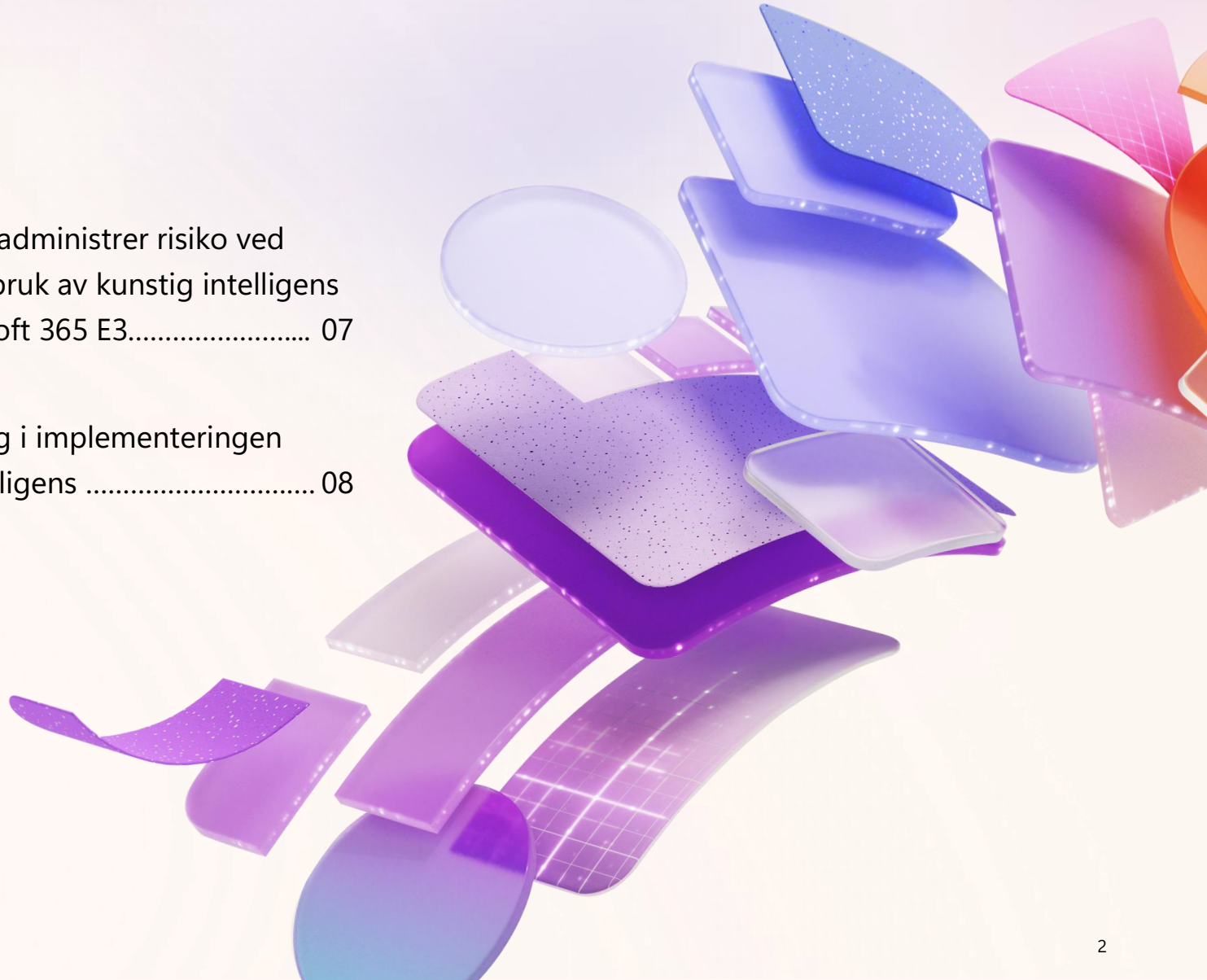
Microsoft 365

Fra tilsyn til innsikt: Håndtering av risikoer ved uautorisert bruk av kunstig intelligens

Innholdsfortegnelse



Innledning

I en nylig arbeidstrendindeksrapport svarte over 80 % av kunnskapsarbeidere i 31 land – deriblant ansatte og ledere – at de opplever å ikke ha nok tid eller energi til å utføre arbeidet sitt. I tillegg rapporterte over 50 % av de spurte bedriftslederne at produktiviteten må økes for å nå målene[1]. Ifølge Microsofts arbeidstrendindeksrapport for 2024 tar mange ansatte i bruk verktøy med generativ kunstig intelligens for å tette dette gapet, og de venter ikke på offisiell IT-godkjenning før de begynner å bruke verktøyene.

Når verktøyene er utenfor IT-avdelingens kontroll, kan de utgjøre en risiko for sikkerheten og etterlevelsen for bedriften. Og bruk av KI-verktøy uten IT-godkjenning fremstår som den nyeste formen for uautoriserte verktøy på dagens arbeidsplasser.

Nå som kunstig intelligens tas i bruk i stadig større grad, jobber virksomhetsledere for å ligge i forkant og redusere de potensielle risikoene disse verktøyene kan medføre. I en nylig iSMG-rapport oppgav over 70 % av de spurte bedriftslederne at personvern og datasikkerhet er den største utfordringen ved å integrere generativ kunstig intelligens med eksisterende IT-infrastruktur[2]. I tillegg rapporterte over 90 % av IT- og teknologiledere som deltok i undersøkelsen, at generativ kunstig intelligens allerede har ført til eller vil føre til økte investeringer i cybersikkerhet i bedriften deres[3].

I dette dokumentet kan du lese om vanlige scenarioer med uautorisert bruk av kunstig intelligens, forstå hvilke risikoer dette kan medføre for bedriften, få fem strategier for å håndtere disse risikoene, og se hvordan Microsoft 365 E3 kan hjelpe.

[1] **Microsofts årlige arbeidstrendindeksrapport fra april 2025.** Microsoft analyserte spørreundersøkelsesdata fra 31 000 heltidsansatte eller selvstendig næringsdrivende kunnskapsarbeidere i 31 land mellom 6. februar 2025 og 24. mars 2025, arbeidsmarkedstrender fra LinkedIn, og billioner av produktivitetssignaler fra Microsoft 365.

[2] **iSMG Second Annual Generative AI Study: Business Rewards vs. Security Risks,** Basert på undersøkelsessvar fra over 360 bedrifts- og cybersikkerhetseksperter i tredje kvartal i seks regioner (Nord-Amerika, Europa, Asia, Sør-Amerika, Australia og Afrika)

[3] **Balansekunsten innen KI-sikkerhet: From Risk to Innovation», NTT DATA, juni 2025,** Basert på data fra en NTT DATA-undersøkelse blant over 2300 ledende beslutningstakere innen generativ kunstig intelligens, deriblant 1500 toppledere i 34 land.

Hva er uautorisert bruk av kunstig intelligens? Og hvorfor er innsyn viktig?

Uautorisert bruk av kunstig intelligens er når ansatte bruker teknologien uten eksplisitt godkjenning eller tilsyn fra IT-avdelingen, ofte utenfor kontroll av offisielle sikkerhets- og etterlevelsesrammeverk. Når ansatte søker måter å øke produktiviteten på og håndtere de økende kravene i arbeidsmengden, kan de ty til slike ikke-godkjente løsninger for å effektivisere oppgaver, samarbeide eller skape nytt innhold, ofte uten å være klar over de potensielle risikoene dette innebærer. Uautorisert bruk av kunstig intelligens er ikke synlig for IT, noe som gjør det vanskelig for bedrifter å vite hvilke apper som brukes og hvilke som utgjør den største risikoen.

Hvorfor oversikt over uautorisert bruk av kunstig intelligens er viktig

Når IT ikke kjenner til en app eller tjeneste, kan de ikke sikre eller støtte den. Dette *innsynsgapet* gjør det vanskelig å nøyaktig kartlegge, håndtere eller redusere risikoer for eksponering av sensitive data, brudd på regelverk og tap av kontroll over virksomhetens informasjon. IT- og forretningsledere må skaffe seg oversikt over uautorisert bruk av kunstig intelligens som brukes i bedriften, håndtere de fremvoksende risikoene knyttet til KI-bruk, og avgjøre hvilke verktøy som skal tillates med de riktige kontrollmekanismene. Muligheten for bedrifter er å gjøre uautorisert bruk av kunstig intelligens om fra en risiko til en mulighet til å innovere hvordan arbeidet utføres – på en sikker måte. For å oppnå dette må det etableres en bedre balanse – slik at ansatte kan utnytte nyttige KI-verktøy innenfor et regulert og sikkert rammeverk for å begrense mulige risikoer.

INNSIKT

Du kan ikke sikre det du ikke ser. Når IT-avdelingen ikke er klar over at en app eller tjeneste brukes, kan de ikke sikre den. Dette er kjernen i problemet med uautorisert bruk av kunstig intelligens – og det fremhever hvorfor en ny tilnærming er nødvendig. Å bare forby alle eksterne verktøy er ikke praktisk hvis ansatte føler at disse KI-verktøyene er avgjørende for at de skal kunne nå målene sine. I stedet må bedriftene få oversikt over uautorisert bruk av kunstig intelligens. Det vil si oversikt over hvilke verktøy ansatte bruker, og deretter implementere relevante kontroller og tilby sikre, godkjente alternativer som dekker bedriftens behov. Utfordringen er kort sagt å styrke medarbeiderne med kunstig intelligens *uten* å gå på akkord med sikkerheten.

Uautorisert bruk av kunstig intelligens på arbeidsplassen: Eksempelscenarioer og potensiell risiko

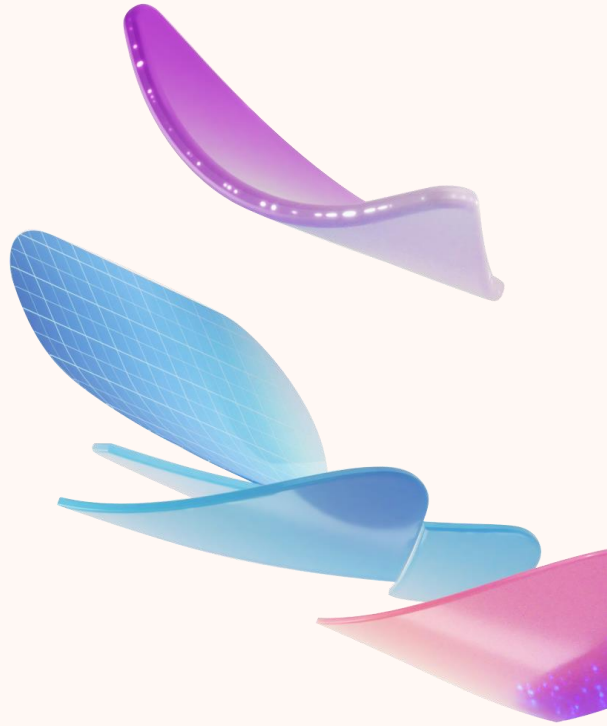
Uautorisert bruk av kunstig intelligens oppstår når ansatte kan ønske å forbedre produktiviteten og påvirkningen, eller prøve ut ny teknologi. Nedenfor følger flere fiktive eksempler for å illustrere hvordan KI-verktøy uten godkjenning kan brukes, og hvilke risikoer de kan medføre:

Rolle	Eksempelscenario	Potensiell risiko ved bruk av ikke-godkjente verktøy
Markedsføring	Bruk av et innholdsverktøy med generativ kunstig intelligens til å lage markedsføringstekster eller formgivning basert på selskapets merkevaredata.	Lekkasjer av sensitiv merkevare- eller produktinformasjon, tap av kontroll over hvordan en ekstern KI-tjeneste kan lagre eller bruke selskapets kreative eiendeler.
Finans	Opplasting av selskapets finansielle data til en KI-drevet analysetjeneste eller visualiseringstjeneste for rask innsikt.	Eksponering av konfidensielle finansielle data (budsjetter, prognoser) til en tredjepart, potensielle brudd på etterlevelsesregler (f.eks. GDPR) hvis kunde- eller ansattdata inkluderes uten tilstrekkelige sikkerhetstiltak.
Kundestøtte	Deling av klientdata eller transkripsjoner av nettpratøkter med brukerstøtte i et KI-verktøy for å utarbeide svar eller oppsummere saker.	Brudd på personverns- og datahåndteringsregler – sensitiv kundeinformasjon kan lagres utenfor selskapets systemer, ingen garantier for dataoppbevaring eller korrekt sletting fra KI-leverandøren.
Førstelinje – detaljhandel	Butikksjefer bruker KI-baserte planleggingsapper på mobilen for å optimere ansattes vaktlister.	Data om bedriftens arbeidsstyrke (ansattes navn, timeplaner) lastes opp til en ikke-godkjent app, med risiko for personvernproblemer. Uoverensstemmelser i arbeidsplaner eller brudd på regelverk kan oppstå hvis KI-forslag ikke er i etterlevelse med arbeidsreguleringene.
Førstelinje – helsevesen	Sykepleiere eller leger som bruker en KI-samtalerobot for å utarbeide pasientnotater eller svare på medisinske spørsmål.	Pasienthelseinformasjon kan bli eksponert for en ekstern tjeneste uten sikkerhetstiltak og dermed bryte med etterlevelses- og konfidensialitetskrav. Medisinske råd gitt av kunstig intelligens kan også være uverifisert, noe som kan medføre en sikkerhetsrisiko.

I hvert av tilfellene ovenfor hadde den enkelte ansatte gode intensjoner og ønsket å øke produktiviteten, men bedriften kan utsettes for risikoer som følge av dette.

Bedriftsinformasjon kan ende opp spredt på ulike usanksjonerte plattformer, noe som skaper *datastyringsutfordringer*. Ukontrollerte apper kan innføre skadelig programvare eller sikkerhetsproblem, og utvider angrepsoverflaten utenfor IT-avdelingens ansvarsområde. Det kan også være konsekvenser for etterlevelse. Fra et IT-støtteperspektiv kan problemer som oppstår på grunn av bruk av uautoriserte KI-verktøy, føre til at brukerstøtten ikke kan hjelpe sluttbrukere siden de ikke har innsikt i eller kontroll over verktøyet.

Fem måter å håndtere risiko på ved uautorisert bruk av kunstig intelligens



Med riktig strategi og riktige verktøy kan du forvandle uautorisert bruk av kunstig intelligens fra en potensiell trussel til en mulighet til å fremme en kultur for sikker innovasjon. Styrk medarbeiderne med KI-produktivitetsverktøy *samtidig som* du opprettholder den nødvendige oversikten for å beskytte virksomheten. Dette er et skifte fra å si «nei, aldri» til å si «ja – men med de riktige beskyttelsestiltakene». De følgende fem tipsene skal hjelpe deg med å håndtere og få kontroll over uautorisert bruk av kunstig intelligens i din bedrift:

01 Kartlegg fotavtrykket til den uautoriserte bruken av kunstig intelligens for å vurdere og prioritere risiko

Du kan ikke beskytte det du ikke ser. Få oversikt over apper som brukes i bedriften ved hjelp av aktivitetslogger. Når du vet hvilke apper som brukes, kan du kartlegge de riktige verktøyene for å håndtere sensitive data, samtidig som du merker deg appene som ikke er i samsvar med sikkerhets- og etterlevelsesreglene. Med denne innsikten kan du ta en mer overveid avgjørelse om hvilke apper du vil tillate, overvåke eller begrense for å redusere potensiell risiko.

02 Implementer hurtige tiltak med sikkerhets- og etterlevelsesregler

Håndhev strengere retningslinjer for å redusere potensiell risiko ved uautorisert bruk av kunstig intelligens. Du kan bruke retningslinjer for betinget tilgang for å begrense bruken av høyrisikoapper, for hindring av datatap for sensitiv informasjon for å motvirke overdeling og datalekkasje, og håndheve grunnleggende flerfaktorautentisering og enhetsetterlevelse for alle brukere. Tiltakene reduserer raskt de mest fremtredende risikoene, selv om du ennå ikke har full oversikt over hvilke KI-apper som benyttes.

03 Lær opp ansatte om den potensielle risikoen ved uautorisert bruk av kunstig intelligens.

Ansatte er ofte ikke klar over risikoene ved bruk av ikke-godkjente KI-verktøy for bedriften. Kommuniser risikoen ved uautorisert bruk av kunstig intelligens ofte med velplasserte advarsler om hindring av datatap, påminnelser om selskapets retningslinjer og kort opplæring for å veilede brukere mot tryggere praksis uten hardhendt håndheving.

04 Tilby godkjente KI-verktøy for å redusere risikoen ytterligere

Der det er mulig, tilbyr du ansatte godkjente KI-verktøy som alternativer til ikke-godkjente verktøy. En effektiv måte å redusere uautorisert bruk av kunstig intelligens på er å dekke de vanligste brukstilfellene i bedriften med en godkjent løsning. Dette gjør det mulig for IT-avdelingen å opprettholde oversikt og kontroll, samtidig som det gir brukerstøtte ved eventuelle problemer som oppstår.

05 Etabler løpende styring

Integrer kontroller i IT-styringsprosessene – gjennomgå aktivitetslogger og rapporter regelmessig, oppdater retningslinjer etter hvert som nye KI-tjenester dukker opp, og hold ledelsen informert om fremdriften (f.eks. forhindrede databruk eller reduksjon i bruken av ikke-godkjente apper). Dette hjelper deg med å håndtere potensiell risiko nå og i fremtiden, i takt med at forholdene endrer seg.

Ved å gjennomføre tiltakene ovenfor kan du fremme både innovasjon og sikkerhet.

Ansatte kan bruke godkjente KI-løsninger på jobb, og IT-avdelingen opprettholder kontroll og etterlevelse med disse løsningene.

Oppdag og administrer risiko ved uautorisert bruk av kunstig intelligens med Microsoft 365 E3

Microsoft 365 E3 gir bedrifter muligheten til å oppdage uautorisert IT, vurdere potensiell risiko og implementere sikkerhets- og etterlevelsesregler *uten* å hemme innovasjon. Denne pakken med integrerte produktivitets-, sikkerhets- og administrasjonsfunksjoner gjør det mulig for deg å håndtere utfordringer med uautorisert kunstig intelligens direkte.

Microsoft 365 E3-løsning	Hvordan det hjelper deg med å håndtere potensiell risiko knyttet til uautorisert bruk av kunstig intelligens
Cloud App Discovery	**Oppdag og iverksett tiltak mot ikke-godkjente apper.** Med Cloud App Discovery kan du laste opp aktivitetslogger og lage øyeblikksrapporter for å få innsyn i over 31 000 skyapper – blant annet over 400 apper med generativ kunstig intelligens. Den viser deg hva som brukes i bedriften, av hvem og hvor ofte. Denne informasjonen gjør det mulig for deg å ta en overveid avgjørelse om hvilke apper du skal tillate eller begrense bruken av.
Microsoft Purview hindring av datatap	**Forhindre lekkasje av sensitive data.** Microsoft Purview kan hindre datatap ved at du definerer og iverksetter retningslinjer som oppdager sensitiv informasjon og blokkerer eller begrenser deling i Microsoft 365-tjenester for e-poster og filer. Du kan for eksempel angi en regel for å overvåke, revidere eller hindre brukere i å dele sensitiv informasjon via e-post eller fildeling, og varsle brukeren.
Microsoft Entra ID P1	**Administrer tilgangen til skyapper.** Med Microsoft Entra ID P1 kan du iverksette regler for betinget tilgang for å kontrollere hvem som har tilgang til hvilke apper og under hvilke betingelser. For eksempel kan du velge å kreve flerfaktorautentisering eller til og med begrense påloggінger med bedriftslegitimasjon på apper du har vurdert som høyere risiko. Microsoft Entra ID P1 gir tilgang til skyressurser for de riktige personene, på godkjente enheter, under godkjente forhold – samtidig som tilgangen til ikke-godkjente apper begrenses.
Microsoft Intune P1	**Håndhev retningslinjer for bruk av enheter og apper.** Microsoft Intune P1 gir deg muligheten til å tillate at administrerte, godkjente enheter brukes til arbeid, og gir deg verktøy for å administrere disse enhetene. For eksempel kan du forby installasjon av ikke-godkjent programvare på bedriftens datamaskiner, eller distribuere konfigurasjoner som begrenser tilgang til bestemte nettsteder eller tjenester.
Microsoft Defender for endepunkt P1	**Begrens trafikken til ikke-godkjente nettadresser.** Microsoft Defender for endepunkt P1 hjelper deg med å redusere risikoen fra nettsteder som du anser er risikable. Det skjer ved å blokkere trafikk til en ikke-godkjent nettadresse fra administrerte enheter. For eksempel vil ansatte som prøver å besøke et kjent risikabelt KI-nettsted på en av bedriftens datamaskiner, bli hindret i å få tilgang til nettstedet.

Ta neste steg i implementeringen av kunstig intelligens →

Alt starter med bevissthet, de riktige verktøyene og en proaktiv plan. Microsoft 365 E3 gir bedriften verktøyene som trengs for å etablere et robust sikkerhetsfundament og et styringsrammeverk for KI-løsninger. Du får oversikt over ikke-godkjente verktøy, kan iverksette retningslinjer for å beskytte sensitive data og opprettholde kontroll over både brukertilgang og enhetssikkerhet. Gjør deg klar til å gå fra en reaktiv holdning (å finne og blokkere uautorisert kunstig intelligens etter at det har dukket opp) til en mer proaktiv tilnærming der du styrer KI-bruken inn i sikre, administrerte kanaler. Ta sikkerhetsvurderingen for kunstig intelligens og lær hvordan du kan forbedre sikkerheten for kunstig intelligens i bedriften. Les mer om mulighetene i Microsoft 365 for Enterprise.