SharePoint konferenz 2019

How to deal with external sharing in Office 365

Nicki Borell
Consultant

ppedv corner4 INFORMATION TECHNOLOGY Microsoft Insight smartpoint

Nicki Borell
Consultant
www.nickiborell.com

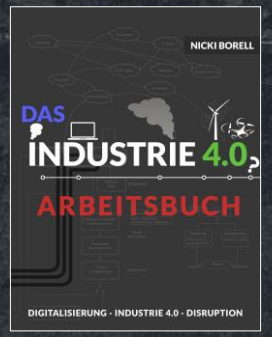
Microsoft® Most Valuable Professional

Microsoft Regional Director

GSA GERMAN SPEAKERS ASSOCIATION

MBER

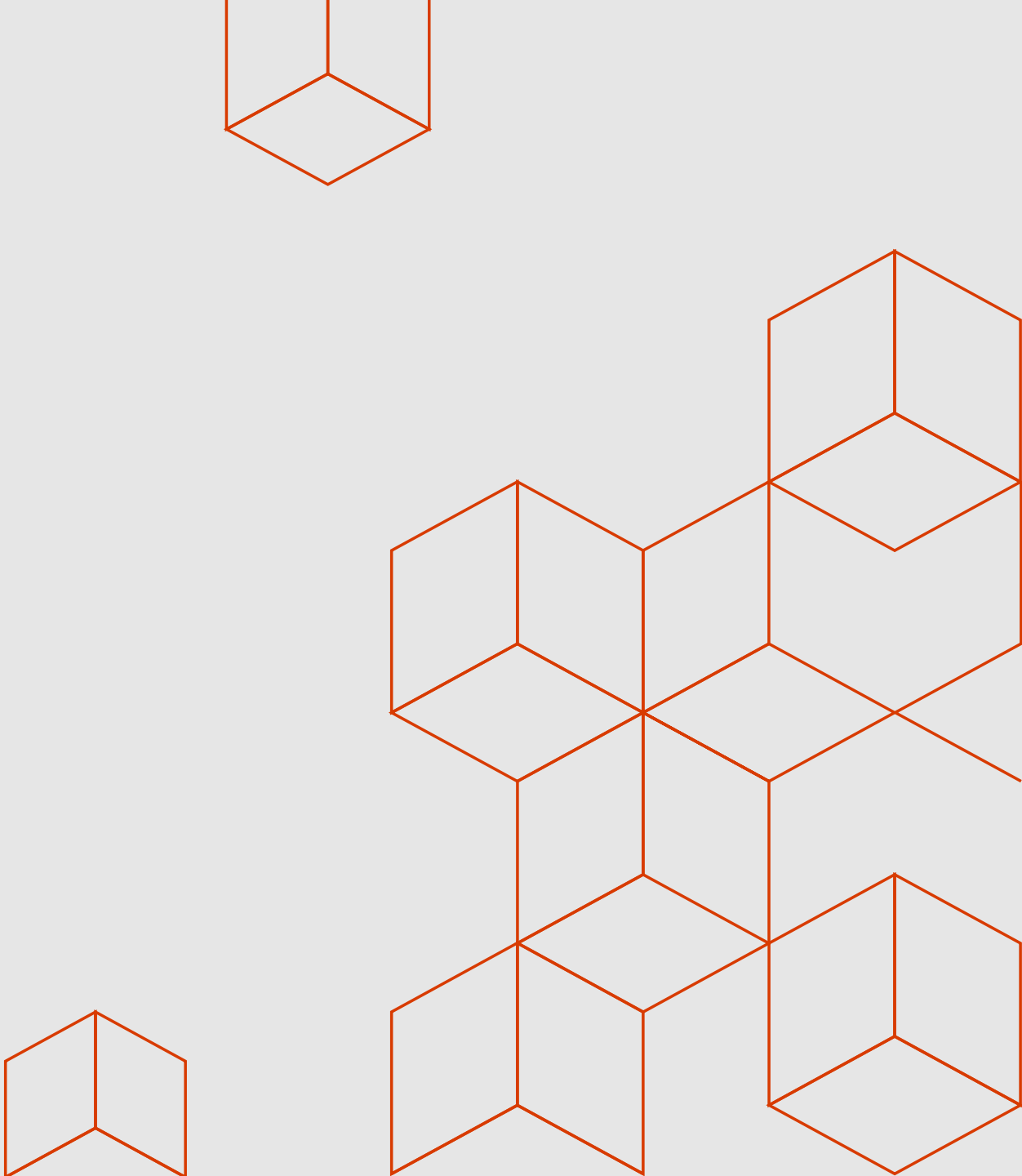
Author:



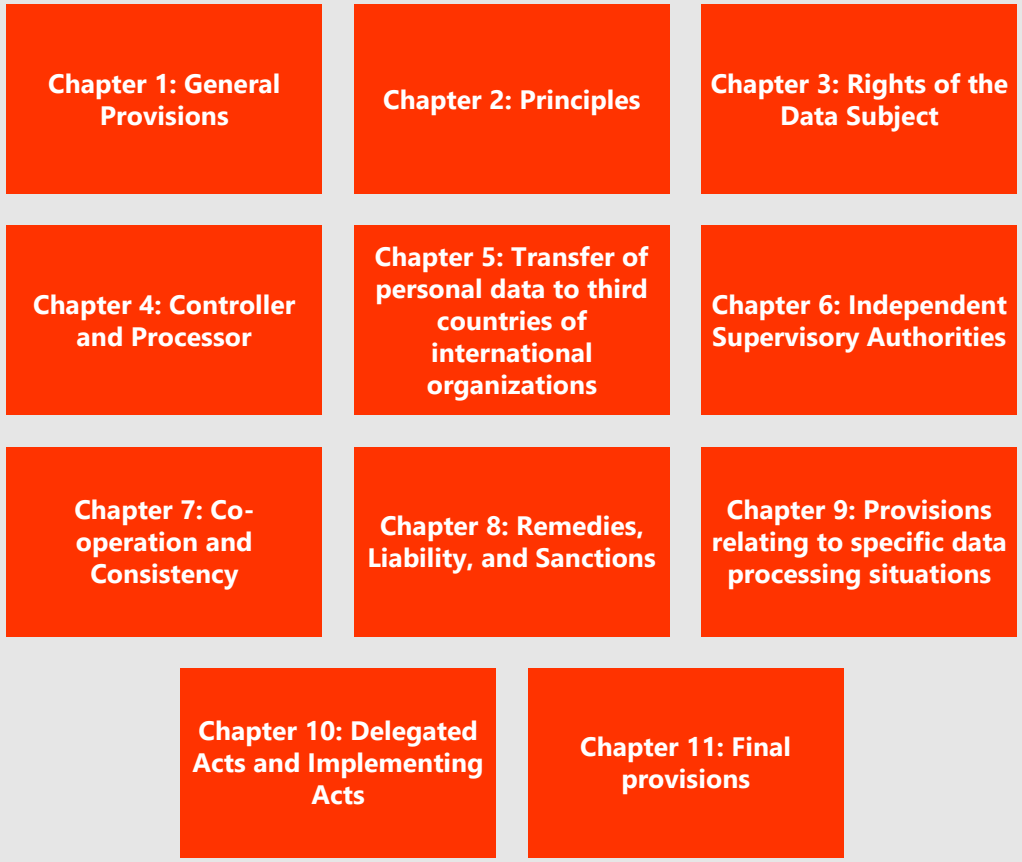
Reduce complexity…Force performance

XPERTS ATWORK

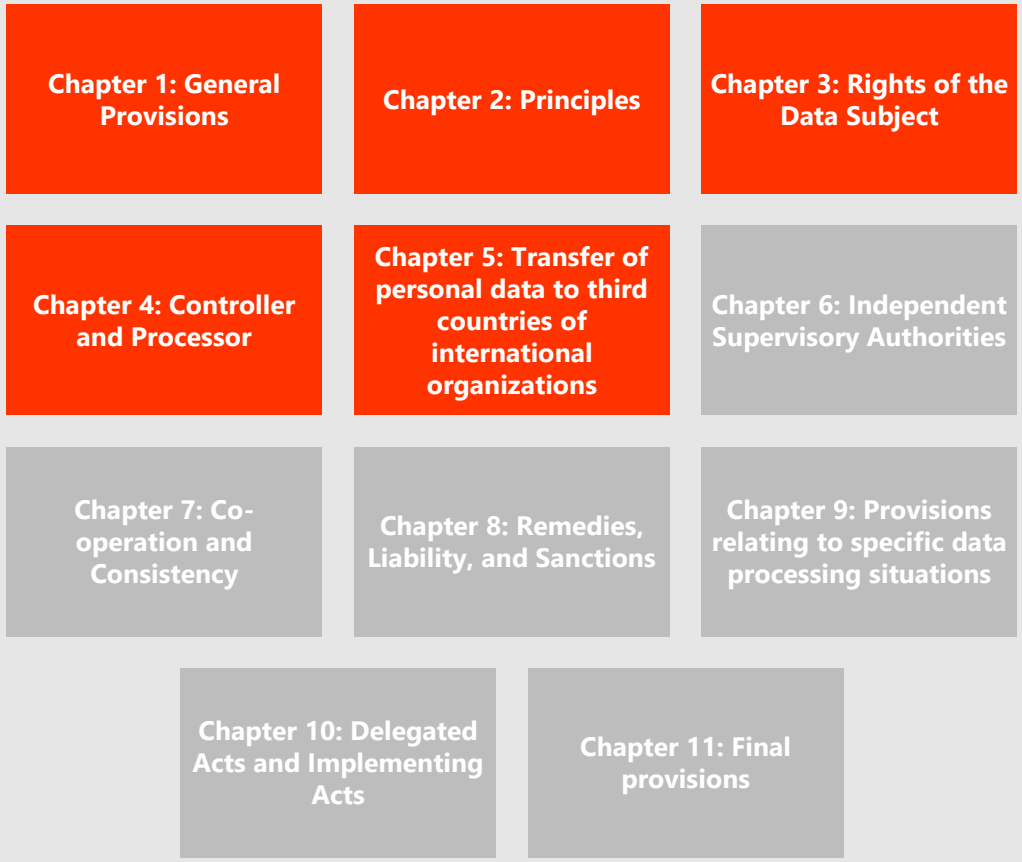
GDPR



GDPR from an IT perspective



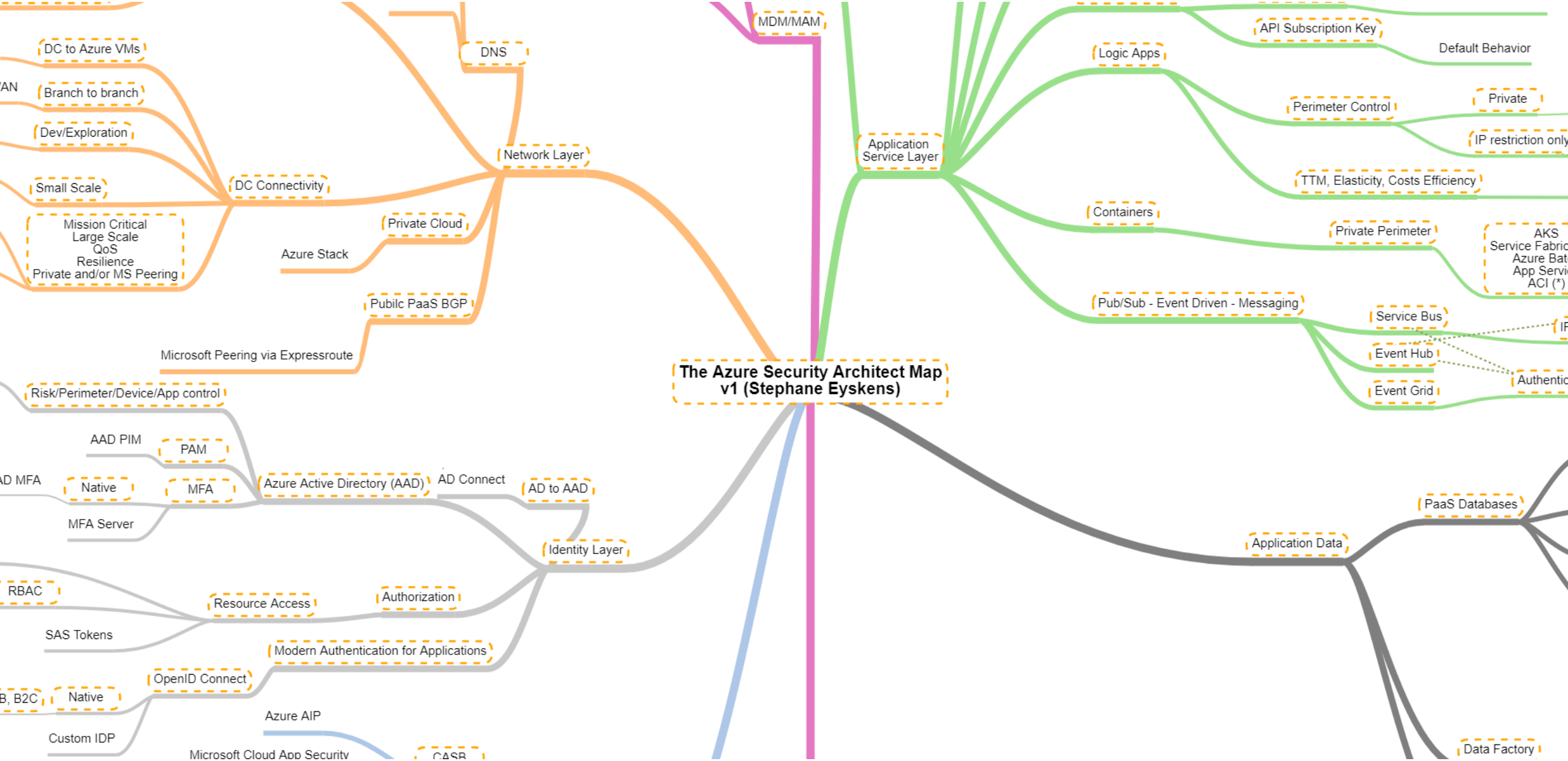
GDPR from an IT perspective



more details: https://bit.ly/2MNyeTQ

Microsoft

Sharing is more than SharePoint & OneDrive for Business


The Azure Security Architect Map v1 (Stephane Eyskens)
Network Layer
DC Connectivity
DC to Azure VMs
Branch to branch
Dev/Exploration
Small Scale
Mission Critical
Large Scale
QoS
Resilience
Private and/or MS Peering
DNS
Private Cloud
Azure Stack
Pubilc PaaS BGP
Microsoft Peering via Expressroute
Identity Layer
Azure Active Directory (AAD)
AD Connect
AD to AAD
PAM
AAD PIM
MFA
Native
MFA Server
Risk/Perimeter/Device/App control
Authorization
Resource Access
RBAC
SAS Tokens
Modern Authentication for Applications
OpenID Connect
Native
Custom IDP
Azure AIP
Microsoft Cloud App Security
CASB
MDM/MAM
Application Service Layer
Logic Apps
API Subscription Key
Default Behavior
Perimeter Control
Private
IP restriction only
TTM, Elasticity, Costs Efficiency
Containers
Private Perimeter
AKS
Service Fabric
Azure Bat
App Servi
ACI (*)
Pub/Sub - Event Driven - Messaging
Service Bus
Event Hub
Event Grid
Application Data
PaaS Databases
Data Factory

The Office 365 security settings matrix

Level	Explanation	Licensing
Default	Default settings of Office 365	No additional license required
Medium	Adjustments of the default Office 365 settings without the use of additional functions / licenses. Configuring Office 365 MFA and Office 365 MDM	No additional license required
High	like "Medium" plus: • Use Cloud App Security to monitor Office 365 and configure actions. • Use Azure AD Premium to enforce MFA and conditional access rules for external users, apps and devices.	• Cloud App Security • Azure AD Premium P1 or P2 (part of EMS or M365 and can also be purchased separately)
Very High	Like "High" plus: • use Intune to control device access and access to applications and manage devices.	Intune (part of EMS or M365 and can also be purchased separately)
Deactivating all external accesses		No additional license required

Level: Medium

Medium Level – OneDrive for Business

	Setting	Details / Options
OneDrive sharing settings	Default link type	*Shareable: Anyone with this link *Internal links *Direct links: Specific people
Change sharing link settings	Advanced settings for shareable links	*Links expire within drop-down list *choose whether shareable links can give people permission to edit shared files and folders
	External Sharing	*Anyone *New and existing external users *Existing external users *Only people in your organization
	Specify any advanced settings for external sharing	*Allow or block sharing with people on specific domains *External users must accept sharing invitations using the same account that the invitations were sent to *Let external users share items they don't own
	Other settings	Display to owners the names of people who viewed their files
Syncing	Show the sync button on the OneDrive website	
	Allow syncing only on PCs joined to specific domains	
	Block syncing of specific filetypes	
Accessing OneDrive for Business	Control access based on network location	Allow access only from specific IP address locations
	Control access from apps that don't use modern authentication	YES or NO
	Control access to features in the OneDrive mobile apps	Needs to have an Intune license assigned to change these settings in the OneDrive admin center.
Notifications	Display notifications to users when OneDrive files are shared with them	YES or NO
	Email OneDrive owners when…:	*Other users invite additional users to shared files *External users accept invitations to access files *An anonymous access link is created or changed

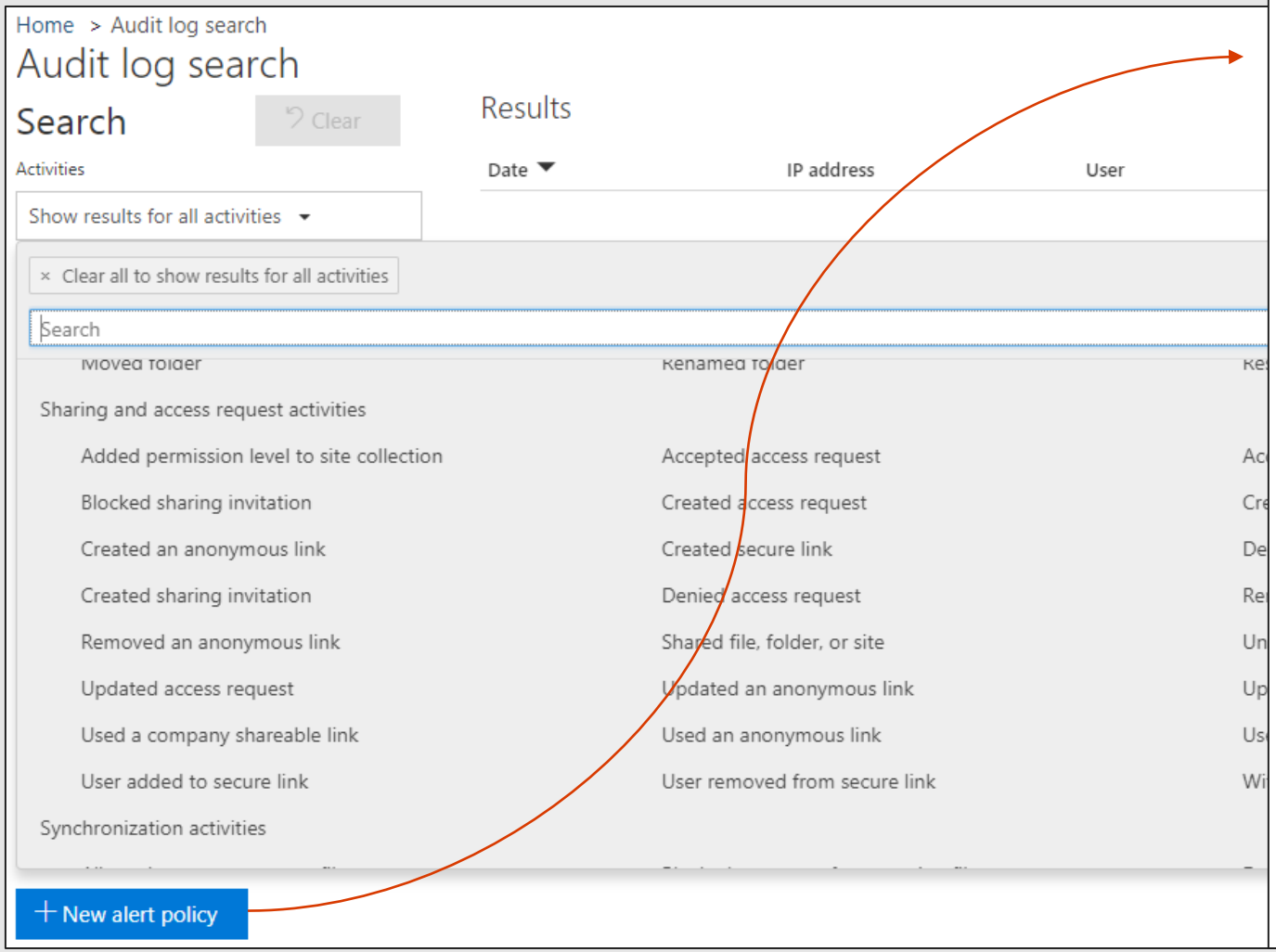
Medium Level - SharePoint

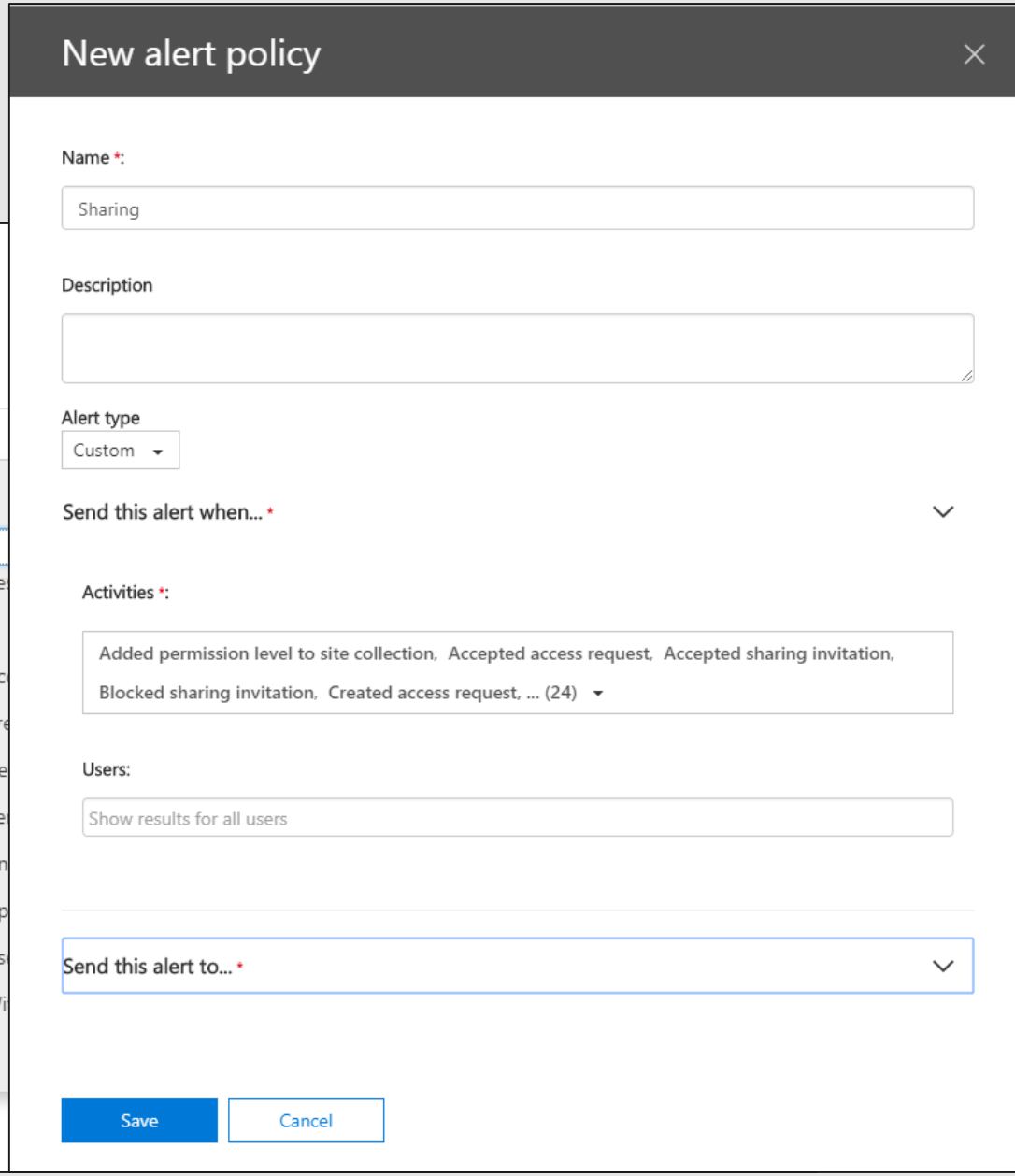
	Setting	Details / Options
SharePoint Online sharing settings	Sharing outside your organization	*Don't allow sharing outside your organization *Allow sharing only with the external users that already exist in your organization's directory *Allow users to invite and share with authenticated external users *Allow sharing to authenticated external users and using anonymous access links **Anonymous access links expire in this many days: **Anonymous access links allow recipients to:
	Who can share outside your organization	*Let only users in selected security groups share with authenticated external users *Let only users in selected security groups share with authenticated external users and using anonymous links
	Default link type	*Direct - specific people *Internal - only people in your organization *Anonymous Access - anyone with the link
	Default link permission	*View *Edit
	Additional settings	*Limit external sharing using domains (applies to all future sharing invitations). Separate multiple domains with spaces. Learn more. *Prevent external users from sharing files, folders, and sites that they don’t own *External users must accept sharing invitations using the same account that the invitations were sent to *Require recipients to continually prove account ownership when they access shared items
	Unmanaged devices	*Allow full access from desktop apps, mobile apps, and the web *Allow limited, web-only access *Block Access
	Control access based on network location	Only allow access from specific IP address locations
	Apps that don't use modern authentication	YES or NO

Medium Level – PowerShell: Set-SPOTenant

	Setting	Details / Options
Useful settings with PowerShell	BccExternalSharingInvitations	All external sharing invitations will be bcc e-mail to:
	BccExternalSharingInvitationsList	All external sharing invitations will be bcc e-mail to:
	DisallowInfectedFileDownload	Prevents the Download button from being displayed on the Virus Found warning page
	NotificationsInSharePointEnabled	
	ODBAccessRequests	Set a policy on re-sharing behavior in OneDrive for Business
	UserVoiceForFeedbackEnabled	

Security & Compliance Center





Medium Level – MFA & MDM

- Multi-factor Authentication for Office 365 users
  - You get a free version of Azure multi-factor authentication as part of your Office 365 subscription.

- Mobile Device Management in Office 365
  - The built-in Mobile Device Management (MDM) for Office 365 helps you secure and manage your users' mobile devices like iPhones, iPads, Androids, and Windows phones.
  - Device management is part of the Security & Compliance Center so you'll need to go there to kick off MDM setup.

Level: High

High - Cloud App Security

Cloud App Security provides access security and auditing at application level.

Integration with DLP and AIP enables extensive data control.

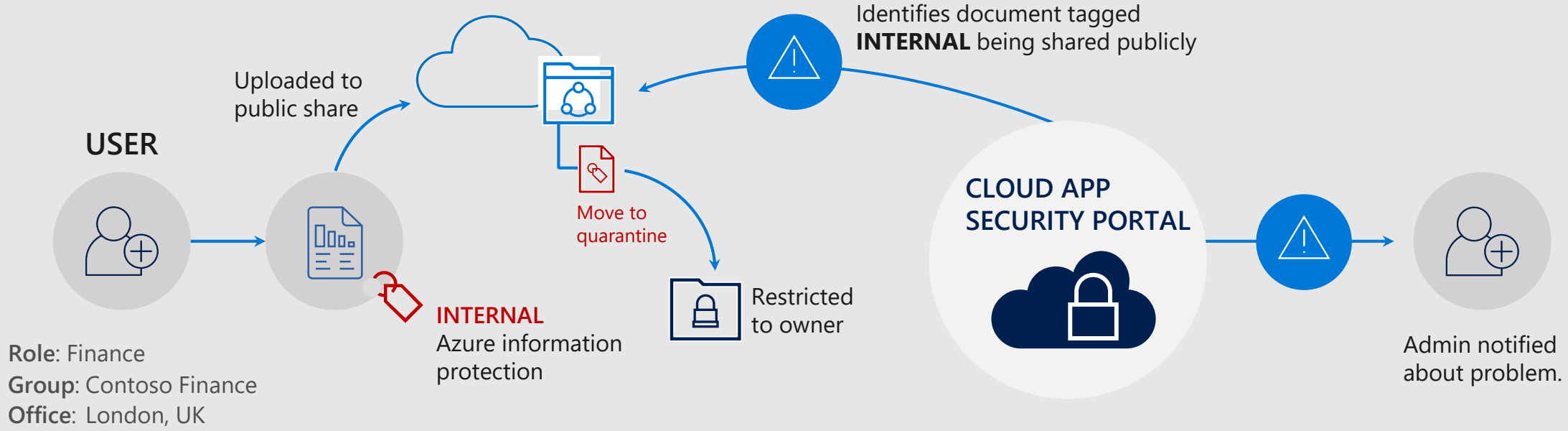
Cloud App Security is availible as:

- Office 365 Cloud App Security
- Microsoft Cloud App Security

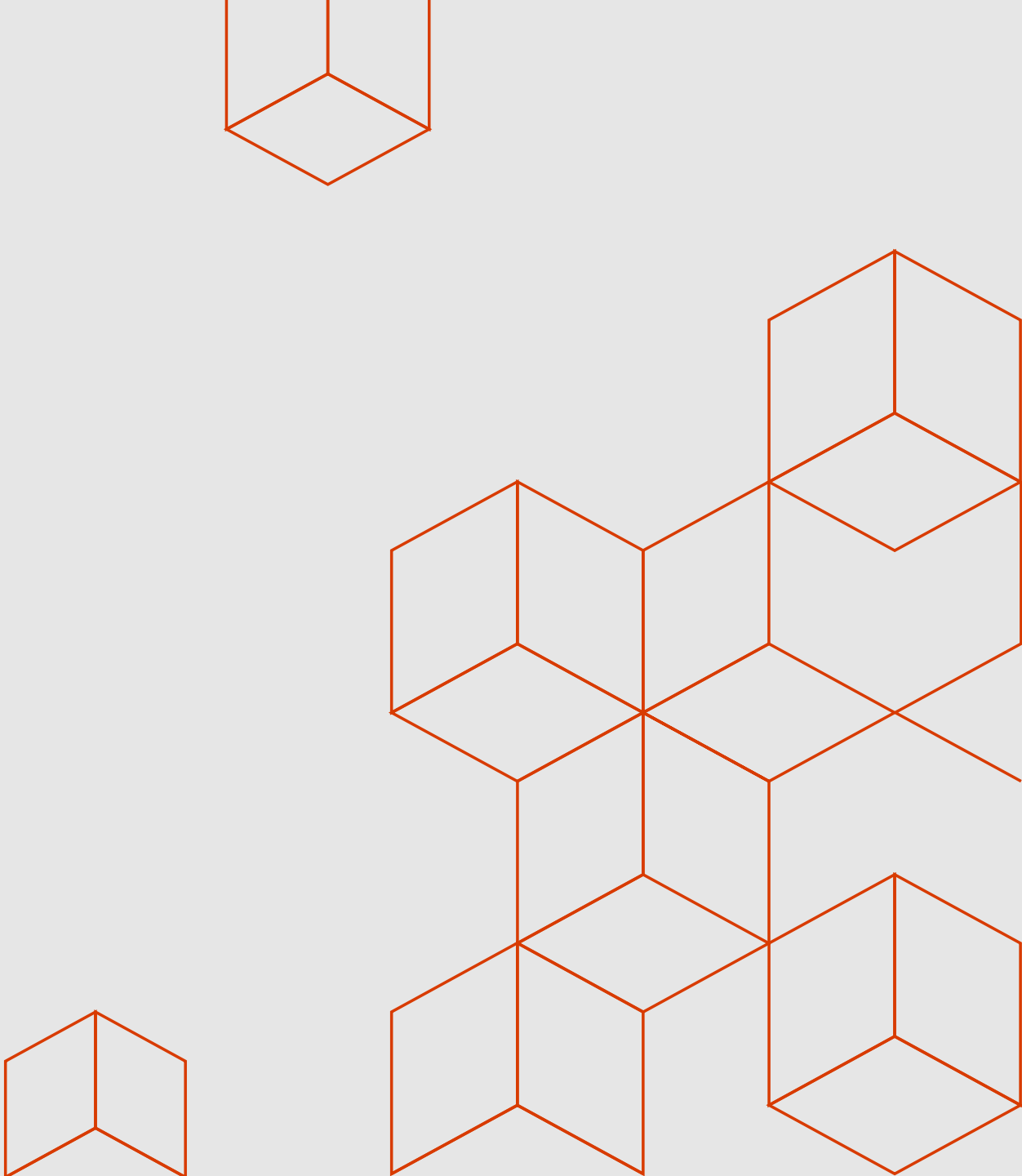
Typical scenarios:

1. Detect threats and automatically take action
2. Protect data and enforce integrated or custom data sharing policies
3. Control access in real time
4. Discovering and assessing risks and Identify cloud apps used on the network.

I want to protect and control data in cloud apps



CAS Demo



High - Azure AD Premium MFA

By default, Office 365 comes with standalone multi-factor authentication options included in user licenses. This is a limited version of MFA and only covers basic functions.

Feature	MFA for Azure AD Administrators	Azure MFA
Protect Azure AD admin accounts with MFA	•	•
Mobile app as a second factor	•	•
Phone call as a second factor	•	•
SMS as a second factor	•	•
App passwords for clients that don't support MFA	•	•
Admin control over verification methods	•	•
Protect non-admin accounts with MFA		•
PIN mode		•
Fraud alert		•
MFA Reports		•
One-Time Bypass		•
Custom greetings for phone calls		•
Custom caller ID for phone calls		•
Trusted IPs		•
Remember MFA for trusted devices	•	•
MFA SDK		•
MFA for on-premises applications		•

Level: Very High

Very High – Microsoft Intune

Intune helps enable your workforce to be productive while keeping your corporate data protected. With Intune, you can:

- Manage the mobile devices & apps
- Protect information by controlling how it is accesses and shares
- Ensure devices and apps are compliant

By default, Office 365 comes with standalone options for managing mobile devices and mobile access that are included in user licenses. This is a limited version of MDM and only covers basic functions.

Very High – Microsoft Intune vs. MDM for Office 365

Functional area	MDM for Office 365	Microsoft Intune
Device management	Devices are managed through the Security and Compliance Center in Office 365.	Intune management console in Azure or integration in System Center
Manageable devices	Cloud-based management iOS, Android and Windows devices.	Cloud-based management for iOS, Mac OS X, Android, Windows 8.1 (phone and computer) and later included in Windows 10
Important functions	• Ensure that corporate e-mail and documents in Office 365 can only be accessed from smartphones and tablets that are managed by the company and fit to IT policies. • Set and manage security policies such as device-level PIN locking and jailbreak detection to prevent unauthorized users from accessing corporate email and data from a device if it is lost or stolen. • Remove company data from an employee's device while preserving personal data.	MDM for Office 365 functions and the following additional functions: • Secure user access to corporate resources with certificates, Wi-Fi, VPN and email profiles • Register and manage company devices to deploy policies and apps • Providing Apps for Users • More secure access to corporate data while ensuring data security by limiting actions such as "Copy", "Cut", "Paste" and "Save As" to Apps managed by Intune. • Manage PCs, Macs, Linux and UNIX servers, and mobile devices

Very High – Microsoft Intune & MAM

MAM (Mobile Application Management) and MDM (Mobile Device Management) are usually combined. The two solutions can be distinguished as follows:

- MDM: addresses lack of control over corporate and personal devices, and lost device security
  - Ensures device compliance through user and device registration, configuration and passcode management
  - Secures devices on the network so you can monitor, report, track and update devices – and even locate, lock and wipe devices, if lost or stolen

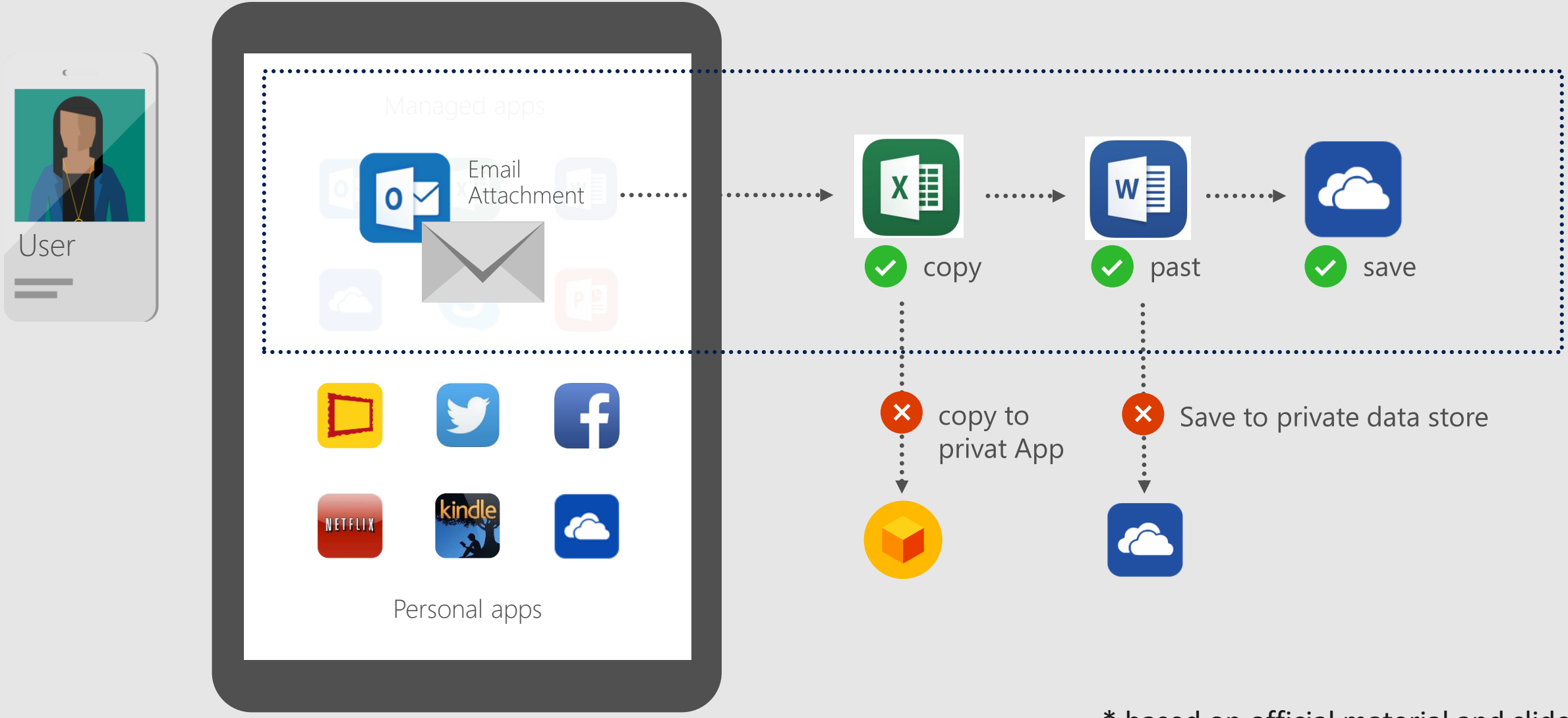
- MAM: addresses lack of compliance with data and privacy requirements, and lost data retrieval
  - User identity policy, single sign-on and conditional access tailored by role and device (with Intune or Active Directory on premises or in the cloud)
  - Monitors and pushes App updates, including mobile document management for online or cloud-provisioned apps like SharePoint and OneDrive

With Azure AD Premium you have the option to combine MAM and MDM (Intune) or to use MAM without MDM (Intune) or MDM with a 3rd party solution.

Device & Application Management*

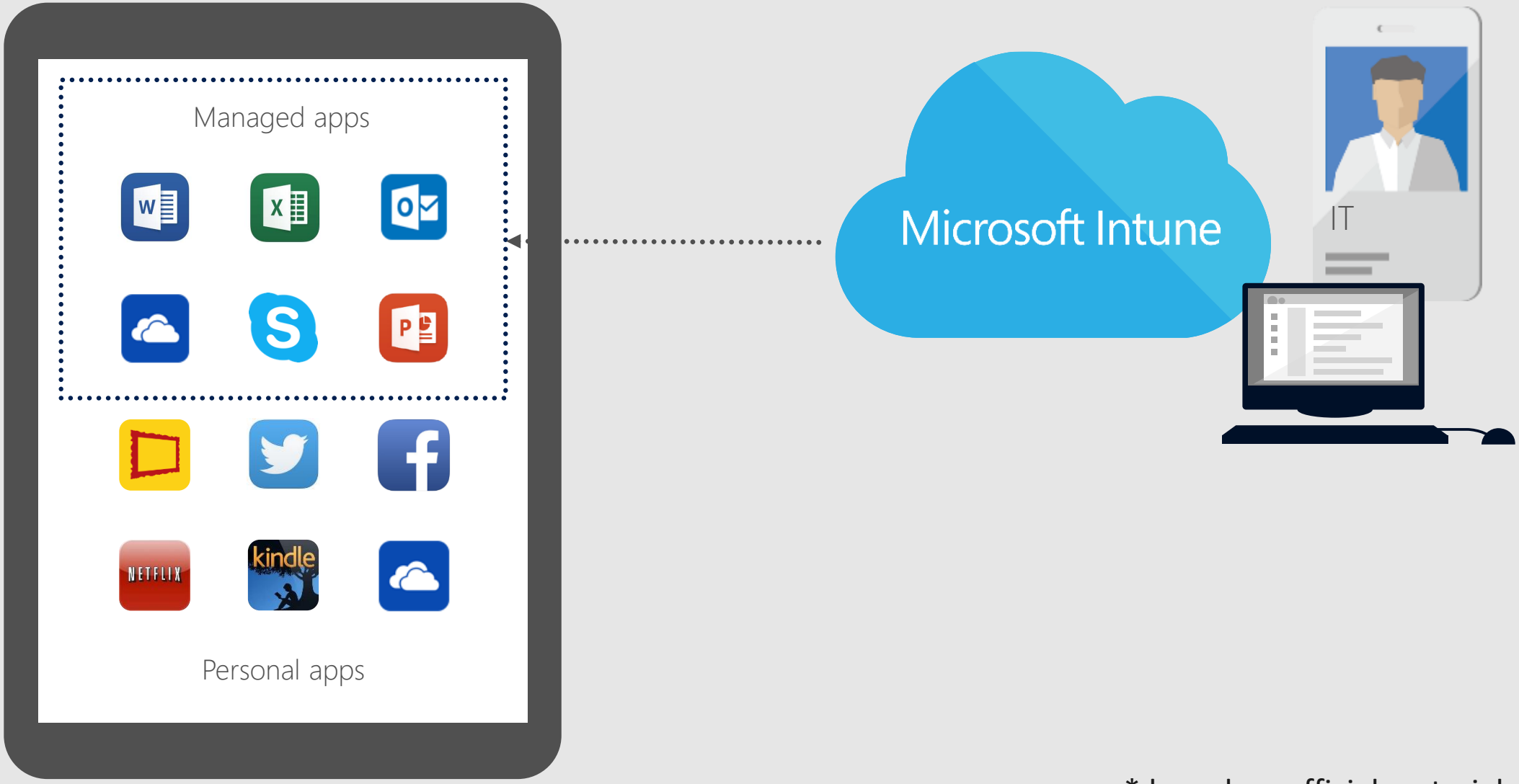
* based on official material and slides

Device & Application Management*



* based on official material and slides

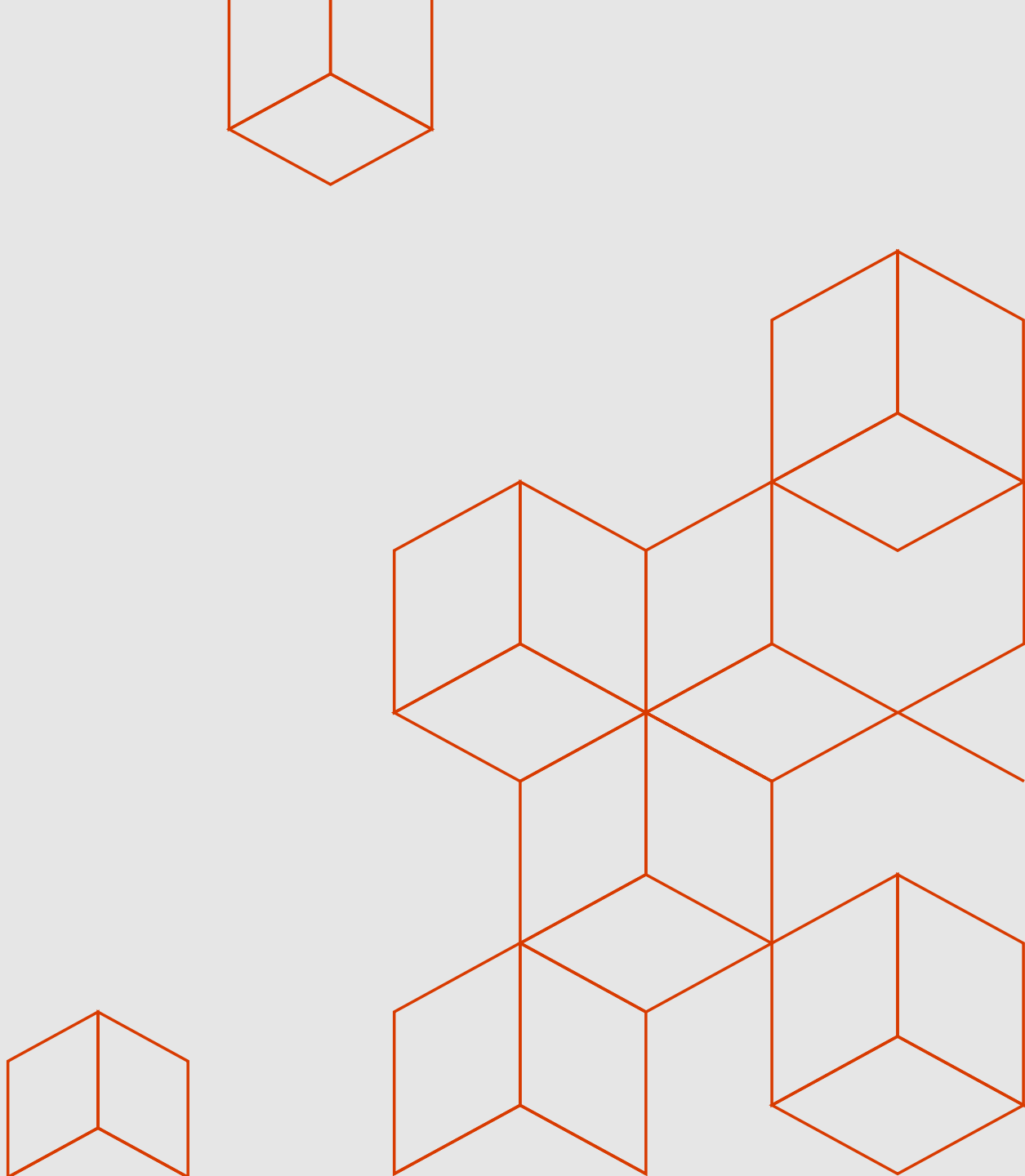
Device & Application Management*



* based on official material and slides

DEMO

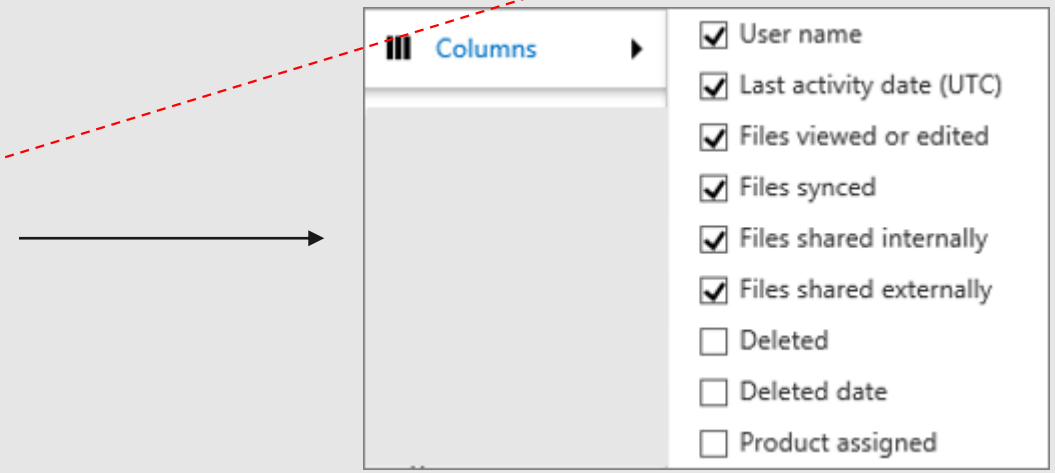
Cloud App Security
Azure Active Directory
Microsoft Intune



Roundup & usefull links

1. Download “A quick guide to secure Office 365” https://bit.ly/2x9iRA7
2. Talk to your process owners and decision maker about the sharing scenarios they have
3. Talk to your data security officer about his needs
4. Use the matrix “A quick guide to secure Office 365” to fined the features and licenses you need
5. Monitor what's going on in your Office 365
6. Use the help Microsoft provides:
   - Azure Security Documentation
   - Office 365 Security Assessment IPKit v1.1
   - Shadow IT Assessment-Questionnaire-v1.0.docx
   - Secure Score Scanner
   - Azure Security Center

…and if you need help – drop me a mail!



Q&A