Empistos arkitektur: privat AI på jeres egen infrastruktur, bygget til at holde

Hvordan Empisto er bygget op, hvordan jeres data bliver inden for egne mure og hvorfor I takket være det modulære design kan tage ny AI i brug uden at starte forfra. Til IT-, sikkerheds- og forretningsledere der vurderer privat AI.

10. november 2026



empisto.ai · lokal · privat · pålidelig

Indhold

01 Resumé

02 Hvorfor arkitekturen betyder noget for AI

03 Designprincipper

04 Overblik over platformen

05 Modulær og fremtidssikret

06 Identitet og adgang

07 Jeres dokumenter

08 Fra spørgsmål til svar

09 AI-modeller

10 Applikationer og værktøjer

11 Sikkerhed og databeskyttelse

12 Udrulning og drift

13 Delt ansvar

14 Læs mere

01 Resumé

Empisto er en privat AI-platform som en virksomhed kører på sine egne servere. Medarbejderne stiller spørgsmål med deres egne ord og får svar fra virksomhedens egne dokumenter, hvert svar med sine kilder. Applikationer til projekter, diagrammer, dataanalyse og forretningssystemer virker direkte i den samme assistent.

Tre idéer går igen i hele arkitekturen. Jeres data bliver på infrastruktur I selv har kontrol over, og intet kræver internettet for at virke. Adgangen afgøres af jeres egne regler før der søges i et eneste dokument, og alt vigtigt bliver logget. Endelig er hver del modulær, så platformen kan tage nye AI-modeller, værktøjer og datakilder til sig efterhånden som de kommer, uden et migreringsprojekt.

Denne beskrivelse forklarer hvordan det lader sig gøre, i den detaljegrad en IT-, sikkerheds- eller forretningsleder har brug for til at vurdere det. Den gennemgår byggestenene, login og adgang, hvordan dokumenterne bruges, hvad der sker når nogen stiller et spørgsmål, AI-modellerne, applikationer og værktøjer, sikkerhed og databeskyttelse, og til sidst hvordan en installation udrulles og drives.

HVOR DEN KØRER

På jeres egne servere, i jeres egen bygning eller i jeres private datacenter.

JERES DATA

Dokumenter, samtaler og logs bliver på jeres infrastruktur.

AI-MODELLER

Åbne modeller der kører på jeres egen GPU-server, valgt pr. team.

LOGIN

De arbejdskonti medarbejderne allerede har, via jeres identityprovider.

INTERNET

Ikke nødvendigt for driften. Enhver forbindelse udadtil er valgfri, og det er jer der slår den til.

TELEMETRI

Ingen. Der sendes intet tilbage til Empisto.

02 Hvorfor arkitekturen betyder noget for AI

Med de fleste AI-tjenester skal virksomheden sende sine dokumenter og spørgsmål til andres servere. Når det drejer sig om kontrakter, patientjournaler, økonomiske data eller noget der er omfattet af en fortrolighedsaftale, er det ofte dér samtalen slutter. Forbrugsafregning giver et problem mere: jo flere der bruger værktøjet, desto sværere bliver regningen at forudsige.

Dertil kommer en tredje risiko som er let at overse. AI udvikler sig hurtigere end noget andet område inden for IT. Årets bedste model er ikke næste års bedste model, og de værktøjer folk vil koble til den,

skifter hele tiden. En platform der er bygget op om én model, én leverandør eller én måde at arbejde på, skal skiftes ud netop som den begynder at tjene sig hjem.

Empistos arkitektur tager højde for alle tre. Den kører inden for jeres mure, på en fast licens i stedet for et taxameter, og den er bygget af udskiftelige dele der er forbundet med åbne standarder.

03 Designprincipper

Én grænse. Alle dele af Empisto kører i jeres eget miljø. Platformen behøver ingen forbindelse til internettet eller til Empisto for at virke, og enhver valgfri forbindelse udadtil er noget en administrator bevidst slår til.

Adgang før svar. Empisto afgør hvilke dokumenter en person må bruge, før der overhovedet søges. Et svar kan aldrig bygge på materiale som personen ikke havde lov til at se.

Alle dele kan skiftes ud. Hver byggesten løser én opgave bag en veldefineret grænseflade. En bedre model eller en ny dokumentlæser afløser den gamle uden at resten berøres.

Udbyg i stedet for at bygge om. Nye funktioner kommer til som applikationer på den samme platform, og hver af dem arver det samme login, de samme adgangsregler og den samme auditlog.

Spor I selv kan efterprøve. Svarene viser deres kilder. Vigtige handlinger skrives i en auditlog der ikke kan ændres. Genereret indhold er markeret som genereret.

04 Overblik over platformen

Figur 1 viser Empisto i fugleperspektiv. Medarbejderne bruger platformen i en webbrowser. En sikker login-gateway er den eneste del der kan nås fra jeres netværk. Bag den står fire lag for arbejdet, og jeres eksisterende systemer bliver hvor de er og kobles på lagene derfra.

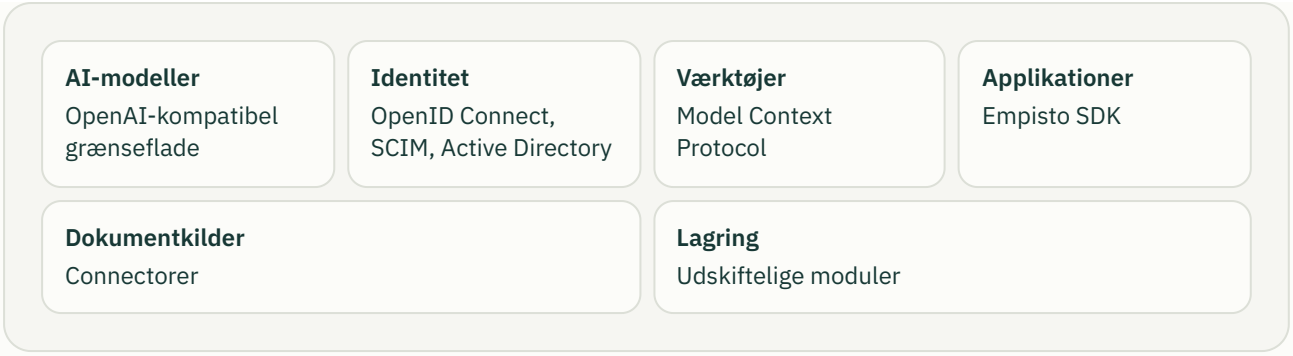


Figur 1. Empisto på jeres servere. Jeres systemer kobles på nedefra, mens cloud-AI bliver udenfor, bag en port der som standard er lukket.

Apps er det medarbejderne arbejder med: AI-assistenten, dokumentbiblioteket og applikationer som Projekter, Diagrammer og Dataanalytikeren. **Kontrol** afgør hvem der må se og gøre hvad, og fører log over hvad der er sket. **Viden** gør jeres dokumenter til noget assistenten kan søge i og citere. **AI-modeller** står for at læse og skrive, på hardware I selv ejer.

05 Modulær og fremtidssikret

En AI-platform skal kunne tage imod modeller, værktøjer og datakilder som endnu ikke findes, og det er Empisto bygget til. Hver del kobles på gennem en veldefineret grænseflade, og hvor der findes en åben branchestandard, bruger Empisto den. Figur 2 viser hvor nye dele kobles på.



Figur 2. Her kobles nye dele på. Hver af dem kan tilføjes eller skiftes ud uden at resten skal ændres.

Del	Sådan kobles den på	Hvad det betyder for jer
AI-modeller	Den OpenAI-kompatible grænseflade som de fleste modelservere bruger	Kør flere modeller side om side, vælg dem pr. team, og tag næste generation i brug ved at tilføje den, ikke ved at migrere
Identitet	OpenID Connect, SCIM og Active Directory	Behold jeres identityprovider og jeres brugerkatalog. Empisto retter sig efter dem
Værktøjer	Model Context Protocol, den åbne standard for at forbinde AI med andre systemer	Kobl forretningssystemer på som værktøjer, hvert enkelt godkendt af en administrator
Applikationer	Empisto SDK	Nye funktioner kommer til som applikationer på det samme fundament og under de samme regler
Dokumentkilder	Connectorer: filservere, NAS-enheder, SharePoint og OneDrive	Nye kilder kommer til som connectorer og læses der hvor de ligger, ligesom de eksisterende
Lagring	Ét udskifteligt modul til hver opgave	Database, søgeindeks, secrets vault og dokumentlæser kan hver især skiftes ud for sig

Delene er gennemprøvede open source-komponenter, og det betyder også at jeres egne folk eller en uafhængig revisor kan undersøge hvordan de virker. Vælger I en anden komponent senere, er det en ændring af ét modul, ikke en ny platform. Jeres dokumenter, arbejdsområder, rettigheder og applikationer bliver hvor de er.

06 Identitet og adgang

Log ind med de konti I allerede har

Medarbejderne logger ind via jeres identityprovider, for eksempel Microsoft Entra ID eller en hvilken som helst anden udbyder der understøtter OpenID Connect. Empisto kan også synkronisere brugere og grupper med jeres brugerkatalog via SCIM eller Active Directory. Når IT fjerner en medarbejder, forsvinder adgangen til Empisto samtidig. Der er ingen separate adgangskoder at holde styr på.

Grupperne i brugerkataloget bliver til rettigheder. En administrator bestemmer hvilke grupper der får hvilken rolle, på hele platformen eller i et enkelt arbejdsområde, og ændringer i brugerkataloget slår igennem uden at nogen skal røre ved Empisto.

Arbejdsområder der følger jeres organisation

Et arbejdsområde er et separat rum for et team, et selskab, et projekt eller en sag. Det har sine egne medlemmer, samtaler og indstillinger og får adgang til de dokumentbiblioteker det har brug for. Arbejdsområder kan lægges inden i hinanden, så de afspejler organisationens opbygning, og indstillingerne arves nedad i træet. Så kan en afdeling bruge sin egen model eller sine egne regler uden at gentage konfigurationen.



Figur 3. Arbejdsområder lagt inden i hinanden efter organisationens opbygning. Indstillingerne arves nedad i træet, mens de personlige arbejdsområder står for sig selv.

Alle har desuden et personligt arbejdsområde der kun tilhører dem selv. Ingen administrator kan læse det. I et fælles arbejdsområde kan teamet som standard se samtalerne, men en samtale kan også holdes privat for den der startede den.

Biblioteker og roller

Dokumenterne ligger i biblioteker, og hvert bibliotek tildeles de arbejdsområder der må bruge det. Rollerne afgør hvad folk kan gøre: administratorer styrer platformen eller et enkelt arbejdsområde, vidensansvarlige tager sig af biblioteker og dokumenter, og medlemmer læser og stiller spørgsmål. Hver applikation lægger sine egne rettigheder ovenpå.

Empisto kopierer ikke rettigheder fra jeres filservere. Hvem der må se et dokument, afgøres af det bibliotek det hører til, og af de roller I tildeler. På den måde er adgangen samlet ét sted og nem at gennemgå.

07 Jeres dokumenter

Dokumenterne kommer ind i Empisto på to måder. Medarbejderne kan uploade dem i browseren, eller en administrator kobler en filserver eller en NAS på, hvorefter Empisto læser dokumenterne der hvor de ligger, med ren læseadgang. Tilkoblede kilder gennemgås efter en tidsplan I selv fastlægger, så nye og ændrede filer kommer med, og slettede filer fjernes. Intet skal flyttes eller migreres.

Empisto læser de formater virksomheder rent faktisk bruger: PDF (også scannede sider), Word, PowerPoint, Excel og CSV, websider og tekstfiler, billeder samt gængse data- og tegningsformater. Tekst i scanninger og billeder genkendes på engelsk, græsk og polsk. Overskrifter, tabeller og sidetal bevares, så et svar kan pege på præcis den side og det afsnit det kommer fra.

Hvert dokument behandles på jeres egne servere af jeres egne modeller. Intet sendes ud af huset for at blive læst, oversat eller indekseret.

08 Fra spørgsmål til svar

Figur 4 følger ét spørgsmål fra det øjeblik det bliver stillet, til svaret står på skærmen. Det tager få sekunder, og hvert eneste trin foregår på jeres servere.

1	LOG IND	Personen genkendes via jeres identityprovider, uden en ny adgangskode.
2	TJEK ADGANG	Empisto afgør hvilke biblioteker personen må bruge i dette arbejdsområde, før der søges i noget.
3	FIND UDDRAG	Søgningen leder kun i disse biblioteker og vælger de uddrag der besvarer spørgsmålet.
4	SKRIV SVARET	En sprogmodel på jeres egne servere læser uddragene og skriver svaret.
5	KILDER OG LOG	Svaret kommer med nummererede kilder, og søgningen skrives i auditloggen.

Figur 4. Et spørgsmåls vej. Adgangen afgøres før søgningen, ikke ved at filtrere bagefter.

To ting er særligt vigtige for et sikkerhedsteam. Fordi adgangen afgøres før søgningen, bliver et uddrag fra et bibliotek som personen ikke må læse, aldrig hentet frem overhovedet. Og fordi hvert svar angiver sine kilder, kan medarbejderne selv tjekke det de får at vide.

Hvis nogen bruger et værktøj undervejs i en samtale, for eksempel til at oprette en opgave i Projekter, skal vedkommende først bekræfte enhver handling der ændrer noget.

09 AI-modeller

Empisto arbejder med åbne AI-modeller der kører på jeres egen GPU-server, via den grænseflade de fleste modelservere bruger. Platformen er ikke bundet til én bestemt model eller leverandør. I vælger selv modellerne: en sprogmodel til svarene, en søgemodel til at finde uddrag og eventuelt modeller til billeder og tale.

Modellerne vælges pr. arbejdsområde. Den juridiske afdeling kan arbejde med én model mens resten af virksomheden bruger en anden, og en ny model kan prøves af i ét team før alle andre får den. Kommer der en bedre åben model, er det en konfigurationsændring at tage den i brug, ikke et projekt.

Hardware. Modellerne kører på GPU'er fra NVIDIA eller AMD. Dimensioneringen afhænger af hvilke modeller I vælger og hvor mange der bruger dem samtidig, og den indgår i hvert prisoverslag vi laver.

Cloudmodeller. Empisto leveres uden nogen cloud-AI sat op, og ved normal brug forlader intet jeres netværk. Til de teams der vil bruge en cloudmodel til en del af deres arbejde, tilbyder Empisto en løsning med egne kontroller: slået fra som standard, tilladt eller afvist pr. arbejdsområde, følsomme dokumenter holdt inde, personoplysninger fjernet først og hver forespørgsel logget.

Genereret indhold er markeret. Svar, eksporterede dokumenter og genereret lyd markeres som AI-genereret for at understøtte gennemsigtighedsforpligtelserne i EU's AI-forordning.

10 Applikationer og værktøjer

Applikationer

Applikationer giver assistenten nye funktioner uden at træde uden for platformens regler. De bruger alle det samme login, overholder de samme adgangsregler og skriver i den samme auditlog. De er bygget med Empisto SDK, og hver installeret applikation er en verificeret version.

Applikation	Hvad den gør
Projekter	Boards, opgaver og arbejdsgange som assistenten kan oprette og opdatere fra en samtale
Diagrammer	Laver svar og tabeller om til diagrammer
Dataanalytiker	Besvarer spørgsmål om regneark ved at køre analyser i et isoleret miljø uden netværksadgang og med kun læseadgang til data
ERP-forbindelse	Spørgsmål om ordrer, lager og fakturaer, med kun læseadgang

Værktøjer

Med værktøjer kan assistenten arbejde sammen med andre systemer. De kobles på via Model Context Protocol, en åben standard, så den samme tilgang virker for både dagens og morgendagens systemer.

Hvert værktøj skal igennem de samme kontroller:

1. **Godkendelse.** En administrator godkender hvert værktøj før nogen kan bruge det, og godkender det igen hvis det bliver ændret.
2. **Pr. arbejdsområde.** Et arbejdsområde får kun de værktøjer det bliver tildelt.
3. **Bekræftelse.** Et værktøj der vil ændre noget, beder først personen om at bekræfte.
4. **Logning.** Hver gang et værktøj bruges, bliver det skrevet i auditloggen.

11 Sikkerhed og databeskyttelse

Netværksgrænsen

Medarbejderne kan kun nå Empisto gennem den sikre login-gateway, over en krypteret forbindelse. De øvrige dele er ikke eksponeret for brugerne, men arbejder inde på jeres servere og i jeres interne netværk. Empisto har ikke brug for noget fra internettet for at køre, og der er ingen telemetri, ingen brugsrapportering, intet opdateringstjek og ingen licensserver. Der sendes intet tilbage til os.

De få forbindelser udadtil der kan forekomme, er alle valgfrie og under jeres kontrol.

Forbindelse	Hvornår den bruges	Hvem der bestemmer
Jeres identityprovider	Når medarbejderne logger ind, hvis jeres udbyder er en cloudtjeneste som Microsoft Entra ID	Jeres valg af identityprovider
Eksterne værktøjer	Kun hvis en administrator tilføjer et værktøj uden for jeres netværk	Administratorens godkendelse, pr. arbejdsområde
Websider i en chat	Slået fra som standard. Er funktionen slået til, kun websteder der står på listen	Administrator
AI-modelservere	Kun de servere jeres administratorer registrerer	Administrator

En installation kan også sættes op som air-gapped, og så er eksterne værktøjer og websider slået helt fra.

Jeres data

Dokumenter, samtaler, søgeindekset og auditloggen gemmes alle på jeres egne servere. De adgangskoder og nøgler Empisto skal bruge, opbevares i en dedikeret secrets vault, aldrig i konfigurationsfiler. Data i hvile krypteres af jeres infrastruktur, med disk- eller volumenkryptering på serverne.

Auditloggen

Vigtige handlinger bliver logget: ændringer af arbejdsområder, medlemmer og roller, af biblioteker og dokumenter, af modeller og indstillinger, hver søgning og hvert svar samt al brug af værktøjer. Ingen kan ændre eller slette en post gennem Empisto, heller ikke administratorer. Loggen viser hvem der

gjorde hvad og hvornår, ikke indholdet af det der blev spurgt om. Autoriserede administratorer kan gennemgå og eksportere den.

Opbevaring og sletning af data

Medarbejderne kan eksportere deres samtaler til Word, PDF eller Markdown. Der kan fastsættes en opbevaringsperiode for hver type data, og én persons data kan eksporteres eller slettes efter anmodning, mens auditloggen bevarer sporet af hvad der er sket.

12 Udrulning og drift

Empisto kører som en række containere på Linux-servere. De fleste virksomheder starter med to servere, én til platformen og én til AI-modellerne. Med en passende GPU kan begge dele køre på samme maskine.



Figur 5. En typisk installation, og hvordan den vokser. Platform- og AI-rollerne kan også dele én server med nok GPU-hukommelse.

Installation og opdateringer. Empistos teknikere installerer og opdaterer platformen sammen med jeres IT-team, på et tidspunkt I vælger, ud fra signerede og versionerede udgivelser. Til netværk uden internetadgang findes en offlinepakke.

Overvågning. Hver tjeneste rapporterer sin egen tilstand, og logs sendes videre til de overvågningsværktøjer I allerede bruger.

Backup. En komplet backup omfatter databaserne, søgeindekset og dokumentlageret. Vi kan levere en krypteret og planlagt backupprocedure der dækker alle tre.

13 Delt ansvar

Når I kører AI på jeres egen infrastruktur, fordeles arbejdet på en måde som det er værd at blive enige om tidligt.

Område	Empisto står for	I står for
Hardware og styresystem	Råd om dimensionering og en referencekonfiguration	Serverne, styresystemet og dets opdateringer

Område	Empisto står for	I står for
Netværk	Listen over de forbindelser Empisto har brug for	Firewalls, netværkssegmenter og sikkerhedscertifikatet
Identitet	Tilkobling af Empisto til jeres identityprovider og brugerkatalog	Identityprovideren, dens grupper og personerne i dem
Databeskyttelse	Adgang pr. bibliotek og rolle, auditloggen	Diskkryptering på serverne, og hvem der må logge ind på dem
Backup	Backupproceduren	At køre backup og teste gendannelse
AI-modeller	Anbefalinger og opsætning	Valget af modeller og deres licensvilkår
Opdateringer	Nye udgivelser og hvordan de installeres	Servicevinduer og godkendelse

14 Læs mere

Arkitektursiden viser den samme platform i et enkelt sprog, med en interaktiv gennemgang af ét spørgsmål. Sikkerhedssiden besvarer de seks spørgsmål sikkerhedsteams stiller først, og siden om modulært design viser hvordan hver del kan skiftes ud. Vil I have en teknisk samtale med folkene bag Empisto eller et prisoverslag til jeres miljø, så start her.