Microsoft Security- und Verwaltungstools für E-Mails & Geräte

Exchange Online (EXO)	EXO ist die gehostete **Cloud-Lösung** von Microsoft Exchange Server. Sie stellt den Usern in Unternehmen Zugriff auf *E-Mail*, *Kalender*, *Kontakte* und *Aufgabenverwaltung* per Webbrowser, Microsoft Outlook oder mit Mobilgeräten zur Verfügung. Cloud-Lösung bedeutet, dass die User / Unternehmen nicht über die vollständige Kontrolle der Hardware und Infrastruktur verfügen. Beispiel: Mit dem Basisangebot von EXO Plan 1 stehen Benutzern 50 GB *Postfachspeicher* zu einem *Preis* von 3,40 Euro *pro Benutzer* und *Monat* zur Verfügung. Microsoft bietet *Exchange Online Protection* als Teil dieses Dienstes an, um E-Mails auf Malware und Spam zu prüfen.
Exchange Online Protection (EOP)	EOP (Abb. 1) ist der cloudbasierte **Filterdienst**, der Ihre Organisation vor Spam, Schadsoftware und anderen E-Mail-Bedrohungen schützt. EOP ist in allen MS 365-Organisationen mit EXO Postfächern enthalten.
Microsoft 365 Defender	MS 365 Defender (Abb. 2) ist eine vereinheitlichte **Enterprise-Defense-Suite**, die Erkennung, Verhinderung, Untersuchung und Reaktionen auf Endpunkte, Identitäten, E-Mails und Anwendungen systemweit koordiniert, um integrierten Schutz vor komplexen Angriffen zu bieten. Mit der integrierten Microsoft 365 Defender-Lösung können Sicherheitsexperten die von den einzelnen Produkten erfassten Bedrohungssignale zusammenfügen und den vollständigen Umfang und die Auswirkungen einer Bedrohung bestimmen; *wie* sie in die Umgebung *gelangt* ist, *was* davon *betroffen* ist und *wie* sie sich derzeit auf die Organisation *auswirkt*. MS 365 Defender führt automatisch Gegenmaßnahmen aus, um einen Angriff zu verhindern oder zu beenden und die Selbstheilung betroffener Postfächer, Endpunkte und Benutzeridentitäten durchzuführen. Es existieren verschiedene M365D-Dienste; Defender für Endpunkt, für Sicherheitsrisikomanagement, für Office 365, für Identity und für Cloud Apps. Defender für Office 365 schützt vor Bedrohungen durch E-Mail-Nachrichten, Links (URLs) und Tools für die Zusammenarbeit. Defender für Office 365 enthält: • **Richtlinien zum Schutz vor Bedrohungen**: Selbstdefinierte Richtlinien, um den geeigneten Schutzgrad festzulegen. • **Berichte**: Echtzeitberichte, um die Leistung von Defender für Office 365 zu überwachen. • **Untersuchung von und Antwort auf Bedrohungen**: Tools, um Bedrohungen zu untersuchen, zu verstehen, zu simulieren und zu verhindern. • **Funktionen für automatische Untersuchung und Reaktion**
Microsoft Endpoint Manager (EPM)	*Endpoint Manager (Abb. 3)* umfasst die ***Dienste*** und ***Tools*** zum Verwalten und Überwachen von mobilen Geräten, Desktop-Computern, virtuellen Maschinen, eingebetteten Geräten und Servern. EPM kombiniert möglicherweise bereits bekannte & benützte Dienste wie z.B. *MS Intune*, *Configuration Manager*, *Desktop Analytics*, *Co-Verwaltung* und *Windows Autopilot*. Diese Dienste sind Bestandteil des MS 365-Stapels und helfen, den Zugriff zu sichern, Daten zu schützen, auf Risiken zu reagieren und Risiken zu verwalten. Die EPM-Marketingarchitektur umfasst drei Stufen auf dem Weg zur Cloudverwaltung. Das Ziel ist die einheitliche Co-Verwaltung von Endpunkten mit *Configuration Manager (Abb. 4)* und *Intune (Abb. 5)*. Auf Stufe 1 kommen *"Tenant Attach"*-Funktionen zum Einsatz, die Configuration Manager-Kunden eine hochflexible Lösung für den Umstieg in die Cloud bieten. Zu diesem Zeitpunkt müssen Windows-Clients nicht zwingend bei Intune registriert werden. Verbinden Sie die Configuration Manager-Site einfach mit der Cloud, um vielseitige Remoteaktionen und Analysen zu nutzen. Auf Stufe 2 folgt die *Co-Verwaltung* der Windows-Umgebung über Configuration Manager und Intune. Windows 10-Geräte werden gemeinsam von Configuration Manager und der Verwaltung mobiler Geräte (MDM) verwaltet. Neukunden oder Betreibern neuer Endpunkte wird empfohlen, von Anfang an Intune in der Cloud zu nutzen. Stufe 3 bietet die Möglichkeit, weitere Workloads stufenweise in die Cloud zu migrieren. Im Rahmen der MS 365-Lizenz wird ein Unternehmen wahrscheinlich EPM einführen, das Intune, Configuration Manager, Desktop Analytics, Co-Verwaltung und Windows Autopilot zu einer einheitlichen Plattform zusammenführt, um die Geräte und Apps der Organisation zu schützen und zu verwalten.
Microsoft Intune	Intune (Abb. 6) ist ein **cloudbasierter Dienst**, der sich auf die **Verwaltung mobiler Geräte (MDM)** und die mobile Anwendungsverwaltung (MAM) richtet. Der Kunde bestimmt, wie die Geräte des Unternehmens, einschließlich Mobiltelefone, Tablets und Laptops, genutzt werden. Intune wurde aus der Cloud und für die Cloud entwickelt und ist eng mit *Azure Active Directory (Azure AD)* verknüpft. Intune lässt sich in *Richtlinien für Azure AD* und bedingten Zugriff integrieren, um den Zugriff auf Apps und Geräte zu verwalten und Unternehmensdaten zu schützen und zu isolieren.

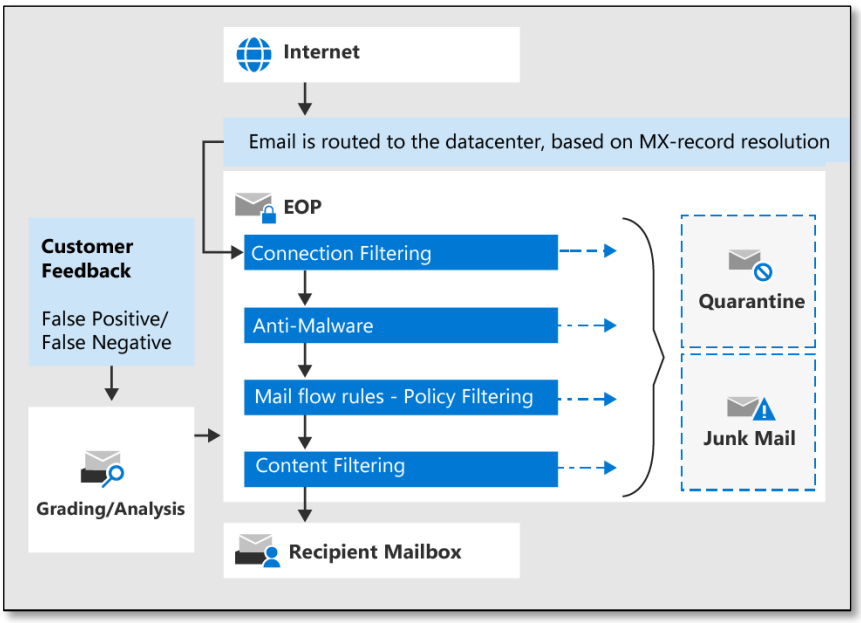

Abb. 1: Exchange Online Protection - ist ein cloudbasierter Filterdienst.

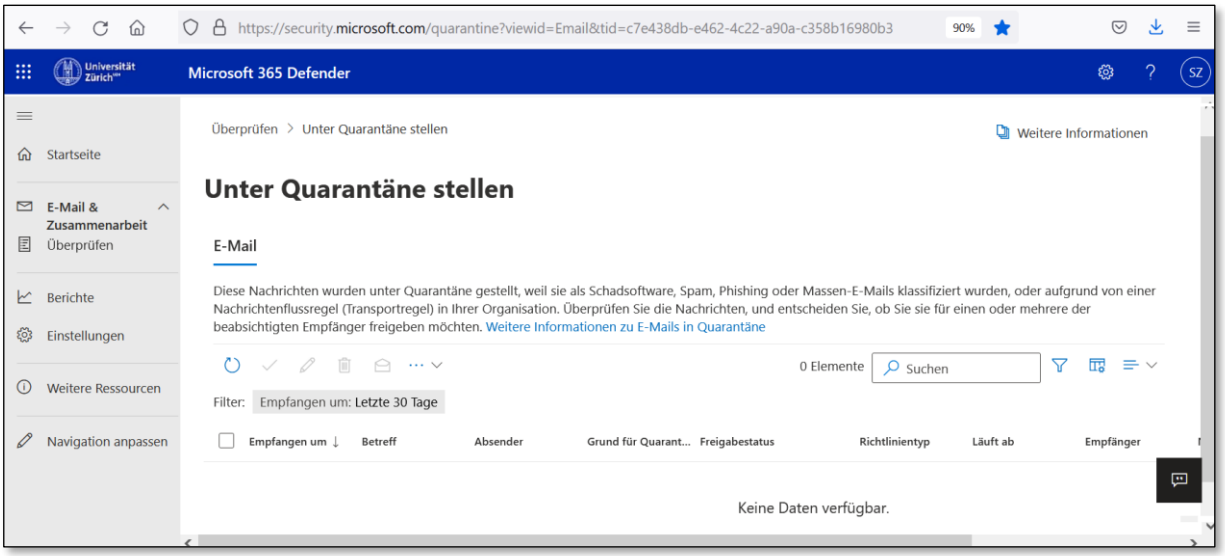

Abb. 2: MS 365 Defender - ist eine Enterprise-Defense-Suite.

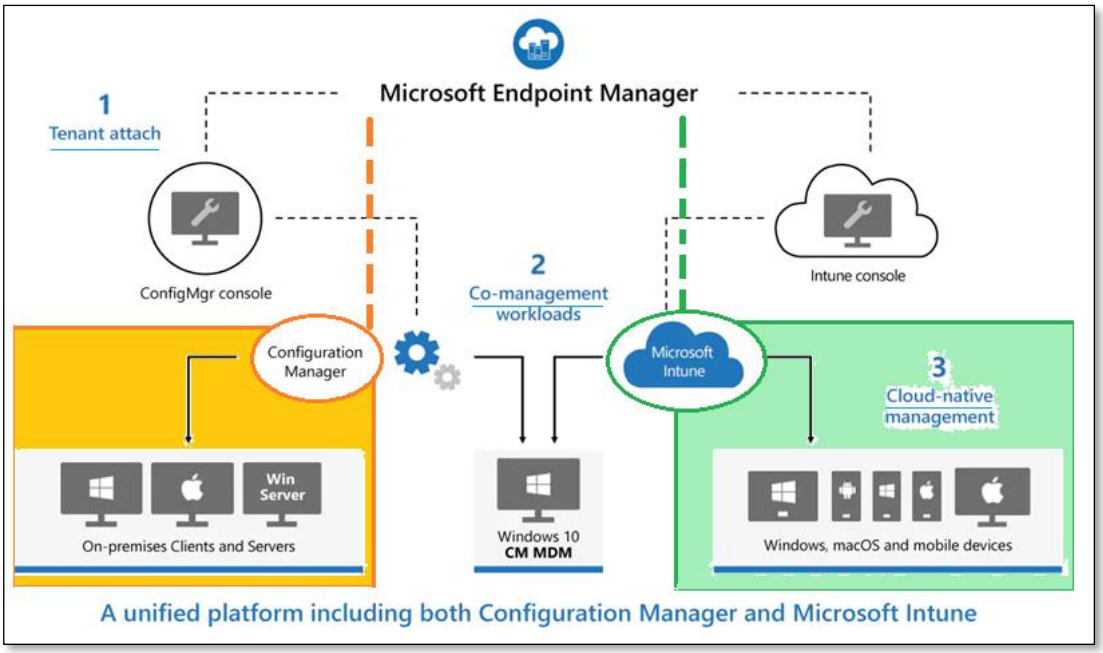

Abb. 3: MS Endpoint Manager (EPM) - stellt Dienste und Tools zur Geräteverwaltung / Überwachung zur Verfügung.

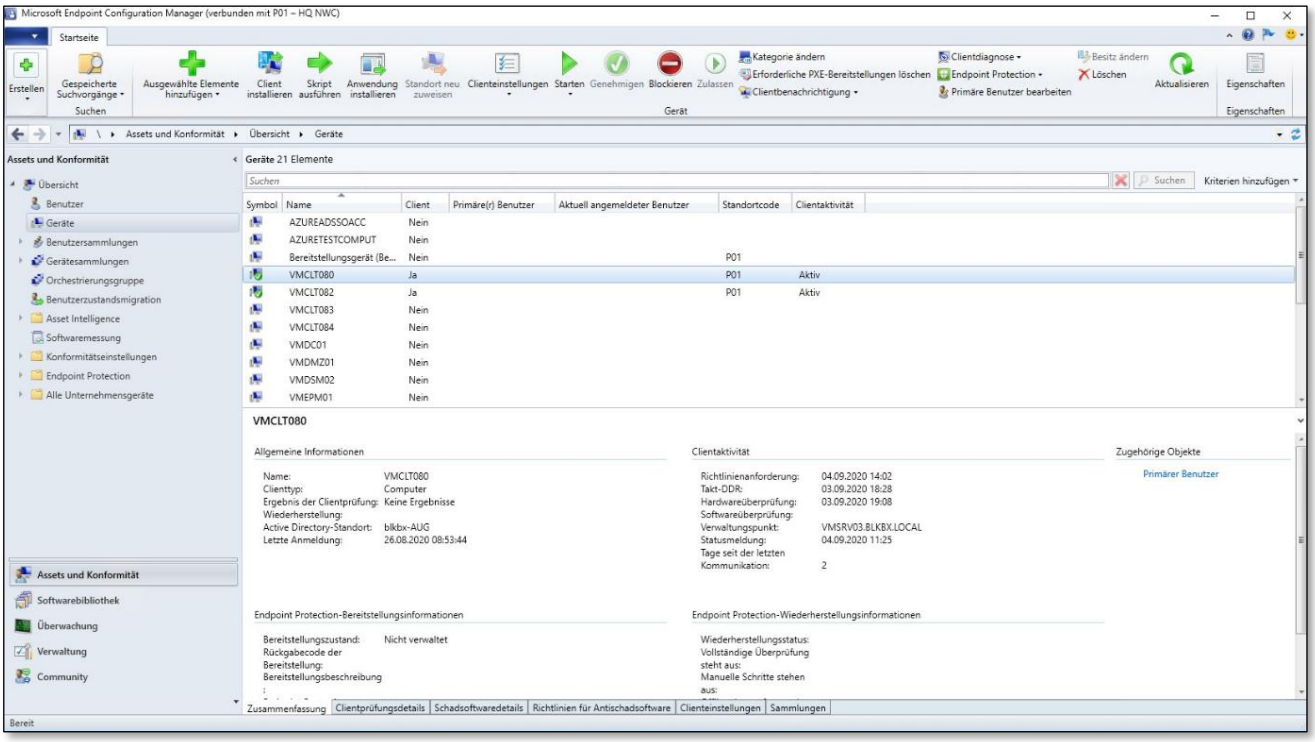

Abb. 4: MS Endpoint Configuration Manager (ECM) - ist ein einzelnes Tool vom EPM.

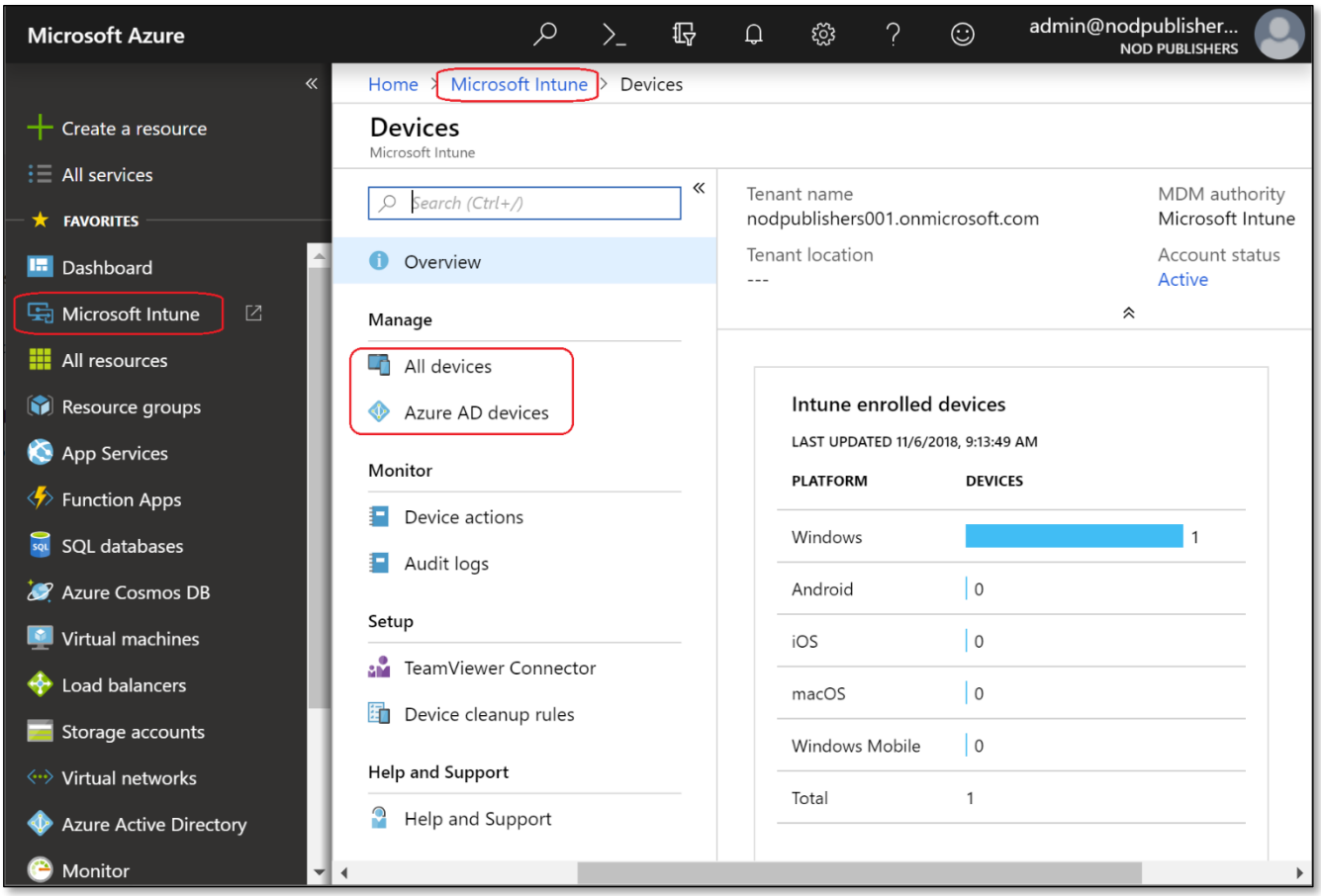

Abb. 5: MS Intune - ist ein weiteres einzelnes Tool vom EPM.

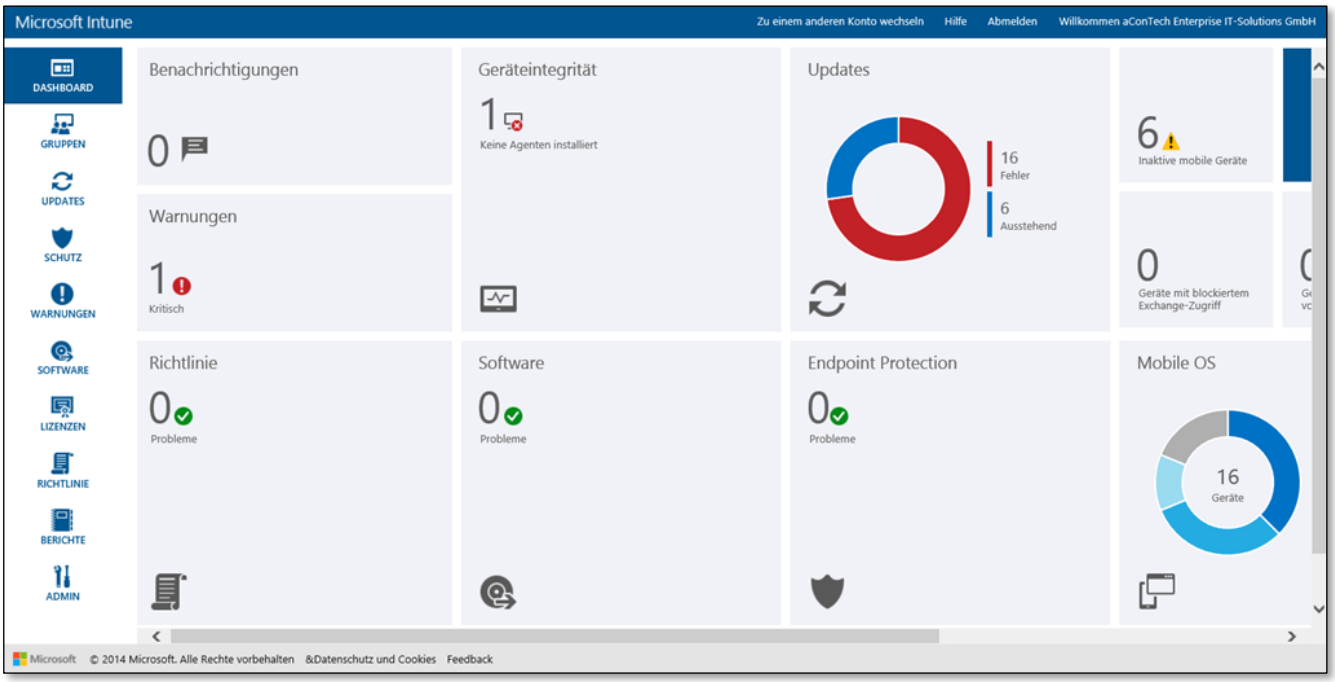

Abb. 6: MS Intune Dashboard