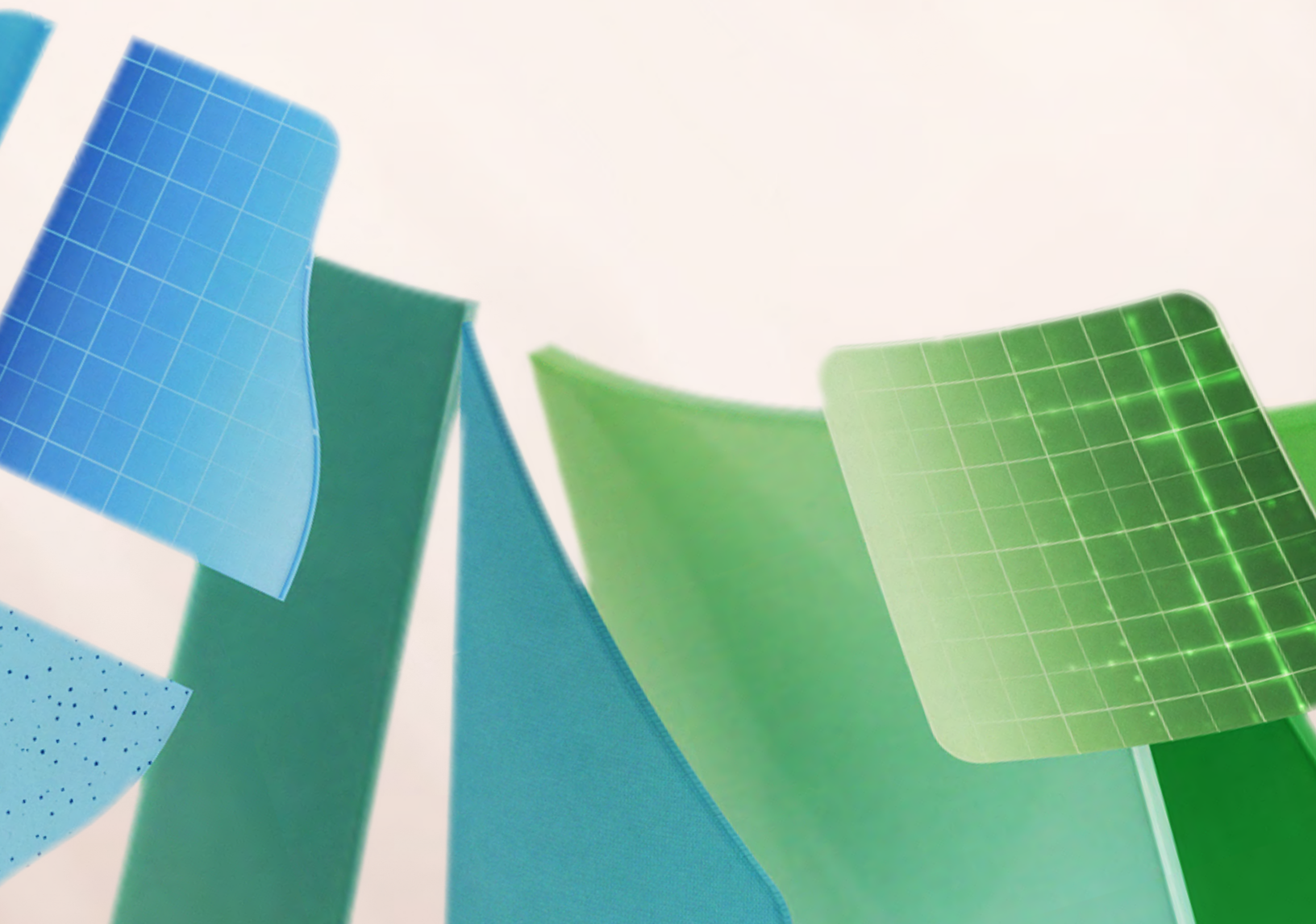


Hold styr på data

Mestring af datastyring for at opnå succes
med AI



Indhold

Introduktion

Datastyring er rygraden i sikker AI-implementering

Generativ AI lover godt for virksomhedstransformation – men for at udnytte dette potentiale skal dine forretningsdata både være af god kvalitet og tilgængelige.

Organisationer, der prioriterer effektiv datastyring, har også et godt udgangspunkt for at opnå en konkurrencemæssig fordel med AI. Datastyring hjælper med at sikre, at de data, der forespørges om og genereres af AI, er korrekte, sikre, kontrollerede og compatible.

Datakvalitet og tilgængelighed:

AI-systemer er afhængige af store datasæt af høj kvalitet for at give den bedst mulige respons med den rette kontekst fra organisationens unikke arbejdsprocesser. Jo bedre datakvalitet desto mere effektive AI-indsigter og forudsigelser.

Overensstemmelse: En effektiv datastyring sikrer overholdelse af lovkrav, hvilket reducerer risikoen for juridiske problemer og bøder.

Sikkerhed: Korrekt datamærkning og -management beskytter følsomme oplysninger mod uautoriseret adgang, irrelevant deling og databrud.

Tillid: Pålidelig datastyring styrker tilliden til AI-output hos interessenter, hvilket fremmer en bredere implementering og støtte til AI-initiativer.

I denne e-bog introduceres kritiske praksisser for datastyring, der skaber en AI-parat organisation. Den beskriver, hvordan du opretter robuste standarder for datakvalitet, sikrer overensstemmelse med lovkrav og implementerer databeskyttelses- og sikkerhedsforanstaltninger. Uanset om det handler om at forhindre, at følsomt mødeindhold bliver delt eksternt eller beskytte mod brud på datasikkerheden, vil du lære strategier til at opbygge tillid til AI-systemer og gøre data let tilgængelige for at skabe handlingsrettet indsigt. Med implementering af disse praksisser kan din organisation udnytte det fulde potentiale ved AI til løbende innovation og konkurrencemæssige fordele.

Anvendelsesscenarier med generativ AI

Accelerere kommunikation:

Udarbejd personligt tilpasset indhold hurtigere, og frigør tid til at opbygge relationer og samarbejde.

Opnå øget effektivitet: Reducer den tid, der bruges på rutineopgaver, skab større produktivitet, og reducer omkostningerne.

Understøttelse af innovation: Hjælp med at generere ideer og forslag til nye produkter og tjenester.

Tilpas kundeoplevelser: Skræddersy indhold og anbefalinger for at fremme loyalitet og engagement.

Forbedring af datastyring i forbindelse med AI-transformation

Alle virksomheder har politikker og processer, der styrer databrug. Strukturerne for datastyring varierer i modenhed og omfang, men få af dem er fuldt optimeret til AI. Mange bedste praksisser for datastyring forbliver de samme, f.eks. sikring af datanøjagtighed og ensartethed, mens andre aspekter kræver opdateringer for at få mest muligt ud af AI-investeringer. Lad os se på nogle få nøgleområder:

Datasynlighed

Detaljeret viden om dataflowet i AI-systemer gør det muligt at finde og afbøde uautoriseret eller upassende brug. Denne synlighed hjælper med at understøtte sikkerhed og overensstemmelse og beskytte følsomme data for at maksimere AI-værdien.

I traditionel datastyring har man fokuseret på at vide, hvor data er og på at kontrollere adgangen. Men efterhånden som AI bliver mere integreret i virksomhedens drift, skal datastyringen kunne holde trit med de skiftende sikkerhedsbehov. Et eksempel kunne være en meget følsom produktlancering, hvor

styring nu skal udvides til at administrere AI-genereret indhold og sikre, at projektrelaterede dokumenter, kommunikation og indsigter, der produceres af AI, er sikre. Dette betyder, at der skal implementeres sikkerhedsforanstaltninger, så kun autoriserede teammedlemmer kan få adgang til og bruge AI til at analysere eller opsummere projektoplysninger.

Ved at administrere databehandlings- og storage-mængder kan organisationer også bedre styre de driftsomkostninger, der er forbundet med AI.

Datakvalitet

AI forøger vigtigheden af data af høj kvalitet, da data af dårlig kvalitet påvirker AI-resultaterne direkte. Når du bruger AI-værktøjer til forespørgsler på dine virksomhedsdata, skal du sikre, at data er opdaterede og troværdige. Lige så vigtigt er det at kende til oprindelsen og kvaliteten af de data, som dine teams bruger til at udvikle deres egne AI-modeller og -apps. Regelmæssige datarevisioner, strenge valideringsprocesser og proaktiv management hjælper med at sikre dataintegritet. Ved at fokusere på disse områder kan organisationer opnå pålidelige AI-resultater, der skaber bedre beslutningstagning og innovation.

Brugeradministration

Med AI interagerer brugerne med data på sofistikerede måder. De kommunikerer med AI-systemer som Microsoft 365 Copilot via prompter på naturligt sprog. Ved at bruge tilladelse og beskyttelser kan AI få adgang til relevant kontekst fra data – såsom filer, chats og mails – sammen med eksterne kilder via plugins for at generere et svar.

Det er vigtigt at overvåge de data, der anvendes i disse processer, for at sikre, at AI giver korrekte, velbegrundede svar. Ved at skabe gennemsigtighed ved hjælp af transparente oplysninger eller links til kilder kan brugerne verificere oplysningerne, reducere risikoen for misbrug af data og sikre overensstemmelse med forordninger.

Overensstemmelse og eDiscovery

Stigningen i AI introducerer nye udfordringer inden for overensstemmelse og eDiscovery (håndteringen af data til retssager), især med hensyn til administration af AI-genererede data og tilpasning til de skiftende lovkrav. Opdatering af strukturer for datastyring for at håndtere disse udfordringer omfatter udvikling af politikker, der omfatter AI-genereret indhold, såsom at sikre, at AI-producerede dokumenter eller kommunikation spores, kategoriseres og opbevares på en sikker måde. Det kan f.eks. være nødvendigt at opdatere politikker for at sikre, at AI-genererede mails eller rapporter tagges og arkiveres korrekt med henblik på fremtidig hentning.

Forbedring af eDiscovery-funktioner vil omfatte integration af AI-værktøjer, der kan søge efter og identificere AI-genereret indhold på tværs af forskellige platforme. I forbindelse med en juridisk forespørgsel skal eDiscovery-værktøjer f.eks. være i stand til at finde og hente specifikke AI-genererede dokumenter, opsummere relevant kommunikation og levere klare revisionsspor for at bevise overensstemmelse. Ved at opdatere disse funktioner kan organisationer bedre administrere data under juridiske revisioner eller undersøgelser. Dette sikrer, at alle relevante AI-genererede oplysninger er tilgængelige, og at det er forsvarligt at bruge dem i retten.

Datasikkerhed

Beskyttelse af AI-drevne aktiviteter bør omfatte Nul tillid-principper på identitetsniveau, hvilket minimerer risikoen for uautoriseret adgang. Regelmæssige opdateringer af endpoints, herunder enheder og applikationer, reducerer antallet af sårbarheder, der kan udnyttes. Kendskab til, hvilke generative AI-værktøjer der anvendes i organisationen, giver mulighed for at blokere ikke-tilladte eller usikre applikationer, hvilket igen forhindrer potentielle sikkerhedsbrud. Ved at begrænse adgangen til AI-værktøjer og -data til kun betroede medarbejdere kan organisationer opnå større dataintegritet og beskytte deres AI-aktiviteter mod potentielle trusler.



Hvad er Nul tillid?

Nul tillid er en sikkerhedsmodel, der fokuserer på verificering af hver anmodning, som om den kom fra et ikke-betroet netværk. I stedet for at antage, at alt inden for virksomhedens firewall er sikkert, implementerer denne tilgang princippet "Hav aldrig tillid, bekræft altid".

Nul tillid-principper

Bekræft udtrykkeligt: Godkend og autoriser altid baseret på alle tilgængelige datapunkter.

Brug minimumsrettigheder for brugere: Begræns brugeradgangen med Just-In-Time og Just-Access (JIT/JEA), risikobaserede, tilpasningsdygtige politikker og databeskyttelse.

Antag, at der sker sikkerhedsbrud: Begræns skader, kontrollér adgang, anvend kryptering, og brug data til at spotte trusler og styrke forsvaret.

Dataforvaltningsrollen i AI-transformation: Oprindelse, kvalitet og pålidelighed

Når organisationer indfører AI som en hjælp til forretningsbeslutninger, skal de sørge for, at disse systemer kan levere korrekte og pålidelige resultater. De data, der danner grundlag for AI-svar, skal være tilgængelige, konsekvente og veldokumenterede.

Dataforvaltning understøtter pålidelig AI ved at implementere styringspolitikker, der sporer, hvor data kommer fra, kontrollerer deres kvalitet og sikrer pålideligheden og nøjagtigheden. Disse praksisser skaber fundamentet for AI-systemer, der leverer pålidelige indsigter og giver mulighed for velinformeret og sikker beslutningstagning.

Dataherkomst: Forståelse af oprindelse og ændringer i oplysninger

Dataherkomst sporer datas rejse gennem en organisation. Det dokumenterer dataenes oprindelse, transformationer og destinationer. Af flere årsager er det vigtigt for AI-drevne virksomheder at forstå data:

- **Gennemsigtighed:** At vide, hvor data kommer fra, og måden de ændres på, hjælper med at bekræfte nøjagtigheden af AI-genereret output og sikrer overholdelse af lovkrav ved at give en klar forståelse af dataenes historik.
- **Sporbarhed:** Dataherkomst gør det muligt for organisationer at spore fejl eller uoverensstemmelser tilbage til deres kilde, hvilket forenkler fejlfinding og datakorrektion.
- **Indvirkningsanalyse:** Forståelse af, hvordan data bruges af generative AI-værktøjer, hjælper med at vurdere den potentielle indvirkning af ændringer i datakilder og behandlingsmetoder på outputnøjagtighed og forretningsresultater.

Datakvalitet: Kvalitet højner værdien af AI-svar

Datakvalitet påvirker pålideligheden af AI-output direkte. Data af høj kvalitet skaber konteksten for AI-modeller, så de kan levere korrekte og værdifulde svar på brugerinput. De vigtigste aspekter af datakvalitet omfatter:

- **Nøjagtighed:** Data skal repræsentere forhold i den virkelige verden korrekt.
- **Fuldstændighed:** Alle nødvendige data skal være til stede og tages med i betragtning.
- **Konsekvens:** Data skal være konsekvente på tværs af forskellige systemer og over tid.
- **Rettidighed:** Data skal være opdaterede og tilgængelige efter behov.

Datapålidelighed: Sikre troværdige data

Datapålidelighed betyder, at data konsekvent opfylder kvalitetsstandarder og er tilgængelige efter behov. For AI-drevne virksomheder er pålidelige data vigtige for at fremme tilliden til AI-værktøjer og de beslutninger, de informerer. Sikring af datapålidelighed omfatter:

- **Dataredundans:** Implementering af backupsystemer, der forhindrer tab og øger tilgængelighed.
- **Regelmæssige sikkerhedskopieringer:** Udføre hyppige sikkerhedskopieringer for at beskytte mod datakorruption eller -tab.
- **Overvågning og advarsler:** Implementering af overvågningssystemer til at registrere og advare interessenter om dataproblemer i realtid.
- **Disaster recovery-planer:** Udvikling og test af planer for at gendanne data og genoptage driften hurtigt efter afbrydelser.

Forholdet mellem styring, sikkerhed og ansvarlig AI

Sammen skaber datastyring og sikkerhed rygraden i ansvarlig brug af AI. Sikre data af høj kvalitet sikrer, at AI fungerer etisk og effektivt. De vigtigste områder, der skal evalueres, er bl.a. dataklassificering, adgangskontrol, kryptering, hændelsesrespons og overholdelse af lovkrav.

Dataklassificering

Dataklassificering er en vigtig del af styringen af, hvordan AI-værktøjer håndterer følsomme oplysninger. Data og møder klassificeres normalt som generelle, fortrolige eller meget fortrolige. Korrekt klassificering sikrer, at AI kun får adgang til relevante oplysninger. Dette reducerer risikoen for at eksponere følsomme data for uautoriserede brugere.

Fejlklassificering kan derimod føre til, at AI behandler data, der skulle have været begrænset, og dette kan resultere i sikkerhedsbrud eller problemer med overensstemmelse. Effektiv datastyring – uanset om det sker via automatiserede værktøjer eller slutbrugerpolitikker – sikrer, at data klassificeres korrekt, beskytter følsomme oplysninger og understøtter AI's muligheder for at levere pålidelige outputs, der overholder lovkrav.

Adgangskontroller

Disse kontroller regulerer, hvem der har adgang til AI-relevante data, og hvilke applikationer eller identiteter der har tilladelse til at interagere med disse data. Svage adgangskontroller kan føre til uautoriseret eksponering af følsomme oplysninger, og dette øger risikoen for sikkerhedsbrud og misbrug.

Datastyring spiller en central rolle i håndhævelse af disse kontroller ved at begrænse dataadgangen til autoriseret personale og specifikke anvendelser for at sikre, at følsomme data håndteres korrekt. Dette beskytter ikke kun dataintegriteten, men sikrer også, at AI-systemer fungerer på sikre, pålidelige datasæt, og dette forbedrer deres pålidelighed og overensstemmelse.

Kryptering

Sikring af data mod opsnapping og manipulation ved hjælp af kryptering er med til at sikre, at generative AI-værktøjer kan finde grundlag for deres svar i korrekt kontekst – f.eks. arbejdsrelaterede data, filer, chats og mails – uden at risikere datalækage.

Datastyringspolitikker kan kræve robuste krypteringspraksisser, der beskytter data gennem hele dets livscyklus. Denne tilgang sikrer, at AI-værktøjer kan levere pålidelige svar, samtidig med at dine data beskyttes, og tilliden bevares.

Reaktion på hændelser

Følsomme organisatoriske data kan blive eksponeret gennem hændelser, der involverer generative AI-værktøjer, som giver uautoriseret adgang til filer, mails eller andre forretningsdata, som systemerne bruger til at generere svar.

I disse scenarier er en proaktiv beredskabsplan for hændelser afgørende. Uden en sådan plan risikerer organisationen ikke kun at afsløre følsomme data, men også at anvende kompromitteret output fra AI. Datastyring omfatter detaljerede svarprotokoller til hurtigt at håndtere brud og dermed minimere deres indvirkning og bevare AI-systemerne pålidelige.

Overholdelse af lovkrav

AI-applikationer skal overholde forordninger, f.eks. GDPR eller CCPA, som regulerer databeskyttelse og beskyttelse af personlige oplysninger. Manglende overensstemmelse kan føre til betydelige sanktioner og nedbryde tillid. Det er også vigtigt at vide, hvor AI-værktøjer behandler data, da mange værktøjer uden omkostninger kan håndtere data globalt eller uden for din virksomheds normale storageplaceringer. Datastyring sikrer, at AI-applikationer ikke kun kører inden for juridiske strukturer, men også bevarer data inden for de rigtige tjenestegrænser, så de overholder organisationens overensstemmelsesstandarder. Denne tilgang understøtter etisk brug af AI og hjælper med at opbygge tillid til AI-teknologi.



4

Opdatering af strukturen for datastyring for at understøtte AI-implementering

I det skiftende AI-landskab er det vigtigt at identificere specifikke områder i din eksisterende datastyringsstruktur, som kan kræve ekstra opmærksomhed. I stedet for at gennemgå hele strukturen kan du fokusere på områder, hvor der er størst sandsynlighed for udvikling, og styre din indsats mod de steder, hvor de vil øge værdien af AI mest, samtidig med at du sørger for, at dine data forbliver beskyttede og sikre. Her er nogle vigtige indsigter, du bør overveje:

Tilpasning af politikker og procedurer

AI indebærer nye former for dataindsamling, -behandling og -anvendelse. Opdatering af datapolitikker kan hjælpe med til at opfylde relevante behov omkring databeskyttelse, overholdelse af lovkrav og etisk anvendelse. For eksempel kan krav om dataanonymisering i specifikke tilfælde beskytte personlige oplysninger, så det er sikrere at anvende dem gennem hele AI-livscyklussen.

Roller og ansvarsområder

Det er vigtigt at indarbejde AI-parathed i alle de roller, der er involveret i datastyring. Medarbejdere, der er fortrolige med AI-datakrav, kan fungere som forvaltere, der støtter datakvalitet og overensstemmelse. Tværfunktionelt samarbejde mellem juridiske teams, it- og datavidenskabsteams kan bidrage til at håndtere AI-specifikke udfordringer mere effektivt.

Tilpasning af datastandarder og -definitioner

Standardisering af dataformater, definitioner og kvalitetsmålinger forenkler implementeringen af politikker, der styrer anvendelsen af AI-værktøjer i en organisation. Tydelige datastandarder gør det nemmere at beslutte, hvilke datasæt AI-værktøjer kan ræsonnere over for at skabe forretningskontekst, og hvilke data brugerne kan uploade til analyse. Dette sikrer, at AI-applikationer anvender de mest relevante og pålidelige data. Dette forbedrer deres effektivitet og understøtter samtidig overensstemmelse med organisationens politikker.

Løbende forbedring

Datastyring er en løbende proces, især med AI. Regelmæssige revisioner og opdateringer af din datastyringsstruktur kan bidrage med at tilpasse den til ny AI-udvikling og lovgivningsmæssige ændringer. AI i sig selv kan anvendes til at kontrollere og forbedre styringsmetoder, finde mangler og foreslå forbedringer. Denne proaktive tilgang forbedrer overensstemmelse og effektivitet, når AI-teknologien udvikler sig.

Værktøjer og teknikker til effektiv datastyring

Afstem i forhold til forretningsmål:

Sørg for, at din datastyringsstrategi understøtter organisatoriske mål for at forbedre beslutningstagning og effektivitet.

Automatiser rutinemæssige

opgaver: Brug automatisering til rutineprægede opgaver som dataklassificering og adgangsstyring for at mindske forekomsten af manuelle fejl og forbedre sikkerheden.

Sørg for, at du har høje standarder

for nøjagtighed: Brug værktøjer til validering og rensning til at understøtte dataintegritet over tid.

Uddan brugerne:

Tilbyd undervisning i værktøjer til datastyring og procedurer for at forhindre fejlhåndtering og sikre overensstemmelse med politikker.

Udfør regelmæssige revisioner:

Gennemgå datapraksisser regelmæssigt, så du sikrer, at de er ajour med lovgivningsmæssige og organisatoriske ændringer.

Konklusion

Effektiv datastyring for AI-aktivering med Microsoft 365

Ansvarlig brug af AI kræver robust datastyring. Effektiv datastyring sikrer datatilgængelighed, nøjagtighed og sikkerhed og gør det muligt for AI i at levere pålidelig indsigt og skabe innovation. Prioritering af datakvalitet, overensstemmelse og sikkerhed forbedrer AI-funktionerne og skaber bedre beslutningstagning og en konkurrencemæssig fordel.

Microsoft 365: Styrker AI-parathed

Microsoft 365 tilbyder førsteklasses produktivitetsapps med indbyggede værktøjer til klassificering, kontrol og beskyttelse af data. Disse funktioner understøtter din struktur for datastyring og giver mulighed for sikker AI-implementering, når du er klar til det. Microsoft 365 hjælper dig med at sikre:

- **Datakvalitet:** Understøt nøjagtighed og pålidelighed af AI-output.
- **Overensstemmelse:** Overhold de lovmæssige krav, og reducer de juridiske risici.
- **Nul tillid-sikkerhed:** Beskyt følsomme oplysninger mod uautoriseret adgang, brud og cybertrusler.

Opdag omfattende produktivitetsværktøjer, der er forbedret med AI-funktioner og robust beskyttelse, så du kan hjælpe din organisation med at fungere effektivt og sikkert.



Udforsk Microsoft 365