VERSTERK JOUW GEGEVENSBEVEILIGING MET MICROSOFT PURVIEW

Hier starten

HOE VEILIG ZIJN JOUW GEGEVENS?

Weet je welke gevoelige gegevens je hebt en waar deze zich bevinden? Hoe beveiligt je momenteel gevoelige gegevens in al jouw omgevingen en hoe voorkom je dat ze verloren gaan? En hoe beheer je insider-risico's? Dit zijn allemaal vragen die bedrijven zich vandaag de dag moeten stellen.

Feit is dat gegevensbeveiliging moeilijk is. Je moet e-mails, berichten, gedeelde opslag en cloud-apps beveiligen, evenals alle apparaten waarop gegevens worden geopend. Bovendien blijft de gemiddelde gegevensvoetafdruk van een bedrijf exponentieel groeien. Stel je zich eens voor: mensen creëren 2,5 quintiljoen bytes aan gegevens en versturen elke dag 333,2 miljard e-mails.[1] En met meer dan 300 miljoen mensen die over de hele wereld extern werken, kunnen incidenten met gegevensbeveiliging altijd en overal plaatsvinden.

Het is een moeilijke kwestie en de organisaties van tegenwoordig worstelen met een gefragmenteerd oplossingendomein. Meer dan 80% van de besluitvormers heeft meerdere producten aangeschaft om te voldoen aan de behoeften op het gebied van naleving en gegevensbeveiliging.[2] Deze strategie kan echter prijzig en complex in het beheer zijn, met het risico dat er nog steeds tekortkomingen voorkomen. Een holistische benadering van gegevensbeveiliging is essentieel.

Dat is waar Microsoft Purview-oplossingen voor gegevensbeveiliging kunnen helpen.

83%
van de organisaties maken in hun leven meer dan één data lek mee[3]

44%
toename van door insiders geleide cyberbeveiligingsinciden ten sinds 2020[4]

15,4 miljoen USD
gemiddelde kosten van activiteiten om interne bedreigingen op te lossen over een periode van 12 maanden[3]

1. Tech Jury, Hoeveel gegevens worden er dagelijks aangemaakt in 2023?, februari 2023
2. Onderzoek van februari 2022 onder 200 Amerikaanse besluitvormers over naleving in opdracht van Microsoft en MDC Research
3. IBM, 'Kosten van een datalek rapport,' 2022
4. Proofpoint, 'Bedreigingen van insiders nemen (nog steeds) toe: Ponemon rapport 2022,' 25 januari 2022.

INTRODUCTIE VAN MICROSOFT PURVIEW

Om de uitdagingen op het gebied van gegevensbeveiliging aan te gaan, moeten organisaties meerdere controles implementeren. Deze controles omvatten het voorkomen van ongeoorloofd gebruik van gegevens in verschillende werkbelastingen, het beveiligen van gevoelige gegevens, waar ze zich ook bevinden gedurende hun levenscyclus, en het begrijpen van de context van gebruikersactiviteiten rond de gegevens.

Microsoft Purview levert de verschillende besturingselementen die je nodig hebt om een uitgebreide oplossing voor gegevensbeveiliging te creëren waarmee je jouw gegevensrisico's beter kunt begrijpen en beperken. Als onderdeel van de oplossing kun je eenvoudig een holistische, actuele kaart van jouw gegevensdomein maken met geautomatiseerde gegevensdetectie, classificatie van gevoelige gegevens en end-to-end gegevensherkomst. Microsoft Purview is beschikbaar als één platform en helpt je jouw gegevensbeveiliging effectief te versterken, zodat jij eenvoudiger een diepgaande aanpak kunt ontwikkelen voor de beveiliging van jouw gevoelige gegevens, ongeacht waar deze zich bevinden.

Bescherm gevoelige gegevens met Microsoft Purview Information Protection, dat inzicht biedt in waar jouw gegevens zich bevinden, gevoelige informatie classificeert via uitgebreide labeling en ingebouwde versleuteling toepast om jouw gegevens te beschermen.

Voorkom gegevensverlies met Microsoft Purview preventie van gegevensverlies, dat controles biedt om gegevensverlies of ongeoorloofd gebruik van die gegevens, zoals onjuist opslaan, opslaan of afdrukken, te voorkomen.

Beheer insider-risico's met Microsoft Purview intern risicobeheer, dat gebruikerscontext rond gegevens biedt en ingebouwde, gebruiksklare modellen voor machine learning toepast om de meest kritieke risico's voor gegevensbeveiliging rond die gegevens te detecteren en te beperken.

Waar komen incidenten met gegevensbeveiliging vandaan?

Over het algemeen veroorzaken gebruikers incidenten met gegevensbeveiliging. Soms is de bedoeling kwaadaardig; diefstal van gegevens en IP door vertrekkende werknemers is helaas niet ongewoon. Andere keren is het onbedoelde blootstelling. Een werknemer kan bijvoorbeeld per ongeluk een document naar de verkeerde persoon sturen of het onbeveiligd achterlaten.

Maar ongeacht wanneer en hoe die gegevens zijn blootgesteld, is het grotere probleem dat de meeste organisaties geen zicht hebben op hoe hun gegevens worden gebruikt en benaderd. En zonder zichtbaarheid weet je gewoon niet wat jouw risico is.

BESCHERM GEVOELIGE GEGEVENS MET MICROSOFT PURVIEW INFORMATION PROTECTION

De allereerste stap bij het beveiligen van gegevens is begrijpen en ontdekken waar ze zich in jouw organisatie bevinden. Daarom heb je een oplossing nodig die je inzicht geeft in jouw hele gegevensdomein, of dat nu on-premises, in de cloud, hybride of multi-cloud is.

Met Microsoft Purview Information Protection kun je al jouw gegevens vanaf één locatie bekijken en beheren, inclusief het volume, het type en de locatie van vertrouwelijke informatie. Van hieruit kun je jouw gegevens eenvoudig classificeren en labelen en besturingselementen toepassen zoals versleuteling, toegangsbeheer en meer.

Microsoft Purview Information Protection helpt ook bij het beveiligen van gegevens gedurende de hele levenscyclus, met persistente labeling en versleuteling ingebouwd in productiviteitstools. En dat is nog niet alles; omdat organisaties gegevens moeten beschermen op plekken waar mensen vanuit meerdere omgevingen werken, worden de zichtbaarheid en bescherming van gevoelige informatie uitgebreid over jouw gehele gegevensdomein, of deze nu on-premises, hybride of cloud is.

Microsoft Purview Information Protection helpt gevoelige gegevens te beschermen

- Ontdek en classificeer gegevens op schaal met behulp van automatisering en machine learning.
- Bescherm gegevens gedurende hun hele levenscyclus met labeling en versleuteling ingebouwd in productiviteitstools.
- Breid de bescherming uit naar andere omgevingen om gegevens te beschermen, waar ze zich ook bevinden.

VOORKOM GEGEVENSVERLIES MET MICROSOFT PURVIEW

PREVENTIE VAN GEGEVENSVERLIES

Mensen werken op afstand. Teams werken nationaal en internationaal samen.
De gemiddelde werknemer gebruikt niet alleen een computer, maar ook mobiele apparaten. Ze werken ook met verschillende apps, in hybride modellen. Kortom, jouw gegevens zijn overal.

Daarom is het noodzakelijk om informatie voorbij het documentniveau te beveiligen door ervoor te zorgen dat al jouw uitgaande kanalen exfiltratie en ongeoorloofd gebruik voorkomen. Maar het is ook belangrijk om gegevens niet te veel af te sluiten, want de productiviteit daalt als gebruikers geen toegang hebben tot de gegevens die ze nodig hebben. Hoe los je deze uitdagingen op? Invoeren Microsoft Purview preventie van gegevensverlies (DLP).

Deze allesomvattende oplossing werkt met de verschillende toepassingen, services en apparaten waar gevoelige gegevens worden opgeslagen, gebruikt of gedeeld, of het nu gaat om Microsoft-systeemeigen platforms of niet-Microsoft services en -apps. Omdat Microsoft Purview DLP cloudeigen is, hoef je geen dure on-premises infrastructuur of agenten te installeren. Bovendien kan het helpen kosten te besparen, omdat je de verschillende oplossingen die je vandaag hebt, kunt consolideren.

Microsoft Purview preventie van gegevensverlies (DLP) helpt gegevensverlies te voorkomen

- Elimineer de noodzaak van on-premises infrastructuur en agenten met een cloudeigen oplossing die bescherming inbouwt in Microsoft 365-apps, -services en Windows-eindpunten.
- Breng bescherming en productiviteit in balans met gedetailleerde beleidscontroles en beheer alle werkbelastingen vanaf één locatie.
- Kies voor een geïntegreerde benadering van gegevens door gebruik te maken van systeemeigen integratie met gegevensclassificatie, inzicht in gebruikersactiviteiten en beheer van beveiligingsincidenten.

BEHEER INSIDER-RISICO'S MET MICROSOFT PURVIEW INTERN RISICOBEHEER

Gegevens verplaatsen zichzelf niet; mensen verplaatsen gegevens. Met andere woorden, datalekken worden meestal veroorzaakt door interne actoren, of het nu gaat om vertrekkende werknemers die gegevens exfiltreren, kwaadwillige gegevensdiefstal of onopzettelijke overmatige blootstelling.

De sleutel is begrijpen hoe en waarom mensen toegang krijgen tot gegevens; als je de context begrijpt, kun je de potentiële risico's voor gegevensbeveiliging en risicovolle gebruikersactiviteiten identificeren die tot incidenten kunnen leiden. Organisaties hebben een holistische aanpak nodig voor het beheren van insider-risico's door de juiste mensen, processen, training en hulpmiddelen samen te brengen.

Microsoft Purview intern risicobeheer correleert verschillende signalen om potentiële kwaadwillende of onopzettelijke insider-risico's te identificeren. Deze risico's omvatten IP-diefstal, gegevenslekken en beveiligingsschendingen. intern risicobeheer stelt klanten ook in staat om beleidsregels op te stellen voor het beheer van beveiliging en naleving. Gebouwd volgens de principes van privacy-by-design, worden gebruikers standaard gepseudonimiseerd en zijn er op rollen gebaseerd toegangsbeheer en auditlogboeken om privacy op gebruikersniveau te helpen garanderen.

Microsoft Purview intern risicobeheer helpt bij het detecteren en beperken van risico's voor gegevensbeveiliging

- Zet privacy op de eerste plaats door het vertrouwen van gebruikers te beschermen en een holistisch insider-risicoprogramma op te zetten met pseudonimisering en sterke privacy controles.
- Vereenvoudig gegevensbeveiliging door verborgen risico's te identificeren met meer dan 100 ingebouwde en kant-en-klare machine-learning-modellen en indicatoren, waarvoor geen eindpuntagents nodig zijn.
- Versnel mitigatie en handel deze sneller af met verrijkte onderzoeken en Adaptieve bescherming waarmee effectieve controles dynamisch worden afgedwongen.

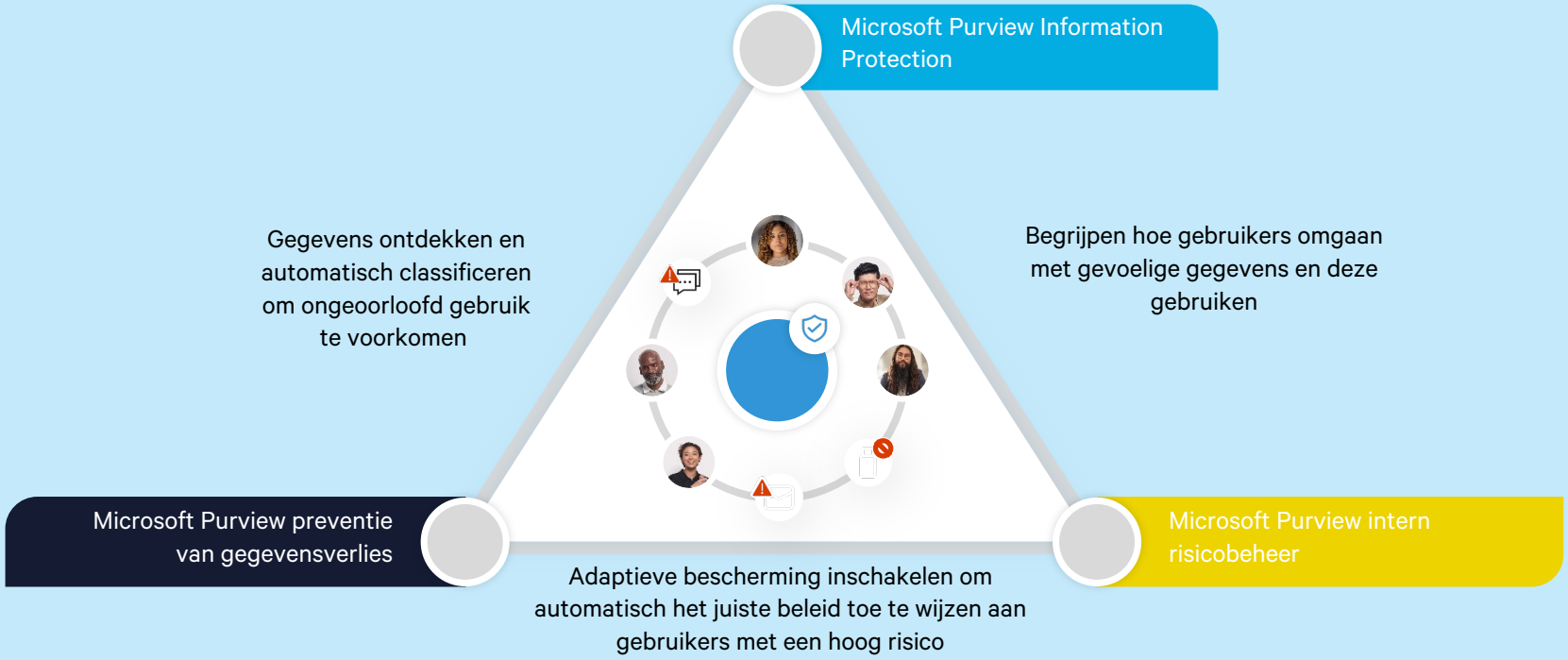
VERSTERK UW GEGEVENSBEVEILIGING MET EEN GEÏNTEGREERDE AANPAK

Microsoft Purview versterkt de gegevensbeveiliging door informatiebescherming, intern risicobeheer en preventie van gegevensverlies aan te bieden in één uniform platform. Deze drie verschillende beschermingslagen helpen niet alleen om gegevens te beveiligen tegen mogelijke incidenten met gegevensbeveiliging, ze werken ook samen als één platform om jouw gegevensbeveiliging te versterken.

Bekijk het op deze manier. Als je Information Protection en preventie van gegevensverlies samen gebruikt, kun je gegevens ontdekken en automatisch classificeren om ongeoorloofd gebruik te voorkomen.

Op dezelfde manier helpt Information Protection en intern risicobeheer je inzicht te krijgen in de gebruikersintentie rond gevoelige gegevens om de meest kritieke gegevensrisico's in jouw organisatie te identificeren.

Als u intern risicobeheer en preventie van gegevensverlies gebruikt, kun je wat wij noemen 'Adaptieve bescherming' inschakelen, waarmee passend DLP-beleid wordt toegewezen op basis van het risiconiveau van de gebruiker. Met Adaptieve bescherming kun je begrijpen in welke context gebruikers informatie opvragen en hoe ze ermee omgaan. Vervolgens kun je de juiste risiconiveaus berekenen en toewijzen, en automatisch de juiste DLP-controles aanpassen op basis van de risiconiveaus van een gebruiker. Als je ze allemaal samenvoegt, helpt Microsoft Purview jou om jouw gegevens beter te beveiligen.



WEES DATABEVEILIGINGSINCIDENTEN VOOR MET ADAPTIEVE BESCHERMING

In de moderne werkomgeving is het risico op gegevensbeveiliging dynamisch. Het type inhoud verandert, net zoals de mensen die met die gegevens omgaan veranderen. Wat mensen met gegevens doen verandert ook. Dat betekent dat gegevensbeveiliging nog ingewikkelder is om te beheren. Helaas werken brede, statische beleidsregels niet meer; aan de ene kant lopen ze het risico dat ze niets doen en aan de andere kant kunnen ze gegevens zodanig te veel beschermen dat mensen helemaal niets gedaan kunnen krijgen. Maar al te vaak moeten beheerders handmatig het bereik van beleidsregels aanpassen en waarschuwingen aanpassen om kritieke risico's te identificeren.

Adaptieve preventie helpt deze problemen op te lossen door jou te helpen de meest kritieke risico's dynamisch aan te pakken. Met Adaptieve preventie detecteert en vermindert Machine Learning-analyse voortdurend de meest kritieke risico's voor zowel inhoud als gebruikers. Het helpt je een beter inzicht te krijgen in risico's door intern risicobeheer te gebruiken om gegevens en gebruikers te classificeren, de inhoud van gebruikers te begrijpen en inzicht te krijgen in hoe die gegevens gebruikt gaan worden.

Vervolgens past Adaptieve bescherming automatisch het juiste niveau van risicobeperkende controles aan op basis van de gedetecteerde risico's. Gebruikers met een hoog risico kunnen bijvoorbeeld onder een strengere controle vallen, terwijl gebruikers met een laag risico gewoon kunnen werken. En het past zich voortdurend aan; de controle kan omhoog en omlaag worden gedraaid als het risiconiveau van de gebruiker verandert.

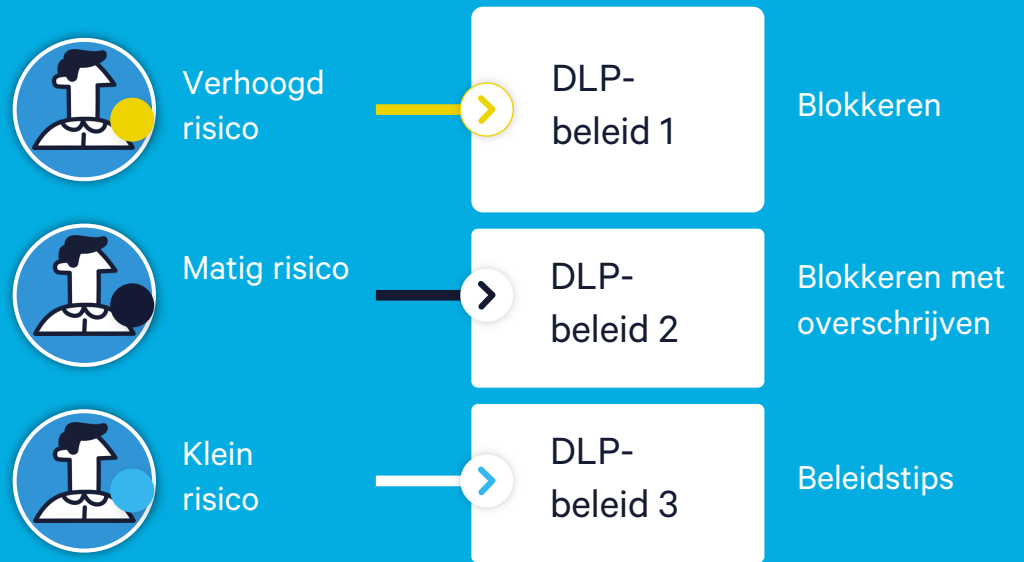
Als gevolg hiervan helpt Adaptieve bescherming niet alleen de werkbelasting van het beveiligingsteam te verminderen, maar maakt het DLP ook effectiever door het beleid voortdurend te optimaliseren.

Intern risicobeheer

Riskante gebruikers opsporen en risiconiveaus toekennen

Preventie van gegevensverlies

Dynamisch preventieve controles toepassen



VERSTERK JOUW GEGEVENSBEVEILIGING VANDAAG NOG!

In vandaag de dag zijn er geen geografische grenzen voor gevoelige gegevens; ze reizen via mensen, plaatsen en apparaten over de hele wereld. De sleutel tot gegevensbeveiliging is het beveiligen van die gegevens, waar ze ook naartoe gaan. Microsoft Purview kan je helpen een gegevensbeveiligingsstrategie op te stellen voor de wereldwijde, samenwerkende bedrijfsomgeving van vandaag. Het is eenvoudig om aan de slag te gaan met ingebouwde bescherming. Het is volledig geïntegreerd voor beheer en veilige samenwerking. En het is intelligent, zodat jij jouw gegevensbeveiliging kunt automatiseren.

Is het niet tijd om jouw gegevens te beveiligen?
Neem contact met ons op voor meer details.

Edwin.degoede@indito.nl
Michael.groenenberg@indito.nl

INDITO.