Microsoft 365 Copilot

Beskyttelse af datasikkerheden i AI-æraen

En vejledning til it-ledere

E-bog

Denne vejledning er skrevet til it-ledere, der har brug for at fremme indførelsen af AI og samtidig beskytte dataene i deres organisationer. Det vil hjælpe dig med at forstå de risici, AI udgør for datasikkerheden og databeskyttelsen, samtidig med at du får den indsigt, der er nødvendig for at kunne lede din virksomheds AI-transformation med tryghed.

Indhold

01
De nye regler for AI-drevet arbejde

02
Forståelse af AI's indvirkning på datasikkerhed

03
Udfordringen med skygge-AI

04
BYOAI-virkeligheden

05
Labyrinten af lovkrav

06
En sikkerhedsfokuseret struktur til evaluering af AI-løsninger

07
Microsoft 365 Copilot: AI, du kan stole på

08
Den sikre vej til AI-transformation

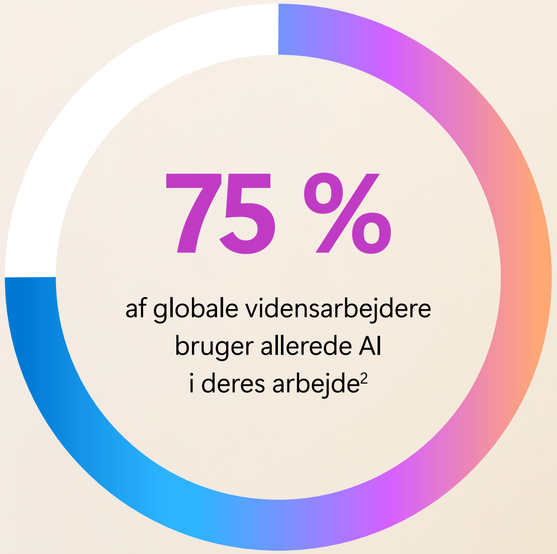
01

De nye regler for AI-drevet arbejde

Generativ AI åbner nye døre for innovation og hjælper teams med at arbejde hurtigere og smartere end nogensinde før. For fremsynede organisationer er AI ikke bare endnu en ny teknologi – det er en forretningsmæssig nødvendighed, der er afgørende for, hvordan de opererer, leverer værdi og opretholder en konkurrencemæssig fordel.

Men denne hurtige implementering giver nye og større udfordringer, som it-chefer er nødt til at håndtere og kontrollere proaktivt. AI-systemer kan aktivt søge efter og kombinere oplysninger på tværs af hele dataøkosystemet, hvilket øger sikkerhedsrisiciene i forhold til traditionelle værktøjer. På trods af AI's hurtige udbredelse er det kun **1 %** af organisationerne, der rapporterer, at de har fuldt integreret AI i deres arbejdsprocesser med korrekte sikkerhedsprotokoller.[1] Ved at implementere robuste sikkerheds- og styringsfunktioner fra starten af dit AI-forløb kan dit team effektivt beskytte følsomme data, opretholde overholdelseskravene og beskytte organisationens oplysninger – samtidig med at innovationen blomstrer.

AI-implementeringsbølgen er her allerede



02

Forståelse af AI's indvirkning på datasikkerhed

Før vi dykker ned i specifikke udfordringer, er det vigtigt at forstå, hvordan AI forandrer datasikkerhedslandskabet fundamentalt. I modsætning til traditionel software, der kun får adgang til data, når den specifikt bliver bedt om det, kan generativ AI aktivt behandle, analysere og oprette indhold baseret på alle de oplysninger, den modtager.

Det udgør en væsentlig forskel af flere årsager:

- AI-værktøjer kan opdage forbindelser mellem data, som mennesker kan overse
- De kan automatisk syntetisere oplysninger på tværs af flere kilder
- De kan generere nyt indhold, der indeholder elementer fra følsomme input

Dine traditionelle sikkerhedsværktøjer er sandsynligvis ikke designet med disse egenskaber i tankerne. Mens konventionel software følger forudsigelige stier, når den får adgang til data, kan AI tage uventede ruter gennem dit informationsøkosystem og potentielt eksponere følsomme data på måder, du ikke havde forventet.

Dette grundlæggende skift kræver nye tilgange til sikkerhed og datastyring, som specifikt adresserer, hvordan AI skal interagere med informationsaktiverne i din organisation.

03

Udfordringen med skygge-AI

Uanset hvor du er i dit AI-implementeringsforløb, finder dine medarbejdere allerede deres egne løsninger og skaber det, der kaldes "skygge-AI".

Denne uautoriserede brug giver betydelige blinde vinkler i dit sikkerhedsforsvar. Når medarbejderne deler virksomhedsdata med eksterne AI-systemer, omgår de eksisterende sikkerhedskontroller og skaber sårbarheder, som de fleste organisationer ikke er klar til at håndtere.

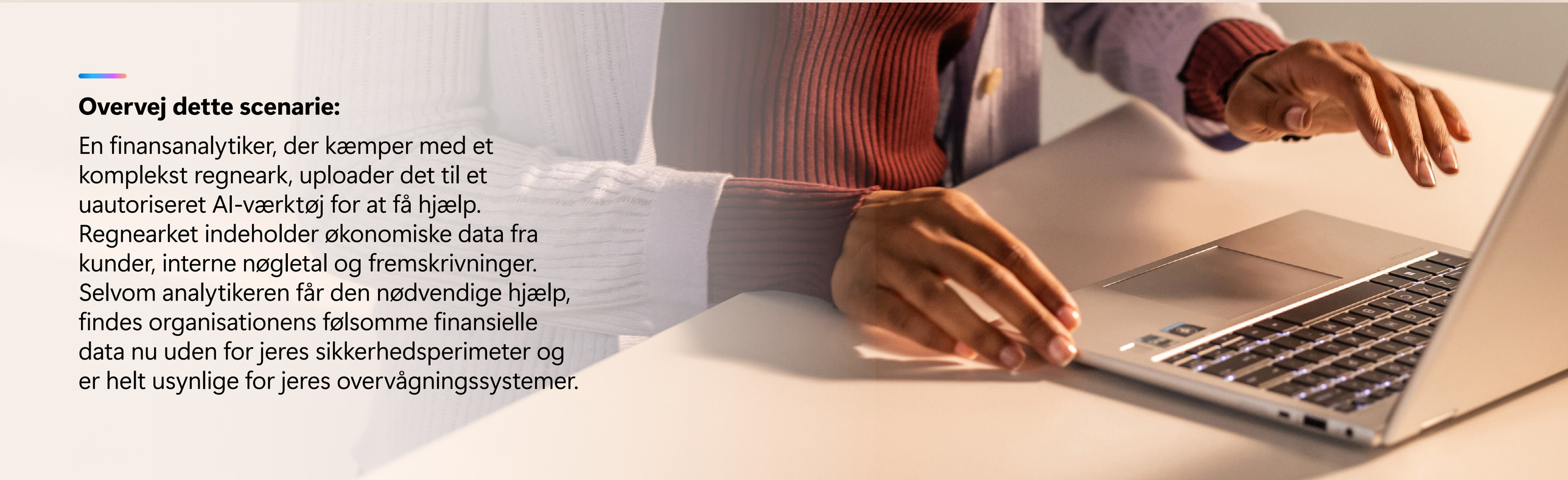
Skygge-AI er ikke bare et sikkerhedsproblem – det kan være et symptom på uopfyldte produktivitetsbehov i din organisation. Når medarbejderne bruger ikke-sanktionerede værktøjer, viser de, hvor dine officielle systemer ikke lever op til deres krav. Håndtering af skygge-AI kræver både stærkere styring og forbedrede produktivitetsløsninger.

Derfor dukker skygge-AI op:

- Medarbejderne er ivrige efter at øge deres produktivitet via AI's imponerende funktioner
- Den daglige arbejdsbyrde kan ikke klares på den tid og med den energi, der er til rådighed
- Teams står over for et stigende pres for at skulle levere mere med de samme ressourcer
- AI-værktøjer til forbrugere tilbyder øjeblikkelige løsninger uden godkendelsesbarrierer
- Officielle it-indkøbsprocesser kan ikke holde trit med innovationstempoet

Risiciene ved skygge-AI:

- Ingen indsigt i, hvilke virksomhedsdata der bliver behandlet af eksterne AI-systemer
- Ingen garanti for, at fortrolige oplysninger ikke bliver gemt
- Ingen ensartede sikkerhedsstandarder på tværs af forskellige AI-platforme
- Ingen revisionsmuligheder med henblik på overholdelse
- Ingen integration med din eksisterende sikkerhedsinfrastruktur



Overvej dette scenarie:

En finansanalytiker, der kæmper med et komplekst regneark, uploader det til et uautoriseret AI-værktøj for at få hjælp. Regnearket indeholder økonomiske data fra kunder, interne nøgletal og fremskrivninger. Selvom analytikeren får den nødvendige hjælp, findes organisationens følsomme finansielle data nu uden for jeres sikkerhedsperimeter og er helt usynlige for jeres overvågningssystemer.

04

BYOAI-virkeligheden

Uden en klar vejledning fra ledelsen tager medarbejderne i stigende grad AI-implementering i egen hånd – **78 %** af AI-brugerne anvender en "bring your own AI"-tilgang (BYOAI) på deres arbejde.[2] Denne tendens er endnu mere markant i små og mellemstore virksomheder, hvor **80 %** af medarbejderne anvender BYOAI-praksisser.[2]

Denne ikke-sanktionerede tilgang giver betydelige ulemper. Medarbejdere holder ofte brugen af AI hemmelig – **52 %** er tilbageholdende med at indrømme, at de bruger AI til vigtige opgaver, og **53 %** er bekymrede for, om brugen af AI får dem til at se ud, som om de kan udskiftes.[2] Dette hemmelighedskræmmeri forhindrer ikke bare organisationer i at realisere alle fordelene ved en strategisk implementering af AI, men den skaber også alvorlige sikkerhedsrisici i et miljø, hvor ledere nævner cybersikkerhed og datafortrolighed som deres **#største** bekymring.[2]

Med tanke på AI's udbredte brug og uundgåelige vækst er spørgsmålet ikke, om du vil tillade AI i din organisation – det handler om, hvordan du leverer en sikker løsning, der lever op til dine medarbejderes behov, samtidig med at din organisations data bliver beskyttet.

05

Labyrinten af lovkrav

Rammer og love om databeskyttelse og -sikkerhed skaber endnu et lag af kompleksitet, når man implementerer AI. Selvom nogle rammer er specielt designet til AI-styring, har andre bredere anvendelsesformål, der stadig påvirker den måde, du håndterer oplysninger på – og straffene for overtrædelser er stadig meget hårde.

Når dine medarbejdere bruger AI-værktøjer uden ordentlig overvågning, kan de komme til at begå overholdelsesovertrædelser. AI gør denne risiko større, fordi den kan få adgang til, kombinere og eksponere regulerede oplysninger på måder, som traditionelle teknologier ikke kan.

Vigtige forordninger, der påvirker din brug af AI:

GDPR

EU's generelle forordning om databeskyttelse (GDPR) giver folk kontrol over deres personoplysninger og kræver klart samtykke til at behandle dem

EU AI Act

EU's omfattende ramme, der er specielt designet til at regulere systemer med kunstig intelligens baseret på deres risikoniveauer

HIPAA

Denne amerikanske føderale sundhedslov opstiller strenge standarder for håndtering af beskyttede sundhedsoplysninger

NIST AI Risk Management Framework

Denne frivillige amerikanske vejledning hjælper organisationer med at håndtere risici i forbindelse med design, udvikling og implementering af AI-systemer

Overholdelsesrisiciene med AI:

- Kundedata, der behandles på servere uden for godkendte regioner
- Personoplysninger, der bruges uden passende samtykke
- Følsomme data, der fastholdes i systemer uden passende opbevaringskontroller
- Ingen revisionsspor for, hvordan beskyttede oplysninger tilgås og bruges
- AI-genereret indhold, der krænker sektorspecifikke overholdelseskrav

Disse overtrædelser kan medføre alvorlige konsekvenser:

- Store bøder (GDPR-bøder kan være på op til **4 %** af din globale omsætning)[4]
- Krav til at meddele berørte parter om brud på datasikkerheden
- Retssager fra de berørte personer
- Dette kan skade din virksomheds omdømme og kundernes tillid

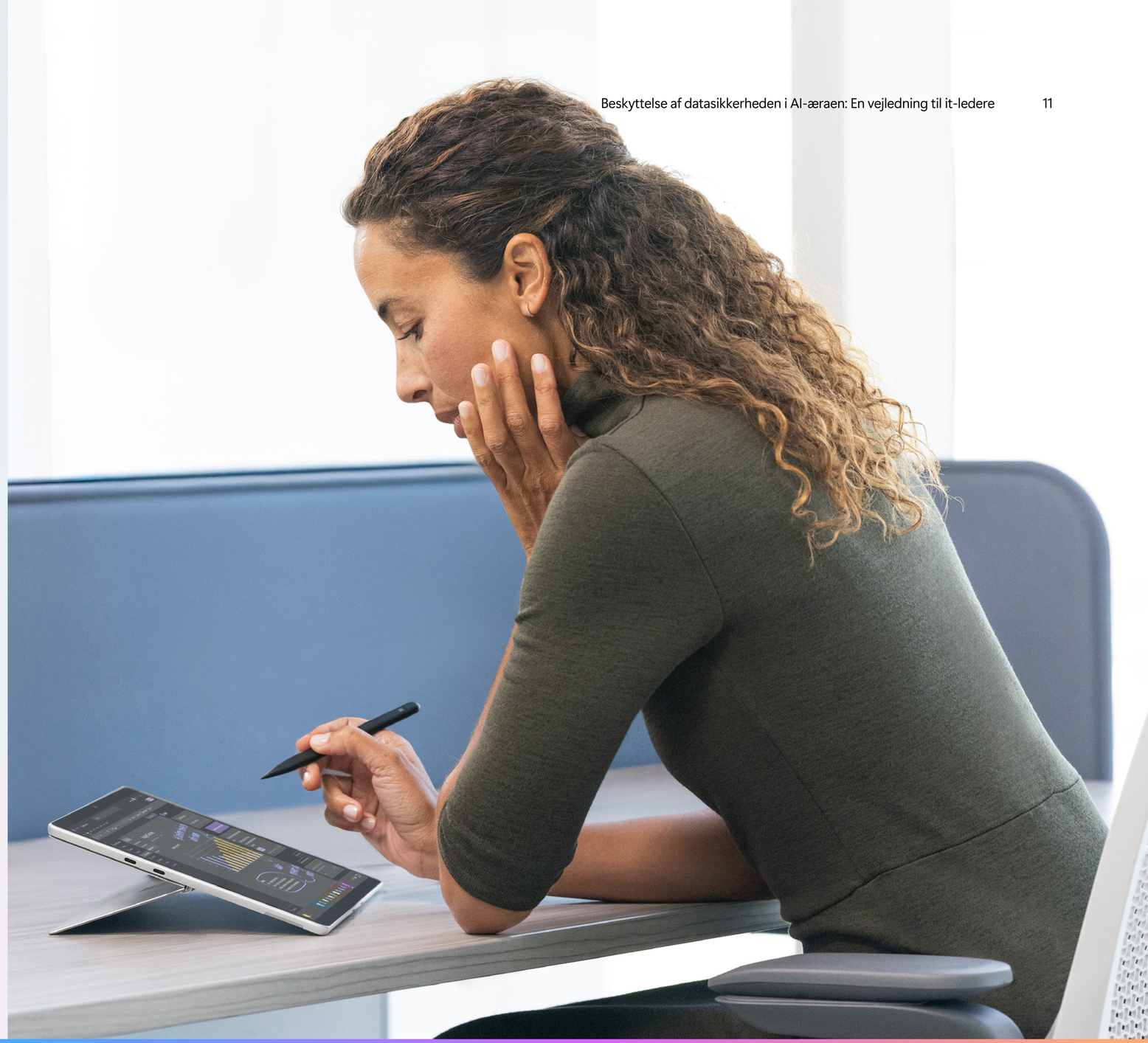
I takt med at brugen af AI vokser over hele din organisation, har du brug for styring, der hjælper folk med at arbejde effektivt, samtidig med at organisationen overholder de regler, der påvirker din virksomhed og dine kunder.

06

En sikkerheds-fokuseret struktur til evaluering af AI-løsninger

Med skygge-AI, BYOAI og forordninger, der skaber betydelige risici, har du brug for en struktureret tilgang til evaluering af AI-løsninger, der sikrer, at de kan hjælpe din organisation med at skabe innovation – samtidig med at du beskytter følsomme data og sikrer overholdelse af skiftende lovkrav.

Følgende struktur stiller seks enkle spørgsmål for at vurdere, om en AI-platform leverer varen på begge fronter.



Spørgsmål 1

Tilbyder den sikkerhed i virksomhedsklassen fra bunden?

Med den rigtige løsning skifter din sikkerhed fra bare at reagere på problemer, efter at de er opstået, til proaktivt at søge efter sårbarheder i din organisations data – før de udvikler sig til større problemer.

Kig efter løsninger, der:

- Giver overblik i realtid på tværs af hele dit dataøkosystem
- Automatisk identificerer potentielle datarisici, før de bliver til hændelser
- Beskytter følsomme oplysninger på alle niveauer

Spørgsmål 2

Kan den nemt indføre og forbedre eksisterende sikkerhedskontroller?

Din organisations sikkerhedspolitikker bør fungere problemfrit med AI. Din AI-løsningsudbyder bør respektere og kunne integreres i dine eksisterende sikkerhedsstrukturer – og ikke kræve, at du opretter helt nye.

Kig efter løsninger, der:

- Problemfrit indfører dine eksisterende sikkerhedspolitikker, følsomhedsetiketter og databeskyttelsesindstillinger
- Anvender detaljerede adgangskontroller på individuelt niveau, så ingen brugere har uretmæssig adgang til data
- Aktivt markerer forsøg på at underminere adgangskontroller

Spørgsmål 3

Omfatter det indbygget styrings- og databeskyttelseskontroller?

Da AI-værktøjer fungerer mere proaktivt, skal dine sikkerhedsforanstaltninger også være proaktive. Implementering af stærk datastyring skaber klare grænser for, hvor dine medarbejdere kan skabe sikker innovation uden at bringe følsomme oplysninger i fare.

Kig efter løsninger, der:

- Centraliserer AI-styringen med automatiseret håndhævelse af politikker på tværs af alle aktiviteter
- Inkluderer tidlig registrering af overdeling af data
- Tilpasser sig de lovgivningsmæssige rammer for at sikre kompatibel AI-brug

Spørgsmål 4

Kan den implementeres konsekvent på tværs af hele organisationen?

Dine medarbejdere har deres egne arbejdsformer og deres egne tidsplaner, og de kan sidde overalt i verden. AI bør komme alle til gavn.

Kig efter løsninger, der:

- Tilbyder problemfri opsætning og nem implementering af AI i daglige arbejdsprocesser
- Giver fleksibel adgang lige fra AI-chat uden omkostninger til skalerbare agentløsninger
- Hjælper medarbejderne med at opbygge AI-kompetencer og integrere dem i deres arbejde

Spørgsmål 5

Kan den integreres problemfrit på tværs af eksisterende strukturer?

Din virksomhed opererer i øjeblikket med sin egen digitale infrastruktur af softwareprogrammer, apps og meget mere.

Kig efter løsninger, der:

- Kan integreres problemfrit med dine værktøjer og programmer for at minimere afbrydelser
- Giver en kontinuerlig AI-oplevelse på tværs af alle apps, så arbejdet kan flyde problemfrit mellem værktøjerne
- Automatiserer og optimerer opgaver inden for eksisterende arbejdsprocesser

Spørgsmål 6

Har brugerne mulighed for at skabe innovation?

Helt grundlæggende bør AI transformere den måde, arbejdet udføres på. Det handler ikke kun om automatisering – det handler om at forbedre produktiviteten og skabe innovation.

Kig efter løsninger, der:

- Omdanner tidskrævende opgaver til strømlinede processer
- Automatiserer rutineprægede opgaver
- Giver medarbejderne mulighed for at frigøre tid og fokusere på prioriteter

07

Microsoft 365 Copilot: AI, du kan stole på

Microsoft 365 Copilot er den løsning med generativ AI, som er udviklet til at levere robust sikkerhed, styring og adgangskontrol – hvilket giver sikker implementering og vedvarende innovation. Den forbedrer produktiviteten med intuitive værktøjer som Copilot Chat, som arbejder der, hvor du selv gør, og Copilot Studio, hvor dit team kan opbygge tilpassede AI-agenter uden kodningsfærdigheder.

Copilot integreres problemfrit i dit Microsoft 365-miljø, hvor løsningen nedarver brugertilladelser, følsomhedsetiketter, politikker til forebyggelse af datatab og geografiske krav til opbevaring af data – uden ekstra konfiguration. Ved at integrere AI i de værktøjer, som dine medarbejdere allerede bruger, afhjælper Copilot sikkerhedsrisici og holder samtidig dataene inden for dit betroede Microsoft 365-miljø.

Microsofts forpligtelser sikrer, at din organisation bevarer kontrollen:

- Dine data er i sikkerhed, når de er inaktive og under transport
- Dine data bliver ikke brugt til at træne AI-modeller
- Du vælger, hvilke oplysninger der skal ligge i skyen
- Du er beskyttet mod AI-risici vedrørende sikkerhed og ophavsret

Specialudviklede styringsværktøjer som Copilot Control System og SharePoint Advanced Management giver it-teams det overblik, de kontroller og de overvågningslogfiler, der er nødvendige for at kunne opretholde overholdelsen af angivne standarder.

Med Microsoft 365 Copilot behøver du ikke at vælge mellem innovation og sikkerhed – du kan få begge dele.

08

Den sikre vej til AI-transformation

AI-revolutionen udgør en enestående mulighed for, at it-ledere kan levere strategisk værdi ved at finde den rette balance mellem innovation og sikkerhed.

Ved at implementere sikre AI-værktøjer som Microsoft 365 Copilot kan du give medarbejderne adgang til værktøjer, som kan skabe større produktivitet, samtidig med at du eliminerer risikoen for skygge-AI. Vejen frem handler om at muliggøre innovation på en sikker måde. Dit lederskab inden for sikker AI-implementering vil positionere it-afdelingen som en transformerende kraft, som hjælper din organisation med at stortrives i denne nye tidsalder, samtidig med at data er i sikkerhed og overholder reglerne.

Kom i gang med Microsoft 365 Copilot

Kilder:

[1] "Superagency in the workplace: Empowering people to unlock AI's full potential," McKinsey & Company, 28. januar 2025. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work.

[2] "AI på arbejdspladsen er her. Nu kommer den vanskelige del". Microsofts indeks over arbejdstendenser, 8. maj 2024. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part.

[3] "Kan AI omstrukturere arbejdet?" Microsofts indeks over arbejdstendenser, 9. maj 2023. https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work.

[4] "Forordning (EU) 2016/679 fra Europa-Parlamentet og Rådet af 27. april 2016 om beskyttelsen af fysiske personer i forhold til behandlingen af personoplysninger og vedrørende den frie bevægelse af sådanne data samt ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen)," Europa-Parlamentet og Rådet for Den Europæiske Union, 27. april 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.