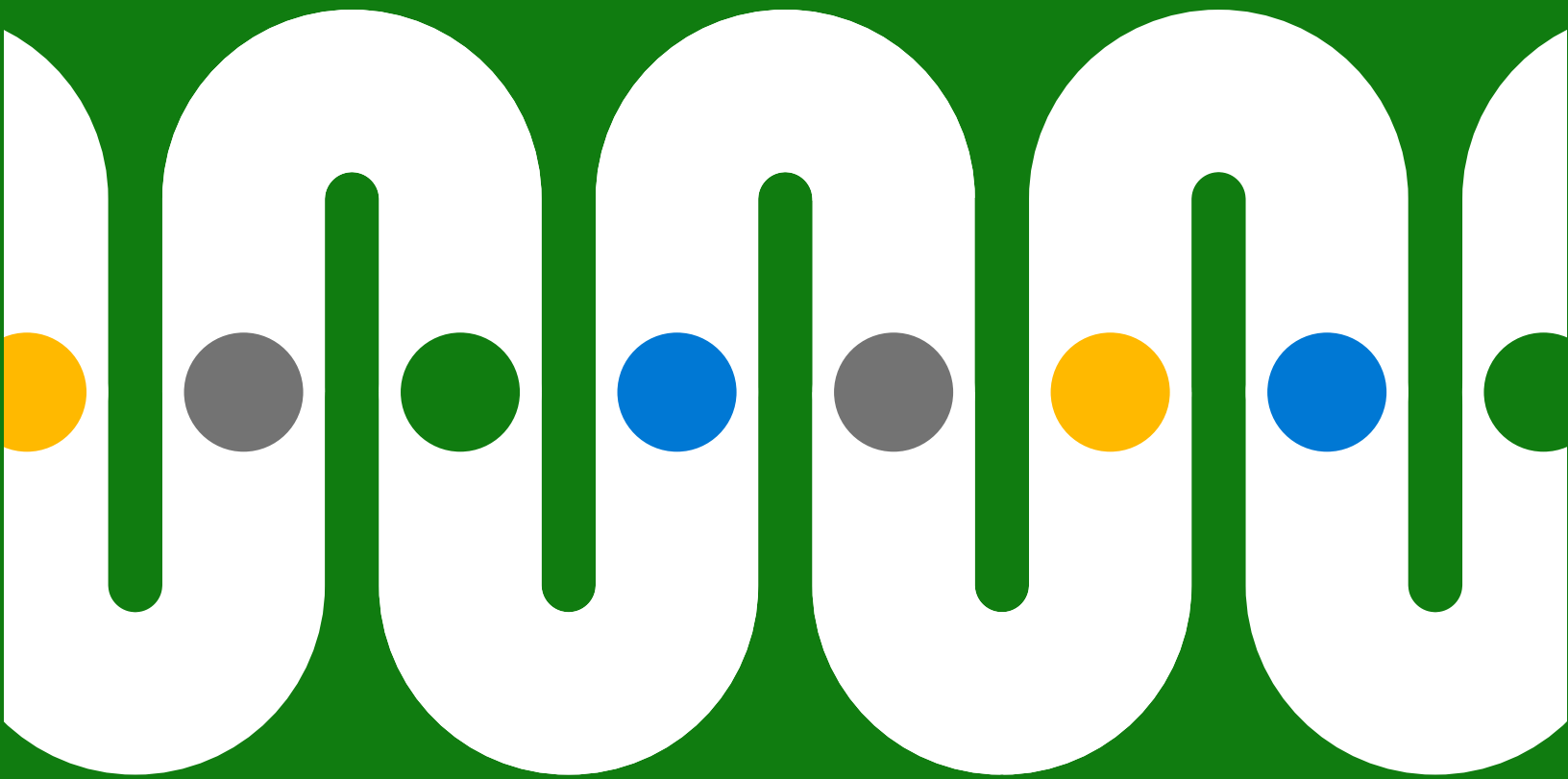
Microsoft Security

Drie stappen om je data van begin tot eind te beschermen



Inhoudsopgave

Inleiding 3

Stap 1
Data onderzoeken 5

Stap 2
Data classificeren 7

Stap 3
Dataverlies voorkomen 8

Voeg databescherming niet toe. Bouw het in. 9

Uit een enquête onder compliancebeslissers bleek dat 95% bezorgd was over uitdagingen op het gebied van databescherming.[2]

Inleiding

Met hybride werken hebben organisaties hun digitale voetafdruk enorm zien toenemen, tot ver buiten het traditionele kantoor.

Dat heeft geleid tot meer datafragmentatie en -lekken, wat nog eens wordt gecompliceerd door de snelle groei van het aantal applicaties, apparaten en locaties. Veel werknemers zijn op zoek naar meer voldoening of flexibiliteit van rol veranderd, wat extra uitdagingen met zich mee heeft gebracht en heeft gezorgd voor blinde plekken in de steeds grotere datadomeinen.[1]

Door al deze factoren zijn CIO's en CISO's hun aanpak van informatiebescherming opnieuw gaan bekijken. In een enquête onder meer dan 500 Amerikaanse compliancebeslissers maakten bijna alle respondenten (95%) zich zorgen om uitdagingen op het gebied van databescherming.[2]

[1] "Hoe Microsoft risico's van binnenuit tijdens de 'Great Reshuffle' kan helpen beperken, Alym Rayani", Microsoft Security. 28 februari 2022

[2] "September 2021 survey of 512 US compliance decision-makers ", Vital Findings in opdracht van Microsoft.

IT- en beveiligingsteams zijn op zoek naar betere manieren om de hele datalevenscyclus in multicloud, hybride cloud- en lokale omgevingen te beheren. Deze begin-tot-eindaanpak bestaat uit drie stappen:

Stap 1: data onderzoeken

Bepaal waar je data zich bevinden, wat voor soort data het zijn en hoe ze worden gebruikt of gedeeld

Stap 2: data classificeren

Classificeer en label data zodat je weet welke beleidsregels en maatregelen voor risicobeperking je moet toepassen

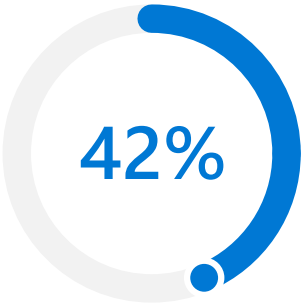
Stap 3: dataverlies voorkomen

Vind met intelligente detectie en bewaking een evenwicht tussen risicobeperking en flexibiliteit voor je mensen

Wat is het doel van deze aanpak? Het doel is om gaten te dichten en risico's te beperken, zonder dat de productiviteit daaronder lijdt.

Stap 1

Data onderzoeken



Op de vraag hoeveel van hun data 'duister' zijn, zei 42% van de organisaties minstens de helft.[3]

Deze 'verborgen' data kunnen vele vormen aannemen, van e-mailbijlagen en opnamen van telefoontjes met klanten tot machinelogboeken en videobeelden.

Als je weinig over je data weet – waar ze zich bevinden, wat voor soorten data je hebt en hoe data worden gebruikt of gedeeld – kun je nooit de juiste beleidsregels of bescherming toepassen.

Moderne organisaties produceren voortdurend grote hoeveelheden data. En dat zijn niet alleen maar documenten, e-mails en berichten, maar alles van beveiligingsopnamen tot geolocatiegegevens, en dat wordt nog verergerd door de wildgroei aan apps, apparaten en opslag, zowel lokaal als in de cloud.

Het onderzoeken van al die data kan moeilijk zijn, en 42% van de organisaties zegt dat ten minste de helft van hun data 'duister' is.[3] Daarmee bedoelen ze informatie die wel is verzameld, maar onbekend is of die niet voor zakelijke doeleinden wordt gebruikt. Soms worden data duister als de werknemer die ze heeft geproduceerd van project of rol verandert, en vaak zijn er simpelweg geen systemen om data op het moment van aanmaken of wijzigen te herkennen.

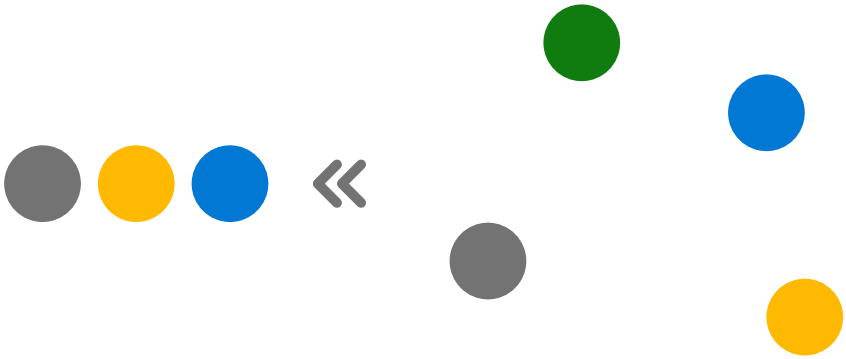
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. Juli 2022.

Wil je het hele onderzoeksproces in één platform samenbrengen?

Lees dan op **Microsoft.com** over datadetectie in Microsoft Purview.

Deze uitdaging zal alleen maar groter worden. De hoeveelheid nieuwe data die worden gecreëerd, vastgelegd, gekopieerd en geconsumeerd, zal tegen 2026 naar verwachting zijn verdubbeld, waarbij bedrijfsdata meer dan twee keer zo snel groeien als consumentendata.[4]

Kunstmatige intelligentie (AI) en machinelearning (ML) kunnen helpen door gevoelige data (zoals e-mailadressen, gezondheidsinformatie, creditkaartnummers of intellectueel eigendom) te herkennen en automatisch te classificeren. AI en ML kunnen ook achteraf de classificatie nauwkeuriger maken en data evalueren. Deze processen kunnen je hele datadomein omspannen, waardoor informatie waar ze zich ook bevindt, in alle clouds, kan worden behouden, verzameld, geanalyseerd, beoordeeld en geëxporteerd.



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. Mei 2022.

Stap 2

Data classificeren

Classificaties en beleid moeten de data overal blijven volgen.

Als een werknemer bijvoorbeeld creditkaartnummers uit een Microsoft Word-document naar Excel kopieert, moeten de classificatie en het beleid automatisch voor beide documenten gelden.

Goede dataclassificatie helpt je bepalen met welke beleidsregels en risicobeperkingsmaatregelen je kunt zorgen dat verschillende soorten data niet per ongeluk of opzettelijk worden misbruikt of zonder toestemming worden bekeken. Met versleuteling en watermerken kun je data nog beter beschermen, zowel in opslag, bij overdracht of bij gebruik.

Maar de classificaties en het beleid moeten de data overal in de organisatie blijven volgen. Labels en beschermingsbeleid kunnen niet tot afzonderlijke documenten worden beperkt, maar moeten je hele digitale domein bestrijken, van lokale tot cloudopslag, van software-als-service (SaaS) tot apps die op je besturingssystemen draaien.

Traditionele classificatiebenaderingen vereisen veel handmatig werk, waardoor het risico van fouten of het onbedoeld over het hoofd zien van kritieke data bestaat. Ingebouwde en trainbare classificaties kunnen dit proces helpen automatiseren, en met een geïntegreerde oplossing kunnen beheerders het beleid centraal voor alle systemen beheren.

Wil je gevoelige data in je omgeving beter beheren en beschermen?

Lees dan op **Microsoft. com** over dataclassificatie en -bescherming in Microsoft Purview.

Stap 3

Dataverlies voorkomen

DLP-beleid kan voorkomen dat wet- en regelgeving wordt overtreden.

Als een werknemer bijvoorbeeld probeert om een werkblad met creditkaartnummers naar een flashstation of een cloudopslag te kopiëren, kan DLP dit gedrag herkennen als tegen de regels en voorkomen.

Wil je gevoelige informatie intelligent detecteren en controleren?

Lees dan op **Microsoft. com** over preventie van gegevensverlies in Microsoft Purview.

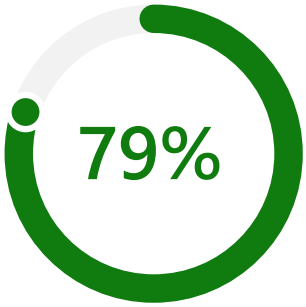
Zodra je data hebt gevonden en geclassificeerd, kun je met DLP-oplossingen (preventie van gegevensverlies) eind-tot-eindbeschermingsbeleid afdwingen om bedreigingen zoals duistere data en datalekken te beperken. Zo kunnen huidige en voormalige werknemers niet – bewust of onbewust – zonder toestemming gevoelige data delen, openbaren of overdragen.

Intelligente DLP-oplossingen gebruiken context om een balans te vinden tussen flexibiliteit en het blokkeren van risicovolle activiteiten. Mensen kunnen bijvoorbeeld na een herinnering over mogelijke risico's en relevant beleid toch verdergaan met hun handeling. Dit kan helpen om gevoelige data te beschermen, terwijl gebruikers ook worden getraind om risico's beter te begrijpen.

DLP-oplossingen helpen intellectueel eigendom en andere essentiële bedrijfsdata te beschermen, en zorgen ook voor betere compliance met regelgeving zoals de Algemene verordening gegevensbescherming (AVG), de Health Information Portability and Accountability Act (HIPAA) en de California Consumer Privacy Act (CCPA).

Een uitgebreide benadering van DLP zorgt dat beleid in je hele organisatie consequent wordt afgedwongen, waardoor ook de zwakste schakels in de datalevenscyclus worden beschermd.

Voeg databescher-ming niet toe. Bouw het in.



Uit een enquête onder compliancebeslissers bleek dat 79% meerdere compliance- en databeschermingsproducten had gekocht.

Een meerderheid had er drie of meer gekocht.[5]

Veel organisaties hebben geprobeerd om informatiebescherming toe te voegen door losse oplossingen voor het beheren van afzonderlijke delen van de datalevenscyclus te gebruiken. Maar hierdoor moeten je teams voor beveiliging, databeheer, compliance en juridische zaken een lappendeken bij elkaar houden die vaak niet effectief is een groot beroep op de middelen doet.

Een 'ingebouwde' aanpak kan de gaten dichten en dataherkenning, dataclassificatie en DLP samenbrengen. Met een geïntegreerde oplossing kan beleid makkelijker centraal worden beheerd en afgedwongen. Het vergt ook minder training voor gebruikers, omdat ze beleidsmeldingen op een vertrouwde manier binnen hun applicaties ontvangen.

[5] "February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) ", in opdracht van Microsoft met MDC Research.

Een ingebouwde en geïntegreerde oplossing: Microsoft Purview

Met Microsoft Purview kun je de uitdagingen van de moderne gedecentraliseerde, datarijke werkomgeving aangaan met een uitgebreide set oplossingen voor het besturen, beschermen en beheren van je hele datadomein.

Ga verder dan beheer.

Meer informatie over het beschermen van je data met Microsoft Purview >

Ben je geïnteresseerd in een specifiek aspect van databescherming? Lees gedetailleerde informatie over hoe Microsoft Purview je kan helpen met:
Data ontdekken >

Data classificeren en beschermen >

Preventie van gegevensverlies >

Microsoft Security