Microsoft 365

Udnyt potentialet i AI med sikre fundamenter

Indholdsfortegnelse

INTRODUKTION

AI-muligheden og den nødvendige sikkerhed

Der er en stigende mangel på produktivitetskapacitet blandt nutidens arbejdsstyrke. 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 mangler tid eller energi til at gøre deres arbejde[1]. Samtidig sagde **over 50 %** af de adspurgte virksomhedsledere, at produktiviteten er nødt til at stige, for at de kan nå deres mål[1]. Det giver en mulighed for at evaluere vores arbejdsmetoder og potentielle løsninger, der kan hjælpe med at eliminere dette problem. AI, herunder agenter, har et stort potentiale som løsning. **Over 80 %** af de adspurgte ledere sagde, at de er overbeviste om, at deres organisationer vil tage AI-agenter i brug for at øge arbejdsstyrkens kapacitet inden for de næste 12–18 måneder[1].

Dette AI-kapløb kræver dog, at man tager sine forholdsregler: innovationen bør afvejes med robust sikkerhed og databeskyttelse for at afbøde potentielle risici. 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]. Ledere står over for et dobbeltsidet krav: de skal sætte fart på AI-implementeringen for at øge produktiviteten og samtidig beskytte data i denne nye tidsalder.

Denne e-bog giver et indblik i eksempler på AI-scenarier, der kan udgøre potentielle risici, gode råd til, hvordan man kan minimere disse risici med Microsoft 365 E3, samt en tjekliste, der hjælper organisationer med at komme i gang eller fortsætte med at forberede sig på AI-implementering i stor skala. Gør dig klar til at tage AI i brug med ro i sindet. Sørg for, at din organisation kan skabe innovation med AI uden at gå på kompromis med organisationens standarder for sikkerhed eller compliance.

Gode intentioner med potentielle risici: Eksempler på AI-scenarier

De største risici ved at bruge og implementere AI opstår ofte, når velmenende medarbejdere prøver at gøre deres arbejde og skabe større værdi. I jagten på øget produktivitet kan teammedlemmer komme til at dele følsomme oplysninger med AI-værktøjer eller bruge applikationer, der endnu ikke er godkendt af IT-afdelingen. Det kan skabe risici og udsætte organisationen for nye trusler.

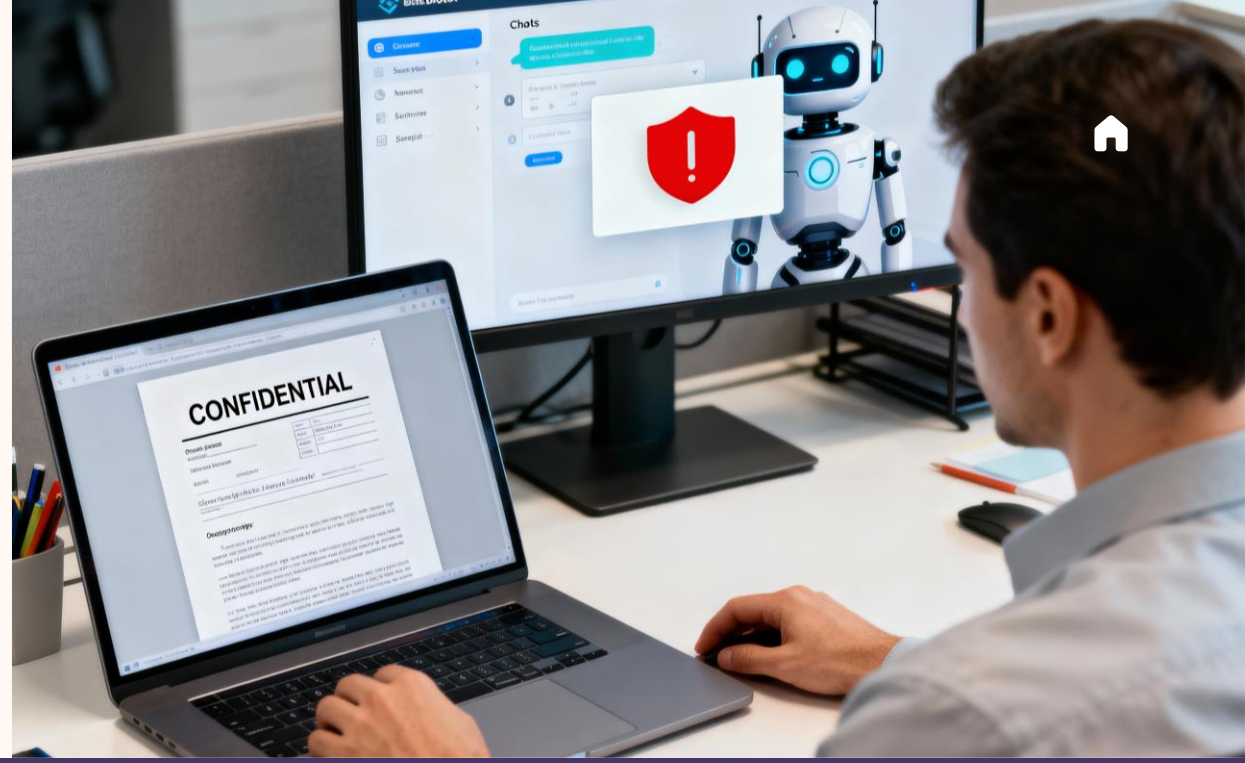
Lad os se på to eksempler på scenarier for at illustrere dette punkt – et scenarie med en kontormedarbejder og et scenarie med en frontlinjemedarbejder.

I disse fiktive eksempler lærer du: 1) hvordan velmenende brug af AI kan føre til brud på sikkerheden, hvis brugen ikke styres korrekt, og 2) hvordan disse potentielle risici kan afbødes med et robust sikkerhedsfundament.

Scenarie 1[4]

En produktmarketingchef bruger et AI-værktøj til at udarbejde en pressemeddelelse

En produktmarketingchef i en produktionsvirksomhed har en stram deadline for at skrive en pressemeddelelse om lanceringen af et nyt produkt i de kommende måneder. For at brainstorme idéer og sætte fart på skriveprocessen kopierer og indsætter denne medarbejder uddrag fra en fortrolig produktkøreplan og en intern økonomisk prognose i en gratis onlinebaseret AI-skriveassistent. AI-værktøjet genererer hurtigt nogle velformulerede afsnit, som medarbejderen derefter bruger i udkastet til pressemeddelelsen. Dette værktøj er dog endnu ikke blevet vurderet eller godkendt af deres organisation.



Potentiel risiko:

Ved at bruge denne eksterne AI-tjeneste har medarbejderen uploadet følsomme virksomhedsdata (produktplaner og økonomiske oplysninger) til et tredjepartssystem, som IT-teamet ikke har indsigt i og ikke kan administrere eller styre. Når dataene deles med AI-værktøjet, mister virksomheden kontrollen over dem, da de befinder sig uden for de godkendte rammer. Organisationen er nu ikke klar over, hvor længe data bliver opbevaret, hvem der har adgang til dem, eller hvordan de bliver brugt af den pågældende tredjepart. Det, der startede som en hurtig produktivitetsgevinst, er blevet til en datalækage. Dette scenarie afspejler potentielle interne risici, når en velmenende medarbejder deler følsomme data med et ikke-godkendt AI-værktøj, hvilket skaber sårbarhed for organisationen.

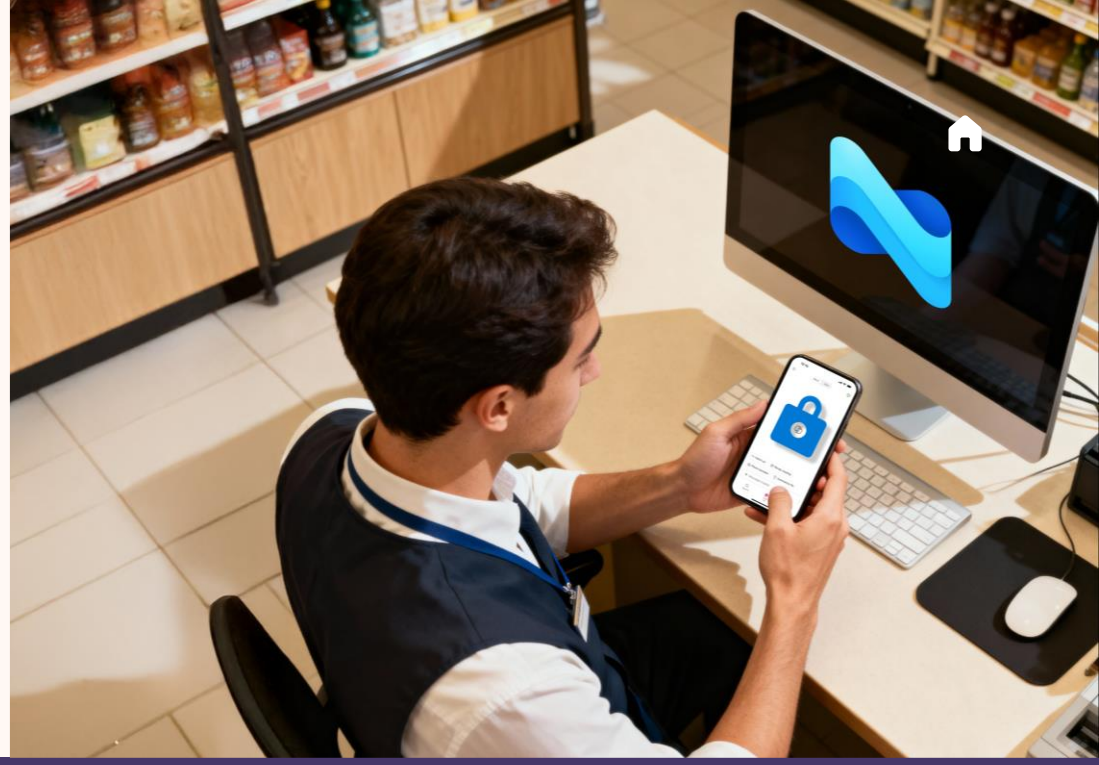
Risikoafbødning med Microsoft 365 E3:

Microsoft 365 E3 indeholder adskillige funktioner og muligheder, der kan hjælpe med at undgå dette udfald. **Microsoft Purview Information Protection Plan 1** giver dig mulighed for at anvende følsomhedsetiketter og kryptering på dokumenter såsom produktkøreplanen og økonomiske projektdokumenter. Hvis disse dokumenter havde været klassificeret og krypteret med følsomhedsetiketter som *Fortroligt* med kryptering, kunne adgangen til dokumenterne have været begrænset til udelukkende autoriserede brugere. Derudover kan **Cloud App Discovery** hjælpe med at identificere, hvilke cloud-apps med generativ AI der anvendes (ud af de mange apps i kataloget med cloud-apps), af hvilke brugere og hvor ofte. IT-afdelingen kunne have konstateret, at der var medarbejdere, som brugte netop dette AI-værktøj, og iværksat tiltag for at begrænse brugen med **Microsoft Defender for Endpoint P1** eller stille et godkendt alternativ til rådighed. Microsoft 365 E3 leverer værktøjerne og kapaciteten til at hjælpe organisationer med at få bedre overblik og afbøde risiciene.

Scenarie 2[4]

En butikschef bruger AI til at udarbejde medarbejderplaner og præstationsnoter

En butikschef i en stor detailkæde er overvældet af administrative opgaver og opdager en AI-produktivitetsapp uden omkostninger, som ser ud til at kunne hjælpe med planlægning og dokumentation. For at spare tid uploader chefen et regneark med medarbejdernavne, telefonnumre, timelønninger, arbejdstidspræferencer og noter om de seneste præstationer til AI-værktøjet. Chefen beder AI-appen om at udarbejde en optimeret arbejdsplan og hjælpe med at udarbejde resuméer af præstationsgennemgange til kommende individuelle samtaler.



Potentiel risiko:

Ved at uploade disse medarbejderdata til en ikke-godkendt AI-app har chefen eksponeret følsomme personoplysninger om sine medarbejdere over for et tredjepartssystem uden for virksomhedens kontrol og tilsyn. Det kan føre til potentielle krænkelser af privatlivets fred og compliance-udfordringer med arbejdslovgivningen. Virksomhedens HR- og IT-afdelinger har ingen indsigt i, hvor medarbejderdataene befinder sig, hvor længe de gemmes, eller hvem der kan få adgang til dem. Det, der startede som et forsøg på at øge effektiviteten, har skabt alvorlige problemer relateret til juridiske forhold, privatliv og medarbejdertillid.

Risikoafbødning med Microsoft 365 E3:

Microsoft 365 E3's funktioner til enheds- og applikationshåndtering kan hjælpe med at afbøde risici i frontlinjesituationer som denne. Med **Microsoft Intune P1** kan forhandlerens IT-team håndhæve beskyttelsespolitikker for applikationer for at hjælpe med at anvende regler på applikationer, der får adgang til arbejdsdata, såsom at begrænse kopiering/indsættelse og dataoverførsel til ikke-administrerede applikationer. Hvis forhandleren opretter politikker for betinget adgang via **Microsoft Entra ID P1**, kan forhandleren muligvis hjælpe med at blokere logonforsøg til virksomhedskonti fra ikke-administrerede apps eller enheder. Hvis chefens telefon ikke overholder kravene, eller hvis appen ikke er administreret, kan disse politikker i denne situation hjælpe med at forhindre dem i at få adgang til og uploade begrænsede virksomhedsfiler til en skygge-AI-applikation.

VIGTIG INDSIGT: I begge scenarier var medarbejdernes mål positivt – at forbedre arbejdseffektiviteten med AI. Udfaldet kan dog være negativt, hvis der ikke er iværksat passende sikkerhedsforanstaltninger og politikker. Disse eksempler understreger, hvorfor implementering af AI uden et sikkerhedsnet kan skabe nye ekstra risici for organisationer. Målet er ikke at forhindre folk i at bruge AI, men at sikre, at den bliver brugt ansvarligt. I det næste afsnit gennemgås de grundlæggende funktioner, man bør overveje, når man evaluerer løsninger, der kan øge produktiviteten, samt Microsoft 365 E3-funktioner, der hjælper organisationer med at opstille sikkerhedsforanstaltninger, som sikrer, at følsomme data forbliver i godkendte og sikre kanaler.

Opbygning af et sikkert, AI-parat fundament med Microsoft 365 E3

Er din organisation klar til at skalere AI? Gennemgå tjeklisten nedenfor, og se, hvordan Microsoft 365 E3 kan hjælpe.

I takt med at implementeringen af AI tager fart, bliver det vigtigere og vigtigere at evaluere din organisations sikkerhedsforsvar og identificere potentielle mangler, før AI bliver skaleret. Microsoft 365 E3 er designet til at være et AI-parat produktivitets- og sikkerhedsfundament – og kombinerer en bred vifte af identitets-, sikkerheds-, compliance- og administrationsværktøjer, der arbejder sammen om at sikre, at du kan skalere din AI-implementering med ro i sindet.

Brug følgende tjekliste som udgangspunkt for at forstå din organisations aktuelle status. Hvis nogle punkter ikke er fuldt implementeret endnu, kan din organisation blive eksponeret for unødvendige risici.

Håndhæv stærke politikker for identitets- og adgangsstyring såsom multifaktorgodkendelse (MFA) og betinget adgang.

Microsoft 365 E3 indeholder **Microsoft Entra ID P1**, som muliggør håndhævelse af robust identitets- og adgangsstyring på tværs af både cloud- og on-premises-miljøer. Løsninger som MFA og politikker for betinget adgang verificerer hvert login og regulerer adgang baseret på kriterier som brugerrolle, enhedstilstand og geografisk placering, hvilket er med til at afhjælpe uautoriseret adgang og overdeling af data. Du kan f.eks. begrænse adgangen til AI-applikationer til bestemte medarbejdergrupper og kræve MFA ved logon, hvilket reducerer risikoen for, at konti bliver kompromitteret. Politikker for betinget adgang kan yderligere beskytte følsomme data ved at forhindre medarbejdere i at få adgang til ikke-sanktionerede applikationer med virksomhedsrelaterede legitimationsoplysninger, og delte enheder kan håndhæve regler ved udlogning for at beskytte mod uautoriseret brug af sessioner.

Aktivér sikkert samarbejde på tværs af administrerede endpoints og enheder.

Microsoft 365 E3 leverer intelligent endpoint-sikkerhed via løsninger som **Intune P1, Defender for Endpoint P1 og Windows E3**. Disse værktøjer hjælper med at administrere og forbedre sikkerheden for pc'er, mobilenheder og apps. Organisationer kan håndhæve webfiltrering for at blokere risikable websteder (herunder ikke-sanktionerede AI-værktøjer) og holde enheder opdateret med sikkerhedsrettelser via **Windows Autopatch og Autopilot**. Disse kontroller hjælper med at holde enheder stabile, administrerede og opdaterede med sikkerhedsrettelser, hvilket gør angrebsfladen mindre. Samlet endpoint- og enhedshåndtering giver organisationer mulighed for at beskytte arbejdsenheder og opretholde overholdelsen af applikationskrav, uanset om medarbejderne bruger deres egne enheder eller enheder, der leveres af virksomheden.

Beskyt data ved hjælp af funktioner som følsomhedsetiketter og politikker til forebyggelse af datatab.

Microsoft 365 E3 leverer kernefunktioner i **Purview** – følsomhedsetiketter, kryptering og forebyggelse af datatab (DLP) – for at beskytte følsomme oplysninger på tværs af dokumenter og mails. Når etiketpolitikker er offentliggjort, kan medarbejdere klassificere filer med økonomiske data, personlige oplysninger eller immaterielle rettigheder (f.eks. med følsomhedsetiketten "Fortroligt"), så der anvendes kryptering og adgangskontrol. DLP-politikker kan registrere og begrænse uautoriseret deling på tværs af **Exchange Online og Microsoft Office SharePoint Online/OneDrive for Business**. Selv når du bruger **Microsoft 365 Copilot**, er disse beskyttelsesmekanismer stadig gældende: Copilot retter sig efter etiketten med den højeste følsomhed og forhindrer brugere uden tilladelse i at få adgang til eller ræsonnere over beskyttet indhold.

Få indsigt i ikke-sanktionerede AI-værktøjer, der anvendes, og skrid til handling på et oplyst grundlag.

Microsoft 365 E3 indeholder **Cloud App Discovery**, som giver dig overblik over, hvilke AI-applikationer der anvendes (ud af dem, der er med i kataloget med cloud-apps), af hvem og de tilhørende risikovurderinger, så du kan træffe beslutning om, hvilke handlinger der skal tages på baggrund af disse oplysninger. Hvis det vurderes for risikabelt, kan IT-afdelingen bruge **Defender for Endpoint P1** til at begrænse enkeltpersoners adgang til den pågældende webadresse på administrerede Windows 11-enheder. Hvis du f.eks. opdager, at 100 brugere anvender et bestemt AI-værktøj til billedgenerering, som ikke er blevet vurderet eller godkendt af IT-afdelingen, kan IT-afdelingen undersøge det baseret på organisationens sikkerheds- og compliance-standarder. Hvis det anses for risikabelt, kan IT-afdelingen foreslå et godkendt alternativ. Disse funktioner giver dig mulighed for at afbøde risici forbundet med skygge-AI og træffe velunderbyggede beslutninger om brugen af AI, som passer til din organisation.

Levér godkendte AI-applikationer såsom Microsoft 365 Copilot.

Ved at tilbyde godkendte AI-applikationer kan man levere betydelig værdi, da medarbejdere får adgang til effektive, godkendte værktøjer, der overholder din organisations sikkerheds- og compliance-standarder. I stedet for at medarbejdere tyr til ikke-godkendte AI-billedgeneratorer eller chatbots, kan IT-afdelingen f.eks. tilbyde godkendte alternativer – såsom **Microsoft 365 Copilot** – som overvåges, understøttes og integreres i virksomhedens eksisterende politikker. **Microsoft 365 Copilot** leverer en sikker AI-løsning i virksomhedsklassen, som er dybt integreret med Microsoft 365-produktivitetspakken. **Copilot** giver medarbejderne mulighed for at arbejde smartere, automatisere rutineopgaver og generere indsigt – samtidig med at identitets- og databeskyttelsespolitikkerne overholdes. Denne tilgang reducerer skygge-IT, hjælper med at begrænse datalækager og giver organisationer overblik og kontrol over, hvordan AI bruges.

Disse funktioner arbejder ikke isoleret fra hinanden – de forstærker hinanden som et integreret forsvar i flere lag. Politikker for identitets-, enheds- og databeskyttelse arbejder sammen om at hjælpe dig med at afbøde trusler. Når sikkerhedsteams ved, at den slags kontrolmekanismer er på plads, kan sikkerheden blive en innovationskraft i stedet for en hæmsko.

Microsoft 365 E3 giver dig mulighed for at etablere de rette sikkerhedsforanstaltninger, så din organisation kan skabe innovation med AI uden at gå på kompromis med sikkerheden.

Fortsæt dit AI-implementeringsforløb

Alle organisationer er på en rejse for at finde ud af, hvordan AI bedst kan understøtte deres mål. Potentialet er lokkende – men AI-implementering skal gå hånd i hånd med robust beskyttelse. Med Microsoft 365 E3 behøver du ikke at vælge nogen af dem fra. Du får en effektiv pakke, der styrker din sikkerheds- og compliance-status, så du kan implementere AI med ro i sindet.

Vurder din parathed til AI-sikkerhed.

Microsoft tilbyder en **AI-sikkerhedsvurdering**[3]. Denne onlinevurdering (på security-for-ai-assessment.microsoft.com) giver anbefalinger til, hvordan du kan styrke din AI-sikkerhed ud fra de oplysninger, du angiver. Den hjælper dig med at evaluere din nuværende AI-sikkerhed på tværs af fire centrale grundpiller: **Forbered**, **Opdag**, **Beskyt** og **Styr**, ligesom den giver brugbare anbefalinger.

Få mere at vide, og tag kontakt til Microsoft.

Dyk dybere ned i Microsoft 365 E3's funktioner, og find ud af, hvordan de kan hjælpe dig med at implementere AI med ro i sindet. www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot:overviewtab. Du kan også kontakte dit Microsoft-kontoteam eller din Microsoft-partner.

1. Indeks over arbejdstendenser for 2025: Årsrapport: Det år, hvor grænsevirksomheden fødes Microsoft, Inc., april 2025. Microsoft analyserede undersøgelsesdata fra 31.000 fuldtidsansatte eller selvstændige erhvervsdrivende vidensarbejdere på tværs af 31 lande mellem den 6. februar 2025 og den 24. marts 2025, LinkedIn-arbejdsmarkedstendenser og billioner af produktivitetssignaler fra Microsoft 365.
2. Second Annual Generative AI Study: Business Rewards vs. Security Risks, iSMG, Inc., februar 2025 – baseret på en undersøgelse blandt over 360 forretnings- og cybersikkerhedsmedarbejdere, udført i 3. kvartal 2024.
3. AI-sikkerhedsvurdering: security-for-ai-assessment.microsoft.com/ Resultaternes nøjagtighed afhænger af nøjagtigheden af dine input. Rapporten er udelukkende til informationsformål og garanterer ikke resultater eller ydeevne. Den bør ikke fortolkes som en forpligtelse fra Microsofts side. De faktiske resultater kan variere afhængigt af faktorer som placering, købsmetode og brug. Microsoft yder ingen udtrykkelige eller underforståede garantier for indholdet af denne rapport eller dette websted.
4. De præsenterede scenarier er fiktive og kun til illustrative formål.