nedscaper

Veilige AI in de praktijk: zo maak je je organisatie Copilot-Ready

Een bewezen route naar Copilot Readiness: van risico-inzicht tot veilige AI-adoptie in de praktijk.

NEDSCAPER.COM

Inhoudsopgave

Veilige AI in de praktijk: zo maak je je organisatie Copilot-Ready

AI-tools zoals Microsoft Copilot beloven een revolutie in productiviteit en efficiëntie. Ze helpen medewerkers sneller informatie te vinden, processen te automatiseren en betere beslissingen te nemen. Maar de mogelijkheden brengen ook nieuwe risico's met zich mee. In deze whitepaper laten we je zien hoe je je organisatie inricht voor het inzichtelijk maken en beperken van de risico's en het pakken van de kansen die AI biedt.

De belofte van AI is groot, maar de praktijk is weerbarstig. Je wilt innoveren, maar de veiligheid van je data en de naleving van wet- en regelgeving geen moment uit het oog verliezen. Als IT- of securityverantwoordelijke heb je een sleutelrol bij het uitbalanceren van innovatie en risicobeheersing. Je moet dus zorgen voor een veilige, compliant omgeving waarin medewerkers verantwoord gebruik kunnen maken van AI, zonder dat de organisatie wordt blootgesteld aan onnodige risico's.

Deze whitepaper geeft je een bewezen route naar Copilot Readiness. Je krijgt inzicht in de belangrijkste uitdagingen, thema's die spelen in de meeste organisaties, een pragmatisch stappenplan en concrete adviezen uit de praktijk. Met het stappenplanplan kun je bovendien direct aan de slag.

Verschillende rollen, verschillende risico's

Voor de Chief Information Security Officer (CISO) staat databeveiliging altijd bovenaan de agenda. De CISO ziet de introductie van Copilot en andere AI-tools als een kans om de organisatie slimmer te laten werken, maar maakt zich tegelijkertijd zorgen over het risico op datalekken en ongewenste toegang tot gevoelige informatie. De CISO vraagt zich dus af: hoe kunnen we AI veilig inzetten zonder dat de beveiliging van onze data in het gedrang komt?

De Security-Analist heeft als taak om inzicht te krijgen in incidenten die gerelateerd zijn aan AI en om deze incidenten op te lossen wanneer ze zich voordoen. De security-analist wil duidelijk hebben welke AI-tools in gebruik zijn, welke data daarbij worden gedeeld en welke risico's dat met zich meebrengt.

De Compliance Officer kijkt vooral naar de juridische en ethische kant van AI-gebruik. Voor deze functie is het essentieel dat het gebruik van Copilot en AI-agents volledig in lijn is met wet- en regelgeving, zoals BIO2 en de AVG. De compliance officer wil zeker weten dat gevoelige of bijzondere persoonsgegevens niet onbedoeld worden verwerkt of gedeeld via AI-tools, en dat de organisatie altijd kan aantonen dat zij aan de juiste verplichtingen voldoet.

Businessmedewerkers zien vooral de kansen van Copilot om sneller en efficiënter te werken, maar worstelen soms met de betrouwbaarheid van de resultaten. Oude of gedateerde documenten kunnen de uitkomsten van Copilot vertroebelen, waardoor bijvoorbeeld beleidsmedewerkers zich afvragen of zij volledig kunnen vertrouwen op de antwoorden die AI geeft. Zij zoeken naar manieren om de kwaliteit van data te verbeteren en het maximale uit Copilot te halen, maar doen dit niet altijd op de juiste of meest veilige manier.

5 belangrijke uitdagingen voor veilige AI

Voor alle genoemde punten uit de vorige paragraaf zijn natuurlijk binnen je organisatie al veel maatregelen genomen. Er is goed nagedacht over privacy-, security- en compliancebeleid en de noodzakelijke technologie is er. Waarom geeft AI dan toch nieuwe uitdagingen? Dat heeft 5 belangrijke redenen:

01 Ontbrekend beleid

Veel organisaties hebben nog geen duidelijk beleid voor het gebruik van AI en datasecurity. Dit betekent dat medewerkers vaak niet weten wat wel en niet is toegestaan, waardoor het risico op onbedoeld verkeerd gebruik toeneemt. Het ontbreken van beleid maakt het bovendien lastig om incidenten goed te beoordelen en af te handelen.

02 Dataclassificatie ontbreekt

Dataclassificatie is vaak niet afdoende ingericht, zowel voor nieuwe als voor bestaande data. Onjuist geclassificeerde data kunnen per ongeluk gedeeld worden met Copilot, met alle risico's van dien.

03 Oversharing

Oversharing is een veelvoorkomend probleem. Door beperkte access controls krijgen medewerkers soms toegang tot meer informatie dan strikt noodzakelijk is. Dit vergroot de kans dat gevoelige data via AI-tools wordt opgevraagd of gedeeld.

04 Oude data

De hoeveelheid oude data binnen organisaties is vaak enorm. Deze data zijn vaak niet geclassificeerd. Het opschonen en classificeren van deze data is een grote, maar noodzakelijke klus.

05 Schaduw-AI

Schaduw-AI is inmiddels een serieus risico. Medewerkers gebruiken AI-tools buiten het zicht van IT, waardoor het lastig is om grip te houden op datastromen en compliance. Dit vergroot de kans op datalekken en niet-compliant gedrag.

Op een aantal van deze knelpunten gaan we hieronder wat dieper in. In het 'Stappenplan: in 6 stappen naar Copilot Readiness' vind je tips om alle vijf de uitdagingen stap voor stap aan te gaan.

Waarom oude data een probleem is: Wanneer is het bedrijfsfeest?

Oude data hebben bovendien nog een probleem: ze vervuilen de output van je AI-tools. Laten we dit concreet maken met een voorbeeld uit de praktijk.

Stel: je organisatie heeft elk jaar een bedrijfsfeest. Dat bedrijfsfeest vindt elk jaar op een ander moment plaats - de ene keer in november, de andere keer in december, maar in ieder geval eens per jaar. Als je aan Copilot vraagt: “Wanneer is het bedrijfsfeest?” Dan is de kans heel groot dat je resultaten terugkrijgt uit het verleden. Waarom? Omdat Copilot simpelweg meer informatie vindt over bedrijfsfeesten uit 2022, 2023, 2024 en 2025 dan over het aankomende feest in 2026. De oude data overschaduwt daarbij de nieuwe data.

Vraag je “Wanneer is het bedrijfsfeest in 2026?” Dan is de kans aanzienlijk groter dat je correcte data terugkrijgt. Het verschil? Je promptingtechniek.

Dit illustreert twee cruciale punten:

Oude data vervuilt je Copilot-resultaten - niet omdat Copilot slecht werkt, maar omdat er simpelweg veel meer oude data zijn dan nieuwe data.

Medewerkers moeten leren effectief te prompten en AI veilig te gebruiken - ze moeten begrijpen hoe het werkt en hoe ze specifieke vragen stellen.

Het betekent trouwens allemaal niet dat je Copilot niet kunt gebruiken tot je data op orde zijn. Het is verleidelijk om je eerst druk te maken over je oude data. Maar realiseer je: de hoeveelheid data die je dit jaar genereert is aanzienlijk meer dan wat je vorig jaar hebt gegenereerd. En volgend jaar geldt dat weer. De vraag is dus: wil je focussen op je oude data, of heeft het meer waarde om in eerste instantie te focussen op die nieuwe data?

Wat veilgheid betreft is ons advies: iets van security is altijd beter dan geen security. Begin dus met classificatie van nieuwe data en werk met uitsluitingen. Je hebt dan een basishygiëne op orde en een goed startpunt voor een veilig gebruik van Copilot.

De epidemie van schaduw-AI

Het probleem van schaduw-AI is waarschijnlijk groter dan je denkt. Hoewel veel organisaties formeel AI-gebruik verbieden of beperken, blijkt uit onderzoek en onze ervaring dat bijna 60% van de medewerkers tóch AI-tools gebruikt, vaak zonder dat IT of security hiervan op de hoogte zijn.

Dit fenomeen, een specifieke vorm van schaduw-IT die we schaduw-AI noemen, onderstreept het belang van sturen op veilig gebruik in plaats van simpelweg blokkeren. Je kunt wel zeggen “we staan het niet toe”, maar medewerkers zoeken naar manieren om hun werk efficiënter te doen en grijpen daarbij naar de tools die voorhanden zijn. Het resultaat zien we in de praktijk: bij vrijwel al onze klanten zien we niet alleen Copilot en ChatGPT, maar ook onbekende AI-tools die op grote schaal worden gebruikt door medewerkers. Tools waarvan IT nog nooit van heeft gehoord en waarvan niemand weet hoe ze met data omgaan.

Om als organisatie te kunnen profiteren van de voordelen van AI zonder onnodige risico’s te lopen, is het essentieel om niet alleen regels op te stellen, maar ook te investeren in:

- **Bewustwording en training** over veilig AI-gebruik
- **Goedgekeurde alternatieven** die medewerkers echt veilig kunnen gebruiken
- **Monitoring** om te zien wat er werkelijk gebeurt
- **Sturing** in plaats van blokkeren

Stappenplan: In 6 stappen naar Copilot Readiness

Een succesvolle en veilige inzet van Copilot vraagt om een integrale aanpak waarin beleid, techniek en adoptie samenkomen. Onderstaande stappen vormen samen een logisch en praktisch stappenplan waarmee je als organisatie gecontroleerd en aantoonbaar compliant aan de slag kunt met AI.

Stap 1

Start met bewustwording en stakeholderbetrokkenheid

Begin met het creëren van draagvlak bij alle relevante stakeholders: IT, security, compliance, HR en het management. Organiseer een kick-off waarin je de kansen én risico's van Copilot bespreekt, en bepaal gezamenlijk de doelstellingen en randvoorwaarden. Zorg dat iedereen begrijpt waarom beleid, classificatie en technische maatregelen essentieel zijn.

Stap 2

Stel beleid en spelregels op

Formuleer een helder AI-beleid. Leg vast welke AI-tools zijn toegestaan, welke data gebruikt mag worden, en welke verantwoordelijkheden en processen gelden bij incidenten of vragen. Dit AI-beleid zou een verlengstuk moeten zijn van het bestaande databeleid, dat de taxonomie voor dataclassificatie bepaalt. In het AI-beleid leg je vast welke labels wel en niet mogen worden aangesproken door AI.

Wet- en regelgeving vormen hierbij het fundament. De NIS2/Cbw verplicht organisaties en hun leveranciers tot een expliciete risicoafweging en het classificeren van alle informatie(systemen). Dit betekent dat je niet alleen moeten bepalen welke typen informatie je verwerkt, maar ook welke aanvullende beveiligingsmaatregelen nodig zijn.In de praktijk betekent dit dat beleid, classificatie en technische controls hand in hand gaan bij het zorgen dat je compliant blijft.

Stap 3

Inventariseer data, rechten en AI-gebruik

Breng in kaart welke data er is, waar deze zich bevindt en hoe deze nu wordt gebruikt. Gebruik tools als Cloud App Discovery om inzicht te krijgen in het gebruik van AI-tools en SaaS-applicaties binnen de organisatie. Controleer via Entra ID welke AI-agents actief zijn en welke rechten zij hebben. Identificeer risicosites in SharePoint en bepaal waar gevoelige data staat.

Stap 4

Richt technische basismaatregelen in

Implementeer technische maatregelen die aansluiten op het beleid:

- Stel SharePoint Advanced Management in om risicosites uit te sluiten van Copilot-indexering
- Implementeer Data Loss Prevention (DLP) voor het blokkeren van gevoelige data (zoals BSN's)
- Zet Defender for Cloud Apps in om ongeautoriseerde AI-tools te blokkeren en het gebruik van goedgekeurde tools te monitoren
- Maak het classificeren van documenten verplicht

Start in deze stap met het labelen van nieuwe data volgens de vastgestelde taxonomie. Sluit oude, risicovolle data tijdelijk uit van Copilot-indexering totdat deze geclassificeerd is. Communiceer duidelijk naar medewerkers welke labels er zijn, wat ze betekenen en hoe ze moeten worden toegepast.

Stap 5

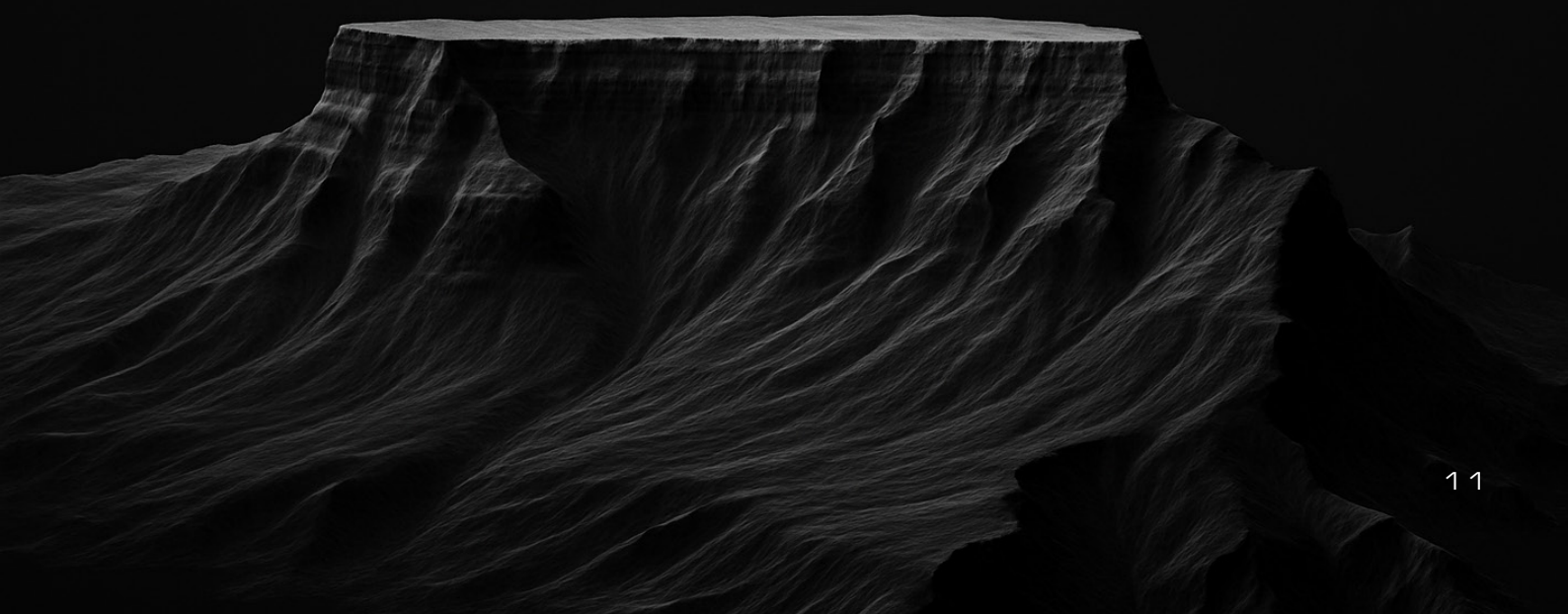
Train en begeleid medewerkers

Organiseer trainingen en awareness-sessies over veilig gebruik van AI, het belang van dataclassificatie en effectieve prompting. Maak duidelijk bij wie medewerkers terechtkunnen met vragen of incidenten. Stimuleer een cultuur van eigenaarschap en verantwoordelijkheid.

Stap 6

Monitor, evalueer en verbeter continu

Gebruik dashboards en rapportages om het gebruik van Copilot, AI-tools en datastromen te monitoren. Verzamel feedback van gebruikers en stakeholders. Evalueer regelmatig het beleid, de technische maatregelen en de adoptie, en stuur bij waar nodig. Schaal de aanpak gecontroleerd op naar meer afdelingen of een bredere scope zodra de basis op orde is.



Hoe Nedscaper je organisatie klaar maakt voor veilige AI

Nedscaper ondersteunt organisaties met een gefaseerde aanpak richting Copilot Readiness. We starten altijd met een risico-assessment en stakeholderworkshop, gevolgd door een 'AI-enablement' waarin we beleid, classificatie en technische maatregelen in de praktijk brengen.

Zo heb je binnen een paar weken al een veel beter beeld van je situatie en een veilige basis voor AI-gebruik.

Daarna begeleiden we je bij de uitrol. Als je wilt, nemen we daarbij ook verantwoording voor de volledige integratie en het lifecycle management van je AI-toepassingen.

Dit zijn de voordelen van onze aanpak:

Snel inzicht in risico's en quick wins
Binnen een week weet je waar je staat.

Praktisch en evidence-based stappenplan
Geen theorie, maar concrete acties.

Draagvlak en betrokkenheid bij alle stakeholders
Van IT tot HR tot de board.

Aantoonbare compliance en dataveiligheid
Metrics en rapportages die auditors overtuigen.

Flexibel opschalen van pilot naar volledige uitrol
Start klein, bewijs de waarde, schaal dan op.

Door Microsoft gecertificeerde specialisten
We kennen de tools van binnen en buiten.

MEER WETEN?

Wil je direct aan de slag met Copilot Readiness?

Boek een gratis intakegesprek en ontdek hoe jouw organisatie veilig en toekomstbestendig kan profiteren van AI.

Martijn Zantinge

Cybersecurity Architect

+31 20 299 9848

connect@nedscaper.com

nedscaper.com/contact/

Over Nedscaper

Nedscaper levert pragmatische, toegankelijke cybersecurity voor organisaties in Europa en Afrika. Onze dienstverlening is gebouwd op Microsoft-technologie en sluit naadloos aan op bestaande systemen en processen. Met Managed XDR bieden we 24/7 bescherming: continue detectie van nieuwe dreigingen, snelle en adequate respons, én persoonlijke ondersteuning om het beveiligingsniveau aantoonbaar te verbeteren.

Bij Nedscaper staat de menselijke factor centraal. Onze consultants begeleiden klanten stap voor stap, vereenvoudigen complexe keuzes en versterken preventieve maatregelen, zodat security niet alleen werkt in de tooling, maar ook in de praktijk. Vanuit onze kantoren in Amsterdam, Kaapstad en Johannesburg, en met een groeiend internationaal partnernetwerk helpen we organisaties, én de mensen binnen die organisaties, met vertrouwen te werken in een steeds digitalere wereld.

In 2025 werd Nedscaper door Microsoft uitgeroepen tot Channel Security Partner of the Year: een erkenning voor onze impact, specialisatie en schaalbare manier van werken.