



This file contains multiple Azure landing zone architectures and diagrams. Please choose which architecture/diagram you'd like to view.


**If you don't know which one, we suggest you start with either
“ALZ Hub & Spoke”, “ALZ VWAN”, or “ALZ Terminology”.**


It also contains the diagrams for Sovereign Landing Zones. See “SLZ Hub & Spoke”, “SLZ VWAN”, or “SLZ Hierarchy”.


VERSION: 2025-09-12

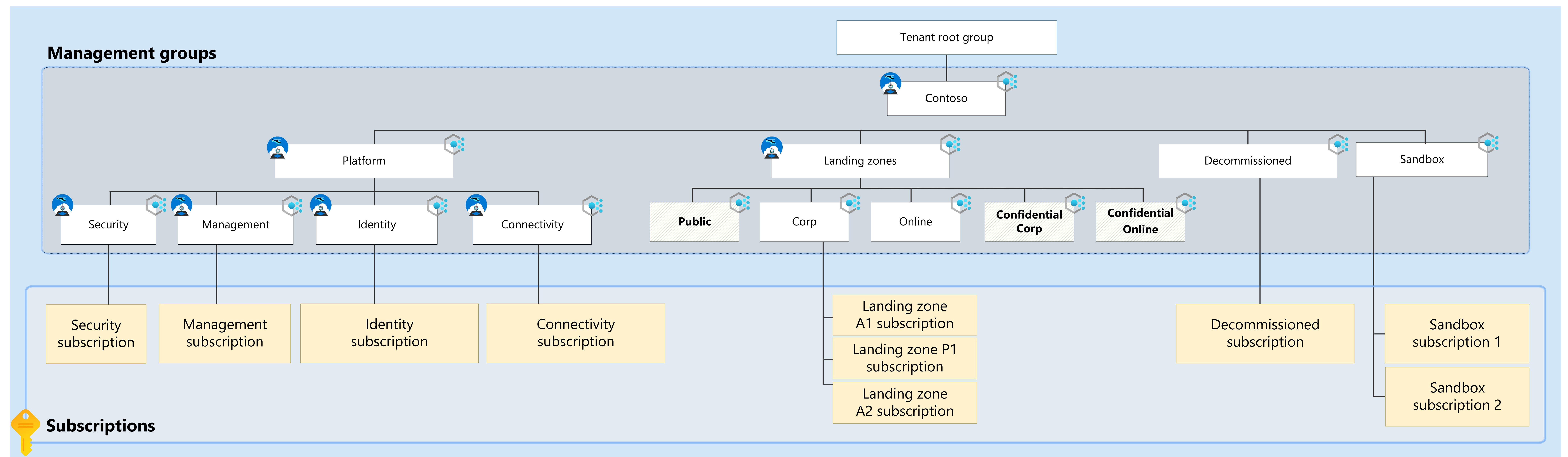






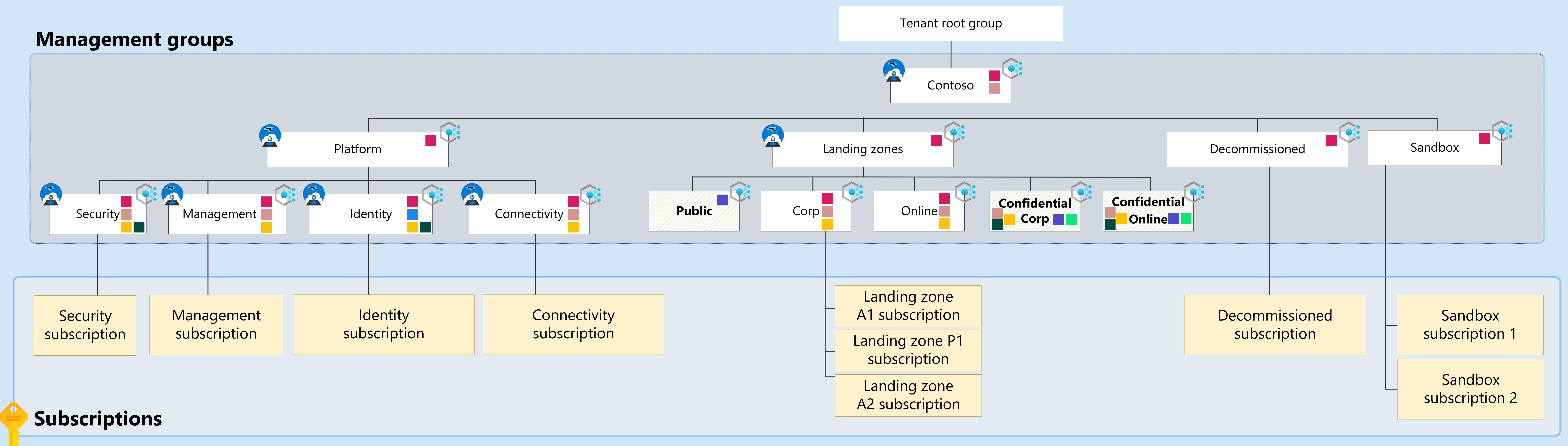


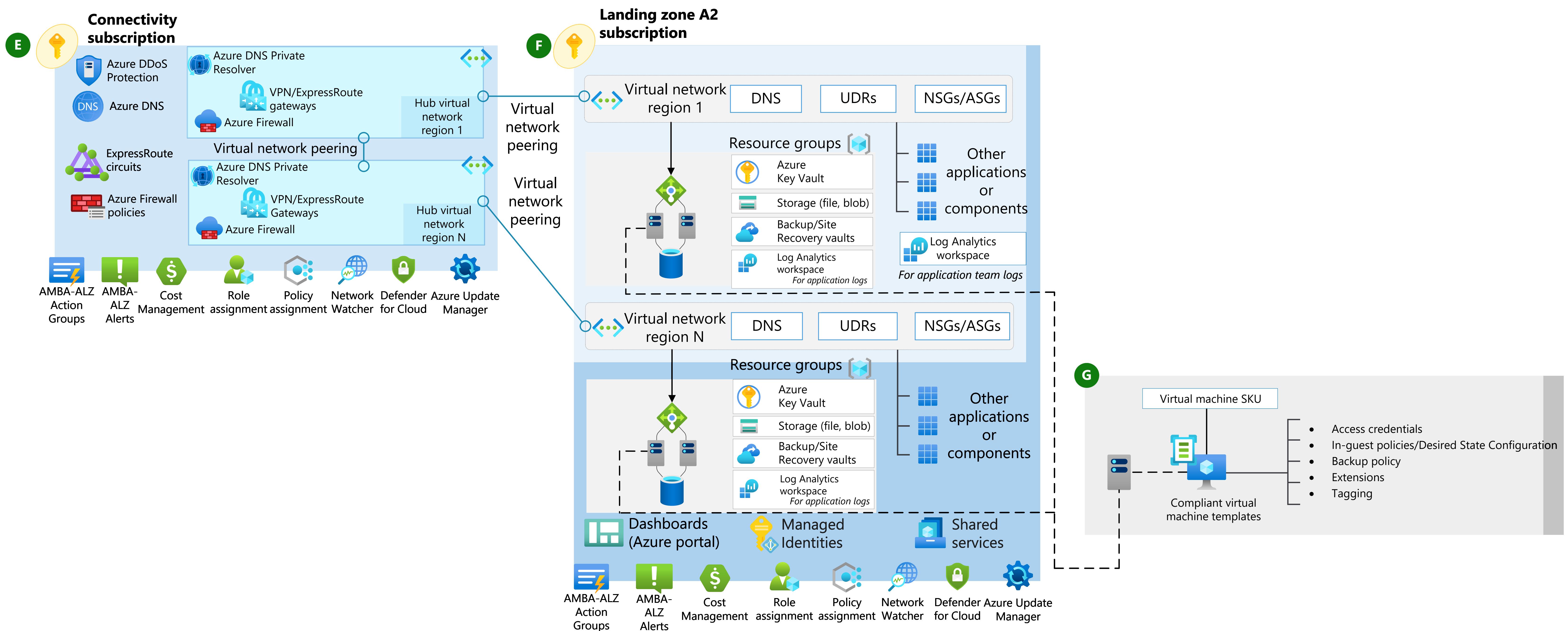


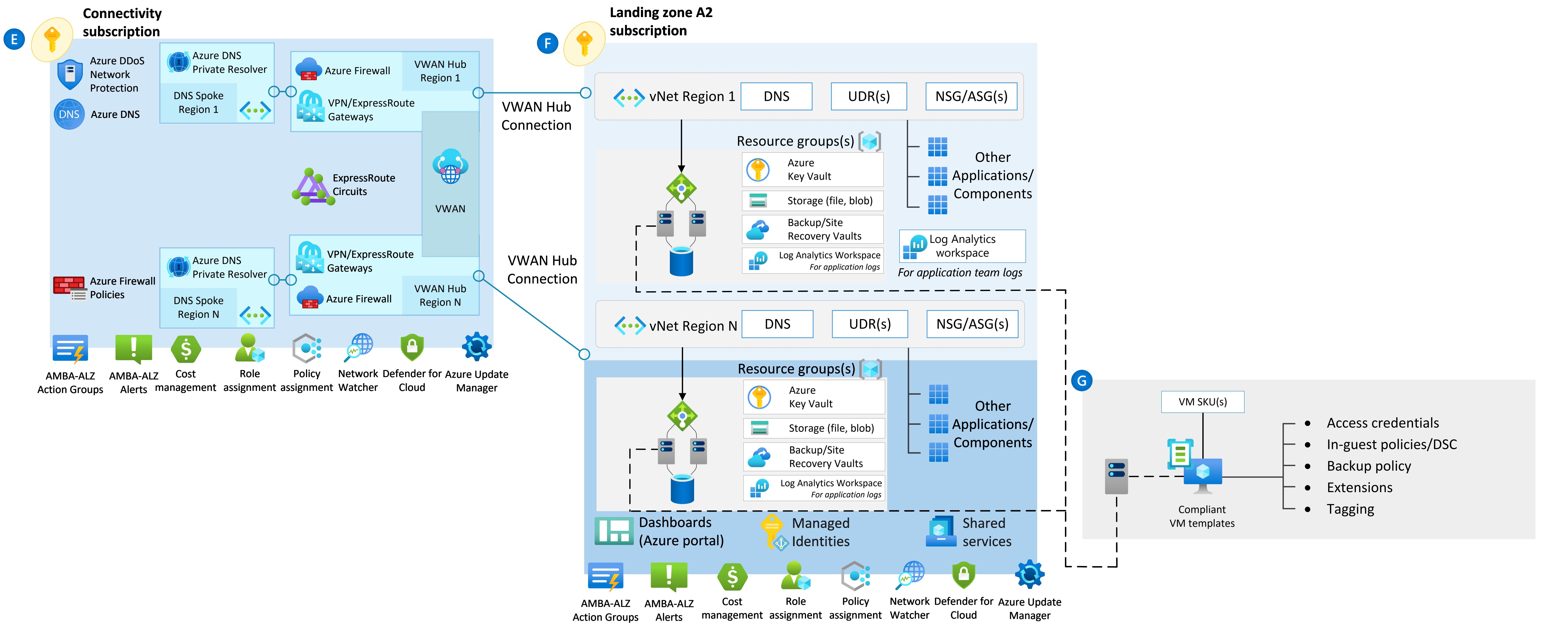


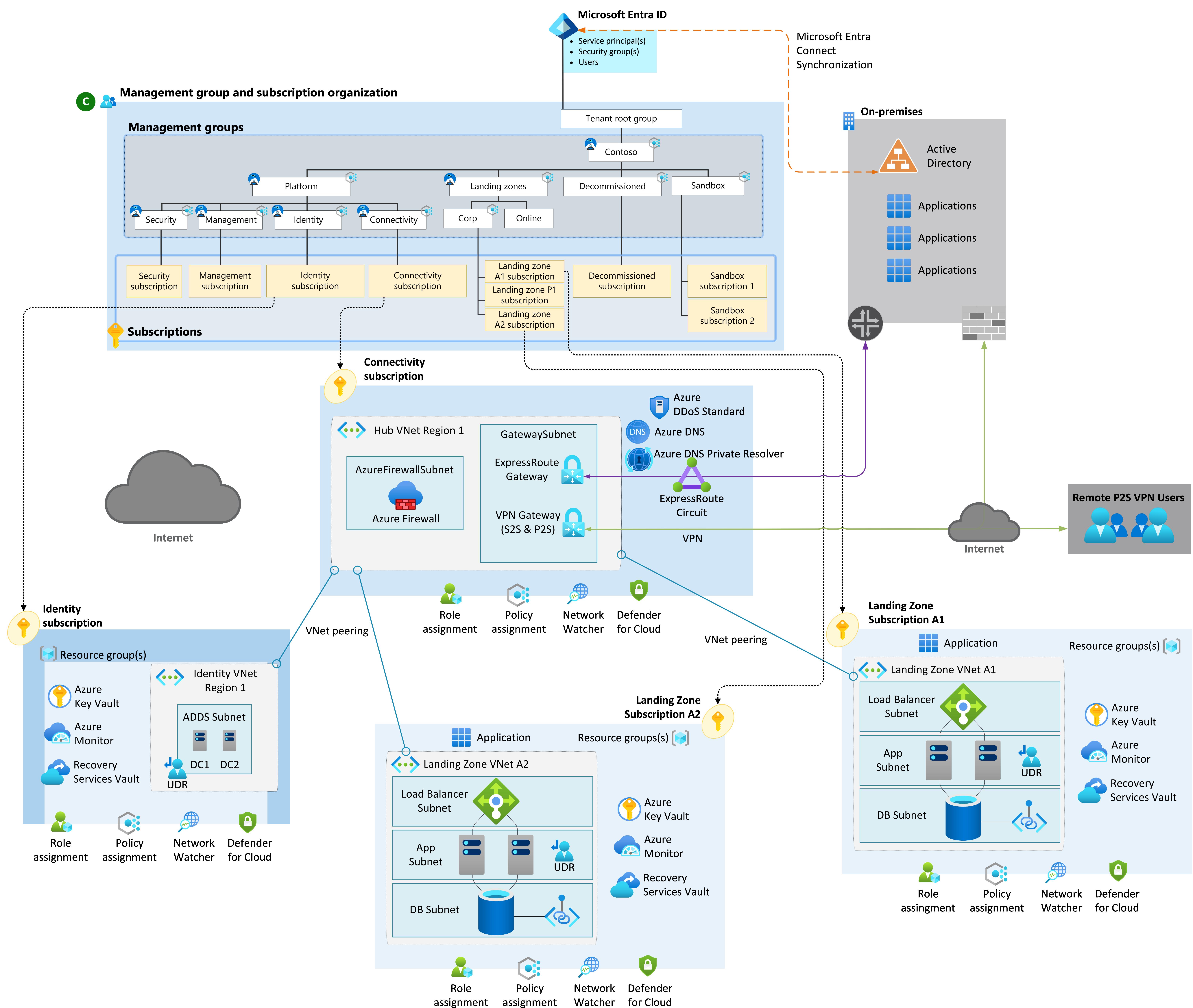
Key:

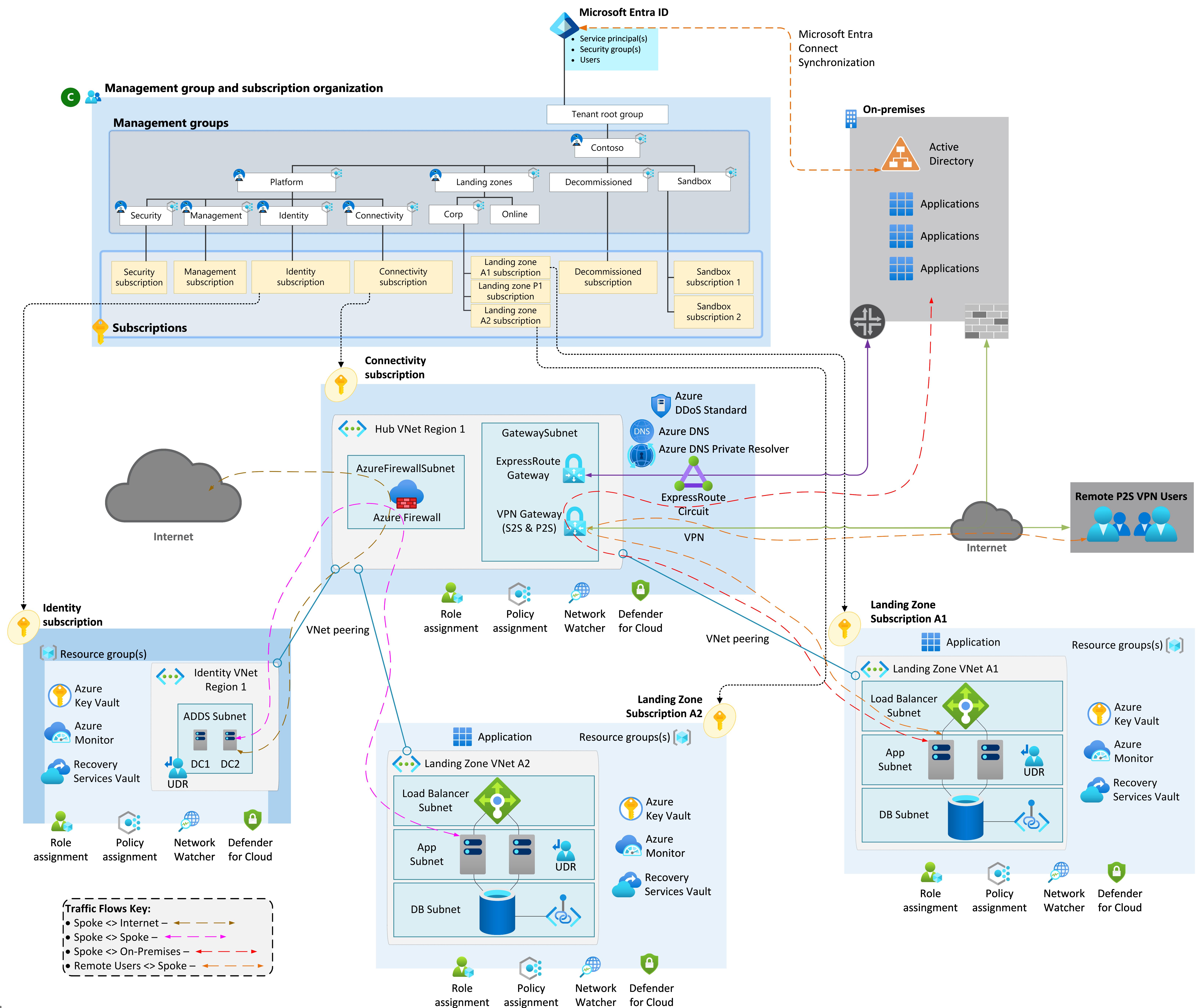
Level 1 – Data residency Region restrictions (allowed locations)	No public IPs on IaaS Public IPs can be created but not attached to IaaS, only PaaS
Level 1 – Data residency + global Region restrictions with exceptions for global services and resources, e.g. DNS Zones	No corp connectivity No Layer 3 (IP/Routing) connectivity to other Subscriptions, e.g. vNet Peering etc.
Level 2 – Encryption-at-rest/in-transit Customer Managed Keys (CMK), Hold Your Own Key (HYOK), TLS, VPN, IPsec, MACsec	
Level 3 – Encryption-in-use Azure Confidential Computing (ACC), Trusted Execution Environment (TEE), Attestation, Secure Key Release	Standard ALZ policies MCSB, MDFC, TLS, Diagnostic Settings, Availability Zones, Private Endpoints, Network security, Azure best practices, etc. <i>More details: aka.ms/ALZ/policies</i>

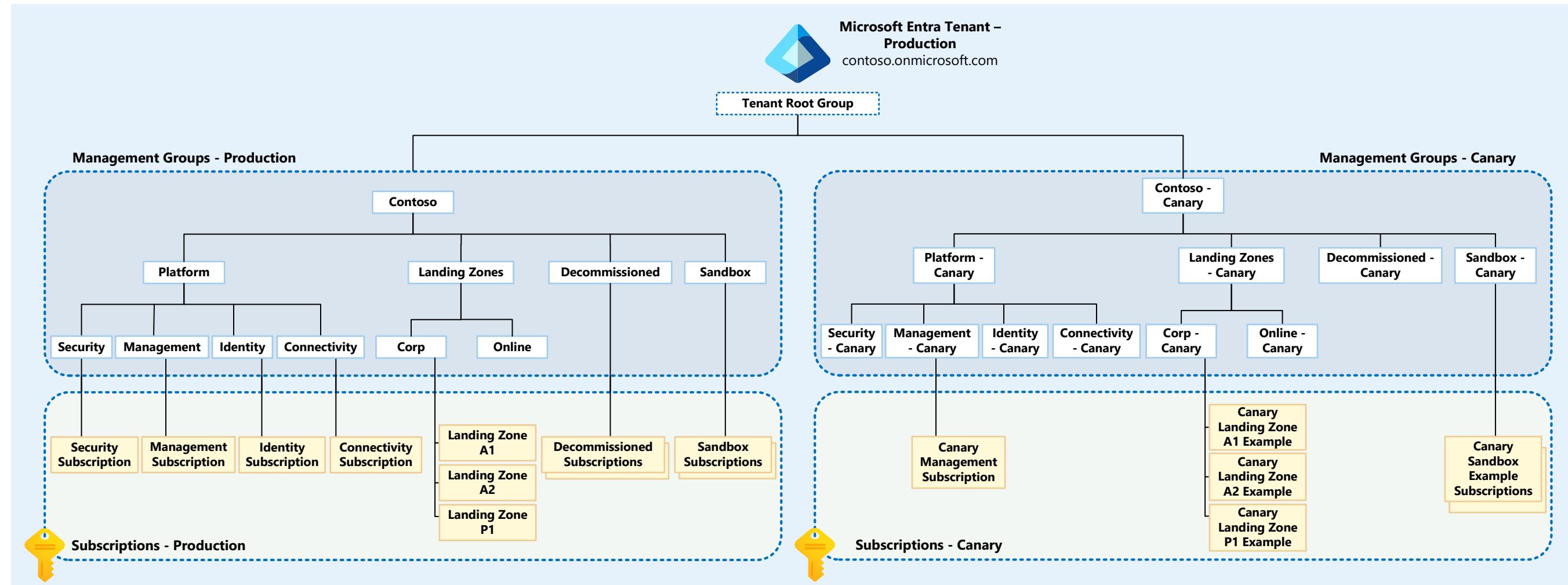
Management groups

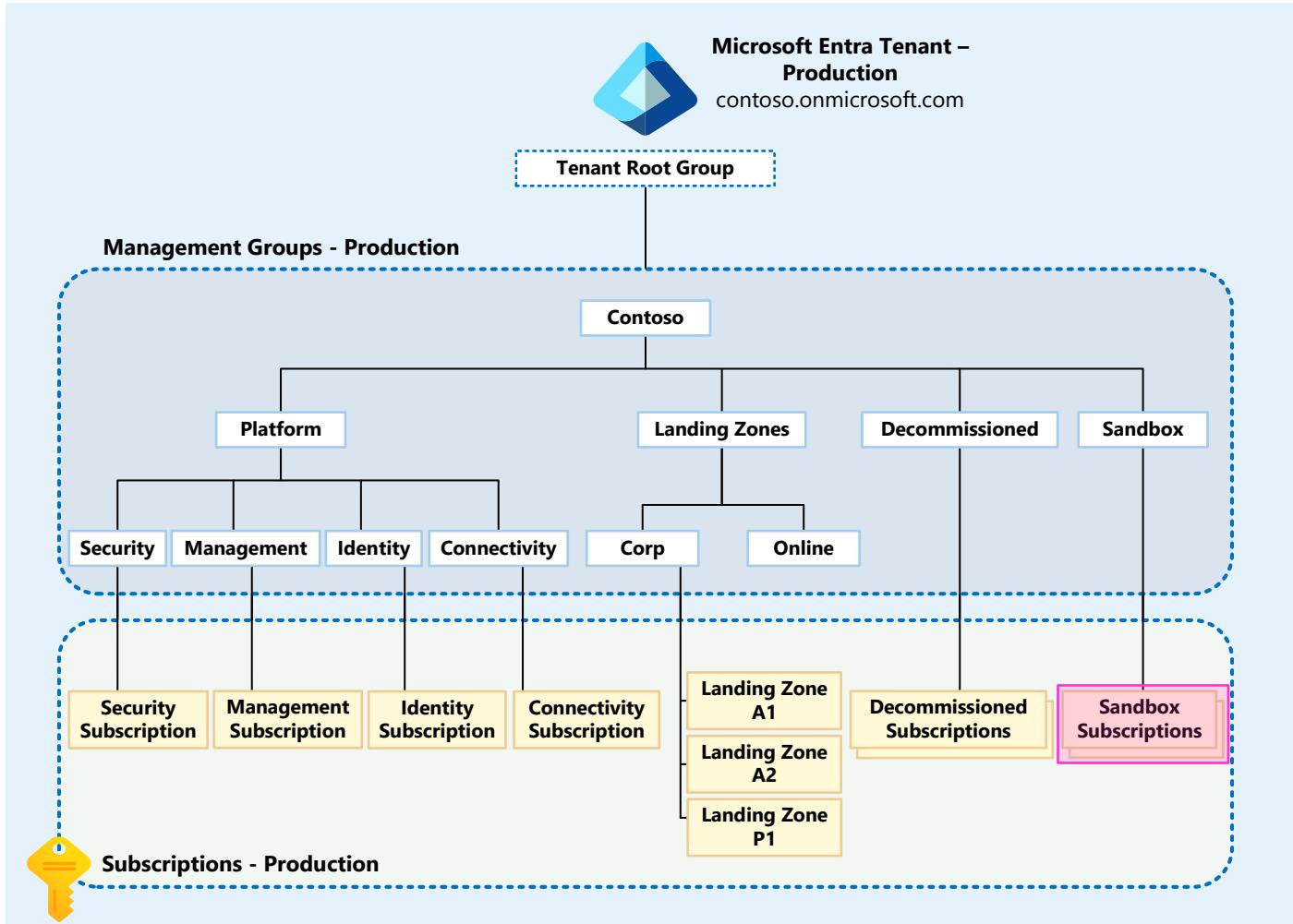


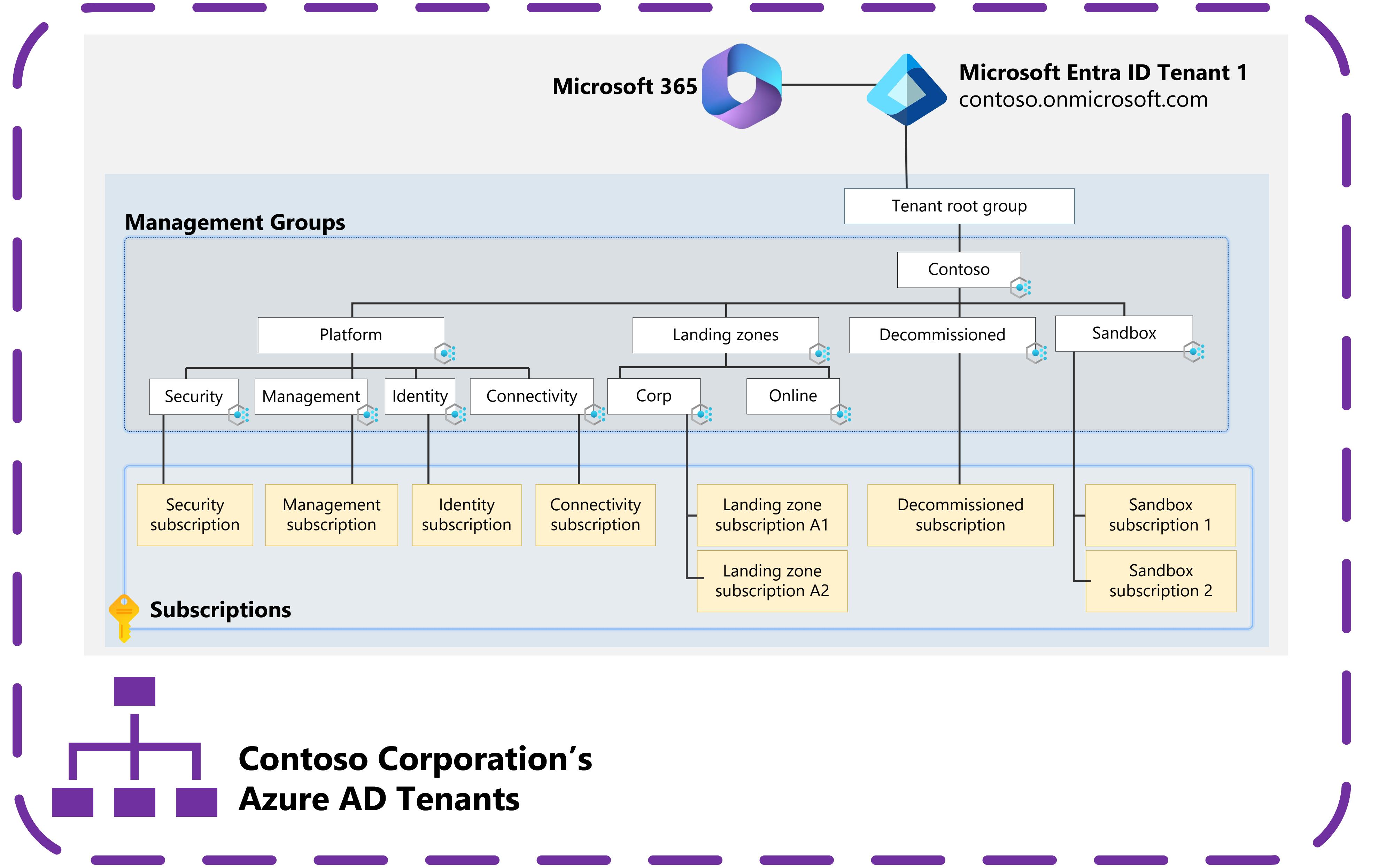


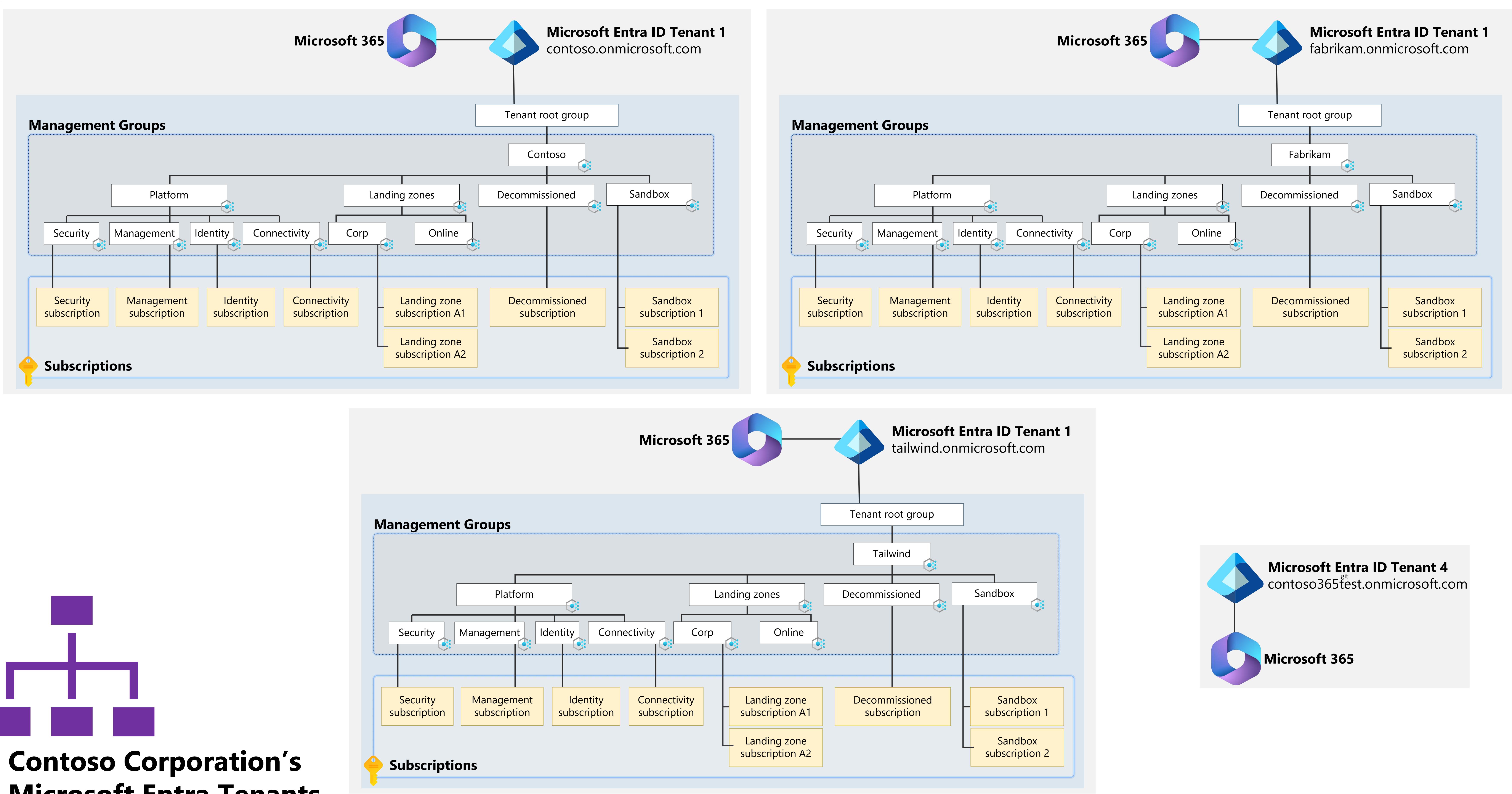





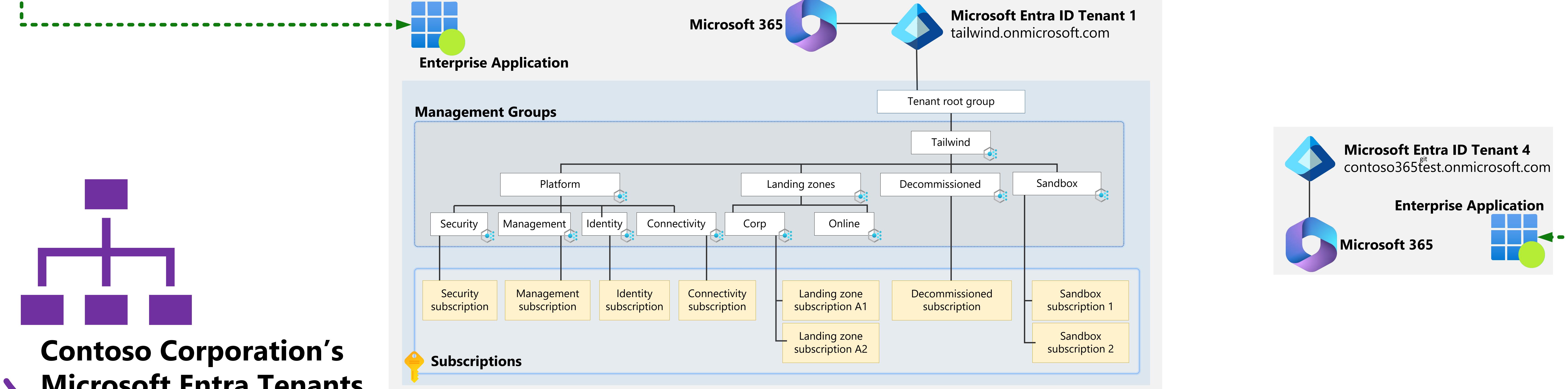
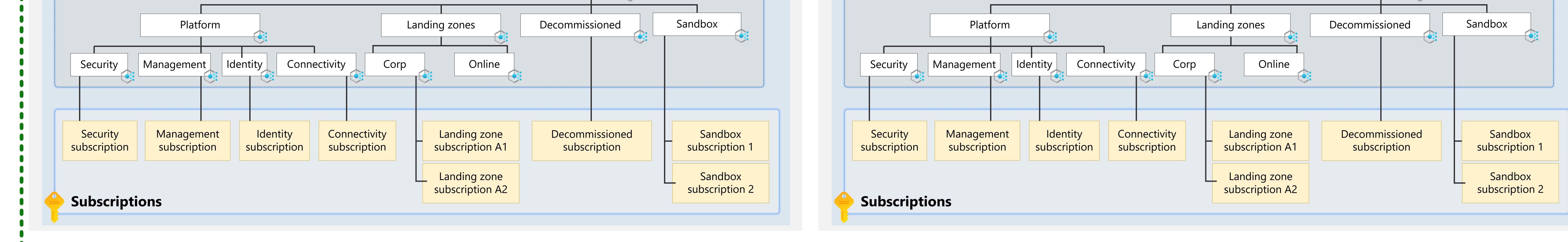




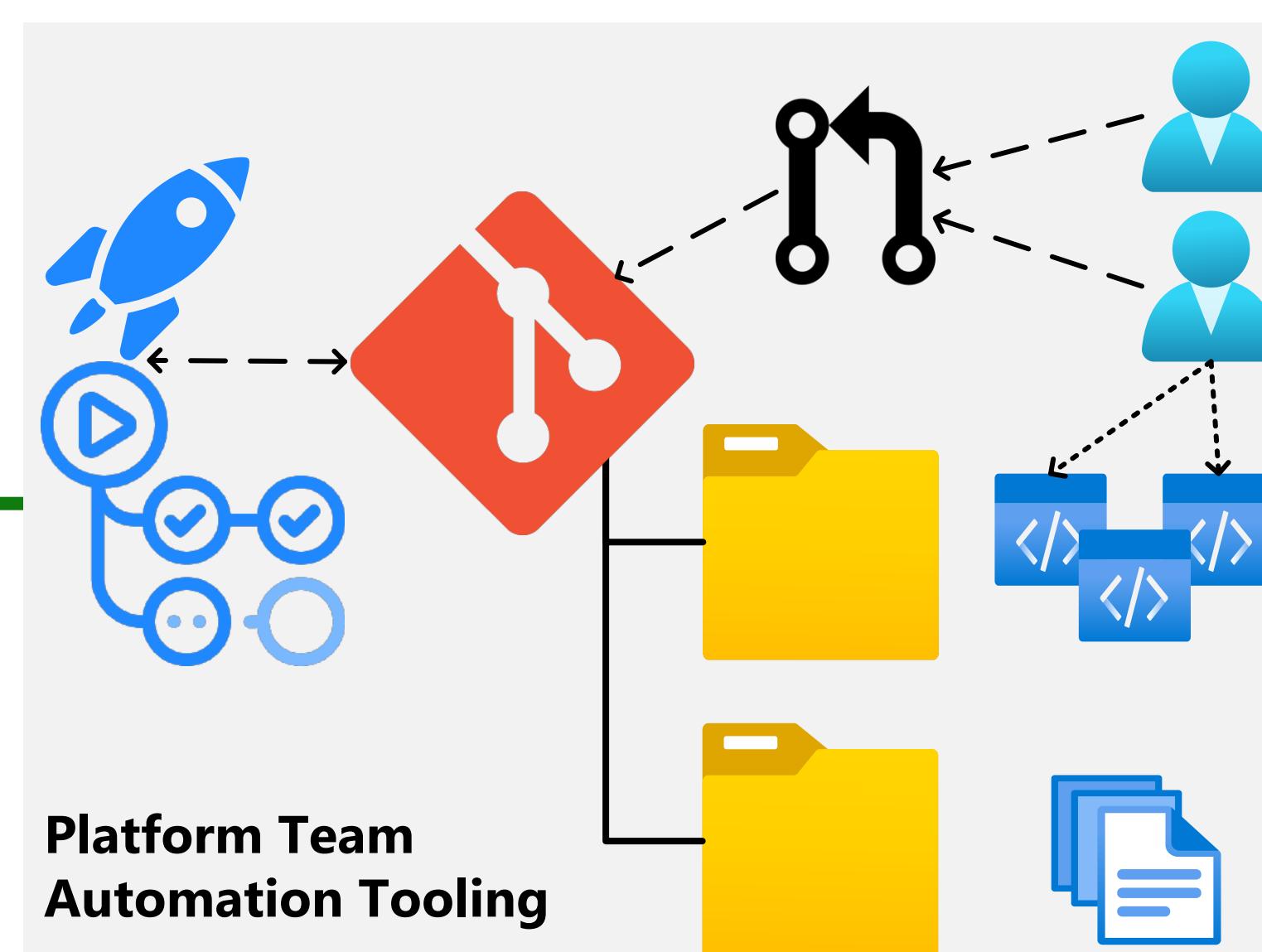








Contoso Corporation's Microsoft Entra Tenants



Contoso Corporation's Platform Automation Tooling

