Microsoft

Veilig samenwerken in de cloud

Remco Ploeg

Uitdagingen binnen het onderwijs

- Cyber aanvallen (WannaCry)
- Phising mails
- Data lekken
- Gestolen wachtwoorden
- Verloren laptops / telefoons
- Data uitwisseling
- Per ongeluk een bestand gedeeld met een student
- .....

Beroepscriminelen hebben zich ontwikkeld tot geavanceerde actoren en voeren langdurige en hoogwaardige operaties uit

Digitale economische spionage door buitenlandse inlichtingendiensten zet de concurrentiepositie van Nederland onder druk

Ransomware is gemeengoed en is nog geavanceerder geworden

PHISHING, SPEARPHISHING EN WHALING

ROTTERDAMSE STUDENTEN BETALEN COLLEGEGELD HOGESCHOOL NA NEPMAIL

Waar moet je op letten met (IT)beveiliging?

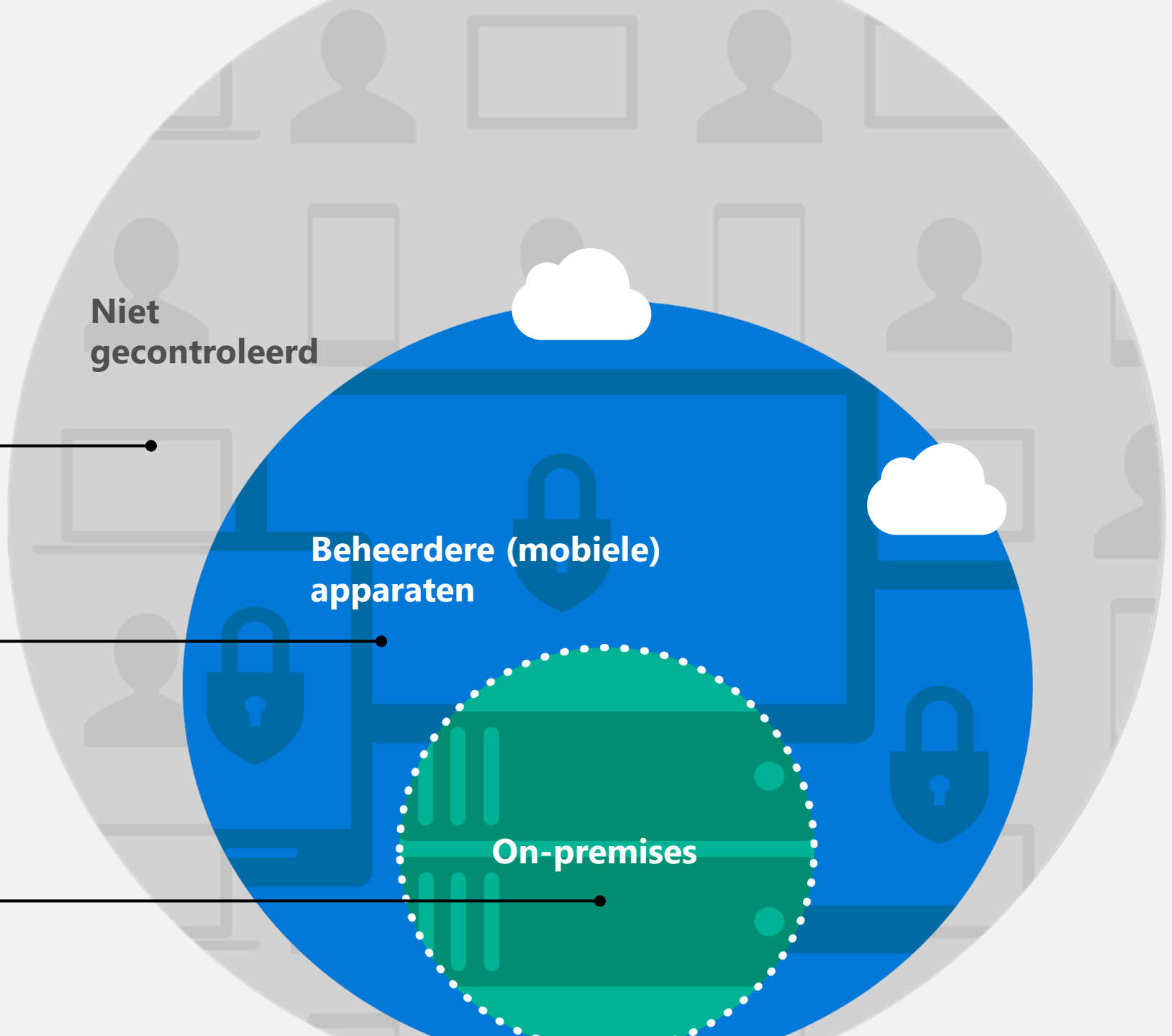
- Gebruikers
  - Bewustwording:
    - Gevaren
    - Wat moet ik doen?
    - Melden
  - Eenvoudig; moet niet lastig zijn
  - …
- Techniek
  - Laatste updates van servers / werkstations (WannaCry)
  - Beveiliging software op werkplek en server
  - Monitoring van incidenten en acteren
  - Wachtwoordbeleid / MFA
    - Windows Hello
  - Beleid
  - Connecties naar databases (met gebruikersnaam/wachtwoord)
  - BACKUP!
  - ….

Hoe heb ik controle?

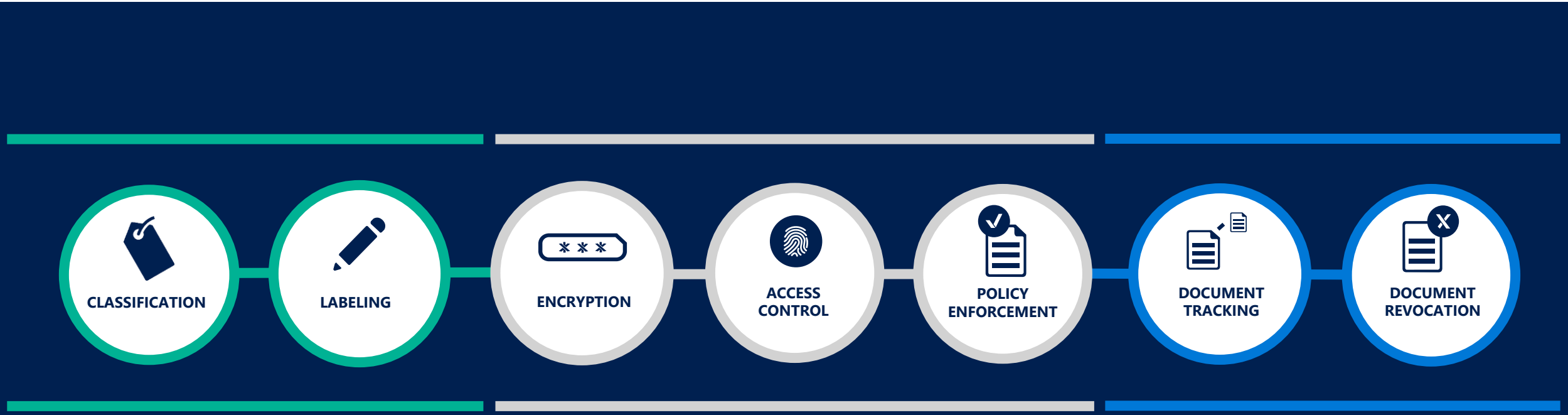
Hybrid data

Beheerde apparaten

‘Veilig’



Beveiligen van je informatie

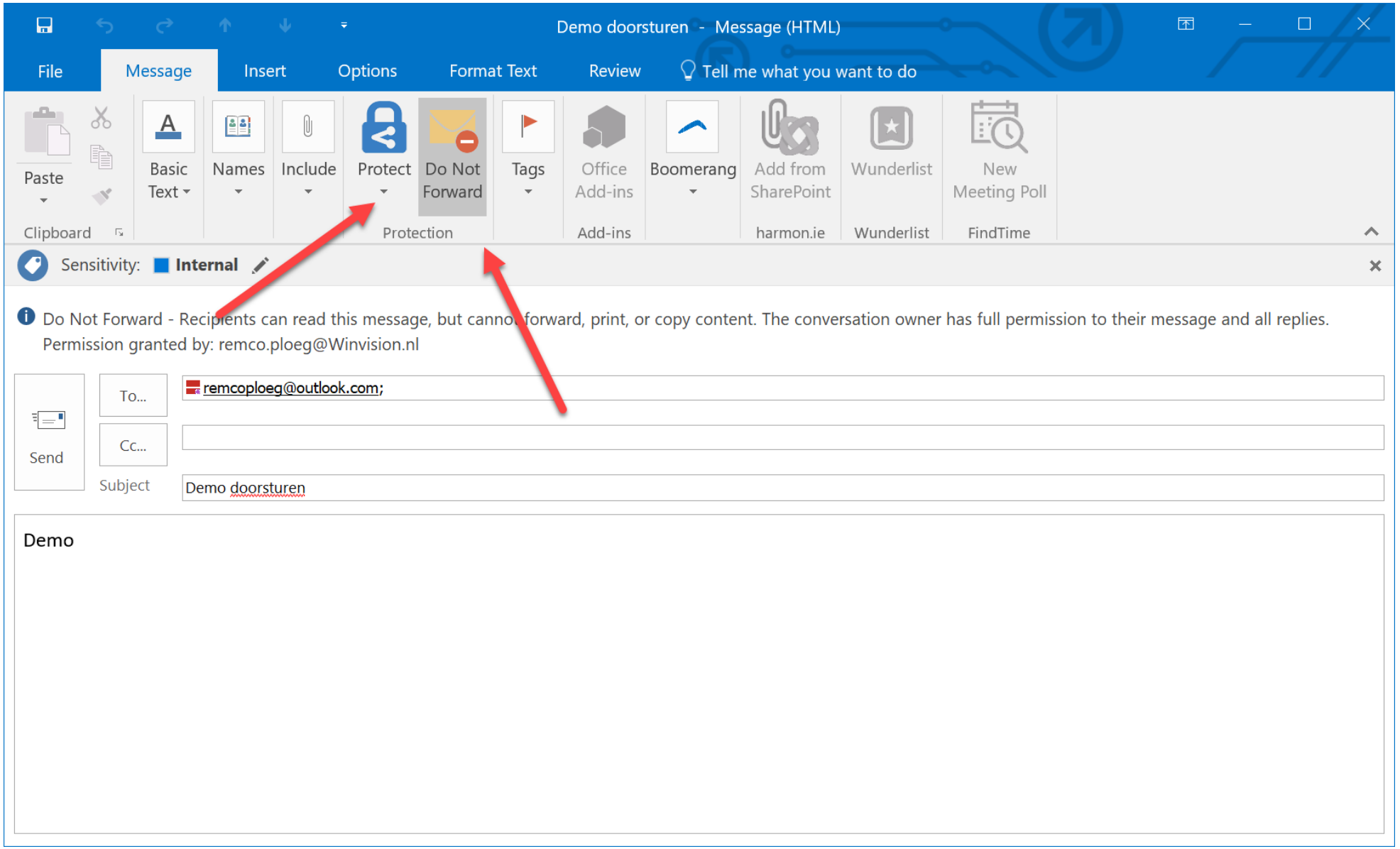


Classificatie en labellen

Beveiligen

Monitoren

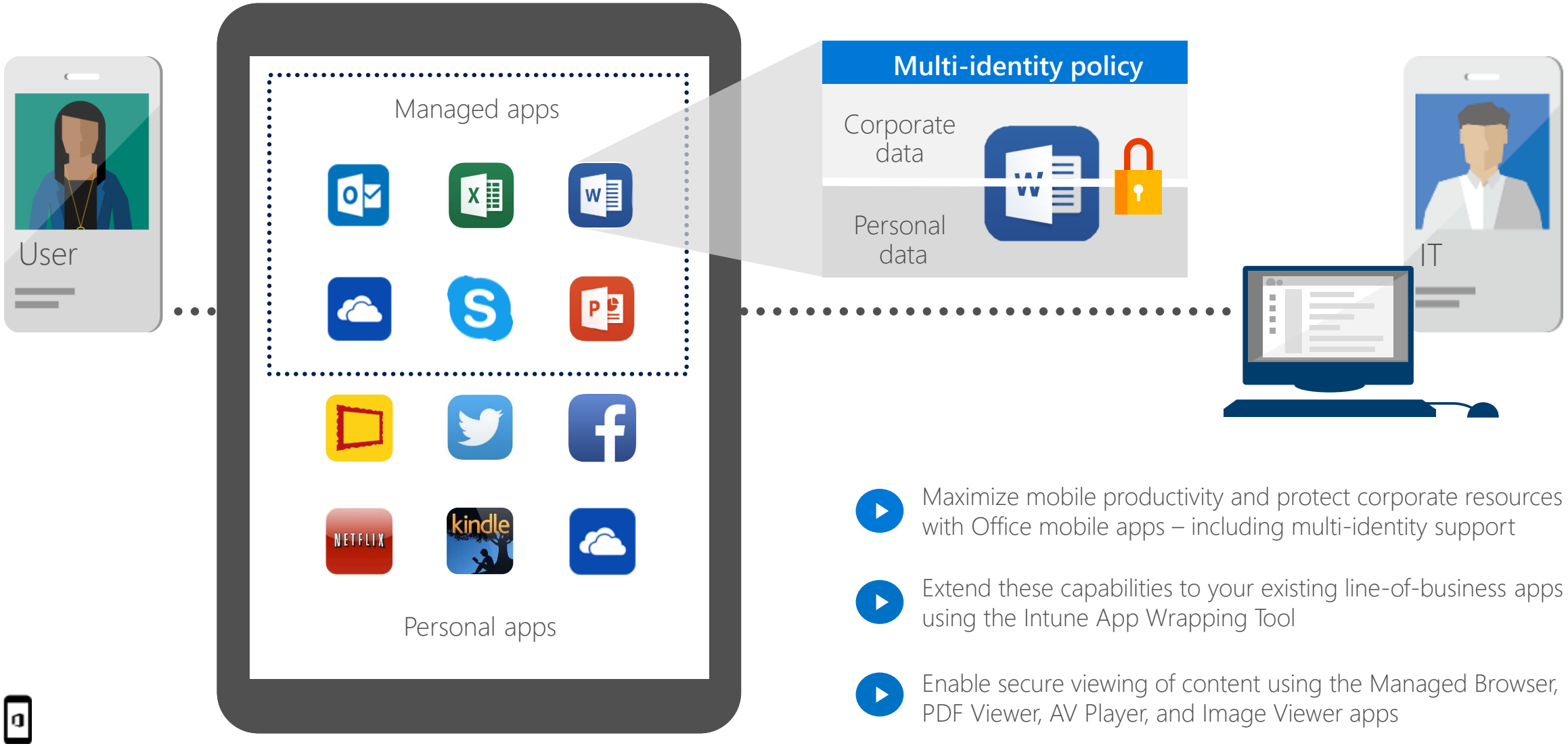
Voorbeeld


Demo doorsturen - Message (HTML)
File
Message
Insert
Options
Format Text
Review
Tell me what you want to do
Paste
Clipboard
Basic Text
Names
Include
Protect
Do Not Forward
Protection
Tags
Office Add-ins
Add-ins
Boomerang
Add from SharePoint
harmon.ie
Wunderlist
Wunderlist
New Meeting Poll
FindTime
Sensitivity: Internal
Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.
Permission granted by: remco.ploeg@Winvision.nl
Send
To...
remcoploeg@outlook.com;
Cc...
Subject
Demo doorsturen
Demo

O365 en EM+S

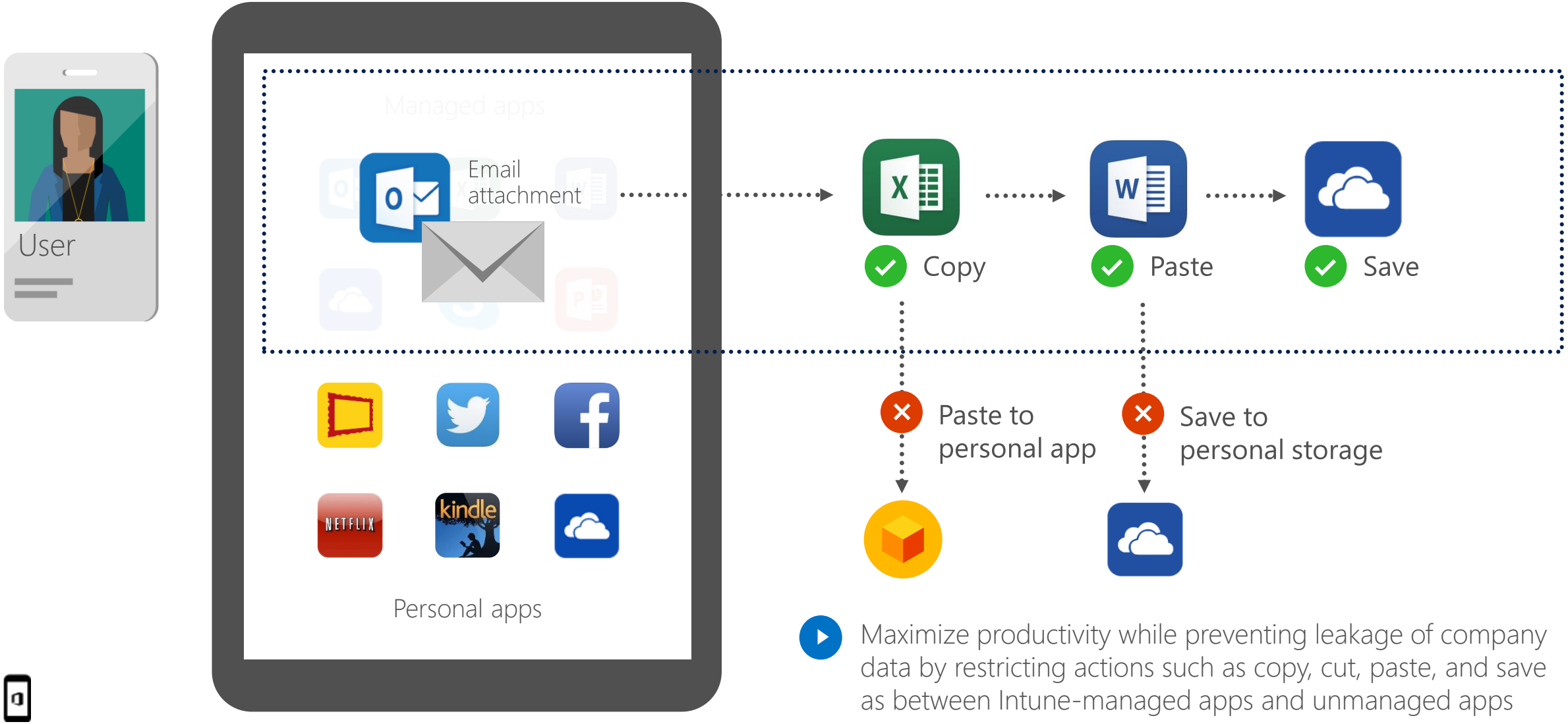
	Identity and access management	Managed mobile productivity	Information protection	Identity-driven security
Enterprise Mobility + Security	**Azure AD for O365+** • Advanced security reports • Single sign-on for all apps • Advanced MFA • Self-service group management & password reset & write back to on-premises, • Dynamic Groups, Group based licensing assignment	**MDM for O365+** • PC management • Mobile app management (prevent cut/copy/paste/save as from corporate apps to personal apps) • Secure content viewers • Certificate provisioning • System Center integration	**RMS for O365+** • Automated intelligent classification and labeling of data • Tracking and notifications for shared documents • Protection for on-premises Windows Server file shares	**Cloud App Security** • Visibility and control for all cloud apps **Advanced Threat Analytics** • Identify advanced threats in on premises identities **Azure AD Premium P2** • Risk based conditional access
Office 365	**Basic identity mgmt. via Azure AD for O365:** • Single sign-on for O365 • Basic multi-factor authentication (MFA) for O365	**Basic mobile device management via MDM for O365** • Device settings management • Selective wipe • Built into O365 management console	**RMS protection via RMS for O365** • Protection for content stored in Office (on-premises or O365) • Access to RMS SDK • Bring your own key	**Advanced Security Management** • Insights into suspicious activity in Office 365

Mobiele apparaten beheren

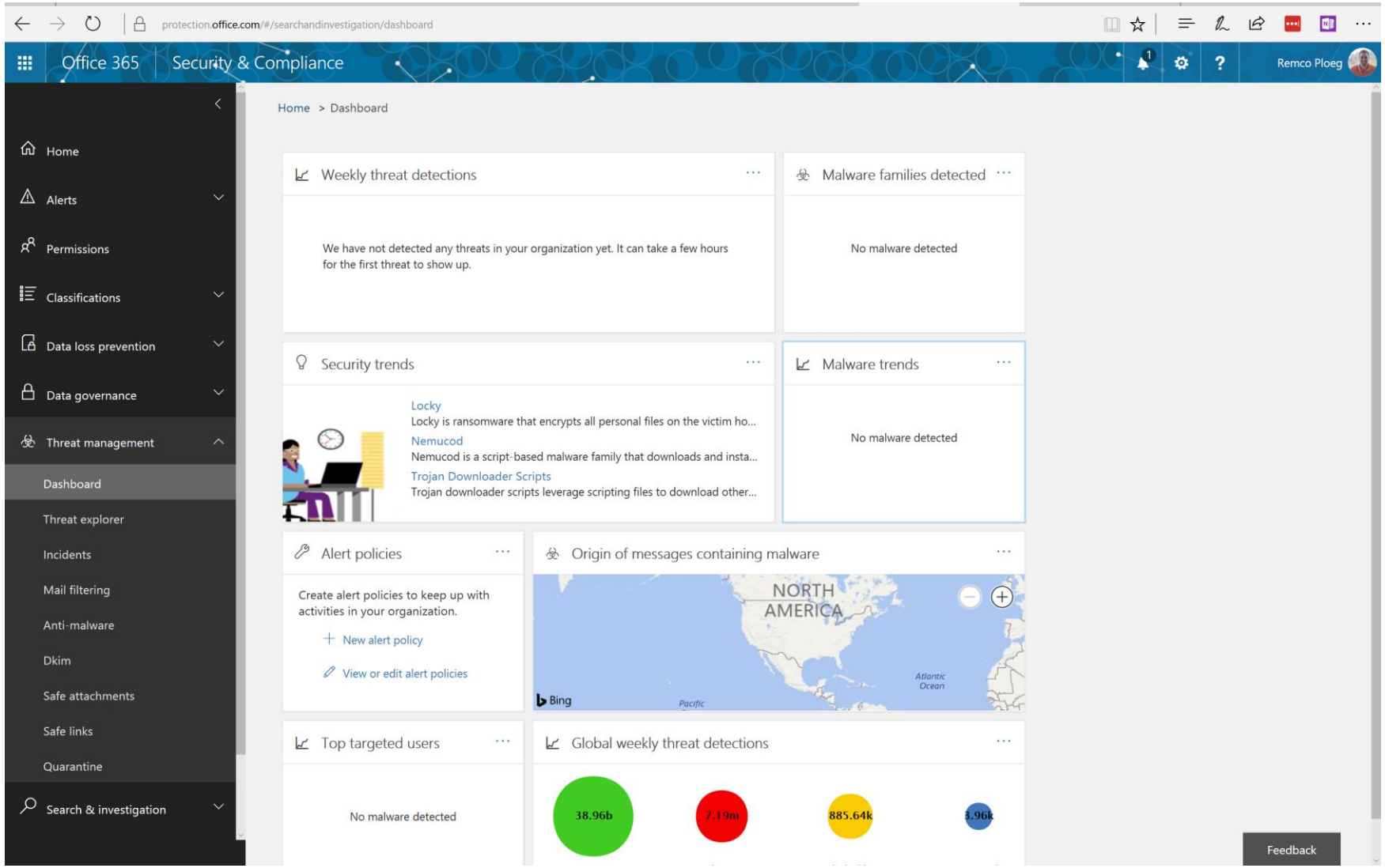


- Maximize mobile productivity and protect corporate resources with Office mobile apps – including multi-identity support
- Extend these capabilities to your existing line-of-business apps using the Intune App Wrapping Tool
- Enable secure viewing of content using the Managed Browser, PDF Viewer, AV Player, and Image Viewer apps

Mobiele applicaties beheren



Demo – Threat management, Classificaties, etc.



Het zijn maar vijf stappen

Best Practice – begin klein!

1. Classificeer	Kleine stappen; zorg voor een kleine pilot met bijv. HR
2. Label	Niet veel labels! Moet eenvoudig blijven
3. Beveilig	Zet policy's aan
4. Monitor	Deel met externe personen en monitor gebruik
5. Respond	Acteer op alerts