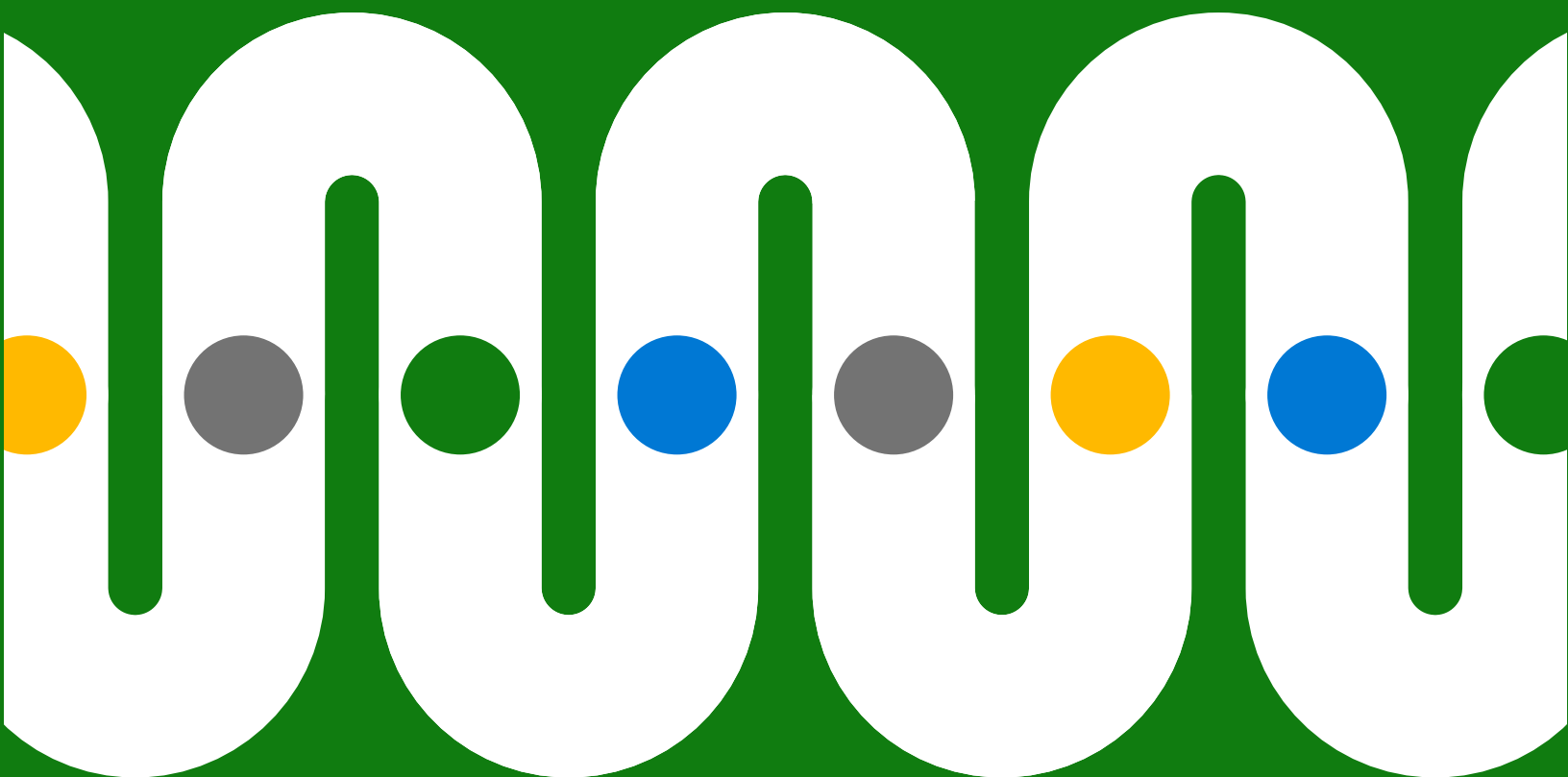


# 3 trin til beskyttelse af dine data fra start til slut



# Indhold

|                                                                                |   |
|--------------------------------------------------------------------------------|---|
| <b>Introduktion</b>                                                            | 3 |
| <b>Trin 1</b>                                                                  |   |
| <b>Identificer data</b>                                                        | 5 |
| <b>Trin 2</b>                                                                  |   |
| <b>Klassificer data</b>                                                        | 7 |
| <b>Trin 3</b>                                                                  |   |
| <b>Forebyg datatab</b>                                                         | 8 |
| <b>Tilføj ikke databeskyttelse som<br/>en eftertanke. Indbyg den i stedet.</b> | 9 |



**En undersøgelse blandt beslutningstagere inden for overholdelse af angivne standarder viste, at 95 % var bekymrede over databeskyttelsesudfordringer.<sup>2</sup>**

# Introduktion

Organisationer har oplevet en stor stigning i deres digitale aftryk med hybridarbejde, der strækker sig langt ud over det traditionelle kontor.

Det har ført til mere fragmentering og eksfiltrering af data – alt sammen kompliceret af hurtig vækst på tværs af et væld af applikationer, enheder og placeringer. Mange medarbejdere har også skiftet roller for at opnå større opfyldelse eller fleksibilitet, og det har blot skabt flere udfordringer og nye blinde vinkler på tværs af stadigt større datamængder.<sup>1</sup>

**Alle disse faktorer har fået CIO'er og CCIO'er til at nytænke deres tilgang til databeskyttelse.** I en sporingsundersøgelse blandt over 500 beslutningstagere inden for overholdelse af angivne standarder var næsten alle (95 %) bekymrede over databeskyttelsesudfordringer.<sup>2</sup>

<sup>1</sup> "[Sådan kan Microsoft hjælpe med at reducere insiderrisici under Den store rekonstruktion, Alym Rayani](#)", Microsoft Security. 28. februar 2022.

<sup>2</sup> "[Undersøgelse blandt 512 beslutningstagere i USA inden for overholdelse af angivne standarder, bestilt af Microsoft fra Vital Findings, september 2021](#)".

It- og sikkerhedsteams er på udkig efter bedre metoder til at administrere hele datalivscyklussen på tværs af multicloud-, hybrid cloud- og on-premises-miljøer. Denne tilgang omfatter tre vigtige trin:



### **Trin 1: Identificer data**

Fastsæt, hvor dine data findes, hvilken type data der er tale om, og hvordan de bruges eller deles



### **Trin 2: Klassificer data**

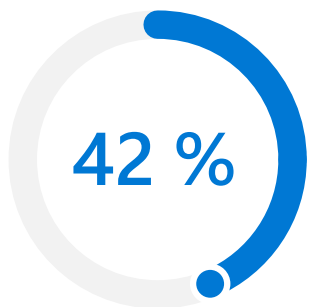
Klassificer og udfør mærkning af data, så du kan anvende passende politikker og risikoafhjælpning



### **Trin 3: Forebyg datatab**

Opnå en balance mellem risikoreduktion og fleksibilitet for dine medarbejdere med intelligent detektering og kontrol

**Målet med denne tilgang?** Lukke huller og minimere risikoen uden at gå på kompromis med produktiviteten.



**Når de bliver spurgt, hvor mange af deres data der er "mørke", sagde 42 % af organisationerne mindst halvdelen.<sup>3</sup>**

Disse "skjulte" data kan tage mange former – lige fra vedhæftede filer i mails og oplysninger om kundeopkald til maskinlogfiler og videooptagelser.

## Trin 1

# Identificer data

Hvis du ikke kan identificere dine data – hvor de findes, hvilken type de er, og hvordan de bruges eller deles – er det umuligt at anvende passende politikker eller beskyttelse.

Moderne organisationer genererer løbende enorme mængder data. Det er ikke kun dokumenter, mails og meddelelser, men alt lige fra sikkerhedsoptagelser til geoplaceringsdata – alt sammen i stadig større mængder grundet spredning på tværs af apps, enheder og storage, on-premises og i skyen.

**Det kan være svært at identificere alle disse data, og 42 % af organisationerne siger, at mindst halvdelen af deres data er "mørke".<sup>3</sup>** Dvs. oplysninger, der indsamles, men er ukendte eller ubrugte til forretningsmæssige formål. Nogle gange bliver data mørke, når den medarbejder, der har oprettet dem, skifter projekter eller roller. Der er ofte simpelthen ingen systemer til at identificere data på tidspunktet for oprettelse eller ændring.

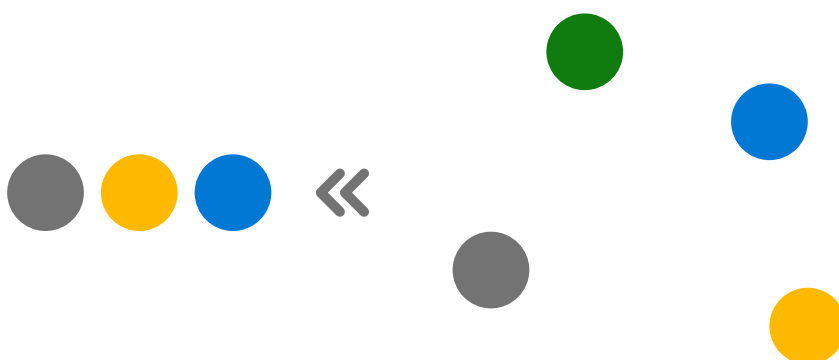
<sup>3</sup> "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. Juli 2022.

Vil du opbygge en arbejdsproces for komplet sporing på én platform?

Læs om datasporing i Microsoft Purview på **[Microsoft.com](https://microsoft.com)**.

Denne udfordring vil kun blive større. Mængden af nye data, der oprettes, registreres, replikeres og forbruges, forventes at være over fordoblet i 2026, og virksomhedsdata vokser mere end dobbelt så hurtigt som forbrugerdata.<sup>4</sup>

Kunstig intelligens (AI) og Machine Learning (ML) kan hjælpe ved at genkende følsomme data – såsom mailadresser, sundhedsdata, kreditkortnumre eller immaterielle rettigheder – og automatisk klassificere dem. AI og ML kan også øge klassificeringens nøjagtighed og gennemgå data med tilbagevirkende kraft. Disse identifikationsprocesser kan spænde over hele din datasamling ved at bevare, indsamle, analysere, gennemgå og eksportere indhold, uanset hvor det befinder sig, på tværs af alle cloud-løsninger.



<sup>4</sup> "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. Maj 2022.



### **Klassifikationer og politikker skal begge følge data, når de bevæger sig rundt.**

Hvis en medarbejder f.eks. kopierer kreditkortnumre fra et Microsoft Word-dokument til Excel, bør klassificeringen og politikkerne automatisk gælde for begge dokumenter.

Vil du administrere og beskytte følsomme data bedre på tværs af dit miljø?

Læs om dataklassificering og -beskyttelse i Microsoft Purview på **[Microsoft.com](https://microsoft.com)**.

## Trin 2

# Klassificer data

Korrekt dataklassificering hjælper dig med at fastsætte passende politikker og risikoafhjælpning for at sikre, at forskellige typer data ikke utilsigtet eller forsætligt misbruges eller tilgås uden autorisation. Kryptering og vandmærker kan yderligere beskytte data – uanset om de er i hvile, i transit eller i brug.

**Men klassificering og politikker skal følge data, når de bevæger sig rundt i organisationen.** Mærknings- og beskyttelsespolitikker kan ikke begrænses til separate dokumenter, de skal spænde over hele din digitale ejendom – lige fra on-premises-lagre, cloud-baserede lagre og SaaS-apps (Software som en service) til operativsystembaserede apps.

Traditionelle klassificeringstilgange involverer betydeligt manuelt arbejde, hvilket medfører risikoen for, at der begås fejl, eller at kritiske data uforvarende overses. Indbyggede klassificeringer, der kan trænes, kan hjælpe med at automatisere denne proces, og en integreret løsning giver administratorer mulighed for at administrere politikker centralt på tværs af alle systemer.





**DLP-politikker kan forhindre handlinger, der ikke opfylder overholdelsen af angivne standarder.**

Hvis en medarbejder f.eks. forsøger at downloade et regneark med kreditkortnumre på et flash-drev eller uploade det til cloud-storage, kan DLP-politikken identificere, at aktiviteten ikke opfylder overholdelsen af angivne standarder og forhindre den.

Ønsker du intelligent registrering og kontrol af følsomme oplysninger?

Læs om forebyggelse af datatab i Microsoft Purview på [\*\*Microsoft.com\*\*](https://www.microsoft.com).

## Trin 3

# Forebyg datatab

Når du har identificeret og klassificeret dine data, kan DLP-løsninger (forebyggelse af datatab) håndhæve komplette beskyttelsespolitikker, der afhjælper trusler som mørke data og dataeksfiltrering, så nuværende og tidligere medarbejdere ikke – bevidst eller uforvarende – deler, eksponerer eller overfører følsomme data uden tilladelse.

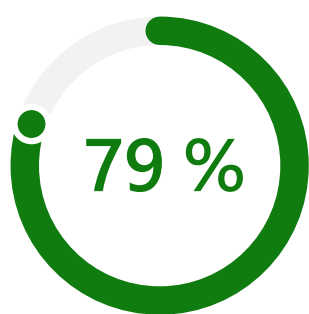
**Intelligente DLP-løsninger bruger kontekst til at finde en balance mellem fleksibilitet og blokering af handlinger med høj risiko.** Enkeltpersoner vil f.eks. kunne fortsætte med en handling, efter de er blevet mindet om potentielle risici og gældende politikker. Dette kan hjælpe med at beskytte følsomme data og samtidig undervise brugerne i bedre at forstå risici.

DLP-løsninger er med til at beskytte immaterielle rettigheder og andre kritiske virksomhedsdata samt hjælpe med at overholde forordninger som den generelle forordning om databeskyttelse (GDPR), HIPAA (Health Information Portability and Accountability Act) og California Consumer Privacy Act (CCPA).

En omfattende tilgang til DLP gennemtvinger konsekvent politikker på tværs af organisationen, hvilket beskytter svagheder ved punkter i datalivscyklussen, der er det svageste "led i kæden".







**En undersøgelse blandt beslutningstagere inden for overholdelse af angivne standarder viste, at 79 % havde købt flere produkter til databeskyttelse og overholdelse af angivne standarder.**

Et flertal havde købt tre eller flere.<sup>5</sup>

# Tilføj ikke databeskyttelse som en eftertanke. Indbyg den i stedet.

Mange organisationer har prøvet en "bolt-on"-tilgang til databeskyttelse ved hjælp af flere løsninger til at administrere separate dele af datalivscyklussen. Men dette tvinger dine sikkerheds-, datastyrings-, overholdelses- og juridiske teams til at sammensætte et kludetæppe, der ofte er ineffektivt og belaster ressourcerne.

En "indbygget" tilgang kan lukke hullerne ved at samle dataidentifikation, dataklassifikation og DLP. Med en integreret løsning er det nemmere at administrere og håndhæve politikker centralt. Det reducerer også undervisningstiden for brugere, der modtager politikmeddelelser på en velkendt måde, lokalt i applikationer.

<sup>5</sup> "Undersøgelse blandt 200 beslutningstagere i USA inden for overholdelse af angivne standarder (n = 100 599-999 medarbejdere, n = 100 1000+ medarbejdere), bestilt af Microsoft med MDC Research, februar 2022."

# En indbygget, integreret løsning: Microsoft Purview

Microsoft Purview hjælper dig med at tackle udfordringerne ved nutidens decentraliserede, datarige arbejdsplads med et omfattende sæt løsninger, der hjælper dig med at styre, beskytte og administrere hele din datasamling.

**Gå længere end styring.**

[Lær mere om at beskytte dine data med Microsoft Purview >](#)

**Er du interesseret i et specifikt databeskyttelsesområde? Få mere detaljerede oplysninger om, hvordan Microsoft Purview kan hjælpe dig med:**

**Datasporing >**

**Dataklassificering og -beskyttelse >**

**Forebyggelse af datatab >**



**Microsoft Security**

©2022 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.