Microsoft 365

Lås upp AI-potentialen med en säker grund

Innehållsförteckning

INLEDNING

AI-möjligheten och den nödvändiga säkerheten

Det finns ett växande produktivitetsgap hos dagens arbetskraft. I den senaste rapporten Index inom arbetstrender uppger **mer än 80 procent** av kunskapsarbetarna som tillfrågades i 31 länder – inklusive både medarbetare och ledare – att de saknade tid eller energi för att utföra sitt arbete[1]. Samtidigt uppger **mer än 50 procent** av de tillfrågade verksamhetsledarna att produktiviteten behöver öka för att målen ska nås[1]. Detta innebär en möjlighet att utvärdera våra arbetssätt och potentiella lösningar så att vi kan överbrygga det här gapet. AI, inklusive AI-agenter, utgör en stor potential som lösning. **Mer än 80 procent** av de tillfrågade ledarna uppgav att de är övertygade om att deras organisationer kommer börja använda AI-agenter för att öka personalens kapacitet under de kommande 12–18 månaderna[1].

Den snabba utvecklingen mot AI kommer med ett viktigt förbehåll: innovation bör balanseras med robust säkerhet och dataskydd för att minska potentiella risker. I en färsk studie från iSMG uppger **mer än 70 procent** av de tillfrågade verksamhetsledarna att förmågan att säkerställa datasekretess och säkerhet är den främsta utmaningen när det gäller att integrera generativ AI med befintlig IT-infrastruktur[2]. Ledare står inför ett tvåfaldigt imperativ: inför AI snabbare för att öka produktiviteten och skydda data i denna nya era.

I den här e-boken erbjuder vi insikter i exempel på AI-scenarier som kan innebära potentiella risker, tips för hur du kan minska dessa risker med Microsoft 365 E3 samt en checklista som hjälper organisationer att komma i gång eller fortsätta förbereda sig för ett AI-införande i stor skala. Gör dig redo för att ta vara på AI på ett tryggt sätt: gör det möjligt för din organisation att innovera med AI utan att ge avkall på organisations säkerhet eller efterlevnadsstandarder.

Goda avsikter med potentiella risker: Exempel på AI-scenarier

De största riskerna med AI-användning och -införande uppstår ofta när medarbetare med goda avsikter försöker göra sitt jobb och skapa större effekt. I strävan efter ökad produktivitet kan teammedlemmar oavsiktligt dela känslig information med AI-verktyg eller använda appar som ännu inte har godkänts av IT-avdelningen. Detta kan skapa risker och utsätta organisationen för nya hot.

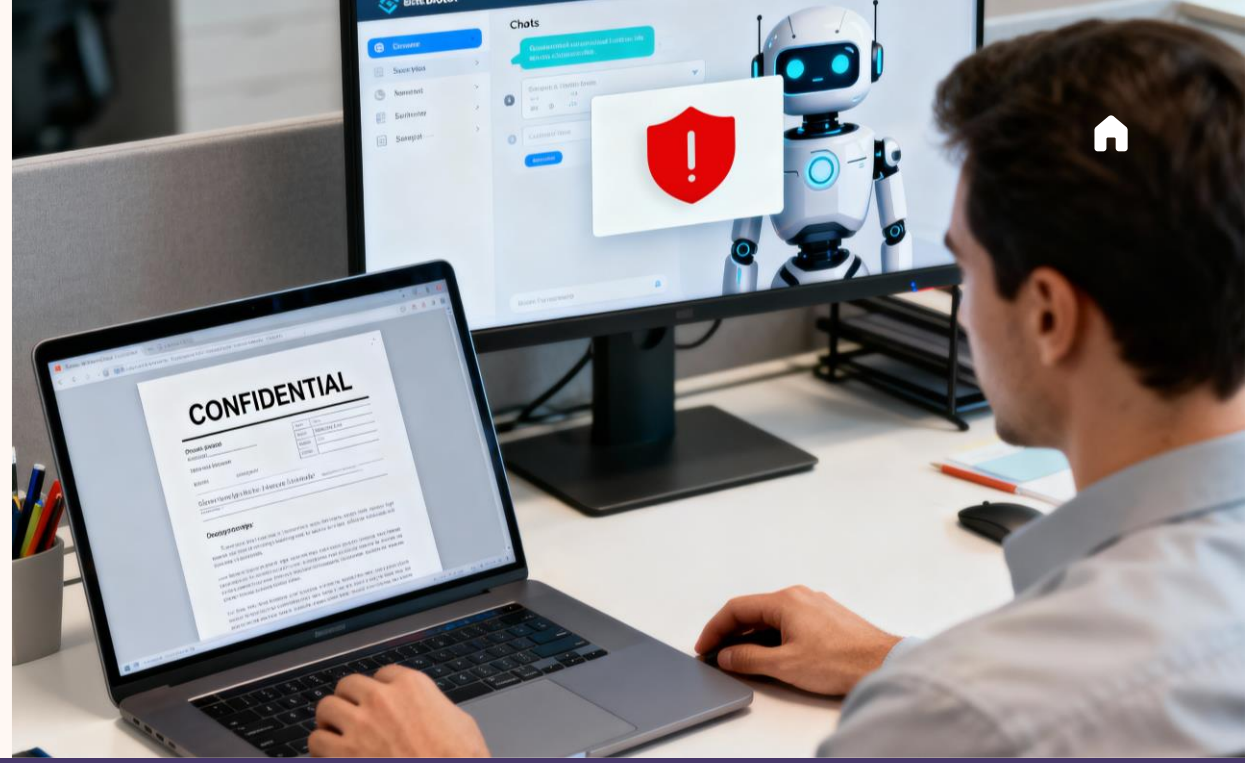
Vi ska ta en titt på två exempelscenarier för att illustrera detta – ett med en kontorsbaserad informationsarbetare och ett med en medarbetare i frontlinjen.

I dessa fiktiva exempel får du lära dig 1) hur en välmenande användning av AI kan leda till säkerhetsbrister om den inte styrs korrekt och 2) hur dessa potentiella risker kan mildras med en robust säkerhetsgrund.

Exempelscenario 1[4]

En produktmarknadschef använder ett AI-verktyg för att utarbeta ett pressmeddelande

En produktmarknadschef på ett tillverkningsföretag måste snabbt utarbeta ett pressmeddelande om en ny produktlansering som ska ske inom de kommande månaderna. För att generera idéer och effektivisera skrivprocessen kopierar och klistrar den här medarbetaren in utdrag från en konfidentiell produktplan och en intern finansiell prognos i en kostnadsfri onlinebaserad AI-driven assistent. AI-verktyget genererar snabbt några välformulerade stycken, som medarbetaren sedan använder i utkastet till pressmeddelandet. Det här verktyg har dock ännu inte granskats eller godkänts av organisationen.



Potentiell risk:

Genom att använda denna externa AI-tjänst har medarbetaren laddat upp känsliga företagsdata (produktplaner och finansiell information) till ett system från tredje part som IT-teamet saknar insyn i och inte kan hantera eller kontrollera. När data delas med AI-verktyget förlorar företaget kontrollen över dem eftersom de befinner sig utanför behörighetsgränserna. Organisationen kan nu inte längre veta hur länge data lagras, vem som har tillgång till dem eller hur dem används av tredje part. Det som började som en snabb produktivitetsvinst har nu blivit ett dataläckage. Detta scenario illustrerar en potentiell intern risk när en välmenande medarbetare delar känslig information med ett oauktoriserat AI-verktyg, vilket skapar en sårbarhet för organisationen.

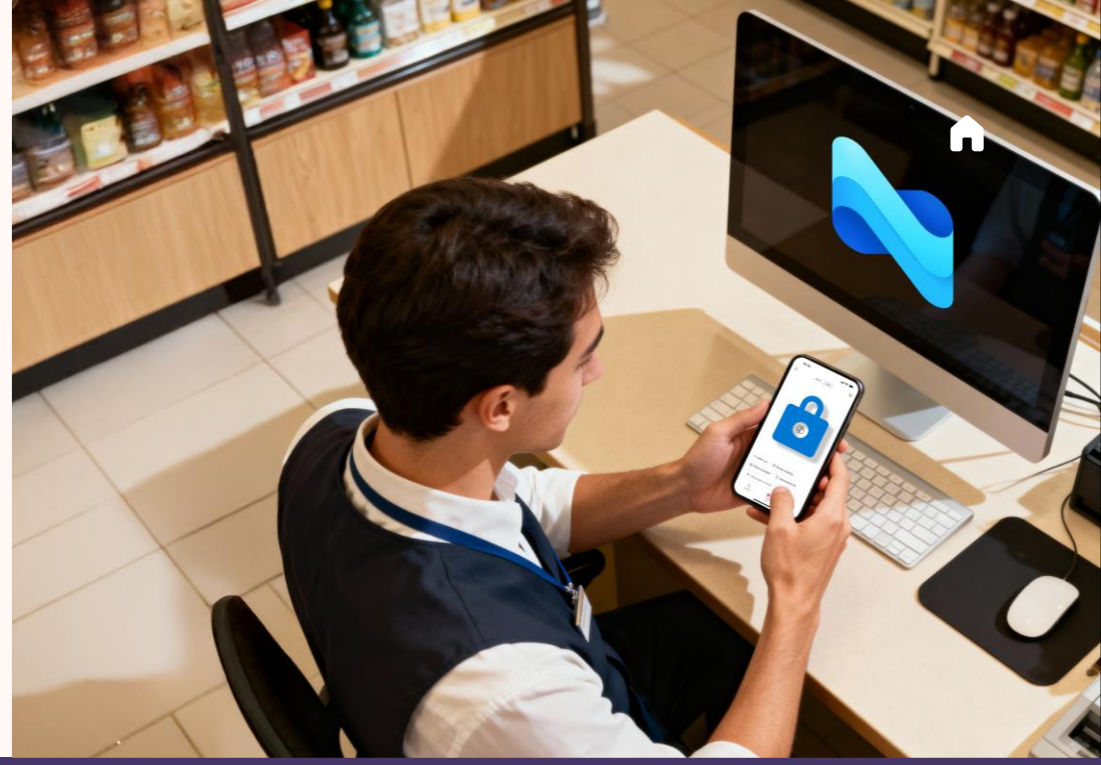
Riskreducering med Microsoft 365 E3:

Microsoft 365 E3 omfattar en rad funktioner och möjligheter som du kan använda för att undvika detta scenario. **Microsoft Purview Information Protection, prenumerationsavtal 1** gör det möjligt att tillämpa känslighetsetiketter och kryptering på dokument som produktöversikter och finansiella projektdokument. Om dessa dokument hade klassificerats och krypterats med känslighetsetiketter, till exempel *Konfidentiellt* med kryptering, kunde dokumentens åtkomst ha begränsats till endast behöriga användare. Dessutom kan **Cloud App Discovery** hjälpa till att identifiera vilka molnappar med generativ AI som används (bland de många apparna i katalogen med molnappar), av vilka användare och hur ofta. IT-avdelningen kunde ha upptäckt att medarbetare använde just detta AI-verktyg och vidtagit åtgärder för att begränsa användningen med hjälp av **Microsoft Defender för Endpoint P1** eller erbjuda ett sanktionerat alternativ. Microsoft 365 E3 omfattar verktyg och funktioner som hjälper organisationer att förbättra synligheten och minska riskerna.

Exempelscenario 2[4]

En butikschef använder AI för att utarbeta arbetsscheman och anteckningar om prestationer

En butikschef i en stor detaljhandelskedja har alldeles för mycket administrativa uppgifter och upptäcker en kostnadsfri AI-produktivitetsapp som lovar att hjälpa till med schemaläggning och dokumentation. För att spara tid laddar chefen upp ett kalkylblad med medarbetarnas namn, telefonnummer, timlöner, önskemål om arbetstider och de senaste anteckningarna om medarbetarnas prestation till AI-verktyget. Chefen ber AI-appen skapa ett optimerat arbetsschema och hjälpa till att utarbeta sammanfattningar av utvärderingssamtal inför kommande enskilda möten.



Potentiell risk:

Genom att ladda upp dessa medarbetardata till en osanktionerad AI-app har chefen exponerat känsliga personuppgifter om sina medarbetare för ett tredjepartssystem utanför företagets kontroll och tillsyn. Detta kan leda till potentiella integritetskränkningar och efterlevnadsproblem med arbetsrättslagar. Företagets HR- och IT-avdelningar har ingen kontroll över var personaluppgifterna nu finns, hur länge den lagras eller vem som kan få tillgång till den. Det som började som ett försök att bli mer effektiv har resulterat i allvarliga juridiska problem samt integritets- och förtroendeproblem mellan arbetsgivare och medarbetare.

Riskreducering med Microsoft 365 E3:

Microsoft 365 E3-funktionerna för enhets- och apphantering kan bidra till färre risker i liknande frontlinjescenarier. Med **Microsoft Intune P1** kan butikskedjans IT-team införa policyer för appskydd för att tillämpa regler på appar som har åtkomst till arbetsdata, såsom att begränsa kopiering/inklistring och dataöverföring till ohanterade appar. Om butikskedjan skapar policyer för villkorsstyrd åtkomst via **Microsoft Entra ID P1** kan detta bidra till att blockera inloggningsförsök till företagskonton från ohanterade appar eller enheter. Om chefens telefon inte uppfyller kraven eller om appen är ohanterad, kan dessa policyer i det här scenariot förhindra att chefen får åtkomst till och laddar upp begränsade företagsfiler till en skugg-AI-app.

Viktig insikt: I båda scenarierna var medarbetarnas syfte positivt – att förbättra arbetseffektiviteten med hjälp av AI. Resultatet kan dock bli negativt om rätt skyddsmekanismer och policyer inte finns på plats. Dessa exempel understryker varför införandet av AI utan säkerhetsnät kan medföra nya och ytterligare risker för organisationer. Målet är inte att motverka AI-användningen, utan att möjliggöra den på ett ansvarsfullt sätt. I nästa avsnitt går vi igenom de grundläggande funktionerna du bör beakta när du utvärderar lösningar som kan förbättra produktiviteten, samt de Microsoft 365 E3-funktioner som hjälper organisationer att införa skyddsåtgärder för att hålla känslig data inom godkända, säkra kanaler.

Skapa en säker, AI-förberedd grund med Microsoft 365 E3

Är din organisation redo att skala upp AI? Gå igenom checklistan nedan och se hur Microsoft 365 E3 kan hjälpa er.

I takt med att AI-användningen ökar blir det allt viktigare att utvärdera organisationens säkerhetsläge och identifiera potentiella brister innan ni skalar upp AI. Microsoft 365 E3 är en AI-förberedd produktivitets- och säkerhetsplattform – som kombinerar ett brett utbud av identitets-, säkerhets-, efterlevnads- och hanteringsverktyg som samverkar för att ge dig möjlighet att skala AI-användningen på ett tryggt sätt.

Använd följande checklista som utgångspunkt för att ta reda på organisationens nuvarande läge. Om några punkter ännu inte är fullt implementerade kan organisationen utsättas för onödig risk.

Inför starka identitets- och åtkomsthanteringspolicyer som multifaktorautentisering (MFA) och villkorsstyrd åtkomst.

Microsoft 365 E3 omfattar **Microsoft Entra ID P1**, vilket gör det möjligt att upprätthålla robust identitets- och åtkomsthantering både i molnet och i lokala miljöer. Lösningar som MFA och policyer för villkorsstyrd åtkomst verifierar varje inloggning och begränsar eller tillåter åtkomsten baserat på villkor som användarroll, enhetens hälsotillstånd och plats, vilket minskar risken för obehörig åtkomst och överdriven datadelning. Du kan till exempel begränsa åtkomsten till AI-appar för specifika medarbetargrupper och kräva MFA vid inloggning, vilket minskar risken för kontointrång. Policyer för villkorsstyrd åtkomst kan ytterligare skydda känsliga data genom att förhindra att medarbetare får åtkomst till icke godkända appar med företagsautentiseringsuppgifter, och delade enheter kan tillämpa utloggningsregler som skyddar mot obehörig sessionsanvändning.

Möjliggör säkert samarbete över hanterade slutpunkter och enheter.

Microsoft 365 E3 möjliggör intelligent slutpunktssäkerhet genom lösningar som **Intune P1, Defender för Endpoint P1 och Windows E3**. Dessa verktyg hjälper till att hantera och öka säkerheten för datorer, mobila enheter och appar. Organisationer kan tillämpa webbfiltrering för att blockera riskabla webbplatser (inklusive icke godkända AI-verktyg) och hålla enheterna uppdaterade med säkerhetskorrigeringar via **Windows Autopatch och Autopilot**. Dessa kontroller bidrar till att enheterna är välfungerande, hanteras korrekt och hålls uppdaterade med säkerhetskorrigeringar, vilket minskar angreppsytan. Enhetlig slutpunkts- och enhetshantering gör det möjligt för organisationer att skydda arbetsdatorer och enheter samt upprätthålla appefterlevnad, oavsett om medarbetarna använder sina egna eller företagets enheter.

Skydda data genom att använda funktioner som känslighetsetiketter och policyer för dataförlustskydd.

Microsoft 365 E3 tillhandahåller grundläggande **Purview**-funktioner – känslighetsetiketter, kryptering och dataförlustskydd (DLP) – för att skydda känslig information i dokument och e-postmeddelanden. När etikettpolicyerna har publicerats kan medarbetarna klassificera filer som innehåller ekonomiska data, personuppgifter eller immateriella rättigheter (till exempel med känslighetsetiketten ”Konfidentiell”) och samtidigt tillämpa kryptering och åtkomstkontroll. DLP-policyer kan identifiera och begränsa obehörig delning över **Exchange Online och Microsoft Office SharePoint Online/OneDrive för företag**. Även vid användning av **Microsoft 365 Copilot** upprätthålls dessa skydd: Copilot använder den högsta känslighetsetiketten och förhindrar att användare utan behörighet får åtkomst till eller analyserar skyddat innehåll.

Få insyn i osanktionerade AI-verktyg som används och vidta välunderbyggda åtgärder.

Microsoft 365 E3 omfattar **Cloud App Discovery**, vilket hjälper dig att förstå vilka AI-appar som används (från dem som ingår i katalogen över molnappar), av vem och med vilka associerade riskpoäng, så att du kan avgöra vilka åtgärder som bör vidtas baserat på denna information. Om det bedöms som för riskabelt kan IT-avdelningen använda **Defender för Endpoint P1** för att begränsa användarnas möjlighet att besöka den URL:en på hanterade Windows 11-enheter. Om du till exempel upptäcker att 100 användare använder ett visst AI-baserat bildgeneratorverktyg som inte har granskats eller godkänts av IT-avdelningen – kan IT-avdelningen undersöka detta baserat på organisationens säkerhets- och efterlevnadsstandarder. Om det bedöms som riskabelt kan IT föreslå ett godkänt alternativ. Dessa funktioner ger dig möjlighet att minska riskerna med skugg-AI och fatta väl underbyggda beslut som rör AI-användningen, som är rätt för din organisation.

Erbjud sanktionerade AI-appar som Microsoft 365 Copilot.

Genom att erbjuda sanktionerade AI-appar kan du uppnå betydande värde genom att medarbetarna får tillgång till kraftfulla, godkända verktyg som uppfyller organisationens säkerhets- och efterlevnadsstandarder. I stället för att medarbetare exempelvis vänder sig till obeprövade AI-baserade bildgeneratorer eller chattrobotar kan IT-avdelningen erbjuda godkända alternativ – såsom **Microsoft 365 Copilot** – som övervakas, stöds och integreras i organisationens befintliga policyer. **Microsoft 365 Copilot** är en säker AI-lösning på företagsnivå, djupt integrerad med Microsoft 365-produktivitetspaketet. **Copilot** gör det möjligt för medarbetare att arbeta effektivare, automatisera rutinuppgifter och skapa insikter – allt medan identitets- och dataskyddspolicyer följs. Denna strategi minskar omfattningen av skugg-IT, hjälper till att begränsa dataläckaget och ger organisationer bättre insyn och kontroll över hur AI används.

Dessa funktioner verkar inte ensamma – de förstärker varandra som ett integrerat försvar i flera lager. Identitets-, enhets- och dataskyddspolicyer samverkar för att hjälpa dig motverka hot. När säkerhetsteam vet att kontroller som dessa finns på plats kan säkerheten ligga till grund för innovation snarare än att utgöra ett hinder.

Med Microsoft 365 E3 kan du upprätta rätt skyddsmekanismer så att din organisation kan driva innovation med AI utan att kompromissa med säkerheten.

Fortsätt din AI-resa

Varje organisation befinner sig på en resa för att ta reda på hur AI bäst kan bidra till att uppnå verksamhetens mål. Löftet är lockande – men AI-införandet måste gå hand i hand med ett robust skydd. Med Microsoft 365 E3 behöver du inte välja det ena eller det andra. Du får ett kraftfullt programpaket som stärker organisationens säkerhet och regelefterlevnad, så att ni tryggt kan använda AI.

Bedöm AI-säkerhetens beredskap.

Microsoft erbjuder en **bedömning av säkerheten för AI**[3]. Denna onlinebedömning (på security-for-ai-assessment.microsoft.com) ger rekommendationer för hur du kan stärka AI-säkerheten baserat på den information du tillhandahåller. På så sätt kan du bedöma den nuvarande AI-säkerheten inom fyra centrala områden: **Förbereda**, **Identifiera**, **Skydda** och **Styra**. Du får dessutom konkreta åtgärdsförslag.

Läs mer och kommunicera med Microsoft.

Fördjupa dig i Microsoft 365 E3-funktionerna och hur de kan hjälpa dig att implementera AI på ett tryggt sätt. www.microsoft.com/sv-se/microsoft-365/enterprise/e3?activetab=pivot:overviewtab. Du kan också kontakta ditt Microsoft-kontoteam eller din Microsoft-partner.

1. Rapporten Index inom arbetstrender, 2025: Året då framkantsföretaget föds Microsoft, Inc., april 2025. Microsoft analyserade enkätdata från 31 000 heltidsanställda (eller egenföretagare) kunskapsarbetare från 31 länder mellan den 6 februari 2025 och den 24 mars 2025, LinkedIn-trender på arbetsmarknaden och biljoner Microsoft 365-produktivitetssignaler.
2. Second Annual Generative AI Study: Business Rewards vs. Security Risks, iSMG, Inc., februari 2025 – baserat på en enkät bland över 360 verksamhets- och cybersäkerhetsexperter, genomförd under tredje kvartalet 2024.
3. Bedömning av säkerhet för AI: security-for-ai-assessment.microsoft.com/ Noggrannheten i resultaten beror på kvaliteten på dina indata. Rapporten presenteras enbart i informationssyfte och ger inga garantier för prestanda eller resultat. Den bör inte tolkas som ett åtagande från Microsoft. Faktiska resultat kan variera beroende på faktorer som plats, köpmetod och användning. Microsoft lämnar inga uttryckliga eller underförstådda garantier avseende innehållet i denna rapport eller webbplats.
4. De scenarier som presenteras är fiktiva och är endast till för illustrativa syften.