

Copilot Readiness Assessment

Is jouw organisatie al klaar voor Copilot?

Microsoft is een belangrijke aandeelhouder in OpenAI, de organisatie achter ChatGPT. Met de integratie van de OpenAI geavanceerde Large Language Models (LLM's) binnen de Microsoft-productfamilies, onder de naam Microsoft Copilot, brengt Microsoft krachtige AI-functionaliteiten naar de gebruikers. Deze tools zijn inmiddels beschikbaar als onderdeel van de productiviteitsbundel "Copilot for Microsoft 365".

Binnen Bechtle hebben we de afgelopen maanden intensief gewerkt met de functionaliteiten van Copilot. Dit heeft ons waardevolle inzichten opgeleverd die we graag met jullie delen. Het Copilot Readiness Assessment is essentieel om je organisatie klaar te stomen voor het gebruik van deze technologie. Het helpt je de sterke én zwakke punten van je huidige security-infrastructuur in kaart te brengen en biedt een duidelijke roadmap om je omgeving optimaal voor te bereiden op Copilot.



Shortread: Copilot Readiness Assessment

Wat is een Copilot Readiness Assessment?

Het Copilot Readiness Assessment is een technische evaluatie op het gebied van data governance en data labeling.

Het biedt inzicht in de sterke en zwakke punten van je huidige security-inrichting. Op basis van deze inzichten bieden wij een rapport aan dat dient als roadmap. Aan de hand van deze roadmap kun je jouw online omgeving optimaal inrichten voor het gebruik van Copilot.



Inhoud van het assessment

Tijdens het assessment doorlopen we de volgende stappen:



1. Pre-engagement call

We starten met een kennismakingsgesprek om te bepalen met welke licenties je werkt en wat je uit het assessment wilt halen. Dit helpt ons om de sessie specifiek af te stemmen op jouw behoeften.



2. Copilot Discovery fase

Samen met jou kijken we, op locatie of remote, aan de hand van een uitgebreide questionnaire hoe ver jij bent in het proces om te werken met Copilot for M365. De questionnaire is ontworpen om inzicht te bieden in het securitybeleid van je organisatie en de Microsoft 365-omgeving. De focus ligt op drie assen:

- **Technische inrichting van de security d.m.v. de juiste licenties en extensies binnen je Microsoft 365-omgeving en data governance;**
- **Beleidsmatige en organisatorische aandacht voor security met een speciale nadruk op data labeling en data management;**
- **Kennis en bewustzijn van de medewerkers.**



3. Diepte-analyse

Tijdens deze fase gaan we dieper in op de quick wins die bereikt kunnen worden door de juiste technische invulling, zoals het toepassen van specifieke licentiestructuren of extensies op de huidige Microsoft 365-licenties.

Wil je meer inzicht in je databeheer? Dan kunnen wij in deze stap van het assessment met Avepoint Policies and Insights for Microsoft 365 hier antwoord op geven. Middels deze tool krijgen we inzicht in de gebruikersactiviteiten van Microsoft 365 om de productiviteit en beveiliging hiervan te verbeteren. Ook identificeert deze tool de beveiligingsrisico's. Daarnaast helpt het bij het monitoren van datagebruik waardoor je dataopslag en documentbeheer kunt optimaliseren.



4. Presentatie van bevindingen

Na het assessment presenteren we in een interactieve sessie de bevindingen en belichten we de specifieke aandachtspunten voor jouw situatie. Op basis van deze bevindingen kun je de eerste stappen zetten om 'Copilot ready' te worden.



Voor wie is het Readiness Assessment?

Het assessment is primair gericht op verschillende stakeholders binnen jouw organisatie die verantwoordelijk zijn voor security en IT-beleid, zoals:



Security Officers



Deze professionals houden toezicht op de naleving van beveiligingsprotocollen en het beheer van beveiligingsrisico's. Ze zorgen ervoor dat de organisatie voldoet aan de nodige beveiligingsnormen en -voorschriften.

CISO's (Chief Information Security Officers)



Deze leidinggevendenden zijn strategisch verantwoordelijk voor de informatiebeveiliging en de bescherming van gegevens binnen de organisatie. Ze ontwikkelen en implementeren beveiligingsbeleid en -strategieën om de organisatie te beschermen tegen cyberdreigingen.

IT-managers



Deze managers beheren de dagelijkse IT-operaties en zorgen ervoor dat de IT-infrastructuur veilig en efficiënt functioneert. Ze spelen een cruciale rol in de implementatie van beveiligingsmaatregelen en het waarborgen van de beschikbaarheid en integriteit van ITsystemen.

Wat zijn de vervolgstappen?

We hebben een breed aanbod aan verdiepende trainingen en assessments die wij kunnen inzetten op basis van de inzichten die we verkregen hebben in het Copilot Readiness assessment;

- Deepdive in Data Governance: Door middel van de Purview Quickscan of Avepoint Policies and Insights for Microsoft 365;
- Copilot Inspiratiesessie: Voor verdere inspiratie en ideeën over hoe Copilot van meerwaarde kan zijn in jouw organisatie;
- Copilot Accelerate: Aan de slag met Copilot. Een workshop ingericht op jouw unieke bedrijfsbehoeften, met de nadruk op operationele verbetering en gebruikersacceptatie;
- Threat Protection Engagement Workshop: Voor een diepere focus op beveiliging.



Shortread: Copilot Readiness Assessment

Meer weten?

Wil je meer weten over Copilot Readiness Assessment? Neem dan contact op via onderstaande knop.