

Het pleidooi voor IT-consolidatie



Inhoud

01

De wildgroei van IT is
uit de hand gelopen



02

Bevrijd je IT-team van
losstaande oplossingen



03

De kracht van eenheid



04

Bescherm het
gebruik van AI



05

Een geïntegreerd platform



06

Neem het voortouw
bij IT-consolidatie



De kans om je IT te consolideren

Dit eBook is bedoeld voor IT-leiders die niet langer alleen chaos willen beheren, maar hun IT-infrastructuur, -beheer en -personeel in harmonie willen samenbrengen. Leer hoe je de prestaties verbetert, complexiteit en kosten reduceert, efficiëntie verhoogt, de beveiliging versterkt en je organisatie voorbereidt op AI door te consolideren in één geïntegreerd platform.

01

De wildgroei van IT is uit de hand gelopen

Als je een digitaal ecosysteem beheert, kan geïntegreerde controle een onhaalbare zaak lijken. **De vereisten van je organisatie op gebied van productiviteit, beveiliging en AI-gereedheid veranderen continu. Om hieraan te voldoen, moet je oplossingen vaak tool voor tool patchen.** Met deze aanpak blijft de zaak weliswaar in beweging, maar het resulteert ook in een complex IT-systeem met veel losstaande elementen, waarvan het onderhoud tijdrovend en duur is.

IT-teams kunnen snel ondergesneeuwd raken in deze complexe en vaak dure stack van tools voor endpoint management, identiteits- en toegangsbeheer, berichten, e-mail, productiviteit - de lijst is eindeloos. Verschillende tools komen vaak van verschillende leveranciers, met elk unieke vereisten en geïsoleerde omgevingen. Geen wonder dat het lijkt alsof budgetten en resources tot het uiterste worden opgerekt.

De complexiteit stelt de gehele organisatie voor uitdagingen. De productiviteit stagneert wanneer medewerkers de hele dag worstelen met meerdere aanmeldprocedures en moeite hebben om informatie te delen tussen tools die niet onderling verbonden zijn. IT-teams moeten toegang tot resources zien te krijgen vanaf verschillende apparaten en locaties, maar gefragmenteerd endpoint management maakt het moeilijker voor ze om de beveiliging te handhaven. Het is tijd om al IT-tools bijeen te brengen en het beheer te vereenvoudigen.

Het ecosysteem van gespecialiseerde IT-tools en -leveranciers groeit maar door en dat gebeurt snel.



Bevrijd jezelf van de complexiteitstax

Bij elke nieuwe softwarelicentie kom je in hetzelfde patroon terecht: weer een oplossing, weer een kostenplaats en een laag van complexiteit erbij. IT-leiders moeten veel zien te doen met een beperkt budget en op de een of andere manier nog steeds middelen vinden om nieuwe AI-initiatieven te ondersteunen. Om het budget in de hand te houden, moeten veel IT-leiders continu kijken of hun infrastructuur dubbele en ongebruikte licenties bevat. In 2024 zochten IT-leiders op de volgende manieren naar mogelijkheden om te besparen:

83% reduceerde de uitgaven voor niet-gebruikte software²

82% verbeterde de contractvoorwaarden met leveranciers²

79% schafte goedkopere licentieopties aan²

Deze strategieën kunnen bescheiden besparingen opleveren, maar ze hebben een nadeel. Het beheer van dit groeiende aantal applicaties leidt tot een 'complexiteitstax'. Je moet waardevolle tijd en personeel inzetten om tools te controleren en niet-actieve functionaliteit te verwijderen, terwijl je tegelijkertijd de beveiligings- en toegangsinstellingen voor losstaande oplossingen moet beheren. IT-teams kunnen geen waardevolle tijd besteden aan werk met een hoge impact. Die moeten ze steken in licenties controleren, met leveranciers onderhandelen en incrementele besparingen zoeken terwijl ze ook nog alle bestaande oplossingen afzonderlijk moeten onderhouden. Deze tijdrovende taken leiden de focus af van zinnvoller werk.

Ondanks deze maatregelen om kosten te besparen sluipt de complexiteitstax toch weer naar binnen. Het enige duurzame pad naar de toekomst is om je benadering van technologie te herzien. Als je alles consolideert tot één alomvattend platform, neem je complexiteit weg en stel je je teams in staat zich te concentreren op het transformeren van hun activiteiten.

15%

van de organisaties gaf meer dan USD 5 miljoen aan **audits van softwareleveranciers** uit in de afgelopen 3 jaar²

61%

van de professionals in IT-assetbeheer zegt **nog steeds geen volledig zicht te hebben** op IT-assets die de zakelijke resultaten beïnvloeden.²

02

Bevrijd je IT-team van losstaande oplossingen

Voor organisaties met een breed assortiment aan technologische aanbiedingen is de dagelijkse realiteit van IT-werk vermoeiend. Elke eenvoudige oplossing vereist aparte expertise en het technologie-ecosysteem wordt een doolhof van van elkaar losstaande tools.

IT-teams raken overbelast door alle taken voor beheer, onderhoud, integratie en support. Elke specialistische tool vereist actief beheer, dus je hebt meerdere specialisten met gespecialiseerde vaardigheden nodig om de systemen in de lucht te houden. Nu al meldt **64%** van de IT-bedrijfsleiders dat ze moeite hebben geschikt personeel te vinden vanwege een gebrek aan benodigde vaardigheden of ervaring.³ Dat maakt het moeilijker om deskundige kennis voor je team te werven, te integreren en te behouden.



03

De kracht van eenheid

Er bestaat een betere benadering voor IT-beheer. Als je je IT-omgeving consolideert tot een uniforme oplossing, kun je de IT-overbelasting verminderen en een sterk, flexibel en gefocust team onderhouden. Dit biedt je de volgende mogelijkheden:

Beheer stroomlijnen van leverancierscontracten, onderhoud en operations

Productiviteit verbeteren door beheer van support en aanvragen te versnellen

Proactieve beveiliging van je IT-omgeving met uniform overzicht en beheer

Dit gaat niet alleen over het stroomlijnen van systemen. Het gaat erom de weg vrij te maken voor wat het belangrijkste is: je team in staat stellen de toekomst van hoe je organisatie werkt vorm te geven.

Beperk digitale frictie

Technologie moet geen obstakels opwerpen maar helpen de weg vooruit vrij te maken. Als IT-leider weet je dat **het gebrek aan verbinding tussen productiviteitstools op de hele organisatie drukt**.

62% van de mensen zegt dat ze teveel tijd kwijt zijn aan zoeken naar informatie gedurende de werkdag.⁵ De gemiddelde medewerker spendeert nu **57%** van de werktijd aan vergaderingen, e-mails en chats. Geen wonder dat **68%** van de mensen zegt dat ze niet genoeg ononderbroken focustijd hebben.⁵

Van elkaar losstaande, afzonderlijke oplossingen leiden op subtiele manieren tot frictie in de dagelijkse workflows, maar de frustraties stapelen zich snel op. Meerdere keren aanmelden, geïsoleerd werk, versnipperde informatie, systemen die niet samenwerken: elk punt van frictie is een kleine tax op creativiteit en innovatie.

Als je alles consolideert in één platform, kun je deze obstakels reduceren en ruimte scheppen waarin waardevolle creativiteit kan opbloeien. Stel je voor dat je organisatie is getransformeerd door consolidatie. Je personeel gebruikt een centrale, beveiligde gateway voor toegang tot alle tools en resources die ze nodig hebben. Informatie stroomt vrijelijk en samenwerking vindt plaats op natuurlijke wijze.

Wanneer frictie verdwijnt, ontdekken mensen opnieuw hun vermogen voor werk dat meer zingeving biedt. Het gaat er niet alleen om dat je obstakels uit de weg ruimt. Je moet ook een omgeving scheppen waarin technologie versterkt wat mensen kunnen doen.



Organiseer security centraal

Cyberbedreigingen worden steeds complexer. Kwaadwillende partijen hebben meer en betere resources en werken geavanceerder, met tactieken die ook voor de best voorbereide securityteams een uitdaging vormen. Naarmate securitybedreigingen steeds geavanceerder worden, wordt het steeds lastiger om ze bij te houden. **80%** van de organisaties heeft aanvalspaden die kritieke assets blootstellen.⁶ **82%** van de leidinggevendenden in security werd verrast door een beveiligingslek dat een bestaande beveiligingsmaatregel omzeilde.⁷

Organisaties besteden nu **65%** van hun securitybudget aan producten van derden, terwijl slechts **35%** ervan naar interne inspanningen gaat.⁸

Wat is de reden voor deze onbalans in de uitgaven? Grote ondernemingen werken vaak met een breed assortiment aan tools om te zorgen dat ze voor elke specifieke taak de beste oplossing hebben. Zelfs als dit betekent dat ze moeten jongleren met een grotere suite. Deze aanpak kan leiden tot meer uitgaven en grotere complexiteit.

600 mln.

aanvallen van cybercriminelen vonden plaats in 2024 - per dag⁶

2,75 x

stijging jaar-op-jaar in door mensen geleide ransomware-aanvallen⁶

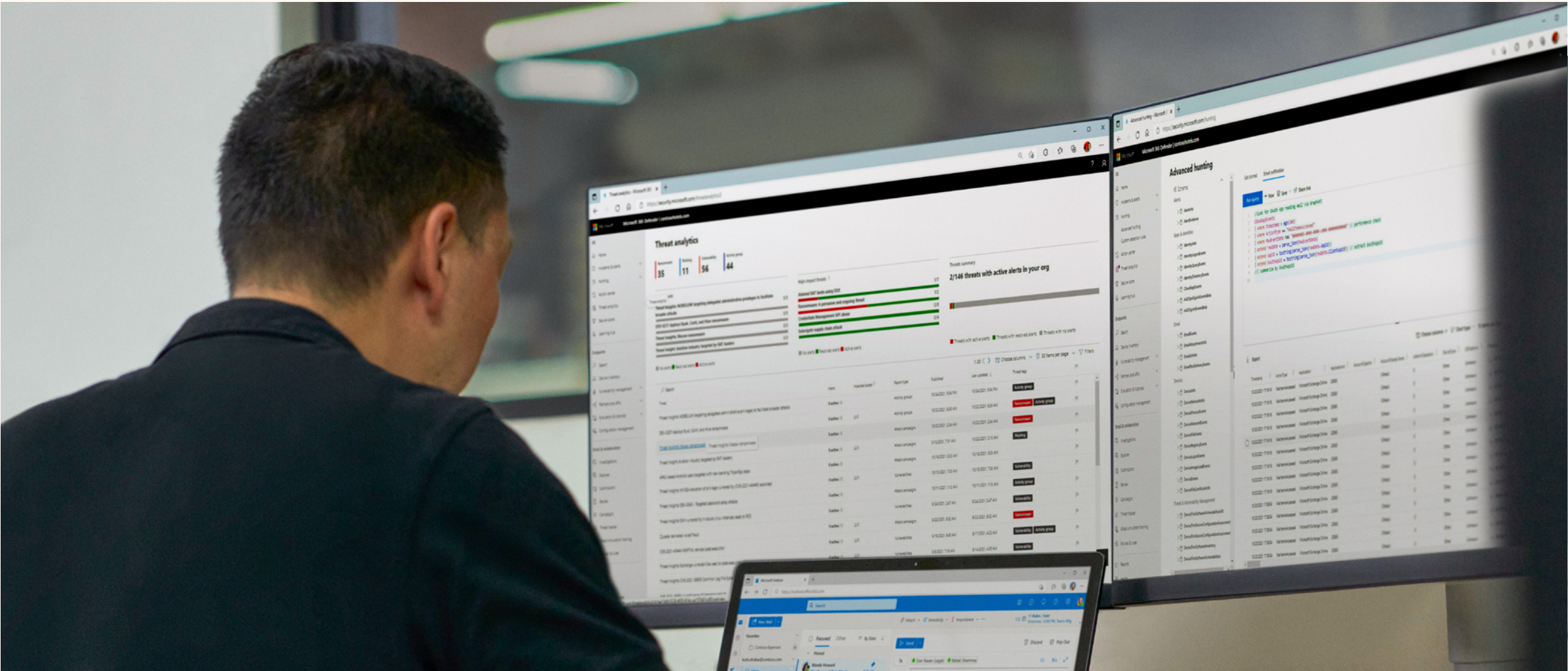
In reactie op toenemende bedreigingen voegen securityteams meer oplossingen toe.

19%

De gemiddelde toename over twee jaar in het aantal securitytools dat grote ondernemingen gebruiken⁷

Als je meer beveiligingstools inzet, kan dat aanvoelen alsof je een sterkere verdediging opzet voor je organisatie. Maar continu achter oplossingen aanjagen kan je organisatie juist kwetsbaarder maken. Een complexe IT-omgeving, met veel onderlinge afhankelijkheden, is moeilijker te begrijpen, te beheren en te beveiligen. Overbelasting door een teveel aan tools voorkomt dat je een helder beeld van de complete technische stack in je gehele onderneming krijgt. Het scheidt ook een groter potentieel aanvalsoppervlak met meer 'zijdeurtjes' in bedrijfssystemen.

Door je beveiliging te consolideren op een uitgebreid platform, transformeer je complexiteit naar duidelijkheid. Dat betekent dat je onbelemmerd zicht hebt op je gehele digitale omgeving. Een alsmaar groeiende verzameling uiteenlopende tools levert net de sterkste beveiliging op. Die krijg je wanneer je de juiste basis legt met een centraal platform.



04

Bescherm het gebruik van AI

Medewerkers wachten erop dat AI de werklast verlicht.

75% van de medewerkers **gebruikt al AI** op het werk⁹

78% van de AI-gebruikers **brengt al eigen AI-tools mee** naar het werk.⁹

Medewerkers wachten niet totdat de securityprotocollen weer bij geraken. Nu 'BYOAI'-tools (Bring your own AI) steeds populairder worden, kunnen organisaties achterop raken. Slechts **24%** van de initiatieven op gebied van generatieve AI omvat robuuste securitymaatregelen.¹⁰

Als organisaties niet de juiste basis leggen voor veilig AI-gebruik, kunnen medewerkers de productiviteitskloof overbruggen met schaduw-AI: niet-goedgekeurde tools buiten jouw systemen en buiten jouw controle.

Schaduw-AI werpt twee belangrijke uitdagingen op:

Geen toezicht

Schaduw-AI zet de deur open voor ernstige risico's. Wat weerhoudt medewerkers ervan om gevoelige informatie te kopiëren naar hun favoriete persoonlijke AI-tool? Elke interactie met ongecontroleerde BYOAI wordt een nieuwe securitybedreiging. Je data worden waarschijnlijk gelekt, of gebruikt om een extern model te trainen.

Beperkt nut

79% van de medewerkers heeft geen probleem met het gebruik van AI voor analytische taken⁵, maar een AI-tool is slechts zo goed als de informatie waartoe die toegang heeft. Gesegmenteerde, geïsoleerde AI-tools bieden vaak onvolledige antwoorden. Daarom hebben BYOAI-tools slechts een beperkt nut voor je personeel.





Organisaties bevinden zich nu op een tweekop: ze kunnen gefragmenteerd AI-gebruik laten uitlopen op mogelijke beveiligingsincidenten, of er controle over nemen en een geïntegreerd platform implementeren dat gereed is voor AI. Als IT-leider heb je een belangrijke strategische kans om je organisatie door deze kritieke tijd te leiden. Bied je gehele organisatie de volledige kracht van AI met een enterprise-suite die productiviteitsapplicaties, beveiliging en compliancemogelijkheden combineert, helemaal ontworpen voor naadloze AI-integratie.

Met een geconsolideerd platform kun je effectief de juiste tools implementeren om de risico's van AI-gebruik te verminderen en je data te beschermen. Consolidatie helpt je ook om een naadloze, beveiligde verbinding tussen de AI-oplossing van je organisatie en bedrijfseigen data, resources en workflows beter te implementeren en beheren. Zo kan je AI-oplossing de nauwkeurige, bruikbare inzichten bieden die werknemers nodig hebben om werk met grote impact te leveren.

Een geïntegreerd platform

Microsoft 365 E3 is een geïntegreerd platform dat IT-beheer vereenvoudigt, de productiviteit van je organisatie verbetert met verbonden ervaringen, tools en endpoints beveiligt en naadloos integreert met AI.

De voordelen van een consolidatie met Microsoft 365 E3

Reduceer je kosten voor IT

Kies een allesomvattende oplossing die beheer vanuit de cloud eenvoudiger maakt en leveranciers consolideert, zodat totale kosten worden geminimaliseerd en het rendement op investering verbetert.

Bescherm je organisatie

Beveilig de toegang tot data, applicaties en resources met een centrale oplossing voor bescherming tegen bedreigingen, sterke meervoudige verificatie, conditional access en continue toegangsevaluatie.

Implementeer generatieve AI op veilige wijze

Door een veilig fundament te bouwen met een uitgebreid platform dat de privacy en beveiliging van data waarborgt, is je organisatie gereed om AI te implementeren met Microsoft 365 Copilot.

Doorbreek de complexiteit van je IT

Centraliseer applicatie-, endpoint- en identiteitsbeheer en verminder het aantal afzonderlijk oplossingen voor productiviteit, waarbij toegang en gebruik worden gecontroleerd zonder de stroom van het werk in je organisatie te onderbreken.

Als je je IT-ecosysteem consolideert met Microsoft 365 E3, kies je voor een veiligere en productievere manier van werken. Met dit alomvattende platform zijn je IT-team en je hele organisatie voorbereid op alles wat op hun pad komt.



Neem het voortouw bij IT-consolidatie

Het tempo van de wildgroei in IT is niet langer houdbaar. Je digitale ecosysteem consolideren is niet alleen een strategische stap. Het is ook essentieel als je de kosten wilt verlagen, het beheer wilt vereenvoudigen, de productiviteit wilt verhogen en de security wilt versterken. Door je tools en processen op één lijn te brengen, kun je je organisatie efficiënter laten werken, sneller laten innoveren en AI met vertrouwen omarmen.



Aan de slag

Informatiebronnen:

¹ "The state of observability in 2024", Dynatrace, 2024.
<https://www.dynatrace.com/info/reports/state-of-observability-2024/>

² "2024 State of ITAM Report", Flexera, 2024.
<https://info.flexera.com/ITAM-REPORT-State-of-IT-Asset-Management>

³ "Challenges in recruiting employees in the IT industry worldwide 2023", Statista, 5 december 2023.
<https://www.statista.com/statistics/1425097/recruitment-challenges-in-the-tech-industry-worldwide/>

⁴ "Is IT Complexity Standing in the Way of Your Organization's Growth?" Harvard Business Review, 9 december 2022.
<https://hbr.org/sponsored/2022/12/is-it-complexity-standing-in-the-way-of-your-organizations-growth>

⁵ "Kan AI de problemen van ons werk oplossen?" Microsoft-werktrendindex, 9 mei 2023.
<https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>

⁶ "Microsoft Digital Defense-rapport 2024", Microsoft Security, 2024.
<https://www.microsoft.com/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024>

⁷ "2022 Security Leaders Peer Report", Panaseer, 2022.
<https://panaseer.com/resources/reports/2022-security-leaders-peer-report>

⁸ "The cybersecurity provider's next opportunity: Making AI safer", McKinsey & Company, 14 november 2024.
<https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer>

⁹ "AI op het werk is gearriveerd. Nu komt het moeilijkste gedeelte." Microsoft-werktrendindex, 8 mei 2024.
<https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>

¹⁰ "Cost of a Data Breach Report 2024" IBM, 2024.
<https://www.ibm.com/reports/data-breach>

¹¹ "Databaseveiliging als basis voor het veilig invoeren van AI", Microsoft Beveiliging, 2024
<https://clouddamcdnprodep.azureedge.net/gdc/gdckHueRY/original>

©2025 Microsoft Corporation. Alle rechten voorbehouden. Dit document wordt in de huidige staat aangeboden. Informatie en meningen in dit document, inclusief URL's en andere verwijzingen naar websites op internet, kunnen zonder kennisgeving worden gewijzigd. Gebruik is op eigen risico. Dit document geeft je geen enkel recht op enig intellectueel eigendom van welk Microsoft-product dan ook. Je mag dit document voor je eigen interne referentiedoeleinden kopiëren en gebruiken.