




To get there, together



Event Hou grip op uw documenten met Azure Information Protection

<https://www.realdolmen.com/nl/webinar-azure-information-protection>



 Print this page



 woensdag 18 November 2020

 11.00-11.45

 Online

WELKOM:

MIJN NAAM IS WIM VAN CLAPDURP
IK WERK BIJ REALDOLMEN ALS M365
CONSULTANT



HOU GRIP OP UW DOCUMENTEN MET AZURE INFORMATION PROTECTION

AGENDA:

SENSITIVITY LABELS

DATA LOSS PREVENTION

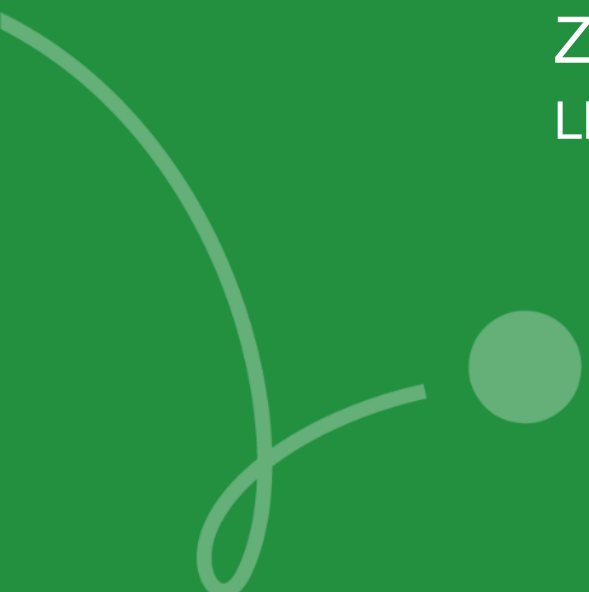
CLOUD APP SECURITY

LIFE CYCLE OF A SENSITIVE FILE

SENSITIVITY LABELS:

BEVEILIG E-MAILS, DOCUMENTEN EN GEVOELIGE GEGEVENS DIE GEDEELD WORDEN BUITEN UW BEDRIJF OF ORGANISATIE MET BEHULP VAN SENSITIVITY LABELS.

ZO KUNNEN ENKEL BEVOEGDE PERSONEN BESTANDEN OPENEN OF LEZEN.



Wat is Microsoft Azure Information Protection?

Is een Cloud gebaseerde oplossing waarmee organisaties documenten en e-mails kunnen classificeren en beschermen door **labels** toe te passen

Controleer en beveilig e-mails, documenten en gevoelige gegevens die buiten het bedrijf worden gedeeld. Van eenvoudige classificatie tot ingesloten **labels** en **machtigingen**: verbeter de gegevensbescherming wanneer u maar wilt met Azure Information Protection, waar de gegevens ook zijn opgeslagen en met wie ze ook worden gedeeld.

Licentie nodig voor Azure Information Protection

EMS E3 of E5	M365 E3 of E5
AAD P1 of P2	AIP voor O365



Wat is een Sensitivity label?

Aan een document of e-mail zal een waarde toegevoegd worden, een LABEL.
Dit label gaat overal waar het document heengaat mee. Het is onlosmakelijk
Van het document.

Hierdoor kunnen rechten op bestanden worden toegevoegd en acties.



Hoe ziet een sensitivity label eruit?

The screenshot shows the Office 365 Security & Compliance portal in a browser. The URL is `protection.office.com/sensitivity?viewid=sensitivitylabels`. The left navigation pane includes: Home, Alerts, Permissions, Classification (expanded), Sensitivity labels (selected), Retention labels, Sensitive info types, Data loss prevention, and Records management. The main content area shows the 'Labels' section with a description: 'Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)'. Below the text are buttons for '+ Create a label', 'Publish labels', and 'Refresh'. A table lists the following sensitivity labels:

Name	Order	Created by	Last modified
Personal	0 - lowest	Global Admin	03/10/2020
Public	1	Global Admin	03/10/2020
General	2	Global Admin	03/28/2020
Confidential	3	Global Admin	03/12/2020
Recipients Only	4	Global Admin	03/10/2020
All Employees	5	Global Admin	03/12/2020

Wat is AIP

Azure Information Protection



Data classification

Het proces om data te classificeren afhankelijk van sensitieve/algemene informatie in een document of E-mail

Rights management services.

Het afdwingen van respectievelijke toestemming op een document, afhankelijk van de classificatie die is gebruikt.





Azure information protection

Data classificatie Service

Data classification

Het proces om data te classificeren afhankelijk van sensitieve/algemene informatie in een document of E-mail





Azure information protection

Rights management Service



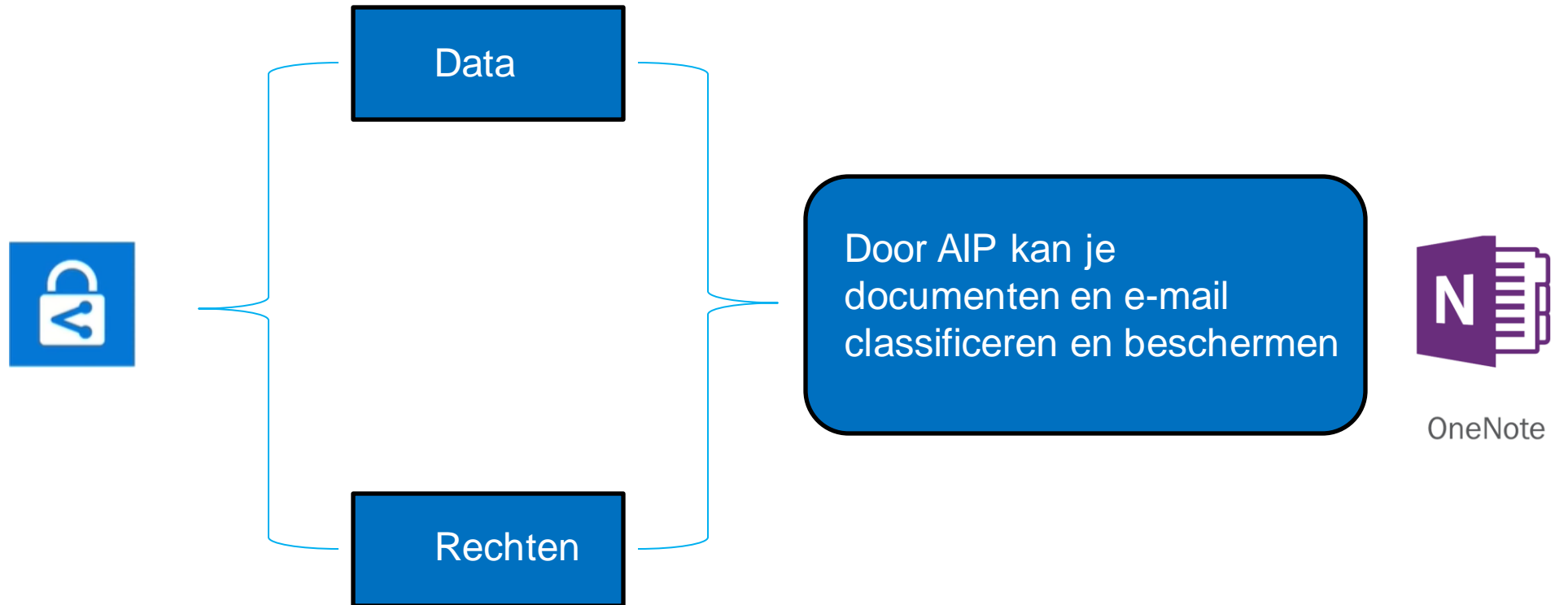
Rights management services.

Het afdwingen van respectievelijke toestemming op een document, afhankelijk van de classificatie die is gebruikt.




Azure information protection

Data Label



LIVE DEMO AIP LABEL





Poll: Heeft jouw organisatie reeds formeel een beleid om documenten te classificeren op basis van gevoeligheid?

DATA LOSS PREVENTION :

VOORKOM HET (ON)BEDOELD DELEN VAN GEVOELIGE INFORMATIE.

WIST U DAT U ELK DOCUMENT OF E-MAILBERICHT MET BVB. EEN GEZONDHEIDSDOSSIER, DAT GEDEELD WORDT MET MENSEN BUITEN UW ORGANISATIE, GEÏDENTIFICEERD KAN WORDEN EN VERVOLGENS AUTOMATISCH DE TOEGANG TOT DAT DOCUMENT GEBLOKKEERD KAN WORDEN?

DLP Data Loss Prevention

DLP zorgt ervoor dat data niet accidenteel naar buiten gestuurd kan worden.

Identificeer gevoelige informatie over verschillende locaties, zoals Exchange online, Sharepoint Online, OneDrive en Microsoft Teams.

Monitor en bescherm gevoelige informatie in de desktop versie van Excel en Powerpoint en Word.

Licentie nodig voor DLP

EOP P2	Office 365 E3 of E5
M365 E3 of E5	

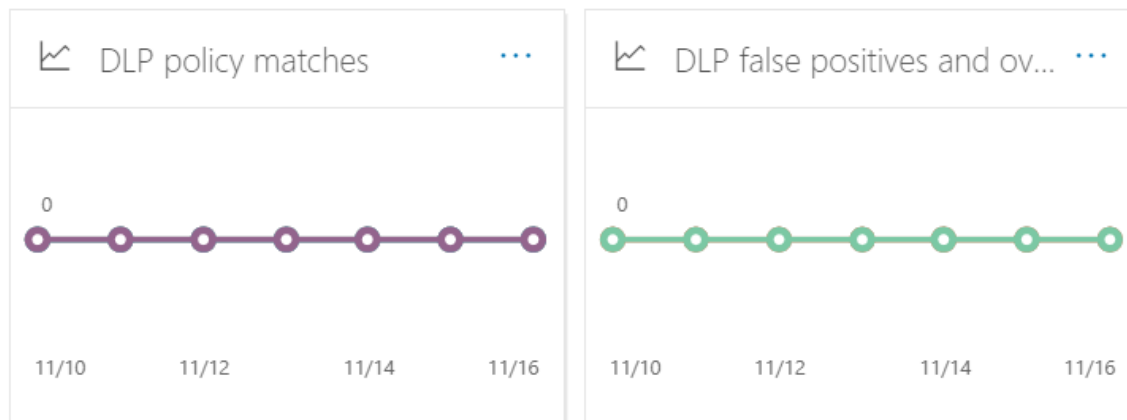


DLP DASHBOARD

[Home](#) > Data loss prevention

Good news! Data loss prevention is now available as a solution in the [Microsoft 365 compliance center](#). We recommend using redirected automatically, but get a head start by [trying it out now](#).

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up p wrong people. [Learn more about DLP](#)



[+ Create a policy](#) [Refresh](#)

<input checked="" type="checkbox"/>	Name	Order [^]	Modified date
<input checked="" type="checkbox"/>	General Data Protection Regulation (GDPR)	0	November 17, 2020
<input checked="" type="checkbox"/>	PCI Data Security Standard (PCI DSS)	1	November 17, 2020



Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later.

[Learn more about DLP policy templates](#)

Show options for

42 results



Financial



Medical and health



Privacy



Custom

Custom policy

Custom policy

Description

Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.



Choose the types of content to protect

This policy will protect content that matches these requirements. You can choose sensitive info types and existing labels.

Content contains *

Any of these ▼

Sensitive info type

Medische termen

Add ▼

Match accuracy

min max

60 100

+ Add group

Find content that contains: ⓘ

Medische termen

Edit

Detect when this content is shared:

with people outside my organization ▼

Use advanced settings ⓘ

Back

Next

Cancel



What do you want to do if we detect sensitive info?

We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?

Notify users when content matches the policy settings

- Show policy tips to users and send them an email notification.

Tips appear to users in their apps (Outlook, OneDrive, SharePoint, and Teams) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)

[Customize the tip and email](#)

Detect when a specific amount of sensitive info is being shared at one time

- Detect when content that's being shared contains:

At least instances of the same sensitive info type.

- Send incident reports in email

By default, you and your global admin will automatically receive the email.

[Click here](#) to change what to include in the report and who receives it

- Restrict access or encrypt the content

- Block people from sharing and restrict access to shared content
- Encrypt email messages (applies only to content in Exchange)

Back

Next

Cancel



Customize access and override permissions



By default, users are blocked from sending email and Teams chats and channel messages that contain the type of content you're protecting. But you can choose who has access to shared SharePoint and OneDrive files. You can also decide if you want to let people override the policy's restrictions.

Block these people from accessing SharePoint, OneDrive, and Teams content

- Everyone [i](#)
- Only people outside your organization [i](#)

Let people who see the tip override the policy

On

- Require a business justification to override
- Override the rule automatically if they report it as a false positive

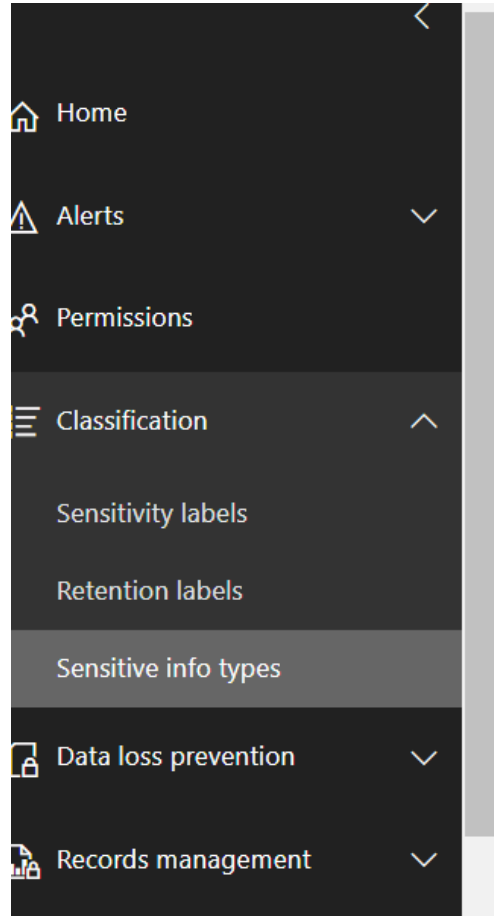
Back

Next

Cancel

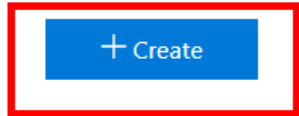


Aanmaken van eigen Sensitive info types:



Home > Sensitive info types

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, span have created.



<input type="checkbox"/> Name	Publisher
<input type="checkbox"/> Medische termen	Engaged Workplace
<input type="checkbox"/> ABA Routing Number	Microsoft Corporation
<input type="checkbox"/> Argentina National Identity (DNI) Number	Microsoft Corporation
<input type="checkbox"/> Australia Bank Account Number	Microsoft Corporation
<input type="checkbox"/> Australia Driver's License Number	Microsoft Corporation
<input type="checkbox"/> Australia Medical Account Number	Microsoft Corporation



Medische termen

Edit

Test type

Delete

Description

Medische termen

Regular expression

Keywords

Pancreas,acuut,anamnes

Dictionary (Large keyw

Matching element

^ Detect content containing

Keywords

Pancreas,acuut,anamnese,anatomie,anesthesie,auscultatie,benigne,biopsie,calor,chronisch,complicatie,congenitaal,conservatieve therapie,constitutie,deficiëntie,diagnose,differentiaal,dolor,drainage,enteraal,exacerbatie,excisie,extirpatie,hematogeen,incisie,incubatietijd,inafaust,indicatie,inspectie,intoxicatie,intracutaan,intramusculair,intraveneus,laesie,laparotomie,lymfogeen,malaise,maligne,medicatie,metastase,morbus,oraal,palpatie,parenteraal,prognose,progressief,prothese,psychisch,psychosomatose,punctie,prik,radiotherapie,recidief,rectaal,remissie,rubor,somatisch,lichamelijk,subcutaan,symptoom,syndroom,profylaxe



LIVE DEMO DLP SCHEEPSWERF/ TRANSPORT FIRMA





Poll: Zou je een DLP policy automatisch laten toepassen?

KRIJG INZICHTEN EN CONTROLE MET
OFFICE 365 ADVANCED SECURITY
MANAGEMENT -> NIEUWE NAAM IS
O365 CLOUD APP SECURITY



Microsoft cloud app security

Cloud app security geeft beheerders de mogelijkheid om alerts of inzichten te krijgen in het gebruik van de gehele Microsoft suite.

Dit kan gaan van bvb wanneer iemand aanmeldt als administrator op een IP adres dat niet corporate is.
Tot users die meer downloaden dan strikt nodig is.
En vele andere inzichten.

Licentie nodig voor Cloud app security

Microsoft Cloud app security (Volledige versie all-in)	Azure AD Cloud app Discovery
EMS E5	EMS E3 of E5
Azure AD Premium P2	Azure AD Premium P1
M365 E5 M365 E5 Security	M365 E3

Verschil met de volledige all-in versie: Hierin zit ook Information Protection en Threat Detection

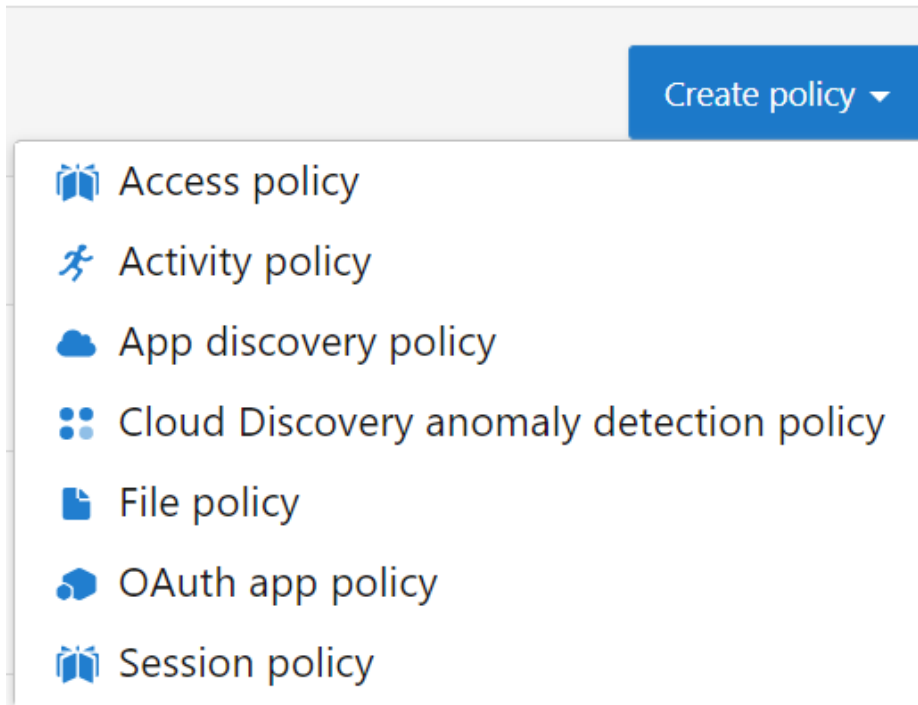
<https://docs.microsoft.com/en-us/cloud-app-security/editions-cloud-app-security-aad#feature-comparison>



Met **Cloud App Security** kan je preventie van gegevensverlies afdwingen, machtigingen en delen beheren, en aangepaste rapporten en waarschuwingen genereren.

In een notendop kan je met CAS inzicht krijgen hoe je data in je omgeving gebruikt wordt en kan je gegevens beschermen.

Create activity policy



Create policy ▾

- Access policy
- Activity policy
- App discovery policy
- Cloud Discovery anomaly detection policy
- File policy
- OAuth app policy
- Session policy



Create activity policy

Policy template *

Mass download by a single user ▾

Policy name *

Mass download by a single user

Policy severity *



Category *

Threat detection ▾

Description

Alert when a single user performs more than 10 downloads within 8 minute.

Create filters for the policy

Act on:

- Single activity
Every activity that matches the filters
- Repeated activity:
Repeated activity by a single user

Minimum repeated activities:

10

Within timeframe:

8

minutes

In a single app

ACTIVITIES MATCHING ALL OF THE FOLLOWING Edit and preview results

- Activity type equals 6 selected
- User From group
- External users as
- IP address Tag
- Microsoft Azure
- User Name
- as Any role

+ (Add filter)

Search: []

- Download document
- Download file
 - FileDownloaded
- Download from Excel
- Download document as odt
- Download folder
 - FileDownloaded
- Download document as pdf



Alerts

- Create an alert for each matching event with the policy's severity

[Save as default settings](#) | [Restore default settings](#)

- Send alert as email ⓘ

security.adm@yourcompany.be x |

- Send alert as text message ⓘ

+32478112233 x

Daily alert limit

5



- Send alerts to Power Automate















[Create a playbook in Power Automate](#)



1 - 2 of 2 Policies

Create policy



Policy	Count	Severity	Category	Action	Modified	
 Administrative activity from a non-corporate IP address Alert when an admin user performs an administrative activity from an IP address that is not included in the corporate I...	1 open alerts		 Threat detection		Nov 17, 2020	  
 Mass download by a single user Alert when a single user performs more than 10 downloads within 8 minute.	0 open alerts		 Threat detection		Nov 17, 2020	  



Cloud App Security: New policy match detected

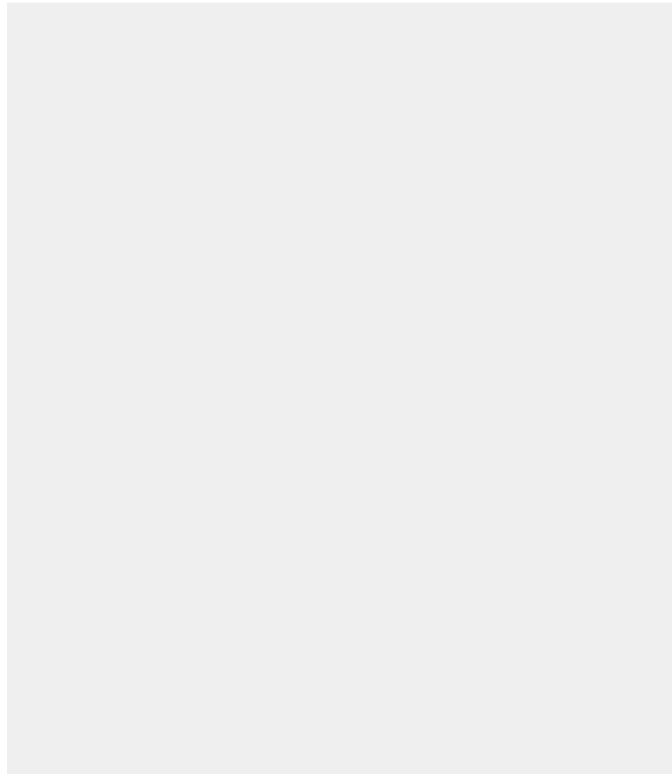


Microsoft Cloud App security <no-reply@cloudappsecurity.com>

To [Redacted]



[If there are problems with how this message is displayed, click here to view it in a web browser.](#)



A new match was detected for your 'Administrative activity from a non-corporate IP address' policy.

Activity: Create activity policy: CAS alert rule **Mass download by a single user**

App: Microsoft Cloud App Security

Client IP address: [Redacted]

Client location: Belgium

Client device: Windows 10

User: Adm [Redacted]
([adm.wim.vanclapdurp@\[Redacted\]onmicrosoft.com](mailto:adm.wim.vanclapdurp@[Redacted]onmicrosoft.com))

Activity time: Tue, 17 Nov 2020 08:49:08 UTC

Alert ID: 5fb38e8fb0703c2f5a08c0b9



LIVE DEMO CLOUD APP SECURITY
[PORTAL.CLOUDAPPSECURITY.COM](https://portal.cloudappsecurity.com)



Poll: Welke policy zou je instellen?



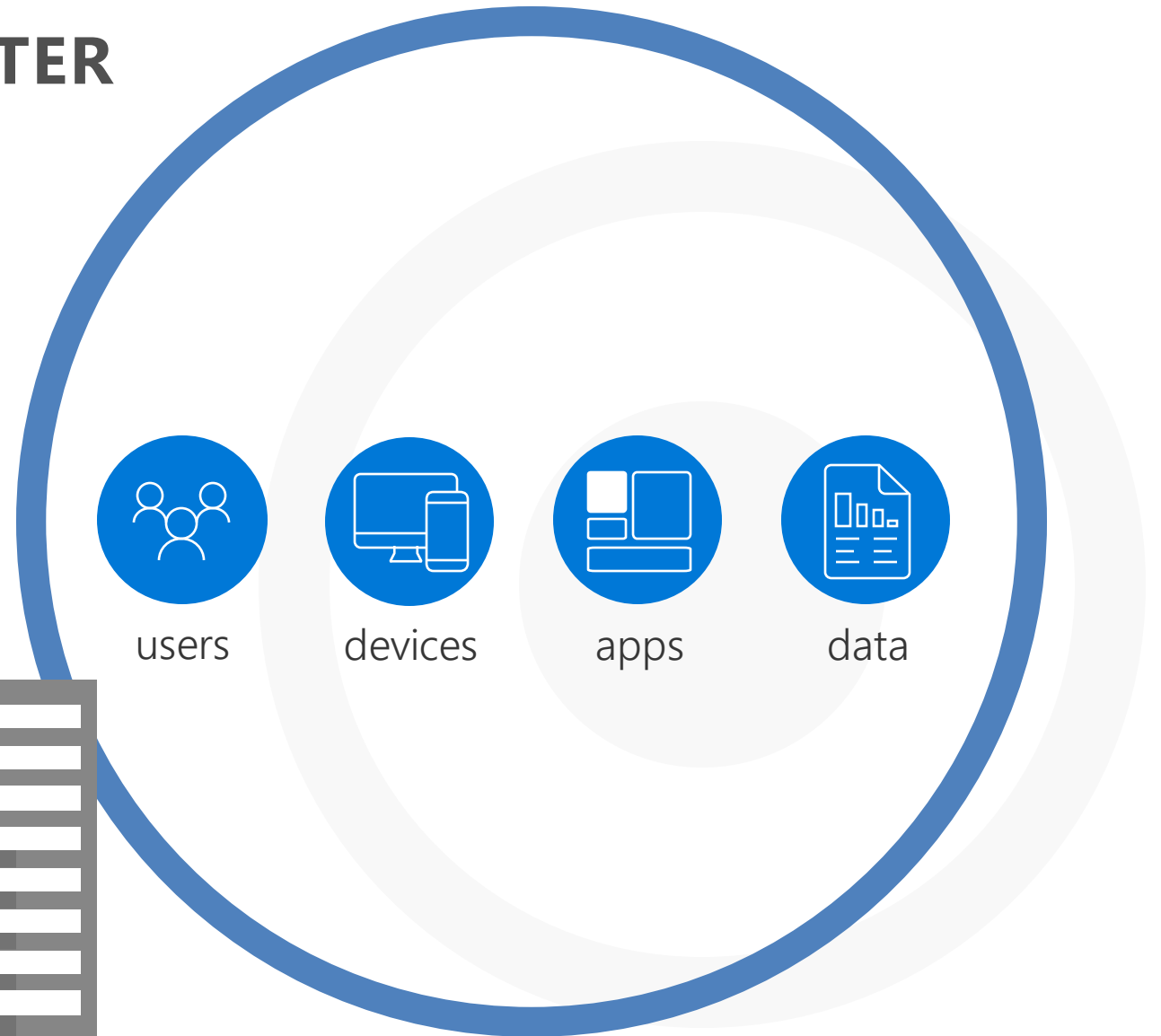
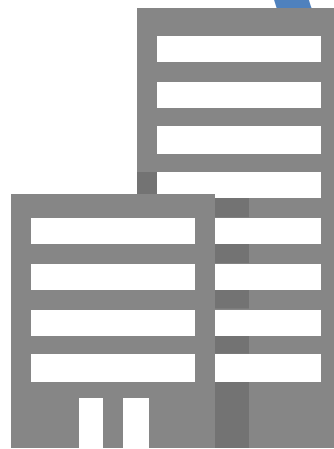
Lifecycle of a sensitive file.

Waar gaan onze files naartoe en wie heeft toegang tot onze bestanden eens ze de organisatie verlaten?

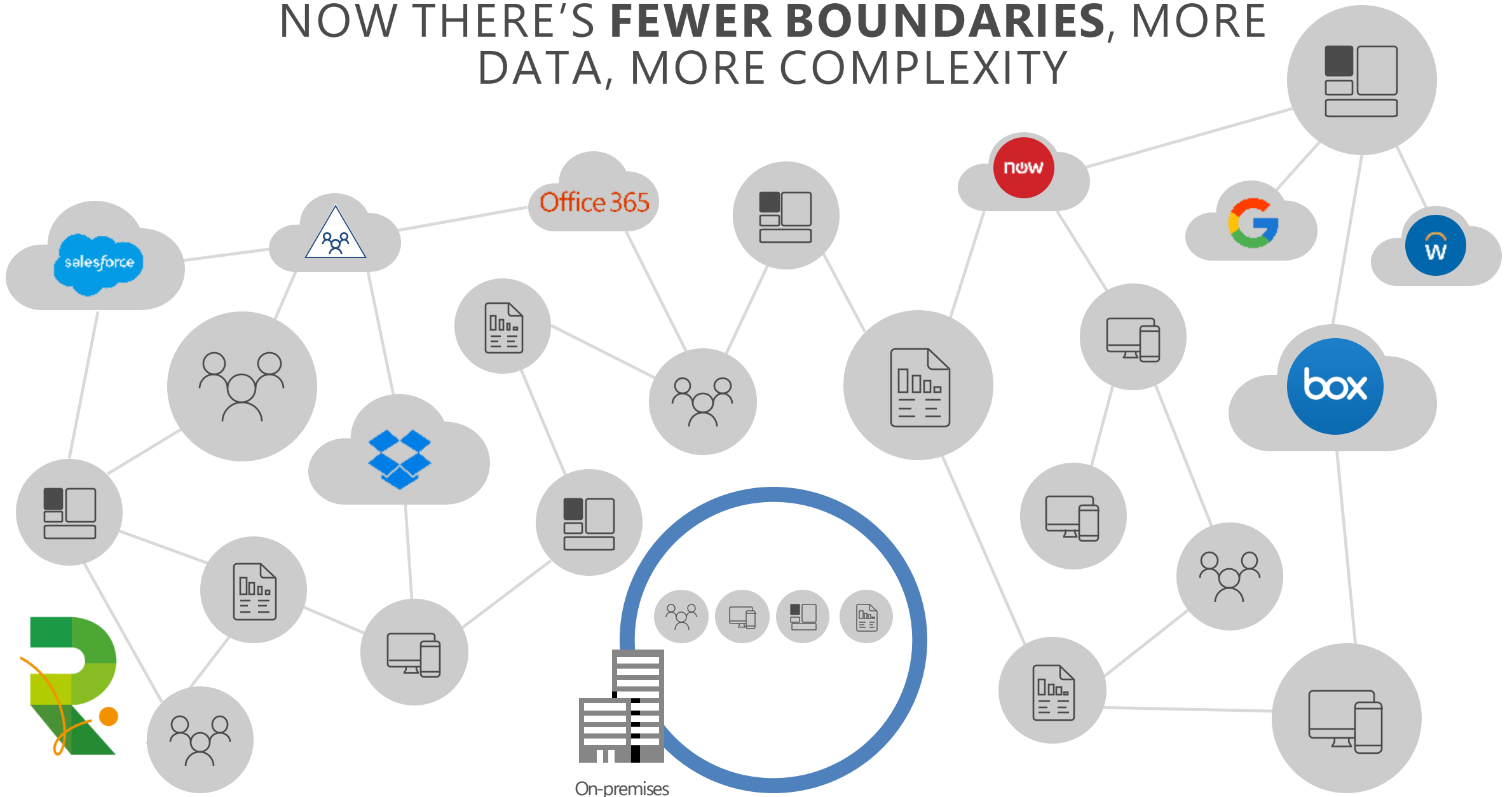
IN THE PAST, THE FIREWALL WAS THE **SECURITY PERIMETER**



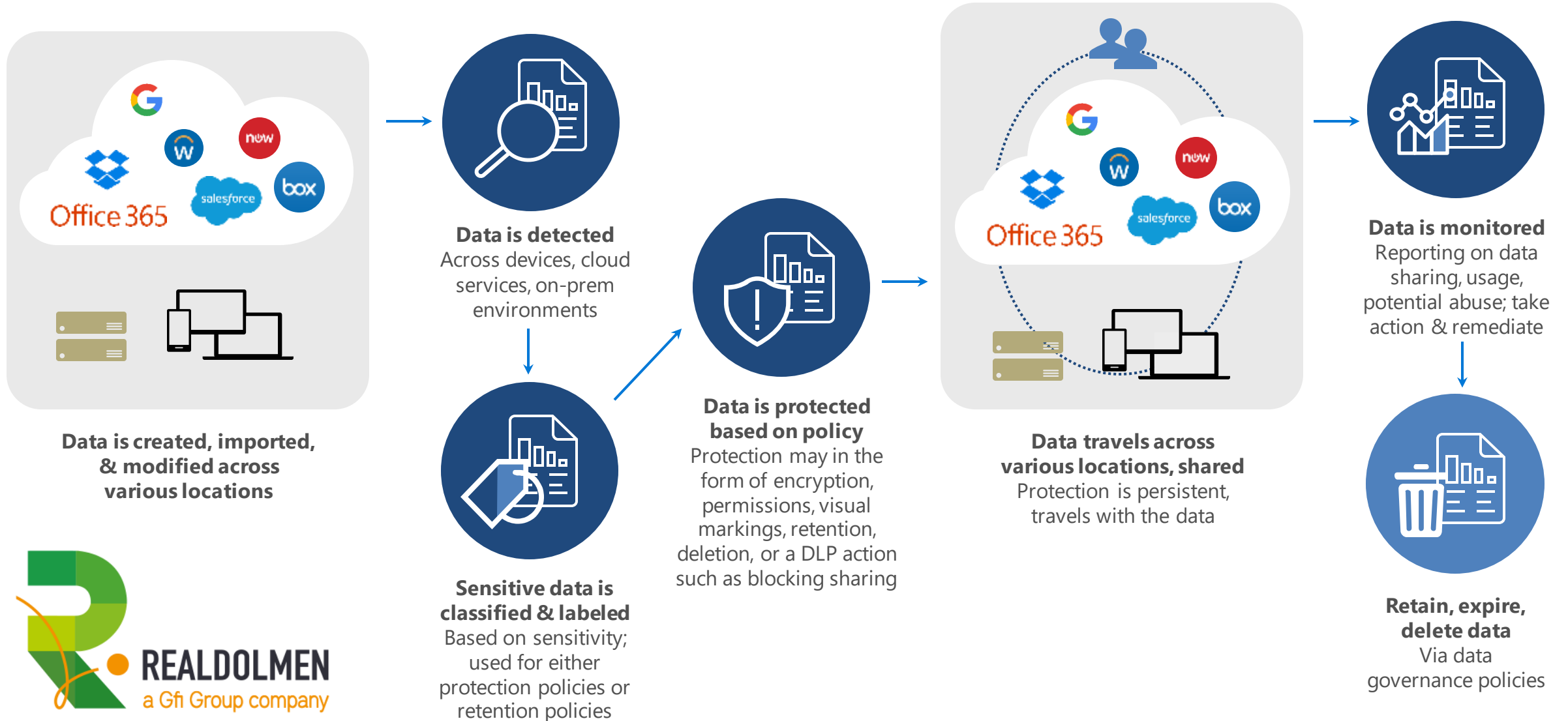
On-premises /
Private cloud

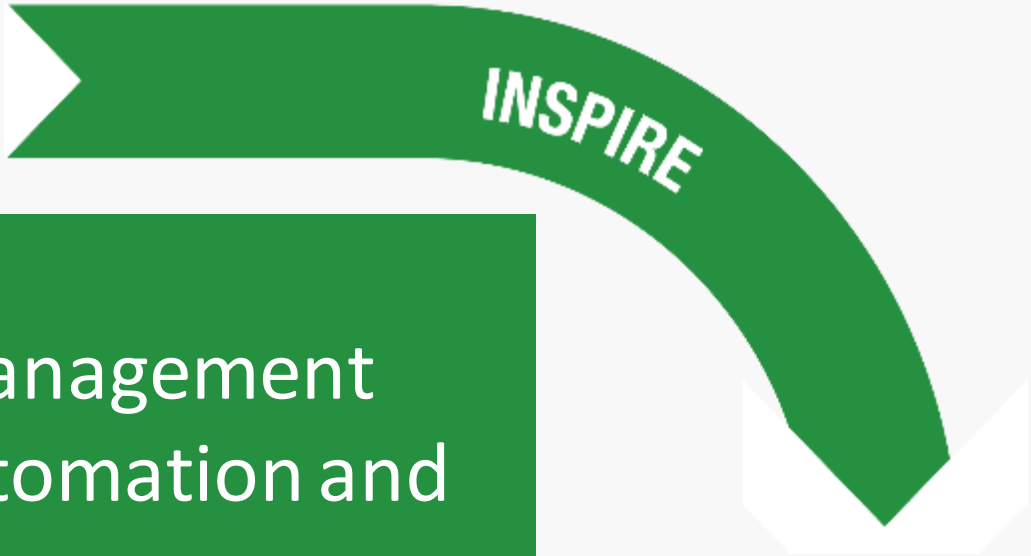


NOW THERE'S **FEWER BOUNDARIES**, MORE DATA, MORE COMPLEXITY



THE LIFECYCLE OF A SENSITIVE FILE





Event


Simplify and Delegate Office 365 Management with Role-Based Access Control, Automation and Hybrid Support


<https://www.realdolmen.com/nl/coreview>



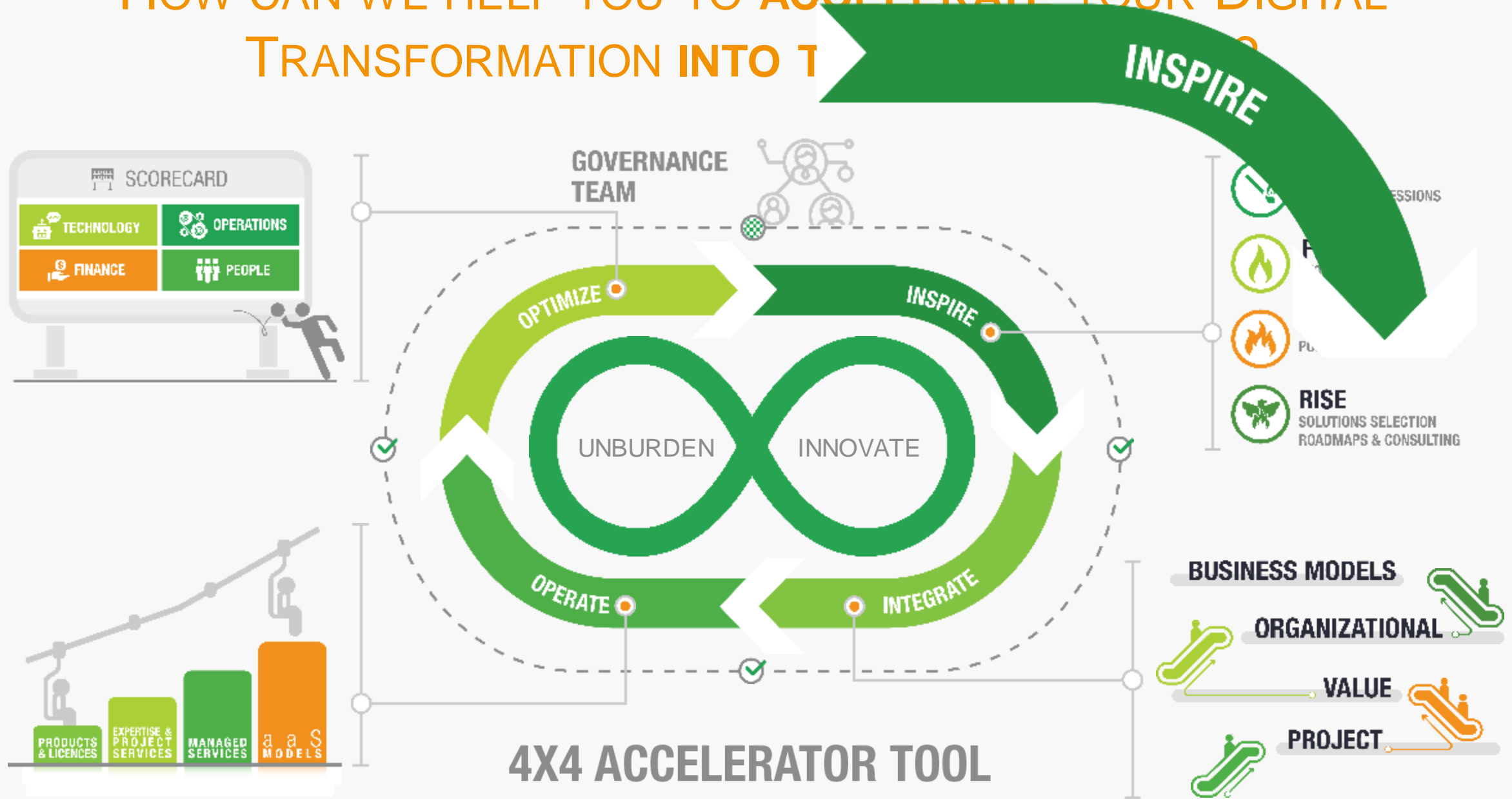
 Print this page

 woensdag 25 November 2020

 11.00-12.00

 Online

HOW CAN WE HELP YOU TO ACCELERATE YOUR DIGITAL TRANSFORMATION INTO T



BEDANKT

To get there, together



REALDOLMEN



HQ Realdolmen Huizingen

A. Vaucampsiaan 42

B-1654 Huizingen

+32 2 801 55 55

www.realdolmen.com