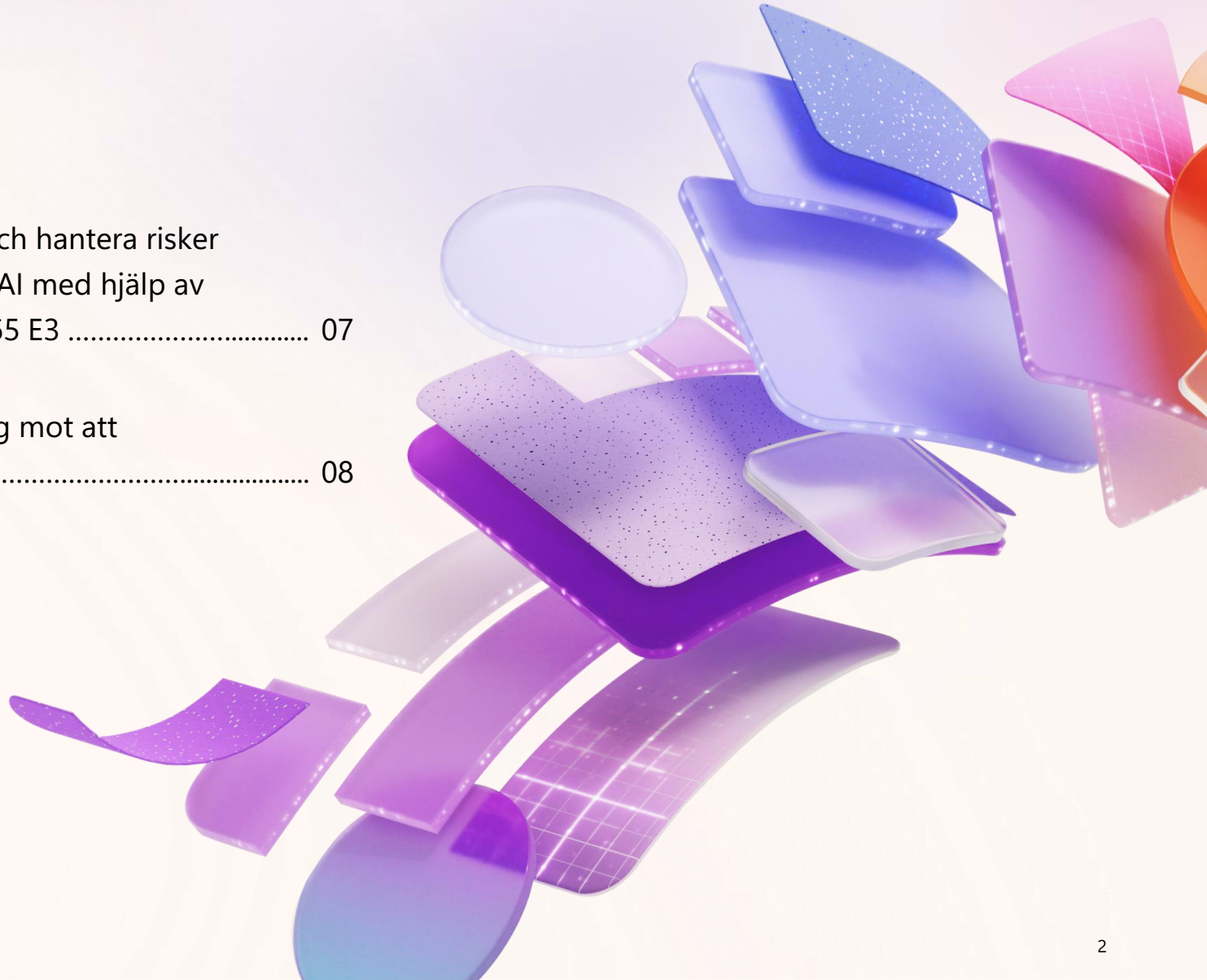
Microsoft 365

Från kontroll till insikt:
Hantera risker med skugg-AI

Innehållsförteckning



Inledning

I den senaste rapporten Index inom arbetstrender uppgav mer än 80 procent av de kunskapsarbetare som tillfrågades i 31 länder – däribland medarbetare och ledare – att de saknade tid eller energi för att göra sitt arbete. Dessutom rapporterade över 50 procent av de tillfrågade verksamhetsledarna att produktiviteten behövde öka för att man skulle kunna nå målen[1]. Enligt 2024 års upplaga av Microsoft rapport Index inom marknadstrender letar många medarbetare efter verktyg inom generativ AI för att åtgärda den bristen, och väntar inte på officiellt IT-godkännande innan de börjar använda verktygen.

När verktygen används utan IT-avdelningens insyn kan de utgöra säkerhets- och efterlevnadsrisker för organisationen. Och skugg-AI – användning av AI-verktyg utan godkännande från IT-avdelningen – håller på att bli den senaste formen av skugg-IT på dagens arbetsplatser.

I takt med att AI-införandet accelererar, försöker verksamhetsledare ligga steget före och motverka potentiella risker som dessa verktyg kaninnebära. I en färsk studie från iSMG uppgav 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]. Dessutom rapporterade över 90 procent av de tillfrågade CIO:erna och CTO:erna att generativ AI redan har lett till eller kommer att leda till större investeringar i cybersäkerhet inom deras organisation[3].

I den här e-boken presenteras några vanliga scenarier där skugg-AI används, potentiella risker för organisationer, fem strategier för riskhantering samt hur Microsoft 365 E3 kan göra arbetet enklare.

[1] **Index inom arbetstrender, årsrapport 2025, Microsoft, Inc., april 2025.** Microsoft analyserade enkätdata från 31 000 heltidsanställda eller egenföretagande kunskapsarbetare i 31 länder mellan 6 februari 2025 och 24 mars 2025, arbetsmarknadstrender från LinkedIn samt biljoner produktivitetssignaler från Microsoft 365.

[2] **iSMG:s Second Annual Generative AI Study: Business Rewards vs. Security Risks,** Baserat på enkätsvar från över 360 affärs- och cybersäkerhetsexperter under tredje kvartalet i sex regioner (Nordamerika, Europa, Asien, Sydamerika, Australien och Afrika)

[3] **The AI Security Balancing Act: From Risk to Innovation, NTT DATA, juni 2025,** baserat på data från en NTT DATA-undersökning med över 2 300 seniora beslutsfattare inom GenAI, inklusive 1 500 personer i ledningsgrupp från 34 länder.

Vad är skugg-AI? Och varför är synlighet viktigt?

Skugg-AI syftar på medarbetarnas användning av verktyg och appar för artificiell intelligens utan uttryckligt godkännande eller tillsyn från IT-avdelningar, ofta utanför de officiella säkerhets- och efterlevnadsramarna. När medarbetare söker sätt att öka produktiviteten och hantera den växande arbetsbördan kan de vända sig till oauktoriserade lösningar för att effektivisera sina uppgifter, samarbeta eller skapa nytt innehåll – ofta utan att inse de potentiella riskerna som är förknippade med detta. Skugg-AI är inte synligt för IT-avdelningen, vilket gör det svårt för organisationen att veta vilka appar som används och vilka som utgör de största riskerna.

Varför det är viktigt att skugg-AI syns

När IT-avdelningen inte är medveten om existensen av en app eller tjänst, kan man heller inte skydda eller stödja den. Denna *synlighetsbrist* gör det svårt att på ett korrekt sätt identifiera, hantera eller motverka potentiella hot kopplade till exponeringen av känsliga data och bristande efterlevnad av regelverk. Dessutom kan man förlora kontrollen över företagets egna information. IT- och verksamhetsledare behöver få synlighet i den skugg-AI som används inom organisationen, hantera de framväxande riskerna med AI-användningen och besluta om vilka verktyg som ska tillåtas med rätt skyddsåtgärder. Möjligheten för organisationer är att omvandla skugg-AI från en risk till en möjlighet att förnya arbetssättet på ett säkert sätt. För att organisationen ska kunna göra detta måste det finnas en bättre balans – så att medarbetarna kan utnyttja användbara AI-verktyg inom ett reglerat, säkert ramverk så att de potentiella riskerna minskar.

INSIKTER

Du kan inte skydda dig mot det du inte kan se. När IT-avdelningen inte är medveten om att en app eller tjänst används kan den inte säkra den. Detta är kärnan i problemet med skugg-IT – och det belyser varför ett nytt angreppssätt behövs. Att helt enkelt förbjuda alla externa verktyg är inte praktiskt om medarbetarna anser att dessa AI-verktyg är avgörande för att de ska kunna uppfylla sina mål. I stället behöver organisationer lyfta fram skugg-AI – skapa insyn kring vad medarbetarna använder, sätta relevanta kontroller på plats och erbjuda säkra, godkända alternativ som uppfyller organisationens behov. Kort sagt är utmaningen att stärka teamen med AI *utan* att ge avkall på säkerheten.

Skugg-AI på arbetsplatsen: Exempelscenarier och potentiella risker

Skugg-AI uppstår när medarbetare vill öka sin produktivitet och effekt, eller prova en ny teknik. Nedan följer flera fiktiva exempel som illustrerar hur osanktionerade AI-verktyg kan användas och vilka potentiella risker de kan medföra:

Roll	Exempelscenario	Potentiella risker med osanktionerade verktyg
Marknadsföring	Använda ett verktyg med generativ AI för att skapa marknadsföringstext eller design med företagets varumärkesdata.	Läckage av känslig varumärkes- eller produktinformation, tappa kontrollen över hur en extern AI-tjänst kan lagra eller använda företagets kreativa resurser.
Ekonomi	Ladda upp företagets ekonomiska data till en AI-driven analys- eller visualiseringstjänst för snabba insikter.	Exponering av konfidentiella ekonomiska data (budgetar, prognoser) till tredje part, potentiella efterlevnadsbrott (till exempel GDPR) avseende kund- eller personaldata som inkluderas utan lämpliga skyddsåtgärder.
Kundsupport	Dela kunddata eller transkriptioner från supportchattar i ett AI-verktyg för att formulera svar eller sammanfatta ärenden.	Brott mot reglerna för integritet och datahantering – känslig kundinformation kan lagras utanför företagets system, det finns inga garantier för datakvarhållning eller korrekt borttagning hos AI-leverantören.
Frontlinjen – detaljhandel	Butikschefer som använder AI-drivna schemaläggningsappar på sina mobiler för att optimera personalens arbetsscheman.	Företagets personaluppgifter (medarbetarnamn, scheman) laddas upp till en osanktionerad app, vilket medför risk för sekretessproblem. Motstridiga scheman eller policyöverträdelser kan inträffa om AI-förslagen inte överensstämmer med arbetslagstiftningen.
Frontlinjen – hälso- och sjukvård	Sjuksköterskor eller läkare som använder en AI-chattrobot för att formulera vårdanteckningar eller besvara medicinska frågor.	Patienthälsoinformation (PHI) kan exponeras för en extern tjänst utan några skyddsåtgärder, vilket bryter mot efterlevnads- och sekretesskraven. De medicinska råden från AI-tekniken kan också vara overifierade och utgöra säkerhetsrisker.

I vart och ett av ovanstående fall hade den enskilde medarbetaren goda avsikter och letade efter en produktivitetsökning, men till följd av detta kan risker uppstå i organisationen.

Företagsinformation kan spridas över oauktoriserade plattformar, vilket skapar *utmaningar inom datastyrning*. Obeprövade appar kan införa skadlig kod eller säkerhetsrisker, vilket utökar angreppsytan utanför IT-avdelningens tillsyn. Det kan också uppstå problem med regelefterlevnaden. Ur ett IT-supportperspektiv kan supportavdelningen ha svårt att bistå slutanvändarna om något går fel med ett skugg-AI-verktyg, eftersom de inte har någon insyn i eller kontroll över det.

Fem sätt att hantera risker med skugg-AI

Med rätt strategi och verktyg kan du omvandla skugg-AI från ett potentiellt hot till en möjlighet att skapa en kultur av säker innovation. Stärk dina team med AI-produktivitetsverktyg *samtidigt som* du upprätthåller den tillsyn som krävs för att skydda verksamheten. Det innebär ett skifte från att säga ”nej, aldrig” till att säga ”ja – men med rätt skyddsåtgärder”. Följande fem tips är utformade för att hjälpa dig att hantera och ta kontroll över skugg-AI i din organisation:

01 Utvärdera och prioritera risker genom att identifiera omfattningen av skugg-AI

Du kan inte skydda det du inte kan se. Få insyn i de appar som används i organisationen via organisationens aktivitetsloggar. När du väl känner till vilka appar som används kan du identifiera vilka verktyg som behövs för att hantera känsliga data, samtidigt som du noterar vilka som inte överensstämmer med dina säkerhets- och efterlevnadspolicyer. Med dessa insikter kan du fatta ett mer välunderbyggt beslut om vilka appar du vill tillåta, övervaka eller begränsa för att hantera potentiella risker.

02 Uppnå snabba resultat med säkerhets- och efterlevnadspolicyer

Aktivera eller tillämpa policyåtgärder om du vill minska antalet potentiella risker med användning av skugg-AI. Du kan använda policyer för villkorsstyrd åtkomst för att begränsa användningen av högriskappar, använda policyer för dataförlustskydd för känslig information för att motverka överdelning och dataläckage, samt tillämpa grundläggande multifaktorautentisering och enhetsefterlevnad för alla användare. Dessa åtgärder minskar snabbt de mest påtagliga riskerna även om du inte har full överblick över de AI-appar som används.

03 Utbilda medarbetarna i de potentiella riskerna med skugg-AI

Ofta är medarbetarna omedvetna om de risker som användning av osanktionerade AI-verktyg kan innebära för en organisation. Kommunicera riskerna med skugg-AI ofta genom välplacerade dataförlustskyddvarningar, påminnelser om företagets policyer och korta utbildningar som kan få medarbetarna att byta till säkrare metoder, utan hårdhänt kontroll.

04 Minska riskerna ytterligare genom att erbjuda godkända AI-verktyg

Erbjud där det är möjligt medarbetarna godkända AI-verktyg som alternativ till osanktionerade. Ett bra sätt att begränsa skugg-AI är att tillgodose de vanligaste användningsfallen i organisationen med en sanktionerad lösning. Detta gör att IT-avdelningen kan behålla insyn och kontroll, samtidigt som användarna får stöd vid eventuella problem.

05 Upprätta löpande styrning

Integrera kontroller i din IT-styrningsrutin – granska aktivitetsloggar och rapporter regelbundet, uppdatera policyer när nya AI-tjänster dyker upp och håll ledningen informerad om framstegen (till exempel minskad användning av osanktionerade appar eller incidenter som har förhindrats). Då blir det enklare att hantera potentiella risker nu och i framtiden, allt eftersom landskapet förändras.

Genom att vidta stegen ovan kan du stärka både innovationskraften och säkerhet.

Medarbetarna kan använda godkända AI-lösningar på arbetsplatsen och IT-avdelningen säkerställer kontroll och efterlevnad över dessa lösningar.

Identifiera och hantera risker med skugg-AI med hjälp av Microsoft 365 E3

Microsoft 365 E3 ger organisationer möjlighet att identifiera skugg-IT, bedöma potentiella risker och tillämpa säkerhets- och efterlevnadspolicyer *utan* att hämma innovationskraften. Uppsättningen med integrerade funktioner för produktivitet, säkerhet och hantering gör det möjligt för dig att direkt hantera utmaningarna med skugg-AI.

Lösningen Microsoft 365 E3	Hur den hjälper dig att hantera potentiella risker med skugg-AI
Cloud App Discovery	**Identifiera och vidta åtgärder mot osanktionerade appar.** Med Cloud App Discovery kan du ladda upp aktivitetsloggar och skapa rapporter med ögonblicksbilder för att få insyn i mer än 31 000 molnappar – inklusive över 400 appar för generativ AI. Du kan då se vad som används i din organisation, av vem och hur ofta. Med den här informationen kan du fatta välunderbyggda beslut om vilka appar som ska tillåtas eller ha begränsad användning.
Dataförlustskydd i Microsoft Purview (DLP)	**Minska läckaget av känslig information.** Med Microsoft Purview DLP kan du definiera och tillämpa policyer som identifierar känslig information och blockerar eller begränsar delning av e-post och filer mellan olika Microsoft 365-tjänster. Exempelvis kan du konfigurera en regel som övervakar, granskar eller förhindrar att användare delar känslig information via e-post eller filer och varnar användaren.
Microsoft Entra ID P1	**Hantera åtkomsten till molnappar.** Med Microsoft Entra ID P1 kan du tillämpa policyer för villkorsstyrd åtkomst i syfte att styra vem som kan komma åt vilka appar och under vilka förhållanden. Du kan till exempel välja att kräva multifaktorautentisering eller begränsa inloggningar med företagsuppgifter till appar som du har identifierat ha hög risk. Microsoft Entra ID P1 ger åtkomst till molnresurser för rätt personer, på enheter som följer efterlevnadsreglerna, under godkända förhållanden – samtidigt som åtkomsten till icke godkända appar begränsas.
Microsoft Intune P1	**Tillämpa användningspolicyer för enheter och appar.** Med Microsoft Intune P1 kan du tillåta att hanterade enheter som följer efterlevnadsreglerna används i arbetet, och du får tillgång till verktyg för att hantera dessa enheter. Till exempel kan verktyget blockera installation av otillåten programvara på företagsdatorer eller skicka konfigurationer som begränsar åtkomsten till specifika webbplatser eller tjänster.
Microsoft Defender för Endpoint P1	**Begränsa trafik till otillåtna URL:er.** Med Microsoft Defender för Endpoint P1 kan du minska riskerna från webbplatser som du bedömer som riskabla, genom att blockera trafik till en icke godkänd webbadress från hanterade enheter. Exempelvis blockeras medarbetare som försöker besöka en känd riskfylld AI-webbplats från en företagsdator.

Ta nästa steg mot att införa AI →

Allt börjar med medvetenhet, rätt verktyg och en proaktiv plan. Microsoft 365 E3 tillhandahåller verktygen som gör det möjligt för din organisation att upprätta en robust säkerhetsgrund och ett ramverk för styrning av AI-lösningar. Du kommer att kunna få insyn i osanktionerade verktyg, aktivera policyer som skyddar känsliga data och behålla kontrollen över både användaråtkomst och enhetssäkerhet. Gör dig redo att övergå från en reaktiv hållning (hitta och blockera skugg-AI efter det uppstått) till en mer proaktiv strategi för att rikta AI-användningen mot säkra och hanterade kanaler. Genomför en bedömning av säkerhet för AI och lär dig hur du kan förbättra säkerhetsläget för AI. Läs mer om de funktioner som ingår i Microsoft 365 för företag.