Can Microsoft help meet the GDPR requirements?

Danny Uytgeerts
Microsoft 365 TSP / P-Seller
Privacy Consultant (certified DPO)
Member of DPO-Pro (Professional association of Belgian DPOs)

danny.uytgeerts@realdolmen.com
www.linkedin.com/in/duytgeerts

High level view of the GDPR

What organizations have to do

Keep records of all processing of personal information

Institute safeguards for cross-border data transfers

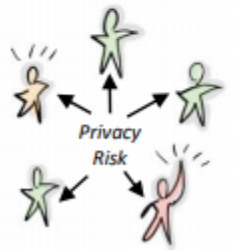
Maintain appropriate data security

Collect personal data lawfully and fairly, and where relevant, get appropriate consent and provide notification of personal data processing activities

Get a parent's consent to collect data for children under 16

Consult with regulators before certain processing activities

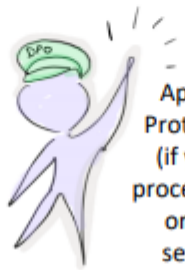
Provide appropriate data protection training to personnel having permanent or regular access to personal data



Conduct Data Protection Impact Assessments on new processing activities

Implement Data Protection-by-Design *(Privacy "baked-in")*

Take responsibility for the security and processing activities of third-party vendors



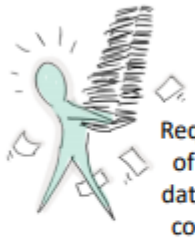
Appoint a Data Protection Officer (if you regularly process lots of data, or particularly sensitive data)

Be able to demonstrate compliance on demand

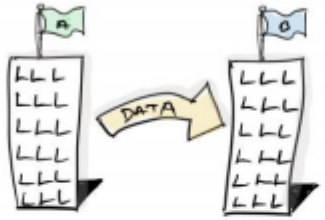
Notify data protection agencies and affected individuals of data breaches in certain circumstances

What individuals can do

Withdraw consent for processing

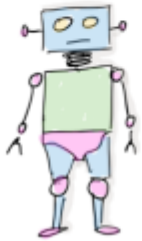


Request a copy of all of their data & request corrections if wrong



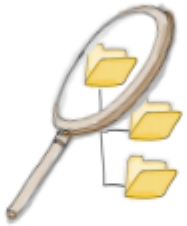
Request the ability to move their data to a different organization

Request that their information is deleted when there's no purpose to retain it

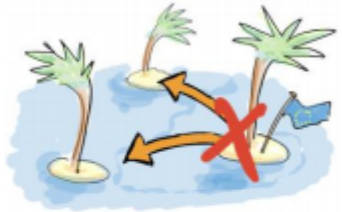


Object to automated decision-making processes, including profiling

What regulators can do



Ask for records of processing activities and proof of steps taken to comply with the GDPR



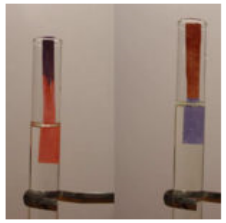
Suspend cross-border data flows

Impose temporary data processing bans, require data breach notification, or order erasure of personal data

Enforce penalties of up to €20 million or 4% of annual revenues for non-compliance

28
NOV

Datalek Amersfoort blijft lakmoestest voor Autoriteit Persoonsgegevens



Het is nu tien maanden terug(28 januari 2016) dat de gemeente Amersfoort een enorm datalek had doordat een medewerker van de afdeling sociale wijkteams zorggegevens van 1900 burgers in een onbeveiligde Excel-sheet per onbeveiligde email naar een verkeerde geadresseerde stuurde. De melding van het datalek aan de Autoriteit Persoonsgegevens(AP) deed de gemeente bovendien niet zelf. De foutief geadresseerde meldde het datalek aan de AP waarna de AP aan de gemeente Amersfoort vroeg hoe het zat. Een bestuurlijk rel was geboren die tot eind september voortsudderde. Nog steeds deed de AP geen uitspraak over het al dan niet opleggen van sancties aan de Gemeente Amersfoort. Op zich is daar wel alle reden voor, zeker in het licht van de zeer forse uitbreiding van de sanctiemogelijkheden die de AP op 1 januari 2016 kreeg. Er blijken flink wat datalekken te bestaan. Het dagblad Trouw meldde op 24 november dat de AP sinds 1 januari bericht kreeg over 4700 datalekken, waarvan er 304 uit de ziekenhuizen kwamen. Dat komt neer op één per dag. De casus Amersfoort is zo interessant omdat het een bijzondere situatie betreft die een soort lakmoestest is voor wat betreft het gezag van de AP in het veld.

Bijzonder

Een aantal punten maken het datalek in Amersfoort heel bijzonder:

- Het gaat om een groot aantal gevoelige gegevens
- Het betreft een groot aantal burgers, namelijk 1900
- Het is niet binnen 72 uur na het verkeerd verzenden gemeld aan de AP
- Er is geen actie binnen 72 uur ondernomen richting de betreffende burgers
- Domme fouten zijn gemaakt door het Excel-bestand niet met een wachtwoord te beveiligen, het bestand niet te versleutelen en geen beveiligde email te gebruiken
- **Het datalek is aan de AP gemeld door de geadresseerde, waarna de AP de gemeente moest vragen hoe het zat**.

Privégegevens bijna 900 Enschedese werkzoekenden op straat na e-mailfout

Gepubliceerd: 06 april 2017 13:37
Laatste update: 07 april 2017 08:33

De gemeente Enschede heeft privégegevens van bijna 900 werkzoekenden per abuis in een e-mail verstuurd aan een groep van dertig andere werkzoekenden.

Dat bevestigt een woordvoerder van de gemeente desgevraagd tegen NU.nl. De 882 getroffen burgers zijn per brief op de hoogte gesteld van het datalek en de gemeente heeft zijn excuses aangeboden voor de fout.

Er is geen sprake geweest van een hack, maar een medewerker heeft per ongeluk een bijlage met de persoonsgegevens bij een e-mail over een vacature gevoegd. In het bestand stonden onder meer burgerservicenummers, geboortedata, telefoonnummers en het soort uitkering dat de werkzoekenden ontvangen.

De fout werd een half uur na verzending opgemerkt, stelt de gemeente in de brief. Met de dertig ontvangers is telefonisch contact opgenomen, om te zorgen dat zij de privégegevens weer zouden verwijderen. Volgens de gemeente is er "geen reden om aan te nemen dat er misbruik van uw gegevens wordt gemaakt".

"De regels rondom verzending van e-mail worden naar aanleiding van deze vervelende situatie verder aangescherpt", concludeert de gemeente.

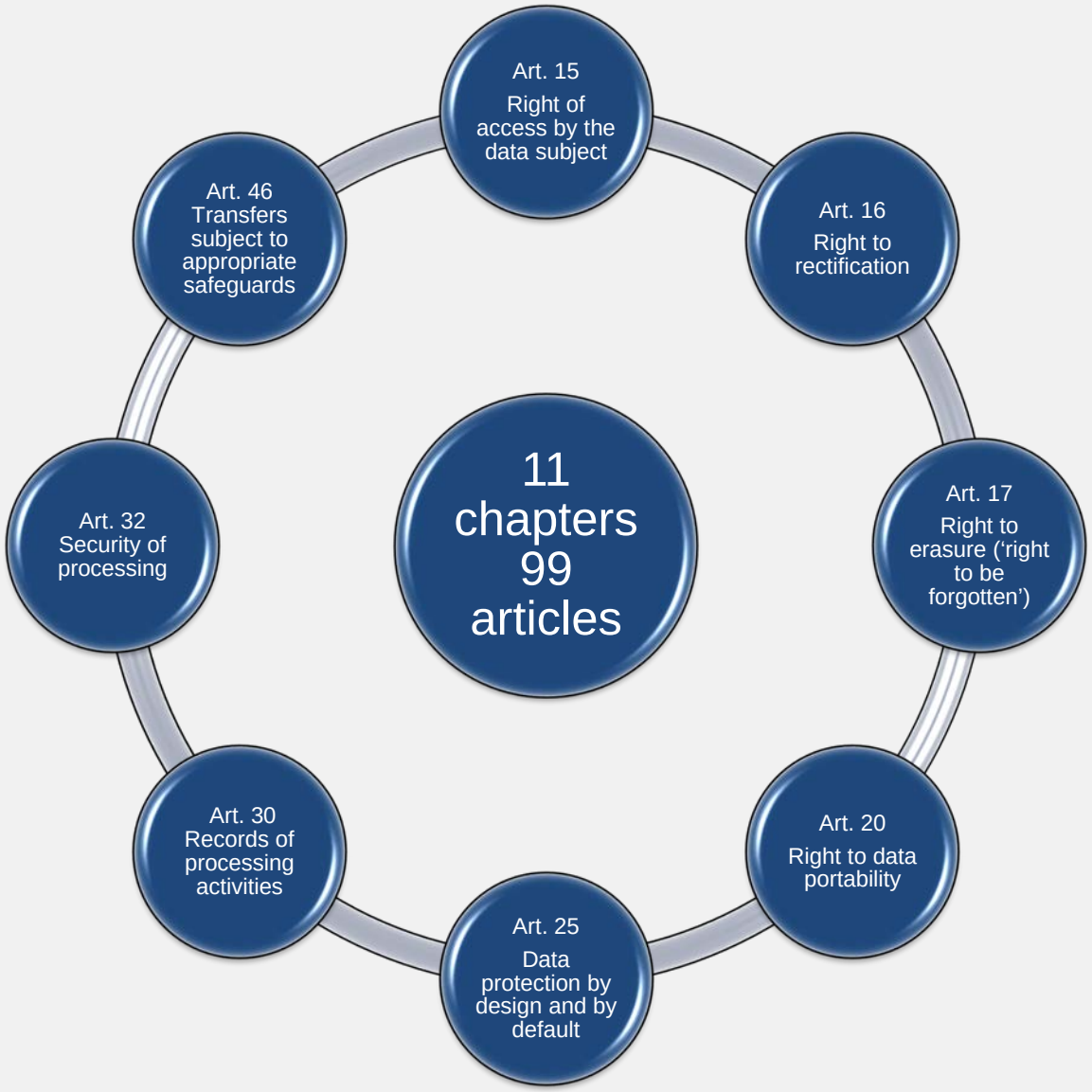
Door: NU.nl

GDPR – IS IT A THREAT OR AN OPPORTUNITY FOR YOUR ORGANIZATION?

- Game changer
  - Identify shadow it
  - Create a data inventory
  - Know your business processes

- Opportunities
  - Data cleanup
  - Eliminate or manage shadow it
  - Consolidate data sources and/or systems
  - Reduce risks (breaches, exposure, impact)

- Important Note:
  - Being compliant with security regulations doesn't automatically mean that you are secure (But it's a big step)
  - Individual service/application readiness is not enough



Try to avoid mapping technology into GDPR articles

NEXT …
4 COMMON CASES TO GIVE YOU INSIGHT AND GET STARTED

CASE 1: I WANT TO DISCOVER ALL PERSONAL DATA

Cloud App Security

Microsoft Information Protection

Advanced e-Discovery

On-Premise

SP – Exch – File Server

Scan data-at-rest
Classify data-at-rest

Office 365

Scan data-at-rest
Classify data-at-rest

Discover & Classify
- Data Security
- Retention

Scan data-at-rest
(API)
Classify data-at-rest

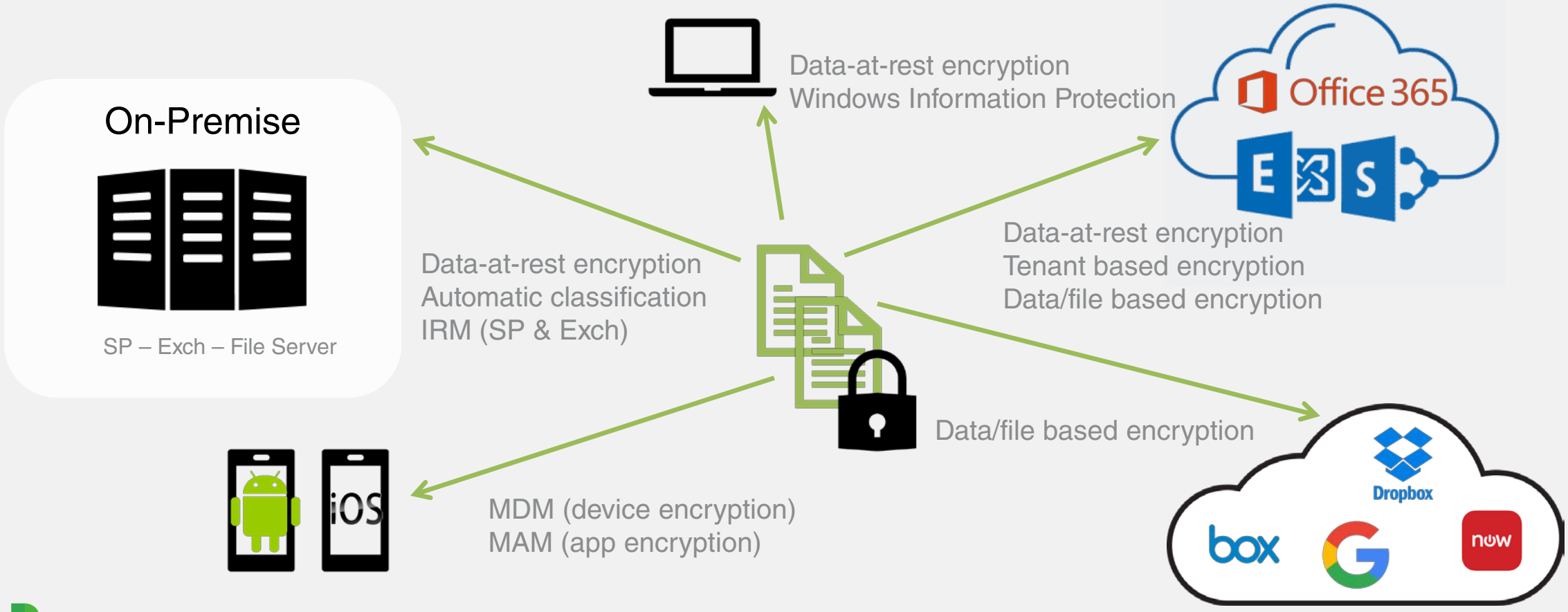
Dropbox

box

now

CASE 2: HOW DO I ENSURE MY DATA IS PROTECTED ON-PREMISE, IN THE CLOUD AND ON MY DEVICES?

Cloud App Security | Microsoft Information Protection | Intune | BitLocker | O365 Customer Key



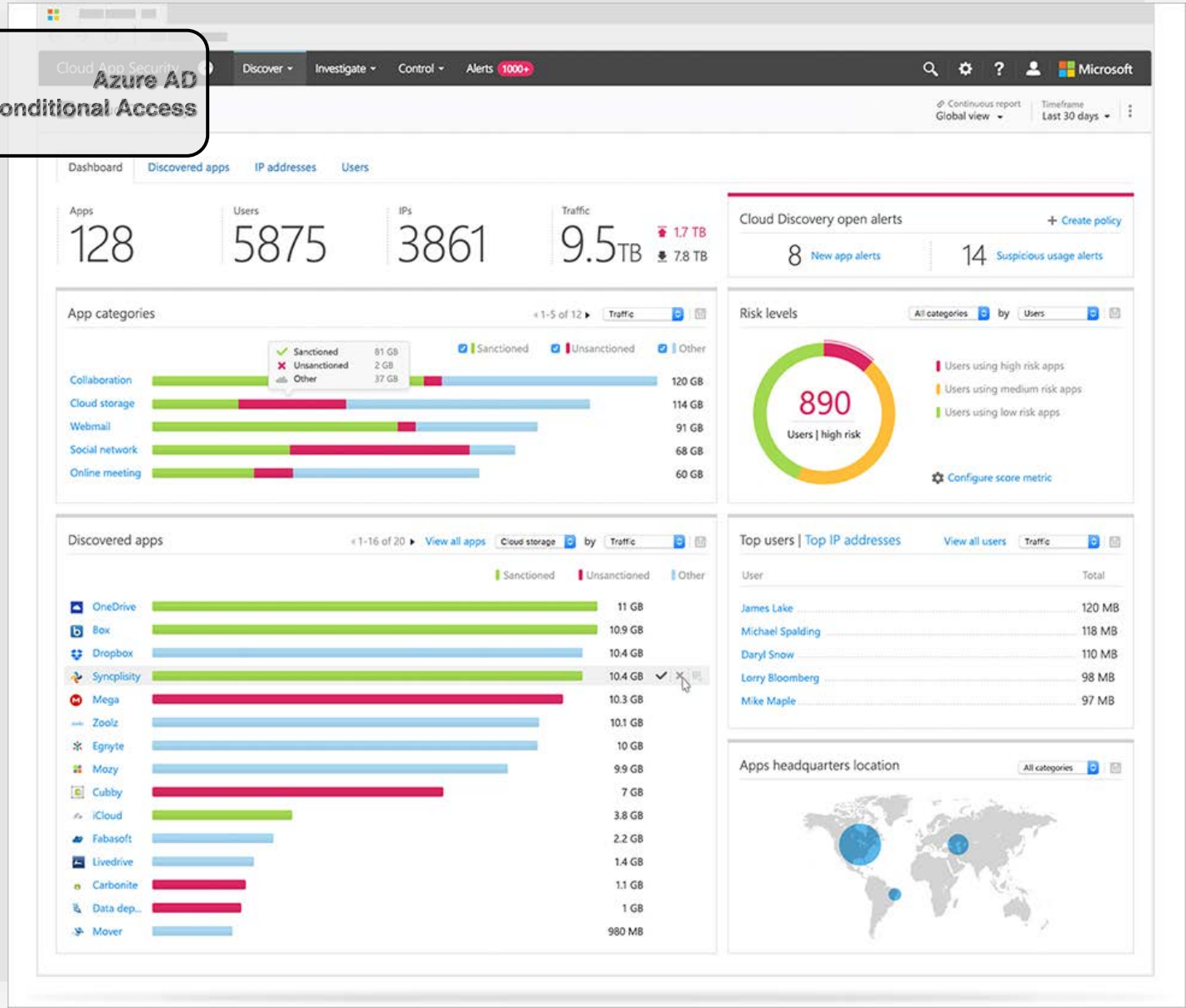
CASE 3: I WANT CONTROL OF MY DATA STORED IN CLOUD APPS

Cloud App Security

Microsoft Information Protection

Azure AD Conditional Access

- Discover
  - Identify cloud apps on your network, gain visibility into shadow IT, ongoing analytics
- Control access in real time
  - Manage and limit cloud app access based on conditions and session context, including user identity, device and location
- Protect your information
  - Get granular control over data and use built-in or custom policiesfor data sharing and DLP
- Detect threats
  - Identify high-risk usage and detect unusual behavior using threat intelligence and research



CONDITIONAL ACCESS: PROXY

Context-aware session policies

Control access to cloud apps based on user, location, device and app

Identify managed devices via VPN (location based), Domain joined devices, Intune compliant devices or client certificates

Supports any **SAML-based** app, any OS

Investigate & enforce app and data restrictions

Enforce browser-based “view only” mode for low-trust sessions

Limit access to sensitive data

Classify, label and protect on download

Visibility into unmanaged device activity

Unique integration with Azure AD

Integral component of Azure AD Conditional Access

Simple deployment directly from your Azure AD portal

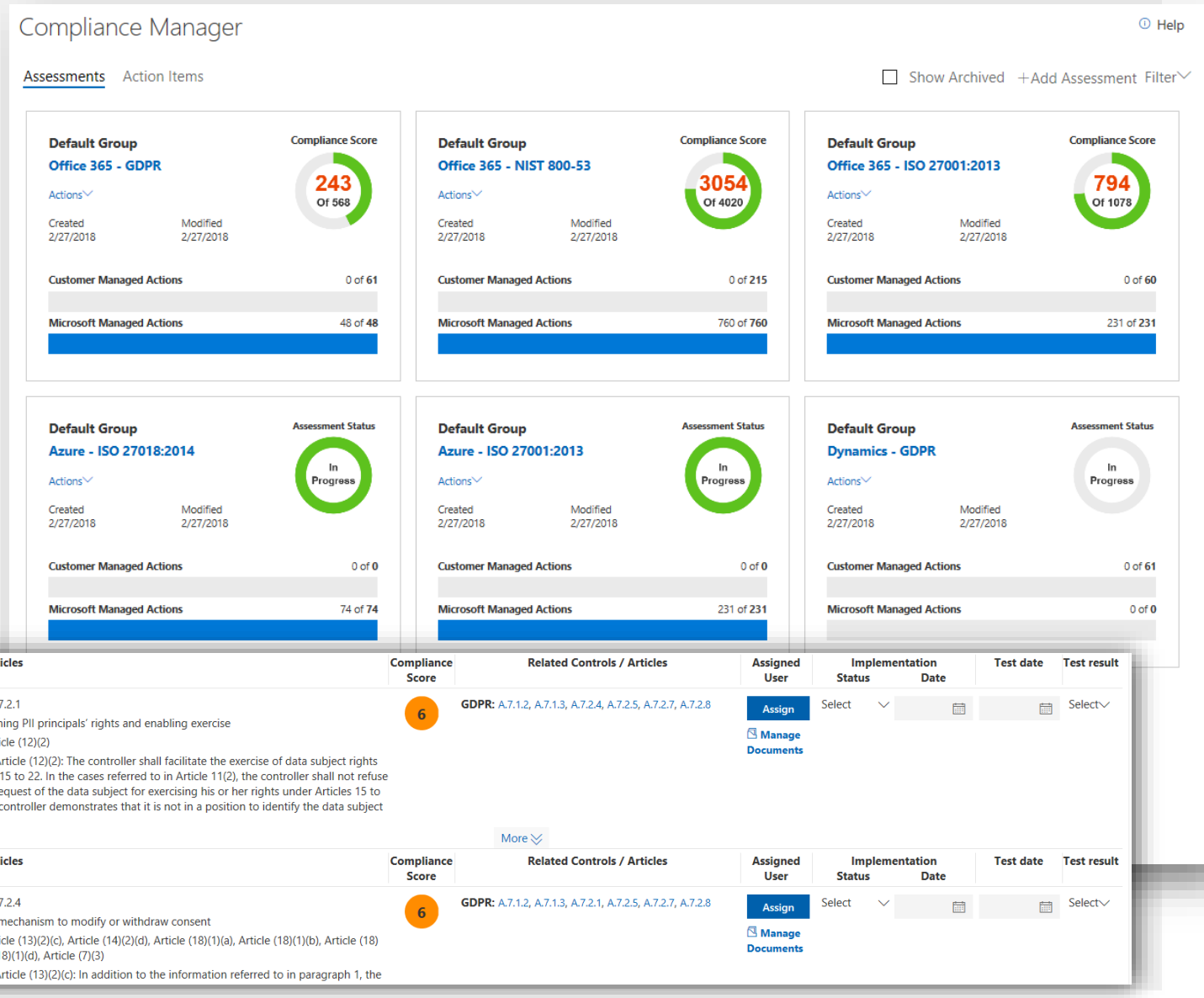
Leverages existing device management mechanisms, no additional deployment required

NEW

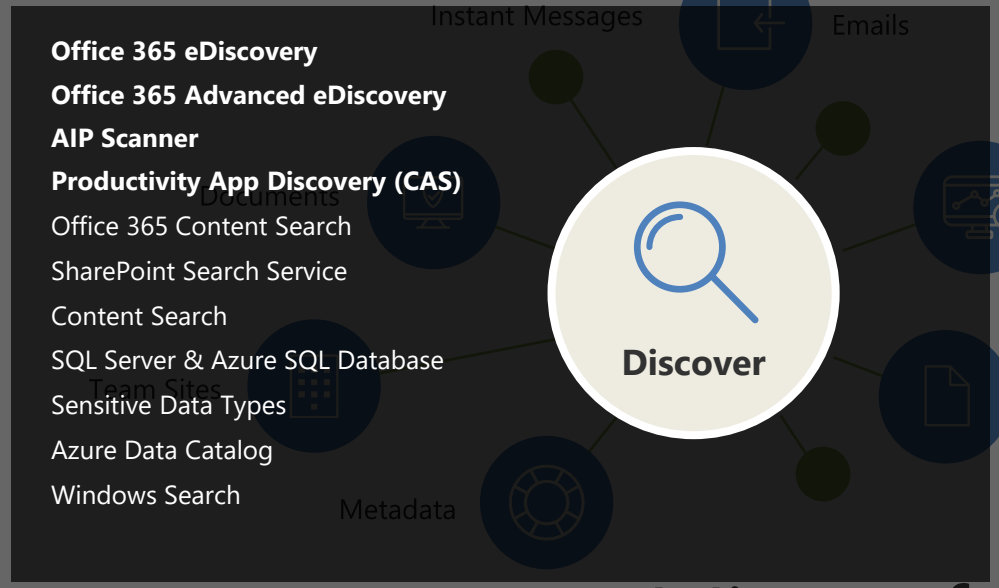
CASE 4: HOW CAN WE PROVE OUR EFFORT REGARDING COMPLIANCY?

Compliance Manager

- Compliance Manager is a **dashboard** that provides a summary of your data protection and compliance stature and recommendations to improve data protection and compliance
  - GDPR – ISO27001 – ISO27018
- Actionable **insights** that are designed to improve your data protection and compliance posture
- Control management and audit-ready **reporting** tools to streamline your compliance workflow



Microsoft's approach to GDPR



Workshop: Can Microsoft help meet the GDPR requirements?

Microsoft defines four pillars in that GDPR process where some products and services provide powerful solutions to handle compliancy:

- **Discover** - Identify what personal data you have and where it resides
- **Manage**- Determine how personal data is used and accessed
- **Protect** - Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches
- **Report** - Execute on data requests, report data breaches, and keep required documentation

Example Solutions:

Azure Information Protection, Cloud App Security, Data Loss Prevention, Privileged Identity Management, Advanced Threat Protection, Compliance Manager, Secure Score, …

Want to **find out more**?

- EU GDPR Portal
  - https://www.eugdpr.org/
- Download the Microsoft 365 GDPR white paper:
  - https://aka.ms/m365-gdpr-paper
- Microsoft Trust Center – GDPR:
  - https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx
- GDPR How-to: Get organized and implement the right processes
  - https://azure.microsoft.com/en-us/blog/gdpr-how-to-get-organized-and-implement-the-right-processes/
- O365 Secure Score
  - https://securescore.office.com
- Training for future Data Protection Officers
  - https://education.realdolmen.com/en/Course/DPO001

- **Contact me at danny.uytgeerts@realdolmen.com**