Microsoft 365

Technologie Workshop

Agenda

1	2	3	4
Vorstellungsrunde & Erwartungshaltung	SVA Vorgehen	Microsoft 365	Fragen & Antworten Nächste Schritte

Vorstellungsrunde & Erwartungshaltung

Max Mustermann

Titel

Über mich

Vorstellung

Hier steht ein kurzer Satz über sich selbst als Spezialist oder ein nettes Zitat oder etwas das zu dem Vortrag passt Hier steht ein kurzer Satz über sich selbst als Spezialist oder ein nettes Zitat oder etwas das zu dem Vortrag passt

Platzhalter für ein Badge einer Mitgliedschaft (z.B. bikom) oder eines Zertifikats (z.B. Scrum Master). Falls nicht benötigt/vorhanden bitte löschen

Platzhalter für ein Badge einer Mitgliedschaft (z.B. bikom) oder eines Zertifikats (z.B. Scrum Master). Falls nicht benötigt/vorhanden bitte löschen

Microsoft Solutions Partner
Modern Work

Vorstellung

Microsoft Solutions Partner
Modern Work

Max Mustermann
Titel

+49 176 12 34 56 78
Max.mustermann@sva.de
www.sva.de

Standort Wiesbaden
Borsigstraße 26
65205 Wiesbaden

Max Mustermann
Titel

+49 176 12 34 56 78
Max.mustermann@sva.de
www.sva.de

Standort Wiesbaden
Borsigstraße 26
65205 Wiesbaden

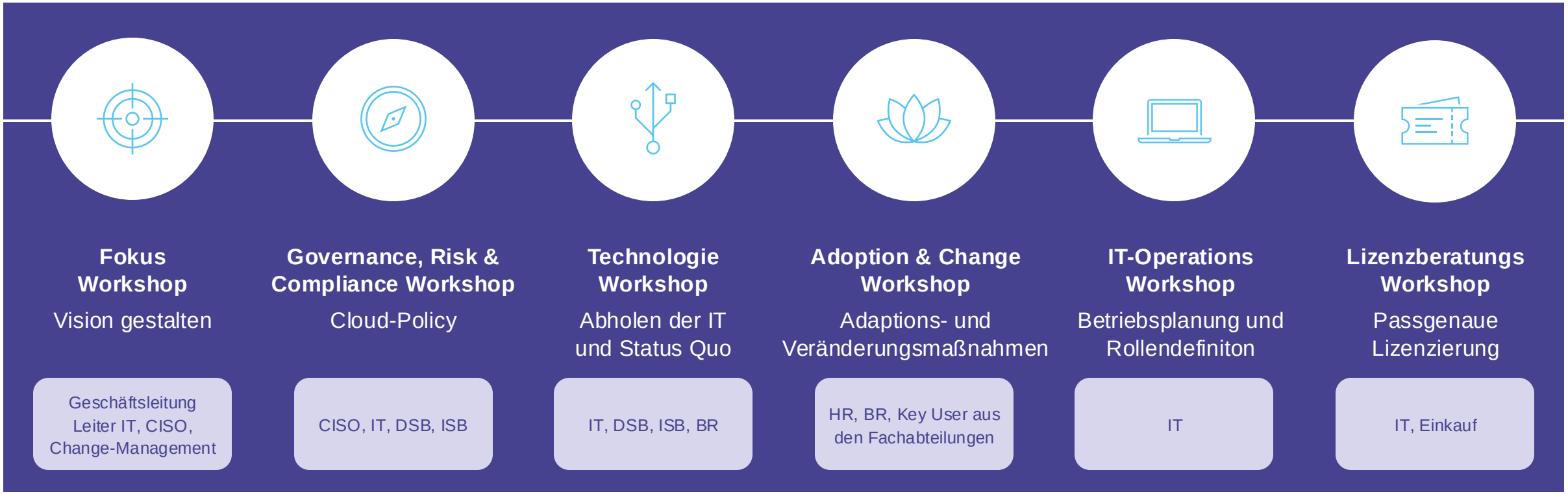
Workshop Ziele

- Gemeinsames Verständnis
- Diskussion auf Augenhöhe
- Möglichkeiten kennenlernen
- Scoping und Big Picture
- Umfang des Umsetzungsprojektes

Microsoft 365

SVA Vorgehen

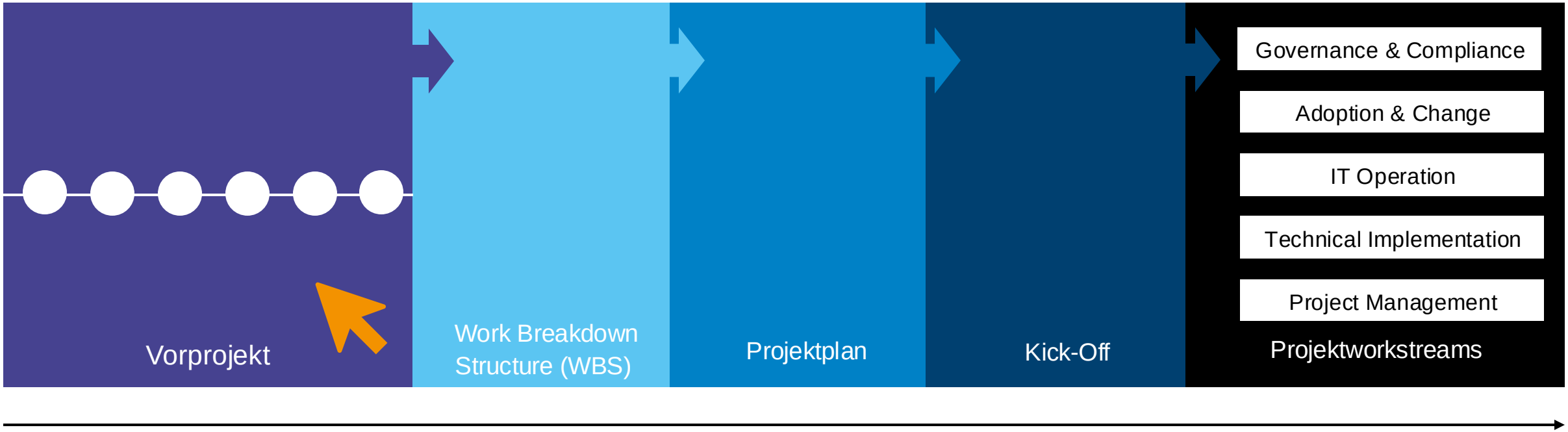
Vorprojekt



Planungsworkshop und Ergebnispräsentation

Work Breakdown Structure (WBS)

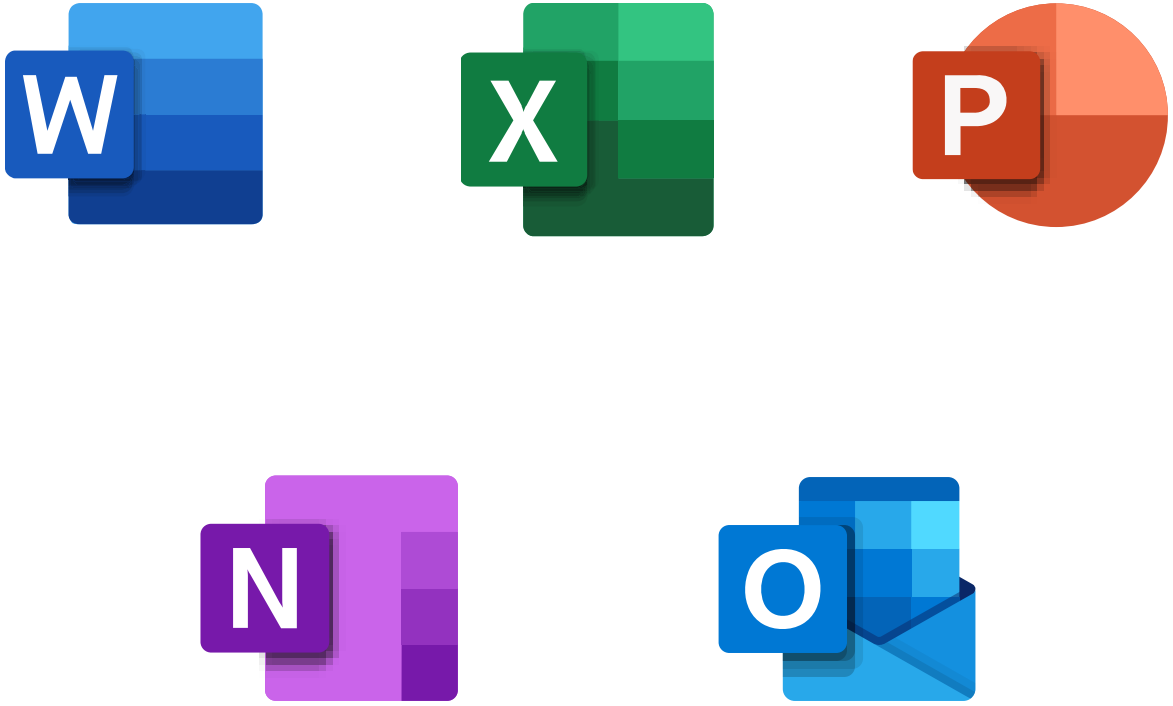
Schritt für Schritt



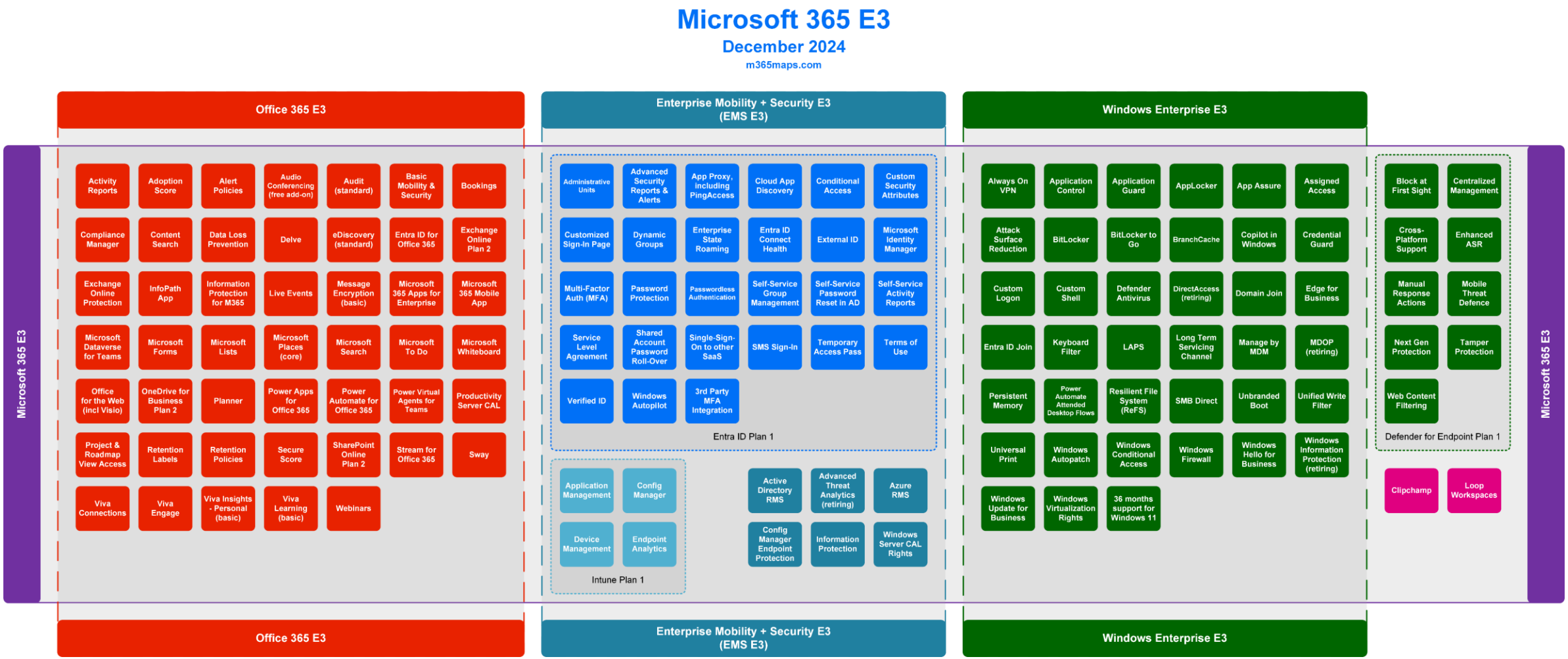
Microsoft 365

Überblick
Identitäten, Geräte
Kommunikation, Kollaboration
Sicherheit, Compliance

Microsoft Office früher…



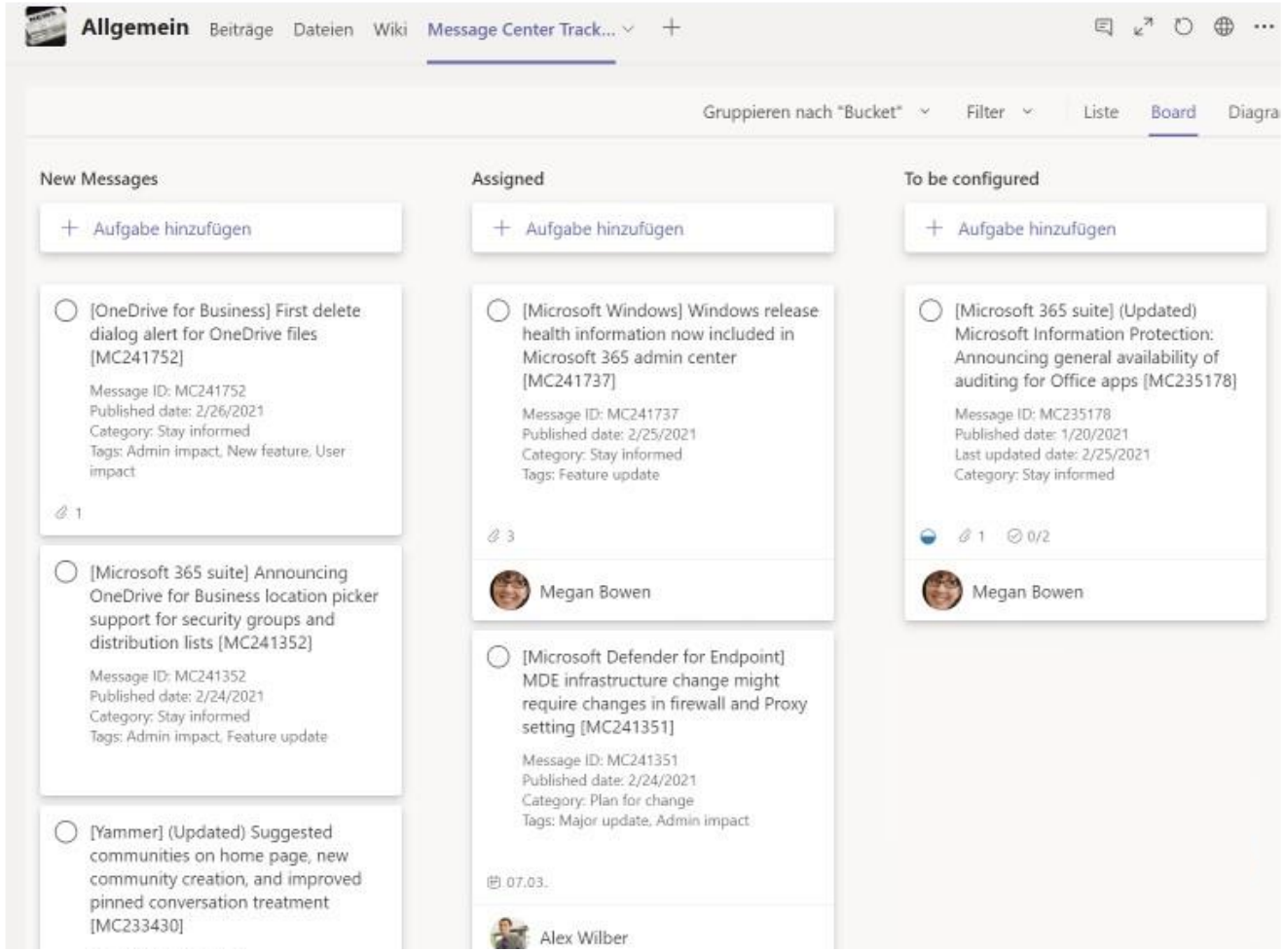
…und Microsoft 365 heute



Der Evergreen Ansatz in Microsoft 365

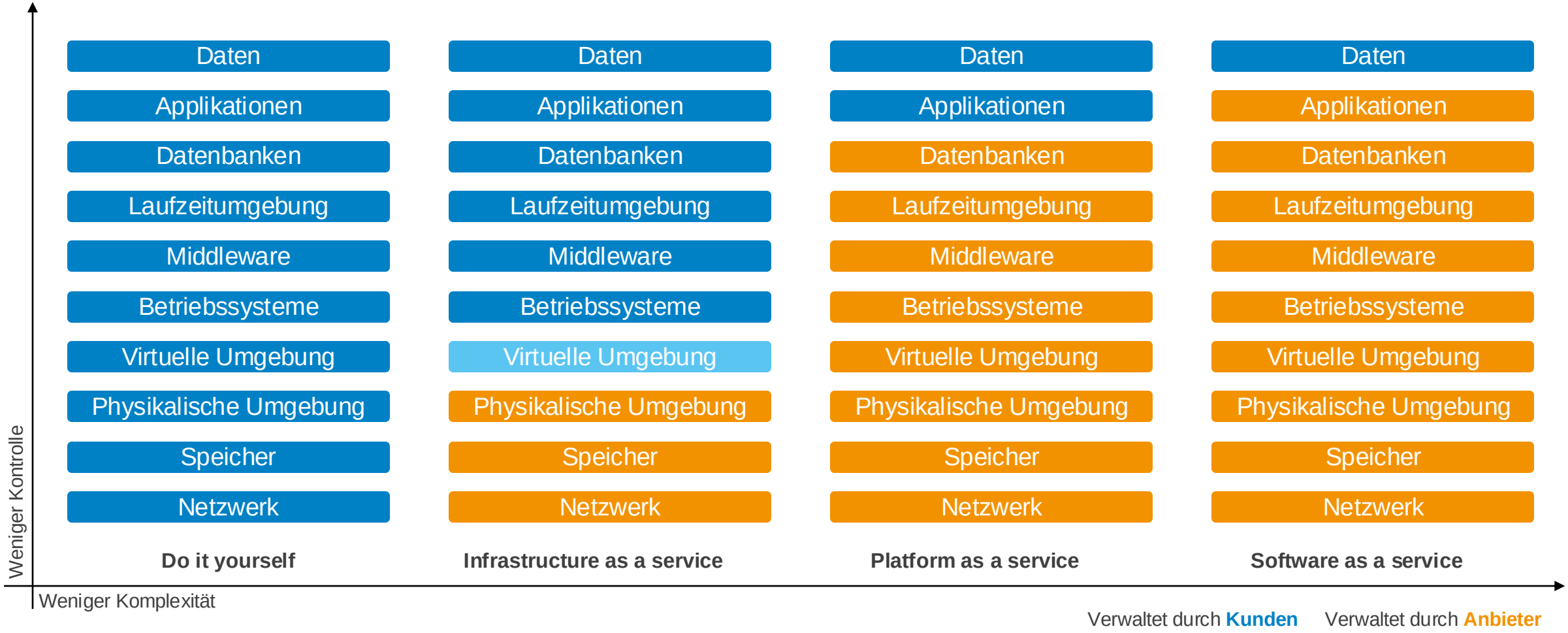
- Cloud-Dienste werden stetig aktualisiert
  - Keine „echten“ Major Releases
- Neue Funktionen werden automatisch verteilt und aktiviert
  - Herausforderung: Nutzer & IT vor Überraschungen schützen
- Neue Anforderung an hybride Umgebungen
  - Version „N-1“
- Test Tenant verwenden um Auswirkungen von (neuen) Einstellungen zu testen
- „Mitspracherecht“ aller Nutzer über Feedback Funktionen und Portale
  - https://feedbackportal.microsoft.com/feedback

Microsoft 365 Roadmap



- Microsoft 365 Message Center für alle detaillierten Neuerungen
  - Message center - Microsoft 365 admin center
- Roadmap, öffentlich verfügbar, allgemeiner Überblick
  - Microsoft 365 Roadmap | Microsoft 365
- Status der Dienste kann überwacht werden
  - Microsoft 365 Health Monitor
  - Service health - Microsoft 365 admin center

Cloud Service Modelle



Shared Responsibility und neuer Blickwinkel

- Die IT Umgebung steht nicht mehr (nur) im eigenen RZ, gesichert durch eine Firewall
- Durch die Nutzung von Cloud Services befinden sich die Identitäten außerhalb des Netzwerks

  → Schutz der Identitäten und Daten wird wichtiger

- Informationen und Daten werden vermehrt außerhalb des Unternehmens geteilt
- Herkömmliche Berechtigungsstrukturen verlieren ihre Wirkung

  → Kontrolle über Identitäten und Daten gewinnen

- 4 Dimensionen von „Daten“: Identitäten, Geräte, (Nutz-)Daten, Anwendungen

- Weitere Informationen: Gemeinsame Verantwortung in der Cloud
  https://docs.microsoft.com/de-de/azure/security/fundamentals/shared-responsibility

Glossar

Azure Virtual Datacenter
(IaaS, PaaS)
Azure Plan (pay as you go)

Microsoft 365 (SaaS)
Subscription (pro Nutzer & Monat)

Dynamics 365 (SaaS)
Subscription (pro Nutzer & Monat)

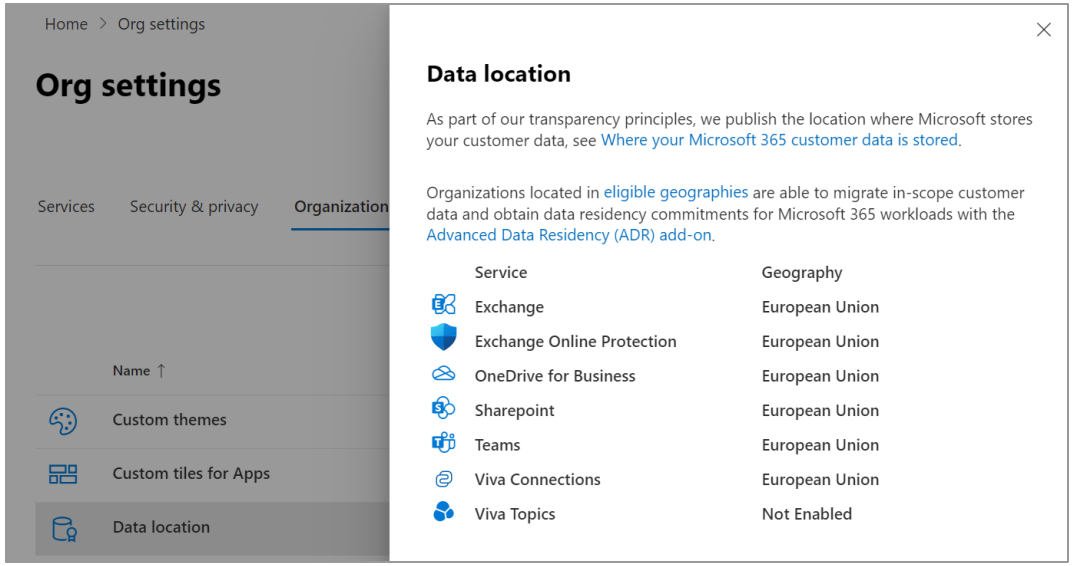
Security & Compliance Tools

Power Platform

Microsoft Tenant (xyz.onmicrosoft.com) & Entra ID

Microsoft 365 Datenspeicherorte

- „Data at rest“ sind immer mit dem Microsoft Managed Key verschlüsselt
- Rechenzentren werden beim Erstellen des Tenant automatisch ausgewählt
  anhand der Kundenadresse und Kapazität
- Der Ablageort ist im M365 Admin Center einsehbar
- Ablageorte der weiteren Dienste sind online dokumentiert.
- Ein kostenfreier Umzug in die deutschen Rechenzentren ist nicht mehr möglich!
- Die EU Data Boundary sorgt dafür, dass Daten nicht außerhalb der EU transferiert werden und wird seit 2022 sukzessive ausgerollt.



Netzwerk

Netzwerk

- Nutzdaten werden immer verschlüsselt zu Microsoft 365 übertragen
- Microsoft Global Network
  - Eigene Dark Fibre Verbindungen weltweit
  - > 2700 direkte Provider-Peerings
- „Front Doors“
  - als Einstieg in das Microsoft Netzwerk
  - werden über DNS ermittelt

- Microsoft Best Practices
  - Lokale WAN Breakouts
  - Split Client-VPN
  - Keine Proxy-Server einsetzen
  - URLs, IPs, Ports gemäß Artikel freischalten
    - Weitere Ausnahmen für spezielle Dienste wie Entra ID Connect, Hybrid Join …

Netzwerk

Volle Kontrolle & Verantwortung

Oft hohe Kosten für WAN Verbindungen

Kaum Kontrolle

ISP Wahl

Höhere Bandbreiten zu geringeren Kosten

Das ist nicht der Zugriffsweg für M365 Dienste

Firmen Netzwerk → Internet

Volle Kontrolle & Verantwortung

Oft hohe Kosten für WAN Verbindungen

Kaum Kontrolle

ISP Wahl

Höhere Bandbreiten zu geringeren Kosten

0 Jitter & Verluste

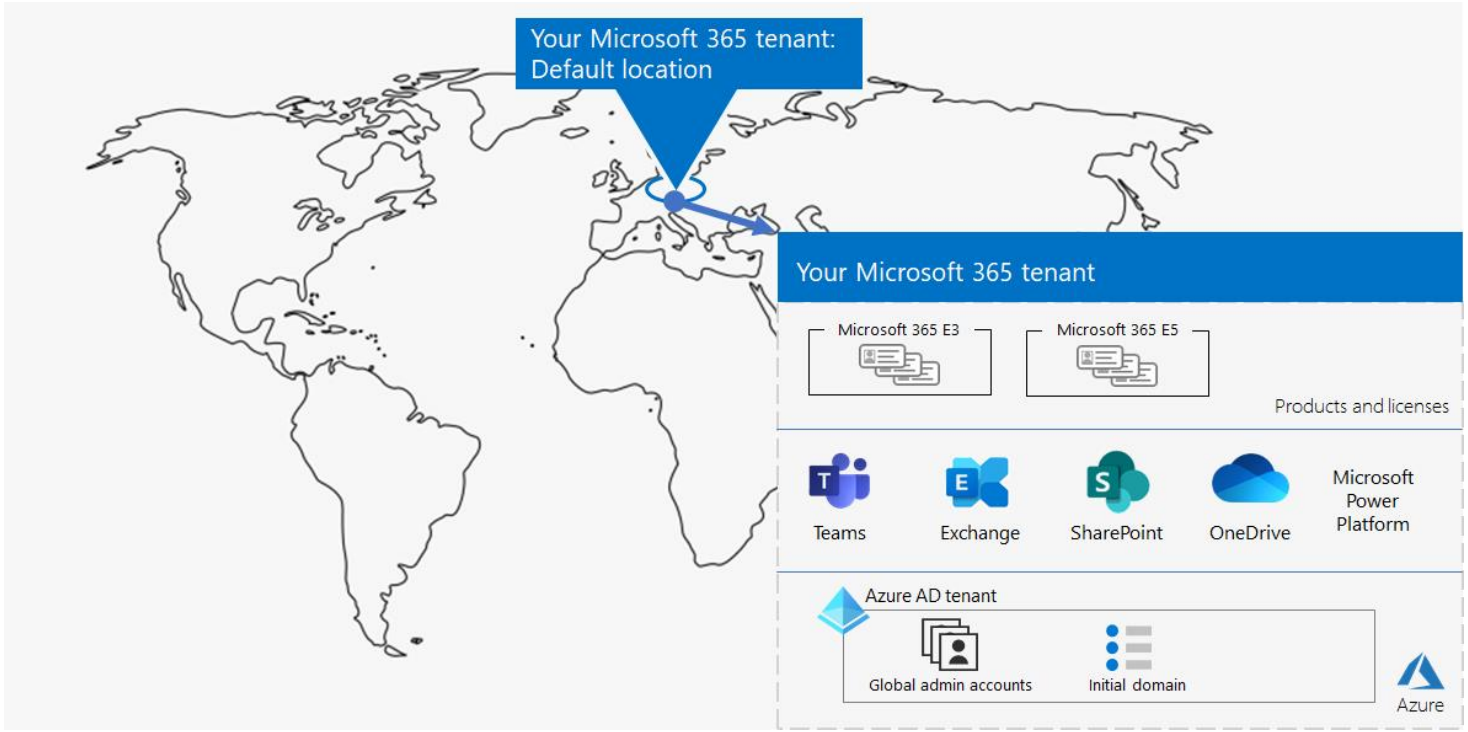
Latenz ergibt sich nur durch Entfernung & Lichtgeschwindigkeit

Teil von Microsoft 365 & Azure

Firmen Netzwerk → Internet → MS Netzwerk

Netzwerk Check

- Quick Check
  - https://connectivity.office.com/
- Ende-zu-Ende Betrachtung
  - Switches etc. auf Kapazitäten prüfen
- SVA-Empfehlung
  - LAN/WAN-Assessment durchführen



Backup

Warum eine zusätzliche Backup-Lösung?

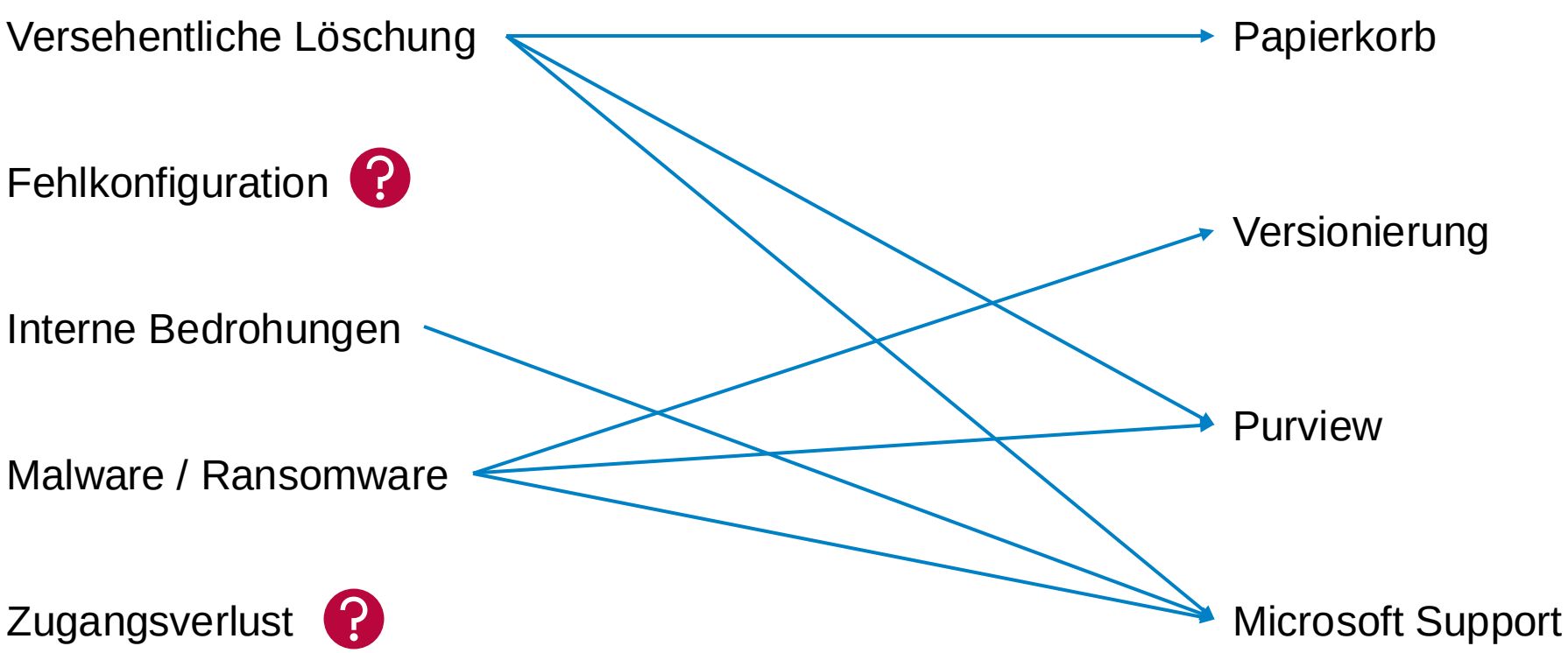
Unbeabsichtigte Löschung	• Falsche Taste gedrückt; falsche Daten hervorgehoben • Anwendungen von Drittanbietern, die sich mit Ihren Daten verbinden (z. B. ein E-Mail-Programm, das auf die falsche Weise synchronisiert)
Fehlkonfiguration	• Tippfehler in einem Skript • Unbeabsichtigte Nebeneffekte von neuen Funktionen/Aktualisierungen
Beabsichtigte Löschung	• Kompromittierter Mitarbeiter • Verärgerter Administrator
Malware/Ransomware	• Verschlüsselung von Daten • Beschädigung von Daten
Verlust des Zugangs	• Ausfall von Diensten Aussperrung durch Hackerangriff

Bordmittel in Microsoft 365

Microsoft erstellt keine vollständigen Daten-Backups mit Ausnahme von SharePoint Online

Dienst	Lösung	Standardwert	Maximal
Exchange Online	Gelöschte Elemente	unlimitiert	unlimitiert
Exchange Online	Wiederherstellbare Elemente	14 Tage	30 Tage
Share Point / One Drive	Site (Collection) Recycle Bin	93 Tage	93 Tage

Welche Lösung für welche Bedrohung?



Microsoft 365 Backups – ja oder nein?

- Lizenzen
- Infrastruktur
- Verwaltungskosten

- Betriebsausfallzeit
- Verlust des Versicherungsschutzes
- Ransomgelder
- Firmenruf

M365 Backup | Fragestellungen

- Welche Dienste sollen abgesichert werden?
  - Exchange Online, SharePoint Online, Teams …
- Wo sollen die Backups abgelegt werden?
  - Gleiche Cloud, Andere Cloud, Lokaler Storage?
- Wie oft werden Backups erstellt? Wie lange darf ein Service ausfallen?
  - „Recovery Point Objective“ (RPO)?
  - „Recovery Time Objective“ (RTO)?
- Aufbewahrungszeitraum?

Microsoft 365 Backup Deployment Modelle

Server-basiert (on-premises)

- Hardware (Cap-Ex) & Betriebskosten (Op-Ex)
- Engpässe immer möglich (LTO-Bänder, Storage usw.)
- Kann meistens mehr sichern (on-prem VMs, SQL, SAN, usw.)

Server-basiert (in the cloud/IaaS)

- Nur Betriebskosten (Op-Ex) ABER...
- nicht so einfach berechenbar wie bei SaaS Services (VMs, Storage, etc. muss man selber bezahlen)

Backup as a Service (BaaS)

- Nur Betriebskosten (Op-Ex)
- Software as a Service (SaaS) für Datensicherung und Notfallwiederherstellung
- In der Regel unbegrenzte Speicherkapazität

Managed Service

- BaaS von SVA gemanaged
- 2 Angebote
- Private Cloud möglich

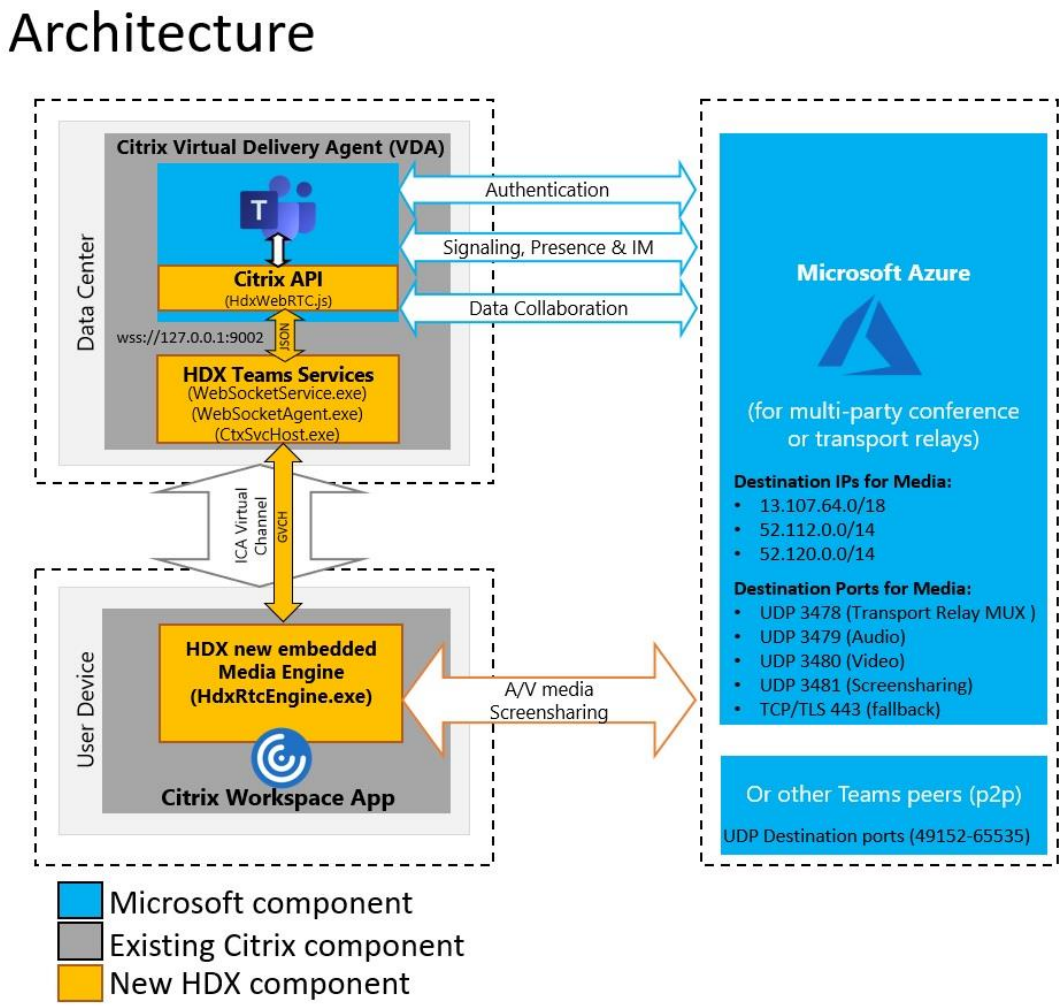
Teams und VDI / RDSH

Microsoft 365 & Citrix

Der Einsatz von Microsoft 365 Diensten auf Citrix Systemen bedarf einer umfassenden Planung.

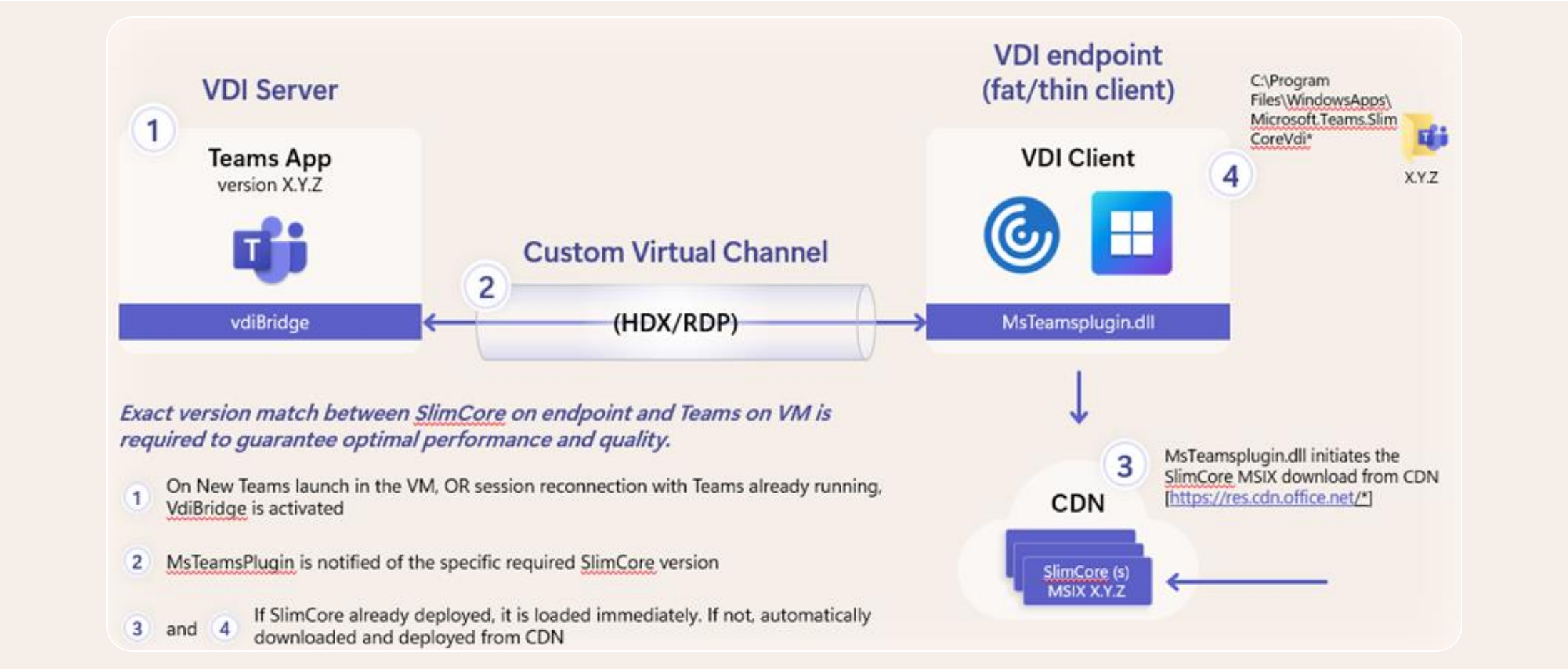
- Optimaler Support der Dienste erst ab Windows Server 2019 / Windows 10
- FSLOGIX Profilcontainer
  - Outlook.ost, OneDrive Cache
  - Limitierungen beachten!
- Apps for Enterprise
  - Shared Computer Activation
  - Lizenztoken
- Hybrid Entra ID Join für Citrix Worker
  - Persistent / Non-Persistent Worker müssen unterschiedlich berücksichtigt werden
  - Besondere Berücksichtigung in Conditional Access
- Teams
  - „Machinewide Installer“ verwenden, regelmäßige Aktualisierung muss manuell erfolgen!
  - Aktuellste Versionen einsetzen für Offloading
  - Limitierungen in Teams Meetings beachten & kommunizieren
  - Rechenleistung der Hardware berücksichtigen – GPU!
  - Session-Dichte wird reduziert

Citrix und Teams



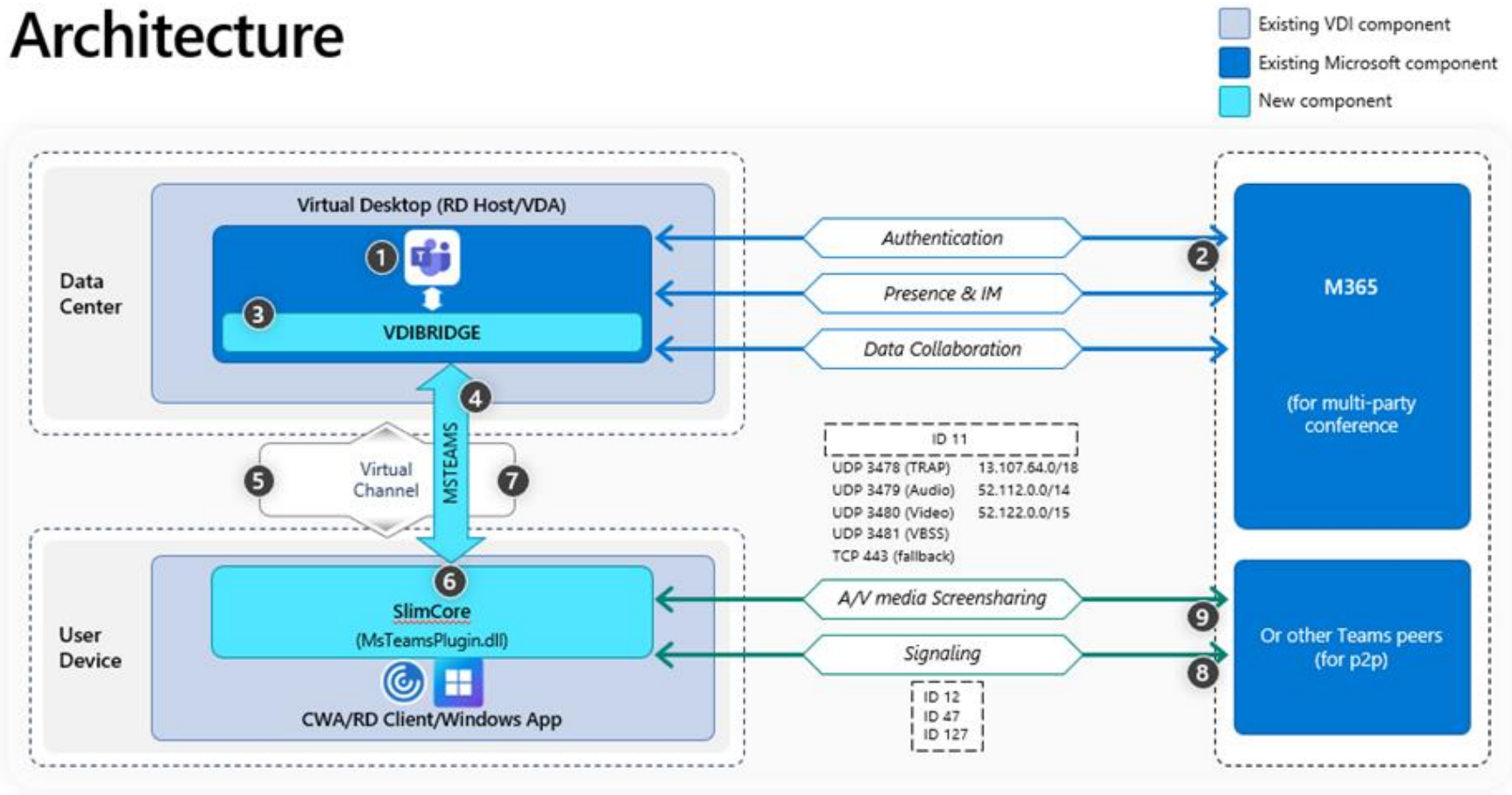
Quelle: https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html

Teams und VDI – neu ab ca. H2 / 2024



Quelle: https://techcommunity.microsoft.com/t5/microsoft-teams-blog/the-future-of-microsoft-teams-in-vdi/ba-p/4175859

Teams und VDI – neu ab ca. H2 / 2024



Quelle: https://techcommunity.microsoft.com/t5/microsoft-teams-blog/the-future-of-microsoft-teams-in-vdi/ba-p/4175859

Lizenzen

Business vs. Enterprise

Business

- Limitiert auf 300 Nutzer je Plan
- Ersetzen keine on-premises CALs für Exchange/SharePoint/Skype for Business
- Shared Computer Activation nur in Business Premium

Limitierungen der Business Pläne:

- Keine Gruppenrichtlinien / Intune Konfiguration in Apps for Business
- Cloud Policy Service ist beschränkt auf Datenschutzeinstellungen
- In Teams ist „Öffnen in App“ nicht als Standard Option verfügbar
- Keine zentralen Office Add Ins
- Dokumentenklassifizierung ist nur manuell möglich und nur in Business Premium

Enterprise

- Keine Nutzerlimitierung
- Pläne können on-premises CALs ersetzen
- Shared Computer Activation ist eingeschlossen

Weitere Informationen zu Einschränkungen:
https://docs.microsoft.com/de-de/office365/servicedescriptions/office-applications-service-description/office-applications-service-description

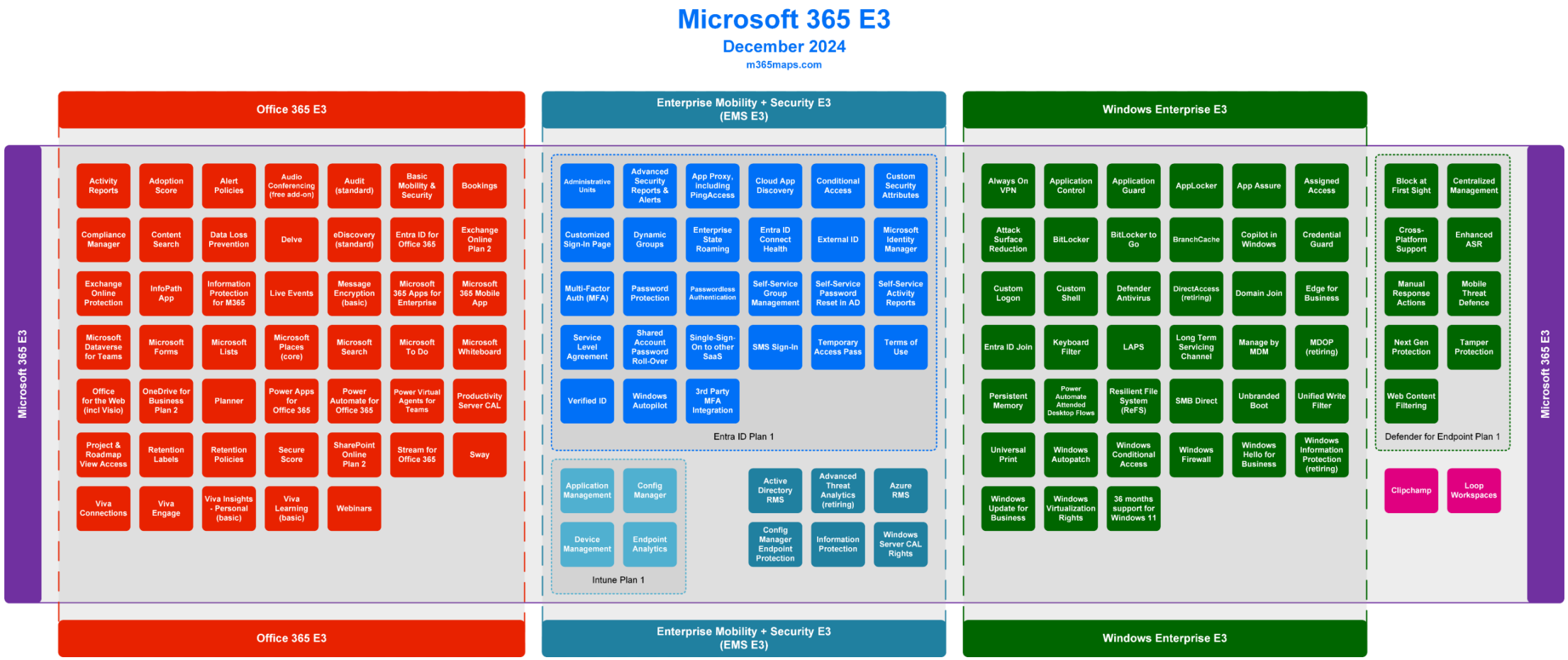
Office LTSC vs. Apps for Business/Enterprise

- Keine Aktivierung auf mehreren Arbeitsumgebungen
- Echte Zusammenarbeit nur in Word
- @-Erwähnungen nur in Word
- Änderungen während der Abwesenheit werden nicht angezeigt
- Viele neue Funktionen zur Unterstützung bei der Erstellung sind nicht vorhanden (eingebettete Animationen, Designs)
- Eingeschränkte Compliance Funktionen z. B. bei Sensitivity Labels

- Detaillierte Übersicht der Unterschiede:
  https://www.microsoft.com/en-ww/microsoft-365/enterprise/microsoft-365-apps-for-enterprise

- Office 2021 wird bis Oktober 2026 für den Zugriff auf M365-Dienste unterstützt:
  https://docs.microsoft.com/en-us/deployoffice/endofsupport/microsoft-365-services-connectivity

Lizenzübersicht



Modern Work Plan Vergleich der Microsoft: https://www.microsoft.com/de-de/microsoft-365/enterprise/microsoft365-plans-and-pricing?market=de

Der Weg zur Lizenzierung

Kriterien für die Vertrags- und Produktauswahl

- Nutzungsszenarien & funktionale Anforderungen
- Cloud Strategie
- Vorhandene Verträge & Lizenzen
- Erfordernis von Software Assurance
- Standardisierung
- Budget, Zahlungsoptionen und Preisschutz
- Vertragslaufzeit und gewünschte Flexibilität
- Einsatzgebiete (EU, weltweit…)
- Lizenzmetrik (per User, per Device, …)

- CSP Modell „New Commerce Experience“
- Seit Juli 2022 nur noch „NCE“
- Abo-Laufzeiten 1 / 12 / 36 Monate
- Monatliche Laufzeit mit Aufpreis
- Add-Ons ausschließlich 12 Monate
- Storno nur innerhalb von 7 Tagen
- Kein Windows-Downgrade-Recht
- Keine SA-Services
- Keine Office-Server bei M365-Plänen
- Virtuelle Clients nur auf Azure & QMTH

Technische Reihenfolge

Für die optimale Nutzung der Microsoft 365 Dienste ergeben sich Abhängigkeiten.

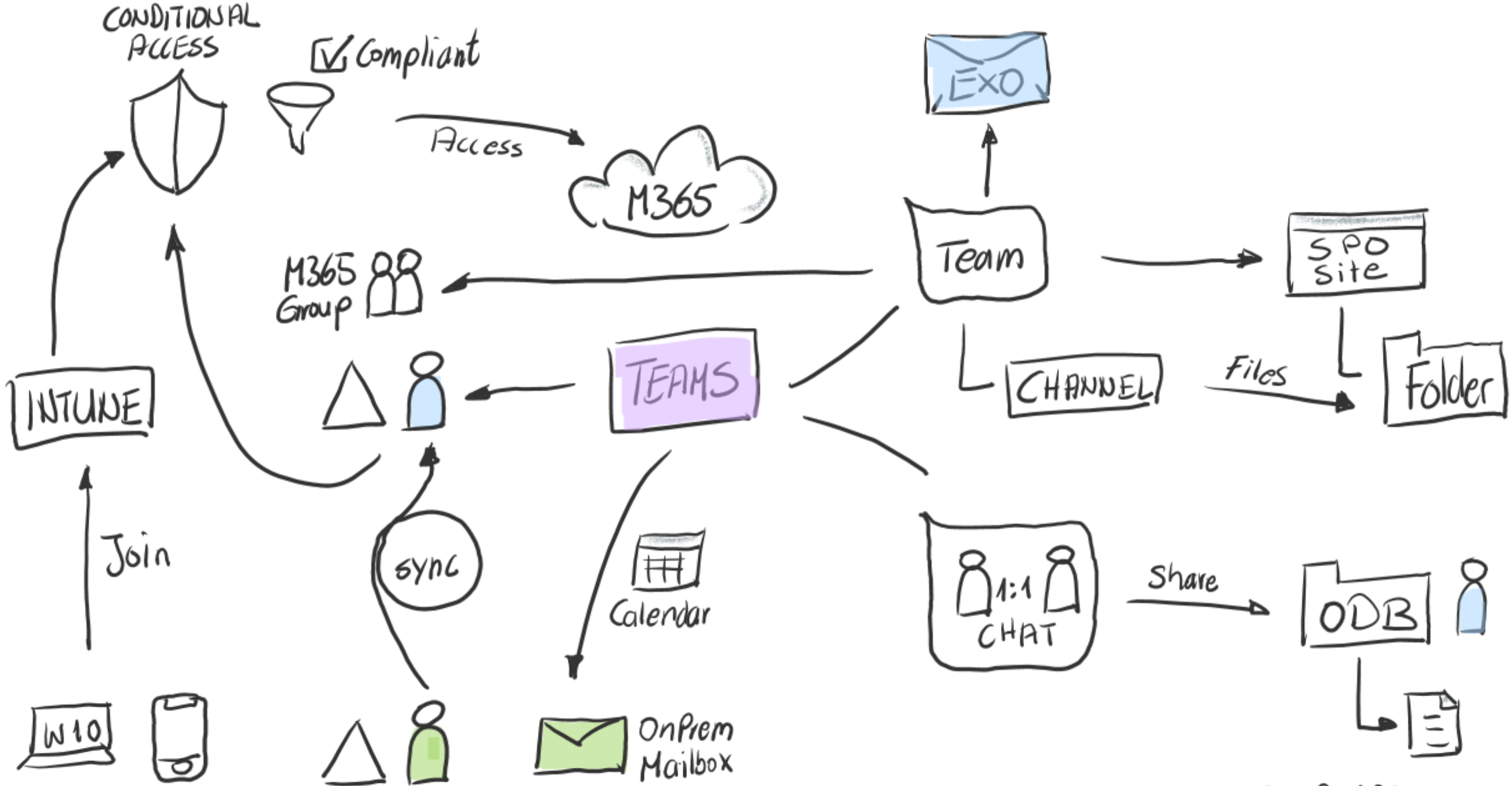
Daher empfehlen wir die folgende Vorgehensweise:

Identity
Devices
Security

Exchange
Hybrid

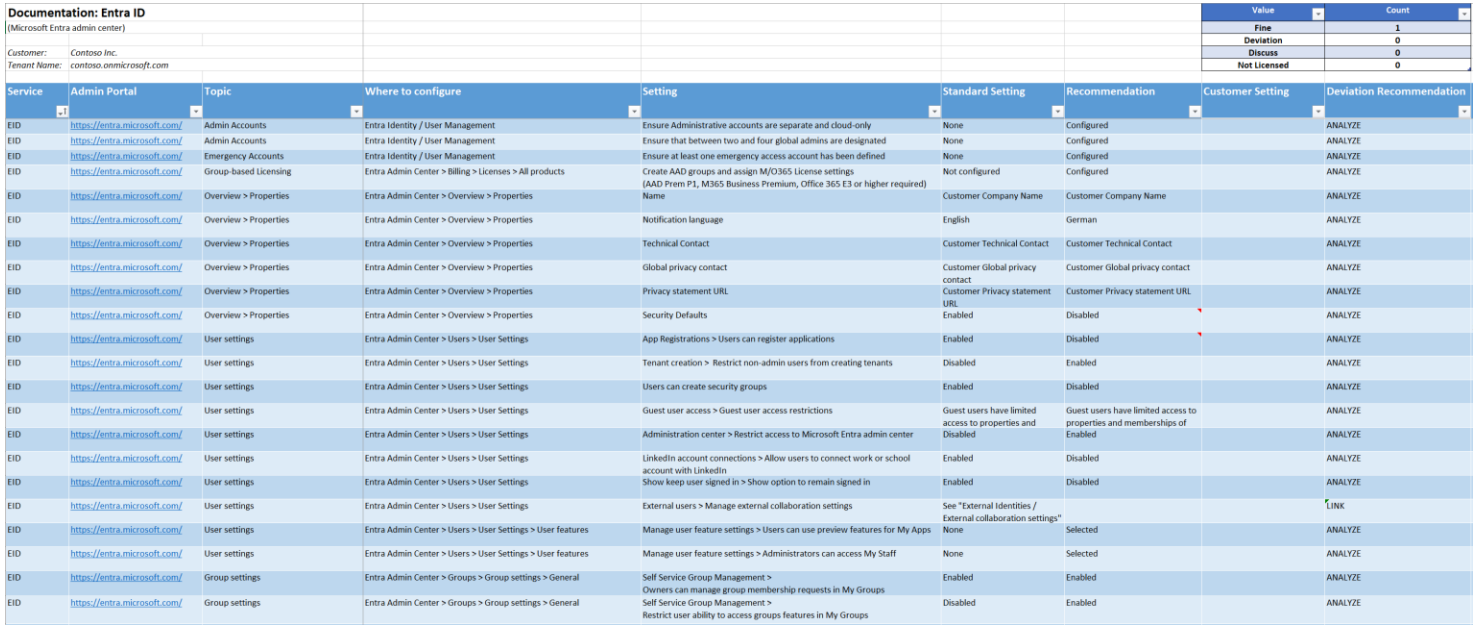
OneDrive &
SharePoint

Microsoft
Teams


CONDITIONAL ACCESS
Compliant
Access
M365
EXO
M365 Group
Team
SPO Site
INTUNE
TEAMS
CHANNEL
Files
Folder
Join
sync
Calendar
1:1 CHAT
Share
ODB
W10
OnPrem Mailbox
JENS.KUENZLER@SVA.DE

Grundkonfiguration des Tenants

- Hinterfragen der Microsoft Standard-Einstellungen
- Domänenregistrierung
- Grundkonfiguration der einzelnen Dienste
  - Entra ID Portal
  - Microsoft 365 Admin Center
  - SharePoint Online, OneDrive for Business
  - Teams
  - Exchange Online



Documentation: Entra ID
(Microsoft Entra admin center)

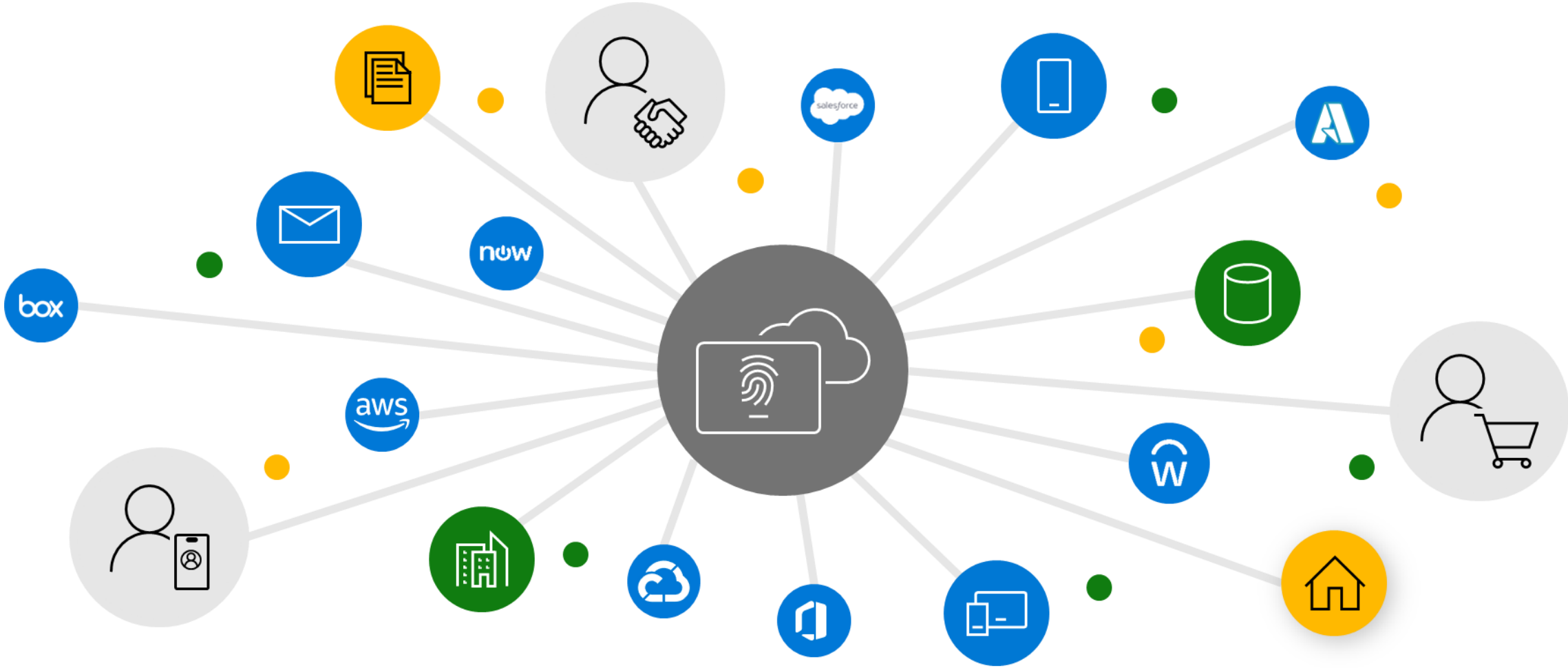
Customer: Contoso Inc.
Tenant Name: contoso.onmicrosoft.com

Value	Count
Fine	1
Deviation	0
Discuss	0
Not Licensed	0

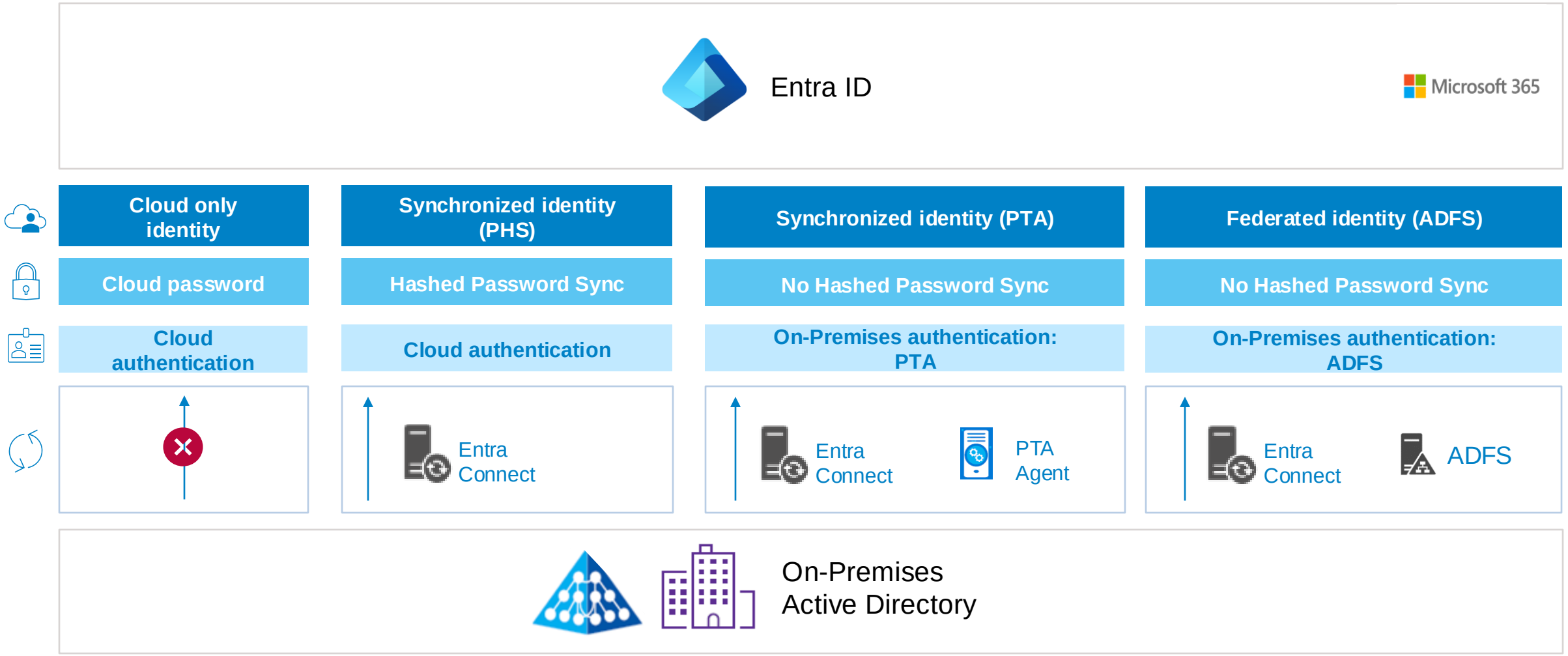
Service	Admin Portal	Topic	Where to configure	Setting	Standard Setting	Recommendation	Customer Setting	Deviation Recommendation
EID	https://entra.microsoft.com/	Admin Accounts	Entra Identity / User Management	Ensure Administrative accounts are separate and cloud-only	None	Configured		ANALYZE
EID	https://entra.microsoft.com/	Admin Accounts	Entra Identity / User Management	Ensure that between two and four global admins are designated	None	Configured		ANALYZE
EID	https://entra.microsoft.com/	Emergency Accounts	Entra Identity / User Management	Ensure at least one emergency access account has been defined	None	Configured		ANALYZE
EID	https://entra.microsoft.com/	Group-based Licensing	Entra Admin Center > Billing > Licenses > All products	Create AAD groups and assign M/O365 License settings (AAD Prem P1, M365 Business Premium, Office 365 E3 or higher required)	Not configured	Configured		ANALYZE
EID	https://entra.microsoft.com/	Overview > Properties	Entra Admin Center > Overview > Properties	Name	Customer Company Name	Customer Company Name		ANALYZE
EID	https://entra.microsoft.com/	Overview > Properties	Entra Admin Center > Overview > Properties	Notification language	English	German		ANALYZE
EID	https://entra.microsoft.com/	Overview > Properties	Entra Admin Center > Overview > Properties	Technical Contact	Customer Technical Contact	Customer Technical Contact		ANALYZE
EID	https://entra.microsoft.com/	Overview > Properties	Entra Admin Center > Overview > Properties	Global privacy contact	Customer Global privacy contact	Customer Global privacy contact		ANALYZE
EID	https://entra.microsoft.com/	Overview > Properties	Entra Admin Center > Overview > Properties	Privacy statement URL	Customer Privacy statement URL	Customer Privacy statement URL		ANALYZE
EID	https://entra.microsoft.com/	Overview > Properties	Entra Admin Center > Overview > Properties	Security Defaults	Enabled	Disabled		ANALYZE
EID	https://entra.microsoft.com/	User settings	Entra Admin Center > Users > User Settings	App Registrations > Users can register applications	Enabled	Disabled		ANALYZE
EID	https://entra.microsoft.com/	User settings	Entra Admin Center > Users > User Settings	Tenant creation > Restrict non-admin users from creating tenants	Disabled	Enabled		ANALYZE
EID	https://entra.microsoft.com/	User settings	Entra Admin Center > Users > User Settings	Users can create security groups	Enabled	Disabled		ANALYZE
EID	https://entra.microsoft.com/	User settings	Entra Admin Center > Users > User Settings	Guest user access > Guest user access restrictions	Guest users have limited access to properties and	Guest users have limited access to properties and memberships of		ANALYZE
EID	https://entra.microsoft.com/	User settings	Entra Admin Center > Users > User Settings	Administration center > Restrict access to Microsoft Entra admin center	Disabled	Enabled		ANALYZE
EID	https://entra.microsoft.com/	User settings	Entra Admin Center > Users > User Settings	LinkedIn account connections > Allow users to connect work or school account with LinkedIn	Enabled	Disabled		ANALYZE
EID	https://entra.microsoft.com/	User settings	Entra Admin Center > Users > User Settings	Show keep user signed in > Show option to remain signed in	Enabled	Disabled		ANALYZE
EID	https://entra.microsoft.com/	User settings	Entra Admin Center > Users > User Settings	External users > Manage external collaboration settings	See "External Identities / External collaboration settings"			LINK
EID	https://entra.microsoft.com/	User settings	Entra Admin Center > Users > User Settings > User features	Manage user feature settings > Users can use preview features for My Apps	None	Selected		ANALYZE
EID	https://entra.microsoft.com/	User settings	Entra Admin Center > Users > User Settings > User features	Manage user feature settings > Administrators can access My Staff	None	Selected		ANALYZE
EID	https://entra.microsoft.com/	Group settings	Entra Admin Center > Groups > Group settings > General	Self Service Group Management > Owners can manage group membership requests in My Groups	Enabled	Enabled		ANALYZE
EID	https://entra.microsoft.com/	Group settings	Entra Admin Center > Groups > Group settings > General	Self Service Group Management > Restrict user ability to access groups features in My Groups	Disabled	Enabled		ANALYZE

Identitäten

„Alles dreht sich um die Identität“

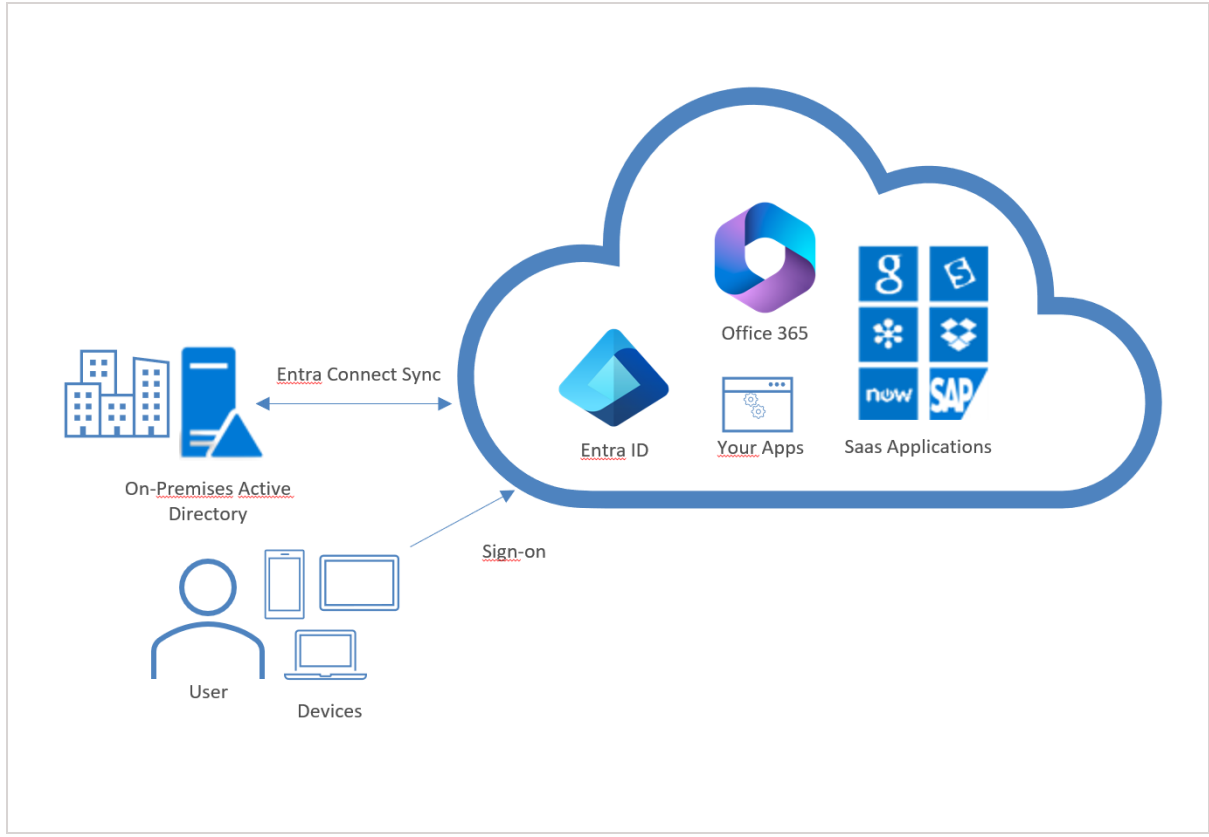


Modelle der Identitäten und Authentifizierung



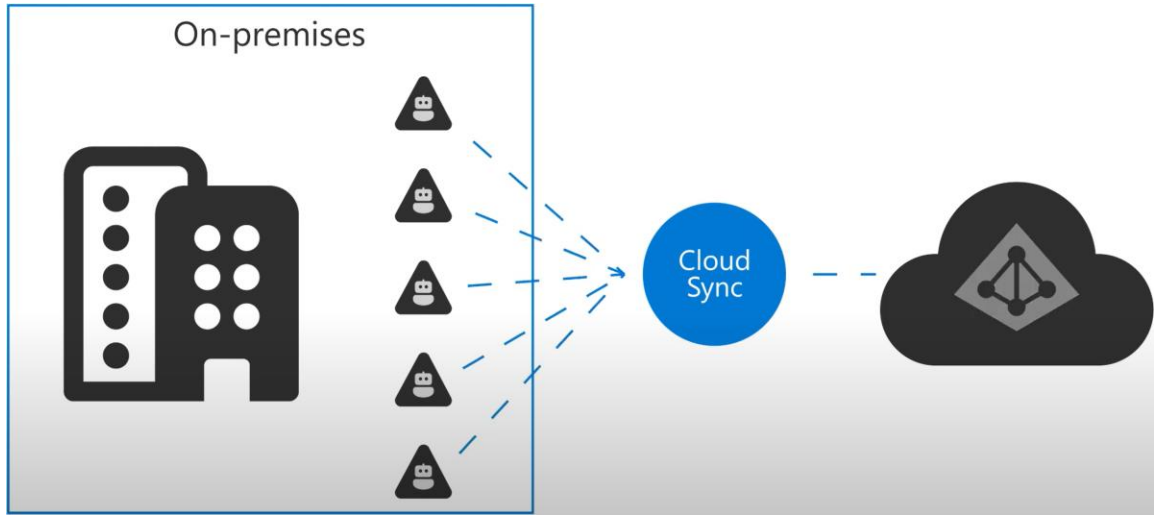
Entra Connect Sync

- Lokale Identitäten werden in die Cloud synchronisiert
- IDFIX durchführen vor Synchronisierung
- Öffentliche Domäne im Tenant (UPN-Suffix) erforderlich
- Cloud-Zugangsdaten = On-Premises-Zugangsdaten
- Filterung zum Regeln der Synchronisierung
  - OU- und/oder LDAP-Attribut Filterung
  - nicht das gesamte AD wird synchronisiert
- Optional: Live & Staging Mode
- Entra Connect ist ein Tier-0 System!



Entra Cloud Sync

- Lokale Identitäten werden in die Cloud synchronisiert
- IDFIX durchführen vor Synchronisierung
- Öffentliche Domäne im Tenant (UPN-Suffix) erforderlich
- Cloud-Zugangsdaten = On-Premises-Zugangsdaten
- Filterung zum Regeln der Synchronisierung
  - OU-Filterung
  - nicht das gesamte AD wird synchronisiert
- ABER:
  - nur ein Provisioning Agent wird On-Premises wird installiert
  - Die Verwaltung findet im Entra ID Portal statt
  - Feature Gap beachten

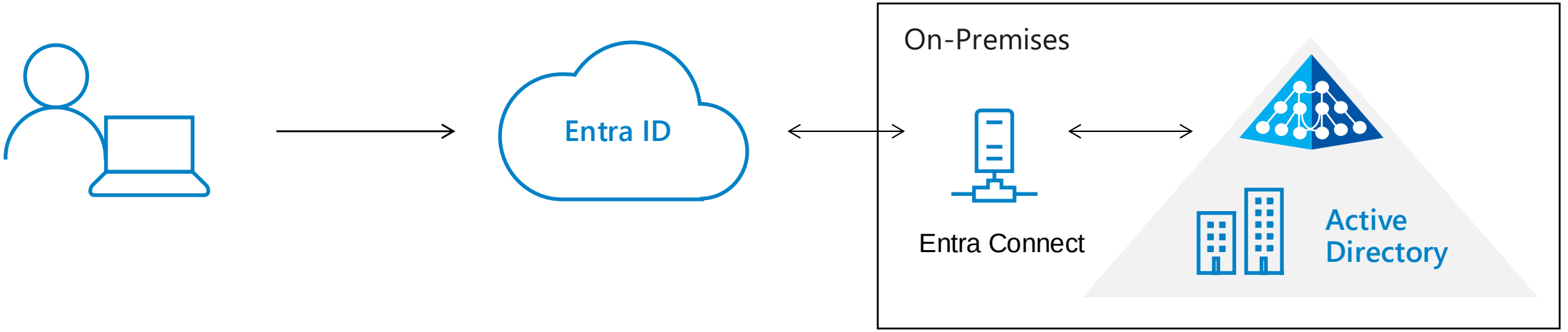


Entra Connect Sync vs. Cloud Sync

- Cloud Sync unterstützt keine Geräte-Synchronisierung
- Cloud Sync unterstützt nur Password Hash Sync
- Cloud Sync unterstützt keine LDAP-Attribut-Filterung

Feature	Connect-Synchronisierung	Cloudsynchronisierung
Herstellen einer Verbindung mit einer einzelnen lokalen AD-Gesamtstruktur	•	•
Herstellen einer Verbindung mit mehreren lokalen AD-Gesamtstrukturen	•	•
Herstellen einer Verbindung mit mehreren getrennten lokalen AD-Gesamtstrukturen		•
Installationsmodell mit einfachen Agents		•
Mehrere aktive Agents für Hochverfügbarkeit		•
Unterstützung für Benutzerobjekte	•	•
Unterstützung für Gruppenobjekte	•	•
Unterstützung für Kontaktobjekte	•	•
Unterstützung für Geräteobjekte	•	
Zulassen grundlegender Anpassungen von Attributflüssen	•	•
Synchronisieren von Exchange Online-Attributen	•	•
Synchronisieren der Erweiterungsattribute 1–15	•	•
Synchronisieren von benutzerdefinierten AD-Attributen (Verzeichniserweiterungen)	•	•
Unterstützung der Kennworthashsynchronisierung	•	•
Unterstützung der Passthrough-Authentifizierung	•	
Verbundunterstützung	•	•
Nahtloses einmaliges Anmelden	•	•
Unterstützt die Installation auf einem Domänencontroller	•	•
Unterstützung für Windows Server 2016	•	•
Filtern nach Domänen/Organisationseinheiten/Gruppen	•	•
Filterung nach den Attributwerten eines Objekts	•	
Zulassen eines minimalen Attributsatzes für die Synchronisierung (MinSync)	•	•
Zulassen der Entfernung von Attributen aus dem Attributfluss von AD nach Microsoft Entra ID	•	•
Zulassen einer erweiterten Anpassung des Attributflusses	•	
Unterstützung für das Kennwortrückschreiben	•	•
Unterstützung für das Geräterückschreiben	•	Kunden sollten hierfür zukünftig die Cloud Kerberos-Vertrauensstellung verwenden.
Unterstützung für das Gruppenrückschreiben	•	•
Unterstützung für das Zusammenführen von Benutzerattributen aus mehreren Domänen	•	
Support für Microsoft Entra Domain Services	•	
Exchange-Hybridrückschreiben	•	•
Unbegrenzte Anzahl von Objekten pro AD-Domäne	•	
Unterstützung für bis zu 150.000 Objekte pro AD-Domäne	•	•
Gruppen mit bis zu 50.000 Mitgliedern	•	•
Große Gruppen mit bis zu 250.000 Mitgliedern	•	
Domänenübergreifende Verweise	•	•
Gesamtstrukturübergreifende Verweise	•	
Bedarfsorientierte Bereitstellung		•

Password Hash Sync



Gute Nutzererfahrung

- Gleiche Kennwörter für Cloud- und On-Premises Applikationen
- Fail-Over Möglichkeit im Falle einer Beeinträchtigung anderer Authentifizierungsmöglichkeiten

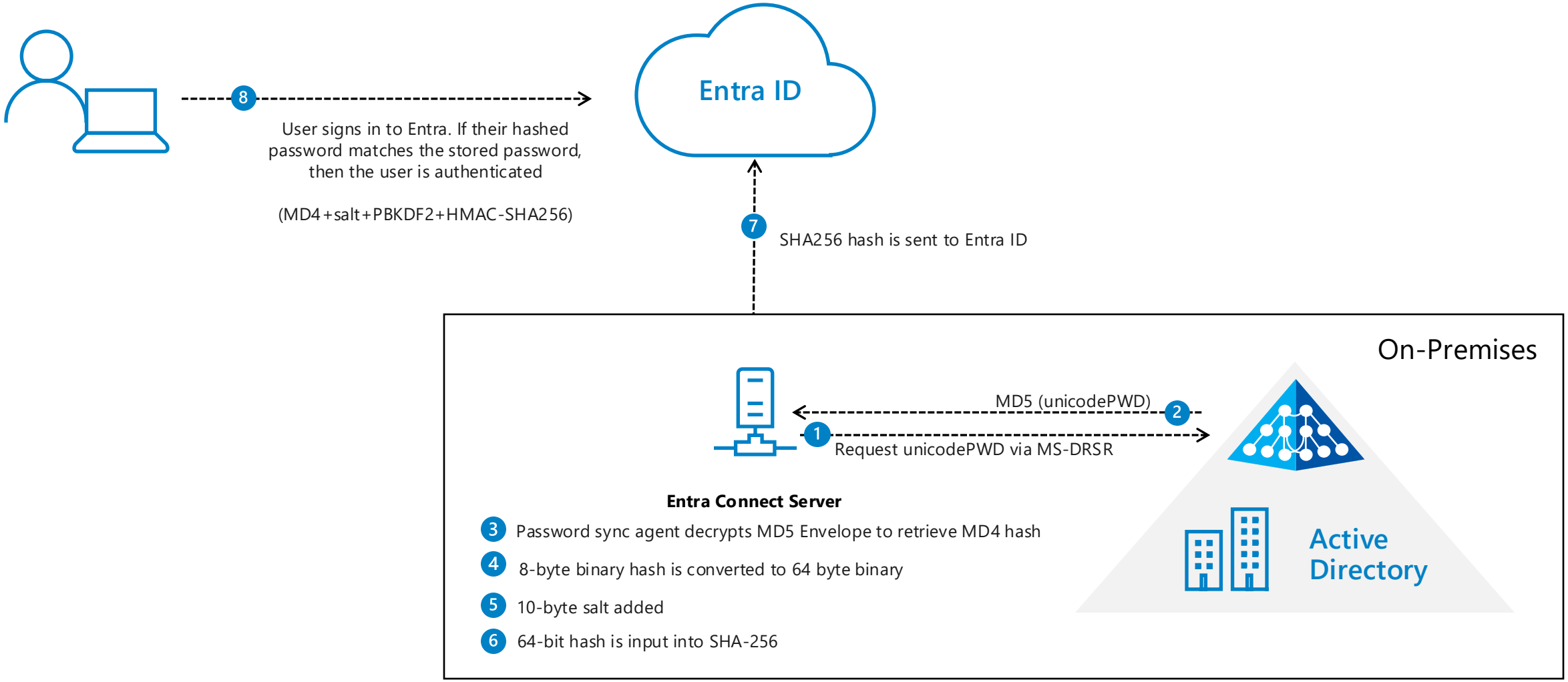
Sicher und vertrauenswürdig

- Nur nicht reversible Hashes werden in der Cloud gespeichert
- Report kompromittierter Anmeldedaten (Entra ID P2)
- Integriert in Smart Lockout, Identity Protection und Conditional Access

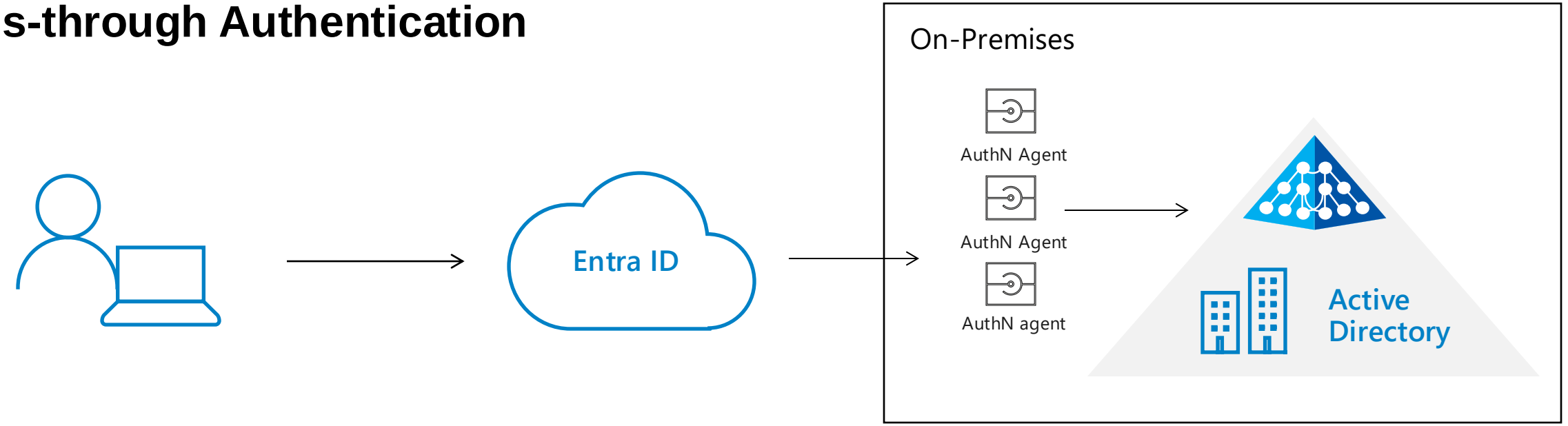
Einfach in Installation und Betrieb

- Kein Agent On-Premises erforderlich
- Small On-Premises footprint

Password Hash Sync Deep Dive



Pass-through Authentication



Gute Nutzererfahrung

- Gleiche Kennwörter für Cloud- und On-Premises Applikationen
- Unterstützt ebenfalls Self Service Password Reset (Entra ID P1)

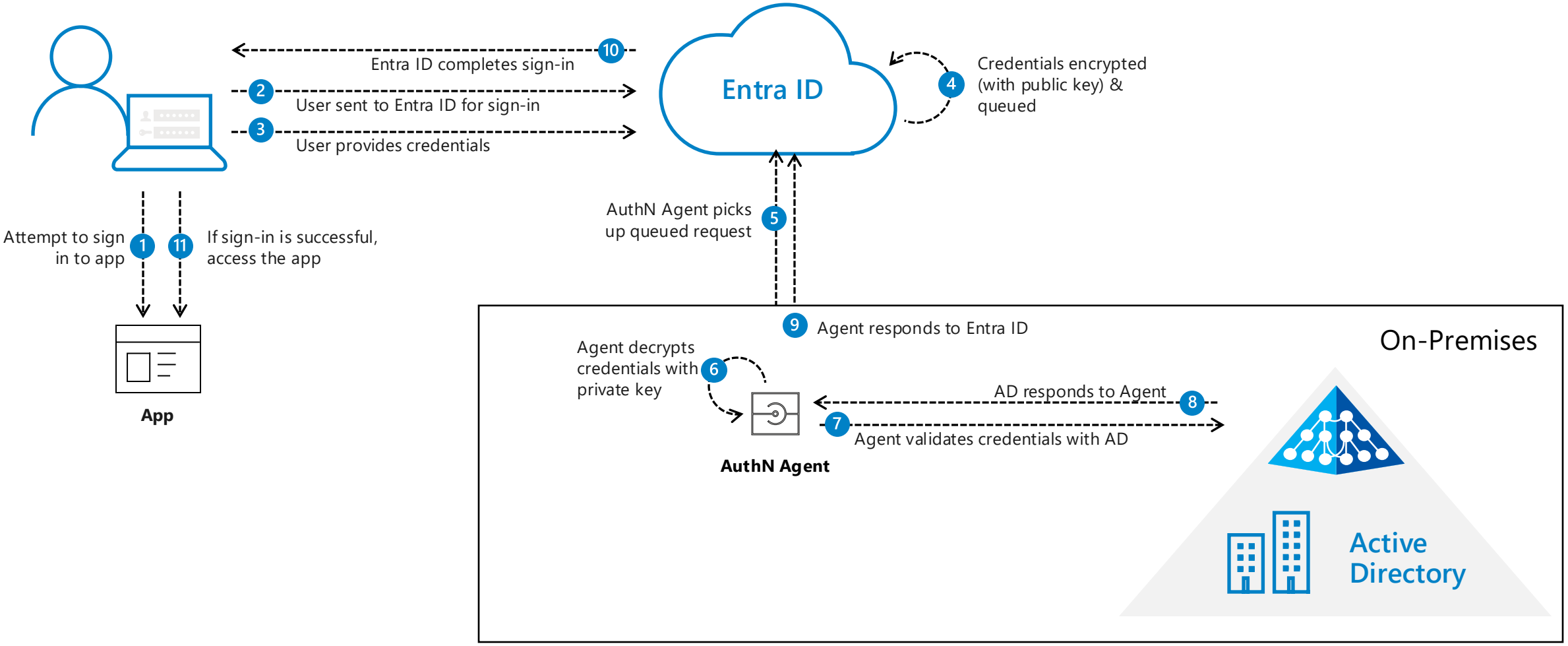
Sicher und vertrauenswürdig

- Passwörter verbleiben im eigenen AD
- Keine Vorraussetzungen für DMZ oder eingehende Firewall-Regeln
- Integriert in Smart Lockout, Identity Protection und Conditional Access

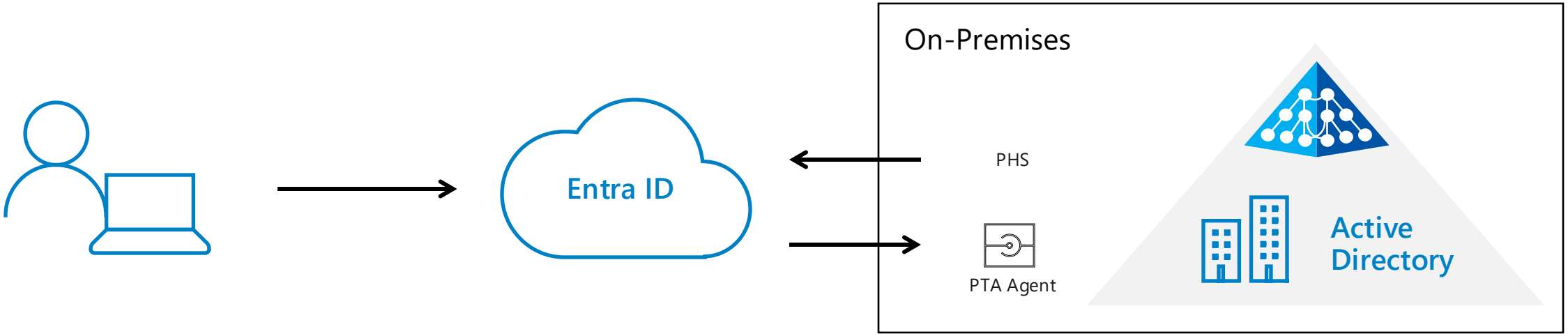
Einfach in Installation und Betrieb

- Agenten-basierte Bereitstellung
- Hochverfügbarkeit out-of-the-box
- Kein Management Overhead, einfacher Betrieb

Pass-through Authentication Deep Dive

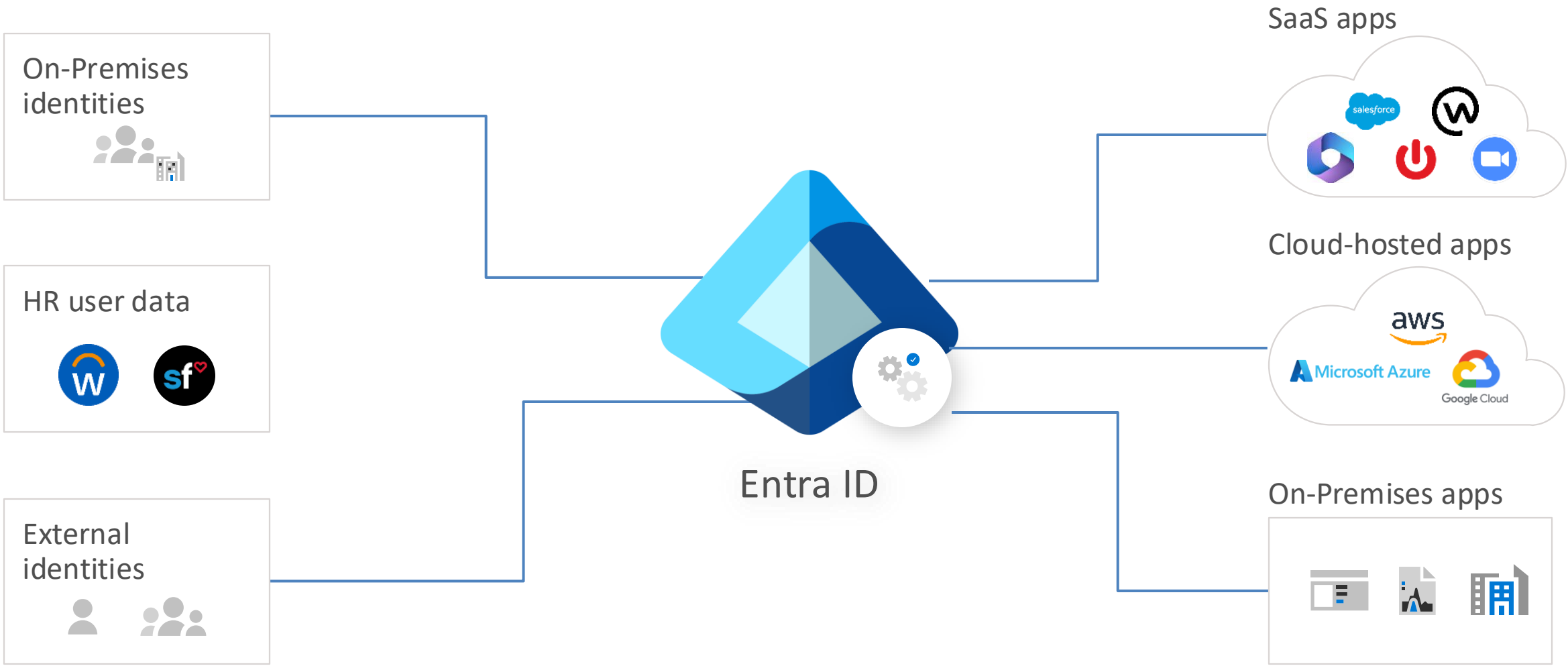


Kombination | PHS + PTA



Praxis-Empfehlung	Sicher und vertrauenswürdig	Einfach in Installation und Betrieb
PTA → Anmeldung an On-Premises AD PHS → Password Hash sync nach Entra ID	Report kompromittierter Anmeldedaten (Entra ID P2)	PTA als primäre Authentifizierungsmethode
Anmeldung an On-Premises AD	AD Account Policies wirken (account expires, account lockout)	PHS als manueller Fall-Back zu PTA

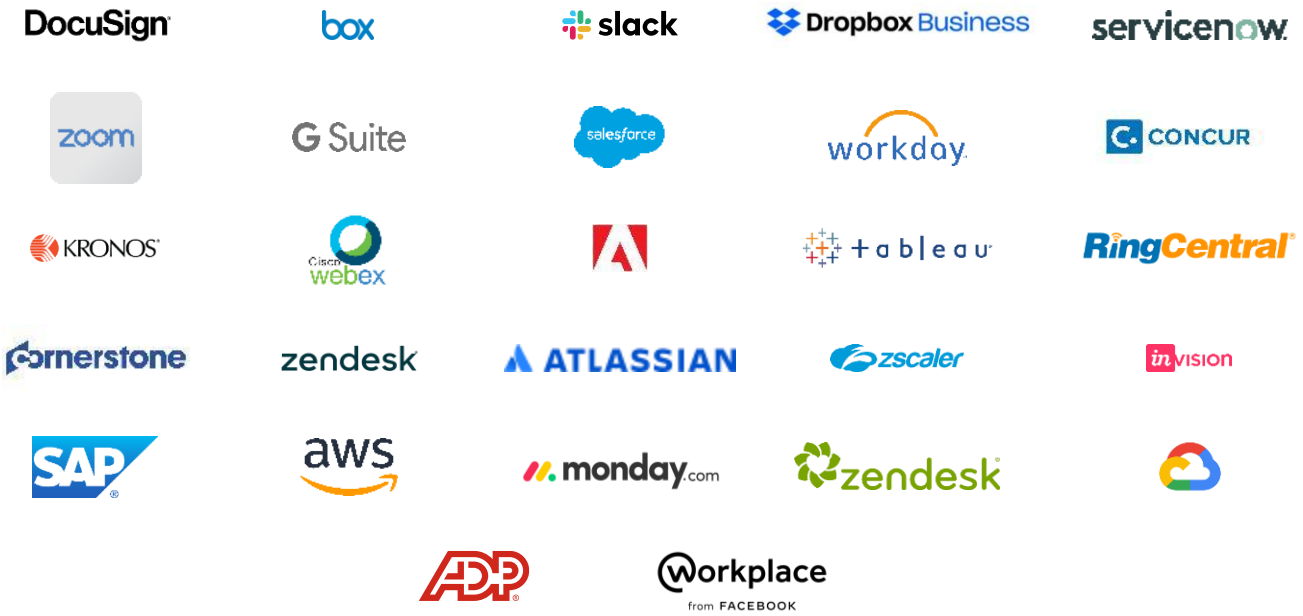
Integration weiterer Systeme in Entra ID



Entra ID Anwendungen mit Moderner Authentifizierung

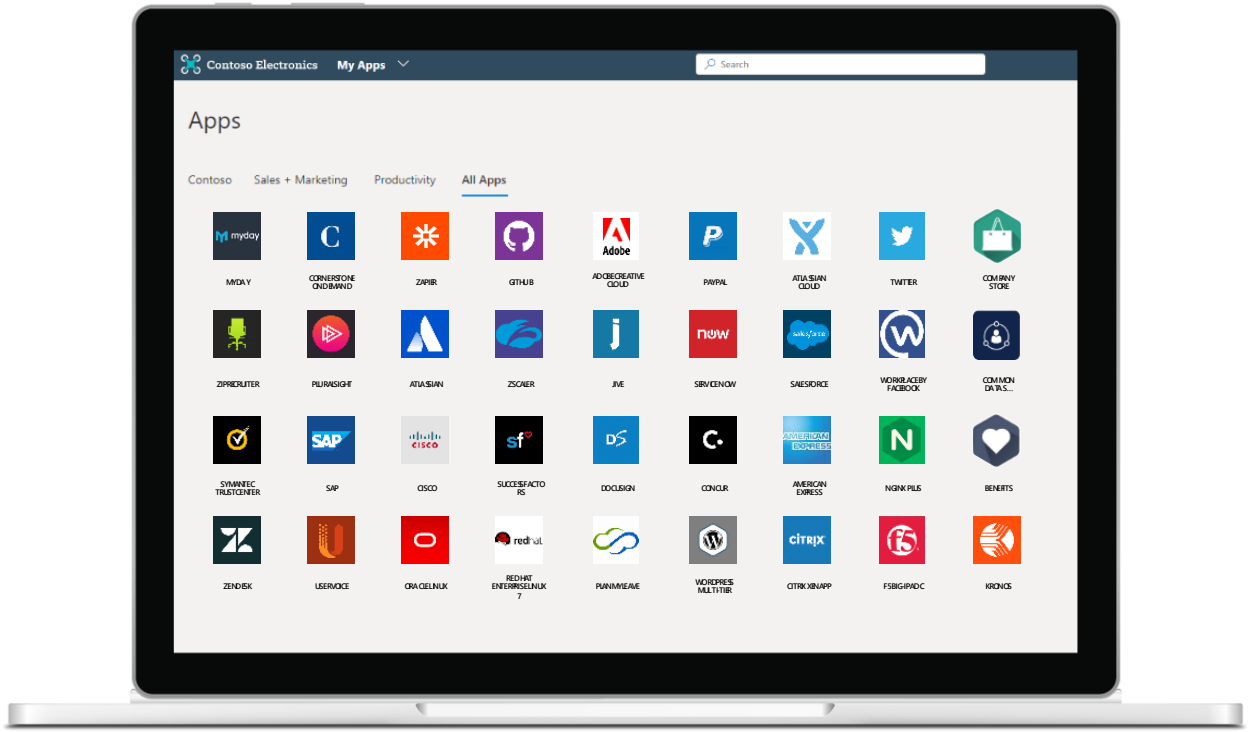
- Nutzung der Entra ID App-Gallerie mit vorbereiteten Drittanbieter-Integrationen
- Alternativ können auch eigene Anwendungen erstellt und integriert werden

Thousands of pre-integrated apps in the gallery



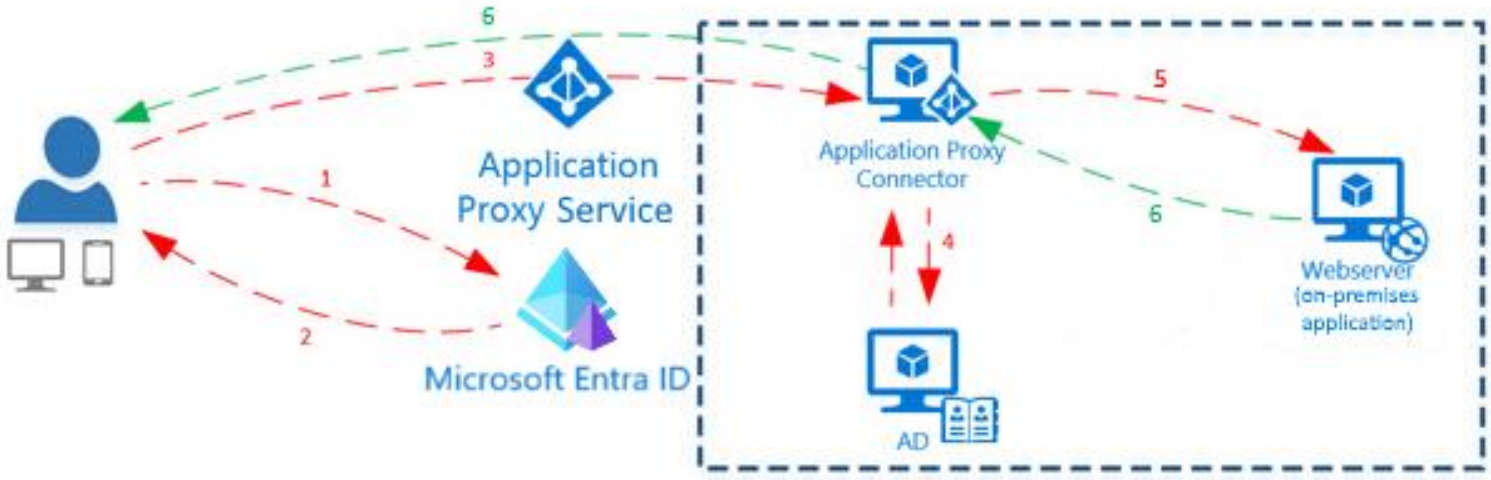
App Integration in Entra ID

- Single Sign-on (SSO)
- App Portal präsentiert alle integrierten Anwendungen
- App-Sammlungen können über Entra ID definiert werden

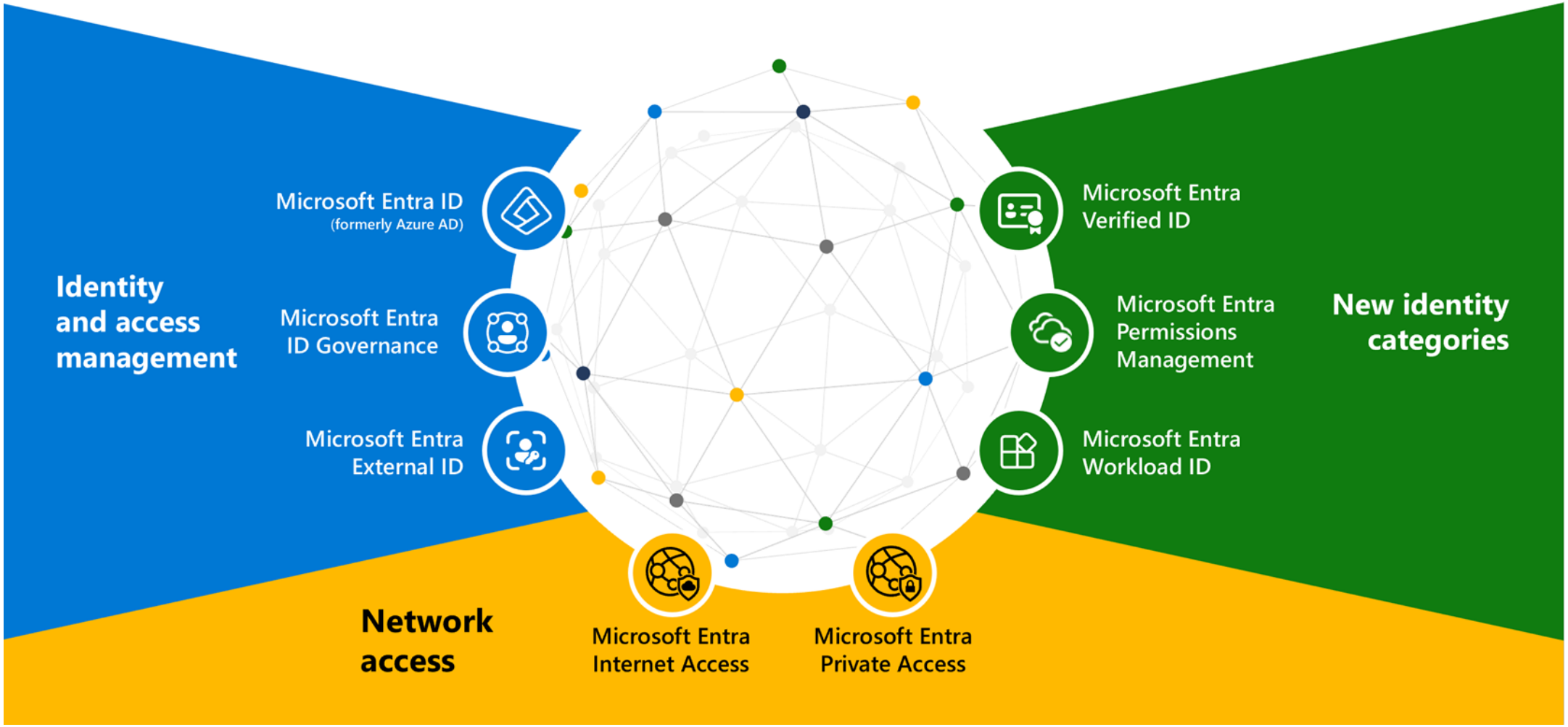


Entra Application Proxy

- Ausgehende Verbindung des Connectors
- Anmeldung über Entra
  - MFA, Conditional Access
- Native Unterstützung für verschiedene Authentifizierungsmethoden
  - Header-based
  - Forms- or password based
  - Integrated windows authentication
  - SAML
  - Remote desktop gateway



Entra Suite Überblick



Zero Trust

Identitäten

Identitäten müssen legitimiert werden

Applikationen

Verwalten der Applikationen und der dort verarbeiteten Daten

Daten

Schutz sensibler Informationen (personenbezogene Daten, Geschäftsgeheimnisse)

Geräte

Verwalten von Geräten, Unterscheidung zwischen Managed Devices und Fremdgeräten

Abwehren von Cyberangriffen / Permanente Risikobewertung

- Single sign-on
- MFA / Passwordless
- Conditional Access & continuous access evaluation
- Risk-based Conditional Access policies
- Self-service end-user tools

Hybrid Identity | Zusammenfassung

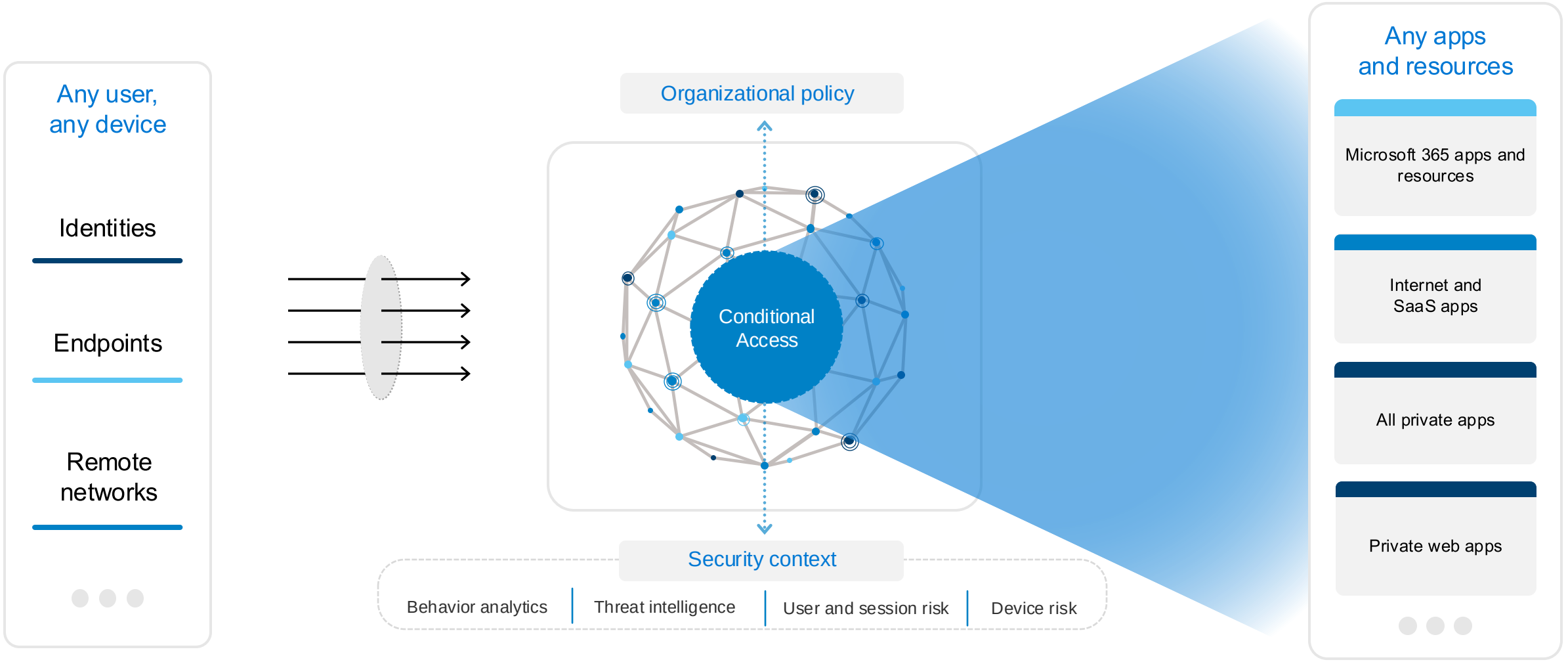
Wichtige Punkte für unser „Big-Picture“

- PHS oder PTA?
- UPN=MAIL?
- Scoping per LDAP Filter oder OU?
- Entra Connect oder Cloud Sync
- AD Domain Update / Cleanup?

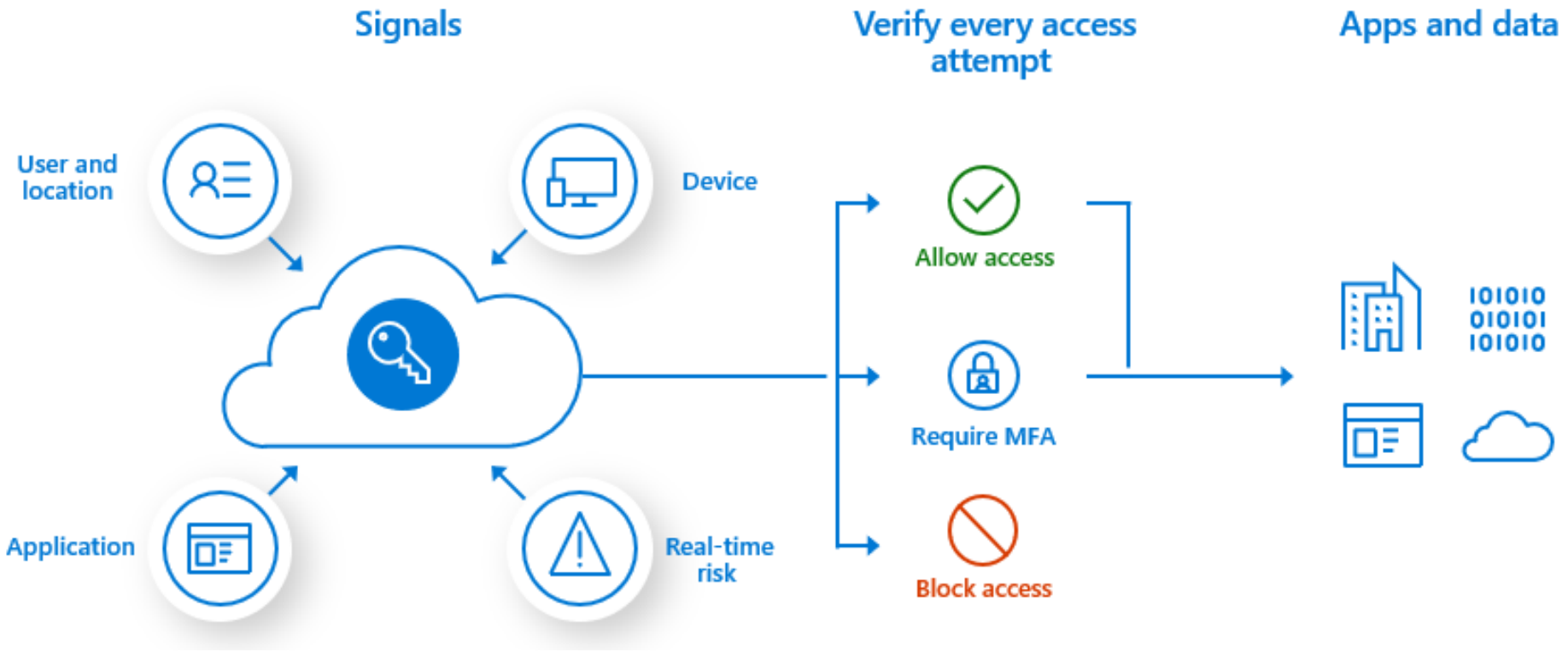
- Weitere wichtige Punkte für das Umsetzungsprojekt?

Security

Conditional Access

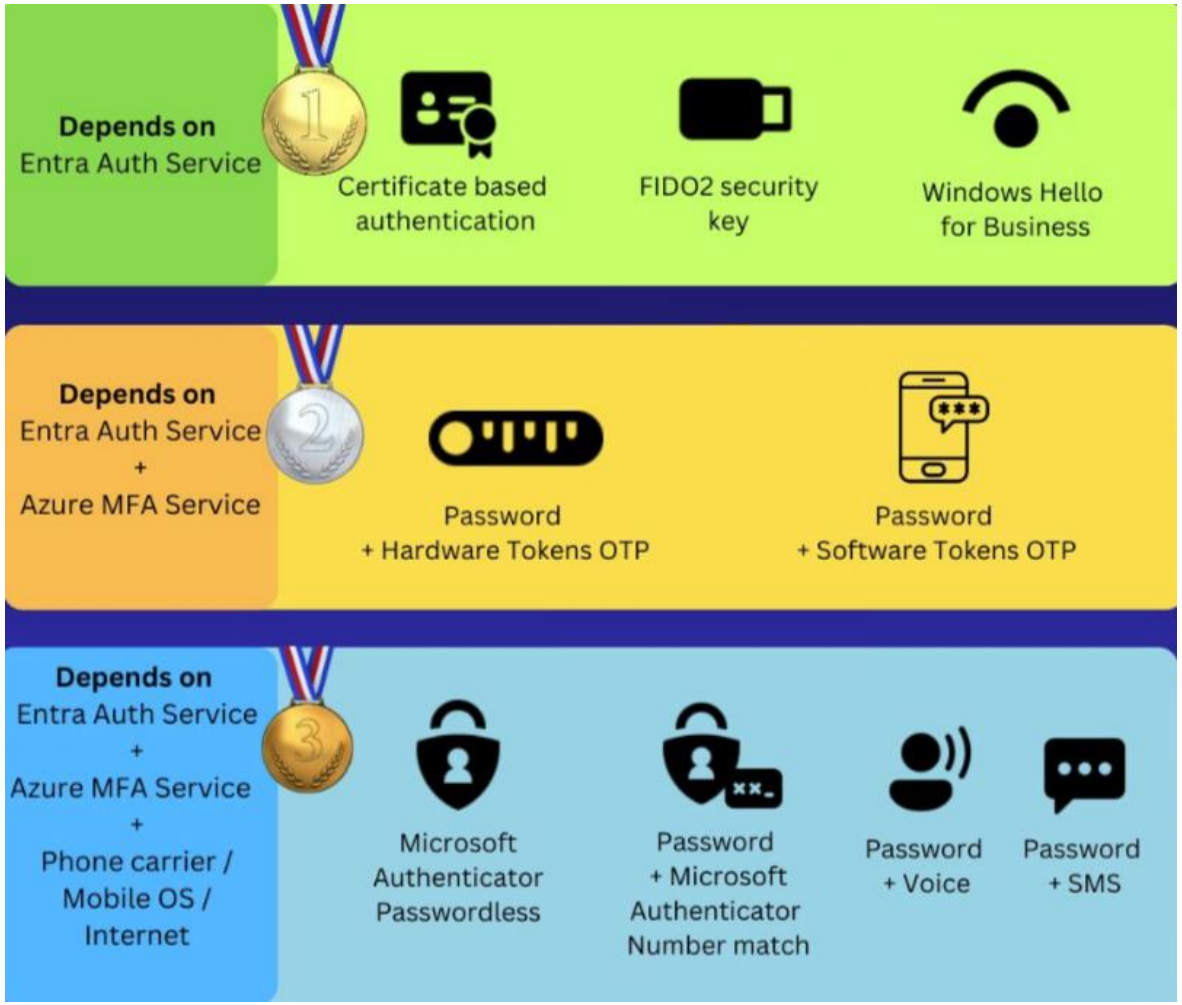


Conditional Access



Multifaktor Authentifizierung

- Verwendung von Hardware-Token (MFA & FIDO2)
- Verwendung des Gerätes als zusätzlicher Faktor
- Verwendung von biometrischen Faktoren
- Eliminierung von unsicheren Kennwörtern
- Möglichst kein SMS und Voice mehr nutzen.
  - SMS können abgefangen werden und sind unverschlüsselt
  - Anrufe sind nicht eineindeutig und unzuverlässig

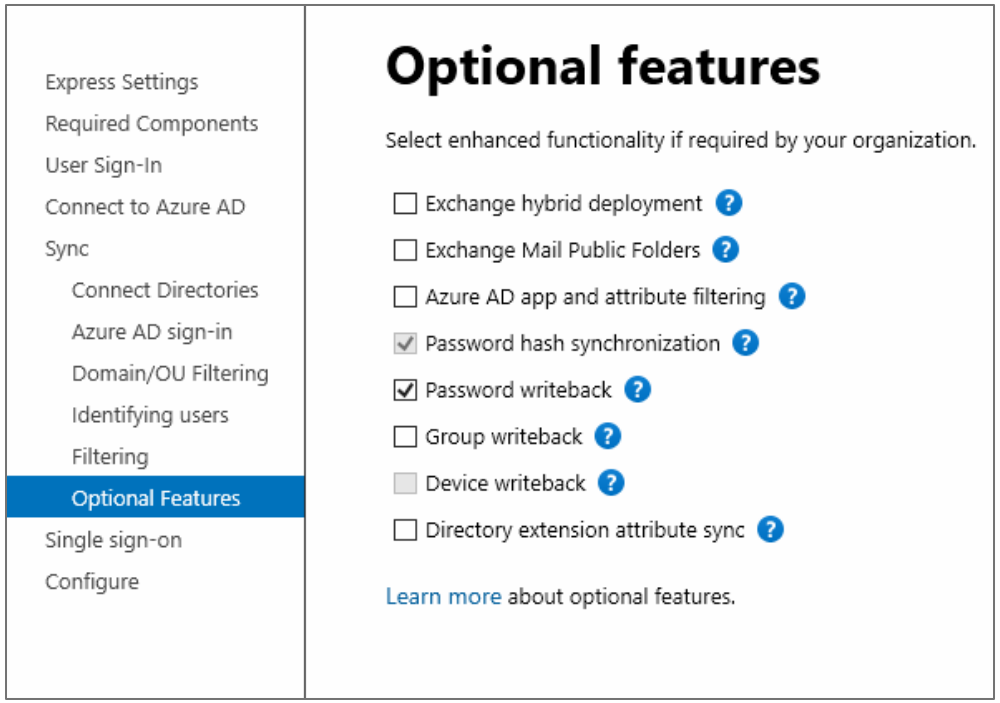


SSPR & Password writeback

- User Self Service zur Kennwortzurücksetzung (Self Service Password Reset) und Konten-Entsperrung
  - Ausnahme: Administratoren

- In Entra ID geändertes Kennwort wird in das lokale AD zurückgeschrieben
- Aktivierung der Funktion in Entra Connect
- Berücksichtigung der AD-Kennwortrichtlinie

- Einheitliche Registierung mit MFA
- Authenticator, Token



Administration in der Cloud

- Dedizierte Cloud-Only Admin Konten (@tenant.onmicrosoft.com)
- Admin Konten werden nicht von On-Premises synchronisiert

- **Gut:** MFA Aktivierung ist Pflicht (Conditional Access Policy)
- **Besser:** Administration nur über ein Compliant Device (Conditional Access Policy)
- **Am Besten:** Nutzung einer PAW (Privileged Access Workstation)
  - Dedizierte Hardware
  - Kein Domänen Mitglied
  - Eingeschränkter Internet Zugang (nur notwendige Admin Portale)

- Global Admin Rolle nur in Ausnahmen nutzen (notwendige Rollen delegieren)
- Zeitgesteurte Zuweisung von Administrativen Rollen (PIM / Entra ID P2)

- **Besser nicht:** Jump Server nutzen → Sammlung vieler Credentials

- **Break the Glass Admin Konto** für den Notfall-Zugriff
  - FIDO-Key als MFA Methode einplanen

Privileged Identity Management

- Just in Time Administration & Least Privilege
- Zeitgesteuerte Zuweisung von Berechtigungen
- Rollenbasierte Berechtigungszuweisung
- Zusätzliche Genehmigung erforderlich
- Zuweisung wird auditiert
- Angabe einer Ticketnummer / eines Grundes möglich
- Nur in Entra ID Plan 2 enthalten

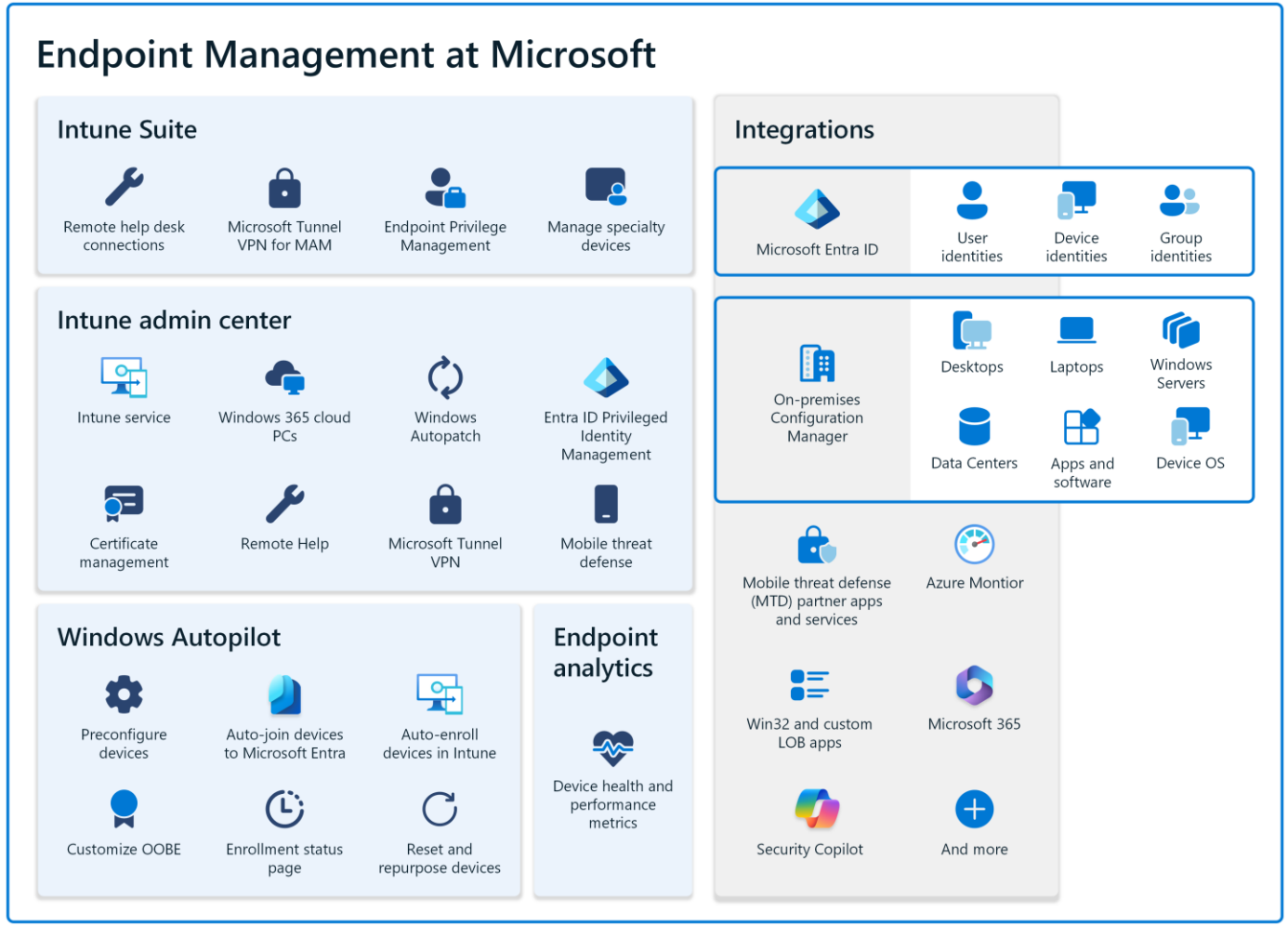
Microsoft Security | Zusammenfassung

Wichtige Punkte für unser „Big-Picture“

- Conditional Access Policies als Gatekeeper
  - Cloud admins = Cloud Konten
  - Welche Geräte dürfen zugreifen?
  - Welche MFA Methoden für Nutzer?
  - Device Authentication / Compliant Devices
- Self Service Password Reset / Writeback
- Least priviledged Administration → PIM

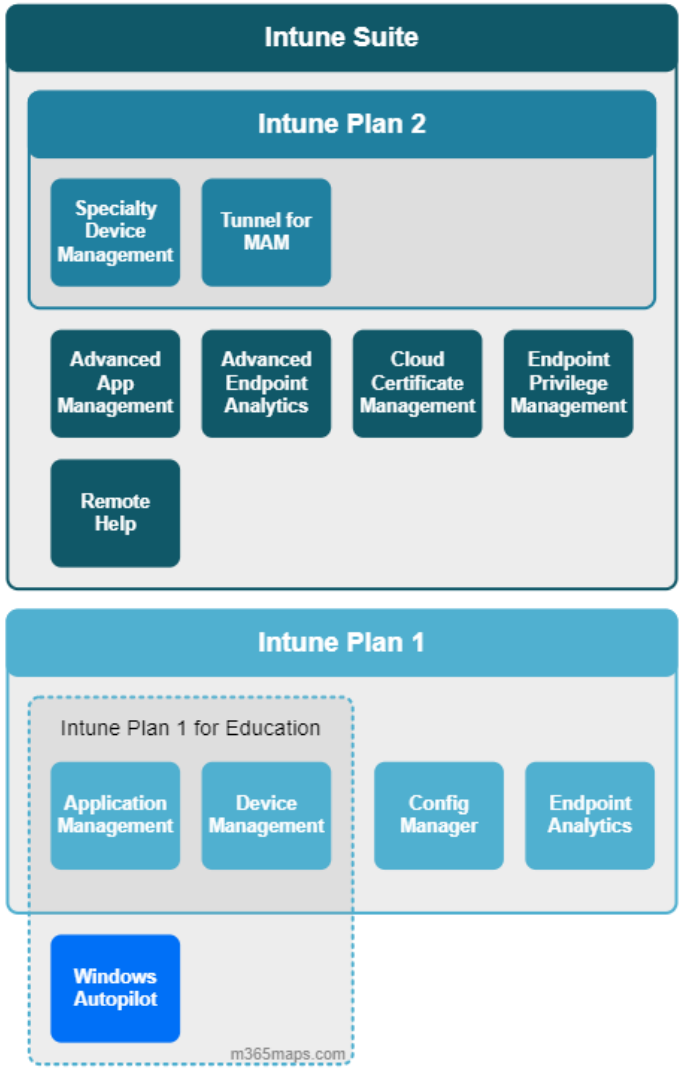
Microsoft Intune

Microsofts UEM Lösung: Intune



Microsofts Intune Lizenzen

Microsoft Intune P1
Add-On



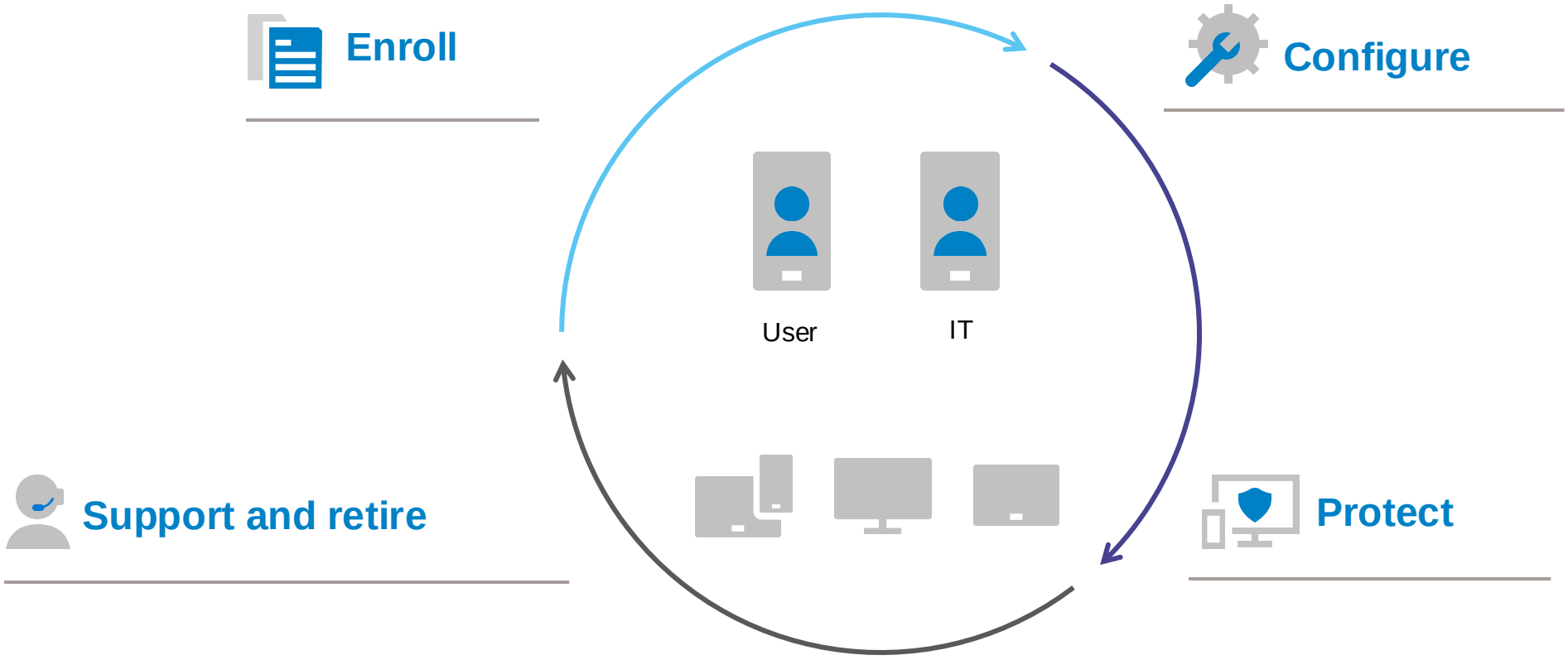
Microsoft Intune P1
Add-On

M365 Business Premium

M365 Enterprise

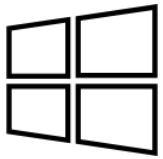
M365 Education

Device Lifecycle bei Microsoft



MDM managed Devices

Microsoft Intune



Windows

macOS

Android

iOS & iPadOS

Linux

Verschiedene Geräte, verschiedene Joins

Typ	OS	Beschreibung	Domain Member	Workgroup Member	Intune Enrollment
Entra ID Registered	Win10/11 iOS, MacOS Android	Anmeldung mit lokalem / AD Benutzer Nutzer und Gerät sind verknüpft	**Ja**	**Ja**	Möglich
Entra ID Joined	Win10/11	Anmeldung mit Entra ID Benutzer Benutzer können wechseln	Nein	**Ja**	Möglich
Entra ID Hybrid Joined	Win10/11	Anmeldung mit AD Benutzer Benutzer können wechseln	**Ja**	Nein	Möglich

Abgrenzung Entra ID Join

Die folgenden Folien beschäftigen sich hauptsächlich mit:

- Clients mit Windows Betriebssystem
- Azure Virtual Desktop
- Windows 365
- Sonstige Clients die auf einem vollen Windows OS basieren (Kiosks, Shared Desks etc.)

Explizit ausgenommen sind:

- Windows Server (noch…)
- Terminal-Server oder vergleichbare Lösungen (wie Citrix oder VMWare Horizon), davon ausgenommen ist der Zugriff auf diese.

Wann ist Entra-Join only die richtige Wahl?

Mögliche Gründe

- „Neue Mitarbeiter können kein AD mehr“
- „Wir möchten schlanker arbeiten“
- „Computer sollen überall verfügbar sein“

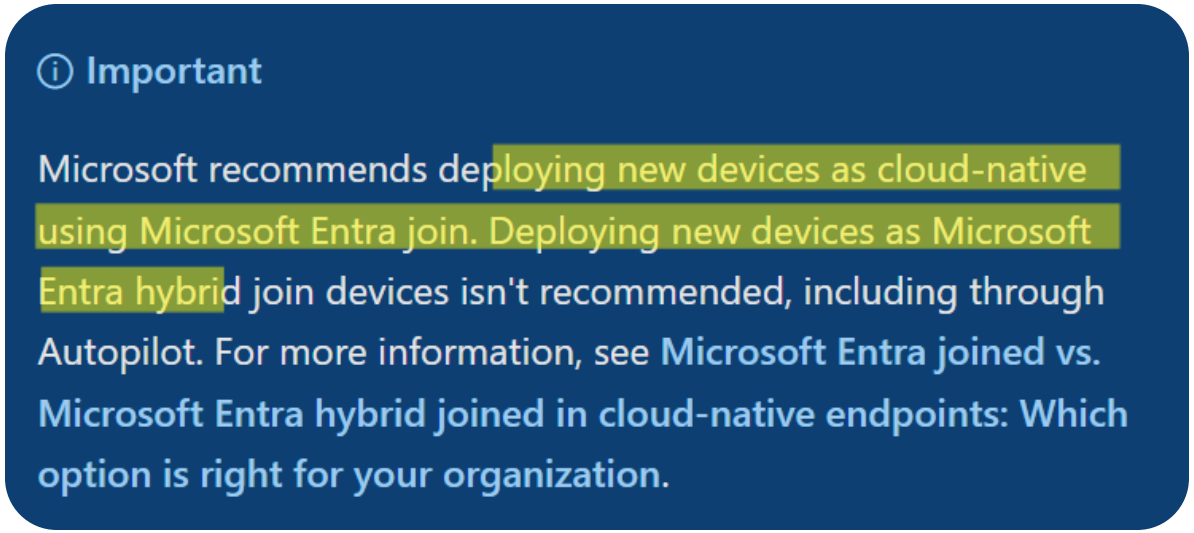
Ausrichtung auf Microsoft-Strategie

- „Wir möchten MS-konform sein“
- „Wir möchten mehr Dienste von M365 nutzen“
- „Autopilot ist geplant“

Microsoft schiebt langsam aber sicher neue Features Richtung „Entra-Join only“-exklusiv

MEHJ? Microsoft Entra Hybrid Join

- Keine Weiterentwicklung von ADDS
- Komplexe Infrastruktur inkl. Betrieb
- Autopilot mit Hybrid-Join schwierig und fehleranfälliger
- Kein Zero-Trust Vorgehen
- Kein **Modern Management**



Wann ist Entra-Join only die richtige Wahl?

- Großteil von Computern benötigen **kein AD** – der *Benutzer* benötigt ggf. eine hybride Identität
- Weniger On-Premises Abhängigkeiten gewünscht oder Cloud-Only Strategie geplant
- Viele BYOD-Computer

- Fazit: **Fast immer** die bessere Wahl

Wann ist Entra-Join only nicht die richtige Wahl?

- Starke Abhängigkeiten zur Geräte-Identität (>50% der Geräte) (nicht Benutzer!) im AD.
  Mögliche (lösbare) Blocker:
  - Applikationen die Geräteidentität benötigen (sehr selten)
  - RADIUS mit Geräteidentifikation statt certificate based 802.1x (Sonderfall NPS)
  - Network Access Control basierend auf Geräteidentität
- Non-Cloud Vorgaben (Ärzte, Versicherungen, Banken, …)
- Non-Internet Clients „Air-Gapped“ (Produktion, siehe AD-Joined only)
- „Shared-Devices“ können schwierig(er) sein, hier kommt es auf die Kundensituation an

Anforderungsanalyse notwendig!

→ Was genau benötigt ein Gerät in ADDS?

→ Ist die Lösung noch zeitgemäß?

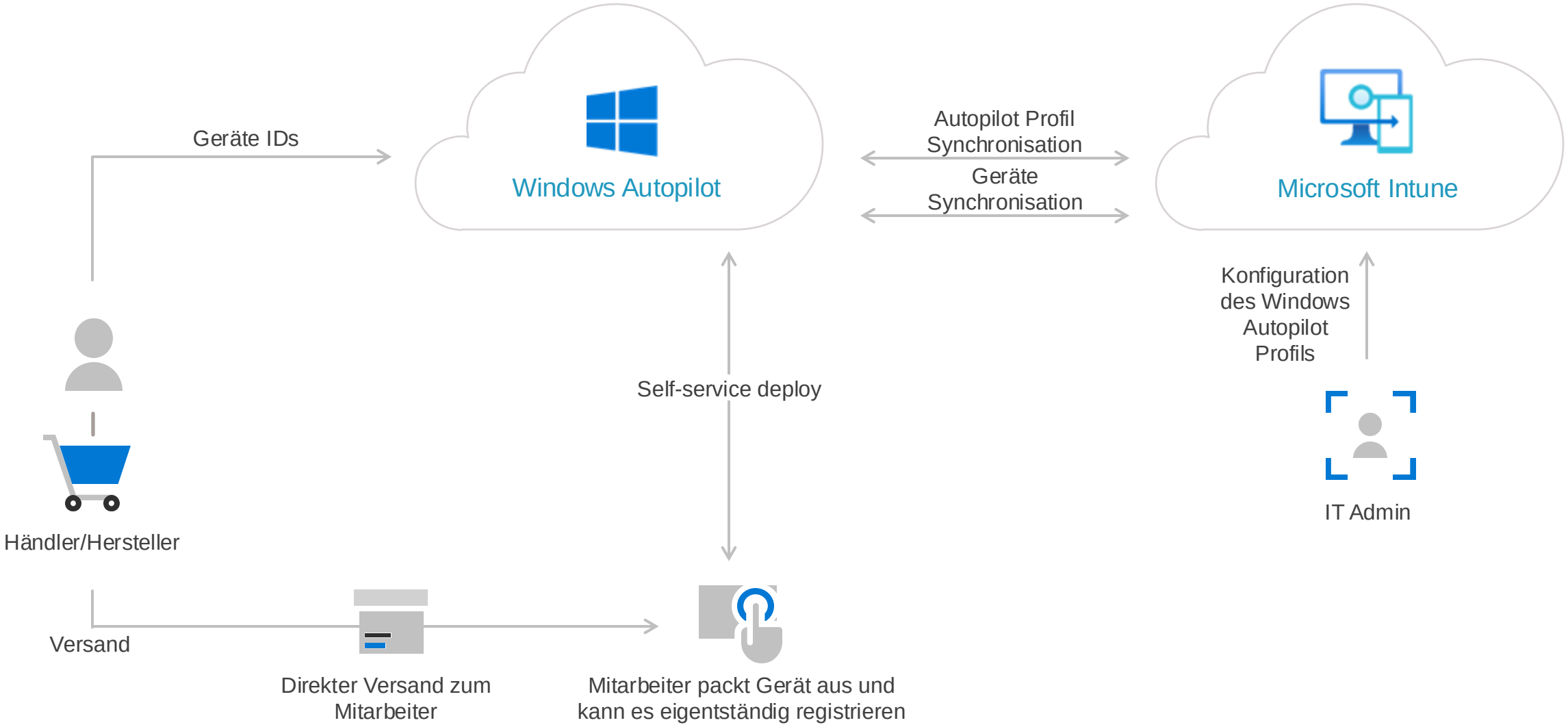
Wann ist Entra-Join only nicht die richtige Wahl?

- Nicht auflösbare Authentifizierung des Computer-Kontos gegenüber Legacy-Diensten (selten)
- Support durch Softwarehersteller für Entra-Join only nicht gegeben (sehr selten)
- PAWs je nach Kundenanforderung

Windows Autopilot | Übersicht

- Standardisierung von Windows-basierten Computern
- Szenarien:
  - User-Driven
    - Useraffiner Rollout angestoßen durch den User
  - Pre-Provision (ehem. White-Glove)
    - Useraffiner Rollout angestoßen durch IT-Admins, Reseller oder OEM
  - Self-Deploying
    - Kioskgerät oder -gerät für mehrere Benutzer
- Überall verfügbar

Windows Autopilot | Prozess



Windows Hello for Business

Allgemeines

- Phishing-resistente Authentifizierungsmethode
- biometrische oder PIN
- Windows 10 und höher

Windows Hello	Windows Hello for Business
Private Geräte (OS Version)	Business Geräte
Authentifizierung anhand biometrischer Daten oder PIN	Schlüssel- oder zertifikatsbasierte Authentifizierung
	Administrierbar

Windows Hello for Business

Voraussetzungen

- Intune Plan 1 oder höher
- Entra ID
- Windows 10 and higher 1903, Windows 11
- iOS/iPadOS 15.x and higher
  - IOS/iPadOS 12.x and higher

Empfehlungen

- TPM (if no TPM present, private key gets enrolled to software KSP → less secure)
- Hardware with biometric support (IR camera, fingerprint)

TRUST: Device itself + Localized Biometric (finger or face)
(PIN can be used but biometric has higher identity assurance and better user experience)

iOS/iPadOS

Prerequisites

- Intune Plan 1 and higher
- iOS/iPadOS 15.x and higher
  - iOS/iPadOS 12.x and higher - ohne Erfolgsgarantie und mit Einschränkungen
- Apple Business Manager or Apple School Manager for the automated corporate device enrollment
  - Apple Enrollment Token
- Apple MDM Push Certificate

Device Enrollment

- Corporate-owned
  - Apple Business/ School Manager
  - Apple Configurator
- BYOD
  - Company portal – User Enrollment
  - Company portal – Webbased Registration

The degree of configuration depends on the device registration type

- Patchmanagement
- Konfigurationsprofiles
- User Permissions
- Etc.

Android Devices

Prerequisites

- Intune Plan 1 or higher
- Android 8.x or higher
  - including Samsung KNOX Standard 3.0 or higher
- Samsung KNOX the automated device enrollment
  - Apple Enrollment Token
- Managed Google-Play Account

Device Enrollment

- Corporate-owned
  - Company-owned, dedicated Android Enterprise devices
  - Company-owned, fully managed Android Enterprise devices
  - Company's own Android Enterprise work profile
- BYOD
  - Personal Android Enterprise-Devices with Workprofile

Linux

Prerequisites

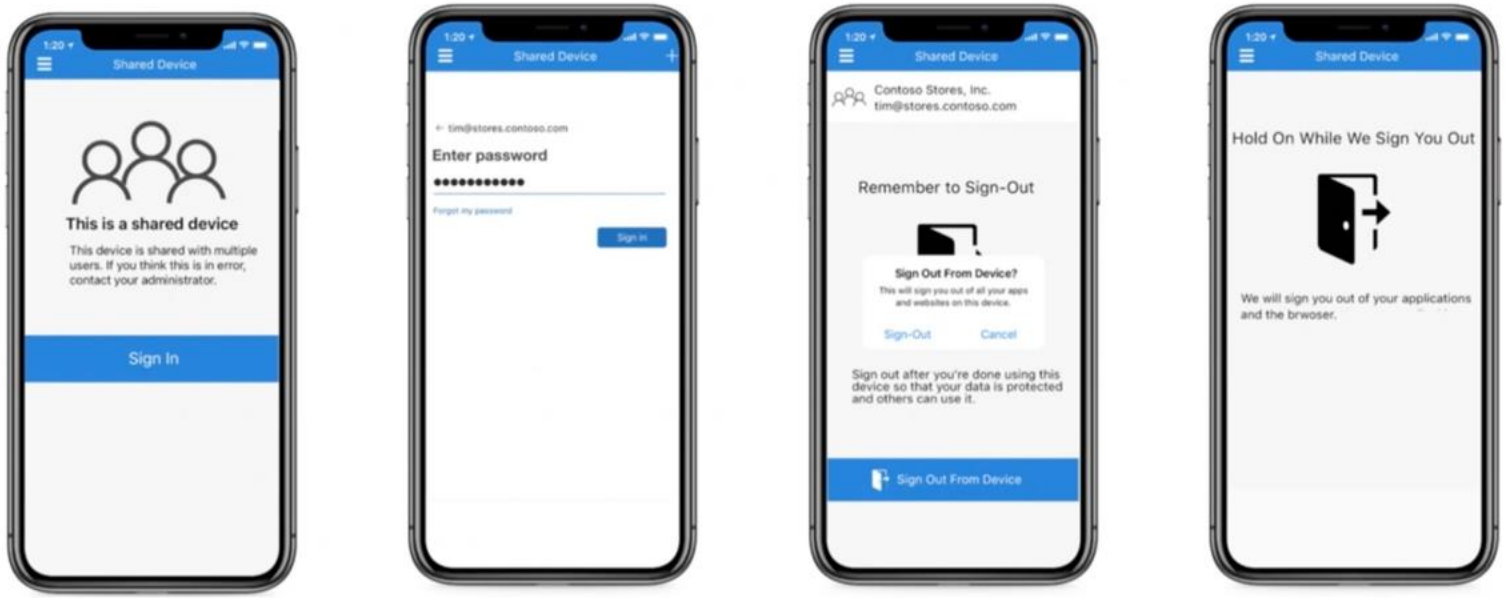
- Intune Plan 1 or higher
- RedHat Enterprise
  - Linux 8
  - Linux 9
- Ubuntu Desktop 22.04 oder 20.04 TS
  - Apple Enrollment Token
- Managed Google-Play Account

Device Enrollment

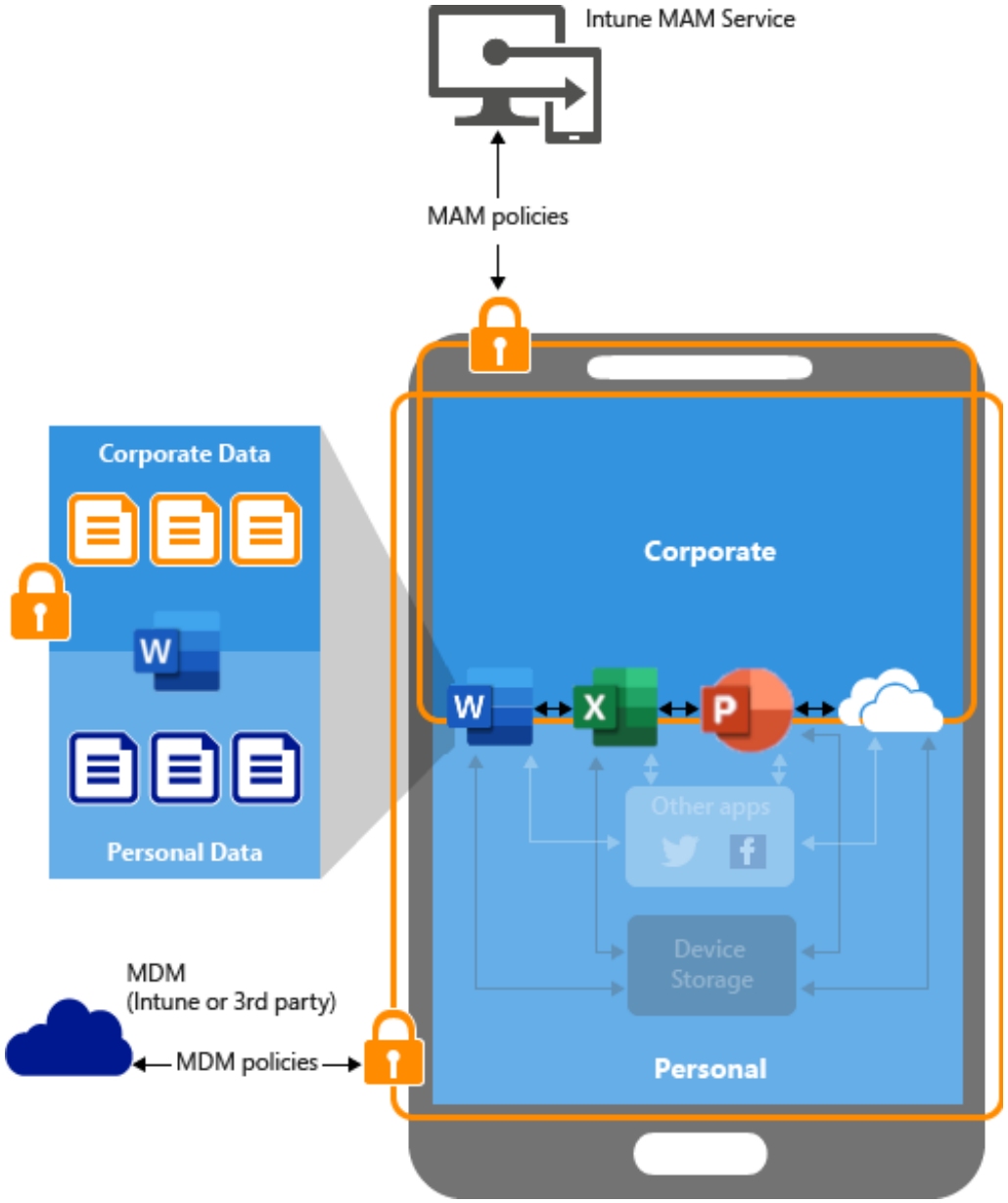
- Corporate-owned
  - Rollout via Intune-App
- BYOD
  - Nicht unterstützt

Shared Devices & Kiosk

Device Plattform	Kiosk	Shared multi-user
Windows	X	X
IOS/iPadOS	X	X
Android	X	X
MacOS	-	X



Apps



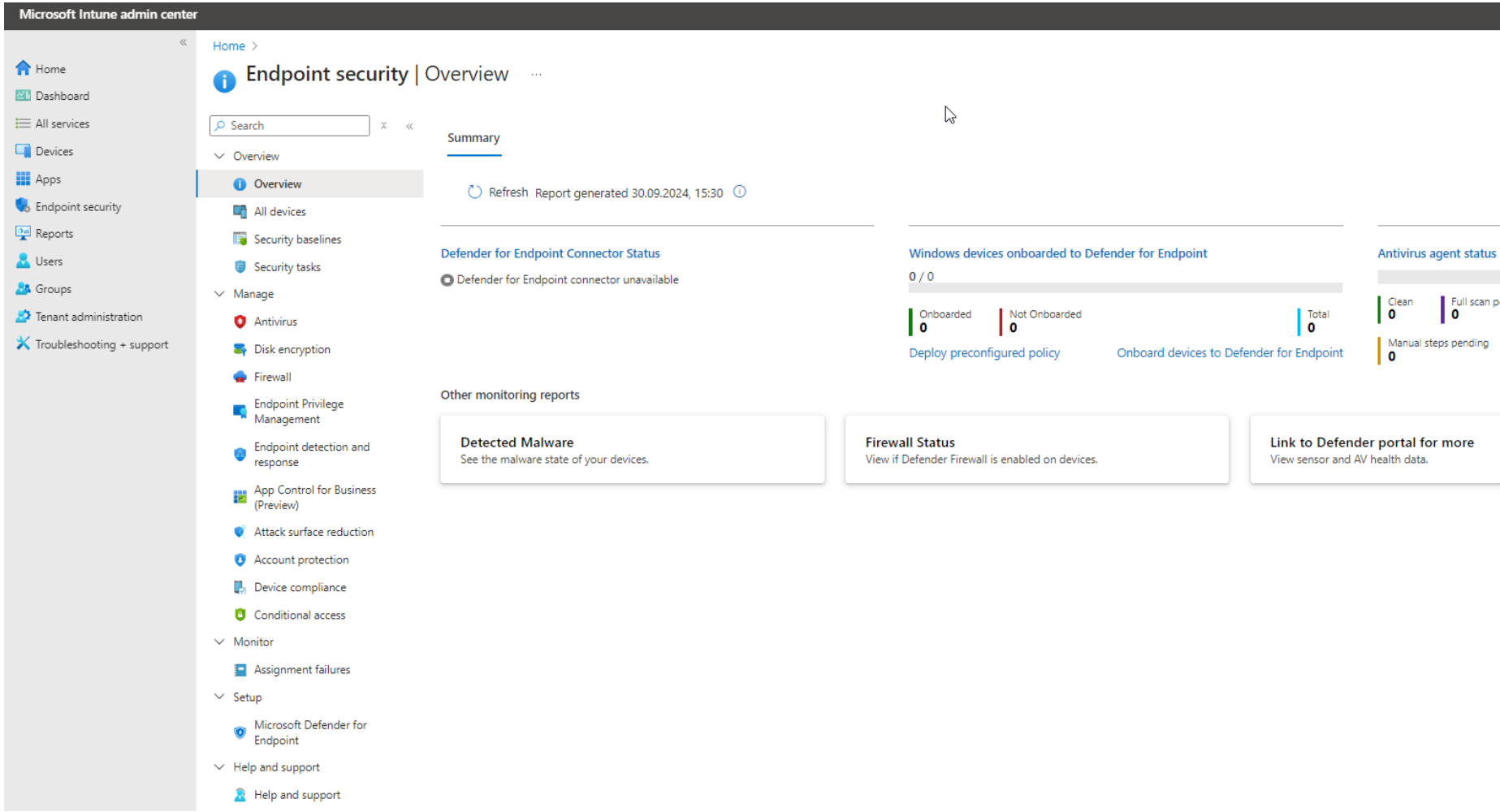
App Protection Policies
+
App Configurations

Device Enrollment
+
Device Configurations

Endpoint Security in Intune

Many paths lead to Microsoft Security settings

- LAPS
- Bitlocker
- Firewall
- Microsoft Defender for Endpoint



Device Management | Zusammenfassung

Wichtige Punkte für unser „Big-Picture“

- Intune als Unified Endpoint Management Tool
- Managed Devices and managed Apps solution
- MEJ or MEHJ?
- Welche Plattformen müssen berücksichtigt werden?
  - Bring your own device oder nur corporate devices?
- Windows Autopilot Deployment

Technische Reihenfolge

Für die optimale Nutzung der Microsoft 365 Dienste ergeben sich Abhängigkeiten.

Daher empfehlen wir die folgende Vorgehensweise:

Identity
Devices
Security

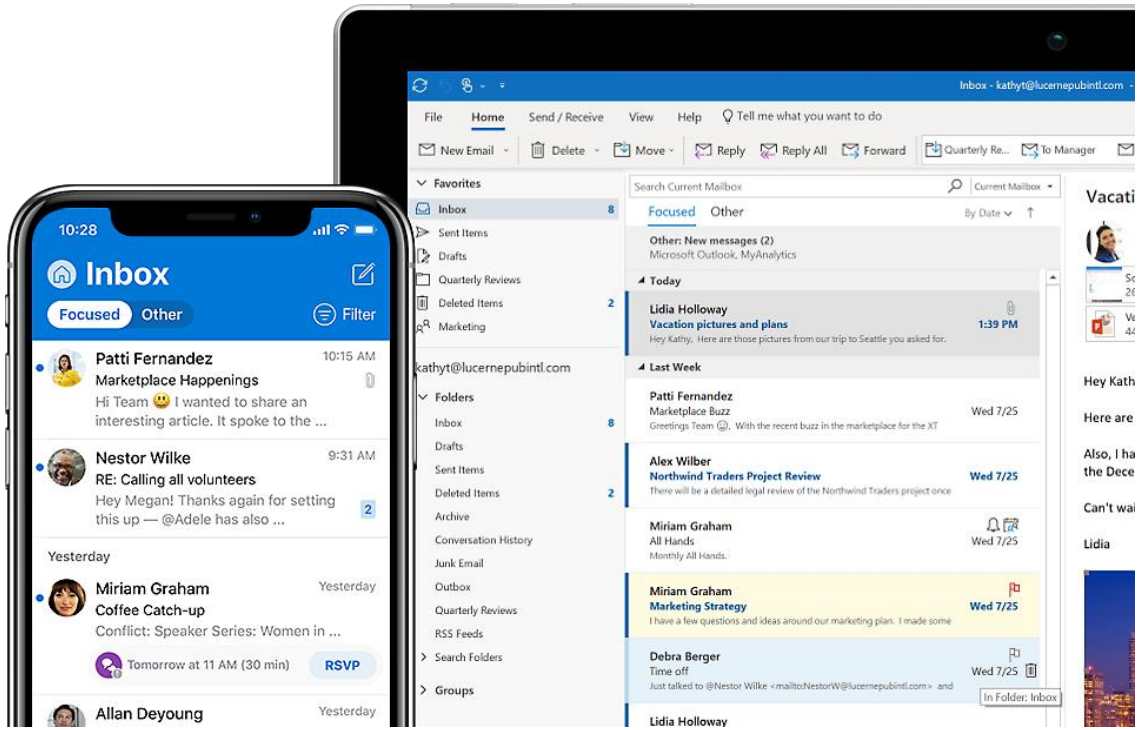
Exchange
Hybrid

OneDrive &
SharePoint

Microsoft
Teams

Microsoft Exchange Basis Informationen

- Groupware Server von Microsoft – Historie seit Exchange 5.5
  - Aktuelle Version: Exchange Server 2019
  - ab Oktober 2025: Exchange Server SE
- Clients:
  - Outlook für Windows, Mac, Android, iOS
  - Outlook on the Web
  - Active Sync (lecacy – nur noch on-premises)
  - IMAP / POP3 / SMTP für spezielle Anforderungen
- Jedes Postfach gehört zu einem AD Objekt
  - Persönliche Postfächer
  - Shared Mailboxes
  - Verteilerlisten
- Jedes Postfach verfügt über eine einheitliche Ordnerstruktur
  - Posteingang, Gesendete Objekte, Gelöschte Objekte, Papierkorb, Kalender, Kontakte, Notizen
  - Aufgaben nur noch On-Premises – in der Cloud: ToDo
- Öffentliche Ordner



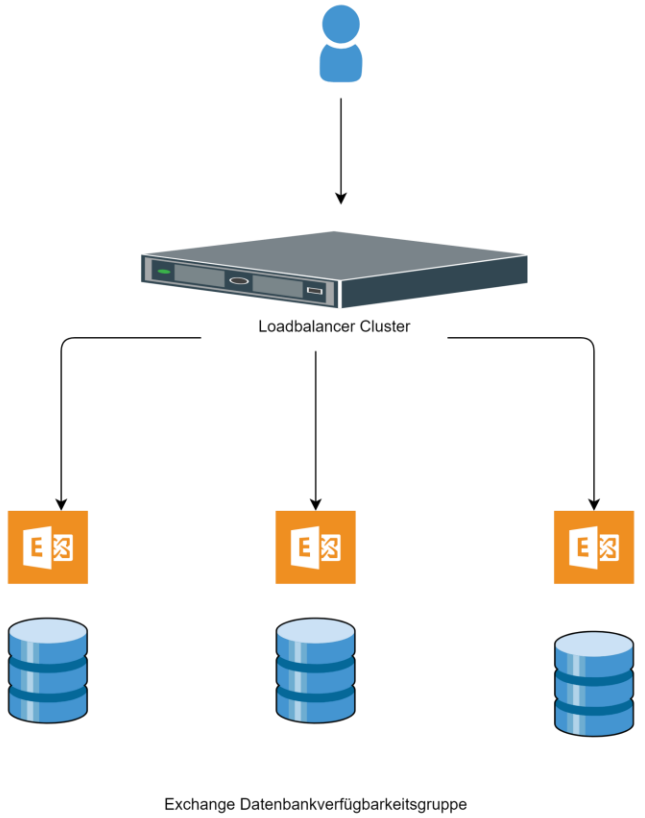
Microsoft Exchange Architektur On-Premises

- Ein Cluster wird über eine Datenbankverfügbarkeitsgruppe (DAG) realisiert.

- Jeder DAG Knoten verfügt über lokales Storage mit geringer IO-Anforderung.
- Datenbanken können eine oder mehrere Kopien auf anderen Cluster-Knoten haben. Die Inhalte werden durch Exchange synchronisiert.
- Ein Failover erfolgt automatisch.

- Der Zugriff von den Clients erfolgt über HTTPS bzw. MAPI/HTTPS.
- Für eine DAG wird ein Loadbalancer Cluster benötigt.
  Der Loadbalancer verteilt die Client-Zugriffe, ermöglicht Failover-Szenarien und steuert auch den E-Mail-Flow.

- Das Exchange Sizing erfolgt anhand des „Role Calculators“.
- Klärung von Details erfolgt in einem Exchange Design Workshop innerhalb des Umsetzungsprojektes.



Microsoft Exchange Hybrid

Warum benötigen wir Exchange Hybrid?

- Postfachmigration nach Exchange Online
- Teams Zugriff auf Kalender in lokalem Postfach
- Einheitliches Globales Adressbuch
- Sicheres E-Mail Routing
- Frei/Gebucht Informationen
- Mail Tipps
- Kalenderzugriff

Zentrale Verwaltung über Exchange On-Premises

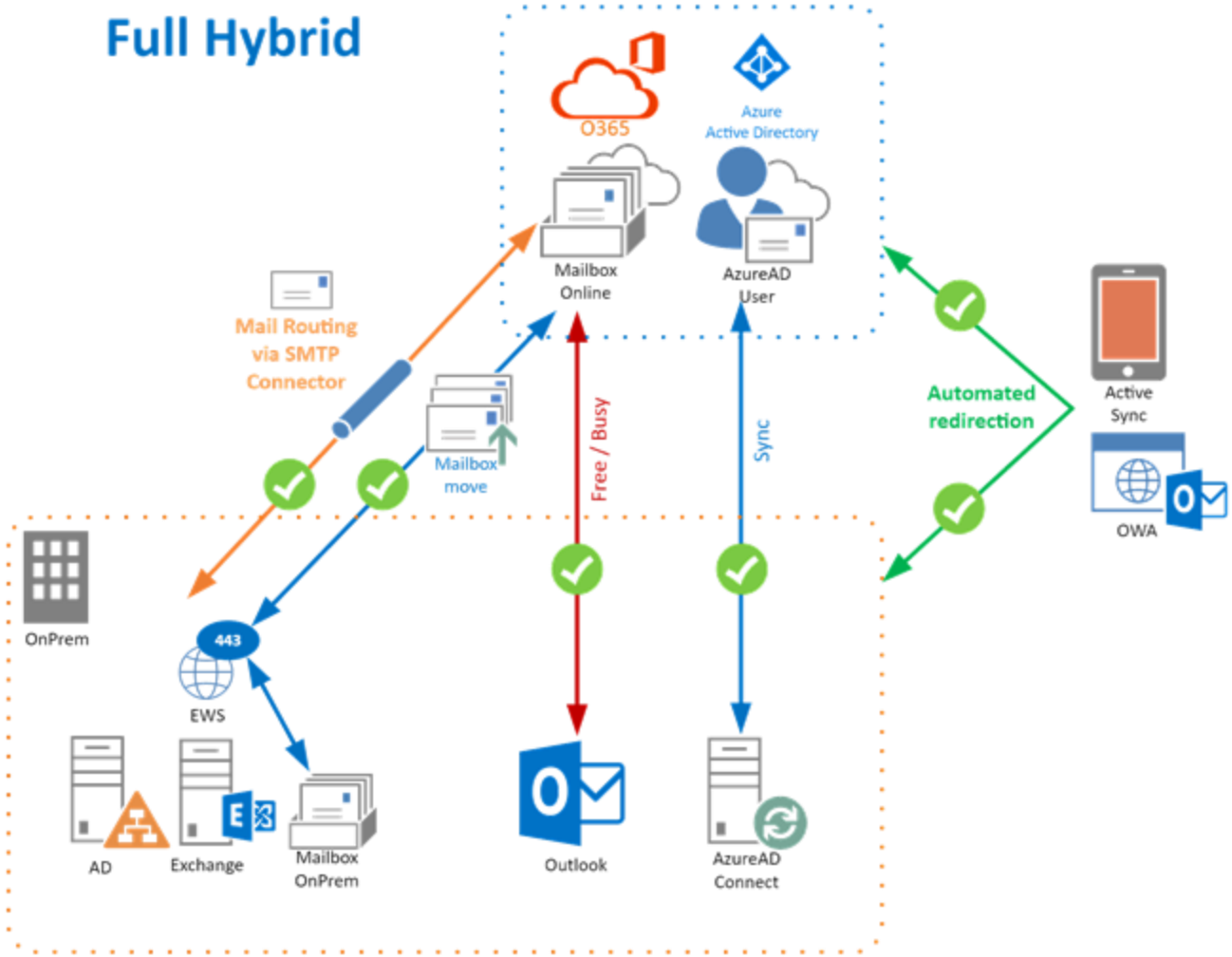
Microsoft Exchange Hybrid Varianten

	Beschreibung	AAD Connect	SMTP Connector	EWS Publishing	Free / Busy Fed-Trust
Minimal Hybrid	Ziel ist eine schnelle Migration ohne Koexistenz	✓	✗	✓	✗
Full Hybrid (Classic)	Vollständige Hybrid Konfiguration mit allen Funktionen	✓	✓	✓	✓
Modern Hybrid (Agent)	Keine Exchange Veröffentlichung notwendig Leicht eingeschränkter Funktionsumfang	✓	✗	✗	✓

Exchange 2016 CU 3 ist Voraussetzung für vollen Funktionsumfang

- Native Mode (keine älteren Serverversionen)
- Modern Authentication
- REST API
- https://learn.microsoft.com/de-de/microsoftteams/exchange-teams-interact

Microsoft Exchange Hybrid Architektur

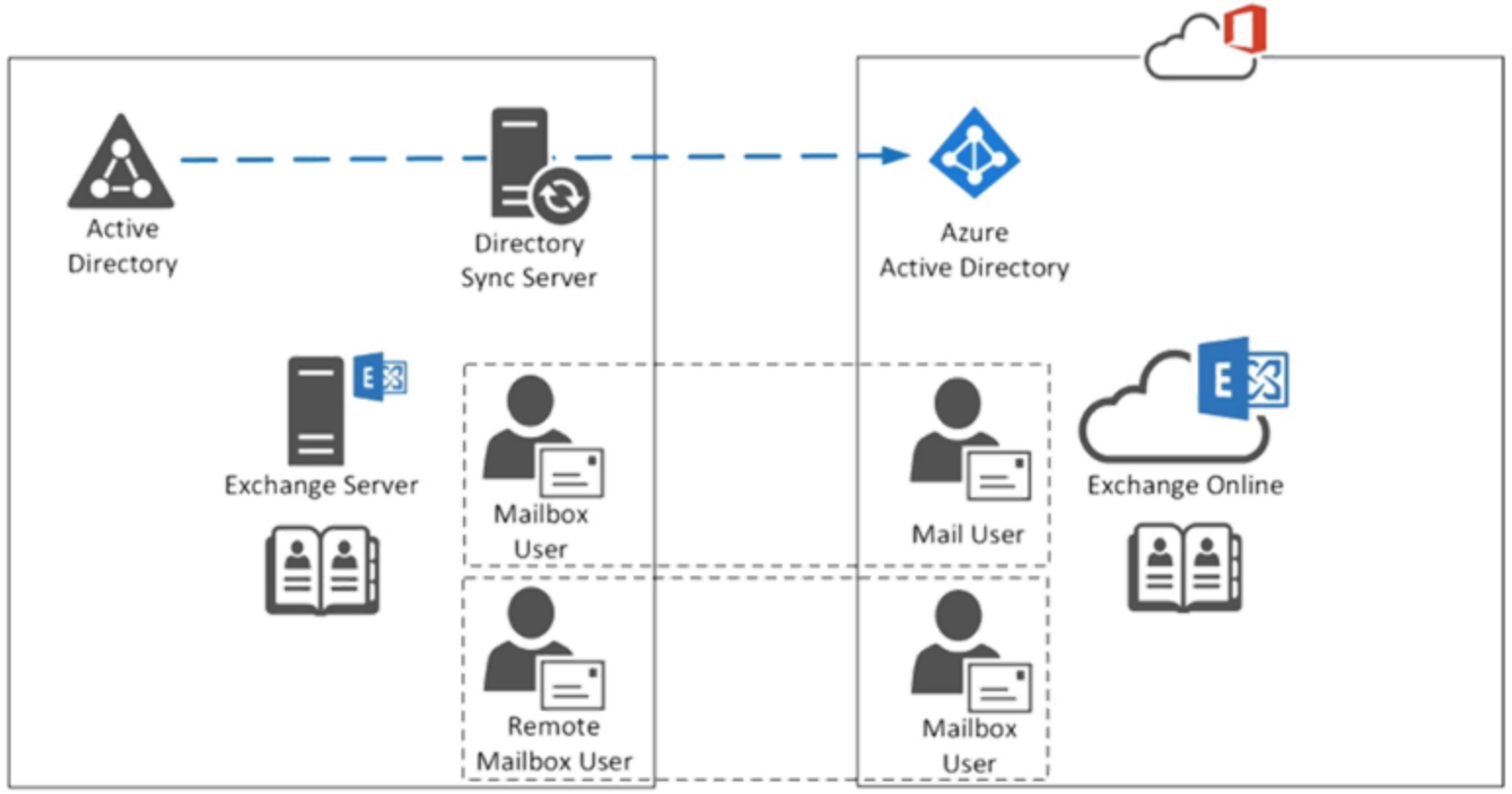


Hybrid Varianten Deep Dive

	Minimal Hybrid	Full Hybrid(Classic)	Modern Hybrid (Agent)
Mailrouting OnPrem ← → EXO Über SMTP Connector (TLS)	Nein (manuell möglich)	Ja	Nein (per Internet)
Gemeinsamer Adressraum	Ja	Ja	Ja
Identisches Adressbuch	Ja	Ja	Ja
Free / Busy Anzeige	Nein (manuell möglich)	Ja	Ja
Out of Office / Mailtipps	Nein	Ja	Ja
OWA / ActiveSync Redirection	Nein	Ja	Ja
Centralized Mail Flow	Nein	Ja	Ja
Teams kann OnPrem Kalender anzeigen	Nein	Ja	Nein
Message Tracking in beiden Umgebungen	Nein	Ja	Nein
Mehrere Migration Endpoints möglich	Ja	Ja	Nein
Mailbox Move in beide Richtungen	Nein	Ja	Ja
Hybrid Modern Authentication (HMA)	Nein	Ja	Nein

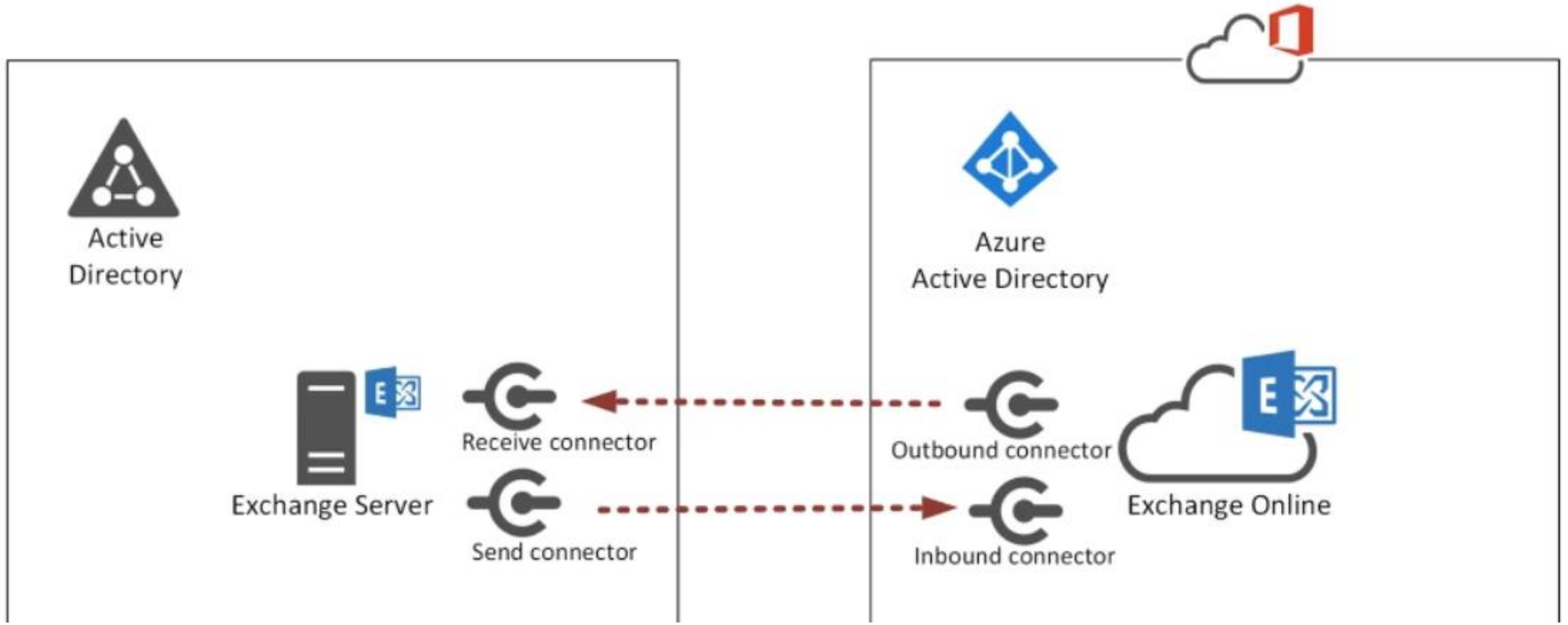
Microsoft Exchange Hybrid

- Sync der Objekte über Entra Connect
- Remote Mailbox Provisierung



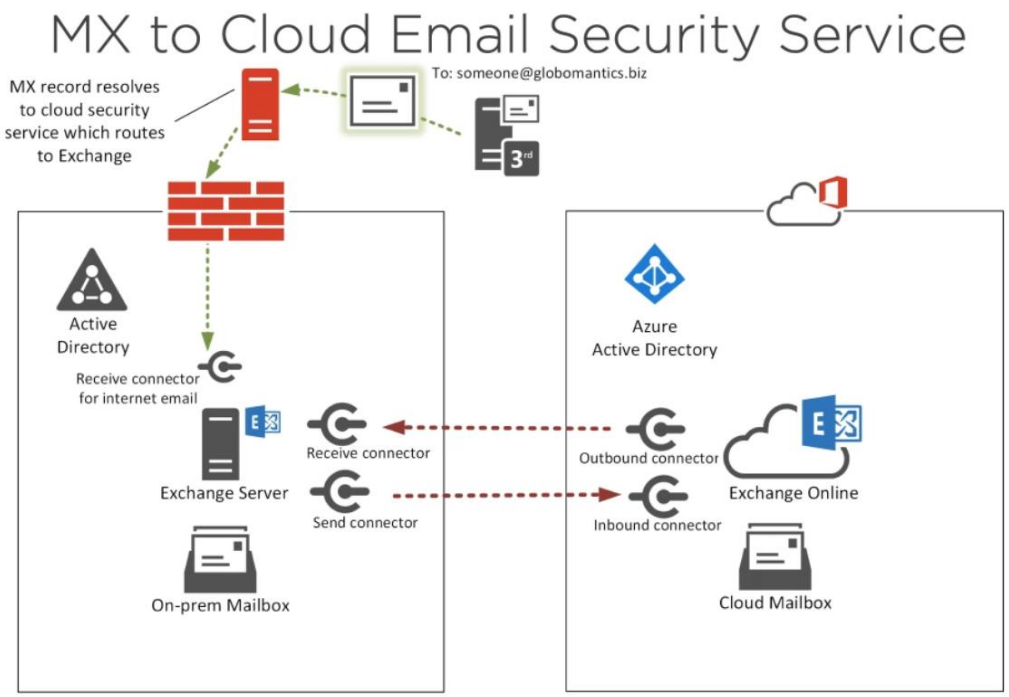
Microsoft Exchange Hybrid

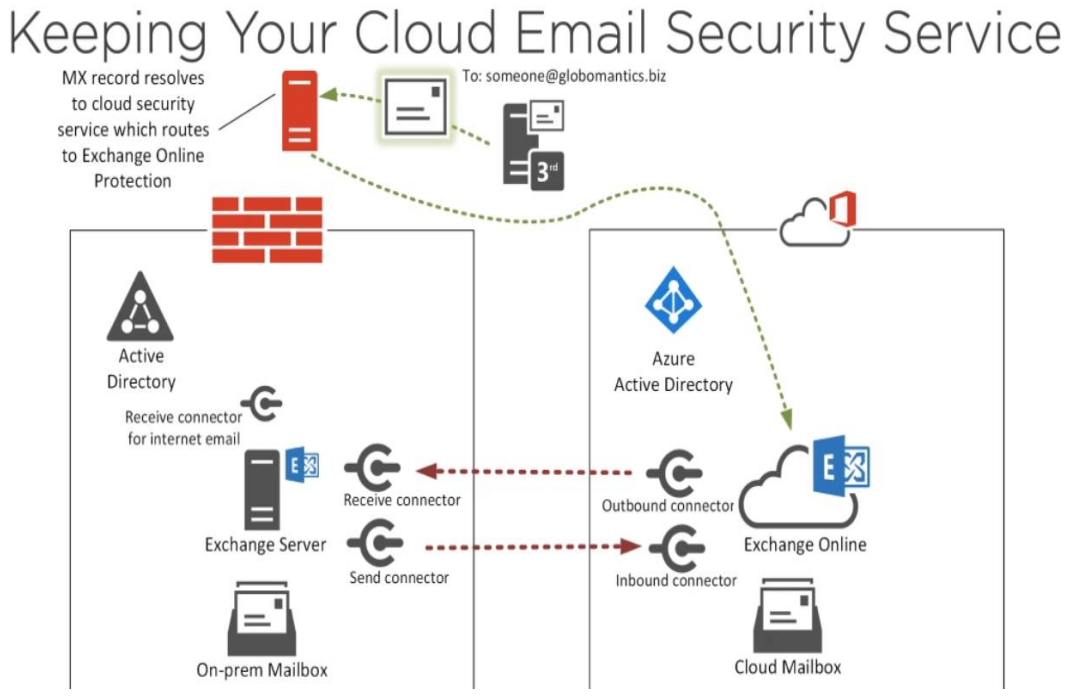
Mail Fluss über dedizierte Connectoren



Microsoft Exchange Hybrid

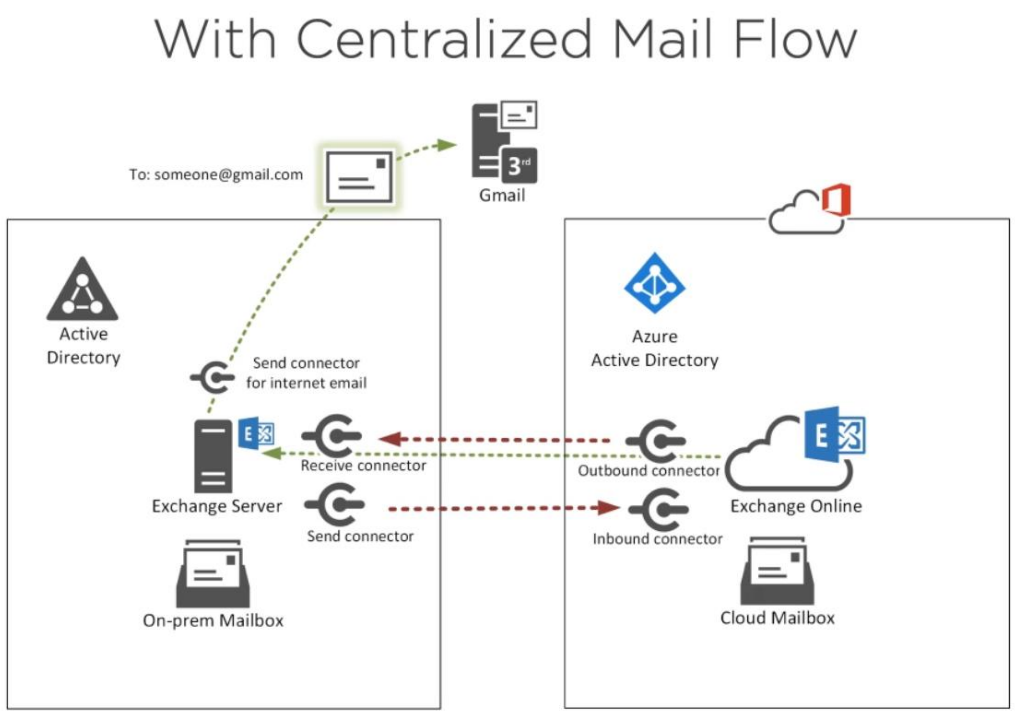
Mail-Flow eingehender Mails:

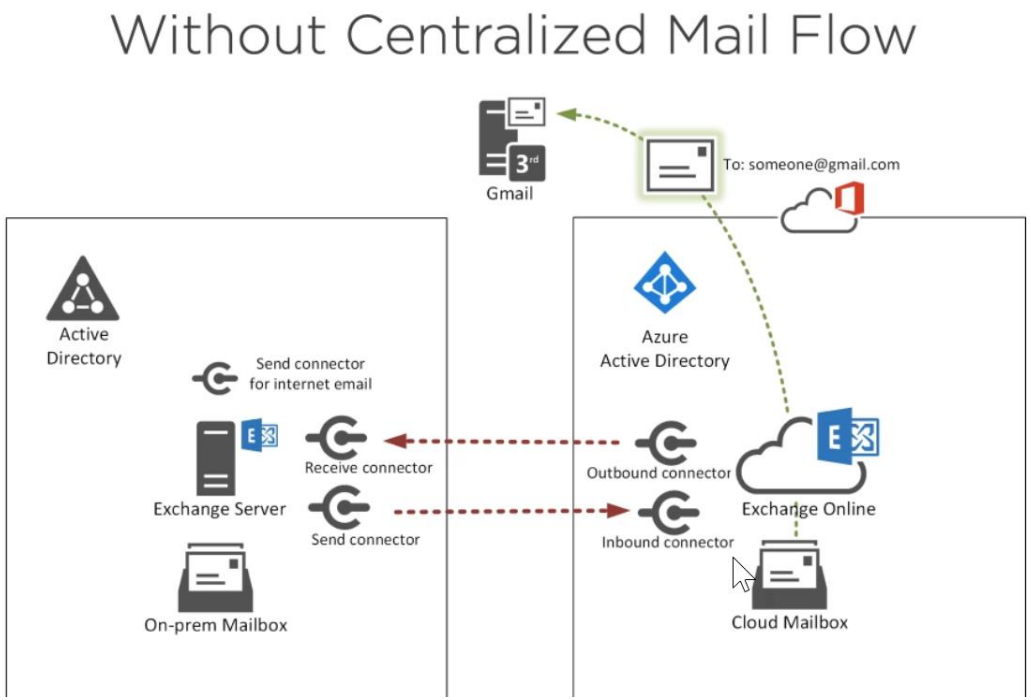




Microsoft Exchange Hybrid

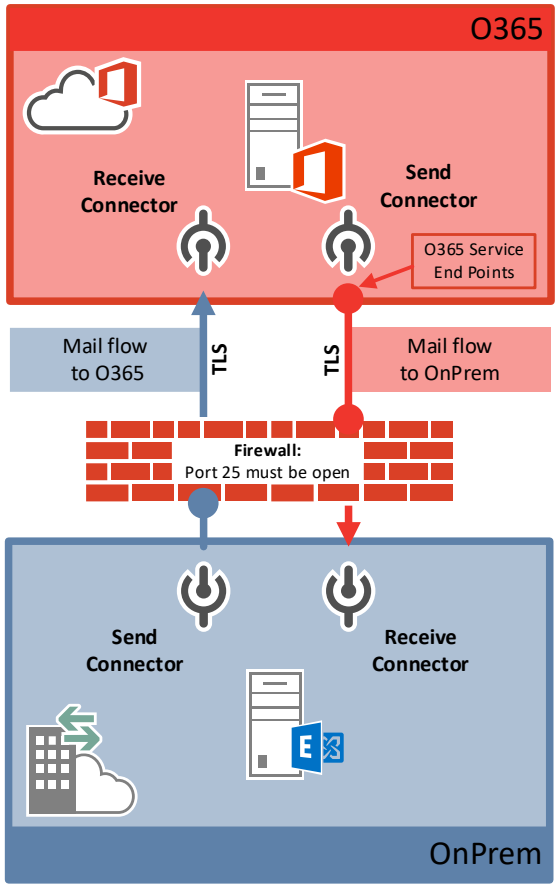
Mail-Flow ausgehender Mails:

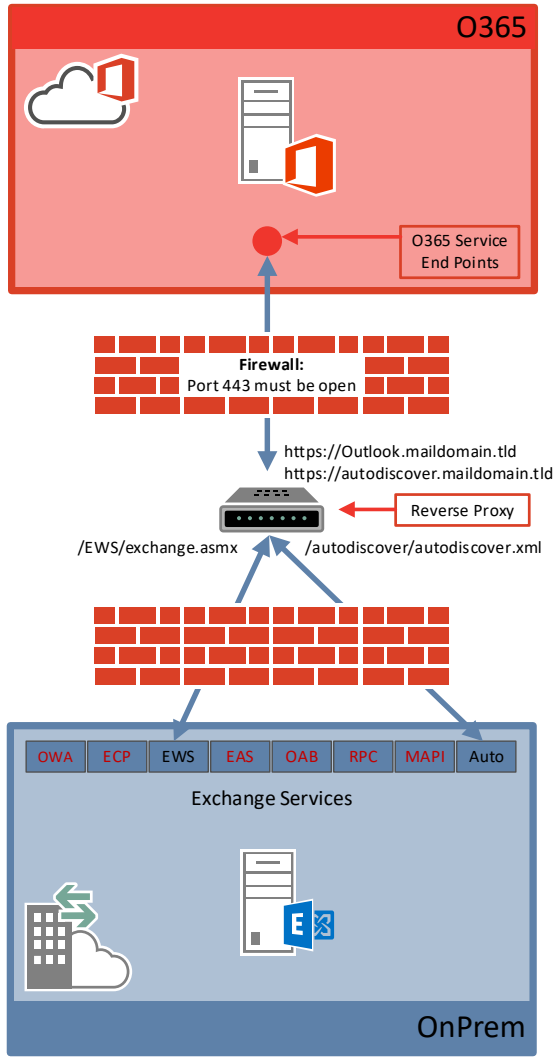




Microsoft Exchange Hybrid

Firewall Anforderungen





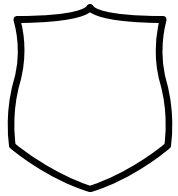
Einschränkungen bei On-Premises Postfächern

- Microsoft 365
  - To Do & Terminabfrage stehen nicht zur Verfügung
  - Keine Anzeige von Microsoft 365 Gruppen in Outlook
  - Share-to-Teams aus Outlook heraus ist nicht möglich
  - Keine Power Apps, Power Automate Flows mit Mailbox Zugriff
  - Keine Konfiguration der Microsoft 365 Gruppen - Mailbox Sprache als Nutzer-Self-Service, daher Benachrichtigungen z.B. von Planner immer in Englisch
  - Bookings steht nicht zur Verfügung
- Outlook App (iOS/Android) bietet mit Online Mailboxen auch Zugriff auf Shared Mailboxes / Stellvertreter-Postfächer
- Teams
  - Voicemail in Teams: keine Transkription
  - Ansicht über alle öffentlichen Teams im Teams Client
  - Terminkategorien aus Outlook werden nicht angezeigt
- Viva Insights liefert nur eingeschränkt Informationen
- Security
  - Keine Conditional Access Policies / Device Authentication für Exchange OnPrem Postfächer
  - Kein Zero Hour Auto Purge (Exchange Online Protection / Defender for O365)

Microsoft Exchange Hybrid Implementierung

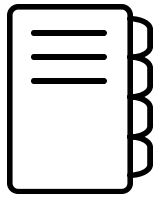
- Voraussetzungen + Architektur
  - Klärung 3rd Party
- Basiskonfiguration
  - Exchange Publishing
- Einrichtung Hybrid
  - Bereinigung vor Migration
- Onboarding Mailboxen
  - Cleanup

Microsoft Exchange Integrationen

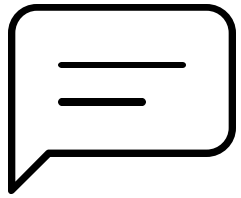


Mailsecurity Gateway

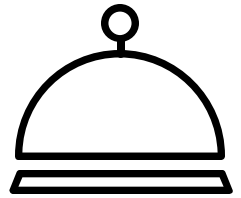
Verschlüsselungs-gateway



Archivierung

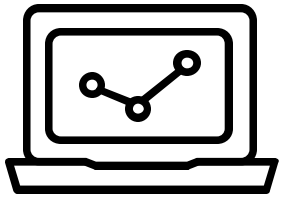


Fax / SMS Gateway

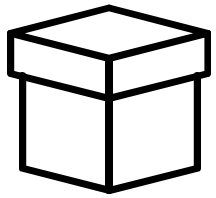


Event-Catering

Signaturlösung



Scanner

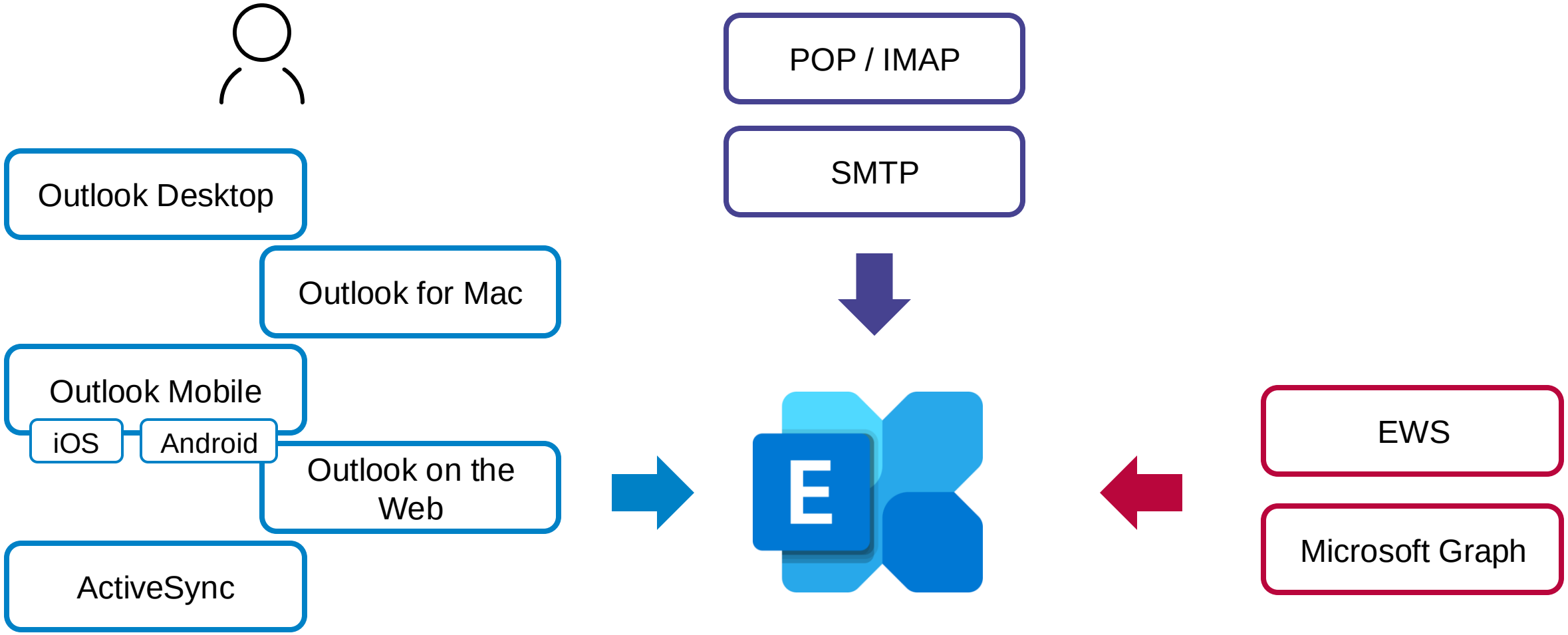


Backup

Digital Signage Boards

...

Microsoft Exchange Zugriffsprotokolle



Microsoft Exchange Management Server

- Nur notwendig bei aktivem Entra Connect
  (read-only Attribute in der Cloud)

- Der On-Premises verbleibende Exchange Server kann unter folgenden Voraussetzungen ausgeschaltet (gelöscht) werden:
  - ab Exchange 2019 CU12 (2022 H1) – Installation Management Tools Server 2019 / Client
  - Alle Mailboxen inkl. Öffentliche Ordner in EXO
  - Kein RBAC benötigt

- Verwaltung nur mit PowerShell Snap In möglich

- Verlagerung von SMTP Rolle für 3rd Party Devices auf andere Lösung erforderlich

E-Mail Signatur Management

- Zentrale Verwaltung von Signaturen und Disclaimer
- Einheitliches Unternehmensdesign für E-Mail Kommunikation
- Automatisierte Bereitstellung
- Verhindern von Inkonsistenzen durch manuelle Prozesse
- Zeitgesteuerte Kampagnen (Events, Aktionen, etc.) auch für einzelne Abteilungen möglich
- Delegieren der Verwaltung (z.B. Marketing Abteilung) möglich

CodeTwo Email Signatures 365

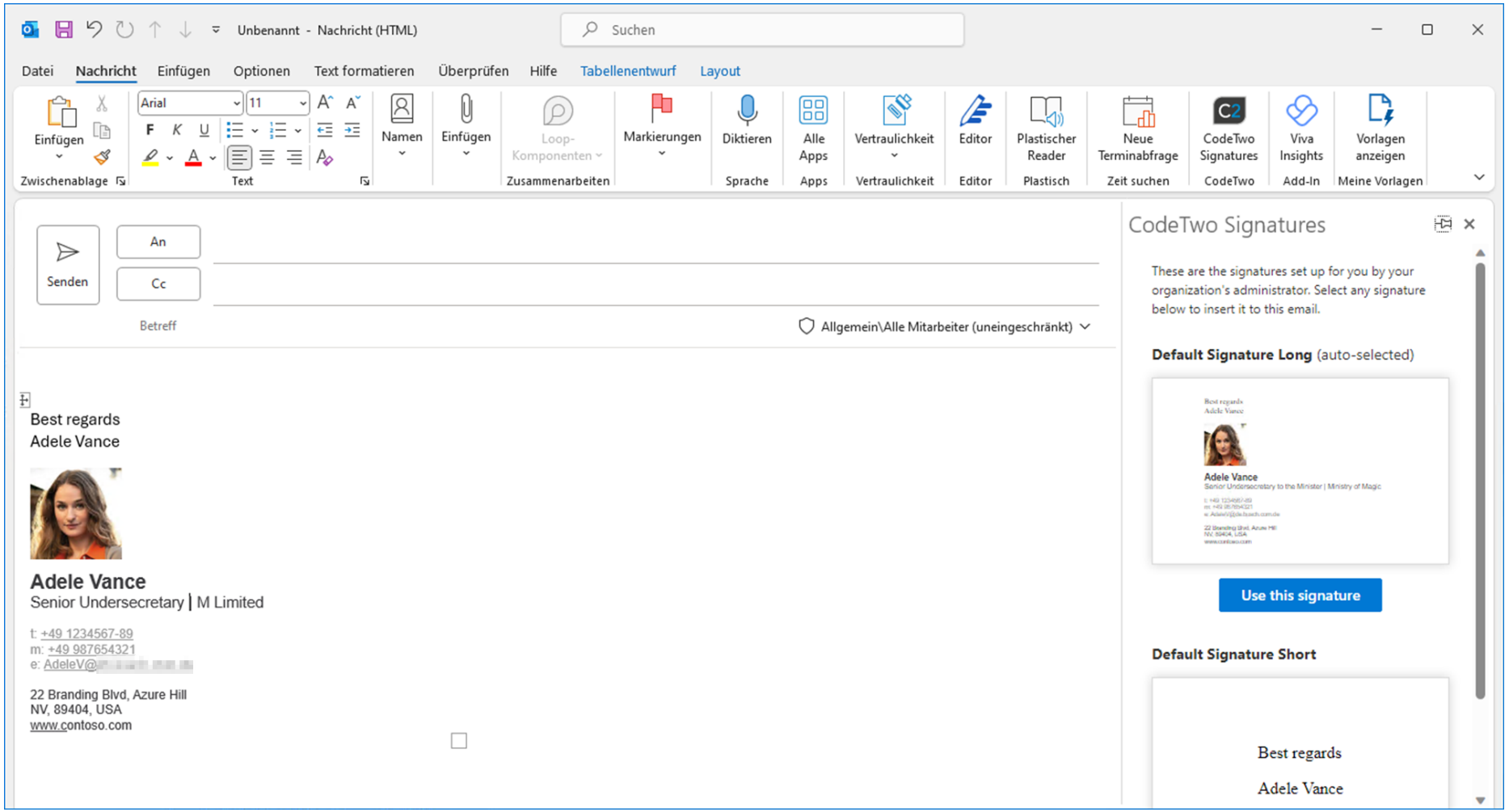
- Zentrales Management (Webinterface)

- Signaturen werden über Templates generiert und mit dem Add-In abgerufen
- Verteilung des Add-In via Login-Skript, Gruppenrichtlinie (GPO), Software Verteilung oder Microsoft 365 Admin Center möglich.
- Zuweisung von Signaturen basierend auf Gruppen- oder Benutzerbenutzerebene

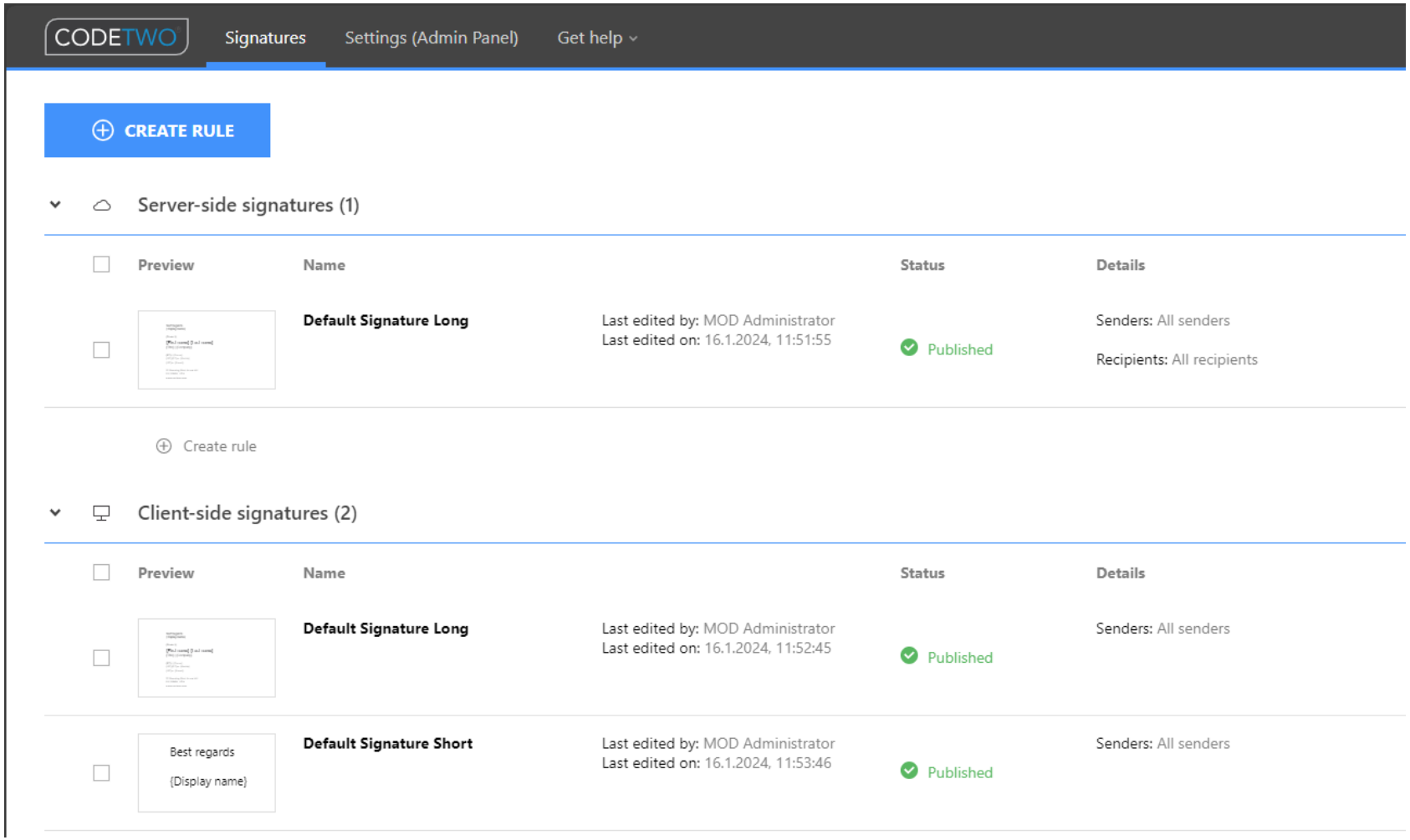
- Auswahl der Signatur durch den Benutzer möglich, wenn mehrere Signaturen zur Verfügung stehen
- Unterschiedliche Signatur für Neue Nachrichten / Weiterleitung und Antworten / OWA / Mobile Devices möglich. Konfiguration des Outlook Profiles erfolgt über Zuweisung der Signatur.

- Anbindung an Microsoft Entra ID
- Im Exchange Hybrid können nur Nachrichten verarbeitet werden, die durch Microsoft 365 (EOP) fließen.
- Office 365 Message Encryption, S/MIME o.ä. nur im Client- oder Combo-Modus unterstützt.
- Unterstützung mehrerer Outlook Profile

CodeTwo Email Signatures 365



CodeTwo Email Signatures 365



Exchange Online | Zusammenfassung

Wichtige Punkte für unser „Big-Picture“

- Wo liegen die Postfächer?
- Schema Erweiterung + Entra Connect
- Lokaler Exchange Server oder Management Shell
- SMTP Relay
- Anpassungsbedarf
- eventuelle Add Ons

Technische Reihenfolge

Für die optimale Nutzung der Microsoft 365 Dienste ergeben sich Abhängigkeiten.

Daher empfehlen wir die folgende Vorgehensweise:

Identity
Devices
Security

Exchange
Hybrid

OneDrive &
SharePoint

Microsoft
Teams

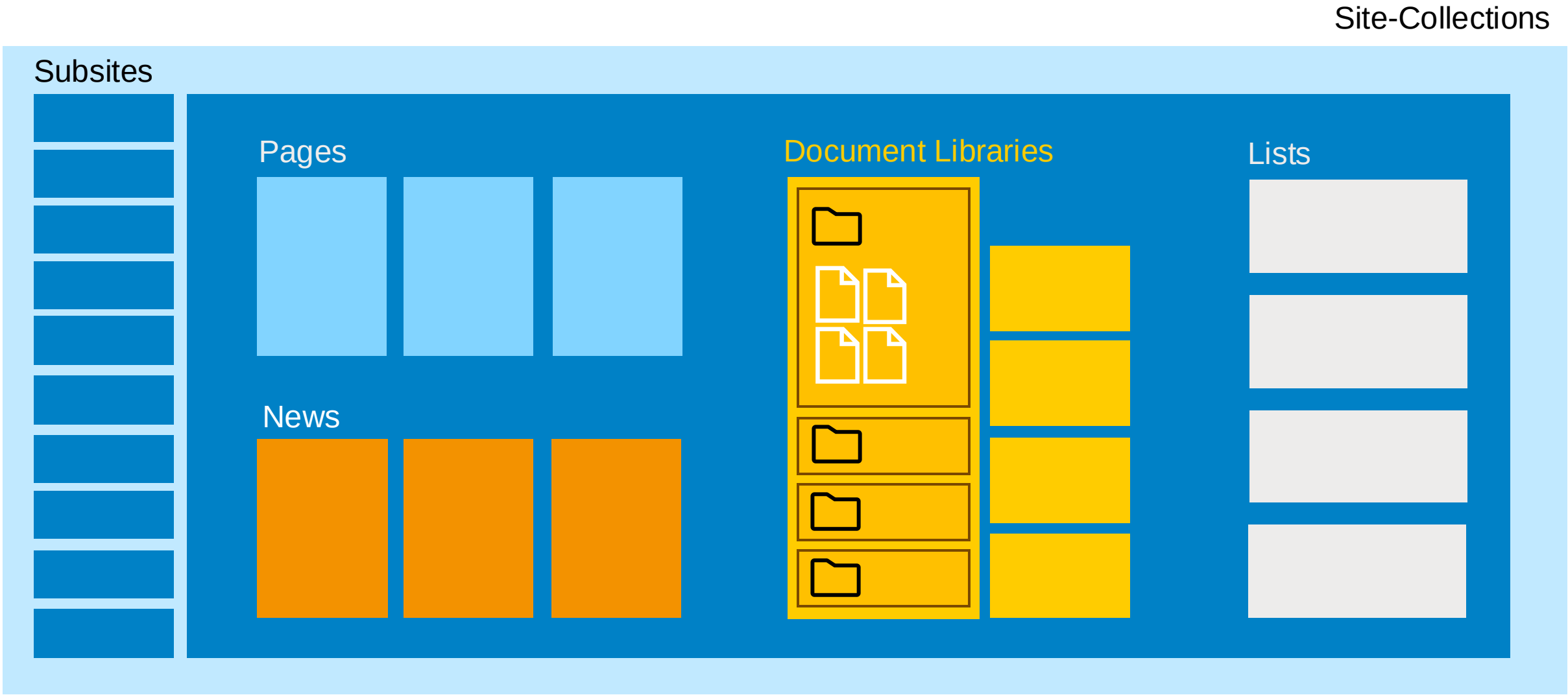
SharePoint Online

- cloudbasierte Kollaborations- und Dokumentenmanagement-Plattform
- Datenspeicherort für Dateien aus Microsoft Teams
- Es ermöglicht Benutzern Dokumente, Inhalte und Ressourcen zu speichern, freizugeben, zu organisieren und gemeinsam zu bearbeiten.
- Es bietet Funktionen wie
  - Versionierung,
  - Genehmigungs-Workflows,
  - Suchfunktionen,
  - Zugriffssteuerungen,
    um die Sicherheit und Integrität von Daten zu gewährleisten.

SharePoint Online – Site-Typen

Feature	Team Site	Communication Site
Wer darf die Seite erstellen?	Recht zur Websiteerstellung (+Personen die M365 Gruppen erstellen dürfen)	Recht zur Websiteerstellung
Wer erstellt Inhalte?	Alle Mitglieder sind Autoren	Kleine Anzahl von Autoren Große Anzahl von Konsumenten
Sicherheit	M365 Gruppen, SharePoint Gruppen	SharePoint Gruppen
Externes Teilen	Standardmäßig eingeschaltet	Standardmäßig ausgeschaltet
Navigation	Standardmäßig Links	Standardmäßig Oben
Technische Abbildung	M365 Gruppe oder Nur Team Site ohne M365 Gruppe	Nur Communication Site

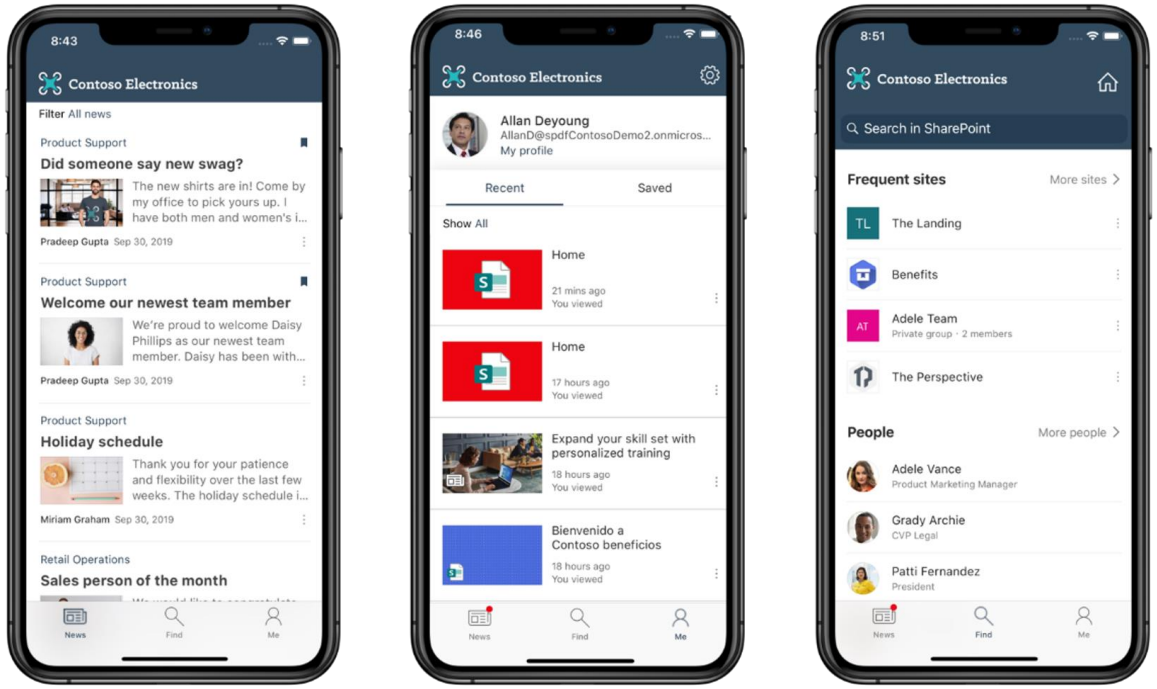
SharePoint Online – Sites Architektur



SharePoint Online – Hub Sites

- Kann sowohl aus einer Team als auch aus einer Communication Site entstehen
- Information Rollup:
  Einer Hub Site werden andere Site Collections zugeordnet, um Inhalte aus mehreren Site Collections auf einer Site anzeigen zu können
- Eine Hub Site definiert eine einheitliche Navigation für alle angehängten Site Collections
- Hub-übergreifende Suche möglich

SharePoint Online – Mobile



- Anzeige von News aus diversen Site-Collections, auf die man Zugriff besitzt
- Anzeige ist automatisch mobile responsive
- Benachrichtigung über App möglich
- Document handling in der OneDrive-App (Analog zum PC)

SharePoint Online – Limits

Speicherkapazität pro Tenant:	1TB + 10GB*Anzahl (Lizenz) außer F1/F3 Lizenzen
Site Collections pro Tenant:	2.000.000
Hubsites pro Tenant:	2.000
Fileuploadlimit:	250GB
Maximale Pfadlänge:	400 Zeichen
Maximale Anzahl von Elementen in Lists/DocLibs:	30.000.000
Maximale Anzahl Lists & DocLibs:	2.000
Versionierung	
Hauptversionen:	max. 50.000
Nebenversionen:	max. 511

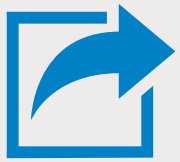
OneDrive for Business

Persönliches Nutzer Laufwerk in der Cloud

- 1 TB Standard Kapazität
- Ab O365 E3-Plan erweiterbar auf bis zu 5 TB / Nutzer
- Zählt nicht in das SharePoint Online Speicher Limit

Sync Client

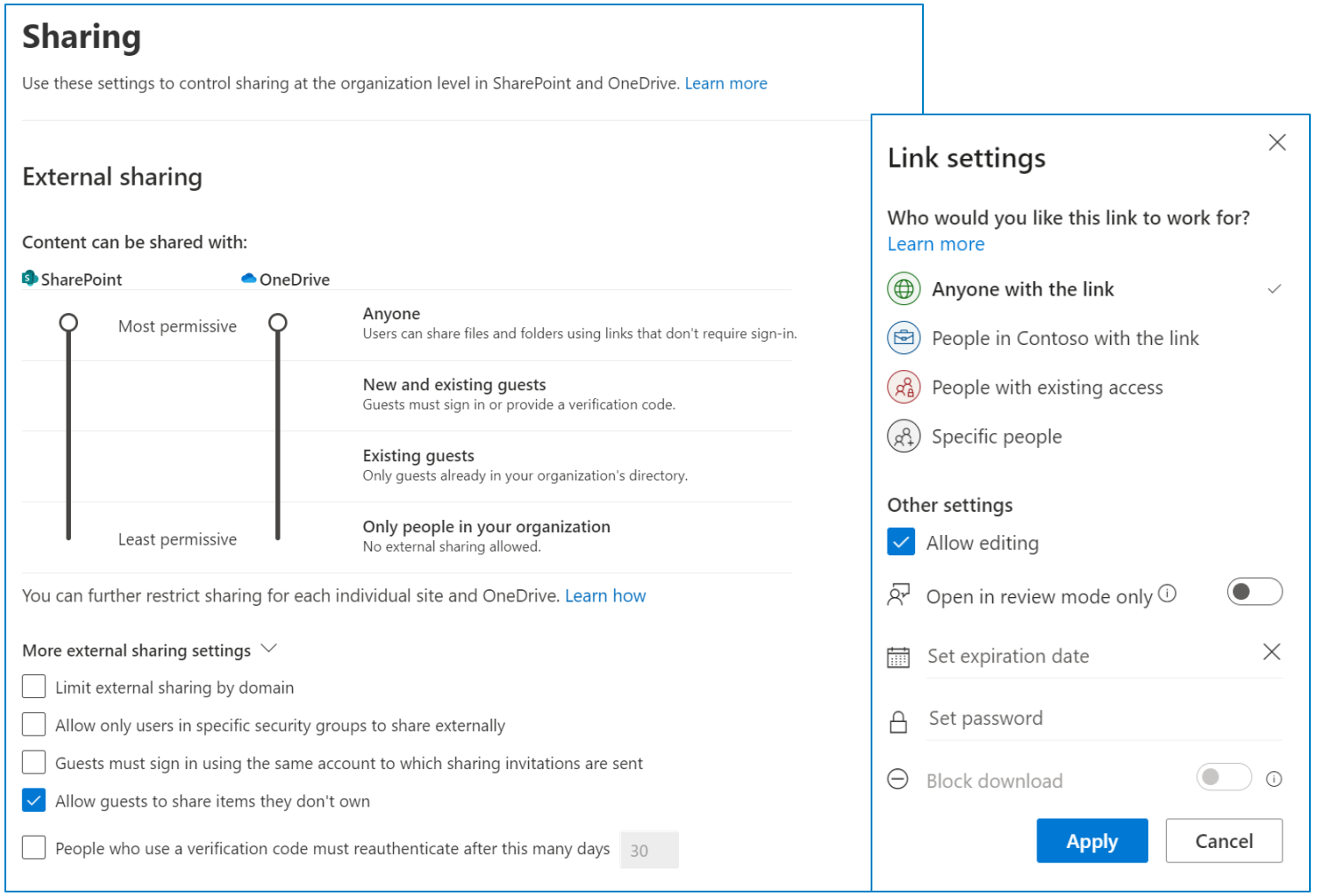
- Ist in Windows integriert
- Known Folder Move leitet Dokumente, Bilder und Desktop nach OneDrive um
- Für andere Plattformen als App verfügbar
- Konfiguration über Gruppenrichtlinien oder Intune



Zusammenarbeit mit Externen

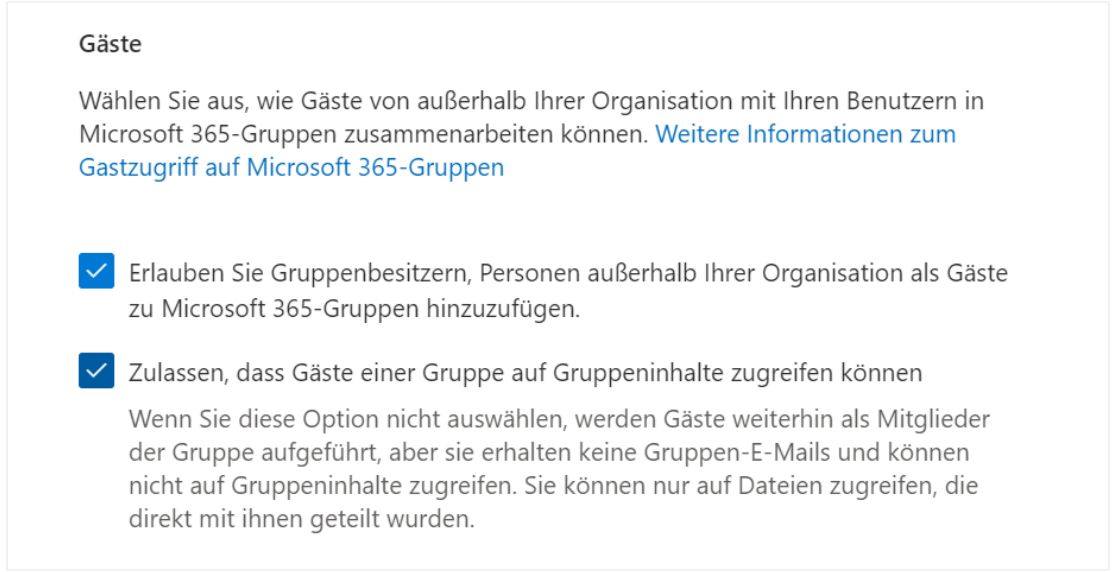
Externes Teilen

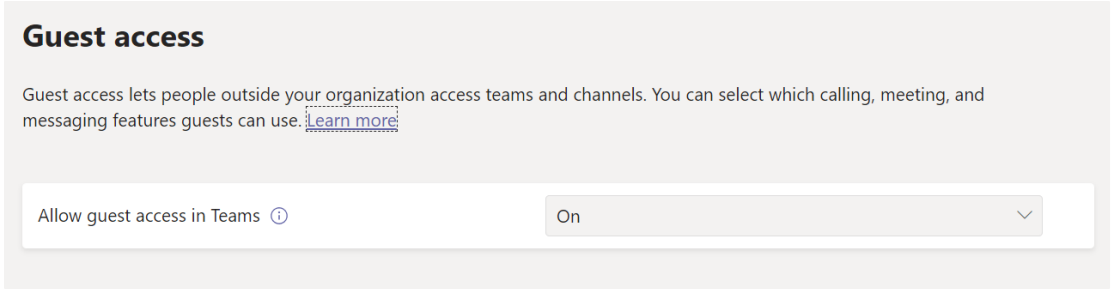
- Ad Hoc Teilen von Dateien oder Ordnern aus SharePoint Online oder OneDrive for Business
- Standard: „Jeder“ sollte angepasst werden
- Alternativ:
  - Gastkonten
  - Verifizierungscode
- Ad Hoc Recipients sind abgekündigt
- Absicherung über Conditional Access und Purview möglich



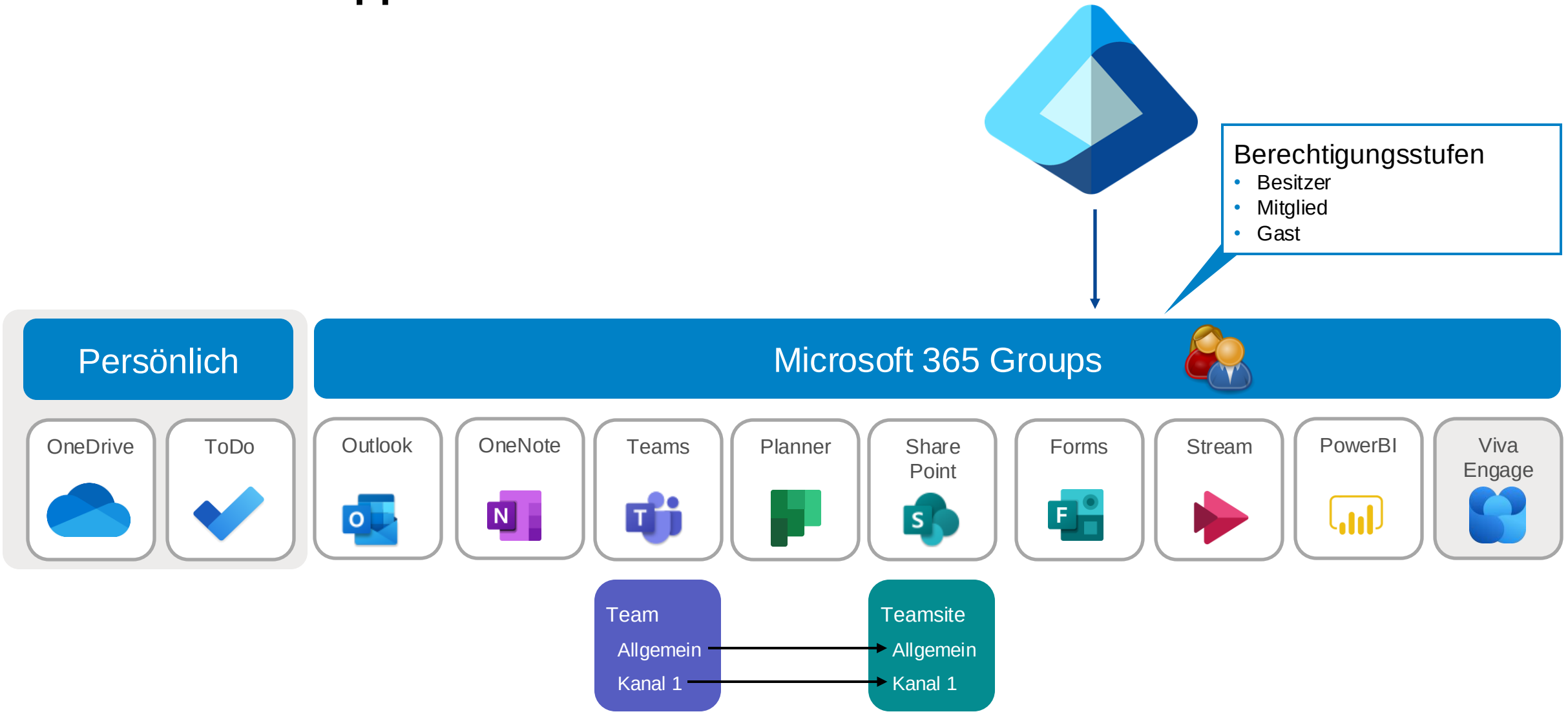
Gastkonten

- Zusammenarbeit mit Externen
- Entra ID Gastkonto auf Grundlage einer eigenen Identität
- Konfiguration in den unterschiedlichen Diensten sollte einheitlich sein (Entra ID, SharePoint, Teams)
- Gastkonten Lebenszyklus festlegen
- Absicherung über Conditional Access und Purview möglich





Microsoft 365 Gruppen



SharePoint & OneDrive | Zusammenfassung

Wichtige Punkte für unser „Big-Picture“

- SharePoint Online als Backend für Teams
- SharePoint Online als Intranet Lösung?
- Sharing Policies
- Gast-Konten
  - Wer darf einladen?
  - Lifecycle?
- Wer darf extern teilen
- OneDrive als Ersatz für das Homelaufwerk?
  - Mit Known Folder Move?

Technische Reihenfolge

Für die optimale Nutzung der Microsoft 365 Dienste ergeben sich Abhängigkeiten.

Daher empfehlen wir die folgende Vorgehensweise:

Identity
Devices
Security

Exchange
Hybrid

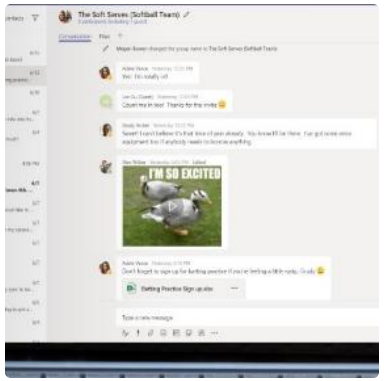
OneDrive &
SharePoint

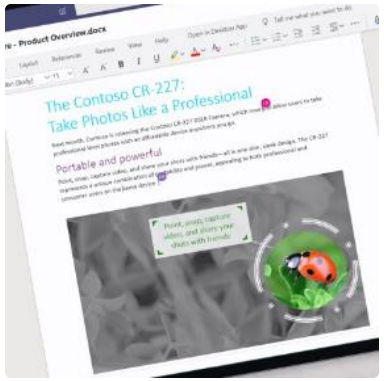
Microsoft
Teams

Microsoft Teams

Zentraler Hub für die tägliche Arbeit

Eine Plattform für Kommunikation und Kollaboration





Besprechungen	Chat	Anrufe	Kollaboration	Automatisierung

Client / App für alle Plattformen und Web-Zugriff

- Limitierungen bei der Nutzung unter VDI/RDSH

Microsoft Teams – Funktionen im Detail

- Kommunikation
  - 1:1 und Gruppenchat – persistent, Teilen von Dateien
  - Audio- und Videochat, Desktopsharing
  - Telefonie – Ablösung klassischer Telefonsysteme
- Besprechungen
  - Desktopsharing, Breakout-Rooms, Meeting-Reaktionen, Chat, Whiteboard, Aufzeichnungen, …
  - Telefoneinwahl statt PC-Audio / von unterwegs
  - Webinar-Funktion
  - Town Halls & Live Events für große Veranstaltungen
- Zusammenarbeit
  - Persistenter Chat, Zusammen arbeiten in Dateien, OneNote, Apps
  - Aufgabenmanagement im Planner
- Automatisierung
  - Power Platform Integrationen

Microsoft Teams – Gast, Extern und Anonym

- Gast
  - Eingeladen in ein Teams-Team
  - Zugriff über Tenant-Wechsel
  - Voraussetzung: Entra ID Konfiguration, M365 Group Konfiguration, SharePoint Konfiguration, Teams Konfiguration passen zusammen
- Shared Channel
  - Eingeladen in einen dedizierten Teams-Kanal
  - Freigabe bettet sich bei „Gast“ in die normale Teams Liste ein
  - Voraussetzung: „Gast“ nutzt ebenfalls Teams mit AAD-Konto, Entra ID erlaubt B2B direct connect, Teams Konfiguration erlaubt Shared Channel
- Externer
  - Ad-Hoc Kommunikation in Teams für Chat, Anrufe, Video, Screensharing
  - Voraussetzung: Teams Konfiguration
- Anonym
  - Meeting Beitritt ohne Microsoft Konto
  - Voraussetzung: Teams Konfiguration

Kanäle in Teams Teams

Allgemein Kanal

- In jedem Team vorhanden
- Kann ausgeblendet werden
- Bis zu 1000 Kanäle pro Team
- Voller Funktionsumfang in „normalen“ Kanälen: Planner etc.

Privater Kanal

- Außerhalb der Microsoft 365 Gruppe, kein Planner
- Zugriff nur für einzelne Nutzer, die auch Mitglied im übergeordneten Team sind
- Bis zu 30 pro Team (inkl. gelöschte)

Geteilter Kanal („shared channel“)

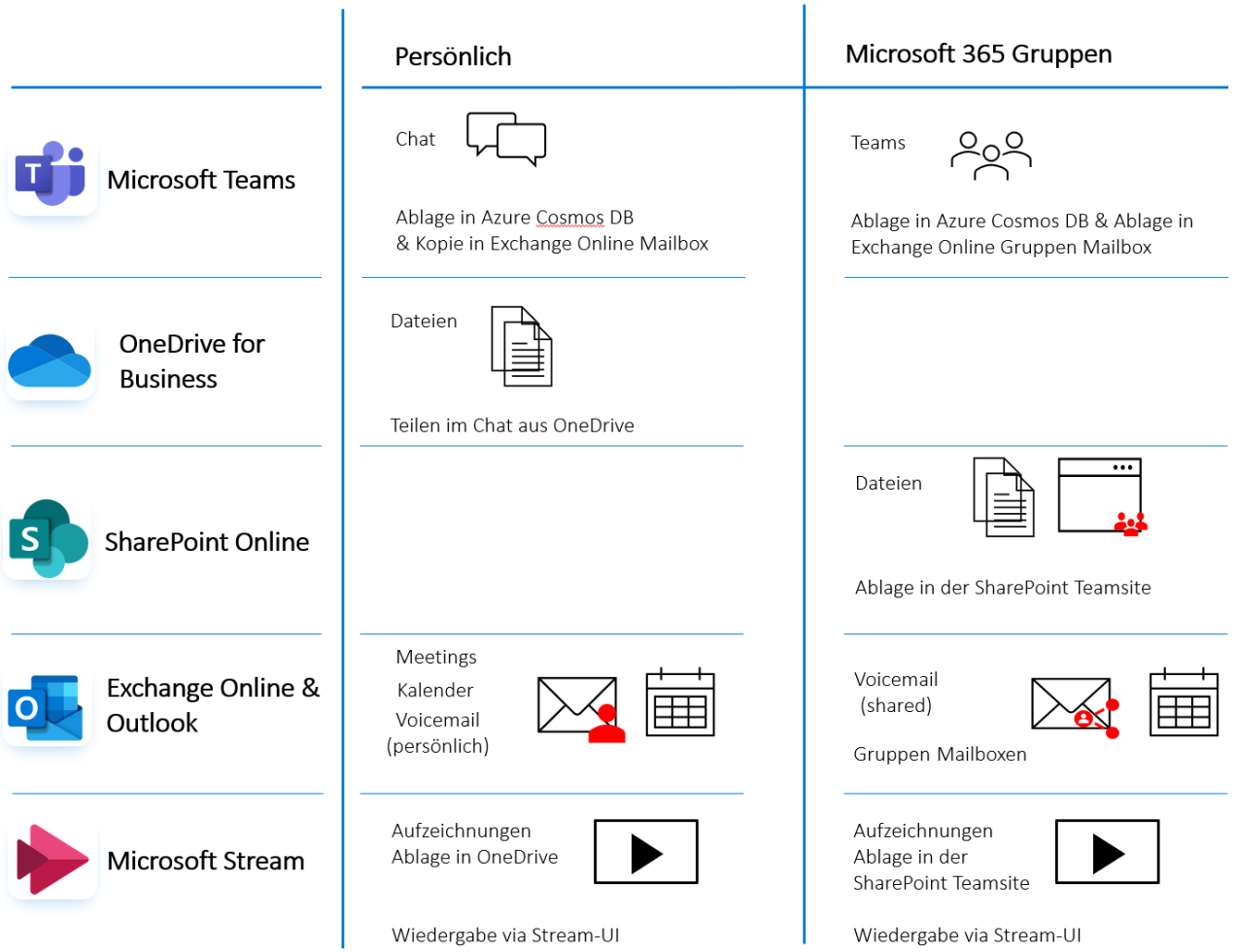
- Außerhalb der Microsoft 365 Gruppe, kein Planner
- Kann intern oder extern mit einzelnen Nutzern oder anderen Gruppen geteilt werden
- Basiert für Externe auf Entra B2B direct connect
  ➞ keine Gastkonten
- Nur mit Entra ID Identitäten
- Kann ein- und ausgehend separat konfiguriert werden
- Bis zu 200 pro Team (inkl. gelöschte)

Microsoft Teams

- Client aktualisiert sich eigenständig
  - Keine Admin-Rechte erforderlich auf Windows Clients
  - Spezielle Installation für VDI / RDSH
- Netzwerkinfrastruktur muss für Echtzeitkommunikation vorbereitet sein
- Administration: Teams Admin Center & PowerShell & Graph
- Teams Grenzwerte und Spezifikationen

Microsoft Teams Architektur

- Microsoft Teams nutzt andere Dienste der M365 Plattform
- Weitere Microsoft- und 3rd-party-Anwendungen nutzen ihre eigenen Datenspeicher



Teams Lizenzen

- Bestandskunden bis 2023: In jeder Suite-Lizenz ab Business Basic / O365 E1 enthalten.
- Seit „EEA“ Lizenzen muss Teams separat dazu gebucht werden.

- Teams Premium erweitert Teams um weitere Funktionen u.a. für Besprechungen und Sicherheit

- Teams Phone System
  - In O365 E5 / M365 E5 enthalten
  - Für alle anderen Pläne als Add On erhältlich
  - Team Shared Device für allgemeine Nebenstellen

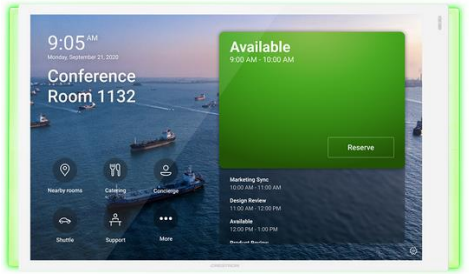
- Teams Essentials
  - Reduzierter Microsoft 365 Tenant
  - Mit oder ohne Entra ID
  - Nur für kleine Organisationen, die Teams nur als Besprechungs-Plattform verwenden möchten

- Teams Room Basic / Pro
  - Für Teams Raum Ausstattungen

Microsoft Teams Hardware

Professionelle Hardware für ideale Nutzererfahrung

- Teams certified devices
  - Konferenzspinne / Tischmikro
  - Persönliche Geräte
    - Headset
    - Kamera
  - Microsoft Teams Rooms (MTR)
    - on Windows
    - on Android
    - Whiteboard Kameras
    - Panel
  - Telefone



Teams | Zusammenfassung

Wichtige Punkte für unser „Big-Picture“

- Teams Nutzung
  - Chat
  - Meeting
  - Teams
- Teams Governance Anforderungen
- Ablösung der TK-Anlage geplant?
- Raum Systeme geplant?

Weitere Microsoft 365 Apps

Nützliche Helfer in Microsoft 365

Forms

- Abfragen
- Umfragen
- Formulare
- Quiz

Lists

- Moderne & intelligente Listen auf SharePoint Basis

Whiteboard

- Zusammenarbeit auf einem virtuellen Whiteboard
- wird in OneDrive bzw. SharePoint gespeichert

Loop

- Flexible Arbeitsbereiche in Teams & Office zur gleichzeitigen Bearbeitung
- wird in OneDrive bzw. SharePoint gespeichert
- Basis in jeder Lizenz enthalten
- Loop Arbeitsbereiche nur in Microsoft 365 Plänen

Nützliche Helfer in Microsoft 365

Bookings

- Self Service Termin Portal für Kunden
- „Booking with me“ = persönliche Buchungsseite
- Basis Exchange Online

Planner

- Aufgabenmanagement für Teams

Stream

- „Youtube“ für das eigene Unternehmen auf SharePoint Basis

To Do

- Persönliches Aufgabenmanagement
- Nur mit Exchange Online Postfächern

Microsoft 365 Apps | Zusammenfassung

Wichtige Punkte für unser „Big-Picture“

- Gibt es Tools, die heute bereits ein- oder ausgeschlossen werden können?

Microsoft Viva

Microsoft Viva – Employee Experience Platform

Mitarbeiterkommunikation & Communities

Viva Connections

Viva Engage

Viva Amplify

Insights & Feedback

Viva Insights

Viva Glint

Viva Pulse

Wissensmanagement

Viva Learning

Ziele managen

Viva Goals

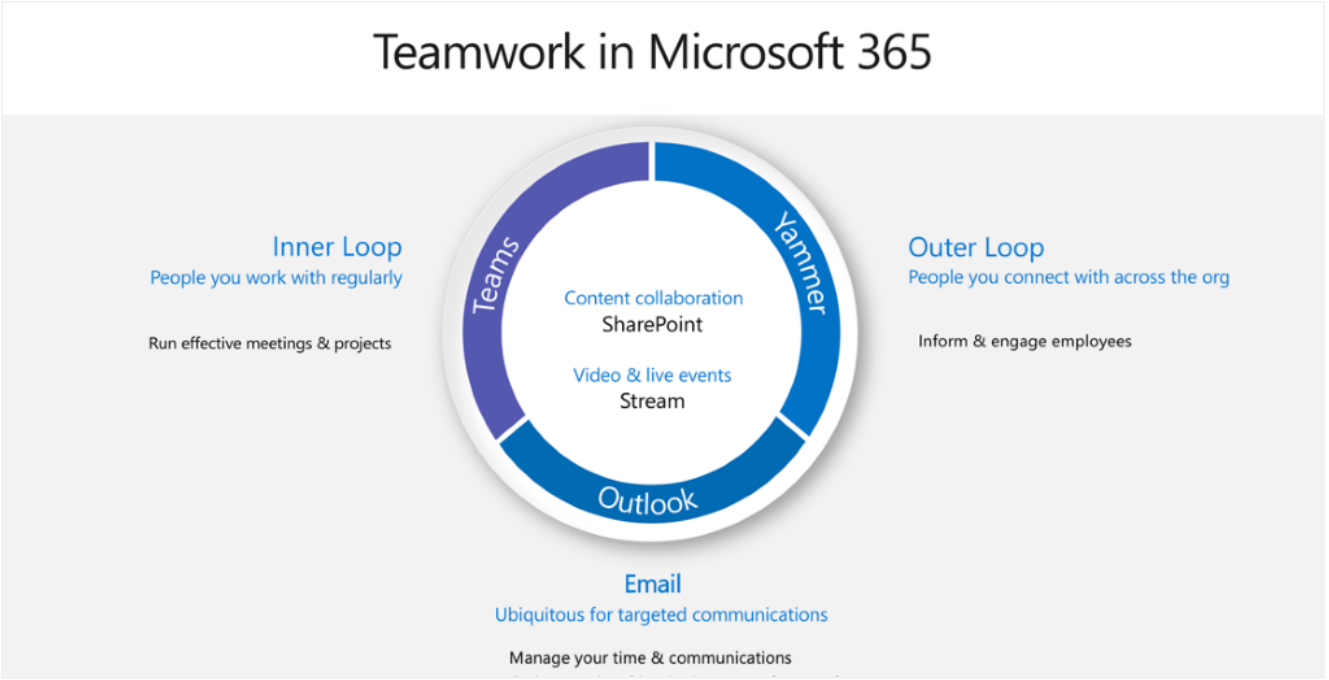
- Die Module Connections, Engage, Learning sind in den Office / Microsoft 365 Basislizenzen enthalten.
- Aplify, Glint, Pulse, Goals können separat oder als Suite gebucht werden.
- Connections, Engage, Insights, Learning können durch Add Ons in der Funktionalität erweitert werden

Viva Engage

- Enterprise Social Network

- Abbildung von „Community of Practice“
- Interessensgruppen zusammen bringen
  - Menschen vernetzen, die sich nicht kennen
  - Expertise austauschen
- Unternehmenskommunikation verbreiten
- Ideen-Management

- Teil einer Microsoft 365 Gruppe
  - Teams oder Engage
- In Teams integriert



Microsoft Viva| Zusammenfassung

Wichtige Punkte für unser „Big-Picture“

- Ist der Einsatz von Viva Tools geplant?

Microsoft Purview

Information protection & governance

Schützen und verwalten Sie Daten, wo immer sie sich befinden

Daten wachsen exponentiell

Einheitlicher Ansatz

Entdecken

Klassifizieren

Richtlinien anwenden

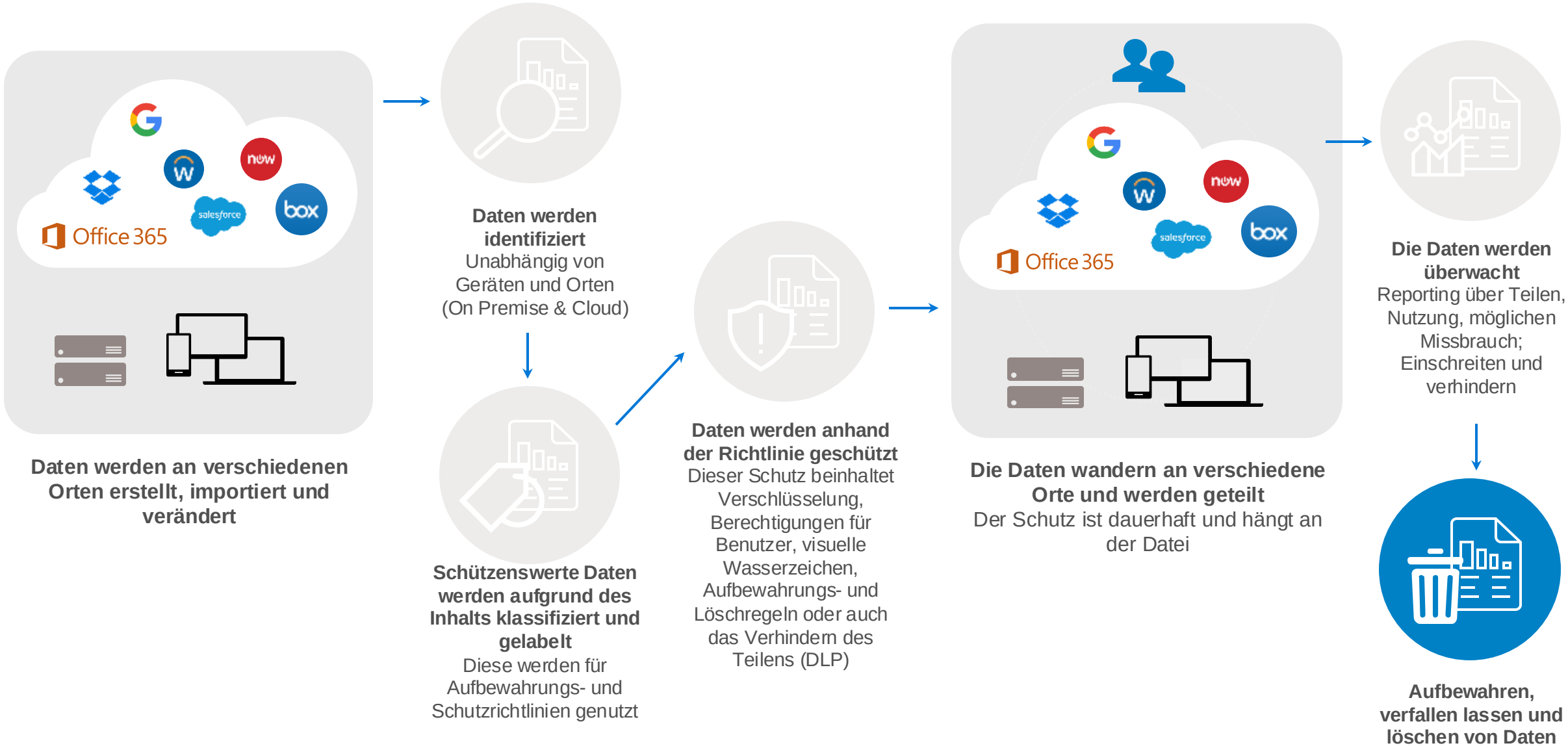
Schutz
- Datenverlust verhindern
- Verschlüsselung
- Zugriff einschränken
- Wasserzeichen

Governance
- Archivierung
- Aufbewahrung & Löschung
- Aktenverwaltung
- Entsorgungsüberprüfungen

Monitoring

- Entdeckung sensibler Informationen
- Inhaltsexplorer
- Aktivitätsexplorer
- Prüfpfad
- Entsorgungsnachweise

Geräte | Apps | Cloud Services | On-premises | ISVs, 3rd-party


Office 365
salesforce
box
Daten werden an verschiedenen Orten erstellt, importiert und verändert
Daten werden identifiziert
Unabhängig von Geräten und Orten (On Premise & Cloud)
Schützenswerte Daten werden aufgrund des Inhalts klassifiziert und gelabelt
Diese werden für Aufbewahrungs- und Schutzrichtlinien genutzt
Daten werden anhand der Richtlinie geschützt
Dieser Schutz beinhaltet Verschlüsselung, Berechtigungen für Benutzer, visuelle Wasserzeichen, Aufbewahrungs- und Löschregeln oder auch das Verhindern des Teilens (DLP)
Office 365
salesforce
box
Die Daten wandern an verschiedene Orte und werden geteilt
Der Schutz ist dauerhaft und hängt an der Datei
Die Daten werden überwacht
Reporting über Teilen, Nutzung, möglichen Missbrauch; Einschreiten und verhindern
Aufbewahren, verfallen lassen und löschen von Daten

Insider Risk Management

Context-aware detection

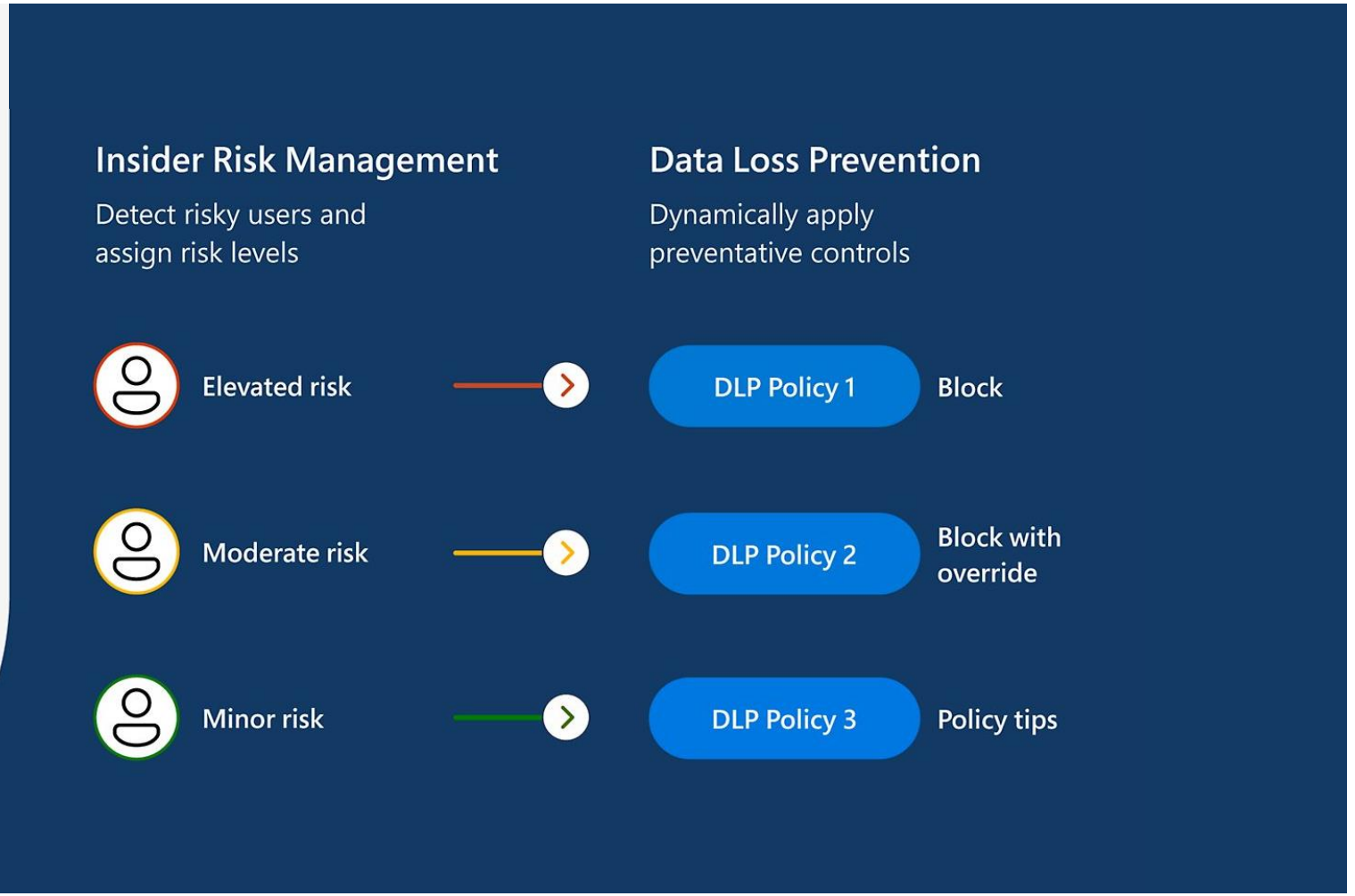
Identify the most critical risks with ML-driven analysis in Insider Risk Management

Dynamic controls

Enforce effective DLP controls on high-risk users while others maintain productivity

Automated mitigation

Minimize the impact of potential data security incidents and reduce admin overhead



Sensitivity Label

Header / Footer | Watermark | Encryption | Permissions

Public/Private| Guests allowed | SPO Sharing

Default Label

Forward | Encryption | Permissions

Azure Information Protection ändert die Art und Weise Berechtigungen zu vergeben

Herkömmlich

- Windows File Shares mit NTFS-Berechtigungen
- Dateien sind innerhalb des Ordners geschützt
- Schutz erfolgt durch den Ablageort
- Kopien an anderen Speicherorten verlieren den Schutz, z.B. Mail Anhang

Purview Information Protection

- Berechtigungen sind in der Datei gespeichert
- Daten werden klassifiziert und verschlüsselt
- Auch außerhalb des geschützten Netzwerks bleibt der Schutz bestehen
- Berechtigungen können granular vergeben werden (z.B. Speichern unter, Drucken)

Retention Policies/Label

Automatisierte Speicherung und/oder Löschung von Daten

Schutz der Daten z.B. vor Manipulation und Verlust

Definition der Retention Policies für folgende Services:

- Exchange, SharePoint, OneDrive, Groups, Teams

Arten

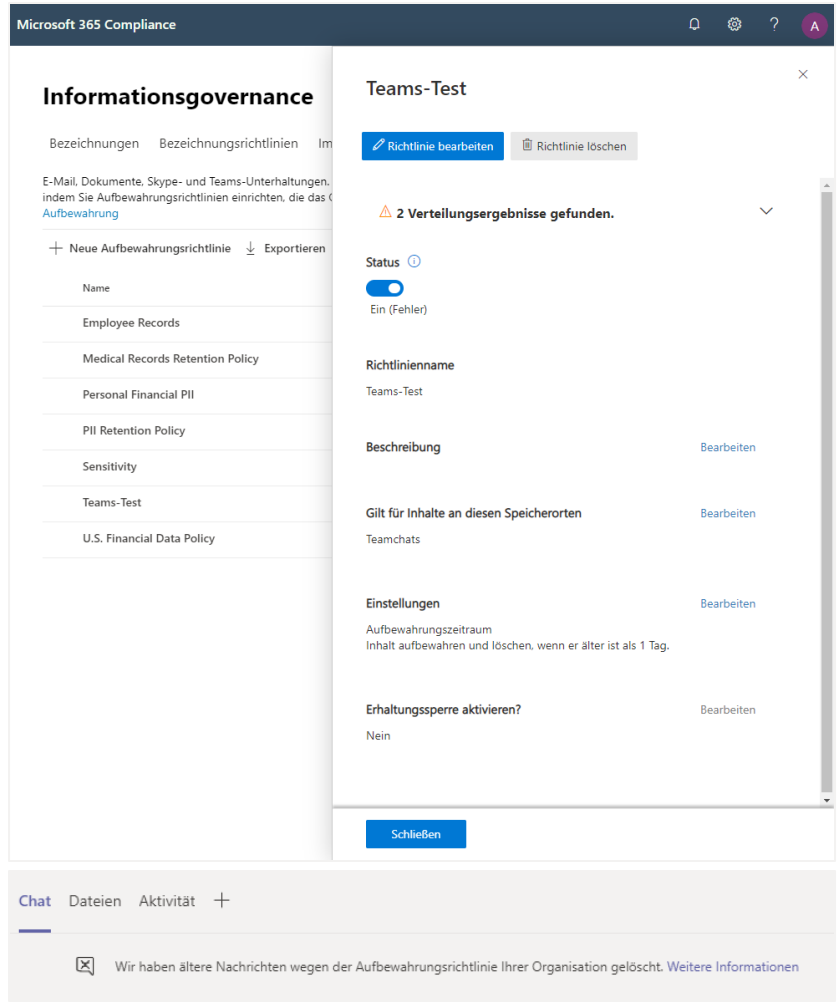
- Aufbewahren | Aufbewahren und Löschen | Löschen

Schutz

- Gesamter Objekte (z.B. SharePoint oder Exchange Mailbox)
- Spezifischer Informationen

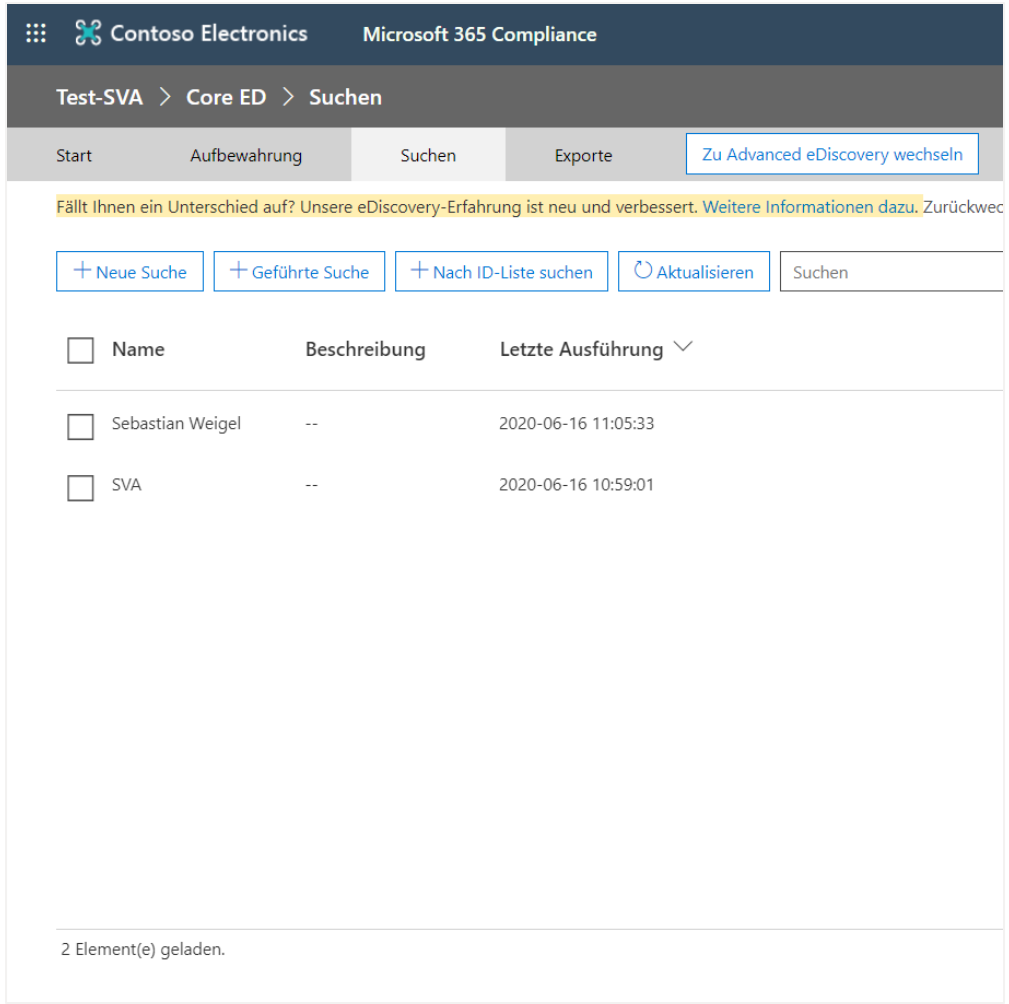
Retention Label

- Retention Label können auf einzelne Elemente angewendet werden
- Können durch Autolabeling auf Grundlage von Sensitive Info Types angewendet werden



eDiscovery (Premium)

- eDiscovery: Finden, Exportieren und Aufbewahren von „elektronisch gespeicherten Informationen“ (ESI)
- Zusätzlich: „Search and Purge“
- Nutzung z.B. für Beweissicherungsverfahren
- Suche basierend auf Stichworten
- Nutzung der gespeicherten Information in M365 (u.a. Exchange, SharePoint, OneDrive, Teams …)
- Durchsuchen mehrerer Quellen gleichzeitig
- Nicht alle Informationstypen werden unterstützt
  (Beispiel: Teams Audioaufzeichnungen)
- Advanced eDiscovery: „Automatisierung der eDiscovery“



Vertrauliche Informationstypen

Erkennung von Inhalten anhand von
- Textmustern

Erkennung über
- Reguläre Ausdrücke (RegEx)
- Schlüsselwortlisten
- Wörterbücher

Geeignet für (u.a.)
- Kreditkarten- oder Kontonummern
- Artikel- oder Produktnummern
- (Interne) Dokumentenbezeichnungen

Weitere Vertrauliche Informationstypen
- Trainierbare Klassifikatoren
- Fingerabdrücke
- Exact Data Match

Name

Beschreibung

Muster

Primäres Element
Hauptelement nach dem gesucht wird
(z.B. RegEx Ausdruck für eine IBAN)

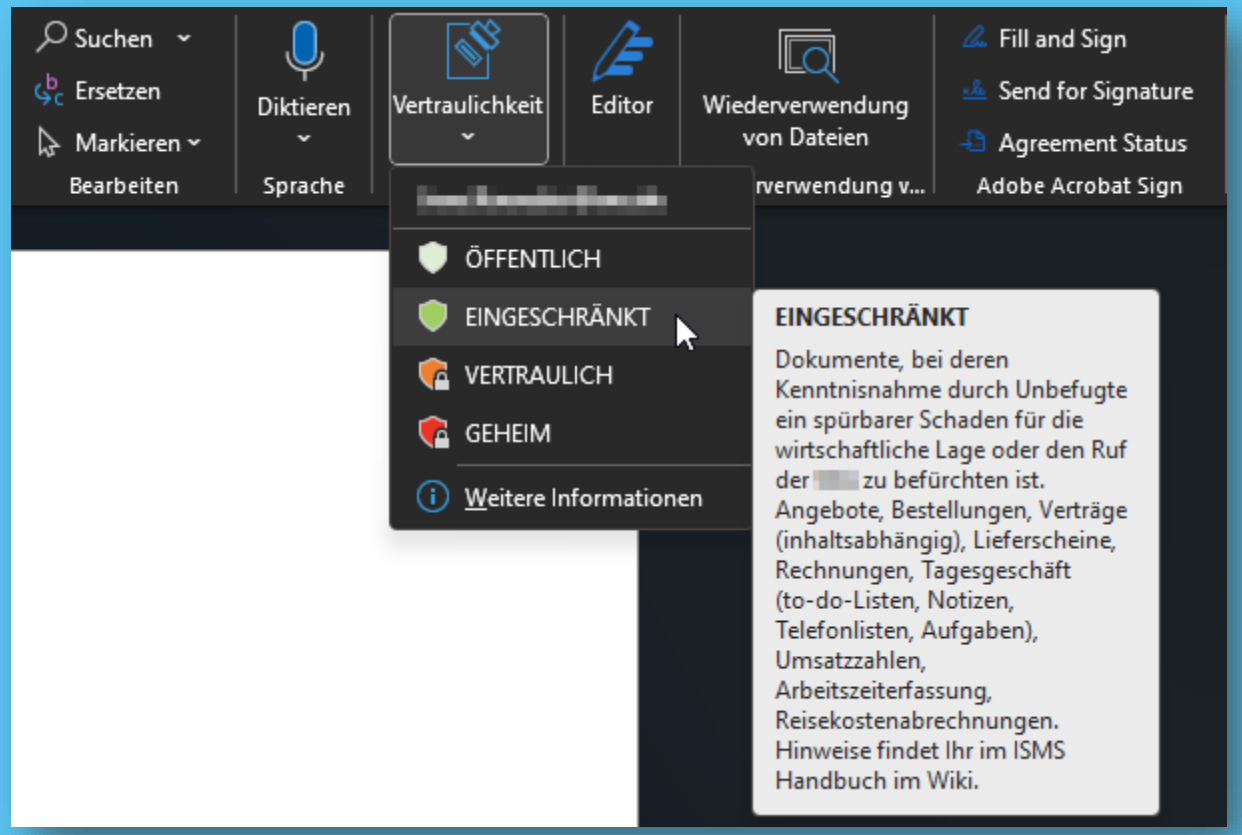
Unterstützendes Element
Elemente die als zusätzlicher Nachweis fungieren
(z.B. Stichwort „IBAN“ in der nähe eine entspr. Nummer)

Konfidenzstufe (hoch, mittel, niedrig)
Gibt an, wie viele unterstützende Elemente gefunden werden müssen (hoch = mehr false negativ; niedrig = mehr false positiv)

Näherung
Abstand (Zeichenanzahl) zwischen prim. und unterst. Elementen

/ Microsoft Purview

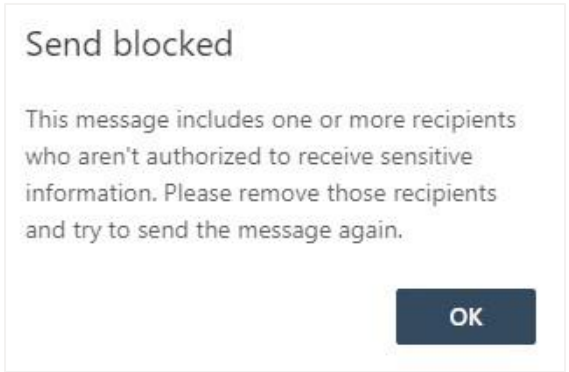
Ansicht in Microsoft Word

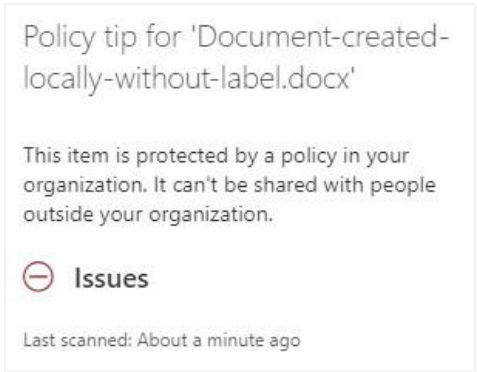


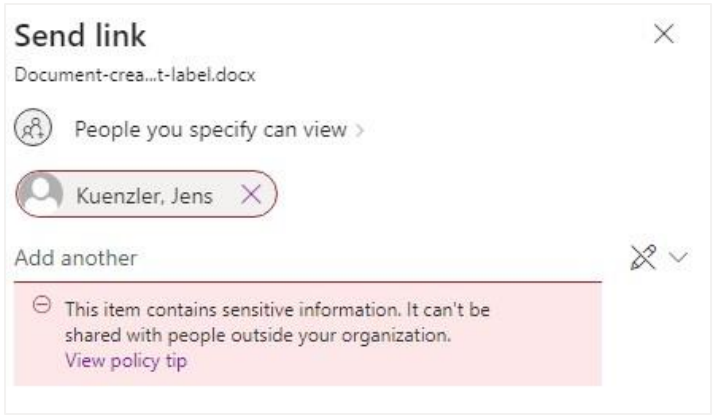
Data Loss Prevention

Verhindern des Teilens von sensiblen Daten

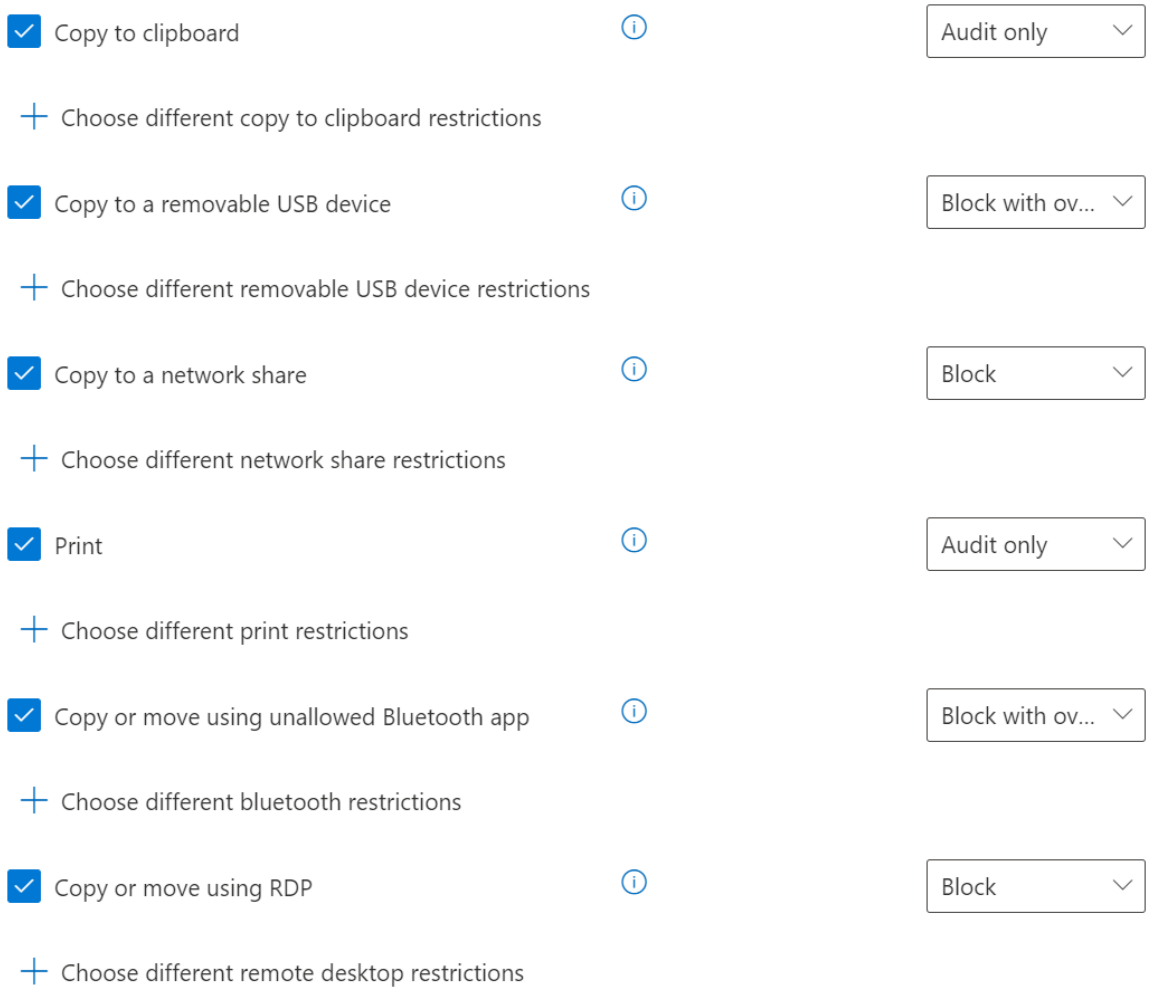
- Beispiel: Finanz- oder Personen-bezogene Daten
- Erkennung von Text-Pattern (Information Types)
- Verschiedene vordefinierte Pattern vorhanden
- Erkennung von Datenklassifizierung (Labeling)
- Externes Teilen unterbinden
- Integriert in:
- Exchange, SharePoint, OneDrive und Teams
- Definition: Analyse welcher Pattern in welcher App
- Möglichkeit der Einblendung von Richtlinien-Tipps

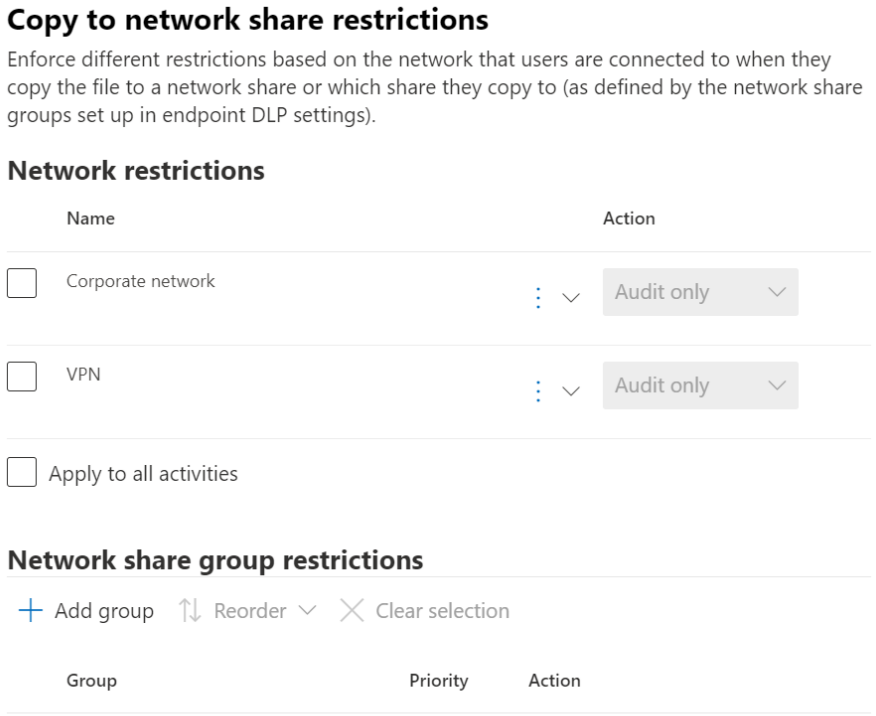






Endpoint Data Loss Prevention





Information Barriers

Teams-Kommunikation zwischen Personen und Gruppen im Unternehmen einschränken

Basis: Exchange Adressbuchrichtlinien

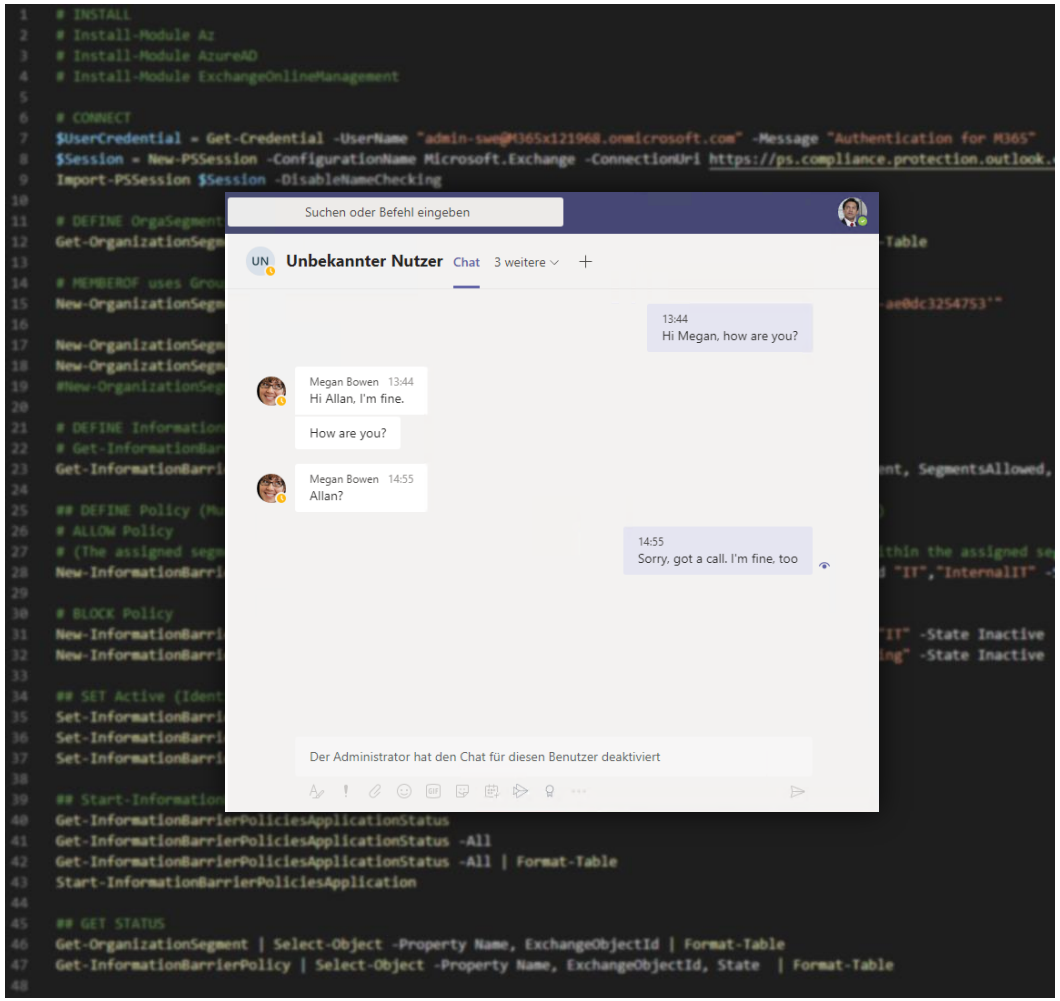
Einschränkungen:

- Chats
- Team-Mitgliedschaft
- Meetings
- Calls

Aktuell: Konfiguration ausschließlich per PowerShell

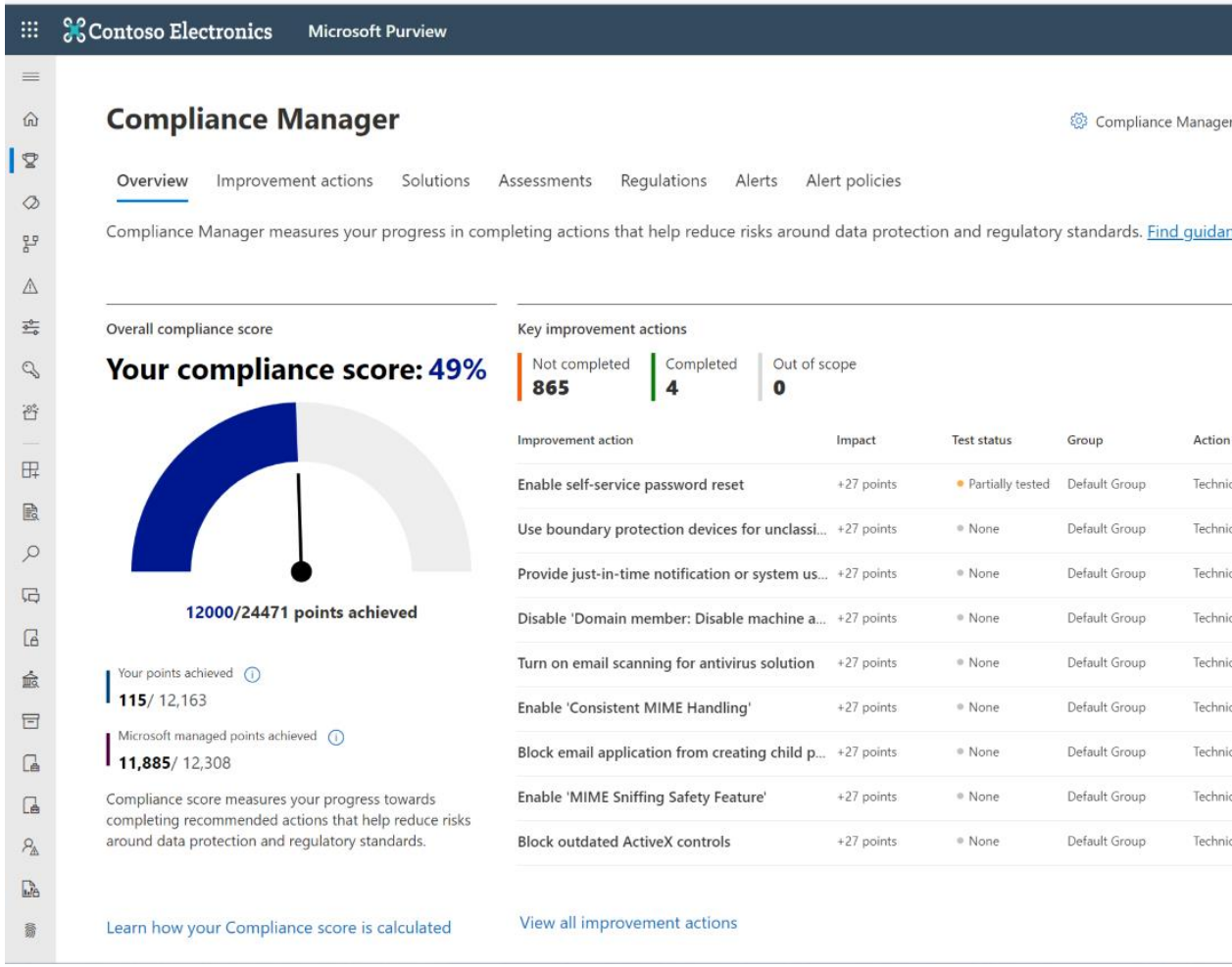
Aktuell: Starke Limitationen

- Benutzer <-> Segment: 1-to-1 Beziehung
- Segment <-> IB Policy : 1-to-1 Beziehung

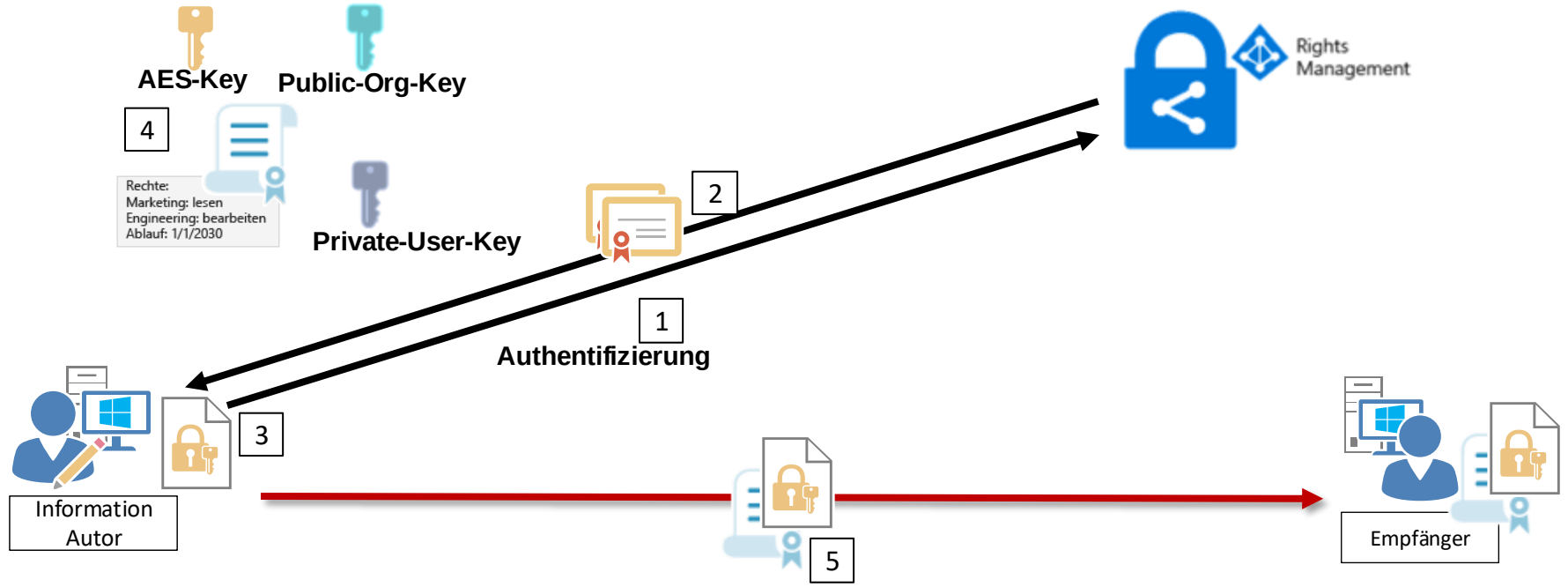


Compliance Manager

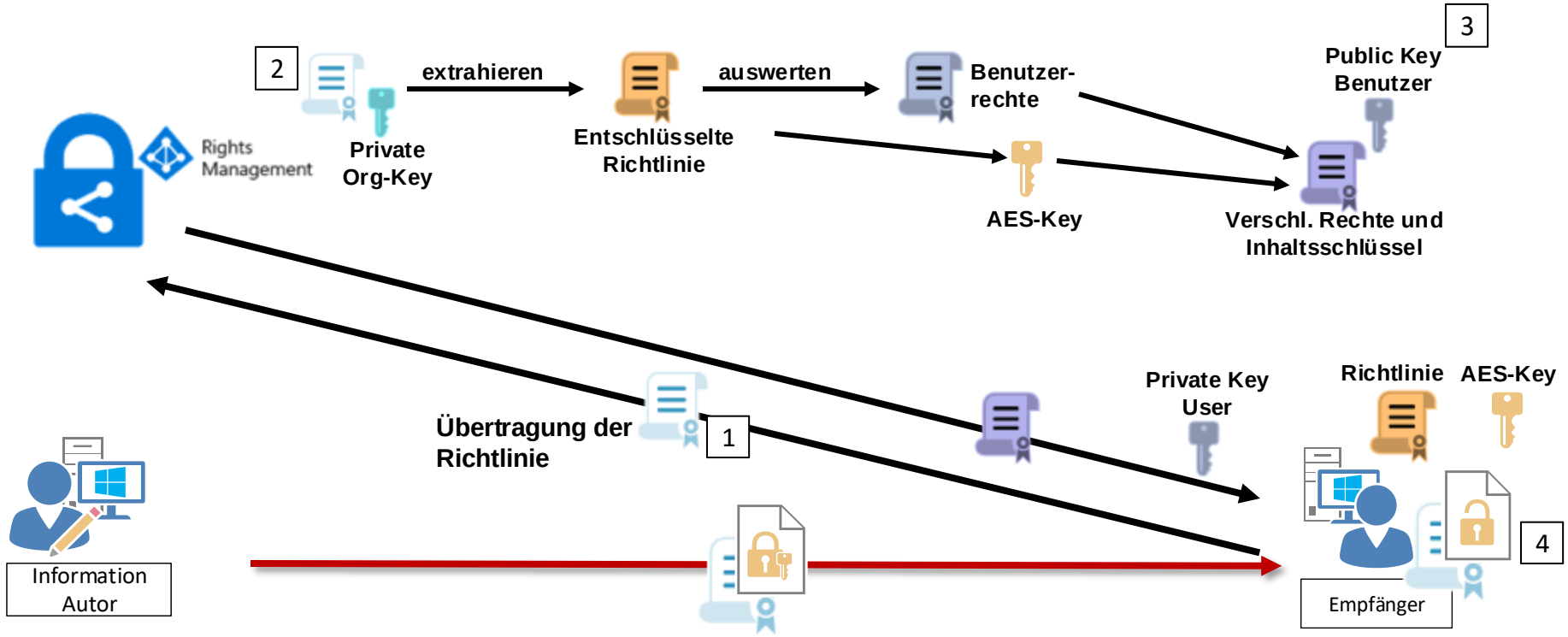
- **Automatische Bewertung und Verwaltung**: Hilft bei der Bewertung und Verwaltung der Compliance in Multi-Cloud-Umgebungen
- **Vorgefertigte Bewertungen**: Bietet Bewertungen für gängige branchenspezifische und regionale Standards und Vorschriften(DSGVO, ISO, CIS, NIST,…)
- **Verbesserungsmaßnahmen**: Detaillierte Anleitungen zu Maßnahmen, um Standards und Vorschriften einzuhalten
- **Compliancebewertung**: Vergibt Punkte für durchgeführte Verbesserungsaktionen und zeigt den aktuellen Compliancestatus an
- **Einbeziehung weiterer Abteilungen:** Durch die Möglichkeit Berechtigung auch für weitere Abteilung wie Compliance, Datenschutz oder ISB auf den Manager zu berechtigen, werden diese stets über den aktuellen Stand der Maßnahmen informiert



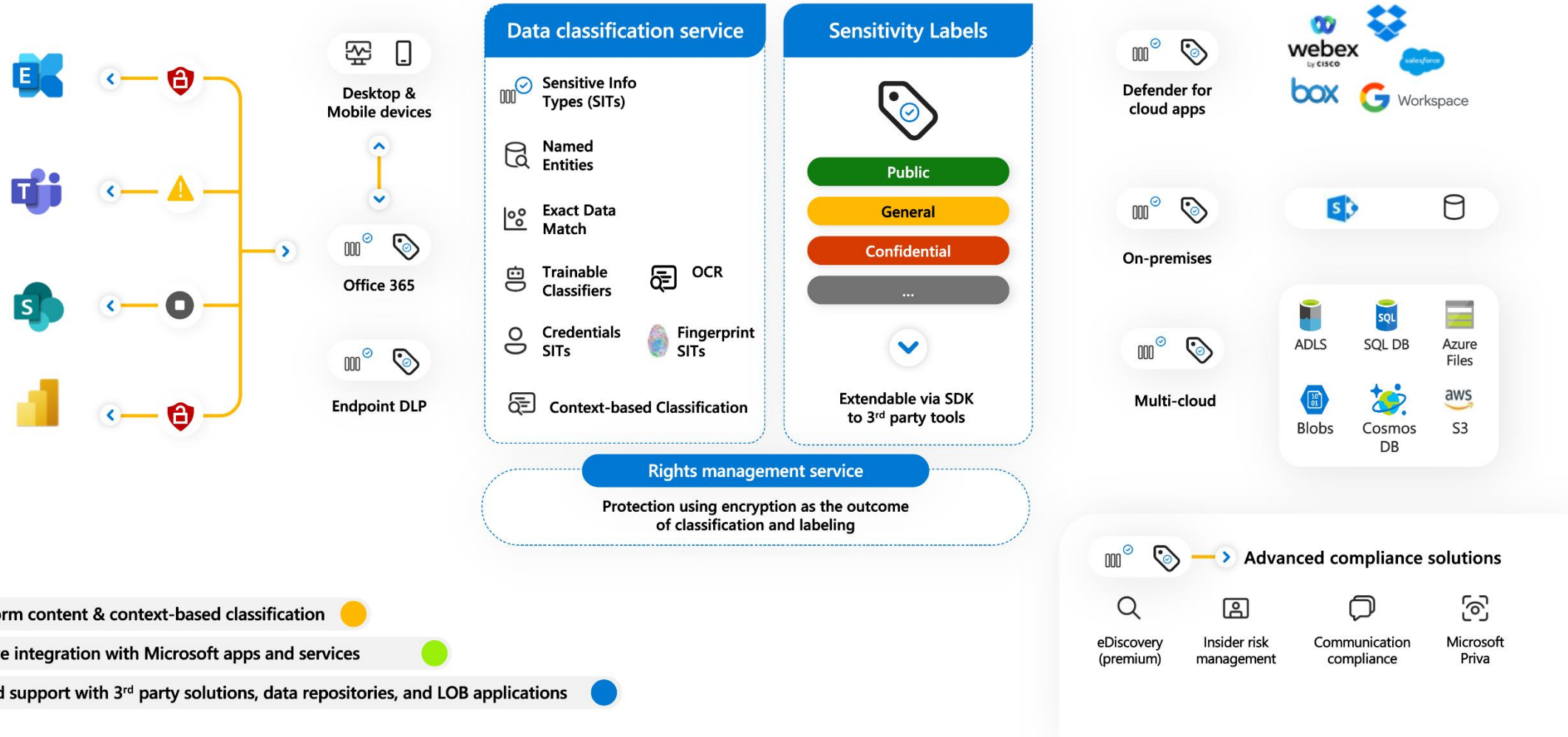
Funktionsweise von Purview – Inhalt schützen



Funktionsweise von Purview – Inhalt nutzen



Microsoft Purview Information Protection



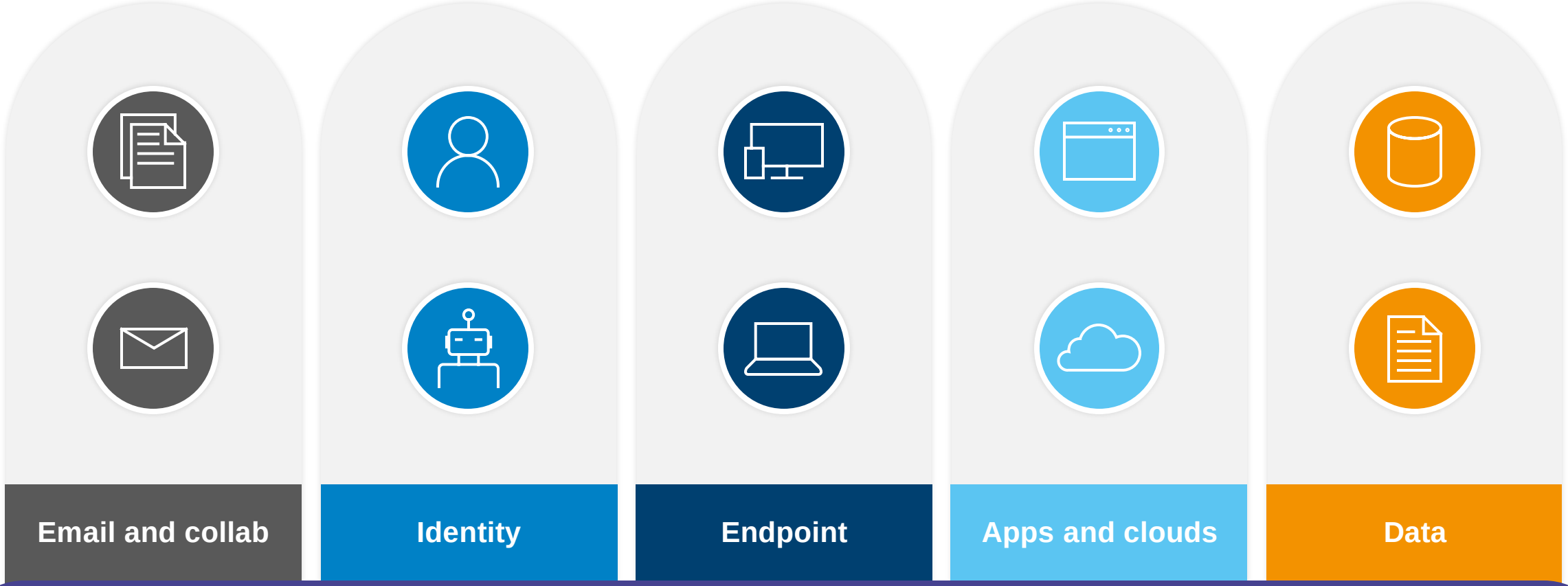
Microsoft Purview| Zusammenfassung

Wichtige Punkte für unser „Big-Picture“

- Welche Produkte sollen in welcher Welle eingeführt / näher betrachtet werden?
- Sensitivity Labels
- Data Loss Prevention
- Retention Policies
- eDiscovery
- Inforation Barriers

Microsoft Defender

Warum Microsoft Security? Weil viele Security in Silos denken…

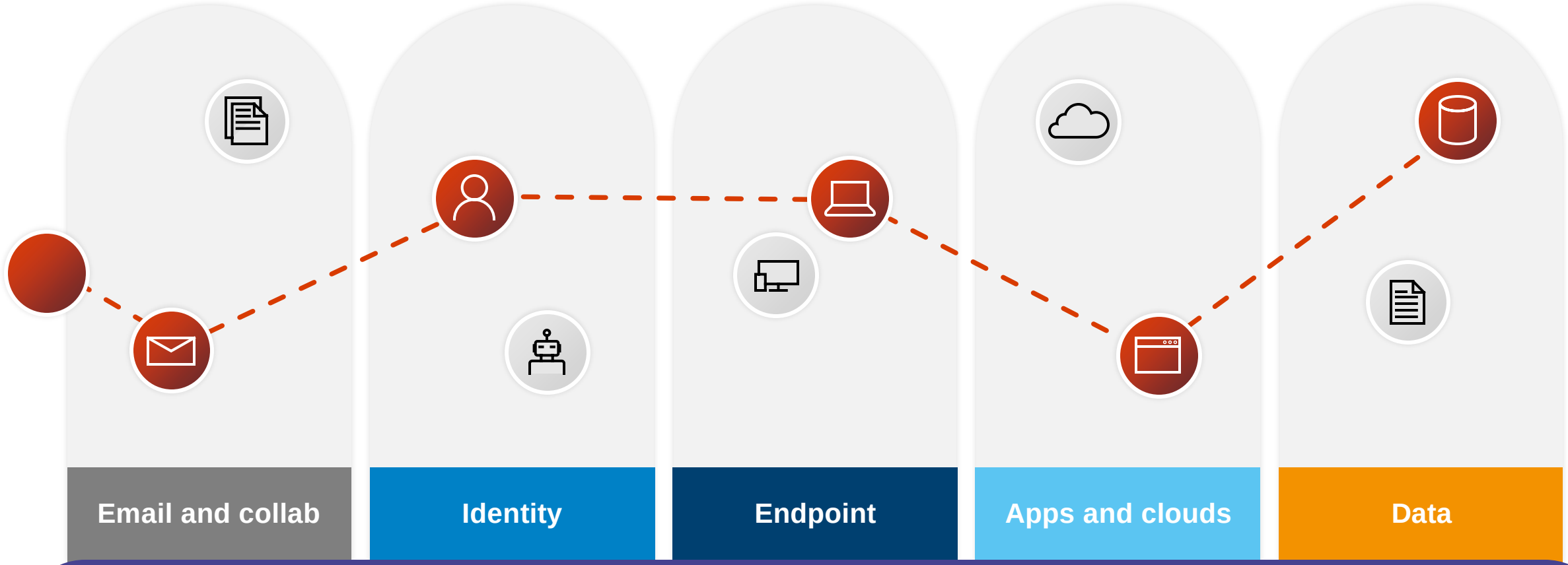


Organizations use an average of

80 security tools[1]

1. Microsoft Internal Research

…und Angreifer aber in Pfaden denken!



The median time for an attacker to access private data from phishing is just

72 minutes[2]

2. 2022 Microsoft Digital Defense Report, p. 21

Microsoft Defender XDR

Microsoft Defender for Office 365

Microsoft Defender for Identity

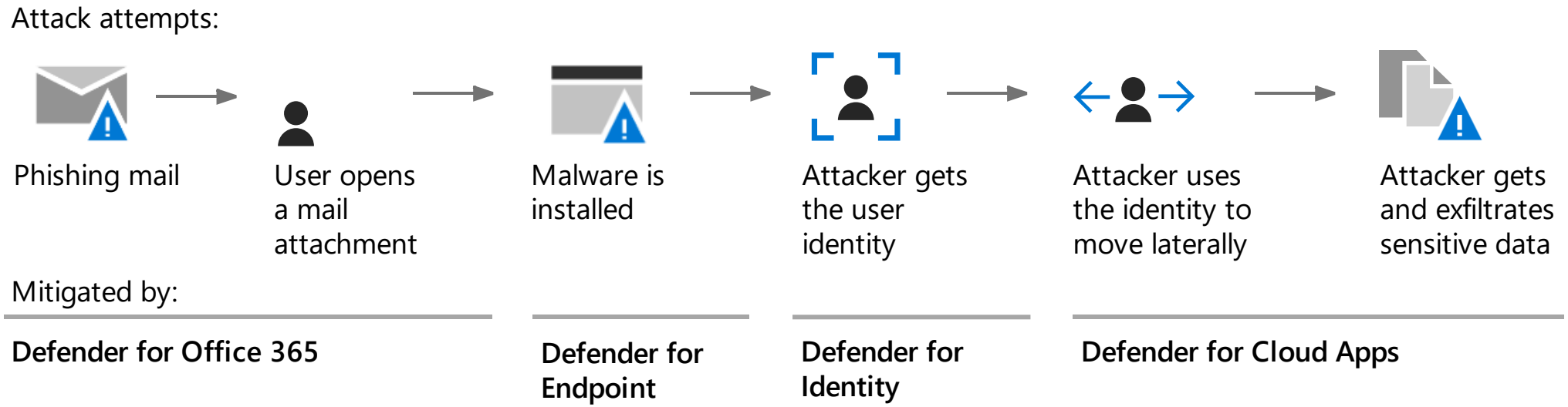
Entra Identity Protection

Microsoft Defender for Endpoint

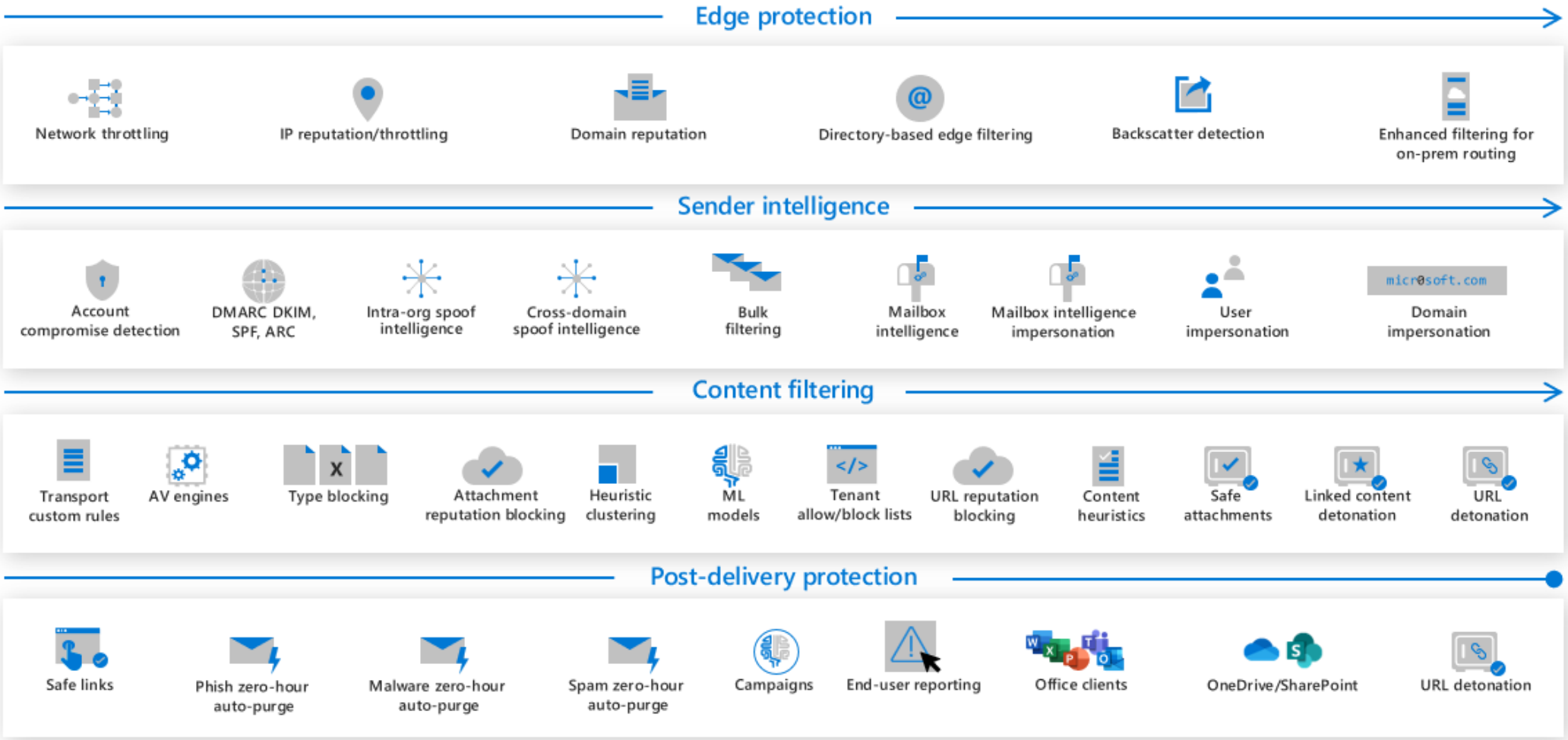
Microsoft Cloud App Security

Microsoft Defender XDR

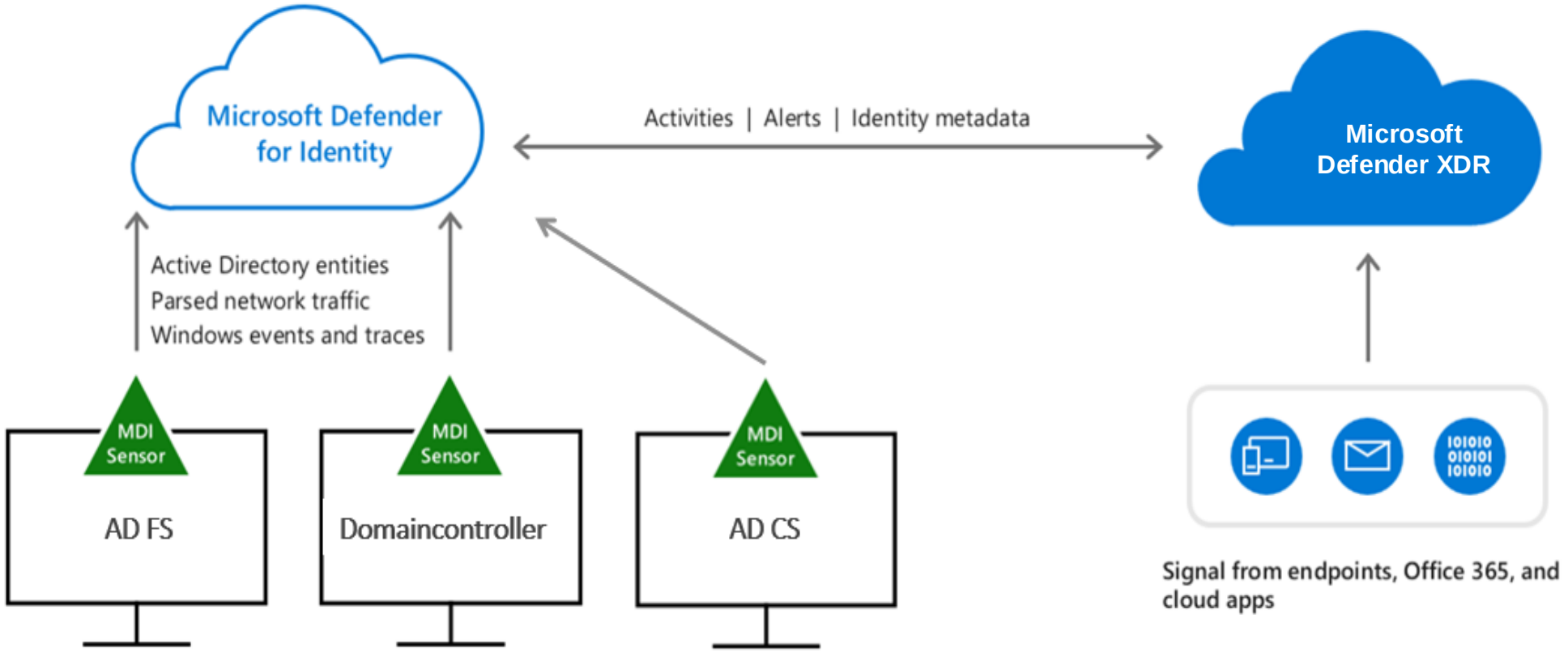
Microsoft Defender XDR bei einem Angriff



Defender for Office 365



Defender for Identity

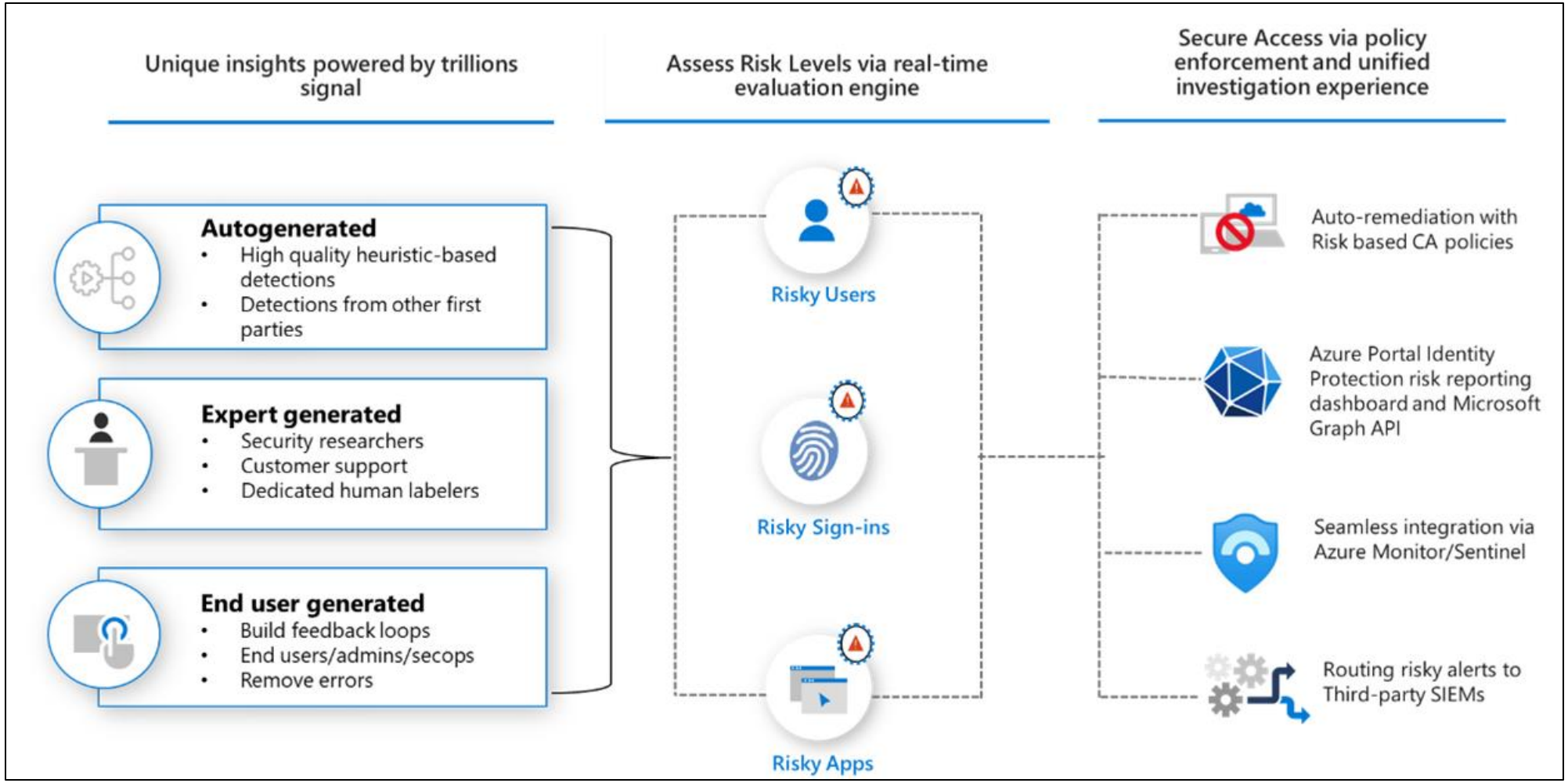


Entra Identity Protection

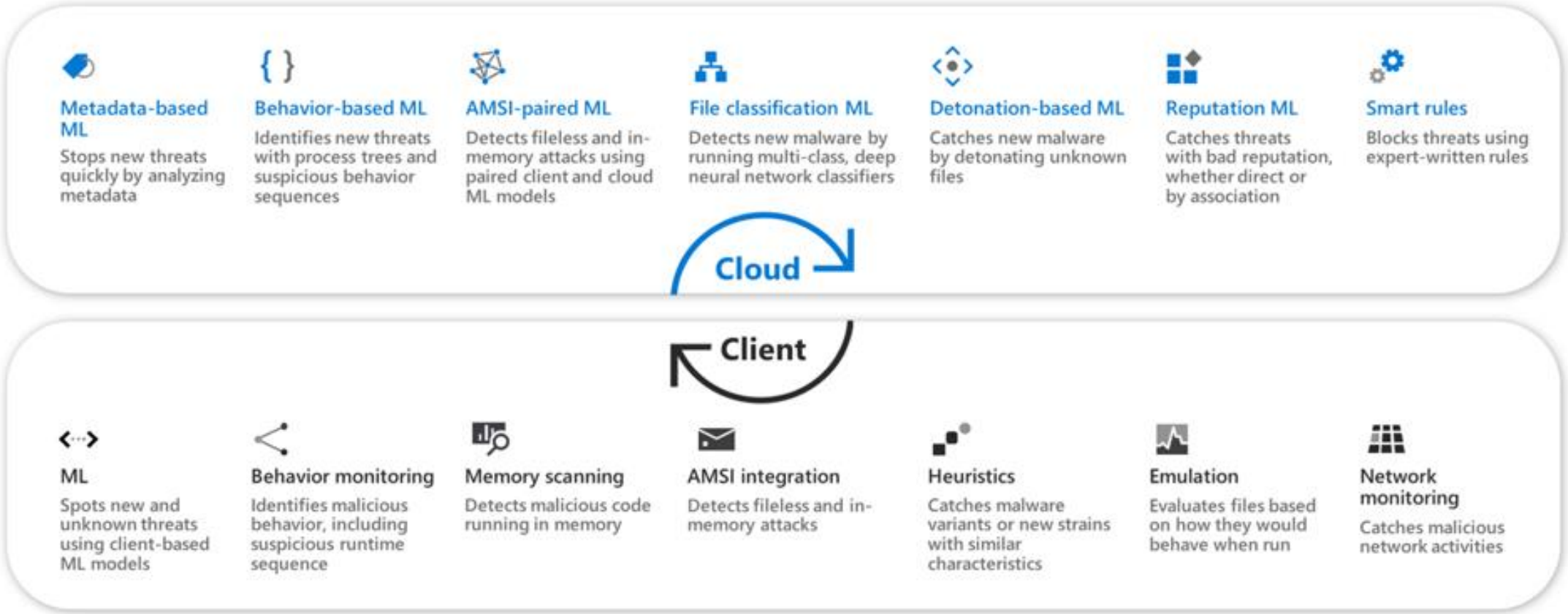
Echtzeit-Bedrohungs-erkennung

Automatisierte Reaktion

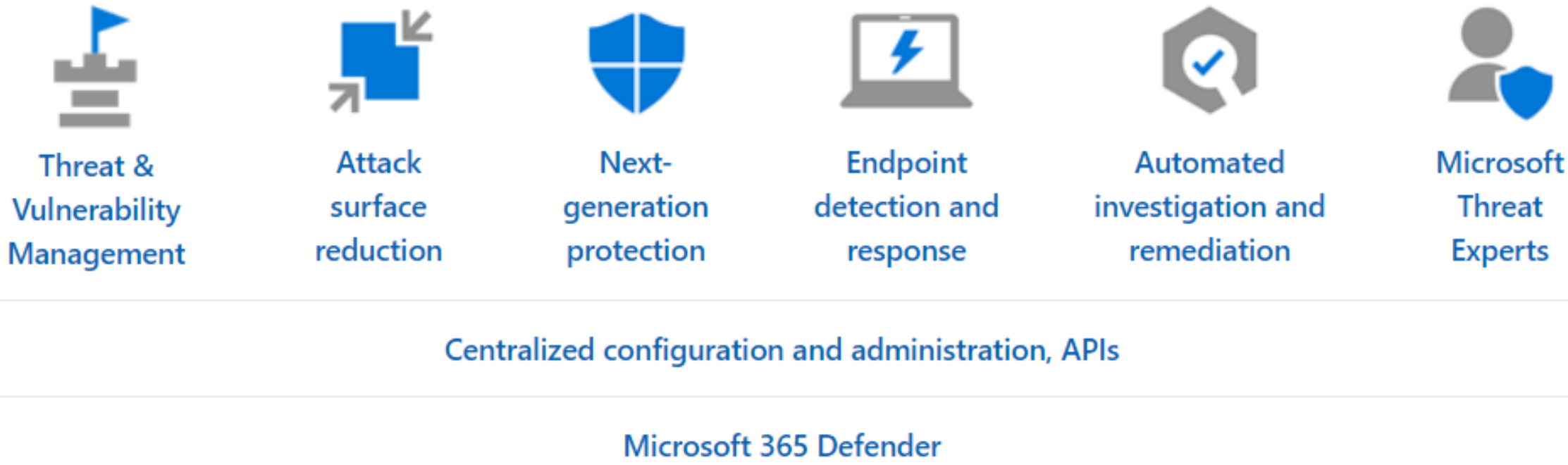
Berichterstattung



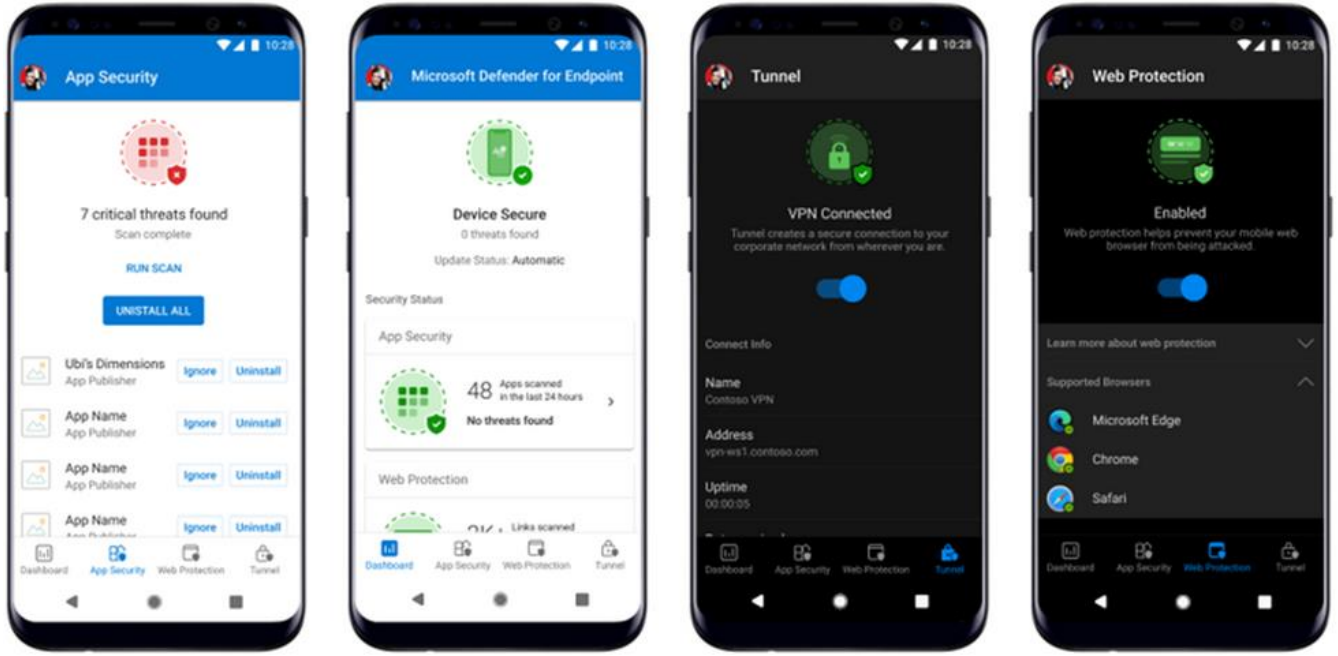
Defender for Endpoint – AV & EDR Funktionen



Defender for Endpoint - Funktionsumfang



Defender for Endpoint – Schutz mobiler Endgeräte



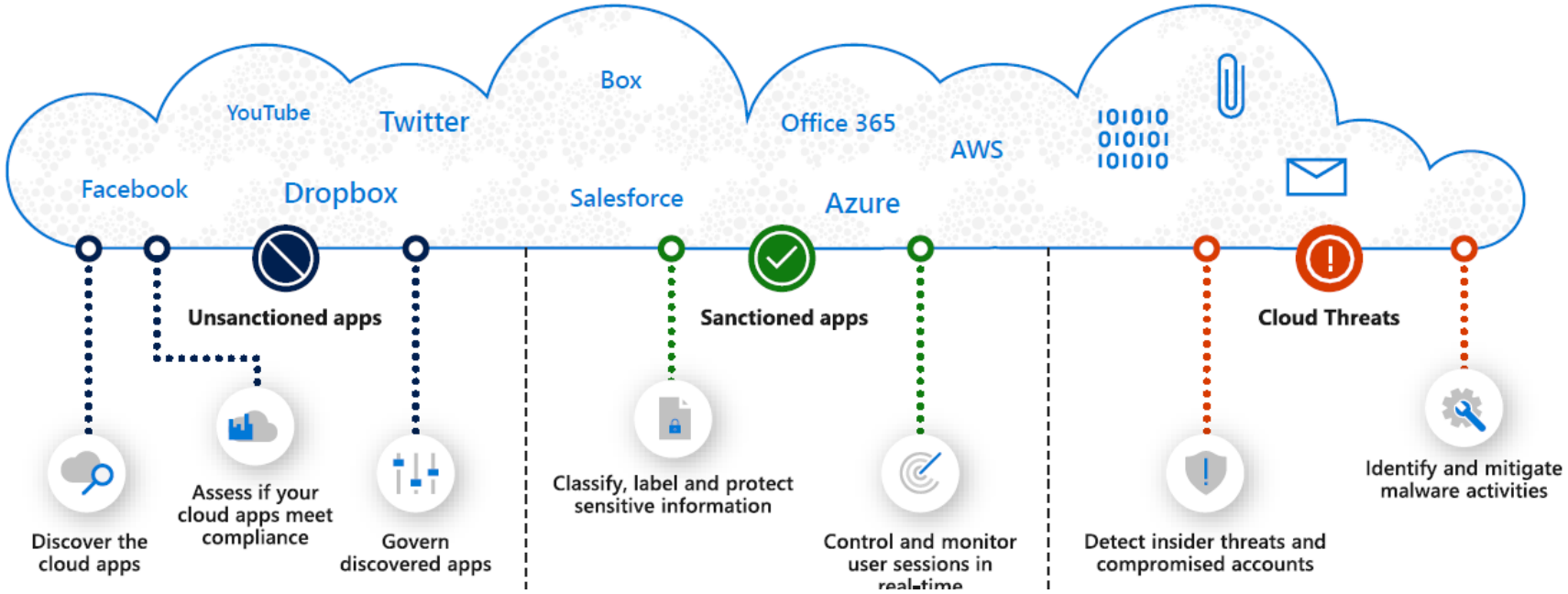
Windows macOS Android Linux

Defender for Cloud Apps

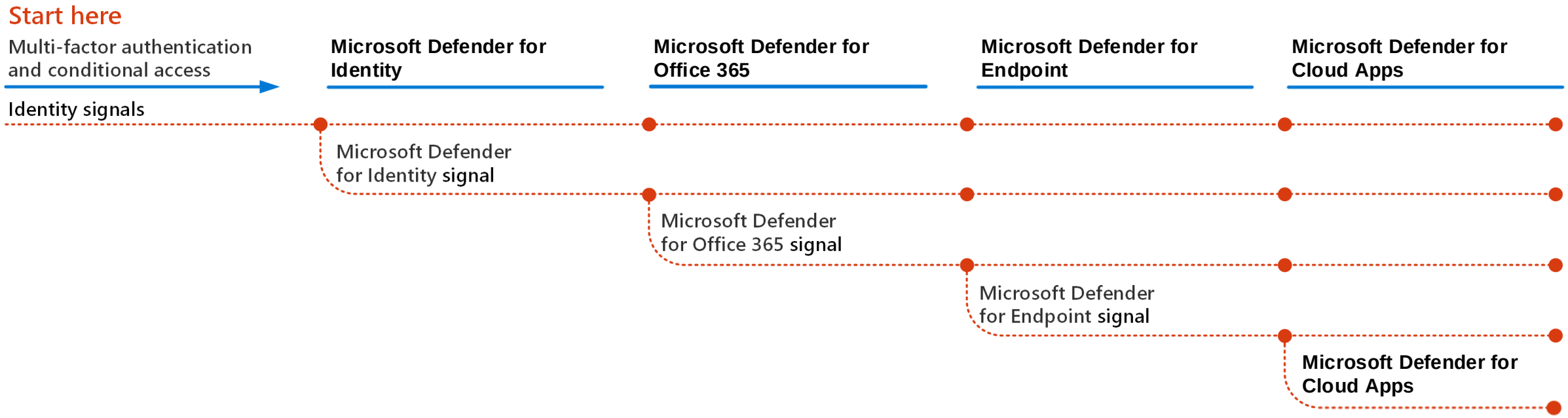
Ermitteln
- Schatten-IT & Web-Anwendungen
- Benutzer

Untersuchen
- Von Benutzer-Aktivitäten
- Von Dateien
- Der Nutzung von neuen Cloud Apps

Steuern
- Erkennung von Benutzerverhalten
- Der Nutzung von Cloud Apps
- Datenexport in Anwendungen



Roadmap Implementierung



Microsoft Security | Zusammenfassung

Wichtige Punkte für unser „Big-Picture“

- Welche Funktionen sollen eingesetzt / lizenziert werden?
  - Microsoft Defender for Identity = OnPrem security feature
  - Microsoft Defender for O365 = E-Mail & Collaboration
  - Microsoft Defender for Endpoint = Devices & more
  - Microsoft Defender for Cloud Apps = SaaS

Microsoft Copilot

Übersicht zu den Microsoft KI Angeboten

Azure & AI

Copilot


Power Platform


D365


M365


Security


Windows


Bing


GitHub

Azure OpenAI


Azure OpenAI Service


Cognitive Services

Copilot Web vs. Copilot for M365

Copilot Web

Was ist es: AI Chatbot

Wer sollte es nutzen: private Personen und Firmen

Wie funktioniert es: Interaktion auf der Website

Auf was greift es zu: Das Internet via bing.

Wo greifen User darauf zu: bing.com/chat

Unterschied

Fakt 1: Datenschutz

Fakt 2: Copilot Web hat immer Zugriff auf das Web, in Copilot for M365 müssen Sie es aktivieren

Copilot for M365

Was ist es: Integriert in jede M365-App, spezifisch für die Aufgaben der App, in der Sie sie ausführen.

Wer sollte es nutzen: Firmen

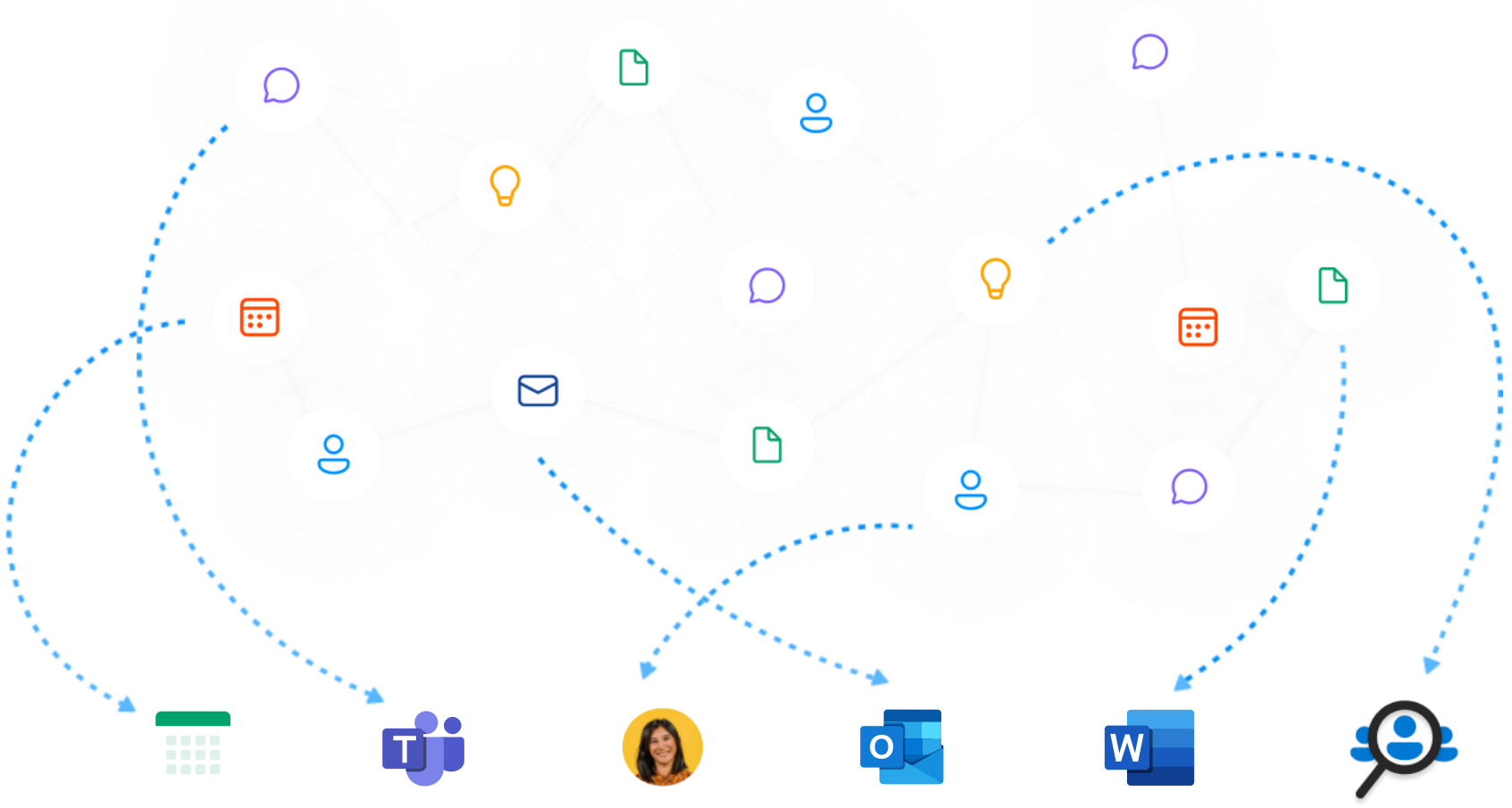
Wie funktioniert es: Interaktion in allem Apps im M365 Kosmos

Auf was greift es zu : Alle Daten in M365 die der Anwender oder mind. 2 Personen geöffnet haben.

Wo greifen User darauf zu: Copilot Icon in jeder App oder copilot.microsoft.com

Microsoft 365 Graph

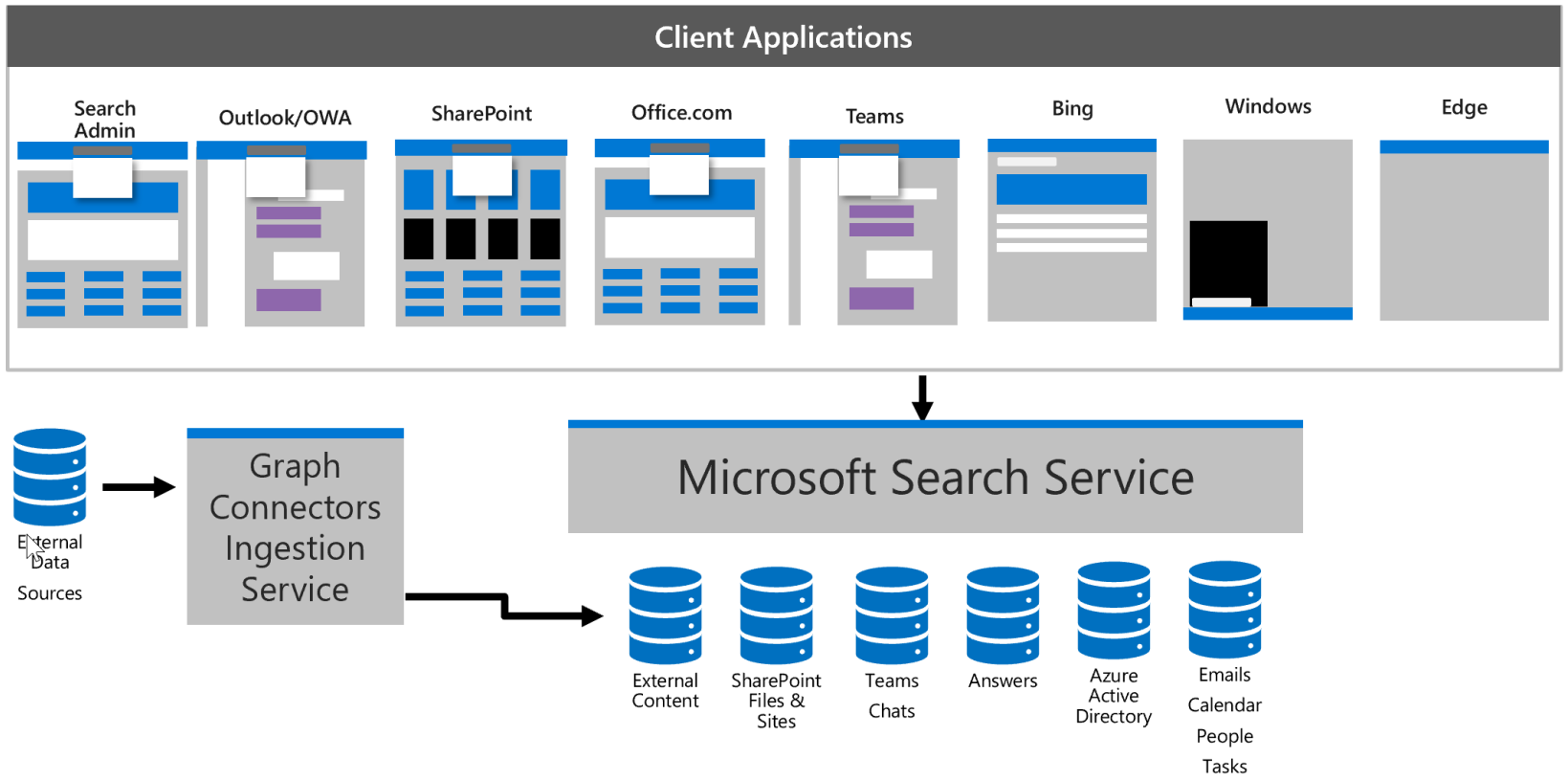
Semantic Fabric über
Microsoft Search



Graph-Verbindung für alle
M365-Entitäten

Verbindung aller Daten und Informationen in M365 als Basis für Copilot Antworten

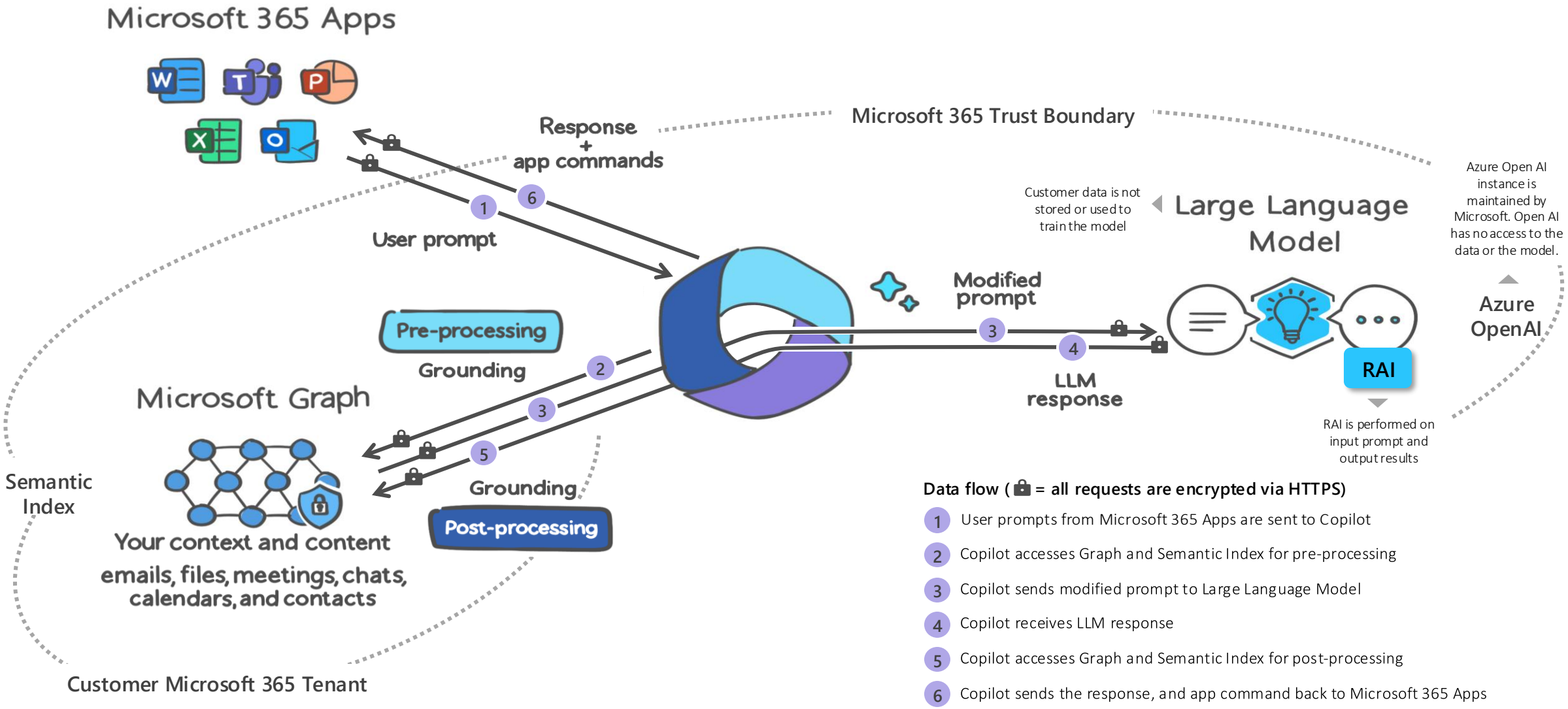
Microsoft 365 Search



Globale Suche über alle M365 Endpunkte

- Erweiterbar per Graph Connector für z.B. OnPremises Systeme als Enterprise Search Lösung
- Grundlage für den Einsatz von Copilot
- Finden von Relevanten Informationen durch priorisierte Suchergebnisse
- Steuern von Ergebnissen durch z.B. HR mittels Redaktionskonzept.

Copilot for Microsoft 365 basic architecture



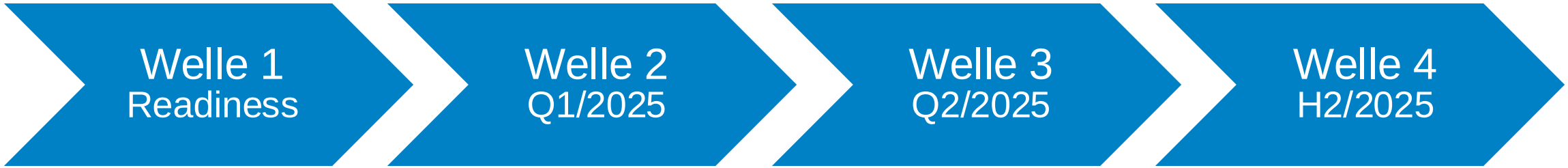
Data flow (= all requests are encrypted via HTTPS)

1. User prompts from Microsoft 365 Apps are sent to Copilot
2. Copilot accesses Graph and Semantic Index for pre-processing
3. Copilot sends modified prompt to Large Language Model
4. Copilot receives LLM response
5. Copilot accesses Graph and Semantic Index for post-processing
6. Copilot sends the response, and app command back to Microsoft 365 Apps

Nächste Schritte

- Abschluss der Workshop Serie
- Planungsworkshop
- Tenant Baseline
- Identitäten & Geräte
- Exchange

Funktionswellen - Beispiel



- Hybrid Identity + Conditional Access und MFA
- Tenant Baseline
- Exchange Hybrid
- LAN/WAN Check
- Intune MDM

- Rollout Apps for Enterprise
- Teams Governance vorbereiten
- Backup Microsoft 365

- Exchange Online Migration
- Teams Meetings, Communication, Collaboration
- SharePoint
- OneDrive
- Planner

- Teams Telefonie

Vielen Dank für die Aufmerksamkeit!

Kontaktieren Sie uns

SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden

Telefon: 06122 53 60
Fax: 06122 53 60
Mobil: 0171 30 74 04 2

info@sva.de
www.sva.de