Purview op Orde

Weten wat gevoelig is.
Beschermen wat belangrijk is.

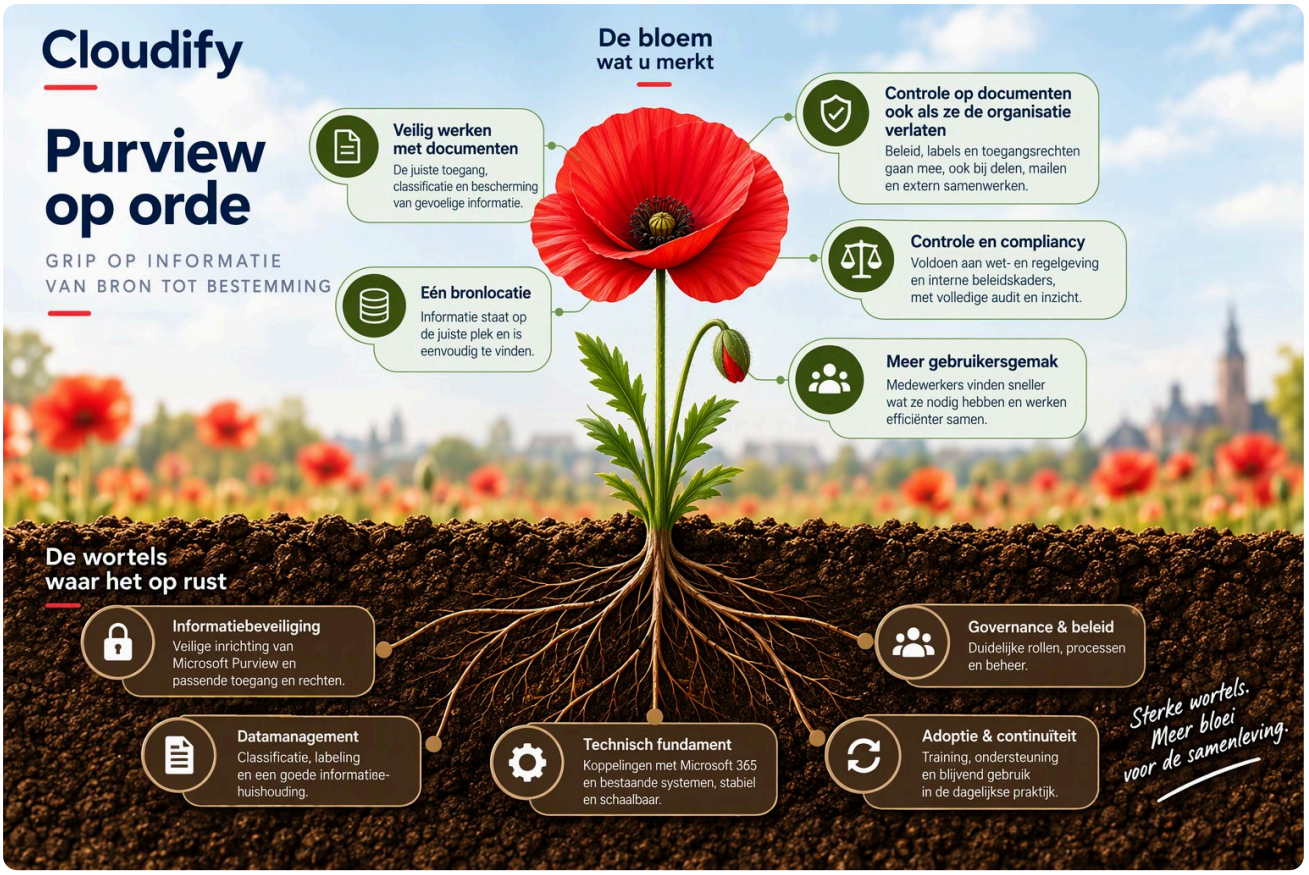
Eén verkeerde handeling is genoeg.

Een medewerker mailt een bestand naar buiten. Niets bijzonders. Het gebeurt honderden keren per dag. Alleen bevat dit bestand persoonsgegevens. Een ander document staat in een Teams-omgeving waar inmiddels veel meer mensen toegang toe hebben dan ooit de bedoeling was. En ergens staat een vertrouwelijk directiestuk zonder label tussen duizenden gewone documenten. Zolang niemand ernaar zoekt, lijkt er weinig aan de hand. Totdat informatie sneller gaat bewegen, AI gemakkelijker kan zoeken en delen, en één verkeerde handeling voldoende is.
Dan wordt zichtbaar wat eigenlijk altijd al het probleem was: u kunt pas echt grip hebben op informatie als u weet wat gevoelig is en daar bescherming aan kunt verbinden.

Met Purview op Orde brengt Cloudify informatiebescherming van beleid naar dagelijkse praktijk. We onderzoeken waar gevoelige informatie en risico’s zitten, ontwerpen een begrijpelijk classificatie- en labelmodel, configureren de afgesproken beschermingsmaatregelen in Microsoft Purview, testen die gecontroleerd en begeleiden vervolgens de uitrol en adoptie.

Informatie onder controle.

Vandaag veilig, morgen klaar voor AI.



Wat levert dat op?

01

Zicht op gevoelige informatie

Weten waar informatie met een hoger beschermingsniveau zit en waar de belangrijkste risico's liggen.

02

Herkenbare classificatie

Een labelmodel dat begrijpelijk is voor medewerkers én technisch toepasbaar is.

03

Bescherming in de werkstroom

Afspraken en policies die informatie helpen beschermen zonder het dagelijkse werk onnodig te blokkeren.

04

Getest vóór brede uitrol

Eerst valideren en tunen met een pilotgroep, daarna gecontroleerd opschalen.

05

Medewerkers die het begrijpen

Communicatie en ondersteuning maken duidelijk wat labels en waarschuwingen betekenen.

06

Blijvend eigenaarschap

Rollen en beheerafspraken zorgen dat de inrichting na livegang onderhoudbaar blijft.

Het resultaat is niet alleen een ingerichte securitytool. U weet waar gevoelige informatie zit, medewerkers herkennen hoe ze ermee moeten omgaan en technische maatregelen helpen voorkomen dat informatie terechtkomt waar deze niet bedoeld is.

Van informatie hebben naar informatie begrijpen

De meeste organisaties hebben geen tekort aan securitybeleid. De uitdaging begint een stap eerder: welke informatie is gevoelig, waar bevindt die zich, wie heeft er toegang toe en welke bescherming past daarbij zonder het dagelijkse werk onnodig ingewikkeld te maken?

Daarom beginnen we niet met twintig labels en honderd technische policies.

We beginnen met het begrijpen van de informatie. Van daaruit bouwen we een model dat werkbaar is voor:

De medewerker	die gewoon het werk wil doen
De business	die eigenaar is van informatie
IT & Security	die de informatie beheersbaar moeten beschermen

Onze aanpak in vijf stappen

01	**Assess**	Nulmeting van Microsoft 365, bestaande informatiebescherming en relevante blootstellingsrisico's. **Resultaat: een heldere baseline en geprioriteerde aandachtspunten.**
02	**Design**	Ontwerp van een eenvoudige, businessgerichte classificatie- en labeltaxonomie en de afgesproken beschermingspolicies. **Resultaat: een gedragen en implementeerbaar ontwerp.**
03	**Deploy & Test**	Configuratie van labels en afgesproken policies, gevolgd door gecontroleerde validatie en tuning met een pilotgroep. **Resultaat: een technisch werkende inrichting die in praktijkscenario's is getest.**
04	**Rollout**	Gefaseerde activering in de productieomgeving, met monitoring en bijsturing. **Resultaat: informatiebescherming die daadwerkelijk landt in het dagelijkse werk.**
05	**Adopt & Govern**	Communicatie, ondersteuning en duidelijke afspraken over eigenaarschap, beheer, uitzonderingen en wijzigingen. **Resultaat: een capability die de organisatie zelf kan blijven onderhouden en verbeteren.**

Wat leveren we concreet op?

DELIVERABLE	WAT HEEFT U ERAAN?
Data Security & Tenant Assessment	Inzicht in de huidige informatiebescherming, blootstelling en belangrijkste risico's
Risico- en prioriteitenbeeld	Duidelijkheid over wat eerst moet worden aangepakt
Classificatie- & labeltaxonomie	Een begrijpelijk model waarmee informatie herkenbaar kan worden beschermd
Purview-design	Vastgelegde keuzes voor de afgesproken Information Protection- en DLP-scope
Geconfigureerde & geteste policies	Bescherming die technisch werkt en in praktijkscenario's is gevalideerd
Pilot & tuning	Minder verrassingen en onnodige verstoring bij bredere uitrol
Adoptie- & communicatiemiddelen	Medewerkers begrijpen wat verandert en wat van hen wordt verwacht
Governance & eigenaarschap	Duidelijkheid over beheer, wijzigingen, uitzonderingen en verantwoordelijkheden

Security die AI mogelijk maakt

AI maakt informatie eenvoudiger vindbaar en bruikbaar. Daardoor wordt een goed ingerichte informatiebescherming belangrijker, niet minder belangrijk.

Purview op Orde past daarom in een bredere Cloudify-productlijn. AI Basis op Orde laat zien waar het fundament aandacht nodig heeft. Purview op Orde brengt informatiebescherming daadwerkelijk in positie. Vanuit die basis kan de organisatie verder met adoptie, use cases en concrete AI-producten.

DE CLOUDIFY-PRODUCTLIJN

01 · FUNDAMENT	02 · BESCHERMEN	03 · ADOPTEREN	04 · WAARDE REALISEREN
AI Basis op Orde	**Purview op Orde**	AI-Kompas	AI Igniter

We beschermen informatie niet om haar stil te zetten. We beschermen haar zodat de organisatie ermee vooruit kan.

cloudify.