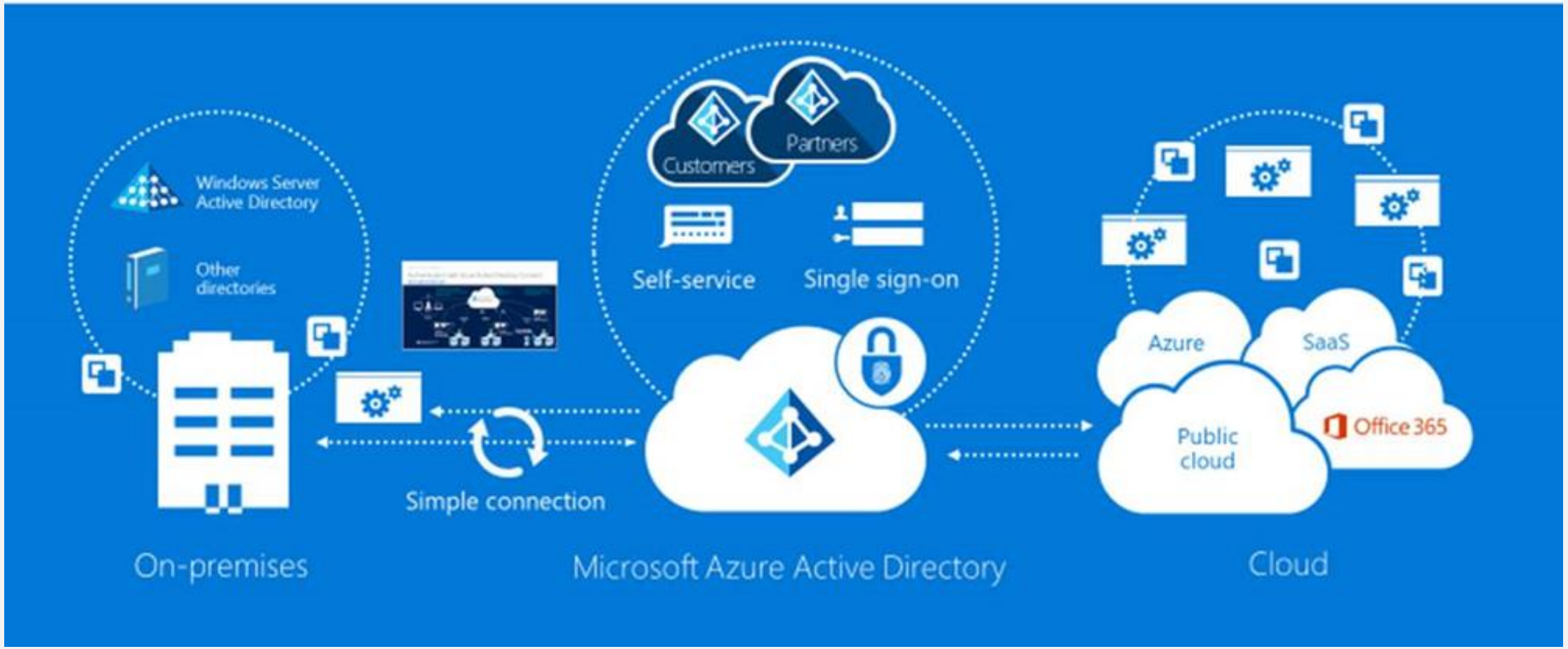
Identity as the core of enterprise mobility

Azure Active Directory as the control plane



M365 GET READY voor GDPR/AVG

MICROSOFT 365 E3

Hybride Enteprise Rechten

- W10 Security Pre-Breach met oa. WIP en Defender
- Office 365 Exchange Online Protection
- Azure Information Protection Plan 1
- Azure Active Directory Plan 1
- Advanced Threat Analytics en Intune
- Litigation (legal) Hold & eDiscovery

E5 FULL SECURITY

GDPR/AVG

- W10 Security Post Breach – W10 Advanced Threat Protection
- Office 365 Advanced Threat Protection
- Azure Information Protection Plan 2
- Azure Active Directory Plan 2
- Cloud App Security
- Office 365 Advanced Compliance (Advanced e-Discovery, Advanced Data Governance, Customer Lock Box, Customer Key)
- Office 365 Threat Intelligence

Microsoft 365 E3/E5 –EMS componenten

TRACEER Breng alle persoonsgegevens binnen de organisatie in kaart	BEHEER Beheer de wijze waarop persoonsgegevens worden gebruikt en ontsloten	BEVEILIG Neem veiligheidsmaatregelen en zorg dat gegevensinbreuken traceerbaar zijn	RAPPORTEER Reageer op verzoeken over gegevens en zorg dat ze beschikbaar zijn
Azure Active Directory Ontdekken en onderhouden van gebruik van het soort toepassingen, gebruikers, cloud of LOB E3 + E5	**Azure Active Directory** Verlenen en intrekken van toegang tot Cloud diensten E3 + E5	**Azure Active Directory** Multi Factor Authenticatie, Conditional Access en Identity Protection met alerts, analyse en maatregelen E3+ E5	**Azure Active Directory** Sign-in pogingen en locaties, logging van applicatie toegang en account onderhoud E3 + E5
Azure Information Protection Identificeren informatietypen met behulp van automatische classificatie E3 + E5	**Azure Information Protection** Handhaven van access control policies op mails en documenten E3 + E5	**Azure Information Protection** Encrypt (automatisch – Plan 2) gevoelige informatie at rest of in transit om ongeoorloofde toegang of gebruik te voorkomen. Denk hierbij aan ondermeer bekijken, bewerken, printen, doorsturen, printscreen E3 + E5	**Azure Information Protection** Reportage op gebruik van documenten vanaf elke locatie in de wereld E3 +E5
Cloud Application Security Krijgen van verbeterde zichtbaarheid van beveiliging controls en policies, inclusief de mogelijkheid op het blokkeren van toegang tot onbeheerde cloud applicaties E5	**Cloud Application Security** Gebruikt de AIP classificatie labels om automatisch governance acties uit te voeren zoals het in quarantaine zetten van files en het intrekken van de mogelijkheid om gevoelige bestanden te delen E5	**Cloud Application Security** Gebruikt machine learning en geavanceerde DLP scanning om te beschermen tegen malware, en het voorkomen dat data naar buiten de organisatie wordt gelekt E5	**Advanced Threat Analytics** Geeft breach notificaties en herstel van de on-premise omgeving E3
Microsoft Intune Ontdek mobile device toepassingen die het apparaat in gevaar kunnen brengen E3		**Microsoft Intune** MDM, MAM en PC Management vanuit de Cloud. Intune geeft toegang tot bedrijfsapplicaties, data en bronnen vanaf elke locatie, op elk apparaat met behoud van de gegevens E3	**Microsoft Intune** Uitgebreide compliance rapportage over het device, operating system en leveranciers E3

Microsoft 365 E3/E5 –OFFICE 365 componenten

TRACEER Breng alle persoonsgegevens binnen de organisatie in kaart	BEHEER Beheer de wijze waarop persoonsgegevens worden gebruikt en ontsloten	BEVEILIG Neem veiligheidsmaatregelen en zorg dat gegevensinbreuken traceerbaar zijn	RAPPORTEER Reageer op verzoeken over gegevens en zorg dat ze beschikbaar zijn
Security & Compliance Center One-stop portal voor het beschermen van data in Office 365. Verschaffen van toegang tot medewerkers voor uitvoeren compliance taken E3			
Advanced Data Governance Voor het behouden en deleten van data op basis van automatische analyse en policy voorstellen E5			
eDiscovery Functies voor casebeheer, zoeken, bewaren, analyseren en exporteren, waardoor snel kan worden voldaan aan eisen mbt onderzoek en wet- en regelgeving E3	**Customer Lockbox** Geeft maximale controle over data in Office365 in het uitzonderlijke geval een Microsoft engineer op verzoek van de klant toegang tot de content krijgt voor het oplossen van een klant probleem E5	**Exchange Online Protection** Beschermt e-mail tegen spam en malware. Ook voor Exchange On Premise mail ! E3 **Office 365 Advanced Threat Protection** Biedt bescherming tegen nieuwe, geavanceerde aanvallen in realtime. Zorgt voor beveiliging tegen onveilige bijlagen en continue beveiliging tegen schadelijke URL's E5	**Customer Lockbox** Geeft maximale controle over data in Office365 in het uitzonderlijke geval een Microsoft engineer op verzoek van de klant toegang tot de content krijgt voor oplossen klant probleem E5
Advanced eDiscovery Gebruikt machine learning, predictief coderen en tekstanalyse om de kosten en issuesmbt het doorzoeken van grote hoeveelheden ongestructureerde gegevens te verminderen E5	**Journaling in Exchange Enterprise** Reageren op wettelijke en regelgevende eisen en naleving hiervan mbt inkomende en uitgaande e-mailberichten E3	**Data Loss Prevention & Legal Hold** DLP zorgt voor het beschermen van gegevens, waar het wordt opgeslagen, verplaatst en gedeeld. Legal Hold zet een mailbox bij onderzoek veilig, zodat de organisatie bij onderzoek de versie van de waarheid heeft E3	**Office 365 Threat Intelligence** Aanalyse en inzicht in de omgevingsbedreigingen inclusief malware, targeted gebruikers en links naar wereldwijde security informatie en cijfers E5
		Office 365 Customer Key Biedt mogelijkheid om eigen encryption keys in te brengen en controle te hebben over het onleesbaar maken van data in Office 365 E5	**Compliance Manager (nieuw)** Voor het managen van Compliancy op één centrale plek. Geeft real-time risico assesments met een score over de compliance prestatie van Microsoft Cloud gebruik afgezet tegen regelgeving Unknown

Microsoft 365 E3/E5 –Windows Enterprise componenten

TRACEER Breng alle persoonsgegevens binnen jouw organisatie in kaart	BEHEER Beheer de wijze waarop persoonsgegevens worden gebruikt en ontsloten	BEVEILIG Neem veiligheidsmaatregelen en zorg dat je gegevensinbreuken kunt traceren	RAPPORTEER Reageer op verzoeken over gegevens en zorg dat ze beschikbaar zijn
Content Search Voorkomen dat Windows Search of PowerShell, bestanden met persoonlijke data kunnen verwerken, die opgeslagen zijn in lokale of gedeelde opslag E3	**Data Governance** Middels Windows permissies kunnen beheerders toegangsrechten beheren tot persoonlijke data E3	**Windows Hello** Vervangt wachtwoorden met sterke twee authenticatiefactoren, welke gebonden zijn aan een specifiek apparaat en gebruik maakt van biometrische gegevens of een PIN E3	**Auditing and Logging** Geeft gedetailleerde data, die geëxporteerd kunnen worden naar andere oplossingen voor diepere analyse of compliance rapportage E3
	Dynamic Access Control Geeft IT de mogelijkheid om dynamisch op basis van gevoeligheid, rol van de gebruiker of de apparaatconfiguratie toegang te verschaffen tot bronnen E3	**Windows Defender ATP** Facilitieert IT om doelgerichte en geavanceerde aanvallen te kunnen detecteren, onderzoeken en reageren. Is gericht op aanvallen die normale virusscanners niet kunnen detecteren E5	**Windows Defender ATP** Facilitieert IT om doelgerichte en geavanceerde aanvallen te kunnen detecteren, onderzoeken en reageren. Is gericht op aanvallen die normale virusscanners niet kunnen detecteren E5
	Data Classification Toolkit Identificeer, classificeer en bescherm data op fileservers en simplifieer Dynamic Access Control E3	**Bitlocker** Zorgt door middel van schijf encryptie dat op het apparaat opgeslagen informatie (data at rest) veilig is. Zelfs indien er geprobeerd wordt om de harde schijf te benaderen, zonder gebruik te maken van het geïnstalleerde besturingssysteem E3	
		Windows Information Protection (WIP) Beschermt tegen het (on)bewust lekken van informatie door middel van verschillende beveiligingsmaatregelen, zoals encryptie E3	
		Credential Guard (Identity Protection) Voorkomt aanvallen met gestolen inlog-ggegevens, zoals Pass-the-Hash of Pass-The-Ticket, via het isoleren van deze 'secrets' zodat alleen goedgekeurde systeemsoftware erbij kan E3	