10. září 2023

Seyfor

If you want something to digitise,

Just sey it!

- Veřejný sektor

Jak realizujeme moderní bezpečné IT prostředí na platformě produktů Microsoft

2023

O nás…

- Seyfor – divize CSC (Cloud & Security Competence Centre)
  - Dříve jsme se jmenovali Mainstream Technologies
- Naše kompetenční portfolio:
  - Microsoft Partner v oblasti cloudu
  - Partner pro technická řešení od společností Fortinet, PaloAlto, Veeam
  - Letité zkušenosti v oblasti většiny „onprem“ produktů portfolia MS (AD, Exchange, SharePoint, System Center, atd.)
- Máme bohaté zkušenosti jak z komerční sféry, tak z prostředí státní správy

Agenda

- Proč Microsoft Cloud
- Klíčové principy návrhu i implementace řešení
- Zero-trust strategie
- Příkladové řešení

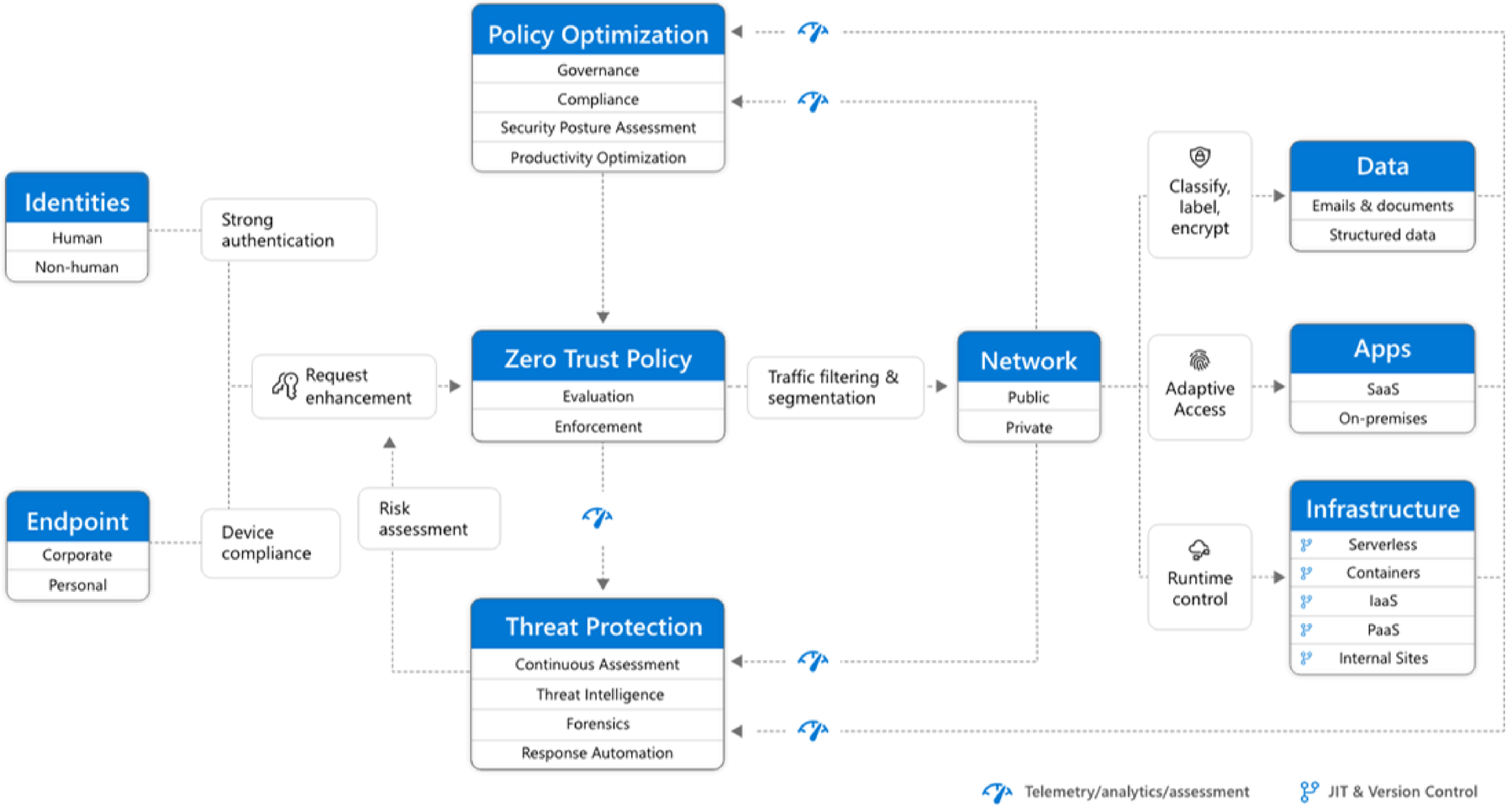
Proč Microsoft Cloud?

- M365 – moderní prostředí pro práci a spolupráci
- Azure – robustní a bezpečná platforma pro provoz aplikací a infrastrukturních služeb
- Bezpečnost na všech úrovních
- Jeden vendor – ucelené řešení
- Důsledné využití cloudových řešení snižuje nároky na počet a odbornost vlastních pracovníků
- Rychlost – lze vybudovat celé produkční prostředí během několika měsíců

Klíčové principy při návrhu i implementaci řešení

- Cloud je primární platformou pro vznik prostředí
- Security by design
- Zero-trust strategie
- Pravidlo Clean source / Clean keyboard
  - Přístup do prostředí pouze z důvěryhodných zařízení
  - Kontrola obsahu všech přenášených souborů přes Azure DevOps
  - Získávání instalačních souborů pouze z autorizovaných zdrojů
- Audit a bezpečnostní dohled na všech vrstvách
  - Archivace logů v Immutable storage
  - SIEM

Zero-trust strategie



Příkladové řešení

Seyfor

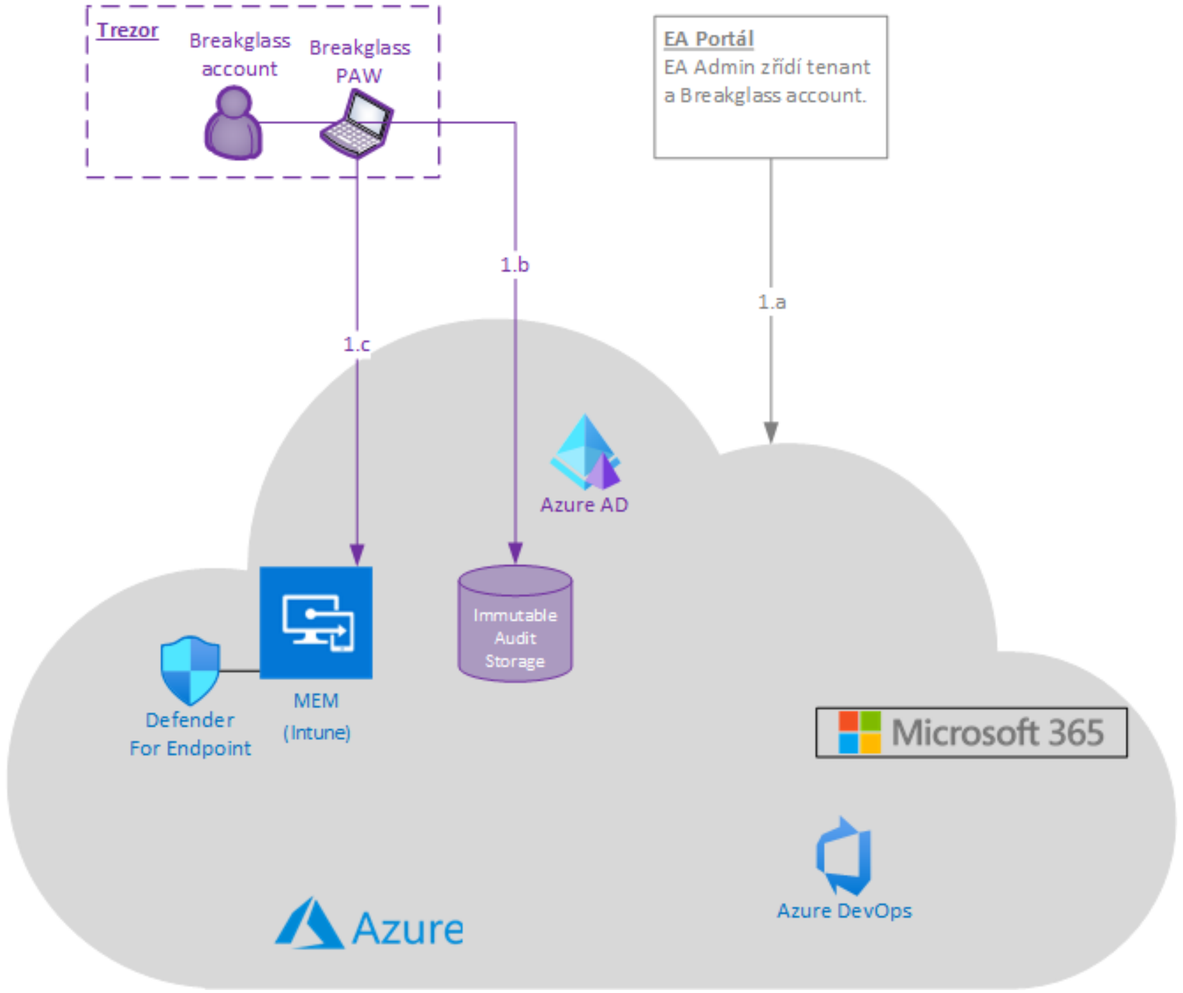
Zadávací kritéria

- Postavit uživatelské prostředí na zelené louce
  - Kancelářské služby -> M365 suite
  - Možnost postupné migrace existujících aplikací a služeb
- Rychlost realizace
- Maximální bezpečnost prostředí i realizace
- Minimální nároky na nový HW
- Vstupní licence:
  - M365 E3 + E5 Security add-on
  - Azure subskripce
  - MS EA licensing
  - Produkty třetích stran, pokud jsou potřebné

Seyfor

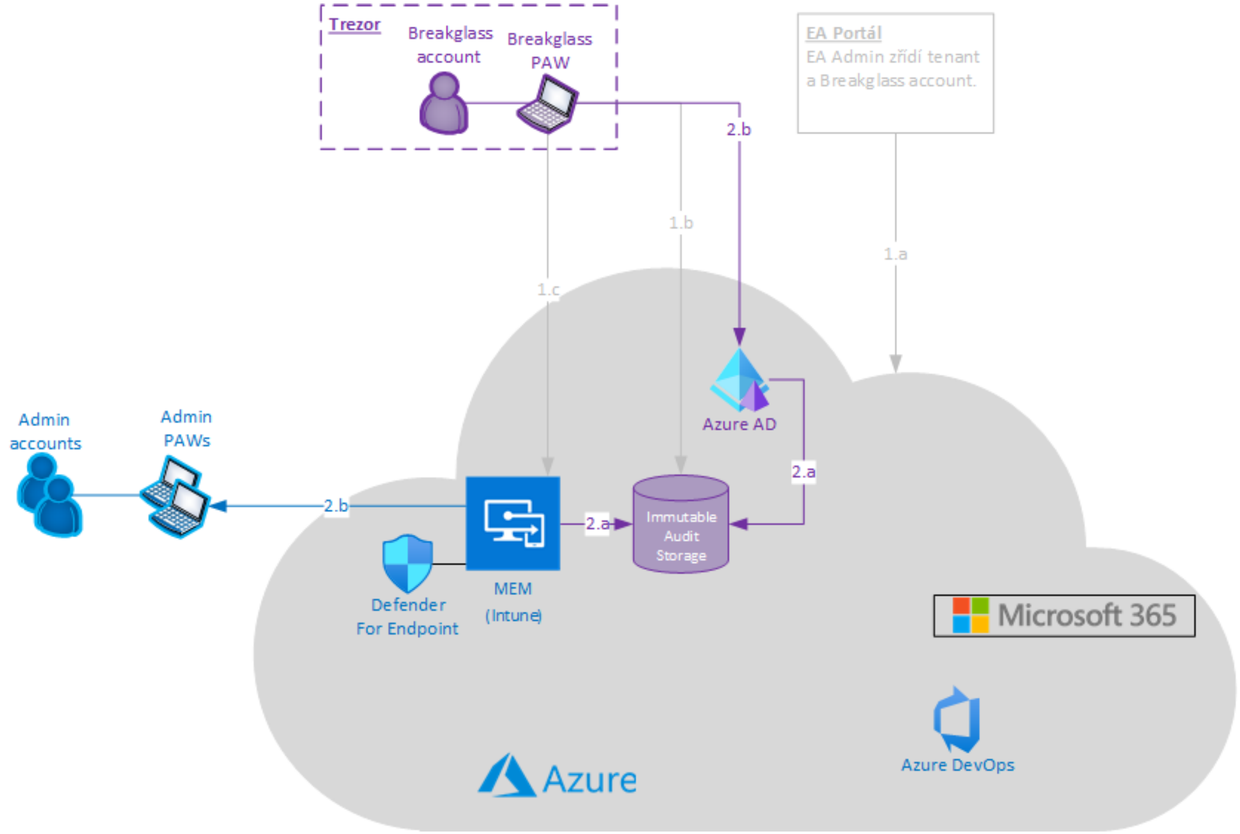
1. Zřízení nového tenantu M365 / Azure

- Nastavení procesu protokolování všech admin aktivit
- Zřízení nového tenantu v Enterprise portálu pod nově registrovaným DNS domain name
- Vytvoření **Breakglass účtu** pro správu MS cloudu
- Vytvoření fyzické **Breakglass standalone PAW** stanice
- Aktivace první subskripce v Azure
- **Aktivace centrálního auditu** prostředí
- Konfigurace prostředí pro PAW management (MEM + Endpoint Defender)



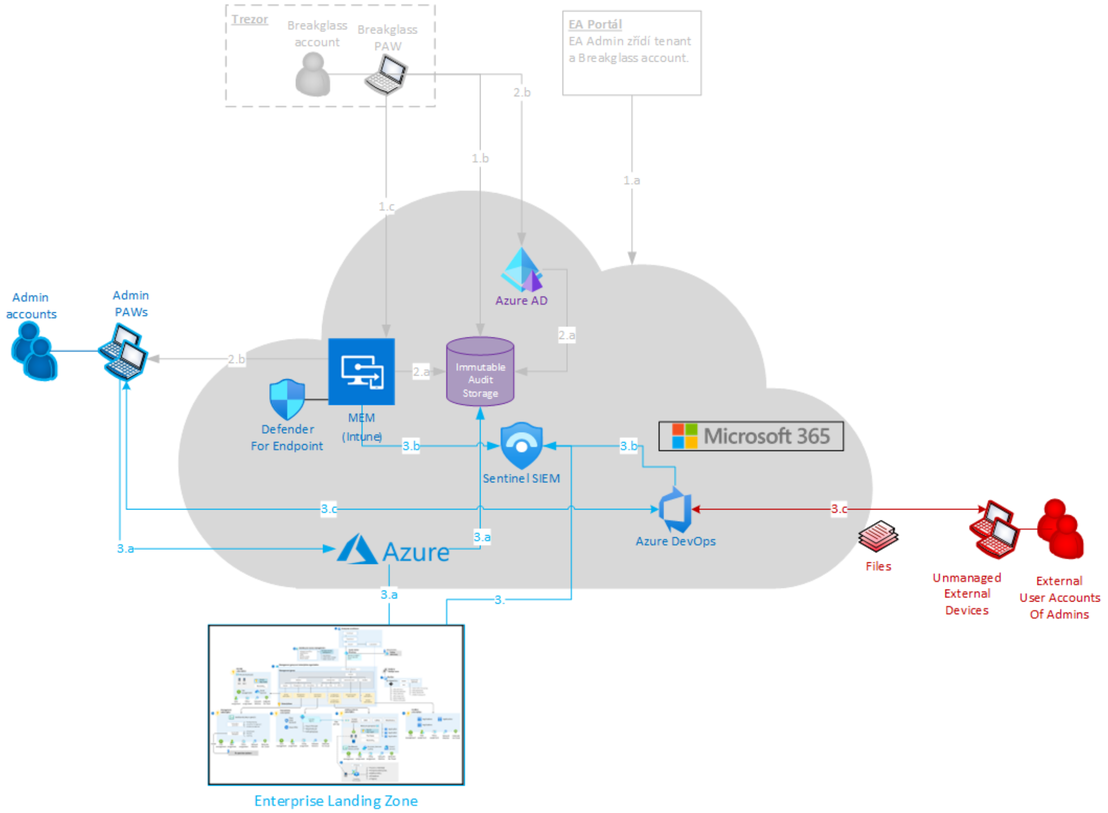
2. Zřízení bezpečného management prostředí

- Zajištění licencí M365
- Napojení AAD a MEM (Intune) na **centrální audit**
- Účty správců v AAD – PIM / PAM / Least-privilege
- Příprava PAW pro správce
- Řízené vydávání PAW oprávněným osobám



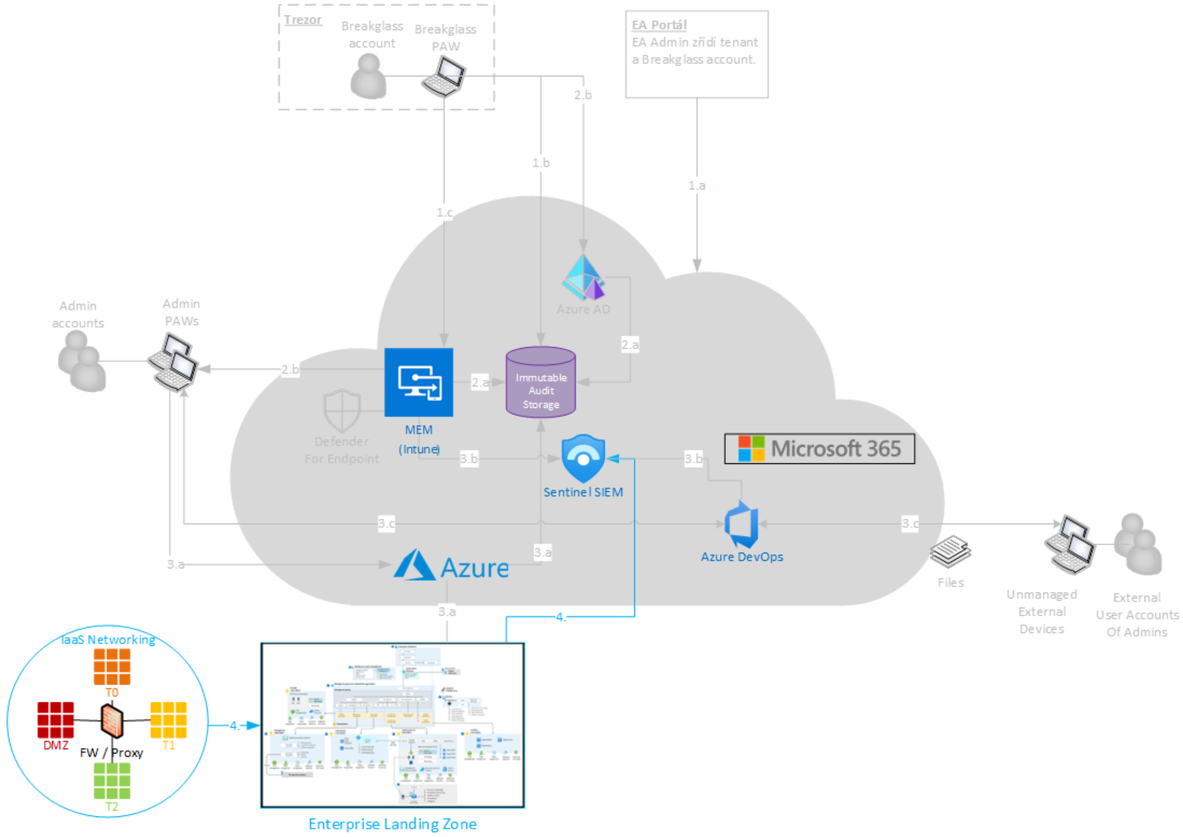
3. Zřízení IaaS prostředí v Azure

- Příprava subskripcí a modelu jejich správy
- Design a zřízení infrastruktury „**AS A CODE**“
  - Enterprise landing zone
- Management výhradně přes PAW a delegované admin účty
- Aktivace MS **Sentinel** jako **SIEM**
  - Všechny komponenty prostředí jsou přidávány jako sledované zdroje včetně vydaných PAW
- Přenos souborů i kódu řízeně a výhradně přes Azure **DevOps**



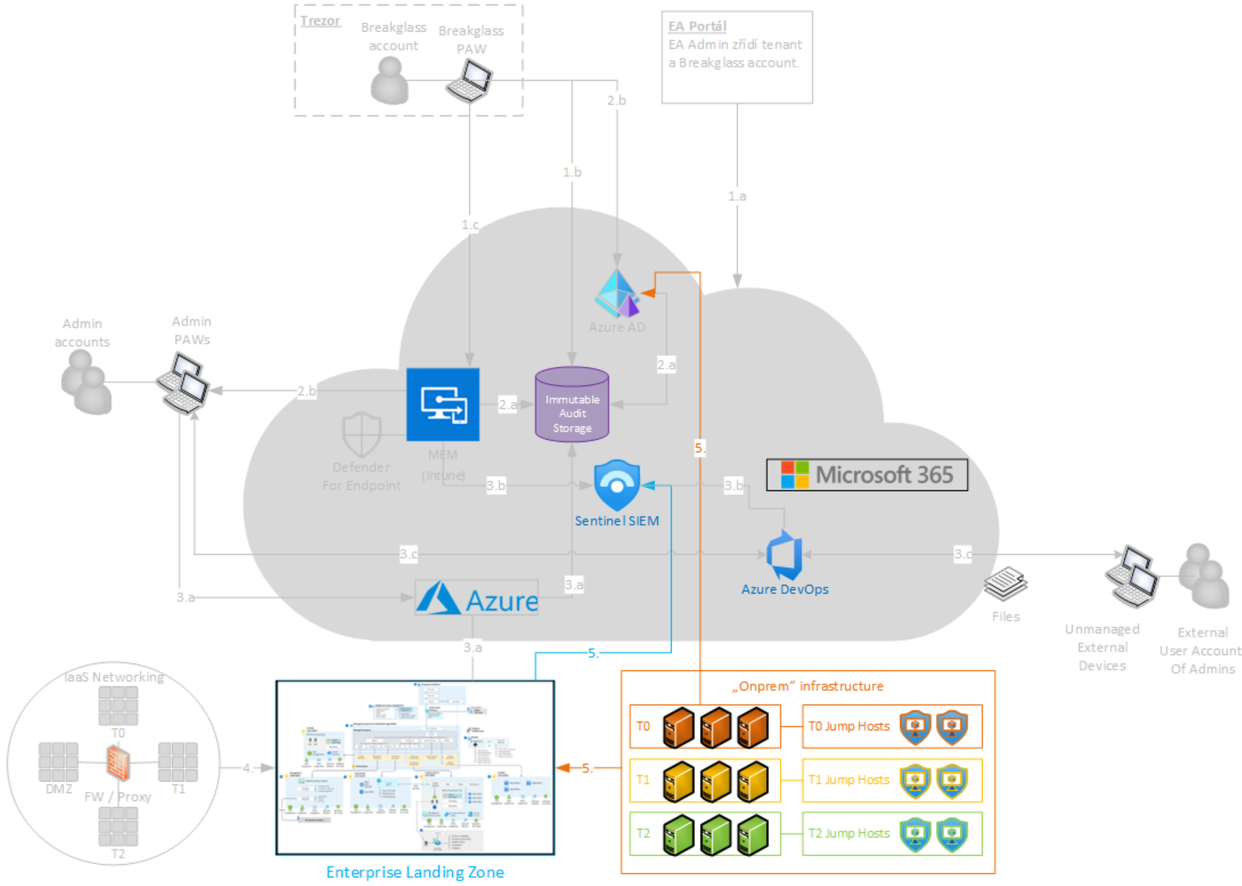
4. Síťová segmentace IaaS

- Segmentace sítě s využitím Private Endpoints
- Nasazení všech virtuálních prvků v HA
  - Azure Load Balancers
  - Fortinet **FortiGate** virtual appliances jako segmentační **FW i Explicit Proxy**
- Audit provozu přes **FortiAnalyzer**
- Napojení na centrální audit a SIEM
- Schvalovací a evidenční proces pro řízení síťových prostupů (jako součást Zero-Trust modelu)



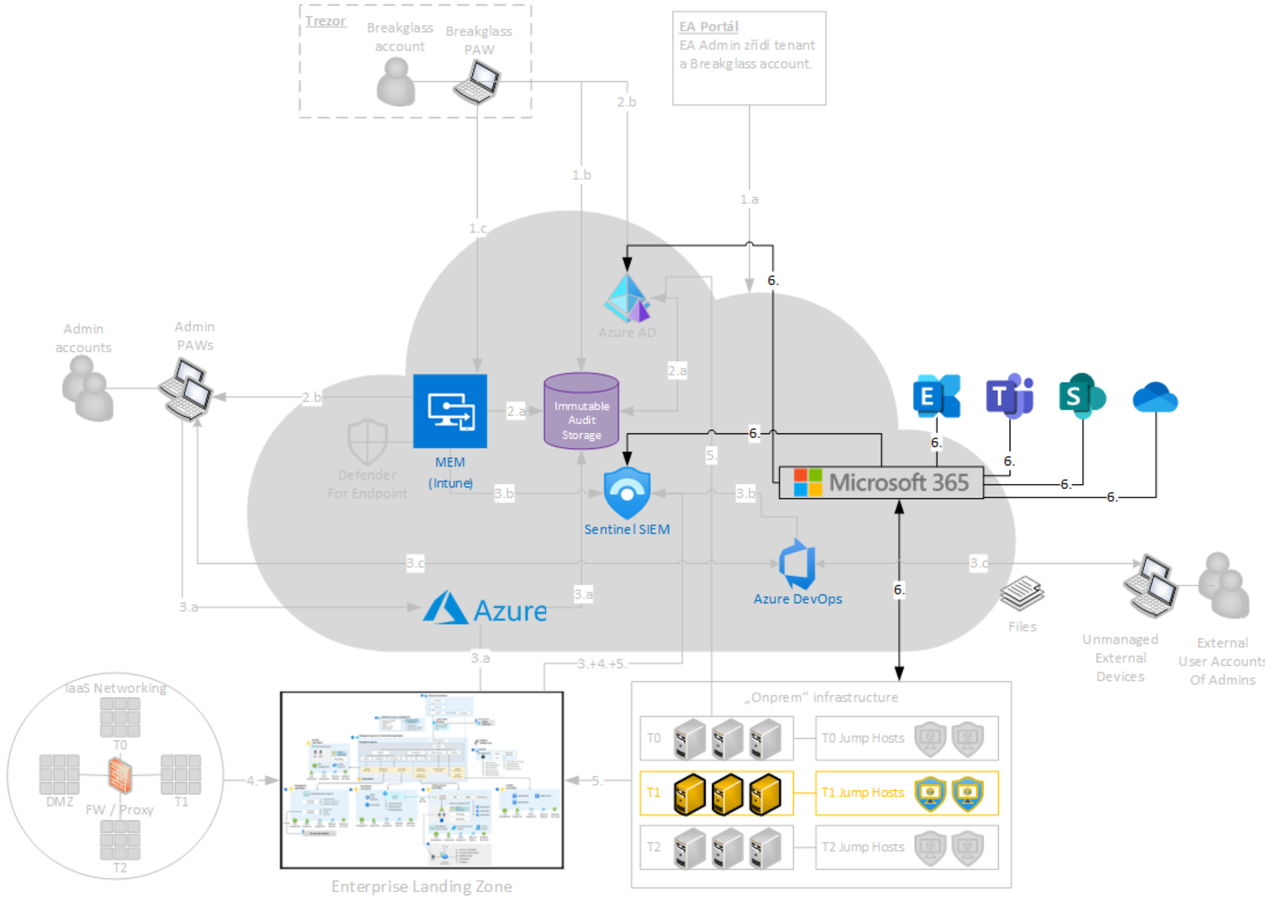
5. Zřízení „on-premises“ infrastruktury v IaaS

- Založení nového **AD forestu**
- Napojení na audit a SIEM
- **Propojení AD s Azure AD** (zejména pro účely SSO a podporu legacy aplikací)
- Implementace AD tieringu
- Security hardening AD
- **Zřízení Jump serverů** pro správu jednotlivých AD tierů – přístup výhradně z PAW
- Zřízení interního PKI primárně pro účely zabezpečení síťové komunikace
- Zřízení hybridní konfigurace služeb, např. MS Exchange a MS SharePoint



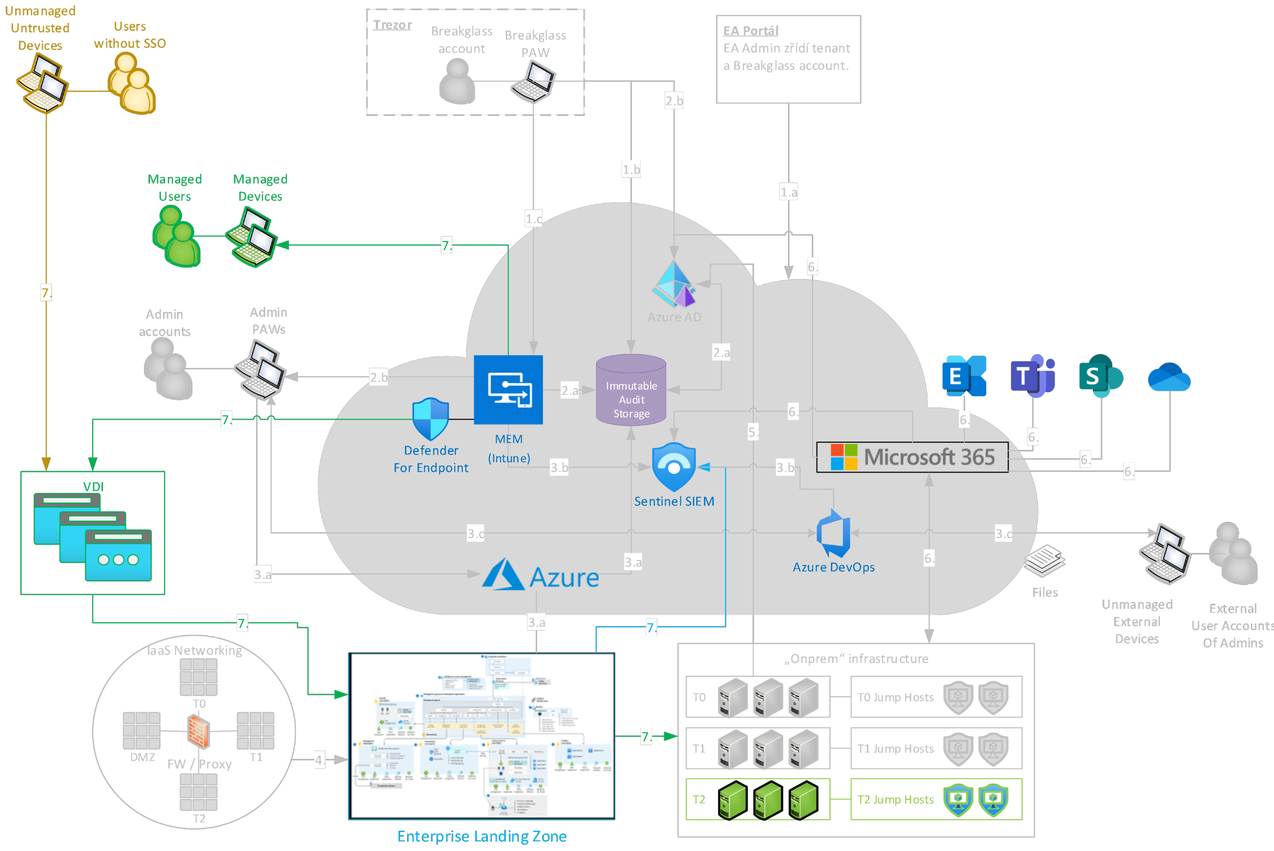
6. Konfigurace služeb M365

- Hardening Azure AD (např. aktivace MFA, Defenderů, PAM, Conditional Access, atd.)
- Bezpečná konfigurace kolaboračních služeb:
  - Exchange Online
  - Teams
  - SharePoint Online
  - OneDrive
- Zabezpečení DNS a MailFlow
  - Zřízení externích DNS a MTA instancí



7. Zřízení uživatelského pracovního prostředí uživatelů

- Kombinace vhodných metod provozu uživatelských zařízení:
  - VDI v Azure – MS nebo Citrix
  - Správa fyzických zařízení v režimu Clean Source / Clean Keyboard
- Konfigurace bezpečného přístupu do prostředí VDI
  - VDI se typicky použije jako primární varianta v případě, kdy máme podezření, že stávající prostředí je kompromitováno.
- Řízení bezpečnosti prostřednictvím Defender for Endpoint / GPO / MEM (Intune)
- Správa fyzických zařízení přes MEM (Intune)
- Vytvoření uživatelských účtů v AD
- Jejich synchronizace do Azure AD
- Nastavení licencování



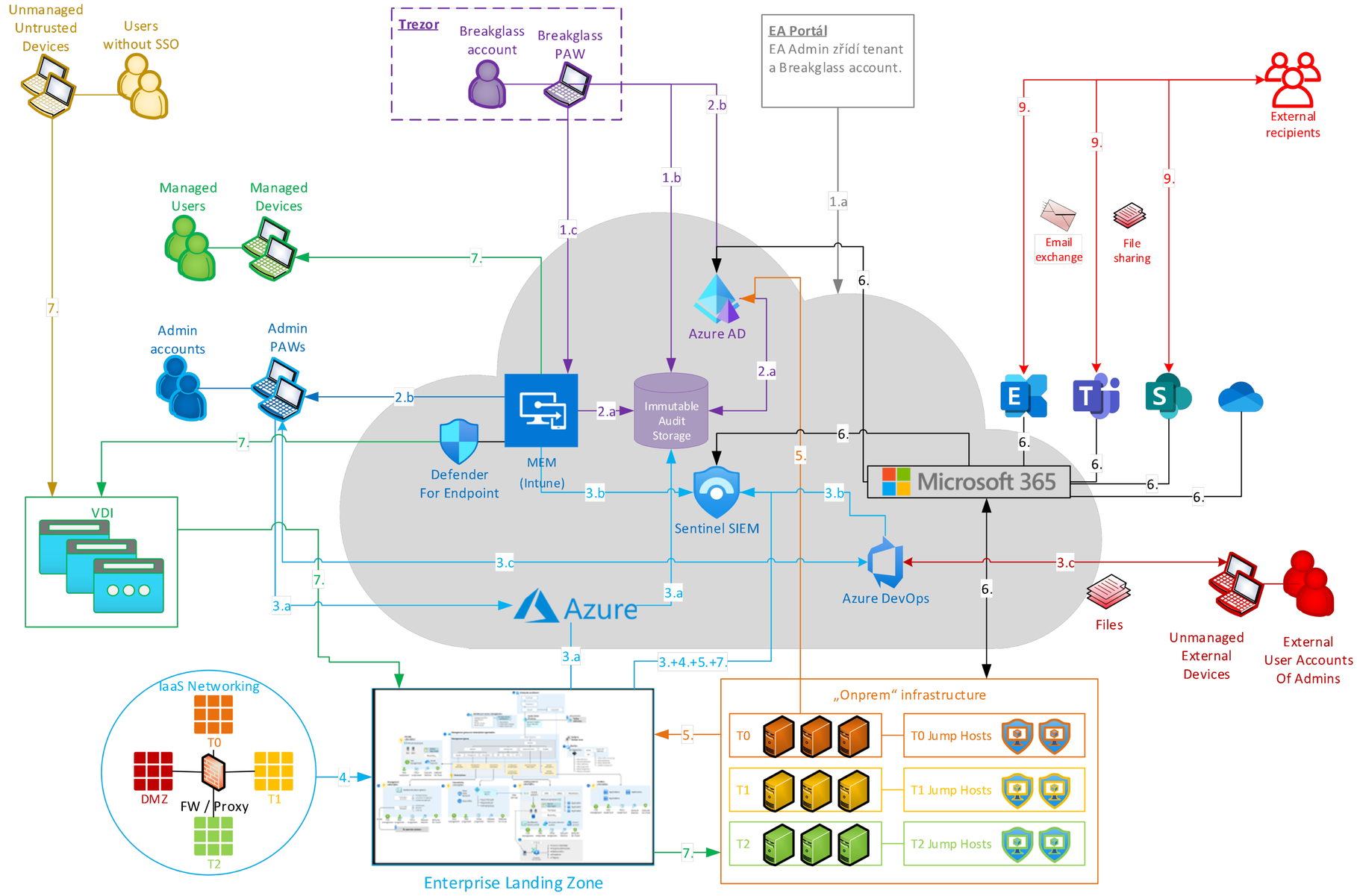
8. Příprava na spuštění prostředí v produkčním režimu

- UAT
- Penetrační testy
- Provozní testy
- Příprava na spuštění pilotního provozu

9. Spuštění pilotního provozu prostředí

- Jsou nastaveny procesy:
  - IT Management governance
  - Service governance
  - User governance
  - Device governance
  - Data governance
  - User support
  - SOC
- Úvodní migrace uživatelských dat a dat IT služeb
- Řízený onboarding uživatelů formou workshopů, školení a dalších vzdělávacích mechanismů podle zvyklostí Organizace

Celkový HL pohled na vybudované prostředí



Shrnutí

- Příkladové řešení jsme byly schopni realizovat v průběhu 5 měsíců při poskytnutí plné součinnosti zákazníkem.
- Timeline:

Aktivity:	1. měsíc	2. měsíc	3. měsíc	4. měsíc	5. měsíc	6. měsíc	7. měsíc	8. měsíc	9. měsíc
Přípravné práce (smlouvy, licence, SoW, HL Design, zdroje, atp.) – není zahrnuto do času realizace – např. 3 měsíce									
1.+2. Zřízení tenanta a nastavení managementu prostředí				Realizace					
3.+4. Zřízení Azure subskripcí a IaaS				Design	Realizace	Change management			
5. Zřízení „onprem“ prostředí				Design	Realizace		Change management		
6. Konfigurace služeb M365					Design	Realizace		Change management	
7. Zřízení uživatelského prostředí				Design		Realizace		Change management	
8. Příprava na spuštění						Příprava		Testy	
9. Spuštění pilotního provozu						Příprava			Spuštění pilotu

Thank you for your attention.

Seyfor