Microsoft 365 Copilot

Garantera datasäkerhet under AI-eran

En guide för IT-ledare

E-bok

Den här guiden är avsedd för IT-ledare som behöver hantera införandet av AI och skydda organisationernas data på samma gång. Den förklarar riskerna AI innebär för datasäkerheten och integriteten och förmedlar samtidigt de insikter du behöver för att leda ditt företags AI-utveckling tryggt.

Innehållsförteckning

01

De nya reglerna för AI-understött arbete

Generativ AI bereder nya innovationsvägar och hjälper team att jobba snabbare och smartare än någonsin. För framåtsyftande organisationer är AI inte en i raden av tekniktrender. Det är ett måste för företag, nödvändigt för verksamheten och hur företagen levererar värde och bibehåller konkurrensfördelar.

Men detta snabba införande medför nya och svårare problem som IT-ledare måste hantera proaktivt och få styr på. AI-system kan aktivt söka efter och kombinera information i hela dataekosystemet, vilket ger säkerhetsrisker utöver de traditionella verktygens. Trots den snabba AI-utbyggnaden säger bara **1 %** av alla organisationer att de har integrerat AI helt i sina arbetsflöden med lämpliga säkerhetsrutiner.[1] Genom att införa säkerhets- och styrningsåtgärder redan i början av AI-färden kan ditt team effektivt skydda känsliga data, upprätthålla efterlevnadskrav och skydda organisationens information – samtidigt som innovationen kan blomstra.

AI införs i rasande fart

02

Förstå AI:s effekt på datasäkerheten

Innan vi skärskådar specifika problem är det viktigt att förstå på vilket sätt AI förändrar datasäkerhetslandskapet så radikalt. Till skillnad från traditionell programvara som bara ansluter till data när den instrueras specifikt att göra det, bearbetar generativ AI data aktivt, analyserar data och skapar innehåll med ledning av informationen tekniken tar emot.

Skillnaden är avsevärd av flera anledningar:

- AI-verktyg kan upptäcka kopplingar mellan data som människor kan missa.
- De kan syntetisera information från flera källor automatiskt.
- De kan generera nytt innehåll med inslag från känsliga indata.

De traditionella säkerhetsverktygen konstruerades förmodligen inte med sådant i åtanke. Konventionell programvara vet man var man har när de använder data, men AI kan ta oväntade vägar i informationsekosystemet, vilket skulle kunna exponera känsliga data på oväntade vis.

Denna markanta förändring kräver nya sätt att handskas med säkerhet och datastyrning som specifikt tar hänsyn till hur AI interagerar med organisationens informationsresurser.

03

Problemet med skugg-AI

Vart ni än har kommit med införandet av AI hittar medarbetarna redan egna lösningar och ger upphov till vad som kallas skugg-AI.

Detta obehöriga bruk ger upphov till allvarliga blinda fläckar i säkerheten. När medarbetarna delar företagets data med externa AI-system kringgår de befintliga säkerhetskontroller och skapar sårbarheter som de flesta organisationer inte är redo att ta sig an.

Skugg-AI är inte bara ett säkerhetsproblem: det kan vara ett symptom på produktivitetsbehov i organisationen som inte tillgodoses. När medarbetarna nyttjar osanktionerade verktyg tyder det på att de officiella systemen inte uppfyller deras krav. Hanteringen av skugg-AI kräver både bättre styrning och avancerade produktivitetslösningar.

Varför skugg-AI dyker upp:

- Medarbetarna vill gärna bli mer produktiva genom genom AI:s imponerande försorg
- Den normala arbetsbördan överstiger allt oftare både tids- och energitillgången
- Teamen pressas allt mer att leverera mer med samma resurser
- AI-verktyg för konsumenter medger omedelbara lösningar utan att någon behöver godkänna det
- Officiella IT-upphandlingsprocesser är för långsamma för innovationstakten

Riskerna med skugg-AI:

- Ingen insyn i vilka företagsdata som bearbetas av externa AI-system
- Ingen garanti om att konfidentiell information inte behålls
- Inga konsistenta säkerhetsstandarder på olika AI-plattformar
- Det går inte att granska efterlevnaden
- Ingen integrering med den befintliga säkerhetsinfrastrukturen

Tänk dig det här scenariot:

En finansanalytiker brottas med ett komplicerat kalkylblad och lägger upp det i ett icke godkänt AI-verktyg för att få hjälp. Kalkylbladet innehåller ekonomiska data om kunder, interna mått och prognoser. Även om analytikern får den hjälp hen behöver har organisationens känsliga ekonomiska finansiella data hamnat utanför säkerhetsområdet utan minsta kontroll för övervakningssystemen.

04

Ofrånkomligheten av BYOAI

Utan tydliga instruktioner från företagsledningen inför medarbetarna i allt större utsträckning AI på egen hand. **78 %** av AI-användarna nyttjar en BYOAI-strategi (bring your own AI) under arbetet.[2] Trenden är ännu tydligare på små och medelstora företag, där **80 %** av medarbetarna nyttjar BYOAI-metoder.[2]

Detta osanktionerade tillvägagångssätt har avsevärda nackdelar. Medarbetarna döljer ofta att de använder AI. **52 %** erkänner högst ovilligt att de använder AI för viktiga arbetsuppgifter, och **53 %** oroar sig för att AI-bruket får dem att verka utbytbara.[2] Detta smusslande hindrar inte bara organisationen från att realisera alla fördelar med strategisk AI-implementering, utan skapar också allvarliga säkerhetsproblem i miljöer där företagsledningen nämner cybersäkerhet och dataskydd som sitt **främsta** bekymmer.[2]

Med tanke på den breda användningen och oundvikliga AI-tillväxten är frågan inte om AI ska få användas i organisationen utan hur man erbjuder en säker lösning som uppfyller medarbetarnas behov samtidigt som organisationens data skyddas.

05

Labyrinten av föreskrifter

Ramverk och lagar som rör dataintegritet och säkerhet skapar ytterligare ett lager av komplexitet när AI införs. Även om vissa ramverk är utformade för AI-styrning och kontroll har andra mer bred tillämpning som fortfarande påverkar hur man hanterar information – och straffen för överträdelser är fortfarande allvarliga.

När medarbetarna använder AI-verktyg utan ordentlig tillsyn kan de oavsiktligt ge upphov till efterlevnadsöverträdelser. AI ökar risken eftersom tekniken kan använda, kombinera och göra tillgänglig reglerad information på sätt som traditionella metoder inte kan.

Viktiga förordningar som påverkar AI-bruket:

GDPR

EU:s allmänna dataskyddsförordning ger folk kontroll över sina personuppgifter, och det krävs tydligt samtycke för att bearbeta dem

EU:s AI-lag

EU:s omfattande ramverk som är utformat för att reglera AI-system utifrån risknivå

HIPAA

Denna amerikanska federala lag för hälso- och sjukvård fastställer stränga standarder för hanteringen av skyddad hälsoinformation

NIST:s ramverk för AI-riskhantering

Detta amerikanska underlag som är frivilligt att följa hjälper organisationer att hantera risker vid design, utveckling och driftsättning av AI-system

Efterlevnadsriskerna med AI:

- Kunddata som bearbetas på servrar utanför godkända regioner
- Personuppgifter som används utan korrekt samtycke
- Känsliga data som finns kvar i system utan lämpliga kvarhållningskontroller
- Ingen granskningskedja för hur skyddad information nyttjas och används
- AI-genererat innehåll som bryter mot sektorspecifika efterlevnadskrav

Dessa överträdelser kan leda till allvarliga konsekvenser:

- Stora ekonomiska påföljder (GDPR-böter kan uppgå till **4 %** av era globala intäkter)[4]
- Krav på att avisera berörda parter om dataintrång
- Rättsliga åtgärder från de drabbade
- Skada på företagets rykte och kundernas förtroende

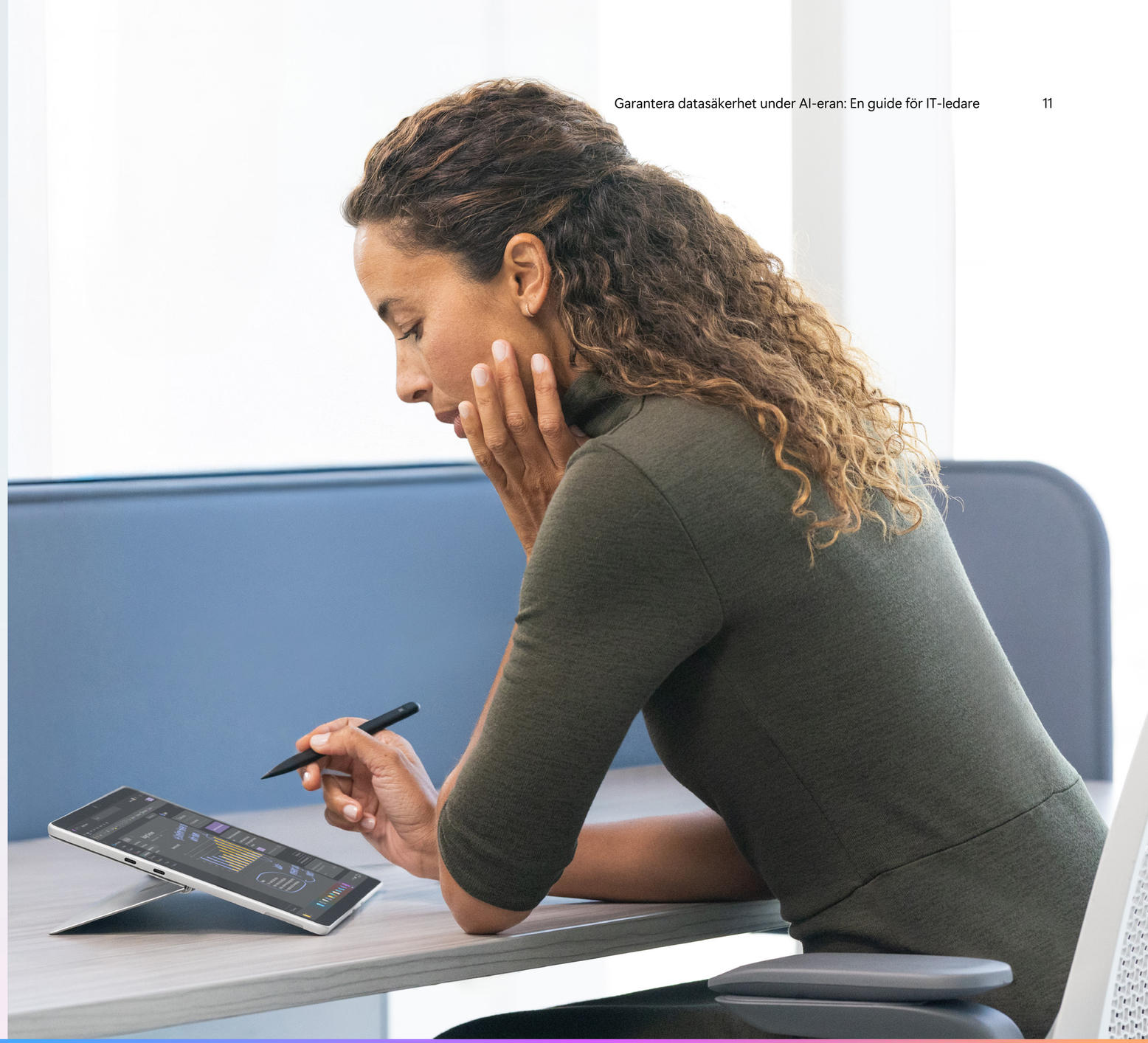
När AI-användningen växer i hela organisationen behöver ni styrning som hjälper människor att arbeta effektivt samtidigt som organisationen följer de regler som påverkar verksamheten och organisationens kunder.

06

Ett ramverk för utvärdering av AI-lösningar med säkerhet i högsätet

Med skugg-AI, BYOAI och förordningar som skapar betydande risker behöver du en strukturerad metod för att utvärdera AI-lösningar som säkerställer att de kan hjälpa organisationen att driva på utvecklingen, samtidigt som du skyddar känsliga data och säkerställer efterlevnad av föränderliga regelverk.

Det följande ramverket innehåller sex enkla frågor för att bedöma om en AI-plattform levererar i bägge fallen.



Fråga 1

Erbjuder det säkerhet i företagsklass från grunden?

Med rätt lösning övergår säkerheten från att bara reagera på problem efter att de har hänt till att proaktivt leta reda på sårbarheter i organisationens data innan de blir större problem.

Leta efter lösningar som

- ger insyn i realtid i hela dataekosystemet
- identifierar potentiella datarisker automatiskt innan de blir incidenter
- skyddar känslig information på alla nivåer.

Fråga 2

Kan det enkelt införa och förbättra befintliga säkerhetskontroller?

Organisationens säkerhetspolicyer bör fungera smidigt med AI. Din AI-lösningsleverantör bör respektera och integrera dina befintliga säkerhetsramverk, inte kräva att du skapar helt nya.

Leta efter lösningar som

- smidigt nyttjar era befintliga säkerhetspolicyer, känslighetsetiketter och informationsskyddsinställningar
- tillämpar detaljerade åtkomstkontroller på individuell nivå så att ingen användare har tillgång till data som hen inte bör ha
- aktivt flaggar försök att komma runt åtkomstkontroller.

Fråga 3

Omfattar det inbyggda styrnings- och integritetskontroller?

Eftersom AI-verktyg fungerar mer proaktivt måste dina säkerhetsåtgärder också vara proaktiva. Genom att införa kraftfull datastyrning skapas tydliga gränser där medarbetarna kan tänka nytt säkert utan att riskera känslig information.

Leta efter lösningar som

- centraliserar AI-styrningen med automatiserad policytillämpning för alla aktiviteter
- inkluderar tidig identifiering av potentiell överdelning av data
- är anpassade till regelverk för att säkerställa regelefterlevande AI-bruk.

Fråga 4

Kan det driftsättas konsistent i hela organisationen?

Dina medarbetare har sina egna arbetssätt, sina egna scheman och kan finnas över hela världen. AI bör gynna alla.

Leta efter lösningar som

- erbjuder smidig konfiguration och enkel AI-användning i dagliga arbetsflöden
- ger flexibel åtkomst från kostnadsfria AI-chattar till skalbara agentlösningar
- hjälper medarbetarna att skaffa sig AI-färdigheter och integrera dem i sitt arbete.

Fråga 5

Integreras det smidigt i befintliga ramverk?

Din verksamhet har nu sin egen digitala infrastruktur med program, appar och mycket annat.

Leta efter lösningar som

- integreras smidigt med dina verktyg och program för minsta möjliga störningar
- ger en kontinuerlig AI-upplevelse i alla appar så att arbetet kan löpa vidare smidigt mellan verktyg
- automatiserar och optimerar uppgifter i befintliga arbetsflöden.

Fråga 6

Har användarna möjlighet att tänka nytt?

I grunden bör AI helt förändra hur arbete utförs. Det handlar inte bara om automatisering utan om att öka produktiviteten och ge utvecklingsutrymme.

Leta efter lösningar som

- förvandlar tidskrävande uppgifter till smidiga processer
- automatiserar repetitiva uppgifter
- ger medarbetarna tid tillbaka så att de kan fokusera på prioriteringar.

07

Microsoft 365 Copilot: AI du kan lita på

Microsoft 365 Copilot är generativ AI-lösningen som är konstruerad för att leverera robusta säkerhets-, styrnings- och åtkomstkontroller, vilket säkerställer säker driftsättning och hållbart innovationsarbete. Det ökar produktiviteten genom intuitiva verktyg som Copilot Chat, som går att använda överallt, och Copilot Studio, där ditt team kan skapa anpassade AI-agenter utan programmeringskunskaper.

Copilot integreras smidigt i er Microsoft 365-miljö, ärver användarbehörigheter, känslighetsetiketter, policyer för skydd mot dataförluster och krav på var data ska förvaras geografiskt – utan extra konfiguration. Genom att bädda in AI i de verktyg som medarbetarna redan använder mildrar Copilot säkerhetsriskerna och behåller data i er betrodda Microsoft 365-miljö.

Microsofts åtaganden garanterar att organisationen har kvar kontrollen:

- Era data är säkra både då de lagras och när de överförs
- Era data används inte för att träna AI-modeller
- Ni väljer vilken information som ska hamna i molnet
- Du skyddas mot AI-säkerhetsrisker och upphovsrättsrisker

Specialbyggda styrningsverktyg som Copilot Control System och SharePoint Advanced Management ger IT-teamen den synlighet, de kontroller och de granskningsloggar som krävs för att bibehålla efterlevnaden.

Med Microsoft 365 Copilot behöver du inte välja mellan innovation och säkerhet – det går bra med båda.

08

Den säkra vägen mot AI-utveckling

AI-revolutionen är en unik möjlighet för IT-ledare att leverera strategiskt värde genom att väga av innovation mot säkerhet.

När du implementerar säkra AI-verktyg som Microsoft 365 Copilot ger du medarbetarna verktyg för att bli mer produktiva samtidigt som riskerna med skugg-AI undanröjs. Vägen framåt handlar om att möjliggöra innovation på ett säkert vis. Ditt ledarskap inom säkert AI-bruk gör att IT-avdelningen uppfattas som utvecklingens riddare och hjälper organisationen att blomstra under denna nya era samtidigt som data är säkra och följer standarden.

Kom i gång med Microsoft 365 Copilot

Källor:

[1] Superagency in the workplace: Empowering people to unlock AI's full potential, McKinsey & Company, 28 januari 2025. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work.

[2] AI på arbetet är här. Det är nu det svåra jobbet börjar, Microsofts årliga index för arbetstrender, 8 maj 2024. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part

[3] Kommer AI att göra arbetet? Microsofts årliga index för arbetstrender. 9 maj 2023. https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work.

[4] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 m skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), Europaparlamentet och Europeiska unionens råd, 27 april 2016 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.