lov, før den rører nyt.	– Sandboxet, men ikke risikofrit: prompt injection og data-exfiltration er stadig relevante risici.
+ Team og Enterprise med admin-kontroller og audit-logging.	– Tunge sporbarhedskrav (finans, pharma) kræver konkret review af DPA, retention og governance.
+ Scheduler-funktionen kører fænomenalt i drift.	– Compliance API dækker endnu ikke alle Cowork-events; logging skal verificeres konkret.

Bedst til

Teams, der hurtigt vil give ikke-tekniske medarbejdere en agent. Interne opgaver på Team eller Enterprise efter konkret vurdering af data og governance.

STEFANOS NOTE: PHD MED 6-ÅRIGE FEJL

Cowork performer som en PhD-studerende med nærmest uendelig hukommelse. Den har læst alt i mappen, kobler det sammen, syntetiserer og producerer i en hastighed der er svær at matche.

Og så laver den fejl som en 6-årig ville lave. Den har stavet ord forkert i overskrifter. Den opfandt engang et helt nyt efternavn til mig og satte det på forsiden af en PowerPoint. Output der er 95 procent perfekt og 5 procent pinligt.

Du skal læse efter. Altid. Den er stærkest når den flytter, strukturerer og organiserer noget der allerede findes. Svagest når hun selv producerer nyt indhold.

COMPLIANCE: HVAD MAPPEN MÅ SE

Jeg har lige lavet en compliance-vurdering af Cowork for et dansk firma i en branche med tavshedspligt. Den korte version:

Free, Pro, Max kører på consumer-vilkår. Chats kan indgå i modeltræning hvis "Help improve Claude" er slået til. Som tommelfingerregel rødt eller gul-rødt for klientdata, fortrolige virksomhedsdata, kildekode og personoplysninger, medmindre der er en eksplicit risikovurdering, samtykke eller retligt grundlag, og passende organisatoriske kontroller.

Claude for Work, Team, Enterprise under commercial terms er en anden historie. Anthropic bruger som standard ikke inputs og outputs til træning. DPA, admin-kontroller og audit-logging er tilgængelige. Compliance API findes som kontrolplan, men dækker endnu ikke fuldt Cowork-aktivitet — logging og compliance-dækning skal verificeres konkret for de aktiviteter, man vil bruge i drift. Kan være egnet til interne opgaver med almindelige personoplysninger, hvis DPA, adgangsstyring, retention, logging og interne politikker er på plads.

Følsomme personoplysninger og fulde KYC-mapper er stadig rødt uden særskilt risikovurdering. EU-dataresidens og modelbehandling er ikke tilstrækkeligt dokumenteret til følsomme use cases uden konkret review.

FOR MICROSOFT-HUSE: HOLD ØJE MED COPILOT COWORK

Microsofts Copilot Cowork er en Microsoft 365 Copilot- og Frontier-kapabilitet, hvor Microsoft arbejder med et multimodel-setup, herunder Anthropic Claude-modeller i visse workflows. Annonceret 9. marts 2026, tilgængelig i Microsofts Frontier-program fra 30. marts og udvidet hen over foråret med mobil, skills og plugins.

Hagen for EU: Microsoft har siden januar 2026 brugt Anthropic som subprocessor for visse M365-experiences. Microsoft Learn dokumenterer eksplicit, at Anthropic-modeller er uden for EU Data Boundary-forpligtelserne. For EU-tenants er Anthropic-modeller som standard slået fra og kræver aktivt admin-tilvalg.

Er I et Microsoft-hus, er det alligevel den mest lovende enterprise-vej: én leverandør og kendte admin-kontroller. Vi venter spændt på, hvordan den udvikler sig den kommende tid.

Vil du dykke ned i hvad Cowork kan og hvad den ikke kan, så læs nummer 2 i serien: ***Claude Cowork i praksis*** *på stefanovincenti.substack.com.*

■ 7. PERPLEXITY COMPUTER / RESEARCH

✓ TESTET HANDS-ON

Hvad det er

Et research-værktøj med et hybridt local/cloud-setup. Perplexity Personal Computer på Mac kan arbejde med lokale filer og apps, men orkestrering, modeller og dele af eksekveringen ligger hos Perplexity. Den tager dig hele vejen fra research til færdigt produkt: dokumenter, slides og regneark kommer direkte ud af researchflowet.

DET TALER FOR	DET TALER IMOD
+ Det bedste research-til-deliverable flow, jeg har set.	– Hybridt local/cloud-flow: lokale filer + cloud-orkestrering og modeller.
+ Leverer færdige dokumenter, slides og regneark.	– Dataflow, DPA, retention og connector-adgang skal vurderes for følsomme data.
+ Modent og hurtigt at komme i gang med.	– EU-dataresidens og modelbehandling er ikke tilstrækkeligt dokumenteret til følsomme use cases uden konkret review.
+ Lav teknisk tærskel, ingen opsætning.	– Min vurdering: til følsomme EU-data er den nok ikke der endnu.

Bedst til

Research-tungt arbejde, der skal ende som et konkret produkt, når dataene ikke er følsomme. Til ikke-følsomt materiale er det svært at slå.

STEFANOS NOTE

Flowet er imponerende. Men „imponerende“ er ikke det samme som „GDPR-klar“. Til følsomme EU-data skal du have plan-type, DPA, dataflow og connector-adgang på plads, før den kører i drift.

Nummer 3 i serien — Perplexity Personal Computer i praksis — udkommer i juni på stefanovincenti.substack.com.

■ 8. HERMES AGENT FRA NOUS RESEARCH

INSTALLERET, UNDER TEST

STATUS: UNDER TEST

Jeg har installeret Hermes og er i gang med at teste den. Vurderingen herunder er derfor foreløbig: den bygger på min første hands-on og på dokumentationen, ikke på måneders drift. Jeg opdaterer, når jeg ved mere.

Hvad det er

En open-source AI-agent fra Nous Research, en seriøs udfordrer til OpenClaw. Selv-hostet og kan køre lokalt (Mac, Linux, WSL2) eller på en server. Persistent memory, egne skills og flere sandboxing-mekanismer tæt på kernen. Nyere end OpenClaw, men designet med sikkerhed i fokus.

DET TALER FOR	DET TALER IMOD
+ Designet med flere sandboxing-mekanismer tæt på kernen end OpenClaw.	– Jeg er midt i min egen test, så vurderingen er foreløbig.
+ Open-source (MIT-licens), fuld indsigt og kontrol.	– Ungt produkt, ikke så gennemprøvet som OpenClaw.
+ Selv-hostet med persistent memory.	– Open-source betyder også: du står selv for drift og sikkerhed.
+ Egne skills, agenten kan blive skarpere over tid.	

Bedst til

Tekniske brugere, der vil eje stacken og vægter sandboxing-mekanismer højt. Et reelt open-source alternativ til OpenClaw for de teknisk stærke.

STEFANOS NOTE

Jeg er i gang med at teste Hermes nu og melder tilbage, når jeg ved mere. Har du kørt den i produktion? Skriv til mig: jeg vil meget gerne høre om det. Vil du selv prøve, har jeg en separat trin-for-trin installationsguide: „Din egen lokale Hermes AI-agent“.

■ 9. SÅDAN VÆLGER DU

Start med dine krav, ikke med værktøjet. Fire match skiller hurtigt feltet. Find den række, der ligner din situation.

Skal ikke-tekniske kollegaer i gang hurtigt?	→	**Claude Cowork.** Laveste tærskel, ingen opsætning. Team eller Enterprise efter konkret vurdering ved tunge compliance-miljøer.
Vil du eje stacken, og har du tekniske hænder?	→	**OpenClaw i et isoleret miljø.** Eller **Hermes**, hvis du vil have flere sandboxing-mekanismer og en open-source profil.
Research, der skal blive til dokumenter og slides, og ikke-følsomme data?	→	**Perplexity Computer / Research.** Det stærkeste flow fra research til færdigt produkt.
Følsomme EU-data eller tung compliance (finans, pharma, life science)?	→	Ingen af de fire uden et konkret review. Perplexity kræver vurdering af dataflow og modelbehandling, Cowork kræver review af DPA og governance, OpenClaw kræver et isoleret miljø. For en stor enterprise er en enterprise-moden vej som **Copilot Cowork** ofte klogere.

Fire spørgsmål, før du vælger

1. **Hvem skal bruge den?**
   Tekniske udviklere, eller almindelige medarbejdere uden teknisk baggrund?
2. **Hvor følsomme er dine data?**
   Offentligt materiale, eller følsomme EU- og kundedata?
3. **Vil du eje stacken?**
   Eller er leverandørens rails i skyen helt fine for jer?
4. **Hvor moden skal den være?**
   Tåler I friktion og tidlige fejl, eller skal den bare virke?

CAPABILITY GAP-PRINCIPPET

Det handler sjældent om teknisk niveau. Det handler om hvor skarpt opgaven er skåret. De der får agenter til at skabe værdi har valgt en lille, kedelig, gentagen opgave med klart input, klart output og klare grænser. De der kæmper, vil bygge noget stort med det samme. Capability gap er afstanden mellem hvad agenterne kan, og hvad dine folk kan få dem til.

BUNDLINJEN

Svar på de fire, så har du dit valg. Bygget på dine krav, ikke på hvad der lyder vildest eller ser flottest ud.

■ 10. OM STEFANO & QUICK REFERENCE

Stefano Vincenti, GenAI-strateg og -arkitekt

25 år i IT og digital transformation, nu på fuld tid med generativ AI. Stefano hjælper nordiske ledelsesteams med at lukke afstanden mellem, hvad AI kan, og hvad deres folk rent faktisk bruger det til. Det sker gennem rådgivning, workshops og train-the-trainer-programmer. Chief AI Officer og medstifter af BotTellMe. Ekstern lektor ved IT-Universitetet i København og ved DIS Copenhagen. Partner hos TryZone.

ET SPØRGSMÅL TIL DIG

Har du kørt Hermes Agent i produktion? Så vil jeg meget gerne høre om det. Skriv til mig på LinkedIn. Det er præcis den slags praksis-erfaring, der gør næste version af denne guide bedre.

Følg Stefano

LinkedIn	linkedin.com/in/stefanovincenti
Blog & guides	aitrainer.dk
Nyhedsbrev	stefanovincenti.substack.com
BotTellMe, GenAI på jeres egne data	bottellme.com
TryZone, rådgivning	tryzone.dk

Kilder & yderligere læsning

• Microsoft Security Blog · OpenClaw-warning, 19. feb 2026 · microsoft.com/security/blog
• Cyera Research · Claw Chain CVE-2026-44112/44113/44115/44118 · cyera.com
• Microsoft 365 Blog · Copilot Cowork, 9. marts 2026 · microsoft.com/microsoft-365
• Microsoft Learn · Flex routing & EU Data Boundary · learn.microsoft.com
• Nous Research · Hermes Agent docs · hermes-agent.nousresearch.com
• Anthropic Help Center · Compliance API · support.claude.com
• General Analysis · Claude Compliance API coverage and gaps · generalanalysis.com
• Perplexity · Personal Computer on Mac · perplexity.ai/personal-computer