Microsoft Security and Management Tools for Email & Devices

Exchange Online (EXO)	EXO is the hosted **cloud solution** of Microsoft Exchange Server. It provides corporate users with access to *email, calendar, contacts* and *task management* via web browser, Microsoft Outlook or with mobile devices. Cloud solution means that users / companies do not have complete control of the hardware and infrastructure. Example: the basic EXO Plan 1 offering provides users with 50 GB of mailbox *storage* at a *cost* of 3.40 euros per *user* per *month*. Microsoft offers *Exchange Online Protection* as part of this service to check emails for malware and spam.
Exchange Online Protection (EOP)	EOP (Fig. 1) is the cloud-based **filtering service** that protects your organization from spam, malware and other email threats. EOP is included in all MS 365 organizations with EXO mailboxes.
Microsoft 365 Defender	MS 365 Defender (Fig. 2) is a unified **enterprise defense suite** that coordinates detection, prevention, investigation and response across endpoints, identities, email and applications system-wide to provide integrated protection against complex attacks. With the integrated Microsoft 365 Defender solution, security professionals can aggregate the threat signals captured by each product and determine the full scope and impact of a threat; how it *entered* the environment, what is *affected*, and how it is currently *impacting* the organization. MS 365 Defender automatically executes countermeasures to prevent or stop an attack and perform self-healing of affected mailboxes, endpoints and user identities. Several M365D services exist; Defender for Endpoint, for Security Risk Management, for Office 365, for Identity and for Cloud Apps. Defender for Office 365 protects against threats from email messages, links (URLs) and collaboration tools. Defender for Office 365 includes: • **Threat protection policies** Self-defined policies to determine the appropriate level of protection. • **Reports**: Real-time reports to monitor the performance of Defender for Office 365. • **Threat investigation and response:** Tools to investigate, understand, simulate, and prevent threats. • **Automated investigation and response capabilities**
Microsoft Endpoint Manager (EPM)	*Endpoint Manager* (Fig. 3) includes the **services** and **tools** to manage and monitor mobile devices, desktop computers, virtual machines, embedded devices and servers. EPM may combine already known & used services such as *MS Intune, Configuration Manager, Desktop Analytics, Co-Management* and *Windows Autopilot*. These services are part of the MS 365 stack and help secure access, protect data, respond to risk and manage risk. The EPM marketing architecture includes three stages on the path to cloud management. The goal is unified co-management of endpoints with *Configuration Manager (Fig. 4)* and *Intune (Fig. 5)*. Stage 1 uses *"tenant attach"* capabilities that provide Configuration Manager customers with a highly flexible solution for moving to the cloud. At this stage, Windows clients do not necessarily need to be registered with Intune. Simply connect the Configuration Manager site to the cloud for versatile remote actions and analytics. Stage 2 involves *co-managing* the Windows environment through Configuration Manager and Intune. Windows 10 devices are co-managed by Configuration Manager and mobile device management (MDM). New customers or operators of new endpoints are recommended to use Intune in the cloud from the beginning. Tier 3 provides the ability to migrate additional workloads to the cloud in stages. As part of the MS 365 license, an organization is likely to adopt EPM, which brings together Intune, Confi-guration Manager, Desktop Analytics, Co-management and Windows Autopilot into a unified platform to protect and manage the organization's devices and apps.
Microsoft Intune	Intune (Fig. 6) is a **cloud-based service** focused on **mobile device management (MDM)** and mobile application management (MAM). The customer determines how the company's devices, including cell phones, tablets and laptops, are used. Intune is built from the cloud and for the cloud, and is tightly integrated with *Azure Active Directory (Azure AD)*. Intune integrates with Azure AD and conditional access *policies* to manage access to apps and devices and protect and isolate corporate data.

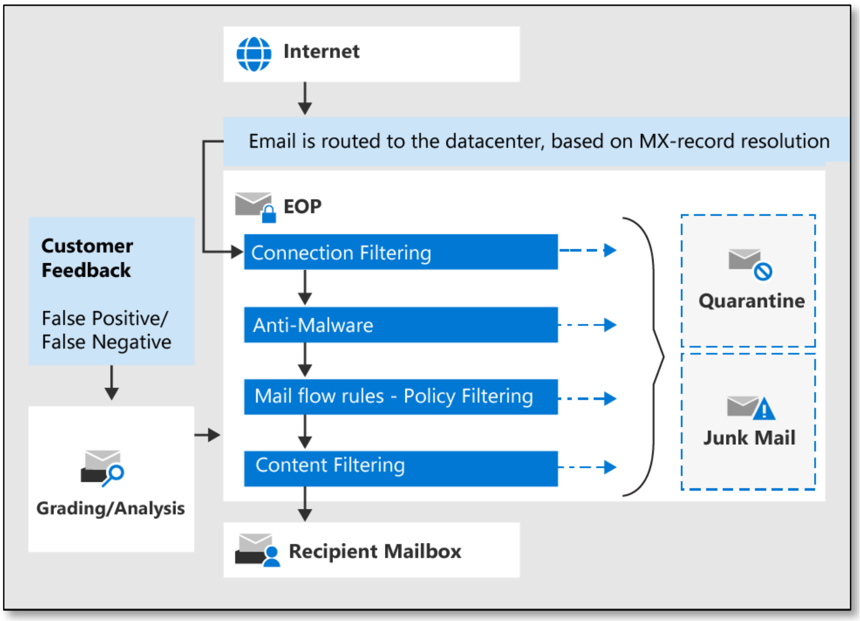
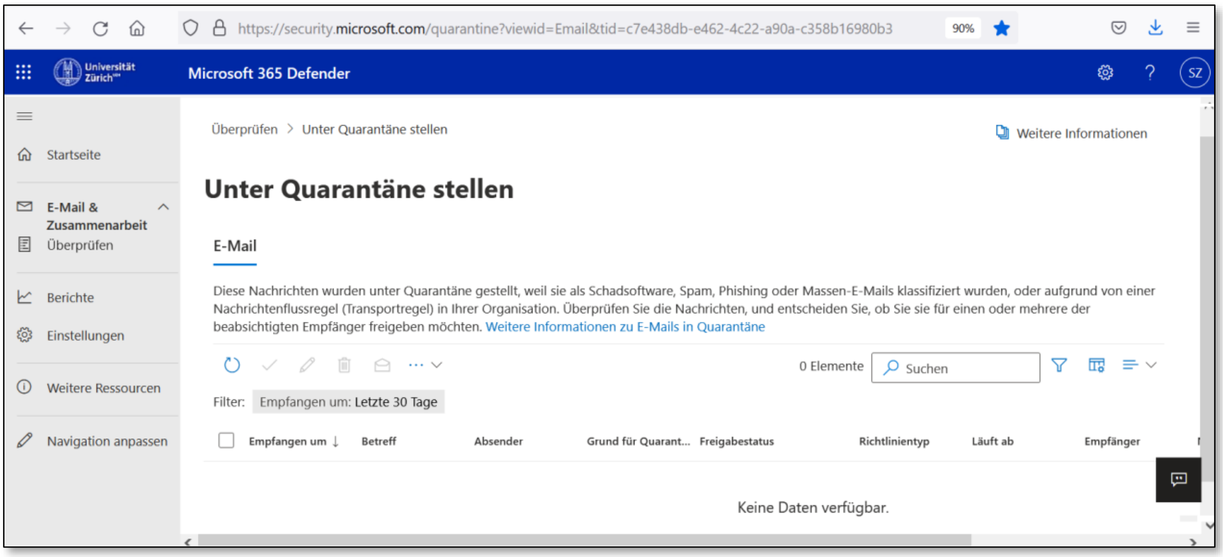


Fig. 1: Exchange Online Protection - is a cloud-based filtering service.


https://security.microsoft.com/quarantine?viewid=Email&tid=c7e438db-e462-4c22-a90a-c358b16980b3 90%

Universität Zürich Microsoft 365 Defender SZ

Startseite
E-Mail & Zusammenarbeit
Überprüfen
Berichte
Einstellungen
Weitere Ressourcen
Navigation anpassen

Überprüfen > Unter Quarantäne stellen

Weitere Informationen

Unter Quarantäne stellen

E-Mail

Diese Nachrichten wurden unter Quarantäne gestellt, weil sie als Schadsoftware, Spam, Phishing oder Massen-E-Mails klassifiziert wurden, oder aufgrund von einer Nachrichtenflussregel (Transportregel) in Ihrer Organisation. Überprüfen Sie die Nachrichten, und entscheiden Sie, ob Sie sie für einen oder mehrere der beabsichtigten Empfänger freigeben möchten. Weitere Informationen zu E-Mails in Quarantäne

0 Elemente Suchen

Filter: Empfangen um: Letzte 30 Tage

□	Empfangen um ↓	Betreff	Absender	Grund für Quarant...	Freigabestatus	Richtlinientyp	Läuft ab	Empfänger

Keine Daten verfügbar.

Fig. 2: MS 365 Defender - is an enterprise defense suite.

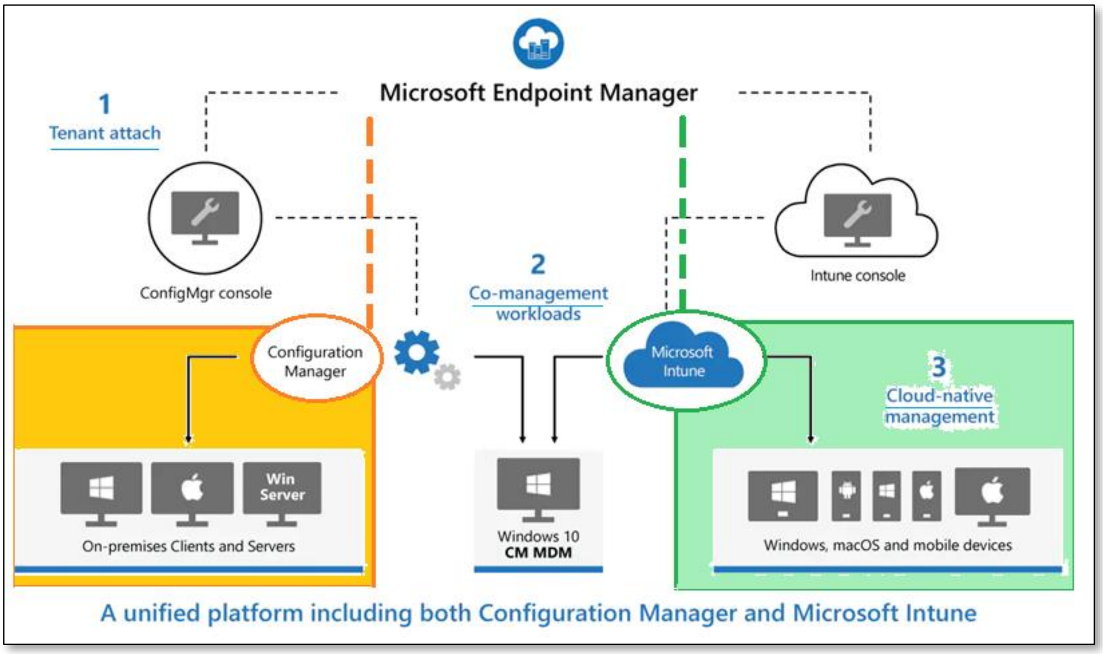
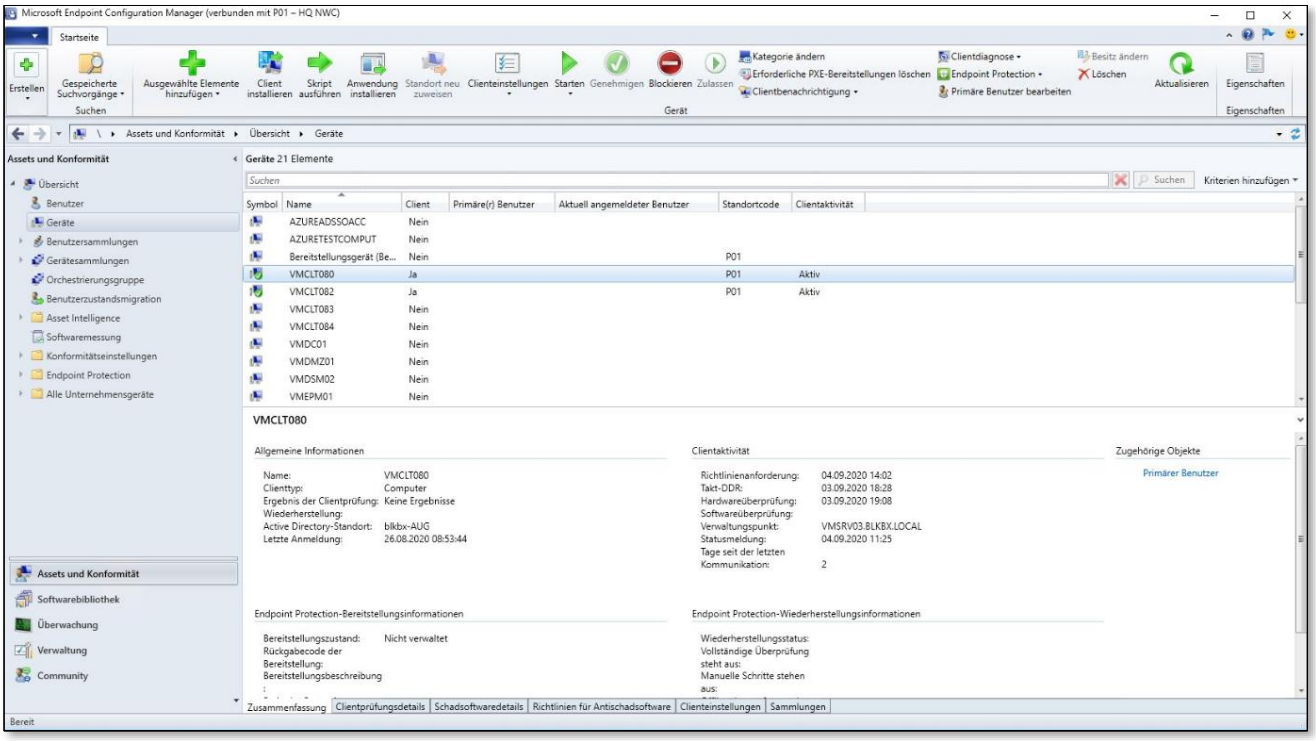

Microsoft Endpoint Manager
1
Tenant attach
ConfigMgr console
Intune console
2
Co-management workloads
Configuration Manager
Microsoft Intune
3
Cloud-native management
Win Server
On-premises Clients and Servers
Windows 10 CM MDM
Windows, macOS and mobile devices
A unified platform including both Configuration Manager and Microsoft Intune

Fig. 3: MS Endpoint Manager (EPM) - provides services and tools for device management / monitoring



Geräte 21 Elemente

Symbol	Name	Client	Primäre(r) Benutzer	Aktuell angemeldeter Benutzer	Standortcode	Clientaktivität
	AZUREADSSOACC	Nein				
	AZURETESTCOMPUT	Nein				
	Bereitstellungsgerät (Be...	Nein			P01	
	VMCLT080	Ja			P01	Aktiv
	VMCLT082	Ja			P01	Aktiv
	VMCLT083	Nein				
	VMCLT084	Nein				
	VMDC01	Nein				
	VMDMZ01	Nein				
	VMDSM02	Nein				
	VMEPM01	Nein				

VMCLT080

Allgemeine Informationen

Name: VMCLT080
Clienttyp: Computer
Ergebnis der Clientprüfung: Keine Ergebnisse
Wiederherstellung:
Active Directory-Standort: blkbx-AUG
Letzte Anmeldung: 26.08.2020 08:53:44

Clientaktivität

Richtlinienanforderung: 04.09.2020 14:02
Takt-DDR: 03.09.2020 18:28
Hardwareüberprüfung: 03.09.2020 19:08
Softwareüberprüfung:
Verwaltungspunkt: VMSRV03.BLKBX.LOCAL
Statusmeldung: 04.09.2020 11:25
Tage seit der letzten Kommunikation: 2

Zugehörige Objekte

Primärer Benutzer

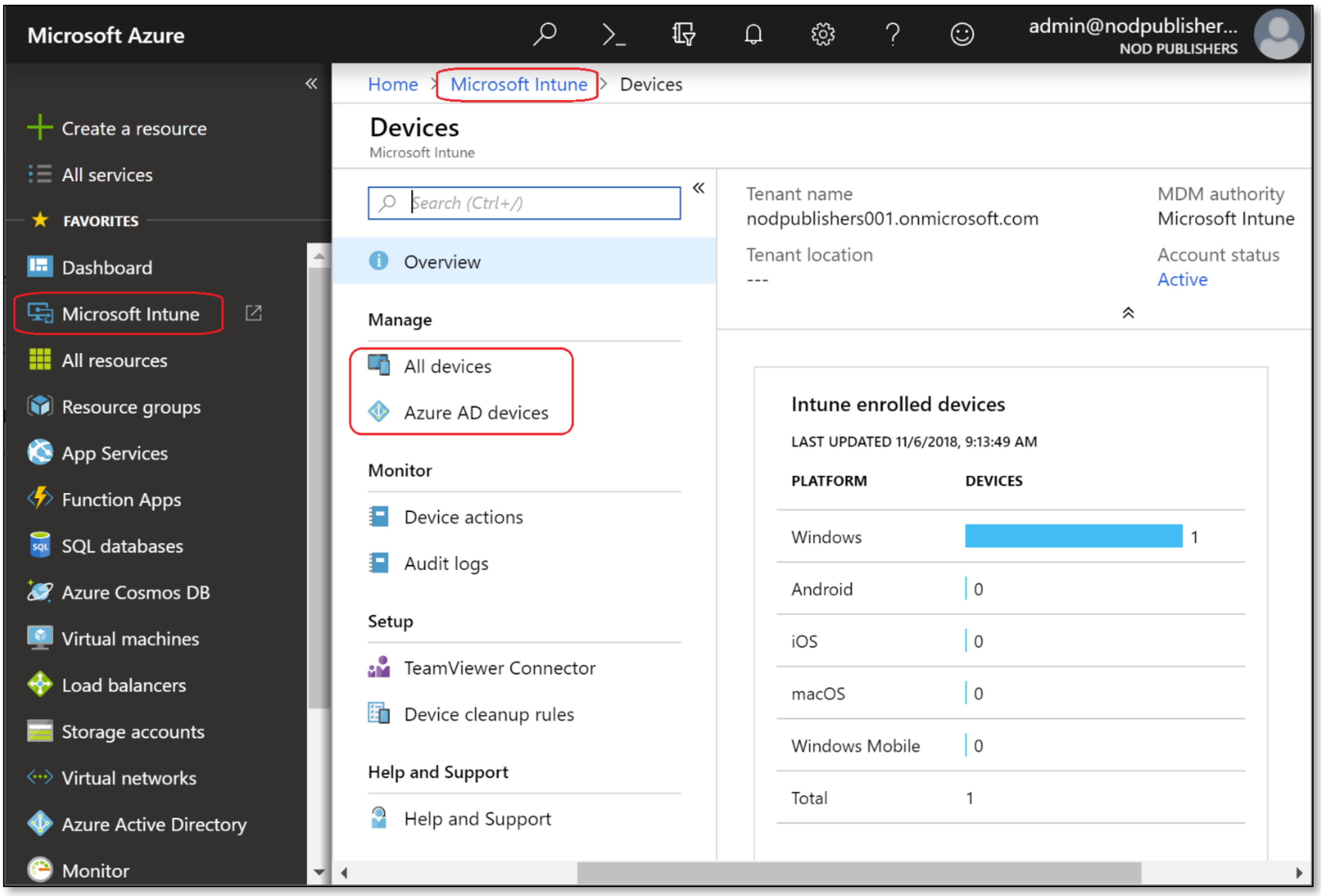
Endpoint Protection-Bereitstellungsinformationen

Bereitstellungszustand: Nicht verwaltet
Rückgabecode der Bereitstellung:
Bereitstellungsbeschreibung:

Endpoint Protection-Wiederherstellungsinformationen

Wiederherstellungsstatus:
Vollständige Überprüfung steht aus:
Manuelle Schritte stehen aus:

Fig. 4: MS Endpoint Configuration Manager (ECM) - is a single tool from EPM.



Devices
Microsoft Intune

Tenant name
nodpublishers001.onmicrosoft.com

MDM authority
Microsoft Intune

Tenant location

Account status
Active

Intune enrolled devices

LAST UPDATED 11/6/2018, 9:13:49 AM

PLATFORM	DEVICES
Windows	1
Android	0
iOS	0
macOS	0
Windows Mobile	0
Total	1

Fig. 5: MS Intune - is another single tool from EPM.

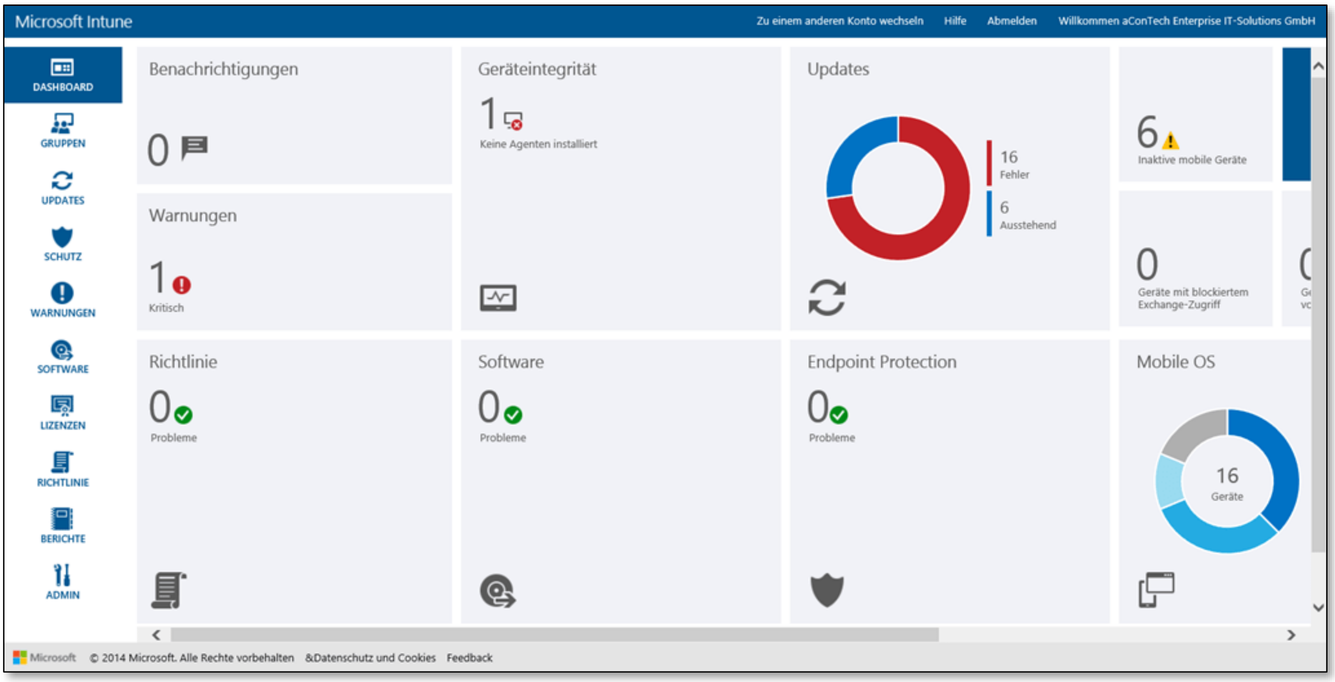


Fig. 6: MS Intune Dashboard