

En case om it-konsolidering



Indhold

01

It-spredning er ude af kontrol



02

Frigør dit it-team fra løsninger,
der ikke er integreret



03

Vigtigheden af
sammenhængskraft



04

Beskyt AI-anvendelse



05

En samlet platform



06

Gå forrest med
it-konsolidering



Muligheden for it-konsolidering

Denne e-bog er til it-ledere, der ønsker at stoppe med at bringe orden i kaos og vil skabe harmoni i deres it-infrastruktur, -styring og -medarbejdere. Find ud af, hvordan du øger ydeevnen, reducerer kompleksiteten og omkostningerne, fremmer effektiviteten, styrker sikkerheden og forbereder din organisation til AI ved at konsolidere til en samlet platform.

01

It-spredning er ude af kontrol

Når det gælder administration af et digitalt økosystem, kan samlet kontrol føles uden for rækkevidde. **For at imødekomme organisationens skiftende krav til produktivitet, sikkerhed og AI-parathed er man ofte nødt til at opdatere løsningerne ét værktøj ad gangen.** Selvom denne tilgang formår at holde tingene i gang, skaber det også et komplekst it-system, der ofte er usammenhængende, tidskrævende og dyrt at vedligeholde.

It-teams kan hurtigt blive overvældet af disse komplekse og ofte dyre værktøjer til styring af endpoints, identitets- og adgangsstyring, meddelelser, mail, produktivitet og meget mere. Forskellige værktøjer betyder ofte forskellige leverandører med unikke krav og siloopdelte miljøer. Det er ikke så mærkeligt, at det føles, som om budgetter og ressourcer er strakt til det yderste.

Kompleksiteten skaber udfordringer for hele organisationen.

Produktiviteten går i stå, når medarbejderne bruger deres dag på at navigere mellem flere loginoplysninger og kæmper for at dele oplysninger på tværs af usammenhængende værktøjer. Når de forsøger at få adgang til ressourcer fra forskellige enheder og placeringer, gør fragmenteret styring af endpoints det sværere for it-teams at opretholde sikkerheden. Det er tid til at samle it- værktøjer og forenkle styringen.

Økosystemet af specialiserede it-værktøjer og -leverandører vokser hele tiden, og det sker lynhurtigt.



Stop med at betale prisen for unødvendig kompleksitet

Hver ny softwarelicens følger et lignende mønster: en ny løsning, et nyt omkostningscenter, et nyt lag af kompleksitet. It-chefer bliver bedt om at gøre en masse med et begrænset budget, og på en eller anden måde skal de stadig finde ressourcer til at understøtte nye AI-initiativer. For at holde budgettet under kontrol er mange it-ledere nødt til at evaluere deres infrastruktur konstant for overlappende og ubrugte licenser. I 2024 jagtede it-ledere besparelser på følgende måder:

83 % reducerede udgifterne til ubrugt software²

82 % forbedrede deres **kontraktforhandling med leverandører**²

79 % købte billigere licensmuligheder²

Disse strategier kan give moderate besparelser, men der er en hage ved dem. Administration af dette voksende kludetæppe af applikationer skaber en "kompleksitetsskat". Det tager værdifuld tid og personale at overvåge værktøjer og fjerne inaktiv funktionalitet, mens man administrerer sikkerheds- og adgangsindstillinger for usammenhængende løsninger. I stedet for at fokusere på arbejde med høj prioritet bruger it-teams værdifuld tid på at overvåge licenser, forhandle med leverandører og lede efter trinvis besparelser, samtidig med at de vedligeholder hver eksisterende løsning individuelt. Disse tidskrævende opgaver stjæler fokus fra mere meningsfuldt arbejde.

På trods af disse omkostningsbesparelser sniger kompleksitetsskatten sig op igen.

Den eneste bæredygtige vej frem er at nytænke din teknologitilgang. Konsolidering på en omfattende platform vil reducere kompleksiteten og give teams mulighed for at fokusere på at transformere virksomheden.

15 %

af organisationer har betalt over 5 millioner USD i **revisioner fra softwareleverandører** i løbet af de sidste 3 år²

61 %

af medarbejdere, der styrer it-aktiver, siger, at de **stadig ikke har fuldt overblik** over it-aktiver, der påvirker forretningsresultater²

02

Frigør dit it-team fra løsninger, der ikke er integreret

For organisationer med en stor serie af teknologiløsninger er den daglige virkelighed med it-arbejde udmattende. Hver enkeltstående løsning kræver sin egen ekspertise, og det teknologiske økosystem bliver en labyrint af usammenhængende værktøjer.

It-teams bliver overbebyrdet med alle de administrations-, vedligeholdelses-, integrations- og supportopgaver, der skal løses. Hvert specialiseret værktøj kræver håndgribelig styring, så du har brug for flere specialister med et smalt sæt kompetencer blot for at holde systemerne kørende. I forvejen melder **64 %** af it-virksomhedslederne om udfordringer, når de skal ansætte kandidater, på grund af manglende nødvendige færdigheder eller erfaring.³ Det gør det sværere for dig at ansætte, onboarde og opbygge ekspertviden i dit team.



03

Vigtigheden af sammenhængskraft

Der er en bedre tilgang til it-administration. Ved at konsolidere til en samlet løsning kan du reducere it-overbelastningen og opretholde et stærkt, fleksibelt og fokuseret team. Det giver dig mulighed for at:

Strømline administrationen af leverandørkontrakter, vedligeholdelse og drift

"Øge produktiviteten ved at fremskynde support og administration af anmodninger

Sørge for proaktiv sikring af dit it-miljø med samlet synlighed og styring

Det handler ikke kun om at strømline systemerne. Det handler om at bane vejen for det, der betyder mest: at give dit team handlekraft til at forme fremtiden for, hvordan din organisation fungerer.

Minimer digital friktion

Teknologi bør hjælpe med at bane vejen fremad og ikke skabe forhindringer. Som it-leder ved du, at **manglende sammenhæng mellem produktivtørværktøjer påvirker hele organisationen.**

62 % af de adspurgte siger, at de har problemer med, at de bruger for meget tid på at lede efter information i løbet af deres arbejdsdag.⁵ Den gennemsnitlige medarbejder bruger nu **57 %** af sin arbejdsdag på møder, mails og chat, så det er ikke mærkeligt, at **68 %** af de adspurgte siger, at de ikke har nok uafbrudt fokustid.⁵

Usammenhængende punktløsninger skaber modstand i de daglige arbejdsprocesser på måder, som man knap bemærker, men frustrationerne hober sig hurtigt op. Flere loginoplysninger, siloopdelt arbejde, spredte oplysninger og systemer, der ikke arbejder sammen – hvert friktionspunkt udgør en lille forhindring for kreativitet og innovation.

Ved at konsolidere til én platform kan du reducere disse barrierer og skabe plads til, at der kan opstå værdifuld kreativitet. Forestil dig, at din organisation bliver transformeret ved hjælp af konsolidering. Medarbejderne bruger en central og sikker gateway til at få adgang til alle de værktøjer og ressourcer, de har brug for. Informationen flyder frit, og samarbejde sker naturligt.

Når friktionen forsvinder, genopdager folk deres evne til mere meningsfyldt arbejde. Det handler ikke kun om at fjerne forhindringer – det handler om at skabe et miljø, hvor teknologien forstærker, hvad folk kan gøre.



Centraliser sikkerheden

Cybertrusselslandskabet er mere komplekst end nogensinde før. Cyberkriminelle har bedre ressourcer, er mere sofistikerede og har taktikker, der kan udfordre selv de bedst forberedte sikkerhedsteams. I takt med at sikkerhedstruslerne bliver mere sofistikerede, bliver det sværere at følge med. **80 %** af organisationerne har angrebsstier, der eksponerer kritiske aktiver.⁶ **82 %** af sikkerhedslederne er blevet overrasket af en sikkerhedsfejl, der slap uden om en kontrol, som de troede var på plads.⁷

Organisationer bruger nu **65 %** af deres sikkerhedsbudgetter på tredjepartsprodukter, mens kun **35 %** bruges på intern arbejdskraft.⁸

Hvad er det, der skaber dette skæve forbrug? Store virksomheder administrerer ofte en bred vifte af værktøjer for at sikre, at de har den bedste løsning til hver enkelt opgave, selv når det betyder, at de skal håndtere et større antal løsninger. Denne tilgang kan føre til øgede udgifter og kompleksitet.

600 mio. angreb fra cyberkriminelle fandt sted om dagen i 2024⁶

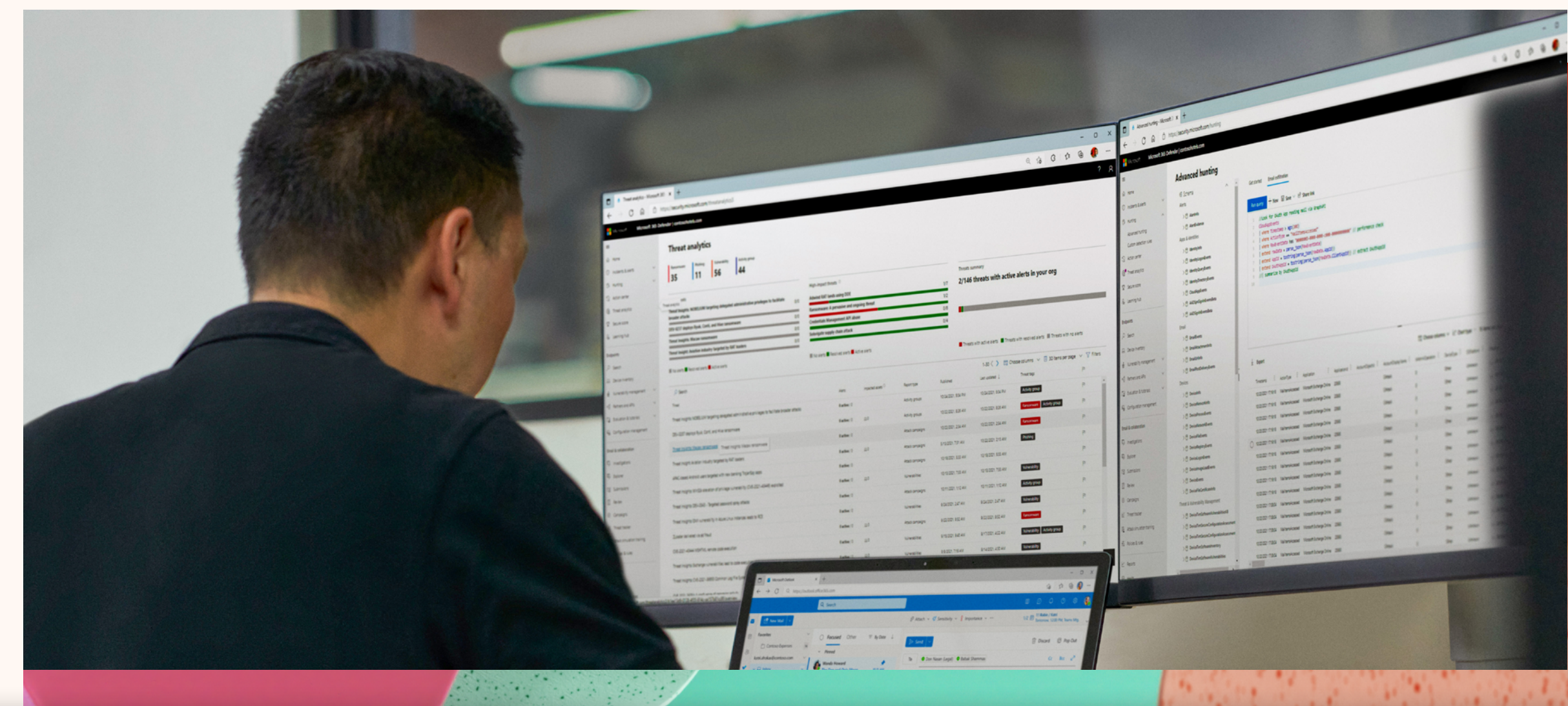
2,75 x stigning i forhold til året før i menneskedrevne ransomware-sammenkædede hændelser⁶

Som reaktion på stigende trusler tilføjer sikkerhedsteams flere løsninger.

19 % gennemsnitlig stigning i løbet af to år i antallet af sikkerhedsværktøjer, som store virksomheder bruger⁷

Hvis du tilføjer flere sikkerhedsværktøjer, kan det virke, som om du etablerer et stærkere forsvar for din organisation. Men en jagt på flere løsninger kan faktisk gøre din organisation mere sårbar. Et komplekst it-miljø – med mange indbyrdes afhængigheder – er sværere at forstå, administrere og sikre. Hvis du har for mange værktøjer, forhindrer det dig i at få et godt overblik over alle dine teknologiløsninger for hele virksomheden. Det skaber også en større potentiel angrebsflade med flere "sidedøre" ind i virksomhedens systemer.

Ved at konsolidere din sikkerhed på en helhedsorienteret platform kan du forvandle kompleksitet til klarhed. Det giver dig et godt overblik over hele din digitale ejendom. Det stærkeste sikkerhedsforsvar findes ikke i en voksende samling af forskellige værktøjer. Det kommer, når du etablerer det rigtige fundament med en central platform.



04

Beskyt AI-anvendelse

Medarbejderne er ivrige efter at få AI til at lette arbejdsbyrden.

75 % af medarbejderne **anvender allerede AI** på arbejdspladsen⁹

78 % af medarbejdere, der bruger AI, **medbringer deres egne AI-værktøjer** på arbejdspladsen⁹

Medarbejderne venter ikke på, at sikkerhedsprotokollerne bliver opdateret. I takt med at BYOAI-værktøjer (Bring Your Own AI) bliver mere og mere populære, kan organisationer sakke bagud. Kun **24 %** af de generative AI- initiativer omfatter robuste sikkerhedsforanstaltninger.¹⁰

Hvis organisationer ikke opbygger det rigtige fundament for sikker brug af AI, kan medarbejderne eliminere deres produktivitmæssige mangler med skygge-AI: ikke-sanktionerede værktøjer, der findes uden for dine systemer og uden for din kontrol.

Skygge-AI skaber to centrale udfordringer:

Ingen tilsyn

Skygge-AI åbner døren for alvorlige risici. Hvad forhindrer medarbejderne i at kopiere følsomme oplysninger til deres personligt foretrukne AI-værktøj? Hver interaktion med ikke-kontrollerede BYOAI-værktøjer bliver til endnu en sikkerhedstrussel. Dine data vil sandsynligvis ende med at blive lækket eller kan blive brugt til at træne en ekstern model.

Begrænset anvendelighed

79 % af medarbejderne ville føle sig trygge ved at bruge AI til analyseopgaver,⁵ men et AI-værktøj er kun så godt som den information, som det kan få adgang til. Segmenterede og siloopdelte AI-værktøjer giver ofte ufuldstændige svar. Derfor giver BYOAI-værktøjer kun begrænset anvendelighed for medarbejderne.





Organisationer står nu ved en skillevej: skal de lade fragmenteret brug af AI udvikle sig til potentielle sikkerhedsfejl, eller skal de tage kontrollen og implementere en samlet AI-parat platform? Som it-leder har du en vigtig strategisk mulighed for at guide din organisation gennem dette kritiske øjeblik. Levér den fulde effekt af AI på tværs af organisationen med en virksomhedsløsning, der samler produktivitetsapplikationer samt sikkerheds- og overholdelsesfunktioner – alt sammen designet til problemfri integration af AI.

En konsolideret platform giver mulighed for at implementere de rette værktøjer på en effektiv måde for at reducere risiciene ved brug af AI og beskytte dine data. Konsolidering hjælper dig også med bedre at implementere og administrere en problemfri og sikker forbindelse mellem din organisations AI-løsning og proprietære data, ressourcer og arbejdsprocesser. Det giver din AI-løsning mulighed for at levere den nøjagtige og brugbare indsigt, som medarbejderne skal bruge for at kunne levere arbejde med høj prioritet.

En samlet platform

Microsoft 365 E3 er en samlet platform, der forenkler it-administration, forbedrer produktiviteten i din organisation med integrerede oplevelser, beskytter værktøjer og endpoints og kan integreres gnidningsløst med AI.

Fordelene ved at konsolidere med Microsoft 365 E3

Reducer it-omkostningerne

Vælg en omfattende løsning, der forenkler administrationen fra skyen og konsoliderer leverandører for at minimere de samlede omkostninger og forbedre investeringsafkastet.

Beskyt din organisation

Sørg for sikker adgang til data, applikationer og ressourcer med en centraliseret løsning, der giver trusselsbeskyttelse, stærk multifaktorgodkendelse, politikker for betinget adgang og løbende adgangsevaluering.

Implementer generativ AI på en sikker måde

Ved at opbygge et sikkert fundament med en omfattende platform, der opretholder databeskyttelse og sikkerhed, bliver din organisation klar til at implementere AI med Microsoft 365 Copilot.

Ryd op i it-kompleksiteten

Centraliser applikations-, endpoint- og identitetsstyringen, og reducer samtidig punktløsninger for at sikre produktivitet – ved at styre adgang og brug uden at afbryde arbejdsstrømmen på tværs af organisationen.

Ved at konsolidere dit it-økosystem med Microsoft 365 E3 vælger du en mere sikker og produktiv måde at arbejde på. Denne omfattende platform rustet dit it-team og hele organisationen til fremtiden.

Gå forrest med it-konsolidering

Nutidens it-spredning er ikke længere bæredygtig. Konsolidering af dit digitale økosystem er ikke kun et strategisk skridt – det er vigtigt for at reducere omkostningerne, forenkle administrationen, fremskynde produktiviteten og styrke sikkerheden. Ved at samle dine værktøjer og dine processer giver du din organisation mulighed for at arbejde mere effektivt, skabe innovation hurtigere og indføre AI med tillid.



Kom godt i gang

Kilder:

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 omstrukturere arbejdet?" Microsofts indeks over arbejdstendenser, 9. maj 2023.
<https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>

⁶ "Microsofts rapport om digitalt forsvar" 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 på arbejdspladsen er her. Nu kommer den vanskelige del". Microsofts indeks over arbejdstendenser, 8. maj 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 "Datasikkerhed som fundament for sikker indførelse af AI" Microsoft Security, 2024.
<https://clouddamcdnprodep.azureedge.net/gdc/gdckHueRY/original>

©2025 Microsoft Corporation. Alle rettigheder forbeholdes. Dette dokument leveres "som det er og forefindes". De oplysninger og synspunkter, der kommer til udtryk i dette dokument, herunder webadresser og andre referencer til websteder, kan blive ændret uden varsel. Du bærer risikoen for at bruge det. Dette dokument giver dig ingen juridiske rettigheder til nogen immaterielle rettigheder i noget Microsoft-produkt. Du må kopiere og bruge dette dokument til egne interne referenceformål.