



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
COLLEGE GELD
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!

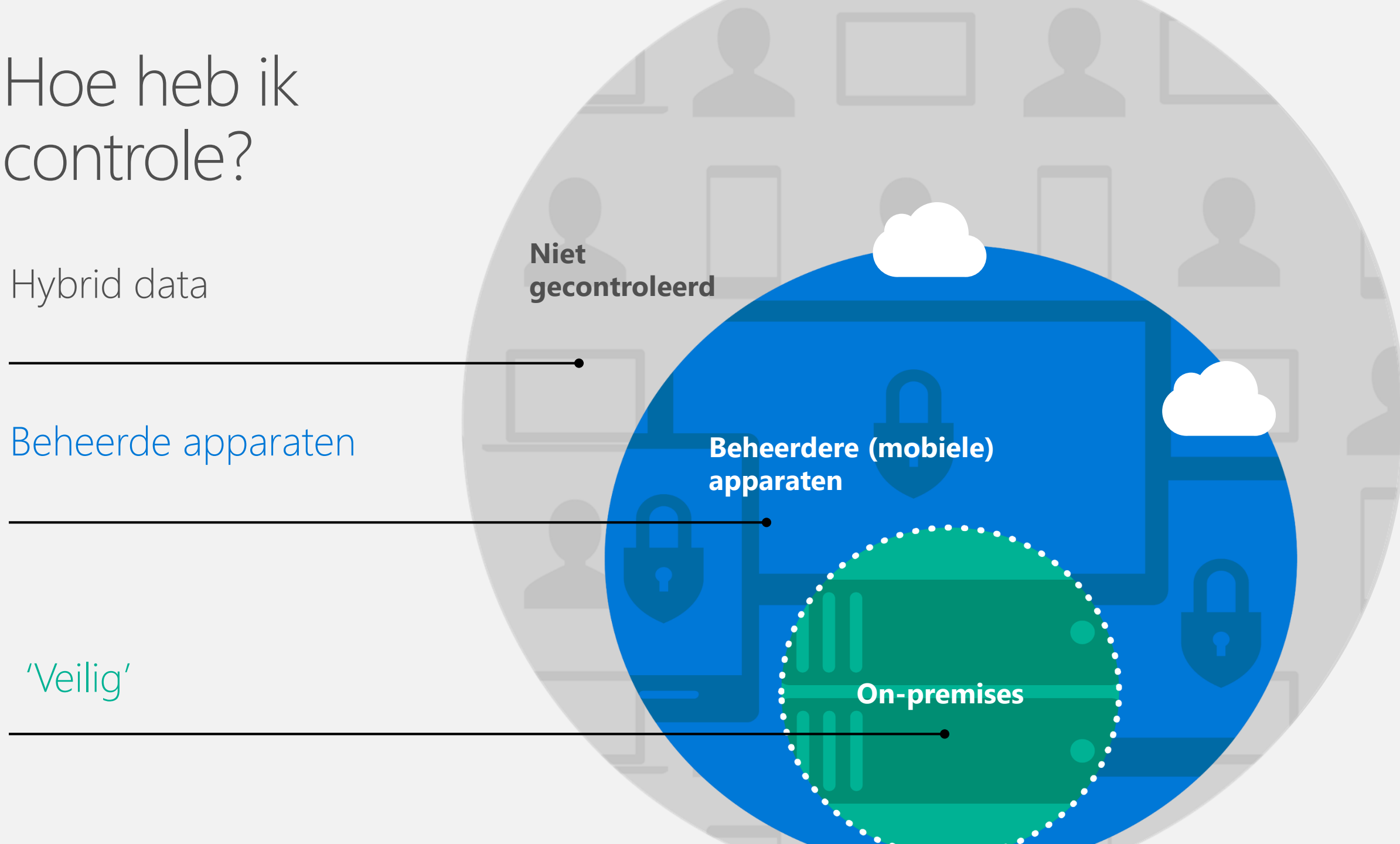
-

Hoe heb ik controle?

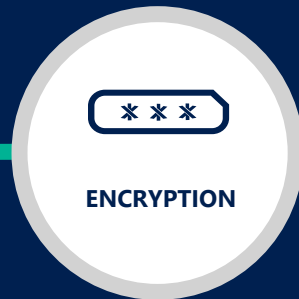
Hybrid data

Beheerde apparaten

'Veilig'



Beveiligen van je informatie



Classificatie en
labelen

Beveiligen

Monitoren

Voorbeeld



The screenshot shows the Microsoft Outlook interface. The ribbon is set to the 'Message' tab, with the 'Protect' button highlighted. Two red arrows point from the 'Protect' button in the ribbon to the 'Do Not Forward' button in the ribbon and to the 'Do Not Forward' notification in the message body. The message body contains the following text:

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

To... remcopleeg@outlook.com

Cc...

Subject Demo doorsturen

Demo

O365 en EM+S

Enterprise Mobility + Security



Identity and access management

- 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

- Basic identity mgmt. via Azure AD for O365:**
- Single sign-on for O365
 - Basic multi-factor authentication (MFA) for O365

Managed mobile productivity

- 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

- Basic mobile device management via MDM for O365**
- Device settings management
 - Selective wipe
 - Built into O365 management console

Information protection

- RMS for O365+**
- Automated intelligent classification and labeling of data
 - Tracking and notifications for shared documents
 - Protection for on-premises Windows Server file shares

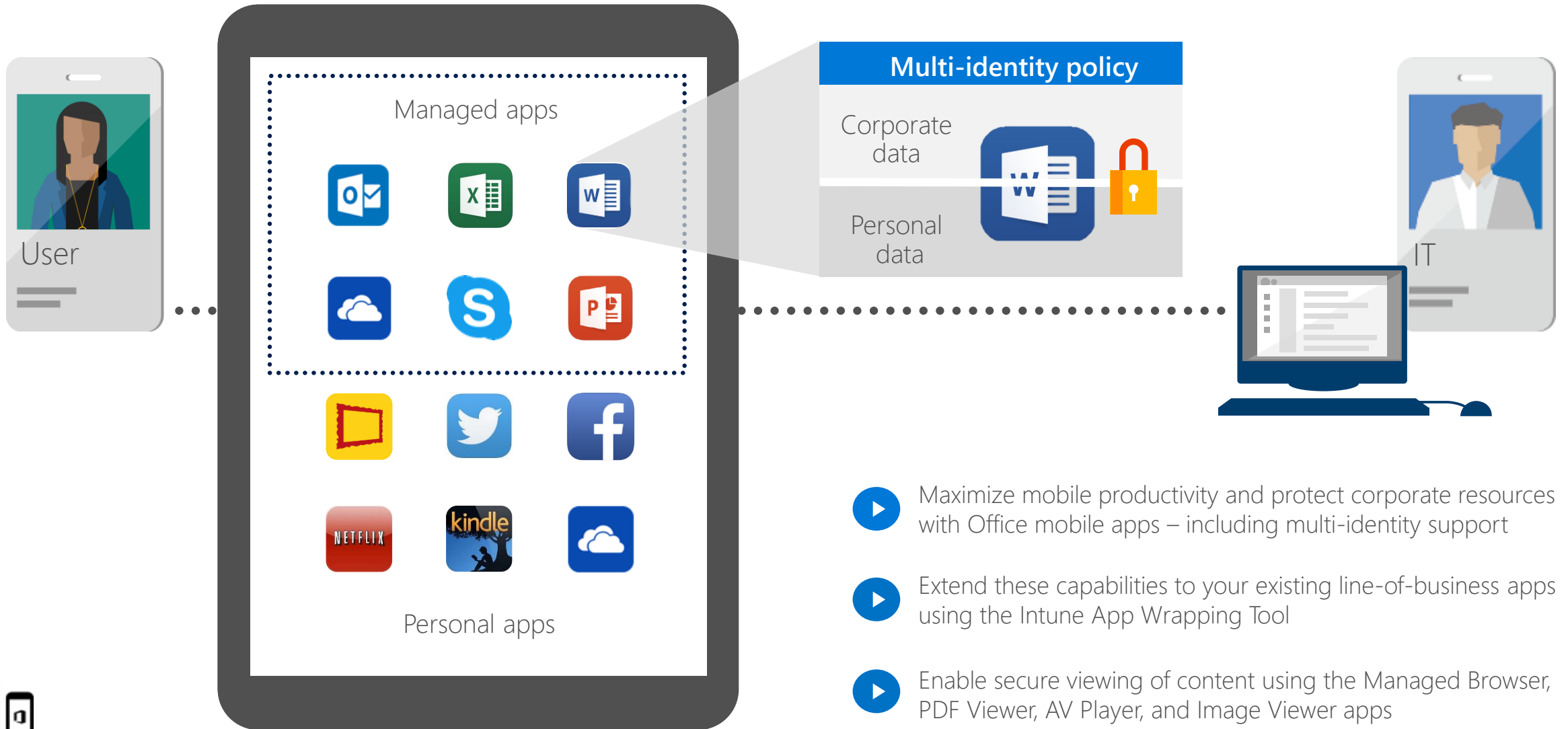
- RMS protection via RMS for O365**
- Protection for content stored in Office (on-premises or O365)
 - Access to RMS SDK
 - Bring your own key

Identity-driven security

- 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

- Advanced Security Management**
- Insights into suspicious activity in Office 365

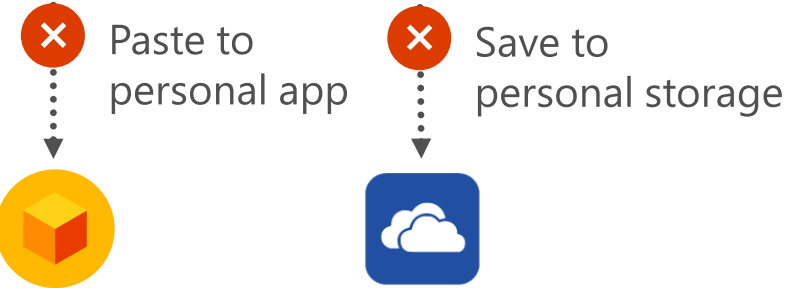
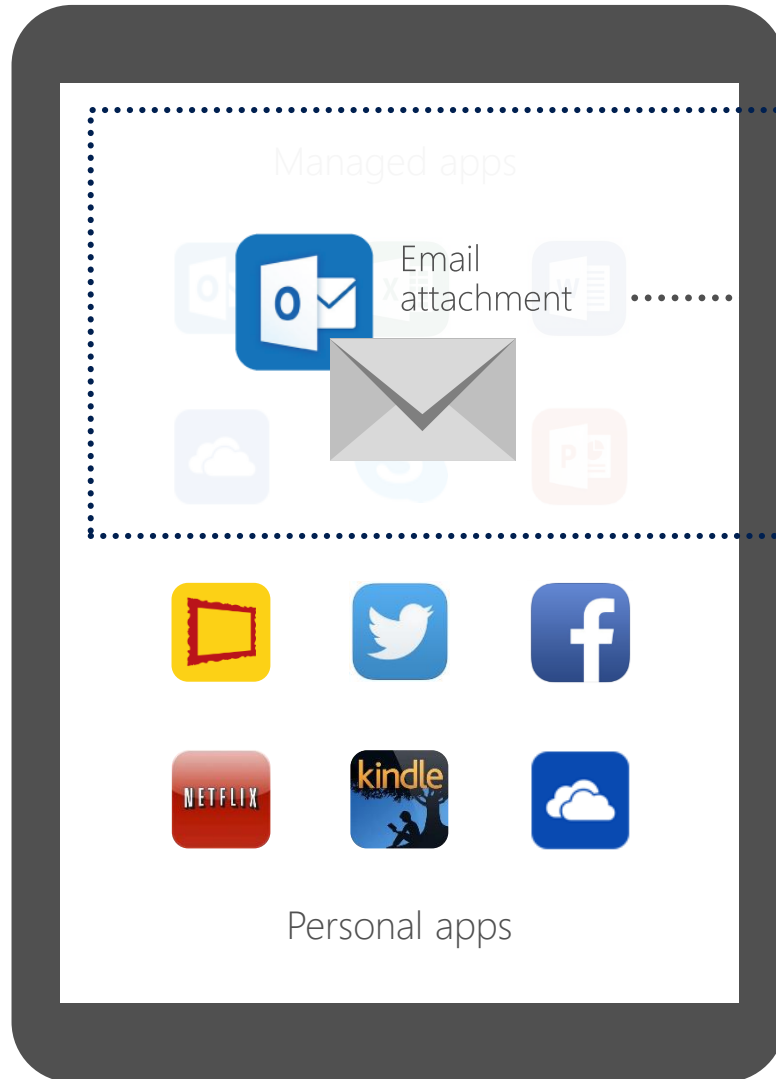
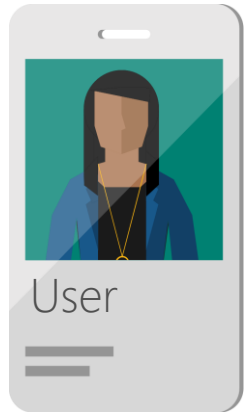
Mobiele apparaten beheren



- ▶ 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



▶ Maximize productivity while preventing leakage of company data by restricting actions such as copy, cut, paste, and save as between Intune-managed apps and unmanaged apps



Demo – Threat management, Classifications, etc.

The screenshot displays the Microsoft Security & Compliance Center dashboard. The left-hand navigation pane includes sections for 'Office 365 Security & Compliance' and 'Threat management'. The main content area is titled 'Home > Dashboard' and features several key components:

- Weekly threat detections:** A message stating, "We have not detected any threats in your organization yet. It can take a few hours for the first threat to show up."
- Malware families detected:** A message stating, "No malware detected."
- Security trends:** A list of threats including Locky (ransomware), Nemucod (script-based malware), and Trojan Downloader Scripts.
- Malware trends:** A message stating, "No malware detected."
- Alert policies:** A section for creating and managing alert policies, with a "New alert policy" button.
- Origin of messages containing malware:** A map of North America showing the geographic source of malware.
- Top targeted users:** A message stating, "No malware detected."
- Global weekly threat detections:** A summary of global threat counts represented by four colored circles: 38.96b (green), 7.19m (red), 885.64k (yellow), and 3.96k (blue).

The interface includes a top navigation bar with the user's name "Remco Ploeg" and a "Feedback" button in the bottom right corner.

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

