Microsoft 365

Frigjør potensialet i kunstig intelligens med et sikkert fundament

Innholdsfortegnelse

INNLEDNING

KI-muligheten og sikkerhetsimperativet

Det er et økende produktivitetskapasitetsgap blant dagens arbeidsstyrke. I den nylige arbeidstrendindeksrapporten oppgir **over 80 %** av kunnskapsarbeidere som er intervjuet i 31 land – inkludert både ansatte og ledere – at de mangler tid eller energi til å utføre arbeidet sitt[1]. Samtidig sa **mer enn 50 %** av de spurte bedriftslederne at produktiviteten må øke for å nå målene[1]. Dette gir en mulighet til å vurdere måtene vi jobber på og mulige løsninger for å bidra til å bygge bro over dette gapet. Kunstig intelligens, inkludert agenter, har stort potensial som løsning. **Mer enn 80 %** av de spurte lederne oppga at de er sikre på at bedriftene deres vil begynne å bruke KI-agenter for å øke kapasiteten i arbeidsstyrken i løpet av de neste 12–18 månedene[1].

Dette jaget mot kunstig intelligens kommer med et forbehold: Innovasjon bør balanseres med robust sikkerhet og databeskyttelse for å redusere potensielle risikoer. I en nylig iSMG-rapport oppga **mer enn 70 %** av de spurte bedriftslederne at personvern og datasikkerhet er den største utfordringen ved å integrere generativ kunstig intelligens med eksisterende IT-infrastruktur[2]. Ledere står overfor to motstridende krav: få fart på innføringen av kunstig intelligens for å øke produktiviteten og beskytte data i denne nye tidsalderen.

Dette dokumentet vil gi innsikt i eksempler på KI-scenarioer som kan utgjøre potensielle risikoer, tips for å redusere disse risikoene med Microsoft 365 E3, og en sjekkliste som hjelper bedrifter med å komme i gang eller fortsette forberedelsene til innføring av kunstig intelligens i stor skala. Gjør deg klar til å ta i bruk kunstig intelligens med trygghet: Slik at bedriften din kan innovere med kunstig intelligens, uten at det går på bekostning av bedriftens sikkerhets- eller etterlevelsesstandarder.

Gode intensjoner med potensiell risiko: Mulige KI-scenarioer

De største risikoene ved bruk og innføring av kunstig intelligens oppstår ofte når velmenende ansatte prøver å gjøre jobben sin og oppnå større effekt. I jakten på økt produktivitet kan medarbeidere utilsiktet dele sensitiv informasjon med KI-verktøy eller bruke apper som ennå ikke er godkjent av IT-avdelingen. Dette kan skape risikoer og utsette bedriften for nye trusler.

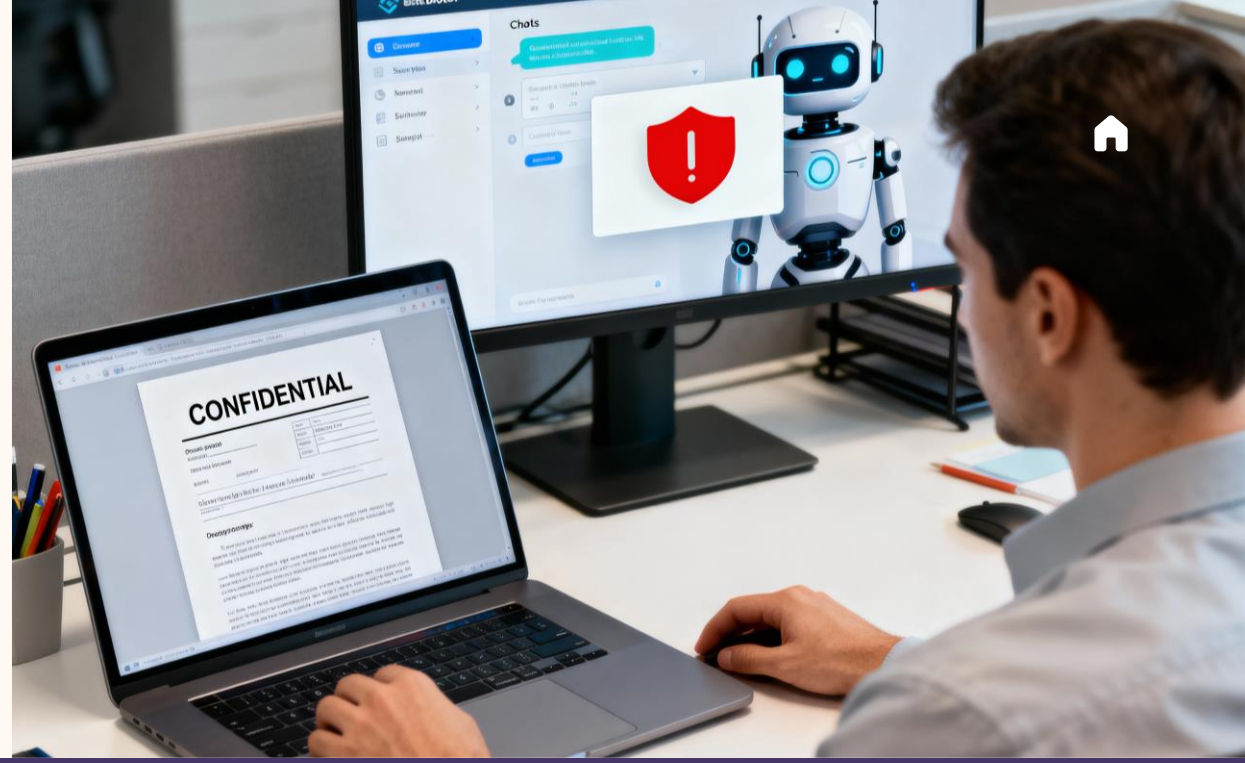
La oss se på to eksempler for å illustrere dette poenget – ett med en kontorbasert informasjonsmedarbeider og ett med en frontlinjearbeider.

I disse fiktive eksemplene får du se 1) hvordan velmenende bruk av kunstig intelligens kan føre til sikkerhetsbrudd hvis den ikke styres riktig, og 2) hvordan disse potensielle risikoene kan reduseres med et robust sikkerhetsfundament.

Eksempelscenario 1[4]

En produktmarkedsføringssjef bruker et KI-verktøy til å utarbeide en pressemelding

En produktmarkedsføringssjef i en produksjonsbedrift har en stram tidsfrist for å utarbeide en pressemelding om et nytt produkt som lanseres i løpet av de kommende månedene. For å generere ideer og effektivisere skriveprosessen kopierer og limer den ansatte utdrag fra en konfidensiell produktplan og en intern økonomisk prognose inn i en kostnadsfri nettbasert KI-skriveassistent. KI-verktøyet genererer raskt noen polerte avsnitt, som den ansatte deretter bruker i utkastet til pressemeldingen. Dette verktøyet har imidlertid ikke blitt kontrollert eller godkjent av bedriften deres ennå.



Potensiell risiko:

Ved å bruke denne eksterne KI-tjenesten har den ansatte lastet opp sensitive selskapsdata (produktplaner og økonomisk informasjon) til et tredjepartssystem som IT-avdelingen ikke har innsikt i og ikke kan administrere eller kontrollere. Når dataene er delt med KI-verktøyet, mister selskapet kontrollen over dem, ettersom de er utenfor autoriserte grenser. Bedriften har ikke lenger kontroll over hvor lenge dataene lagres, hvem som har tilgang til dem, eller hvordan de brukes av tredjeparten. Det som startet som en rask produktivitetsgevinst, har nå utviklet seg til en datalekkasjehendelse. Dette scenarioet illustrerer potensiell intern risiko når en ansatt med gode hensikter deler sensitiv informasjon med et uautorisert KI-verktøy, noe som skaper sårbarhet for virksomheten.

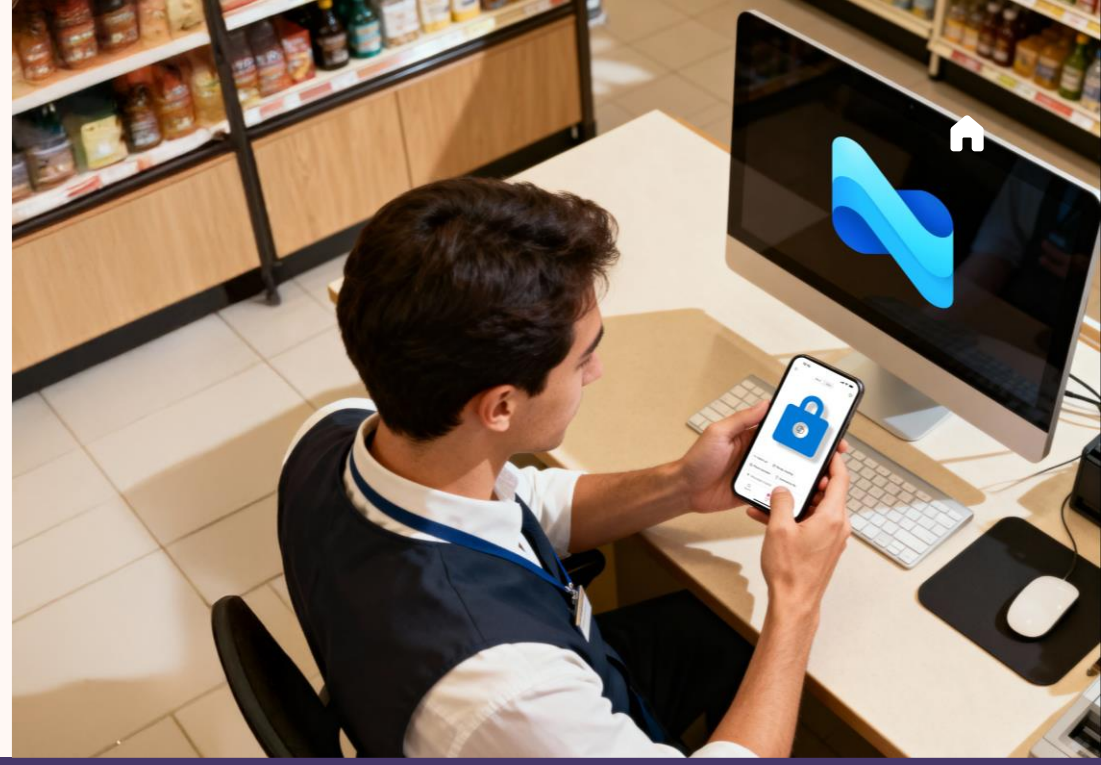
Risikoreduksjon med Microsoft 365 E3:

Microsoft 365 E3 inkluderer flere funksjoner og egenskaper som kan bidra til å forhindre dette utfallet. **Microsoft Purview informasjonsbeskyttelse Plan 1** kan du bruke følsomhetsetiketter og kryptering på dokumenter som produktveikart og økonomiske prosjektdokumenter. Hadde disse dokumentene vært klassifisert og kryptert med følsomhetsetiketter som *Konfidensielt* med kryptering, kunne tilgangen til dokumentene vært begrenset til kun autoriserte brukere. I tillegg kan **Cloud App Discovery** hjelpe med å identifisere generative KI-skyapper som brukes (fra de mange appene i skyappkatalogen), av hvilken bruker og hvor ofte. IT-avdelingen kunne ha avdekket at ansatte brukte dette bestemte KI-verktøyet og tatt grep for å begrense bruken med **Microsoft Defender for endepunkt P1** eller tilbudt et godkjent alternativ. Microsoft 365 E3 tilbyr verktøyene og funksjonene som hjelper organisasjoner med å forbedre synligheten og redusere risiko.

Eksempelscenario 2[4]

En butikksjef bruker kunstig intelligens for å lage utkast til vaktlister og ansattevalueringer

En butikksjef i en stor detaljhandelskjede er overveldet av administrative oppgaver og oppdager en kostnadsfri KI-produktivitetsapp som lover å hjelpe med planlegging og dokumentasjon. For å spare tid laster butikksjefen opp et regneark som inneholder ansattes navn, telefonnumre, timelønn, tilgjengelighetspreferanser og siste evalueringer i KI-verktøyet. Butikksjefen ber KI-appen om å lage en optimalisert vaktliste og hjelpe til med å utarbeide sammendrag av evalueringer for kommende en-til-en-møter.



Potensiell risiko:

Ved å laste opp disse ansattdataene til en ikke-godkjent KI-app, har lederen eksponert sensitive personopplysninger om sine ansatte for et tredjepartssystem utenfor selskapets kontroll og tilsyn. Dette kan medføre potensielle personvernbrudd og etterlevelsesproblemer med arbeidslovgivningen. Selskapets HR- og IT-avdelinger har ingen oversikt over hvor ansattdataene nå befinner seg, hvor lenge de lagres, eller hvem som har tilgang til dem. Det som startet som et forsøk på å bli mer effektiv, har skapt alvorlige juridiske og personvernmessige problemer og problemer med tilliten blant de ansatte.

Risikoreduksjon med Microsoft 365 E3:

Microsoft 365 E3s enhets- og appadministrasjonsfunksjoner kan bidra til å redusere risikoer i forretningskritiske situasjoner som dette. Med **Microsoft Intune P1** kan forhandlerens IT-avdeling håndheve retningslinjer for appbeskyttelse for å hjelpe til med å anvende regler på apper som får tilgang til arbeidsdata, for eksempel ved å begrense kopiering/liming og dataoverføring til uadministrerte apper. Hvis forhandleren oppretter retningslinjer for betinget tilgang via **Microsoft Entra ID P1**, kan de bidra til å blokkere påloggingsforsøk til bedriftskontoer fra uadministrerte apper eller enheter. I dette scenarioet, hvis lederens telefon ikke er kompatibel eller appen er uadministrert, kan disse retningslinjene bidra til å forhindre tilgang til og opplasting av begrensede bedriftsfiler til en skygge-KI-app.

VIKTIG INNSIKT: I begge scenarioene var intensjonen fra de ansatte positiv – å øke arbeidseffektiviteten ved hjelp av kunstig intelligens. Utfallet kan imidlertid være negativt hvis det ikke finnes tilstrekkelige sikkerhetstiltak og retningslinjer. Disse eksemplene understreker hvorfor det å ta i bruk kunstig intelligens uten et sikkerhetsnett kan medføre nye og ytterligere risikoer for bedrifter. Målet er ikke å motvirke bruk av kunstig intelligens, men å ta det i bruk på en ansvarlig måte. Neste del ser nærmere på de grunnleggende funksjonene man bør vurdere når man evaluerer løsninger som kan øke produktiviteten, samt Microsoft 365 E3-funksjonene som hjelper bedrifter med å etablere kontroller som sørger for at sensitive data holdes i godkjente, sikre kanaler.

Bygg et sikkert, KI-klart fundament med Microsoft 365 E3

Er bedriftens din klar for å skalere kunstig intelligens? Se gjennom sjekklisten nedenfor og lær hvordan Microsoft 365 E3 kan hjelpe.

Etter hvert som kunstig intelligens tas i bruk i stadig større grad, blir det stadig viktigere å evaluere bedriftens sikkerhetsstatus og identifisere potensielle hull før kunstig intelligens skaleres. Microsoft 365 E3 er utformet som et KI-klart produktivitets- og sikkerhetsfundament – og kombinerer et bredt spekter av identitets-, sikkerhets-, etterlevelses- og administrasjonsverktøy som sammen gjør det mulig for deg å skalere innføringen av kunstig intelligens med trygghet.

Bruk følgende sjekkliste som et utgangspunkt for å forstå bedriftens nåværende situasjon. Hvis noen punkter ikke er fullstendig implementert ennå, kan bedriften din være utsatt for unødvendig risiko.

Håndhev sterke retningslinjer for identitets- og tilgangsstyring, som flerfaktorautentisering (MFA) og betinget tilgang.

Microsoft 365 E3 inkluderer **Microsoft Entra ID P1**, som muliggjør håndheving av robust identitets- og tilgangsstyring i både skybaserte og lokale miljøer. Løsninger som flerfaktorautentisering og retningslinjer for betinget tilgang verifiserer hver pålogging og begrenser eller tillater tilgang basert på kriterier som brukerrolle, enhetstilstand og plassering, noe som bidrar til å redusere uautorisert tilgang og overdeling av data. For eksempel kan du begrense tilgangen til KI-apper til bestemte ansattgrupper og kreve flerfaktorautentisering for pålogging, noe som reduserer risikoen for kontokompromittering. Retningslinjer for betinget tilgang kan beskytte sensitive data ytterligere ved å forhindre at ansatte får tilgang til ikke-godkjente apper med bedriftslegitimasjon, og delte enheter kan håndheve avloggingsregler for å beskytte mot uautorisert bruk av økter.

Muliggjør sikkert samarbeid på tvers av administrerte endepunkter og enheter.

Microsoft 365 E3 leverer intelligent endepunktsikkerhet gjennom løsninger som **Intune P1, Defender for Endpoint P1 og Windows E3**. Disse verktøyene bidrar til å administrere og øke sikkerheten for PC-er, mobile enheter og apper. Bedrifter kan implementere nettfiltrering for å sperre utrygge nettsteder (inkludert ikke-godkjente KI-verktøy) og sørge for at enheter holdes oppdatert med sikkerhetsoppdateringer via **Windows autooppdatering og Autopilot**. Disse kontrollene bidrar til å holde enhetene i god stand, administrert og oppdatert med sikkerhetsoppdateringer, noe som reduserer angrepsflaten. Enhetlig endepunkt- og enhetsbehandling lar bedrifter sikre arbeidsenheter og opprettholde etterlevelse med apper, uavhengig av om ansatte bruker private eller bedriftseide enheter.

Beskytt data ved å bruke funksjoner som sensitivitetsmerking og retningslinjer for hindring av datatap.

Microsoft 365 E3 tilbyr kjernefunksjoner i **Purview** – sensitivitetsmerking, kryptering og hindring av datatap (DLP) – for å beskytte sensitiv informasjon i dokumenter og e-poster. Når etikettretningslinjer er publisert, kan ansatte klassifisere filer som inneholder økonomiske data, personopplysninger eller immaterielle rettigheter (for eksempel med sensitivitetsmerkingen «Konfidensiell»), og bruke kryptering og tilgangskontroll. Retningslinjer for hindring av datatap kan oppdage og begrense uautorisert deling på **Exchange Online og SharePoint Online/OneDrive for Business**. Selv når du bruker **Microsoft 365 Copilot**, gjelder disse beskyttelsene fortsatt: Copilot respekterer den høyeste sensitivitetsmerkingen og hindrer brukere uten tillatelse i å få tilgang til eller behandle beskyttet innhold.

Få innsikt i ikke-godkjente KI-verktøy som brukes, og ta veloverveide beslutninger.

Microsoft 365 E3 inkluderer **Cloud App Discovery**, som hjelper deg å forstå hvilke KI-apper som brukes (fra de som er inkludert i skyappkatalogen), av hvem, og de tilhørende risikopoengene, slik at du kan avgjøre hvilke tiltak du skal iverksette basert på denne informasjonen. Hvis det anses som for risikabelt, kan IT-avdelingen bruke **Defender for Endpoint P1** til å begrense enkeltpersoners tilgang til å besøke den nettadressen på administrerte Windows 11-enheter. For eksempel, hvis du oppdager at 100 brukere benytter et KI-bildegeneratorverktøy som ikke har blitt gjennomgått eller godkjent av IT-avdelingen, kan IT-avdelingen undersøke det basert på bedriftens sikkerhets- og etterlevelsesstandarder. Hvis det vurderes som risikabelt, kan IT-avdelingen foreslå et godkjent alternativ. Disse funksjonene gir deg mulighet til å redusere risikoer knyttet til skygge-KI og ta veloverveide avgjørelser om KI-bruk som er riktig for din bedrift.

Tilby godkjente KI-apper som Microsoft 365 Copilot.

Det å tilby godkjente KI-apper gir betydelig verdi ved å gi ansatte tilgang til kraftige, godkjente verktøy som oppfyller bedriftens sikkerhets- og etterlevelsesstandarder. For eksempel, i stedet for at ansatte bruker uautoriserte KI-bildegeneratorer eller prateroboter, kan IT-avdelingen tilby godkjente alternativer – som **Microsoft 365 Copilot** – som overvåkes, støttes og integreres i selskapets gjeldende retningslinjer. **Microsoft 365 Copilot** leverer en sikker KI-løsning i bedriftsklassen, dypt integrert med Microsoft 365-produktivitetspakken. **Copilot** gjør det mulig for ansatte å jobbe smartere, automatisere rutineoppgaver og generere innsikt – alt samtidig som gjeldende retningslinjer identitets- og databeskyttelse respekteres. Denne tilnærmingen reduserer skygge-IT, bidrar til å begrense datalekkasje og gir bedrifter innsikt i og kontroll over hvordan kunstig intelligens brukes.

Disse funksjonene opererer ikke isolert – de forsterker hverandre som et integrert, flerlags forsvar. Retningslinjer for identitets-, enhets- og databeskyttelse fungerer sammen for å hjelpe deg med å redusere trusler. Når sikkerhetsavdelinger vet at slike kontroller er på plass, kan sikkerhet bli en tilrettelegger for innovasjon snarere enn en hindring.

Microsoft 365 E3 gir deg muligheten til å etablere de riktige sikkerhetstiltakene, slik at bedriften kan innovere med kunstig intelligens uten at det går på bekostning av sikkerheten.

Frigjør potensialet i kunstig intelligens med et sikkert fundament

Fortsett implementeringen av kunstig intelligens

Alle bedrifter er på en reise for å finne ut hvordan kunstig intelligens best kan tjene deres mål. Løftet er forlokkende – men innføring av kunstig intelligens må gå hånd i hånd med robust beskyttelse. Med Microsoft 365 E3 trenger du ikke å velge det ene eller det andre. Du får en omfattende løsning som styrker sikkerhets- og etterlevelsesnivået ditt, slik at du trygt kan ta i bruk kunstig intelligens.

Vurder sikkerheten til den kunstige intelligensen.

Microsoft tilbyr en **Sikkerhetsvurdering for kunstig intelligens**[3]. Denne nettvurderingen (på security-for-ai-assessment.microsoft.com) gir anbefalinger for å styrke KI-sikkerheten basert på informasjonen du oppgir. Den hjelper deg med å evaluere din nåværende KI-sikkerhet innenfor fire hovedpunkter: **Forbered**, **Oppdag**, **Beskytt** og **Styr**, samt praktiske anbefalinger.

Lær mer og engasjer deg med Microsoft.

Dykk dypere inn i mulighetene med Microsoft 365 E3 og hvordan de kan hjelpe deg med å ta i bruk kunstig intelligens med trygghet. www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot:overviewtab. Du kan også kontakte Microsoft-kundekontakten din eller en Microsoft-partner.

1. Arbeidstrendindeks: Årsrapport, 2025: Året da det banebrytende firmaet ble født Microsoft, Inc., april 2025. Microsoft analyserte undersøkelsesdata fra 31 000 heltidsansatte eller selvstendig næringsdrivende kunnskapsarbeidere fra 31 land mellom 6. februar 2025 og 24. mars 2025, LinkedIn-arbeidsmarkedstrender og billioner av Microsoft 365-produktivitetssignaler.
2. Second Annual Generative AI Study: Business Rewards vs. Security Risks, iSMG, Inc., februar 2025 – basert på en undersøkelse blant over 360 forretnings- og nettsikkerhetsmedarbeidere, gjennomført i 3. kvartal 2024.
3. Sikkerhetsvurdering for kunstig intelligens: security-for-ai-assessment.microsoft.com/ Nøyaktigheten til resultatene avhenger av nøyaktigheten av inndataene dine. Rapporten er utelukkende til informasjonsformål og gir ingen garanti for ytelse eller resultater. Den skal ikke tolkes som en forpliktelse fra Microsoft. Faktiske resultater kan variere basert på faktorer som sted, kjøps- metode og bruk Microsoft fraskriver seg alle uttrykte eller underforståtte garantier angående innholdet i denne rapporten eller på nettstedet.
4. De presenterte scenarioene er fiktive og kun til illustrasjon.