Microsoft 365

Fra tilsyn til indsigt: Håndtering af risici ved skygge-AI

Indholdsfortegnelse

Introduktion 03

Hvad er skygge-AI? Og hvorfor er synlighed vigtigt? 04

Skygge-AI på arbejdspladsen: Eksempler på scenarier og potentielle risici 05

Fem måder at håndtere risici ved skygge-AI på..... 06

Opdag og administrer risiciene ved skygge-AI med Microsoft 365 E3..... 07

Tag det næste skridt i dit AI-implementeringsforløb..... 08

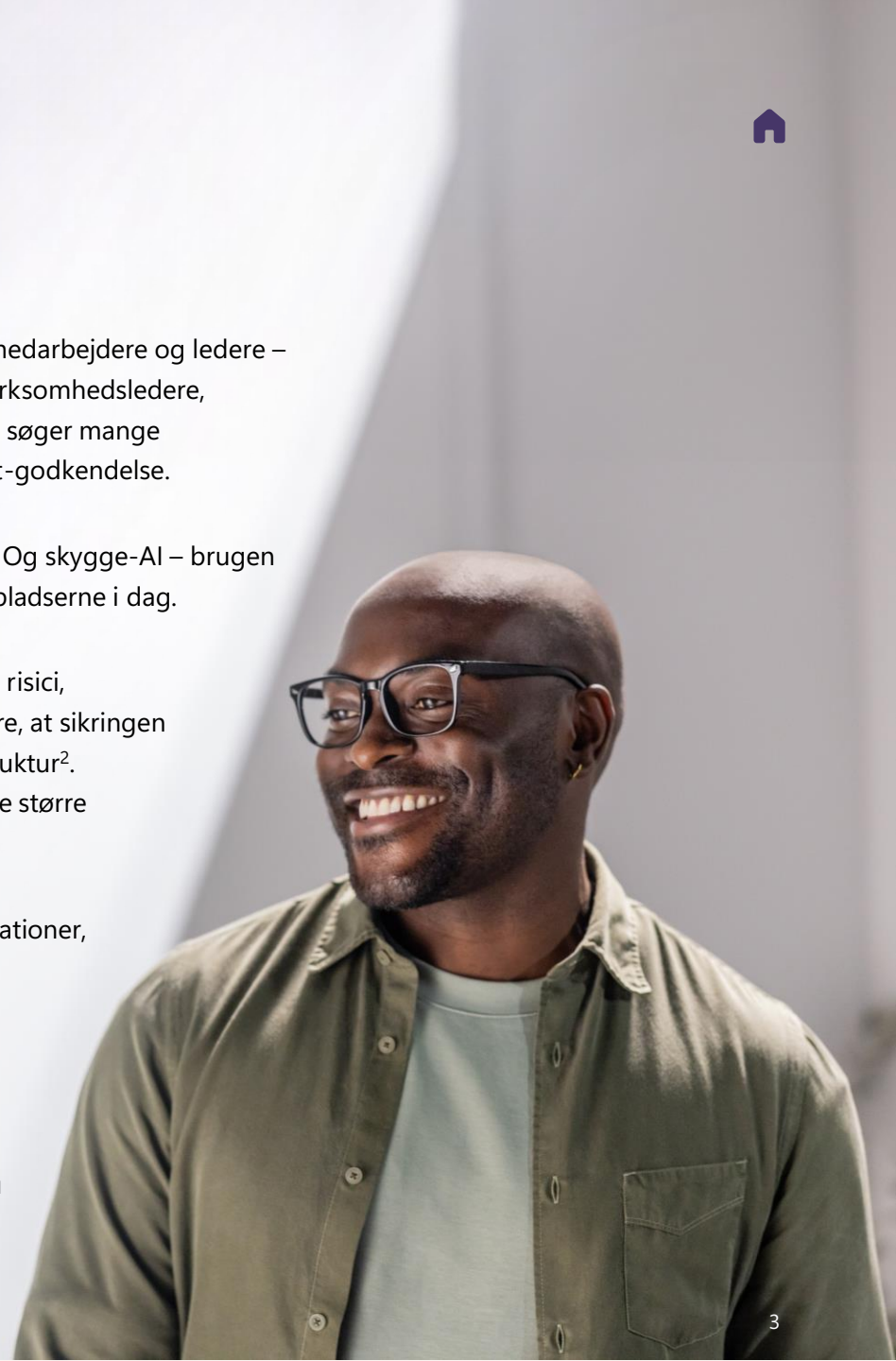
Introduktion

I den seneste Work Trend Index-rapport oplyste over 80 % af de adspurgte vidensarbejdere på tværs af 31 lande – både medarbejdere og ledere – at de følte, at de manglede tid eller energi til at gøre deres arbejde. Derudover rapporterede over 50 % af de adspurgte virksomhedsledere, at produktiviteten var nødt til at stige, for at de kunne nå deres mål[1]. Ifølge Microsofts Work Trend Index-rapport fra 2024 søger mange medarbejdere efter værktøjer med generativ AI for at lukke dette hul og begynder at bruge dem uden at afvente officiel it-godkendelse.

Når værktøjer kører uden for it-afdelingens synlighed, kan de udgøre sikkerheds- og compliance-risici for organisationer. Og skygge-AI – brugen af AI-værktøjer uden godkendelse fra it-afdelingen – har udviklet sig til at blive den nyeste form for skygge-IT på arbejdspladserne i dag.

I takt med at indførelsen af AI tager fart, arbejder virksomhedslederne på at holde sig på forkant og afbøde de potentielle risici, som disse værktøjer kan udgøre. I en nylig iSMG-undersøgelse rapporterede over 70 % af de adspurgte virksomhedsledere, at sikringen af datasikkerhed og databeskyttelse er den primære udfordring ved at integrere generativ AI i den eksisterende it-infrastruktur[2]. Derudover rapporterede over 90 % af de adspurgte CIO'er og CTO'er, at generativ AI allerede har medført eller vil medføre større investeringer i cybersikkerhed i deres organisation[3].

I denne e-bog kan du udforske typiske scenarier, hvor der anvendes skygge-AI, få indsigt i de potentielle risici for organisationer, lære fem metoder til at håndtere disse risici og se, hvordan Microsoft 365 E3 kan hjælpe.



[1] **Den årlige Work Trend Index-rapport fra 2025,** Microsoft, Inc., april 2025. Microsoft analyserede undersøgelsesdata fra 31.000 fuldtidsansatte eller selvstændige vidensarbejdere på tværs af 31 lande mellem den 6. februar 2025 og den 24. marts 2025, tendenser på arbejdsmarkedet fra LinkedIn og flere billioner Microsoft 365-produktivitetssignaler.

[2] **iSMG's anden årlige undersøgelse af generativ AI: Business Rewards vs. Security Risks,** Baseret på svar fra over 360 forretnings- og cybersikkerhedsmedarbejdere i tredje kvartal på tværs af 6 regioner (Nordamerika, Europa, Asien, Sydamerika, Australien og Afrika)

[3] **The AI Security Balancing Act: From Risk to Innovation," NTT DATA, juni 2025,** Baseret på data fra en NTT DATA-undersøgelse af over 2.300 ledende GenAI-beslutningstagere, herunder 1.500 topledere på tværs af 34 lande.

Hvad er skygge-AI? Og hvorfor er synlighed vigtigt?

Skygge-AI refererer til brugen af værktøjer og applikationer med kunstig intelligens af medarbejdere uden eksplicit godkendelse eller tilsyn fra it-afdelinger, ofte uden for officielle sikkerheds- og compliance-strukturers synsfelt. Når medarbejdere søger efter metoder til at øge produktiviteten og håndtere deres stigende arbejdsbyrde, kan de vælge at bruge disse uautoriserede løsninger til at effektivisere opgaver, samarbejde eller generere nyt indhold – ofte uden at være klar over de potentielle risici, der er forbundet med dette. Skygge-AI er ikke synlig for it-afdelingen, hvilket gør det svært for organisationer at vide, hvilke applikationer der bliver brugt, og hvilke der udgør de største risici.

Derfor er synlighed omkring skygge-AI vigtigt

Når it-afdelingen ikke har kendskab til en applikation eller en tjeneste, kan it-afdelingen ikke beskytte eller understøtte den. Dette *hul i synligheden* gør det svært at identificere, håndtere eller minimere potentielle trusler præcist i forhold til eksponering af følsomme data, manglende overholdelse af lovkrav og manglende kontrol over fortrolige oplysninger. It- og forretningsledere har brug for at have overblik over den skygge-AI, der anvendes i deres organisation, håndtere de nye risici, som er forbundet med brugen af AI, og beslutte, hvilke værktøjer der skal tillades under de rigtige sikkerhedsforanstaltninger. Muligheden for organisationer er at transformere skygge-AI fra en risiko til en mulighed for at nytænke den måde, arbejdet udføres på – og på en sikker måde. For at gøre dette skal der være en bedre balance – så medarbejdere får mulighed for at anvende nyttige AI-værktøjer inden for en styret og sikker struktur for at afbøde potentielle risici.

INDSIGT

Du kan ikke beskytte det, du ikke kan se. Når it-afdelingen ikke er klar over, at en applikation eller en tjeneste bliver brugt, kan it-afdelingen ikke beskytte den. Det er kernen i problemet med skygge-AI – og det understreger, hvorfor der er behov for en ny tilgang. Det er ikke praktisk at forbyde alle eksterne værktøjer, hvis medarbejderne føler, at disse AI-værktøjer er afgørende for, at de kan nå deres mål. I stedet skal organisationer bringe skygge-AI frem i lyset – for at få indblik i, hvad medarbejderne bruger, indføre passende kontroller og tilbyde sikre og godkendte alternativer, der opfylder organisationens behov. Udfordringen er kort sagt at give teams mulighed for at bruge AI *uden* at gå på kompromis med sikkerheden.

Skygge-AI på arbejdspladsen: Eksempler på scenarier og potentielle risici

Skygge-AI opstår via medarbejdere, der kan have et ønske om at øge deres produktivitet og effekt eller afprøve en ny teknologi. Nedenfor ses flere fiktive eksempler, der illustrerer, hvordan ikke-godkendte AI-værktøjer kan blive brugt, og hvilke potentielle risici de kan medføre:

Rolle	Eksempel på scenarie	Potentielle risici via ikke-godkendte værktøjer
Marketing	Brug af et værktøj med generativ AI til at oprette marketingtekster eller -design med brug af virksomhedens branddata.	Lækage af følsomme brand- eller produktoplysninger; manglende kontrol over, hvordan en ekstern AI-tjeneste kan gemme eller bruge virksomhedens kreative aktiver.
Finans	Upload af virksomhedens økonomidata til en AI-drevet analyse- eller visualiseringstjeneste for at få hurtig indsigt.	Eksponering af fortrolige økonomidata (budgetter, prognoser) over for en tredjepart; potentielle compliance-overtrædelser (f.eks. GDPR), hvis kunde- eller medarbejderdata medtages uden de rigtige sikkerhedsforanstaltninger.
Kundesupport	Deling af kundedata eller chatudskrifter fra support til et AI-værktøj for at udarbejde svar eller opsummere sager.	Overtrædelse af regler om databeskyttelse og datahåndtering – følsomme kundeoplysninger kan blive gemt uden for virksomhedens systemer; ingen garantier for dataopbevaring eller korrekt sletning fra AI-leverandørens side.
Frontlinje – detailhandel	Butikschefer, der bruger AI-baserede planlægningsapps på deres telefoner til at optimere vagtplaner for medarbejdere.	Virksomhedens medarbejderdata (navne på medarbejdere, vagtplaner) uploades til en ikke-godkendt app, hvilket medfører risiko for problemer med databeskyttelse. Der kan opstå konflikter i vagtplaner eller overtrædelser af virksomhedens politikker, hvis AI-forslagene ikke stemmer overens med arbejdslovgivningen.
Frontlinje – sundhedssektor	Sygeplejersker eller læger bruger en AI-chatbot til at hjælpe med at udarbejde patientplejenoter eller svare på medicinske spørgsmål.	Patienters sundhedsoplysninger (PHI) kan blive eksponeret for en ekstern tjeneste uden nogen sikkerhedsforanstaltninger, hvilket overtræder compliance- og fortrolighedskrav. AI-baseret medicinsk rådgivning kan også være ubekræftet, hvilket udgør en sikkerhedsrisiko.

I hvert af ovenstående tilfælde havde den enkelte medarbejder gode intentioner og ønskede at øge produktiviteten, men organisationen kan pådrage sig risici som følge heraf.

Virksomhedsdata kan ende med at være spredt ud på uautoriserede platforme, hvilket giver *udfordringer med datastyringen*. Ikke-godkendte apps kan introducere malware eller sikkerhedsrisici og udvide angrebsfladen uden for it-afdelingens ansvarsområde. Der kan også være compliance-relaterede konsekvenser. Hvis der opstår problemer med et skygge-AI-værktøj fra it-supportafdelingens synspunkt, kan helpdesk muligvis ikke hjælpe slutbrugerne, da supportmedarbejderne ikke har nogen indsigt i eller kontrol over det.

Fem måder at håndtere risici ved skygge-AI på

Med den rigtige strategi og de rigtige værktøjer kan du forvandle skygge-AI fra en potentiel trussel til en mulighed for at fremme en kultur med sikker innovation. Styrk dine teams med AI-produktivitetsværktøjer, *samtidig med* at du bevarer den kontrol, der er nødvendig for at beskytte din virksomhed. Det er et skifte fra at sige "nej, aldrig nogensinde" til at sige "ja – men med de rette sikkerhedsforanstaltninger." Følgende fem tips er udviklet til at hjælpe dig med at håndtere og få kontrol over skygge-AI i din organisation:

01 Opdag udbredelsen af skygge-it i din organisation for at evaluere og prioritere risici

Du kan ikke beskytte det, du ikke kan se. Få overblik over de applikationer, der bruges i din organisation, via dine aktivitetslogfiler. Når du kender de apps, der er i brug, kan du identificere de rette værktøjer til at håndtere følsomme data, samtidig med at du registrerer dem, der ikke lever op til dine sikkerheds- og compliance-politikker. Med denne indsigt kan du træffe en mere velunderbygget beslutning om, hvilke applikationer du vil tillade, overvåge eller begrænse for at afbøde potentielle risici.

02 Opnå hurtige resultater med sikkerheds- og compliance-politikker

Aktivér eller anvend rettelser af politikker for at kunne afbøde potentielle risici bedre i forbindelse med brug af skygge-AI. Du kan bruge politikker for betinget adgang til at begrænse brugen af applikationer med høj risiko, anvende politikker for forebyggelse af datatab på følsomme oplysninger for at modvirke overdeling og datalækage samt håndhæve grundlæggende multifaktorgodkendelse og enhedskompatibilitet for alle brugere. Disse handlinger reducerer hurtigt de mest iøjnefaldende risici, også selvom du endnu ikke har det fulde overblik over de AI-applikationer, der bliver brugt.

03 Uddan medarbejderne om de potentielle risici ved skygge-AI

Ofte er medarbejderne ikke klar over de risici, som brugen af ikke-godkendte AI-værktøjer kan udgøre for en organisation. Italesæt risiciene ved skygge-AI ofte med velplacerede advarsler om forebyggelse af datatab, påmindelser om virksomhedspolitikker og korte træningssessioner for at skubbe brugerne i retning af en mere sikker praksis uden rigid håndhævelse.

04 Levér godkendte AI-værktøjer for at afbøde risiciene yderligere

Tilbyd medarbejderne godkendte AI-værktøjer som alternativer til uautoriserede værktøjer, hvor det er muligt. En god måde at reducere skygge-AI på er at dække de mest almindelige use cases i din organisation med en godkendt løsning. Det giver it-afdelingen mulighed for at bevare overblikket og kontrollen, samtidig med at brugerne får support til at løse de problemer, der opstår.

05 Etabler løbende styring

Integrer kontroller i din it-styringsrutine – gennemgå aktivitetslogfiler og rapporter regelmæssigt, opdater politikker, i takt med at nye AI-tjenester kommer frem, og hold ledelsen informeret om fremskridt (f.eks. reduktioner i brugen af ikke-tilladte apps eller forhindrede hændelser). Det vil hjælpe dig med at afbøde potentielle risici nu og i fremtiden, i takt med at landskabet udvikler sig.

Ved at implementere ovenstående handlinger kan du styrke både innovationen og sikkerheden.

Medarbejderne kan bruge godkendte AI-løsninger på arbejdspladsen, og it-afdelingen bevarer kontrol og compliance for disse løsninger.

Opdag og administrer risiciene ved skygge-AI med Microsoft 365 E3

Microsoft 365 E3 giver organisationer mulighed for at opdage skygge-it, vurdere potentielle risici og implementere sikkerheds- og compliance-politikker *uden* at hæmme innovationen. Denne pakke af integrerede produktivitets-, sikkerheds- og administrationsfunktioner kan give dig mulighed for at adressere udfordringerne ved skygge-AI direkte.

Microsoft 365 E3-løsning	Sådan hjælper den dig med at håndtere potentielle risici i forbindelse med skygge-AI
Cloud App Discovery	**Opdag og håndter ikke-godkendte applikationer.** Cloud App Discovery giver dig mulighed for at uploade aktivitetslogfiler og oprette snapshot-rapporter for at få overblik over mere end 31.000 cloud-apps – herunder over 400 applikationer med generativ AI. Den giver dig mulighed for at se, hvad der bliver brugt i din organisation, af hvem og hvor ofte. Disse oplysninger giver dig mulighed for at træffe velunderbyggede beslutninger om, hvilke apps du vil tillade eller begrænse brugen af.
Microsoft Purview Data Loss Prevention (DLP)	**Afhjælp lækager af følsomme data.** Med Microsoft Purview DLP kan du definere og anvende politikker, der registrerer følsomme oplysninger og blokerer eller begrænser deling på tværs af Microsoft 365-tjenester for mails og filer. Du kan f.eks. definere en regel, der overvåger, gennemgår eller forhindrer brugere i at dele følsomme oplysninger via mail eller fildeling og advarer brugeren.
Microsoft Entra ID P1	**Administrer adgangen til cloud-apps.** Microsoft Entra ID P1 giver mulighed for at anvende politikker for betinget adgang til at kontrollere, hvem der kan få adgang til hvilke applikationer og under hvilke betingelser. Du kan f.eks. vælge at kræve multifaktorgodkendelse eller begrænse antallet af logonforsøg med virksomhedens legitimationsoplysninger på de apps, som du vurderer som højrisikable. Microsoft Entra ID P1 giver adgang til cloud-ressourcer for de rette personer på enheder, der opfylder kravene, under godkendte betingelser – samtidig med at adgangen til ikke-godkendte apps bliver begrænset.
Microsoft Intune P1	**Håndhæv politikker for brug af enheder og apps.** Microsoft Intune P1 giver dig mulighed for at tillade, at administrerede enheder, der opfylder kravene, bruges til arbejde, og løsningen giver dig værktøjer til at administrere disse enheder. Den kan f.eks. forhindre installation af ikke-godkendt software på virksomheds-pc'er eller implementere konfigurationer, der begrænser adgangen til bestemte websteder eller tjenester.
Microsoft Defender for Endpoint P1	**Begræns trafikken til ikke-godkendte webadresser.** Microsoft Defender for Endpoint P1 hjælper dig med at reducere risici fra websteder, der vurderes som risikable, ved at blokere trafik til en ikke-godkendt webadresse fra administrerede enheder. Medarbejdere, der forsøger at besøge et kendt risikabelt AI-websted på en af virksomhedens bærbare computere, vil f.eks. blive forhindret i at få adgang til det.

Tag det næste skridt i dit AI-implementerings-forløb →

Det hele starter med opmærksomhed, de rigtige værktøjer og en proaktiv plan. Microsoft 365 E3 giver din organisation de nødvendige værktøjer til at opstille et robust sikkerhedsfundament og en stærk styringsstruktur for AI-løsninger. Du vil kunne få indsigt i ikke-tilladte værktøjer, indføre politikker til beskyttelse af følsomme data og bevare kontrollen over både brugeradgang og enhedssikkerhed. Gør dig klar til at bevæge dig fra en reaktiv tilgang (hvor man finder og blokere skygge-AI, efter at den er dukket op) til en mere proaktiv tilgang, hvor brugen af AI dirigeres ind i sikre og administrerede kanaler. Tag AI-sikkerhedsvurdering, og find ud af, hvordan du kan styrke dit sikkerhedsforsvar for AI. Få mere at vide om de funktioner, der er inkluderet i Microsoft 365 til virksomheder.