FOR INSURANCE INDUSTRY

Azure Cloud Security Design

Azure Cloud Security Design for Insurance – Characteristics

- Multiple industry verticals
- High value client business assets in form of complex insurance policies
- Subject to numerous regulations in compliance and privacy protection, varied from industry to industry
- Owner cloud assets are embedded with trade secrets, proprietary know-what and know-how, of which on one-hand, being constantly developed and accessible by authorized employees, and on the other, susceptible to data loss
- High availability real time operation is important but not as critical as it is for some other industries such as manufacturing, utilities, and retail businesses
- Growth demand for computing power and data storage is high

Azure Cloud Security Design for Insurance – Priorities

- Access Control with adequate security without compromising efficiency
- Data Protection
- Data Loss Prevention

Azure Cloud Security Design for Insurance – Design Principles

- Design for self-healing and a high degree of error and failure tolerance
- Make all things redundant – avoid single-point of failure
- Minimize coordination – provide all required services and scalability with right subscriptions but not over-providing
- Partition around limits to minimize the cost
- Design for operation by maximizing use of all Azure native monitoring and logging tools
- Use managed services by leveraging more with PaaS/SaaS and less with IaaS when and where applicable
- Choose right and not best storage options for applications
- Design for evolution with CI/CD pipelines
- Design must be justified by business needs. Business needs must be in line with enterprise business goals
- Design should take geo-distribution of business verticals into account

Azure Cloud Security Design for Insurance – Design Principles

- The afore-mentioned design principles matter in security
- Following those design principles helps reduce risk exposure and enhance security

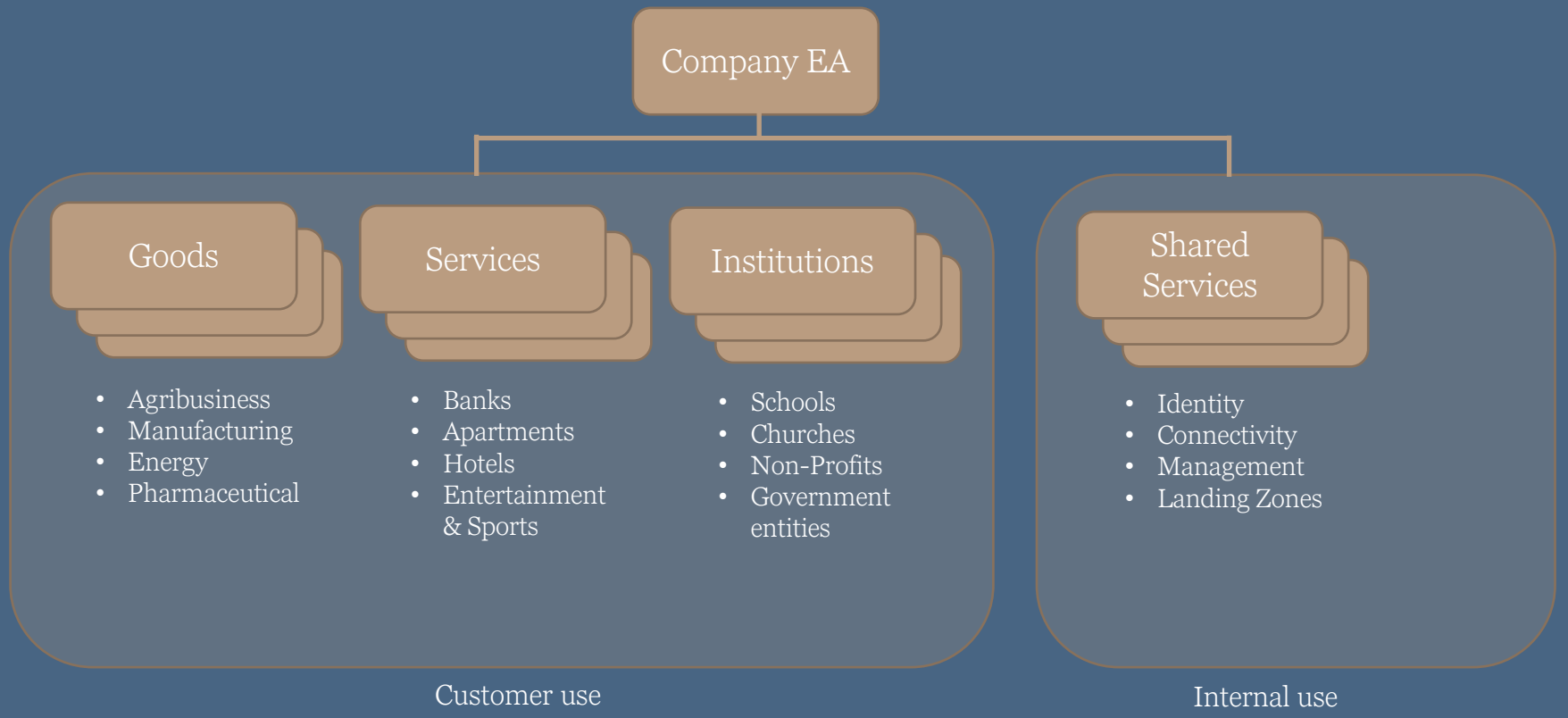
Azure Cloud Security Design for Insurance – Design Features

- Hybrid – Certain assets that must reside and operate on-prem
- Dedicated connectivity – ExpressRoutes
- Microservices and containerization
- Data Loss Prevention – Azure Virtual Desktop for internal use
- CASB and the like for customer-facing applications and external use

Design Components

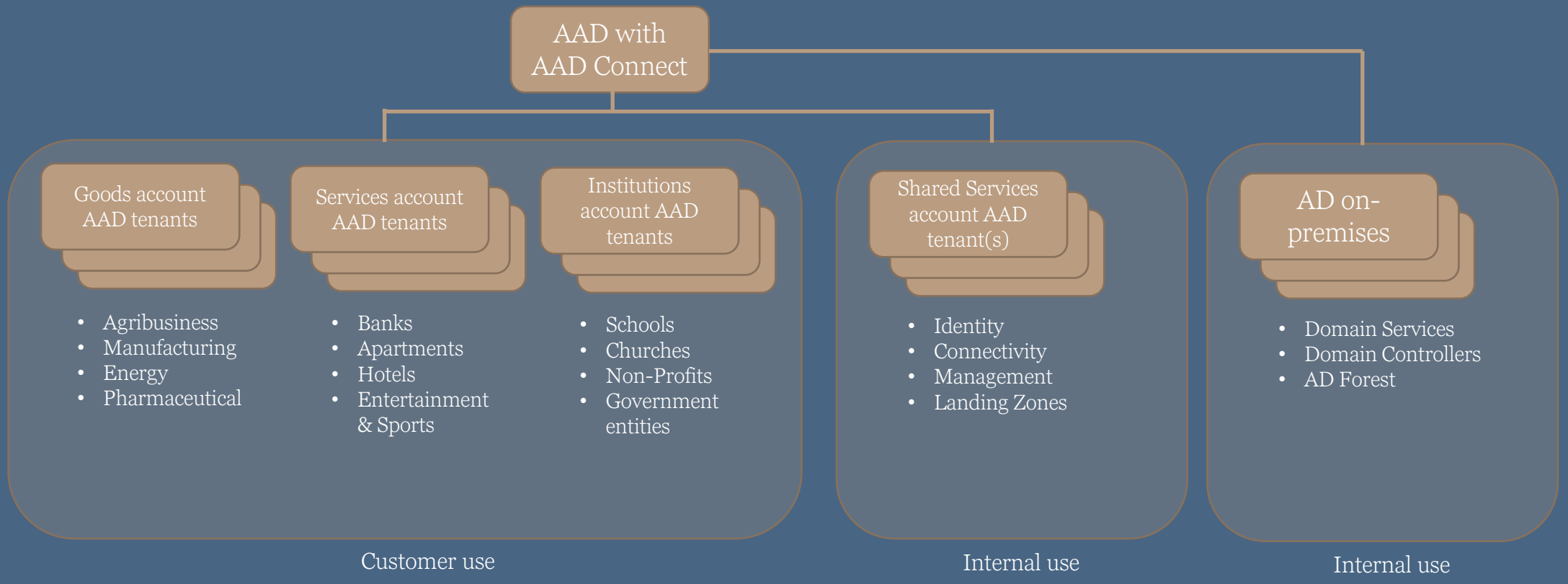
- Enterprise Agreement Enrollment
- Azure Active Directory (AAD) and On-premises Active Directory (AD) integration
- Management Groups and Landing Zones
- Multi-region ExpressRoutes coverage for insurance verticals
- Azure Defender for Cloud

Design Component – Enterprise Agreement Enrollment



EA is hierarchical, it includes accounts; accounts have subscriptions. EA serves two main purposes: Cost management and Azure support

Design Component – Azure Active Directory (AAD)



An account may have one or more AAD tenants. Each tenant has an instance of AAD. AAD can be synchronized with on-premises AD by AAD Connect for Single Sign-On (SSO). In Customer Use space, AAD B2C is used to better handle external identities. Each AAD instance is linked with subscription(s) that provide adequate entitlements to serve the tenant. AAD is part of Microsoft Entra

Design Component – Landing Zones (ALZ)

- ALZ standardizes all tenants
- ALZ automates tenant foundation build
- ALZ is implemented with multiple Infrastructure as Code (IaC) tools

  Bicep

  Terraform

  Blueprints

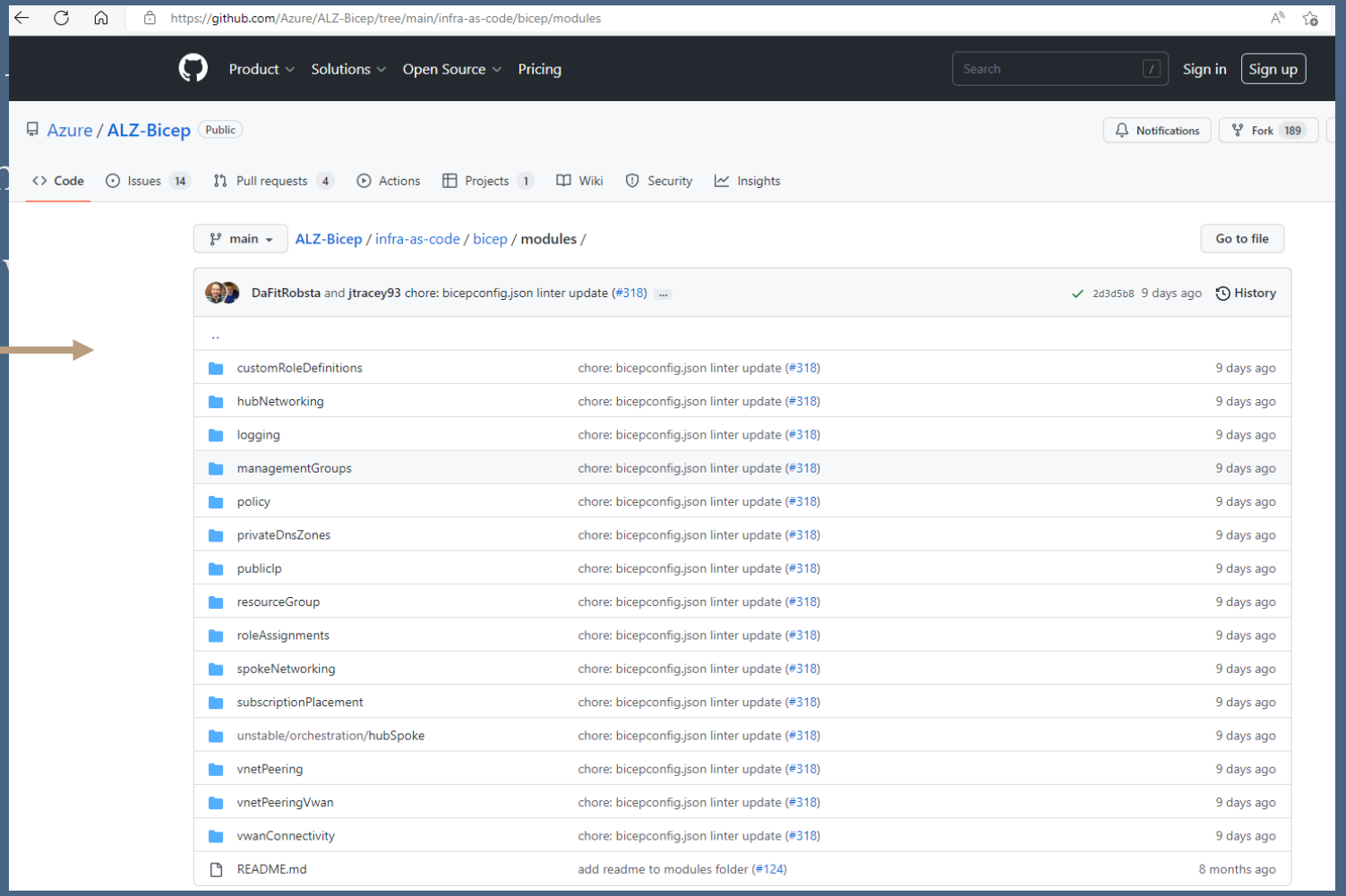
  Azure CLI

  Azure PowerShell

ALZ builds infrastructure foundation in each tenant in accordance with cloud architectural design goals

Design Component – Landing Zones (ALZ)

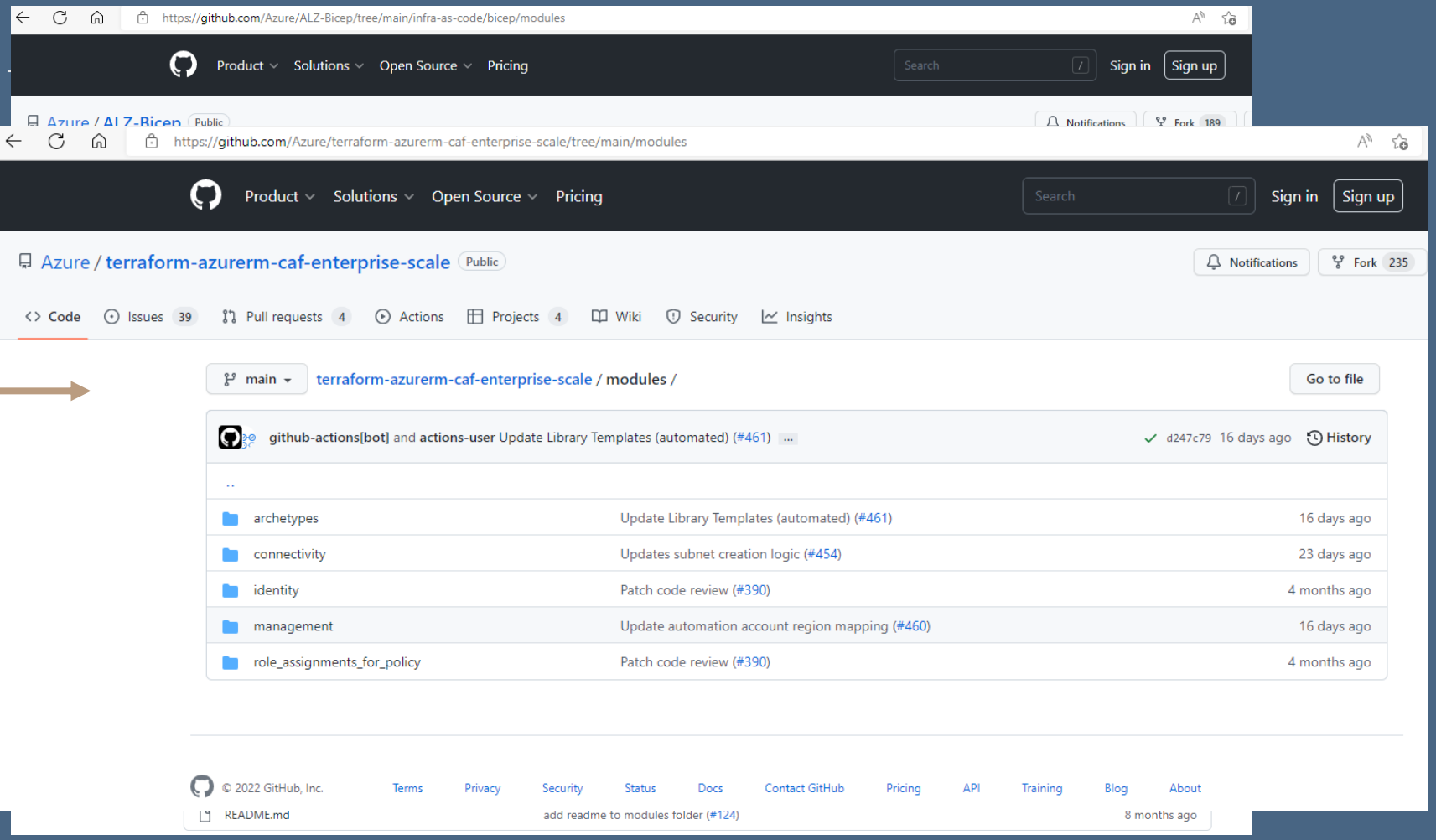
- ALZ standardizes all
- ALZ automates tenan
- ALZ is implemented
  - *Bicep*
  - *Terraform*
  - *Blueprints*
  - *Azure CLI*
  - *Azure PowerShell*



ALZ builds infrastructure foundation in each tenant in accordance with cloud architectural design goals

Design Component – Landing Zones (ALZ)

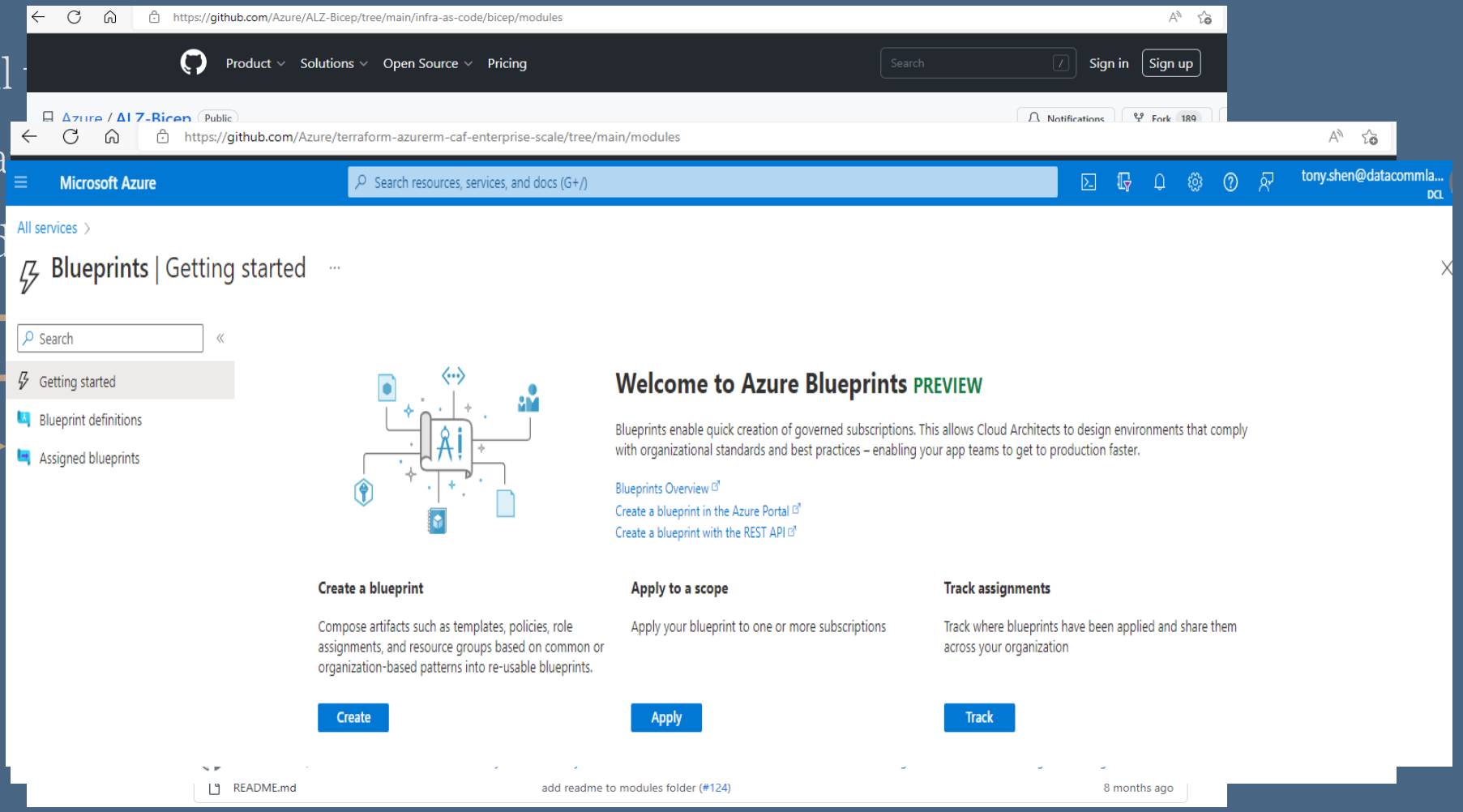
- ALZ standardizes all
- ALZ automates tena
- ALZ is implemented
  - *Bicep*
  - *Terraform*
  - *Blueprints*
  - *Azure CLI*
  - *Azure PowerShell*



ALZ builds infrastructure foundation in each tenant in accordance with cloud architectural design goals

Design Component – Landing Zones (ALZ)

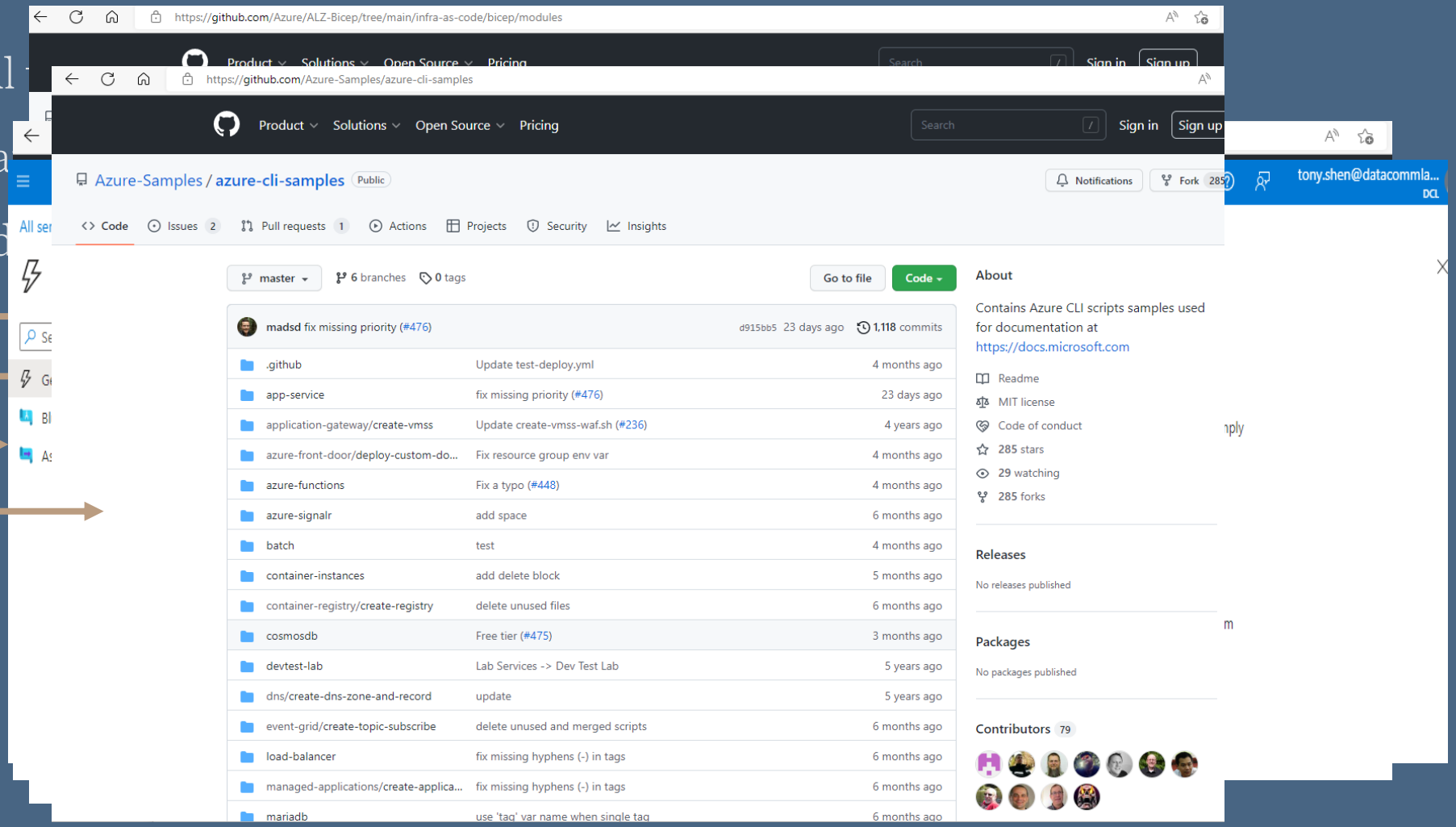
- ALZ standardizes all
- ALZ automates tena
- ALZ is implemented
  - *Bicep*
  - *Terraform*
  - *Blueprints*
  - *Azure CLI*
  - *Azure PowerShell*



ALZ builds infrastructure foundation in each tenant in accordance with cloud architectural design goals

Design Component – Landing Zones (ALZ)

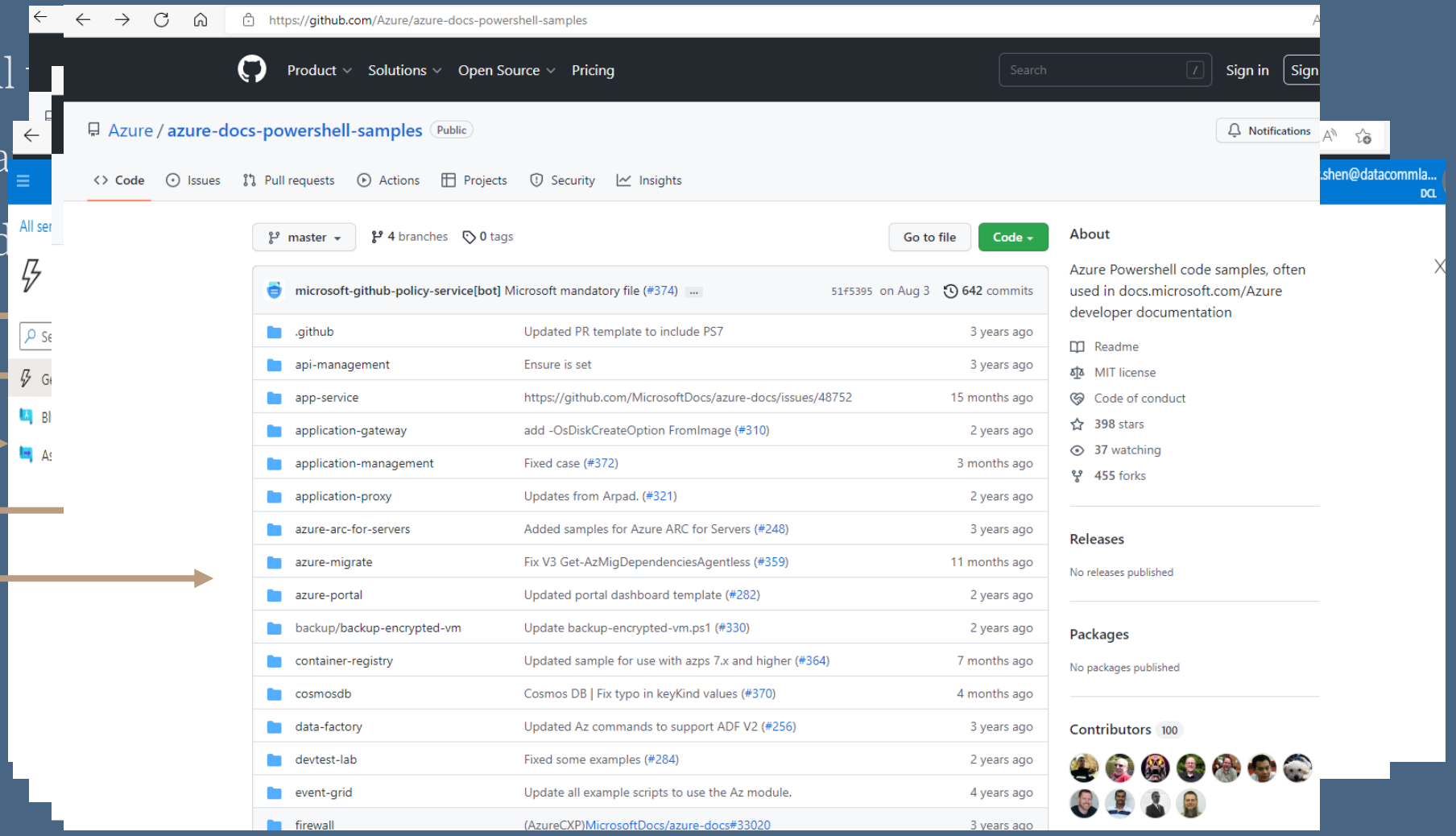
- ALZ standardizes all
- ALZ automates tena
- ALZ is implemented
  - *Bicep*
  - *Terraform*
  - *Blueprints*
  - *Azure CLI*
  - *Azure PowerShell*



ALZ builds infrastructure foundation in each tenant in accordance with cloud architectural design goals

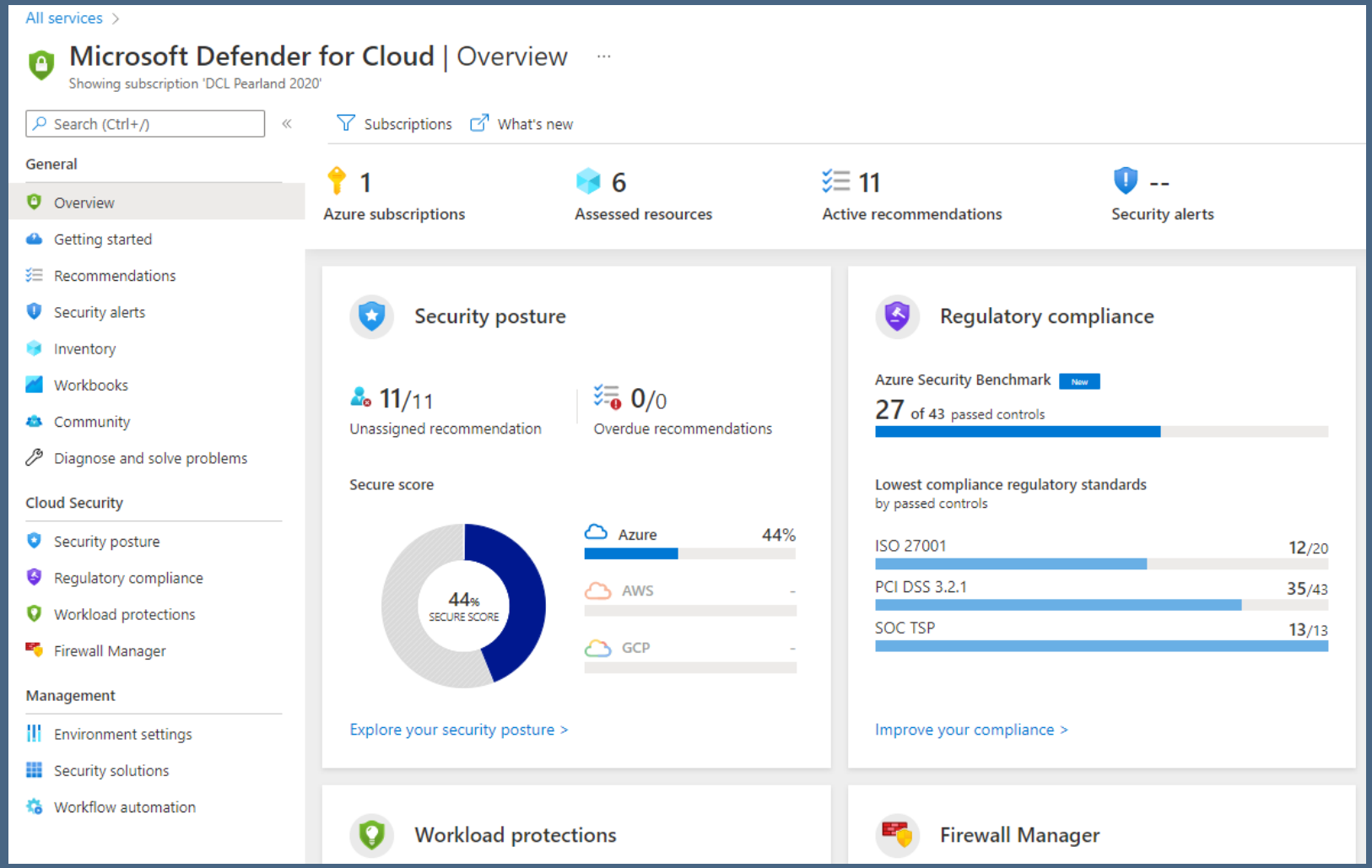
Design Component – Landing Zones (ALZ)

- ALZ standardizes all
- ALZ automates tena
- ALZ is implemented
  - *Bicep*
  - *Terraform*
  - *Blueprints*
  - *Azure CLI*
  - *Azure PowerShell*



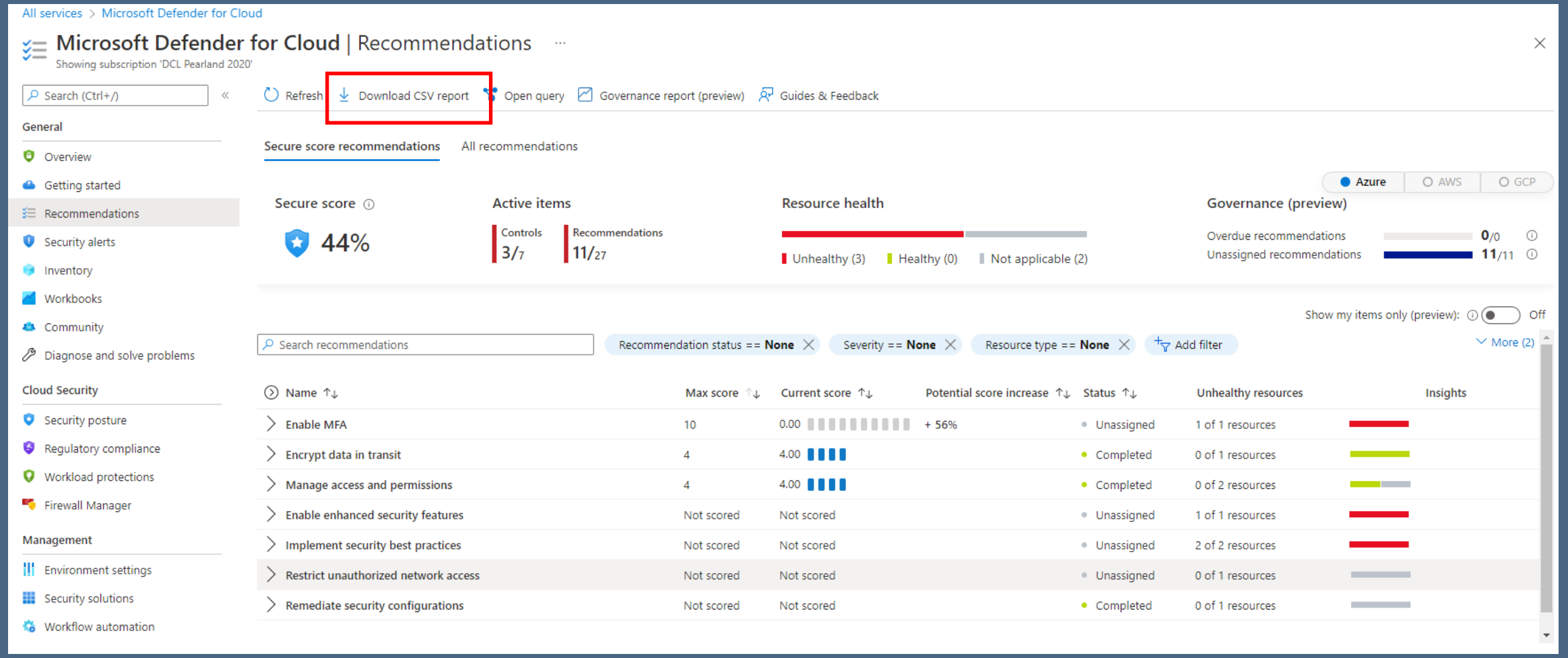
ALZ builds infrastructure foundation in each tenant in accordance with cloud architectural design goals

Design Component – Defender for Cloud



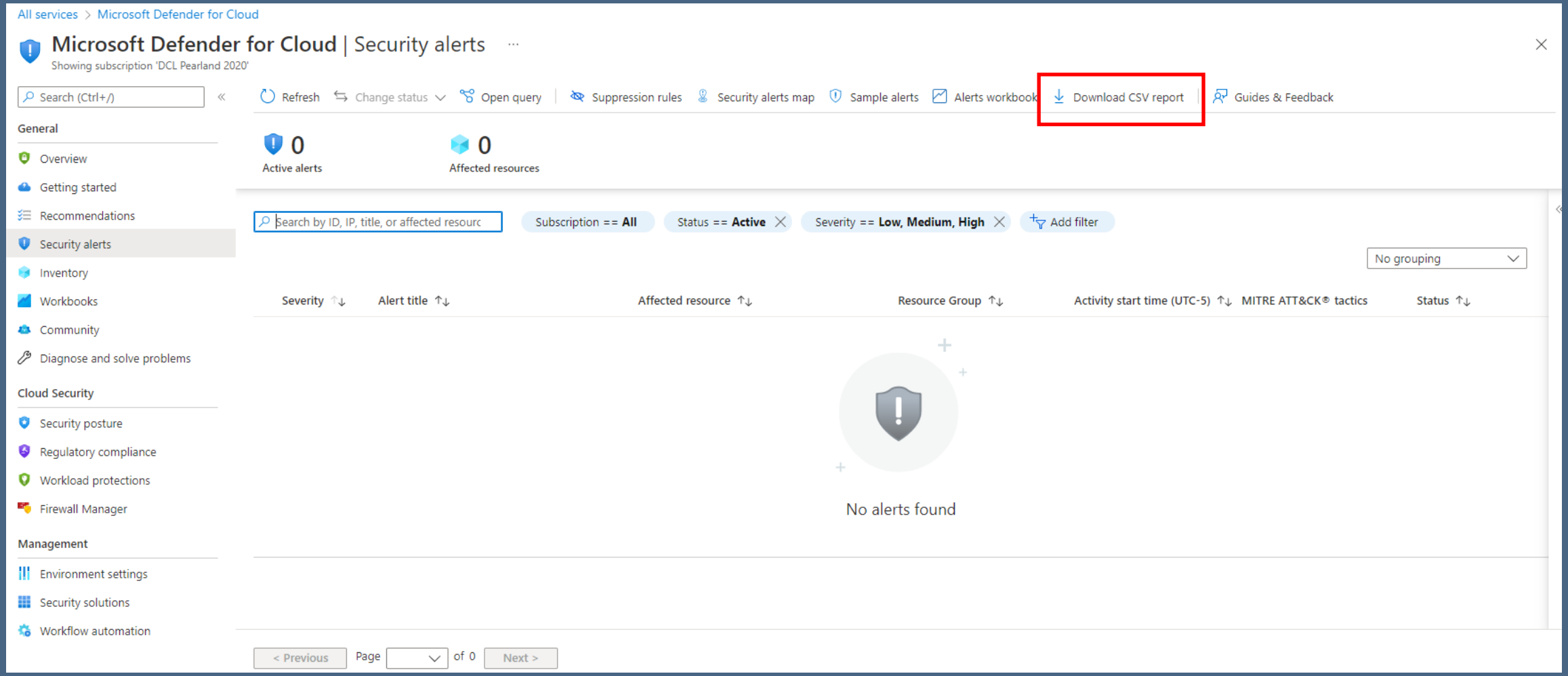
Defender for cloud portal - Overview

Design Component – Defender for Cloud



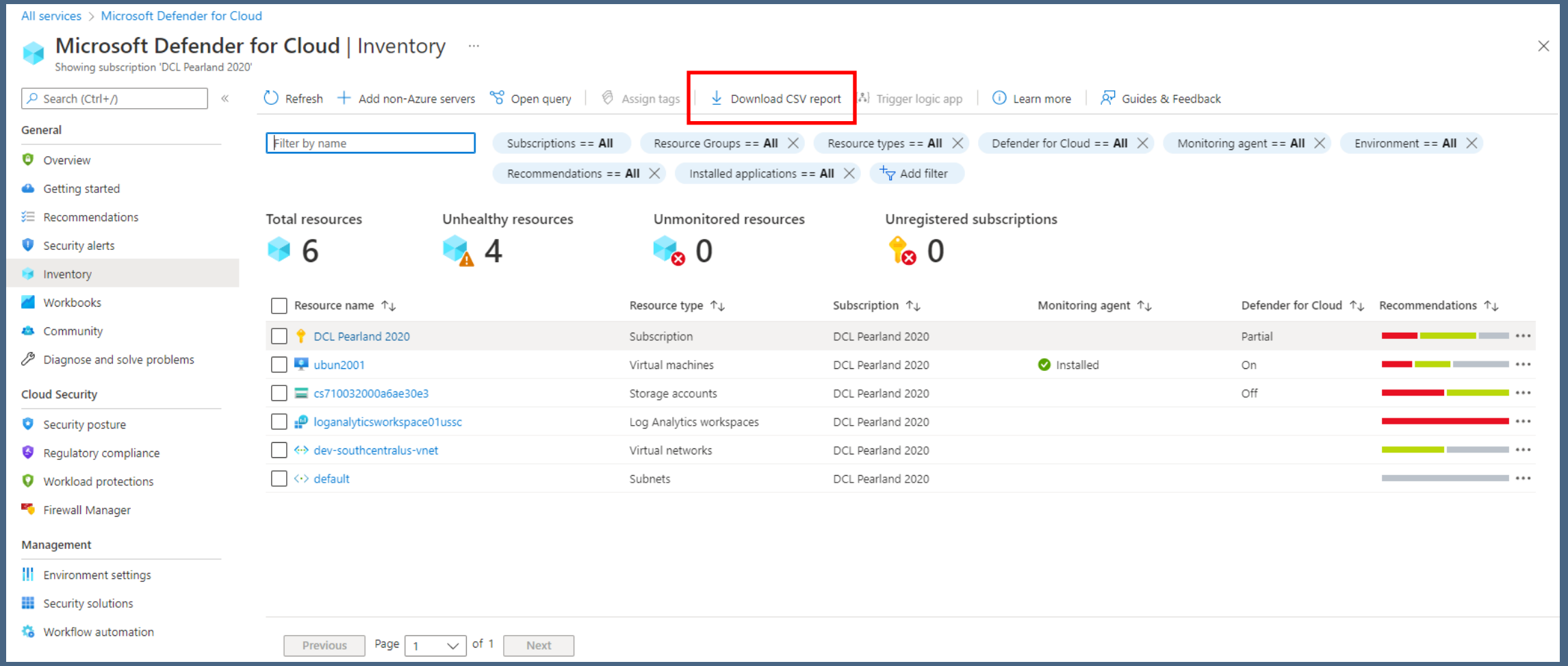
Defender for cloud portal – Recommendations (CSV report download is available)

Design Component – Defender for Cloud



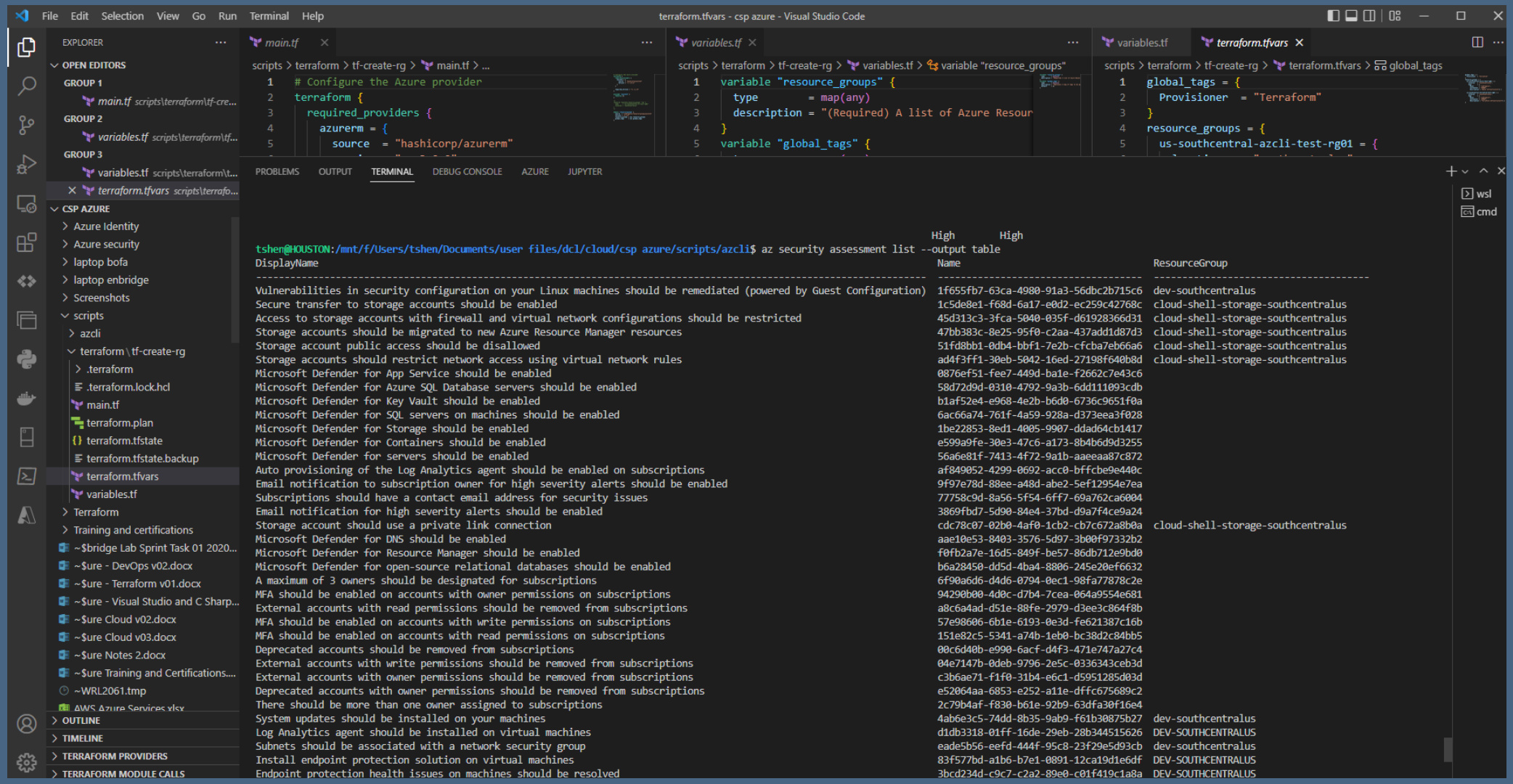
Defender for cloud portal – Alerts (CSV report download is available)

Design Component – Defender for Cloud



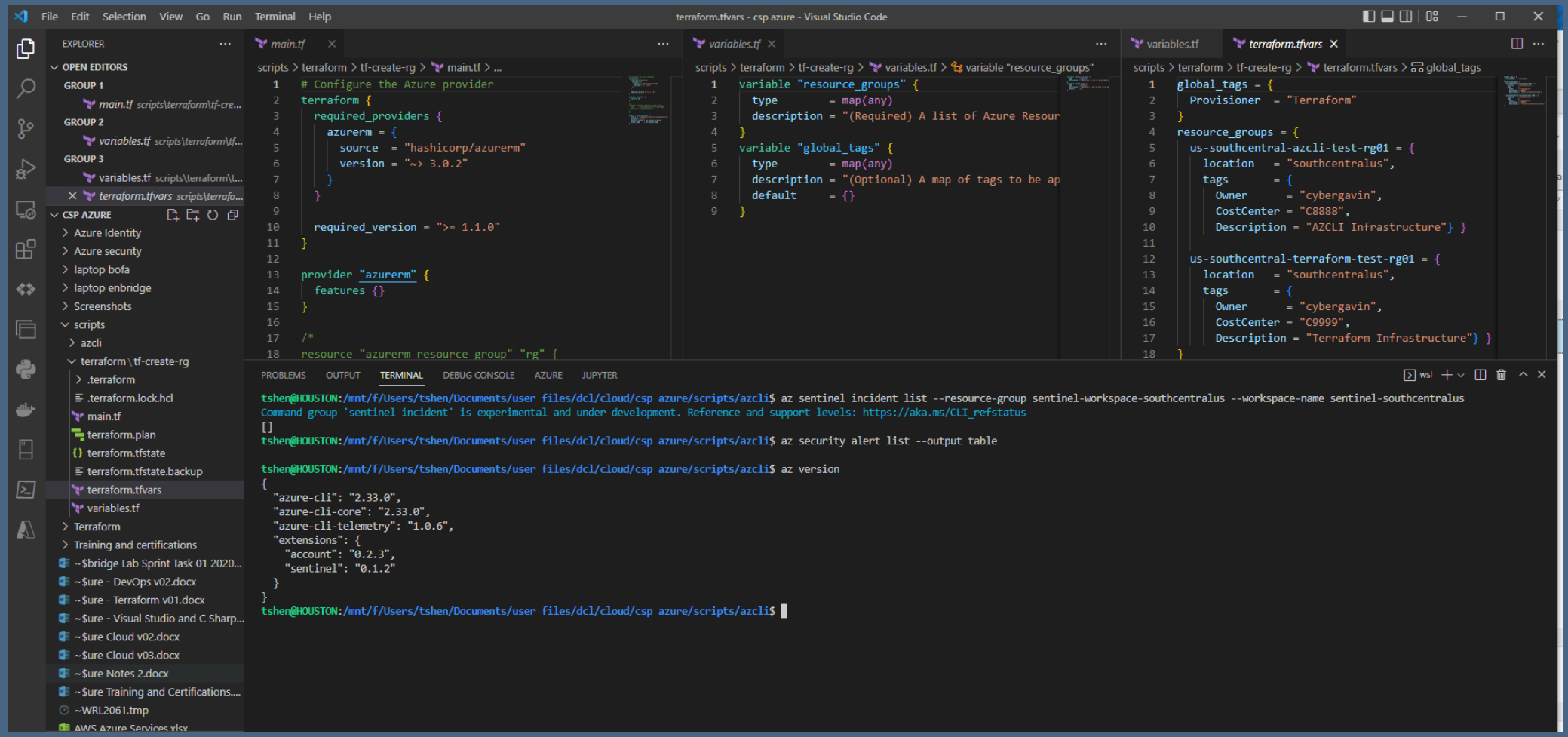
Defender for cloud portal – Inventory (CSV report download is available)

Design Component – Defender for Cloud



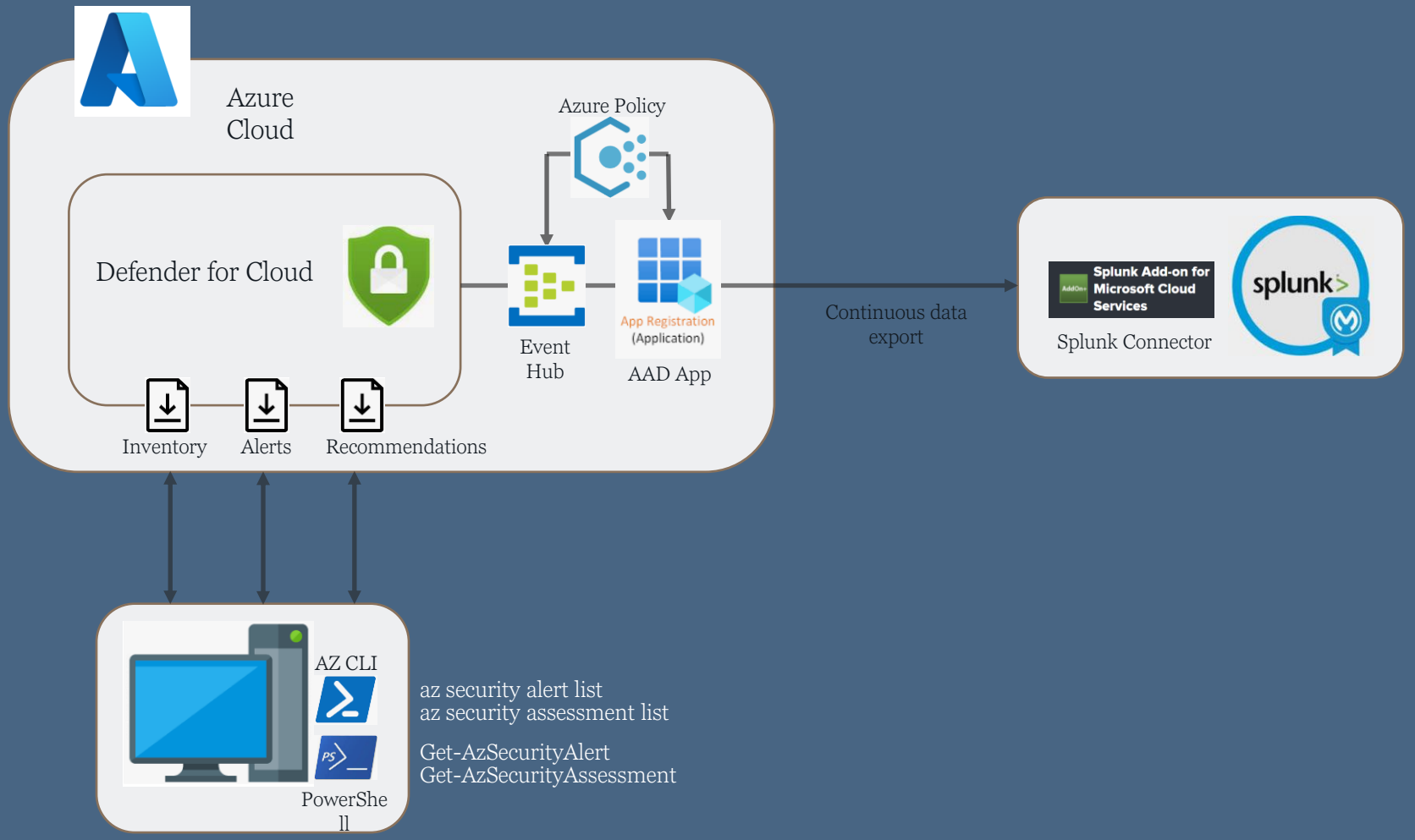
Azure CLI – How to query recommendations

Design Component – Defender for Cloud

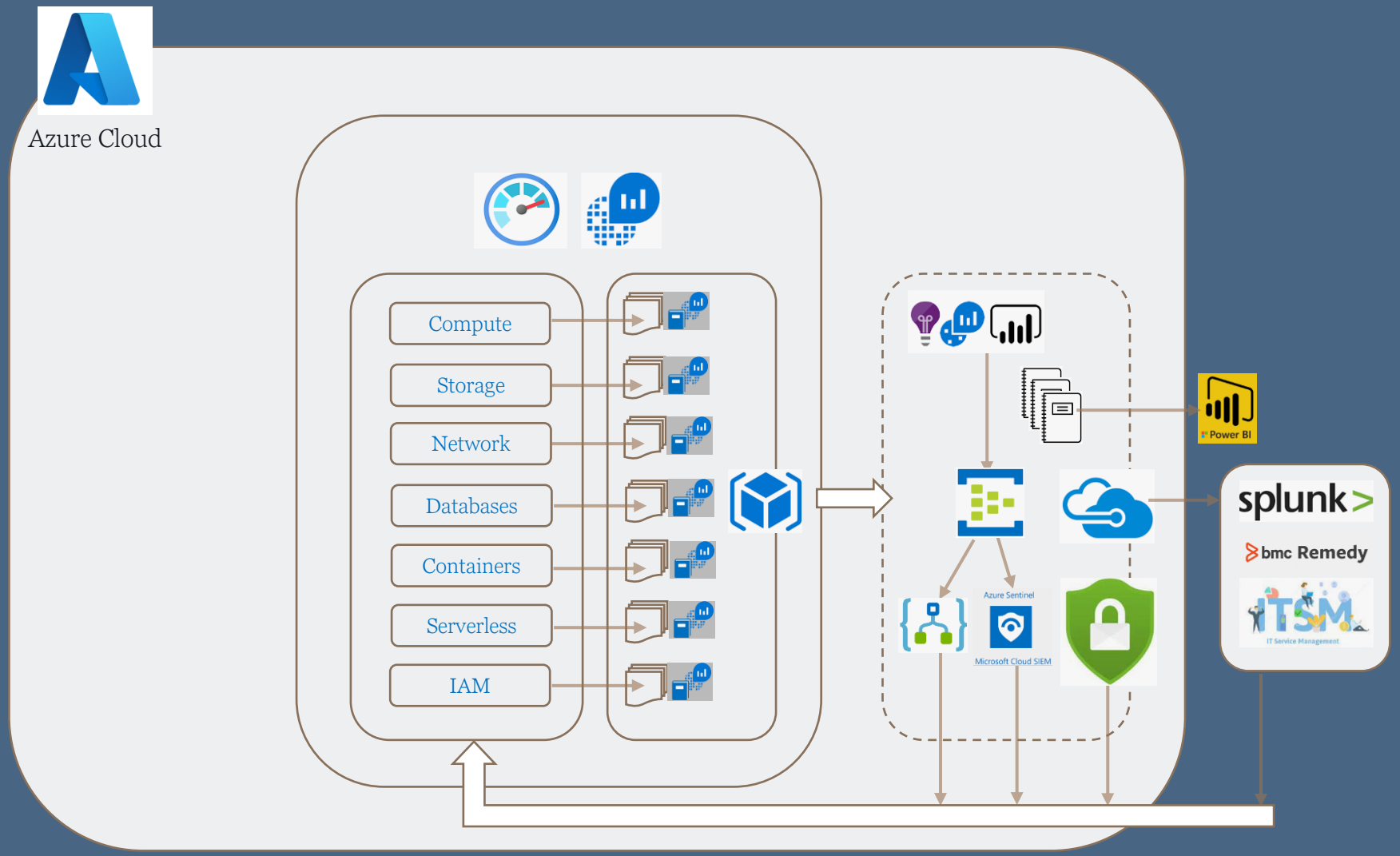


Azure CLI – How to query alerts

Design Component – Defender for Cloud

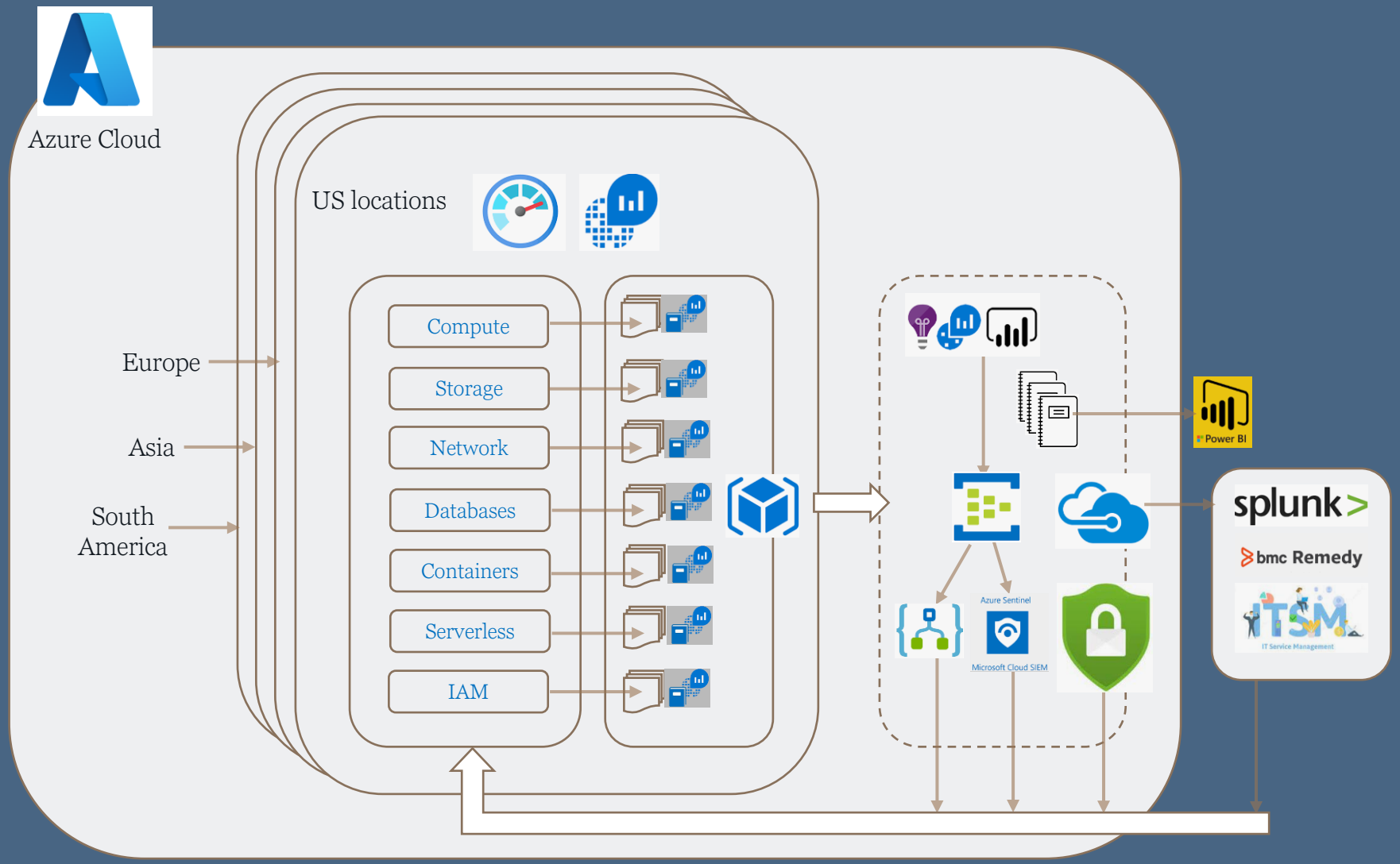


Design Component – Defender for Cloud



Defender for Cloud provides a single pane of glass for security management and more

Design Component – Defender for Cloud



Defender for Cloud provides a single pane of glass for security management and more

Design Component – Defender for Cloud

DFC in free mode →

Defender for Cloud is offered in two modes:

- **Without enhanced security features** (Free) - Defender for Cloud is enabled for free on all your Azure subscriptions when you visit the workload protection dashboard in the Azure portal for the first time, or if enabled programmatically via API. Using this free mode provides the secure score and its related features: security policy, continuous security assessment, and actionable security recommendations to help you protect your Azure resources.

- **Defender for Cloud with all enhanced security features** - Enabling enhanced security extends the capabilities of the free mode to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. Some of the major benefits include:

Design Component – Defender for Cloud

DFC in non-free mode or enhanced mode with all enhanced security features available

- **Microsoft Defender for Endpoint** - Microsoft Defender for Servers includes Microsoft Defender for Endpoint for comprehensive endpoint detection and response (EDR). Learn more about the benefits of using Microsoft Defender for Endpoint together with Defender for Cloud in Use Defender for Cloud's integrated EDR solution.
- **Vulnerability assessment for virtual machines, container registries, and SQL resources** - Easily enable vulnerability assessment solutions to discover, manage, and resolve vulnerabilities. View, investigate, and remediate the findings directly from within Defender for Cloud.
- **Multicloud security** - Connect your accounts from Amazon Web Services (AWS) and Google Cloud Platform (GCP) to protect resources and workloads on those platforms with a range of Microsoft Defender for Cloud security features.
- **Hybrid security** – Get a unified view of security across all of your on-premises and cloud workloads. Apply security policies and continuously assess the security of your hybrid cloud workloads to ensure compliance with security standards. Collect, search, and analyze security data from multiple sources, including firewalls and other partner solutions.
- **Threat protection alerts** - Advanced behavioral analytics and the Microsoft Intelligent Security Graph provide an edge over evolving cyber-attacks. Built-in behavioral analytics and machine learning can identify attacks and zero-day exploits. Monitor networks, machines, data stores (SQL servers hosted inside and outside Azure, Azure SQL databases, Azure SQL Managed Instance, and Azure Storage) and cloud services for incoming attacks and post-breach activity. Streamline investigation with interactive tools and contextual threat intelligence.

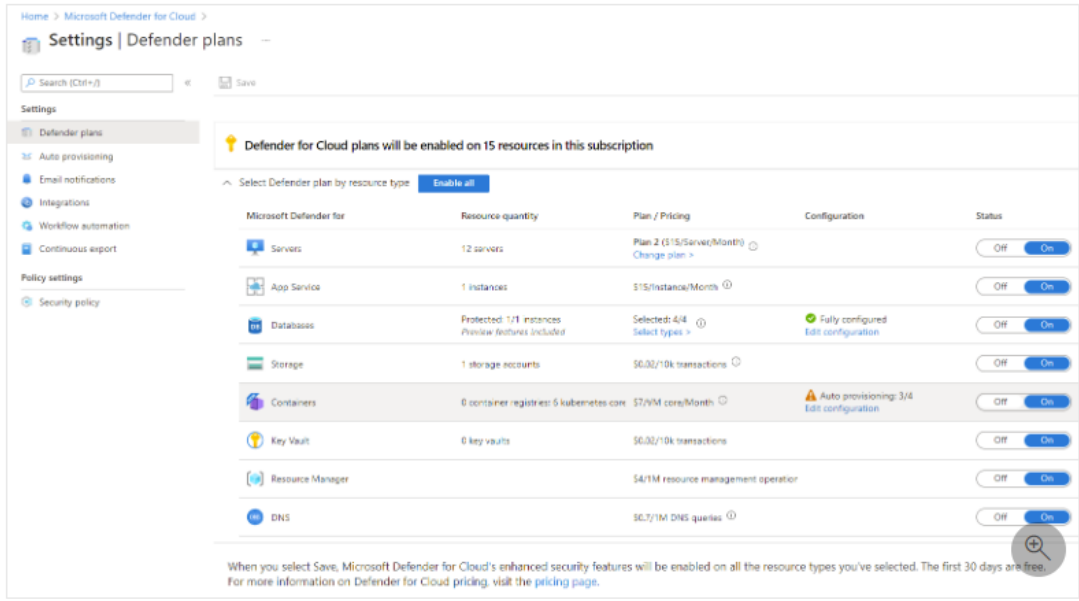
Design Component – Defender for Cloud

Enable enhanced security features

Enable enhanced security features on your subscriptions and workspaces:

- To enable enhanced security features on one subscription:

  1. From Defender for Cloud's main menu, select **Environment settings**.
  2. Select the subscription or workspace that you want to protect.
  3. Select **Enable all** to upgrade.
  4. Select **Save**.

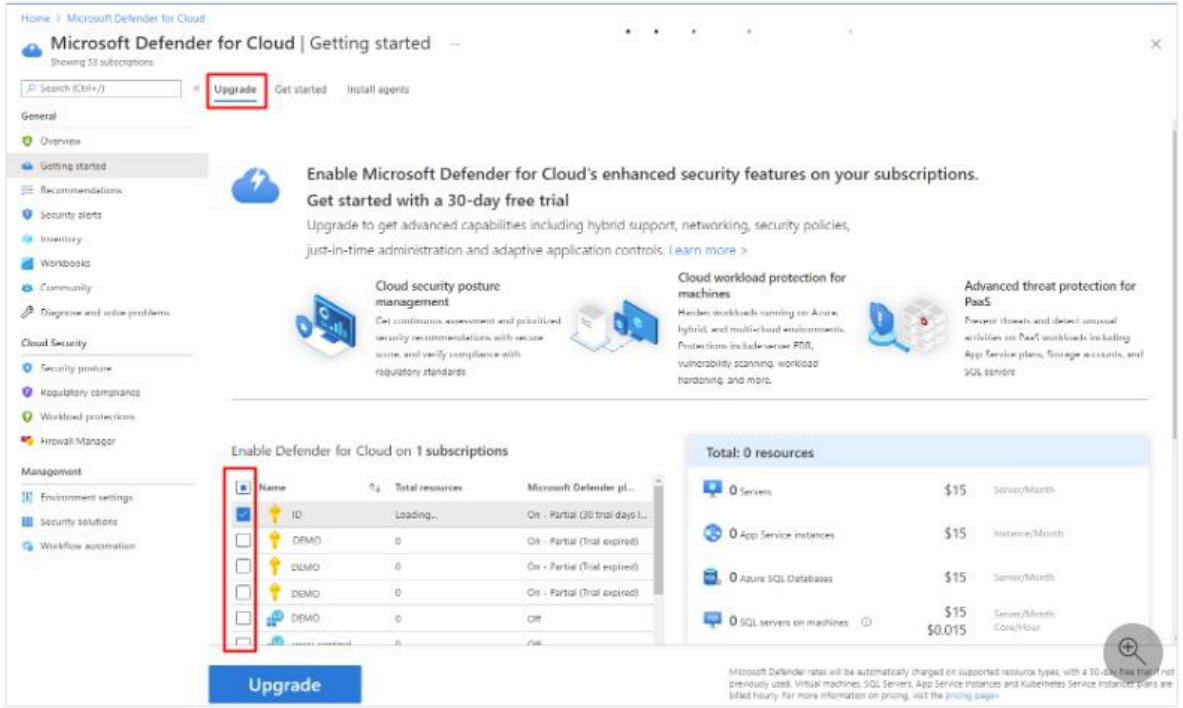


Design Component – Defender for Cloud

Enable enhanced security features

1. From Defender for Cloud's menu, select **Getting started**.

The **Upgrade** tab lists subscriptions and workspaces eligible for onboarding.

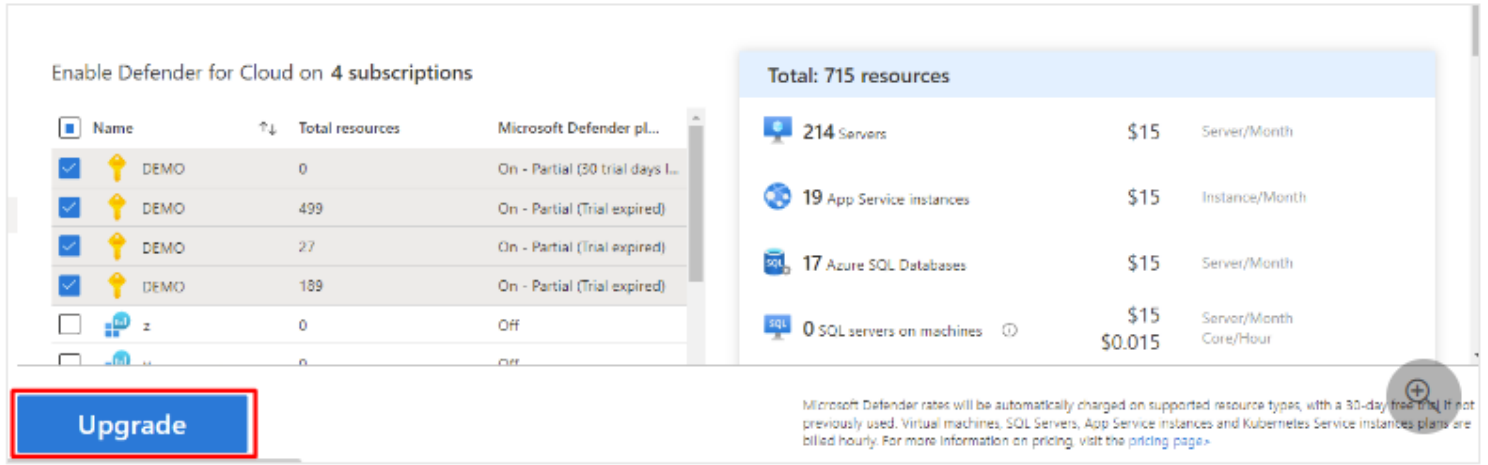


Design Component – Defender for Cloud

Enable enhanced security features

2. From the **Select subscriptions and workspaces to protect with Microsoft Defender for Cloud** list, select the subscriptions and workspaces to upgrade and select **Upgrade** to enable all Microsoft Defender for Cloud security features.

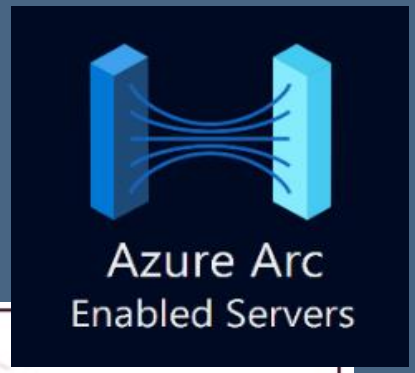
   - If you select subscriptions and workspaces that aren't eligible for trial, the next step will upgrade them and charges will begin.
   - If you select a workspace that's eligible for a free trial, the next step will begin a trial.



Design Component – Defender for Cloud

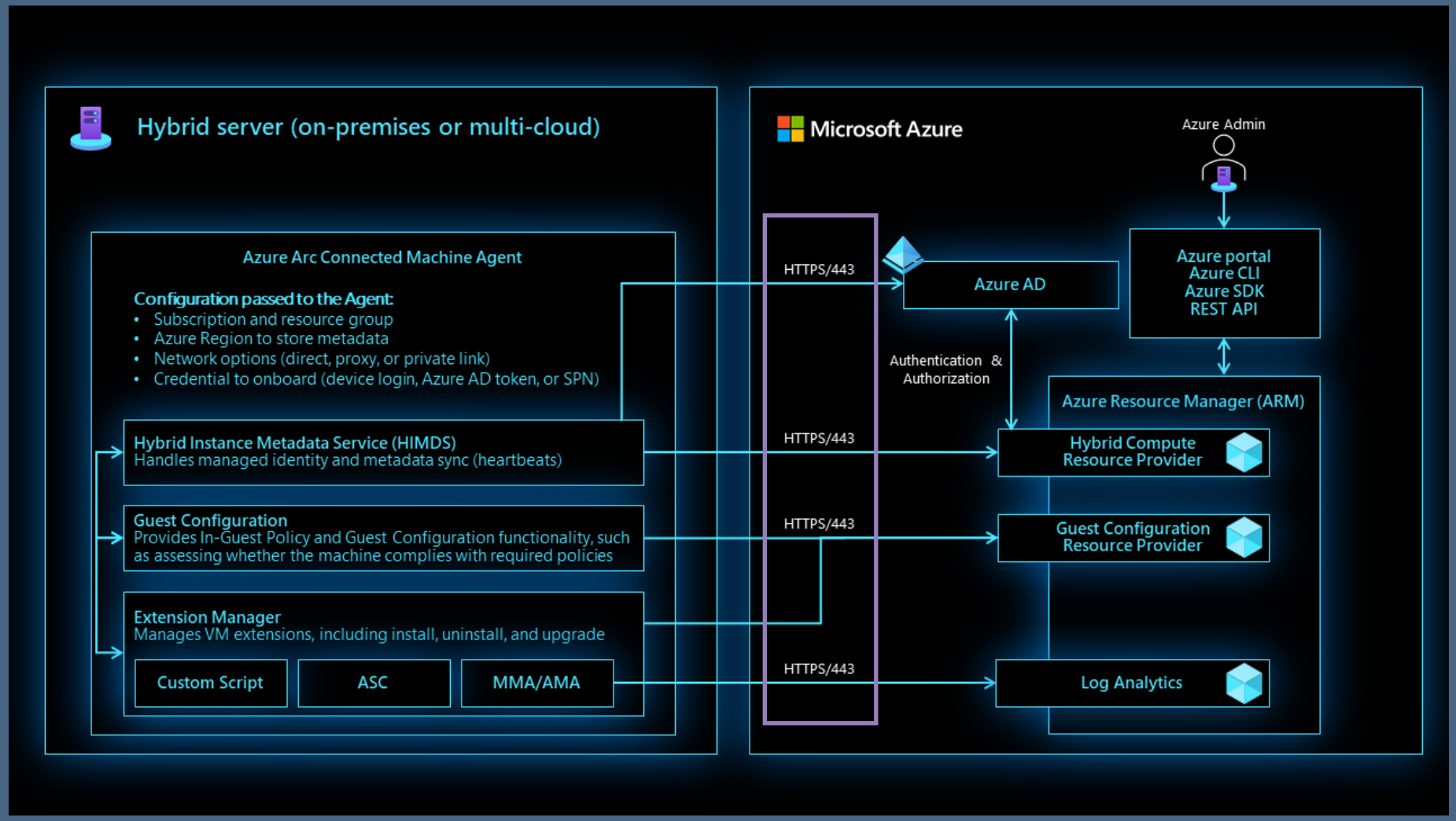
DFC covers non-Azure servers by agents

Arc-Enabled Servers



Design Component – Defender for Cloud

DFC communicates with agents and supporting services via HTTPS/443

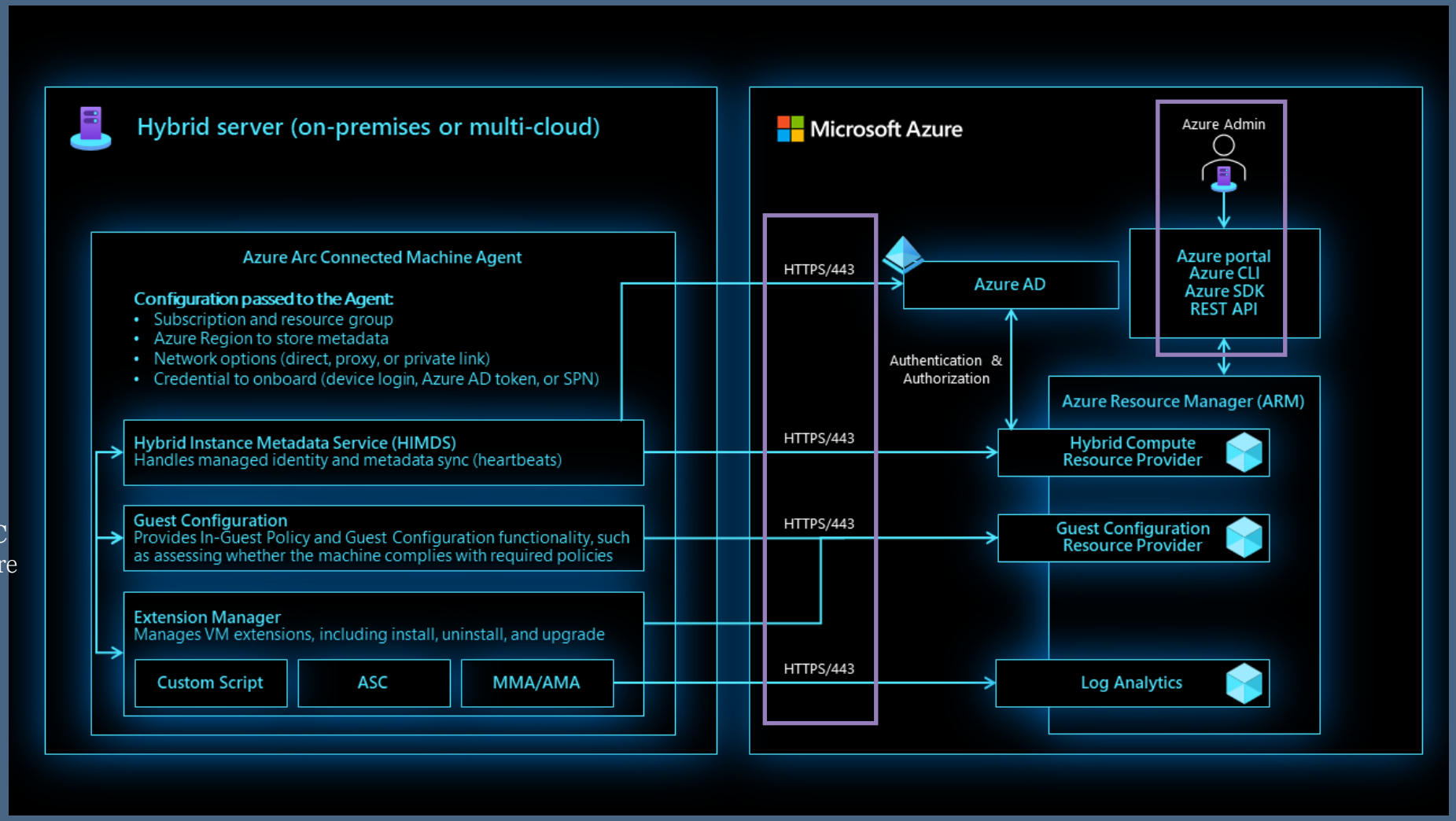


DFC covers non-Azure servers by agents

Design Component – Defender for Cloud

DFC communicates with agents and supporting services via HTTPS/443

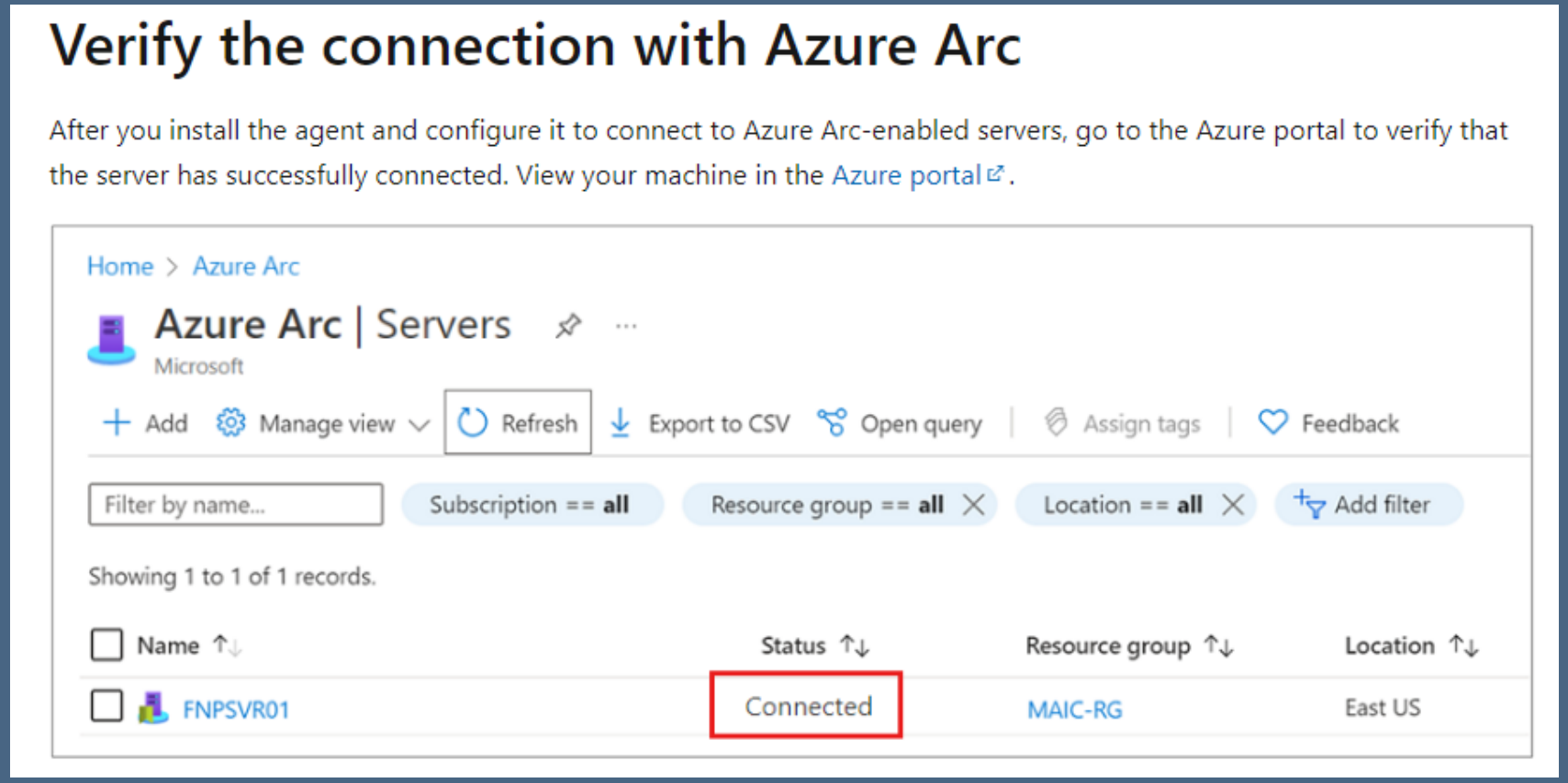
Admin interacts with DFC by Portal, Azure CLI, Azure SDK, and REST API



DFC covers non-Azure servers by agents

Design Component – Defender for Cloud

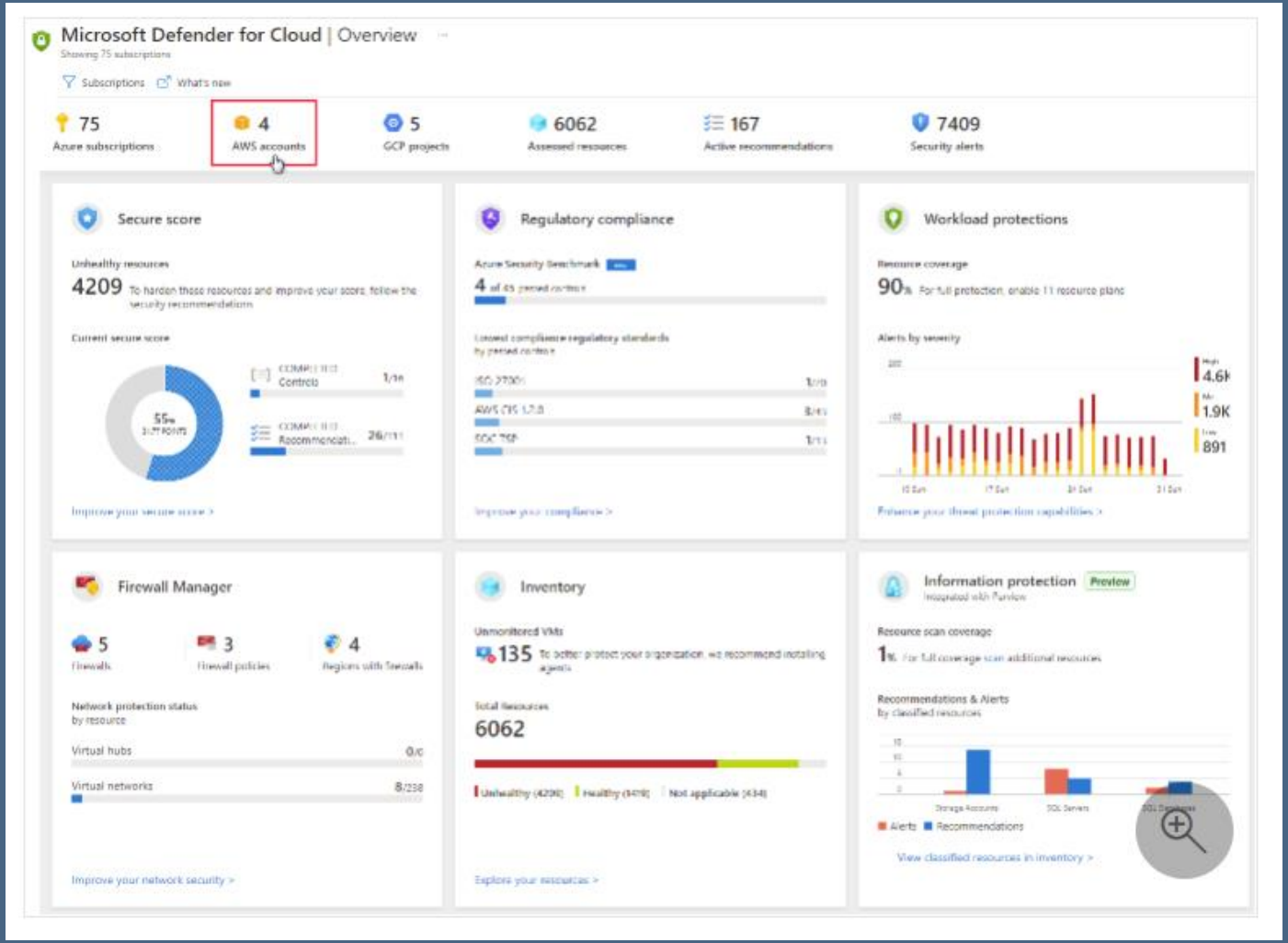
Example of a non-Azure server on-prem with agent running connected to Azure



DFC covers non-Azure servers by agents

Design Component – Defender for Cloud

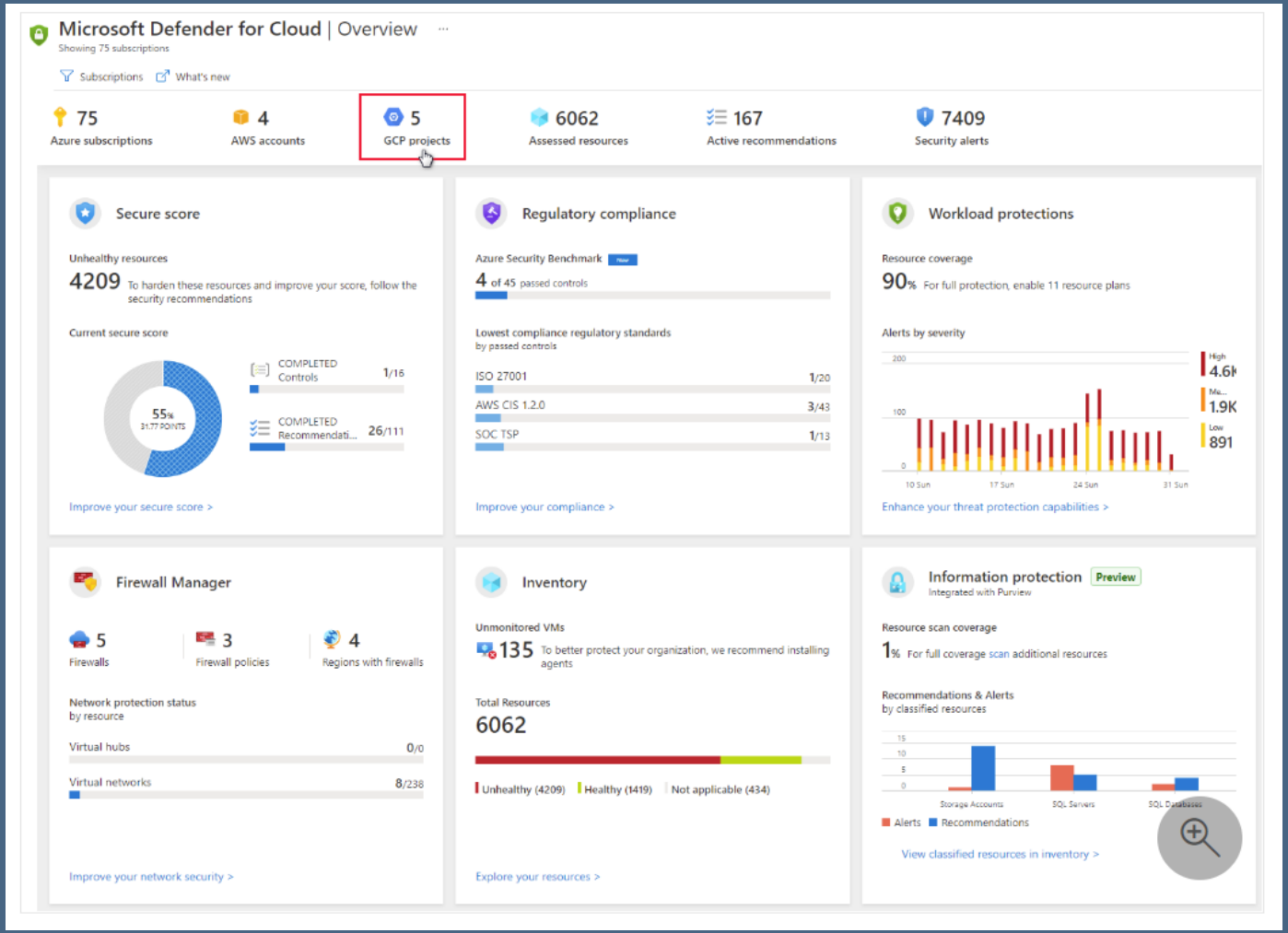
Example of AWS inventory



DFC covers non-Azure servers by agents

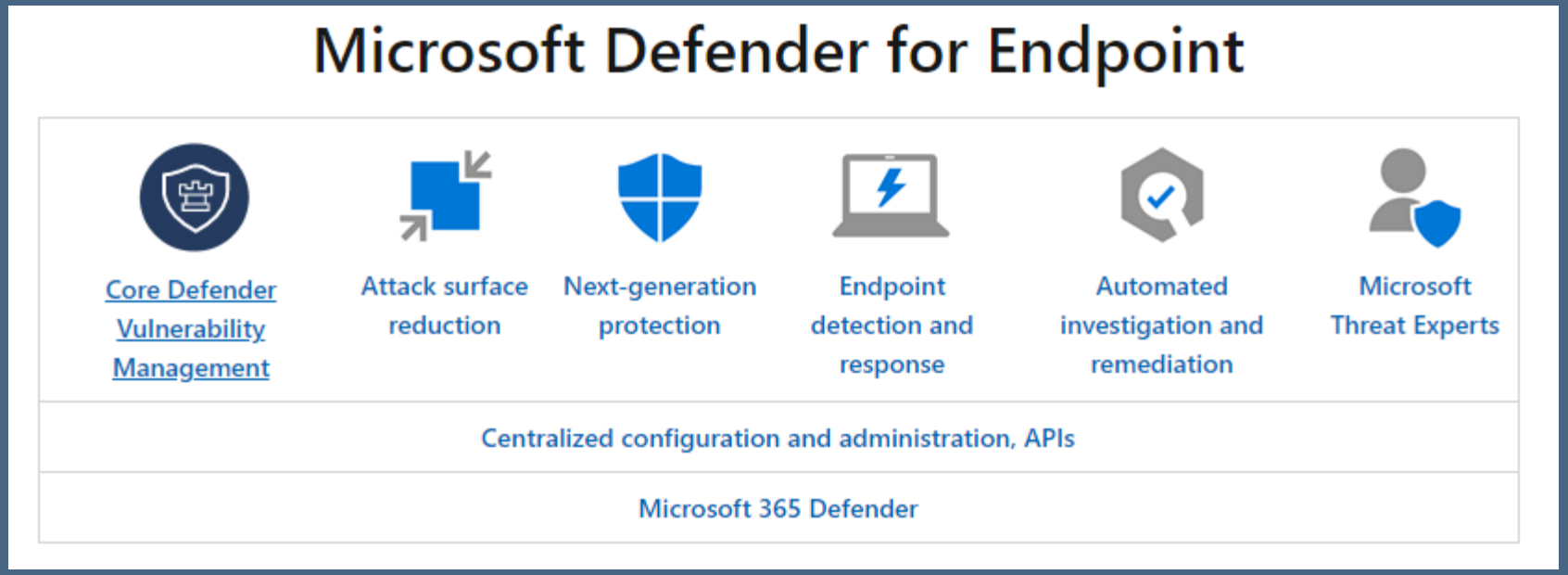
Design Component – Defender for Cloud

Example of GCP inventory



DFC covers non-Azure servers by agents

Design Component – Defender for Cloud



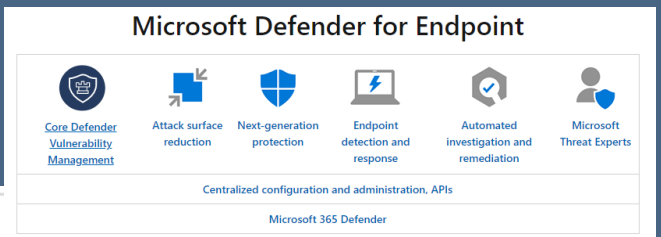
MDE is device/server centric

Design Component – Defender for Cloud

Plan	What's included
Defender for Endpoint Plan 1	• Next-generation protection (includes antimalware and antivirus) • Attack surface reduction • Manual response actions • Centralized management • Security reports • APIs • Support for Windows 10, iOS, Android OS, and macOS devices

MDE has two plans. Plan 1 covers devices

Design Component – Defender for Cloud



Defender for Endpoint Plan 2

All of the Defender for Endpoint Plan 1 capabilities, plus:

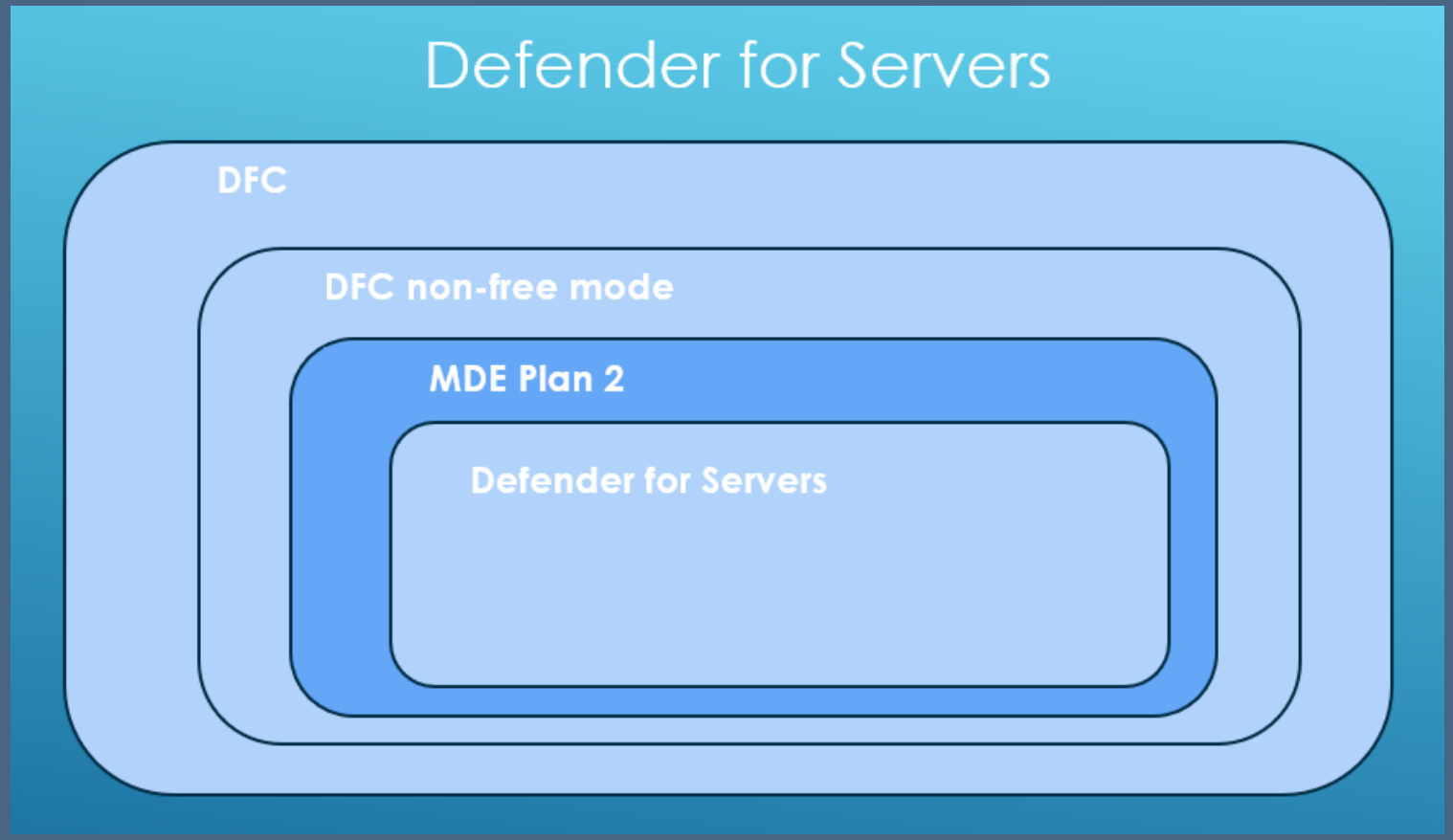
- Device discovery
- Device inventory
- Core Defender Vulnerability Management capabilities
- Threat Analytics
- Automated investigation and response
- Advanced hunting
- Endpoint detection and response
- Microsoft Threat Experts
- Support for Windows (client and server) and non-Windows platforms (macOS, iOS, Android, and Linux)

Plan 2 covers devices and servers

Design Component – Defender for Cloud

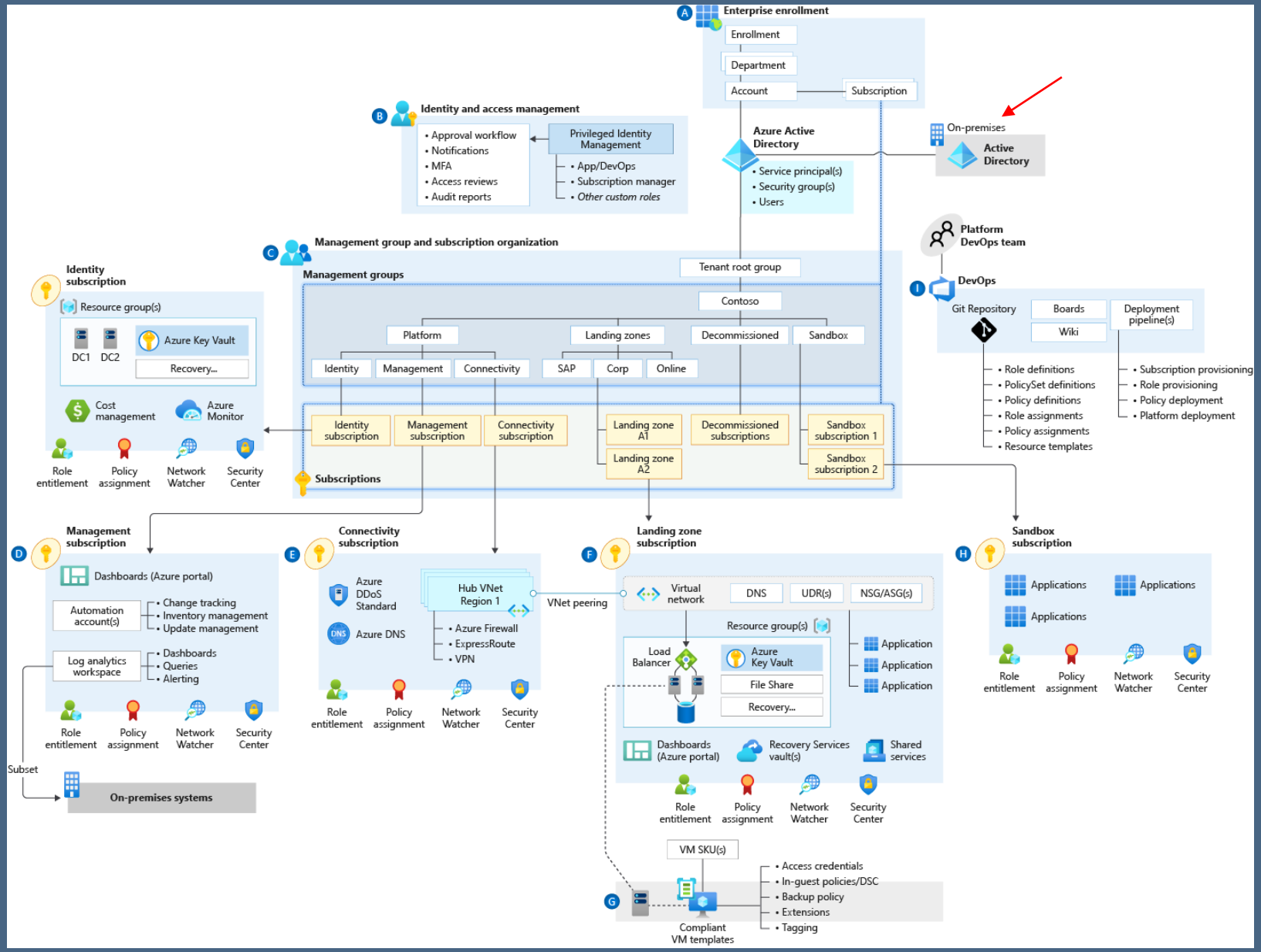
Defender for Servers supports security for servers in a hybrid and multi-cloud environment.
Defender for Servers and MDE Plan 2 overlap in protecting servers

Design Component – Defender for Cloud



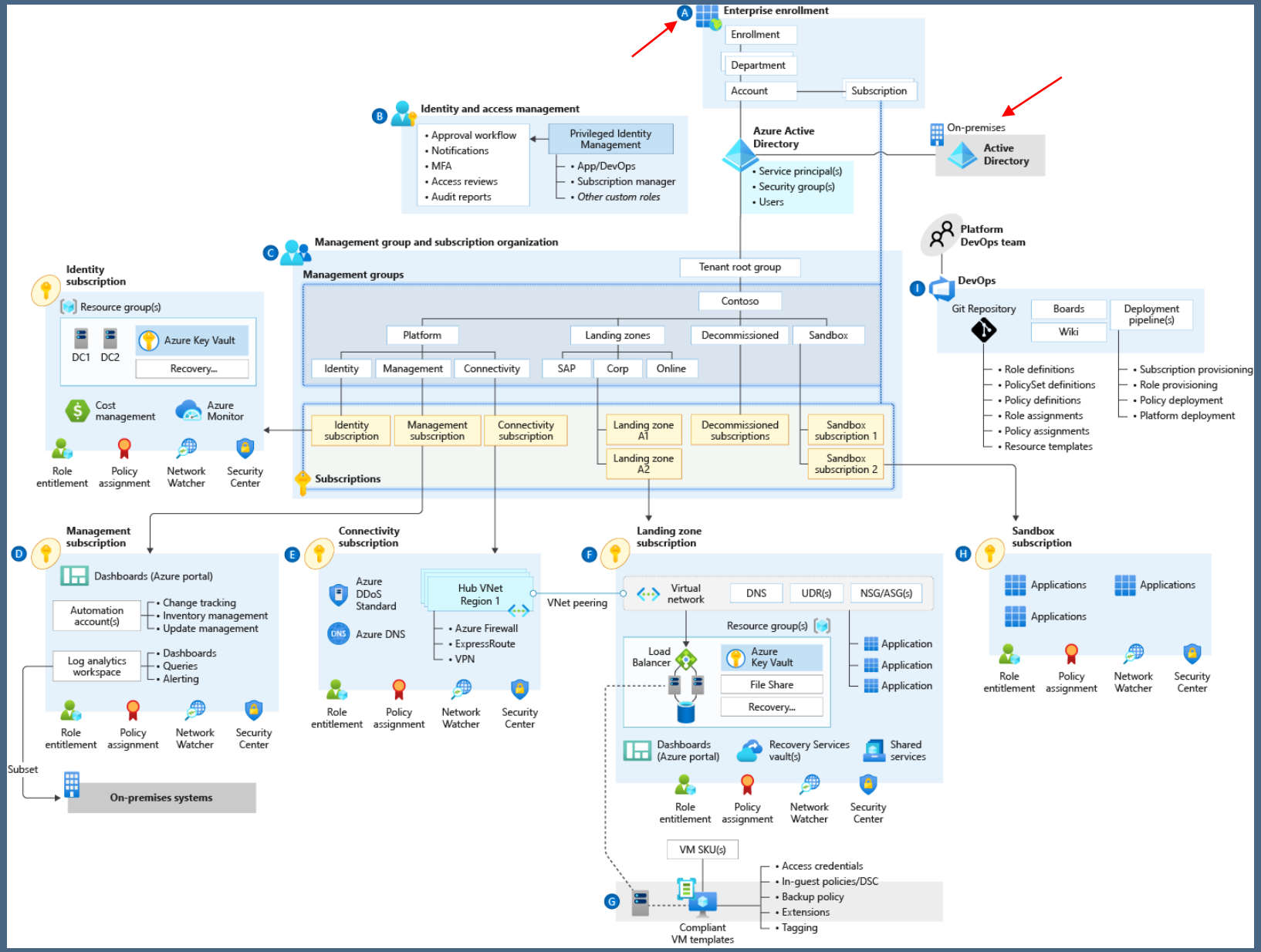
Putting it all together

- Hybrid including both Azure and on-prem



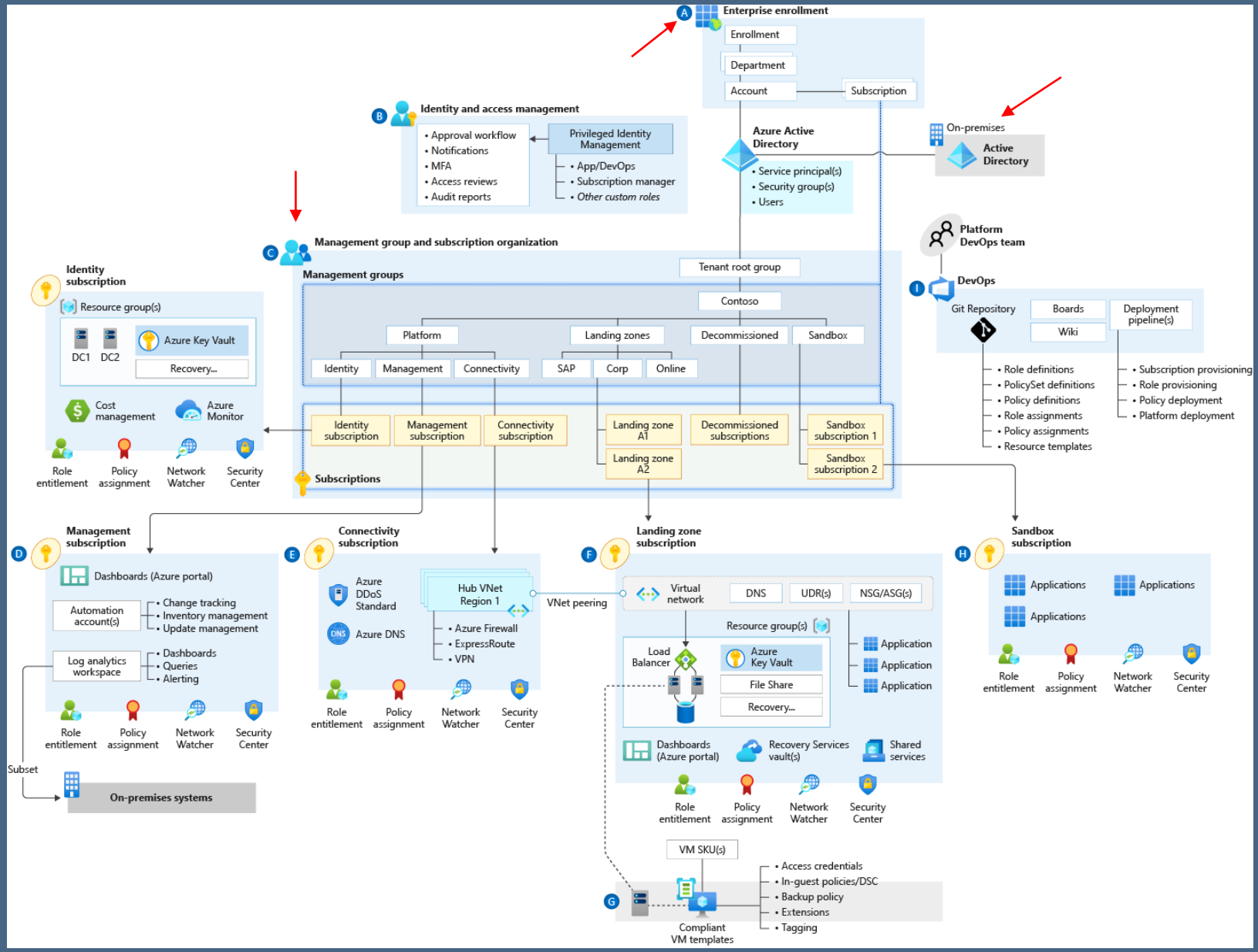
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)



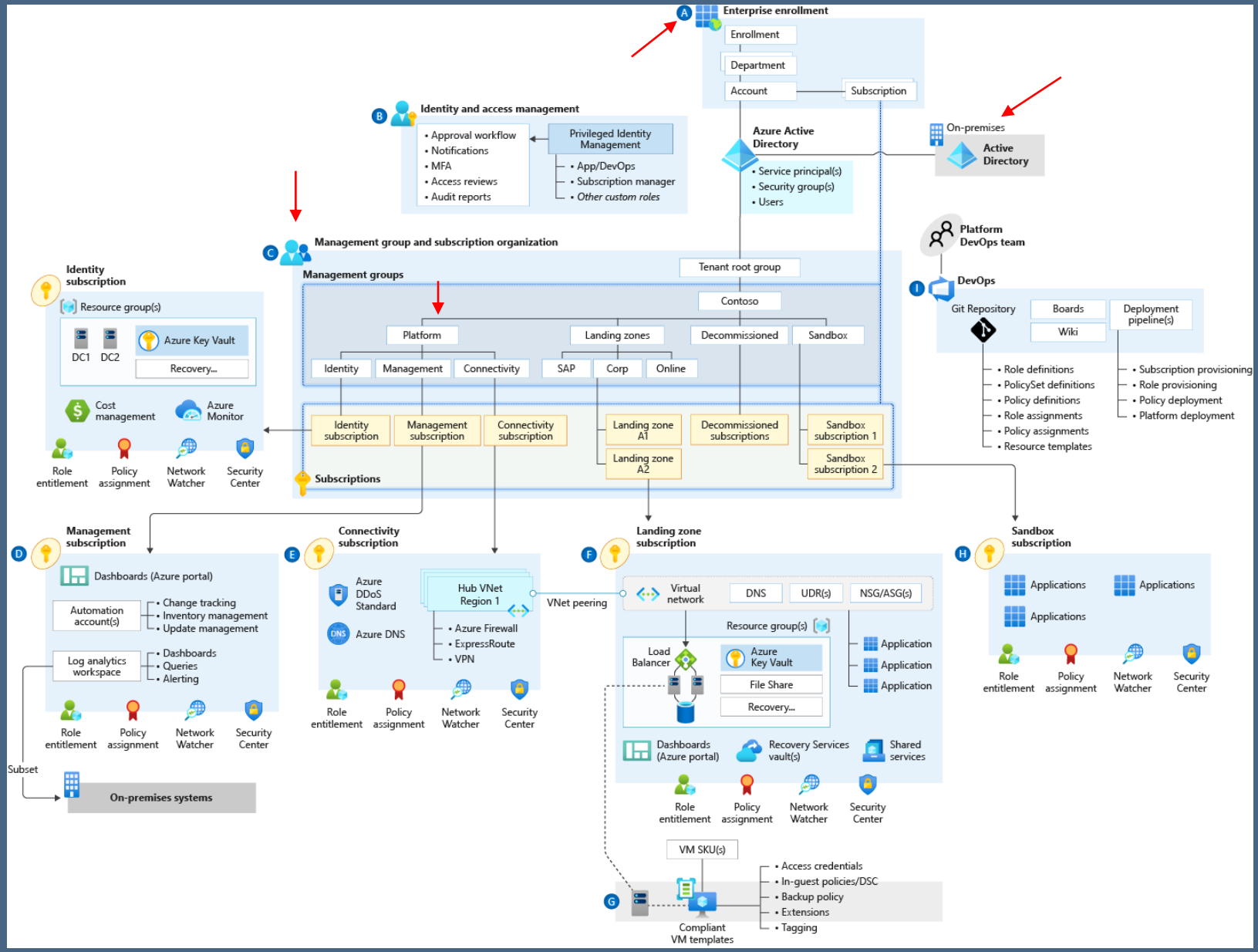
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups (C)



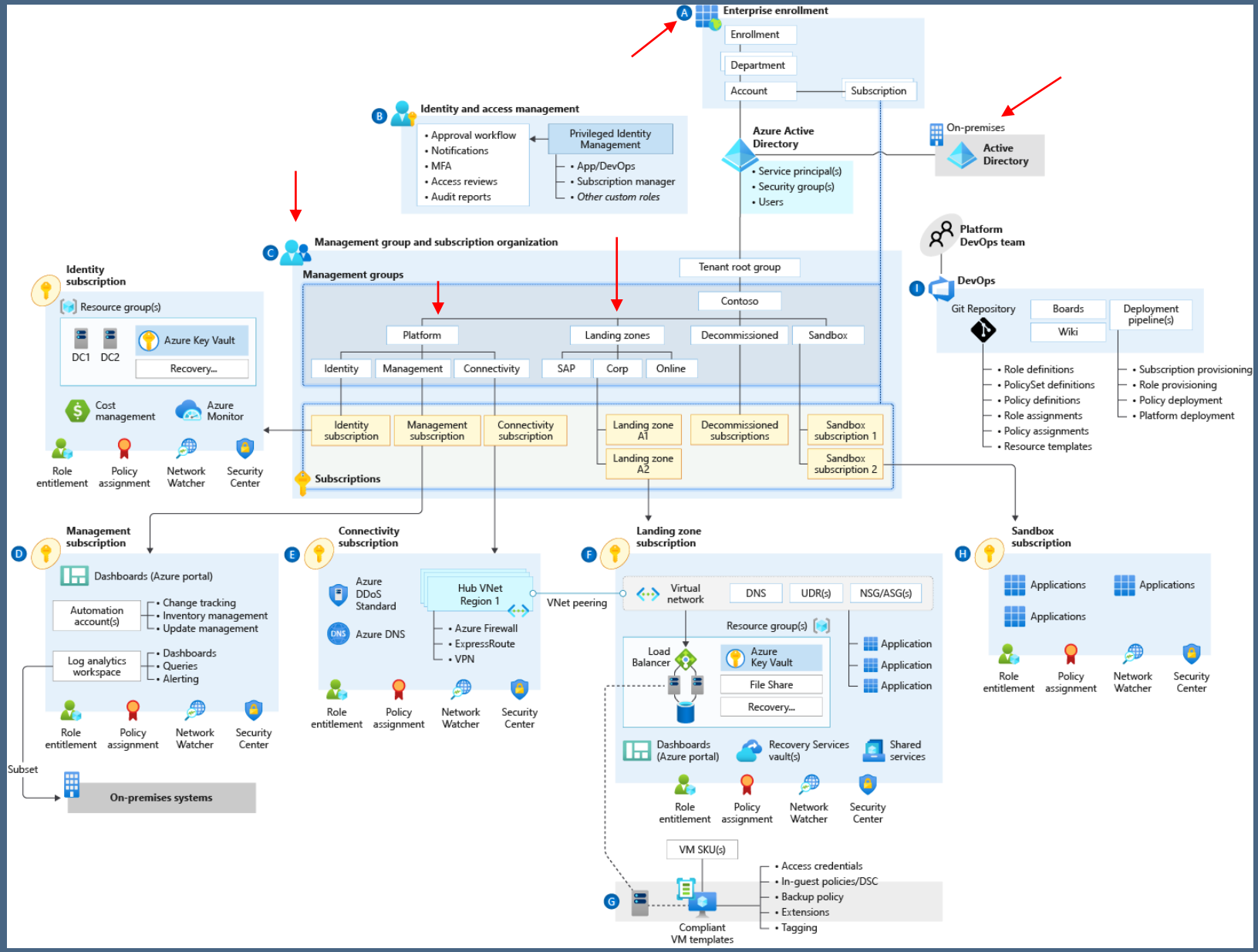
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)



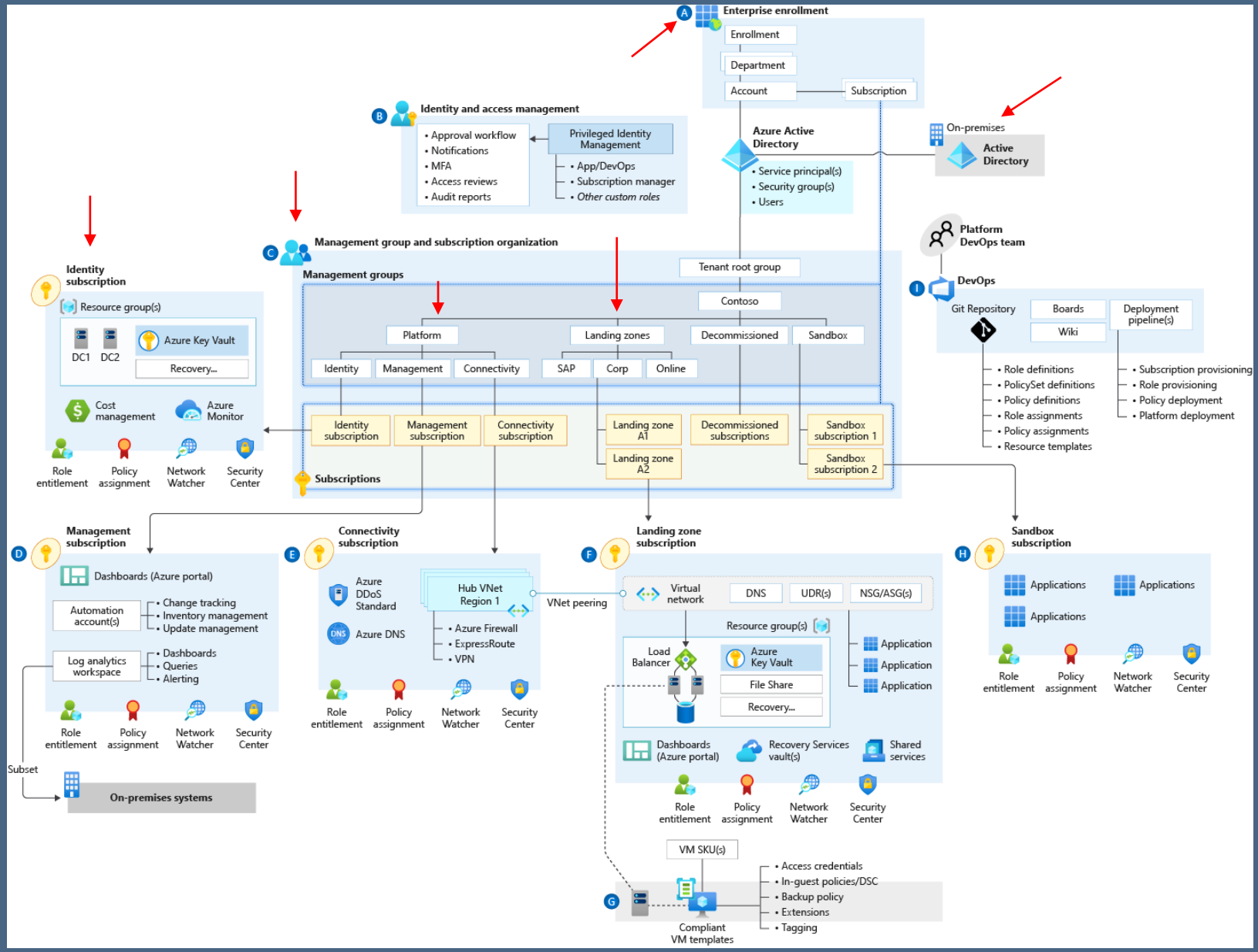
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment



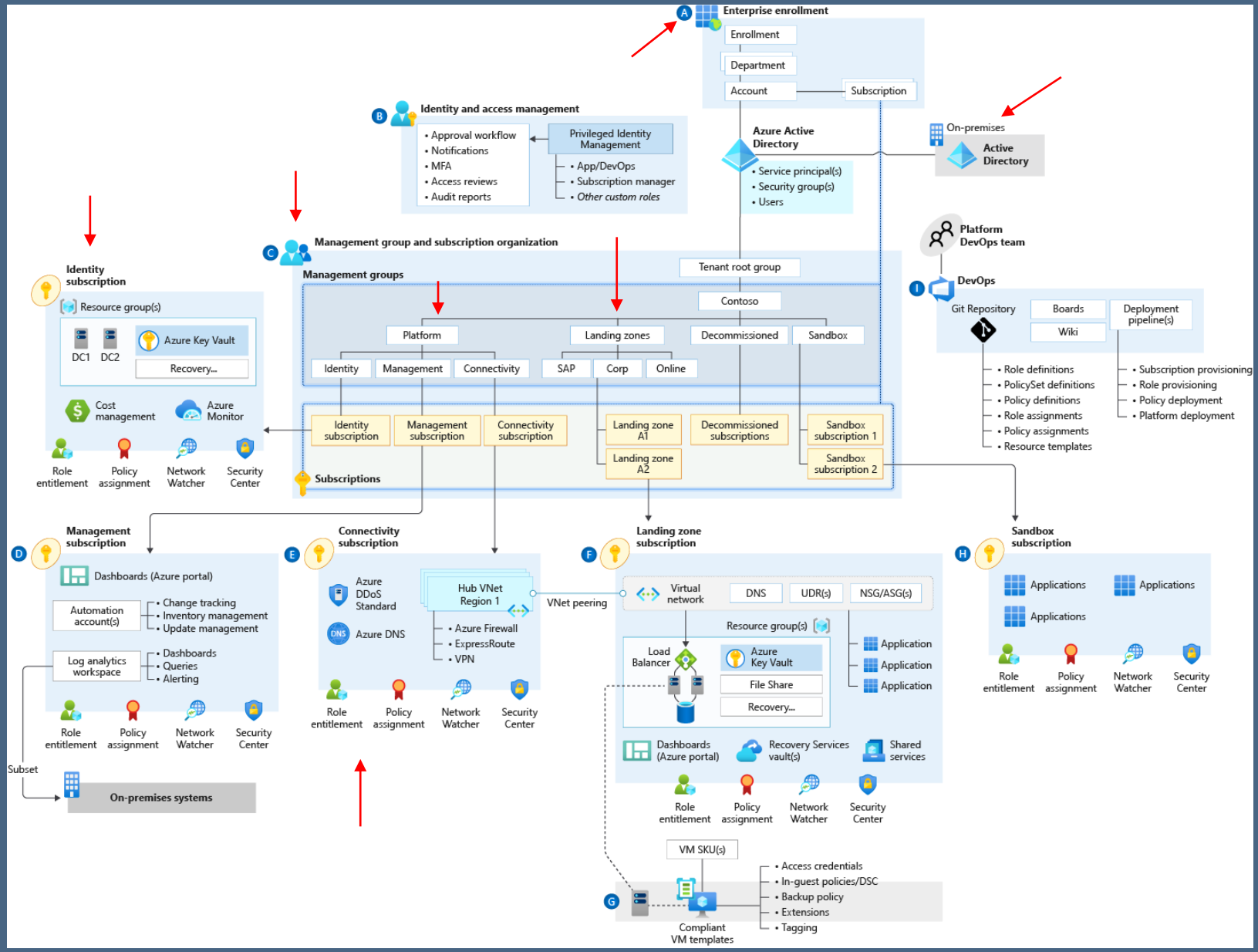
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)



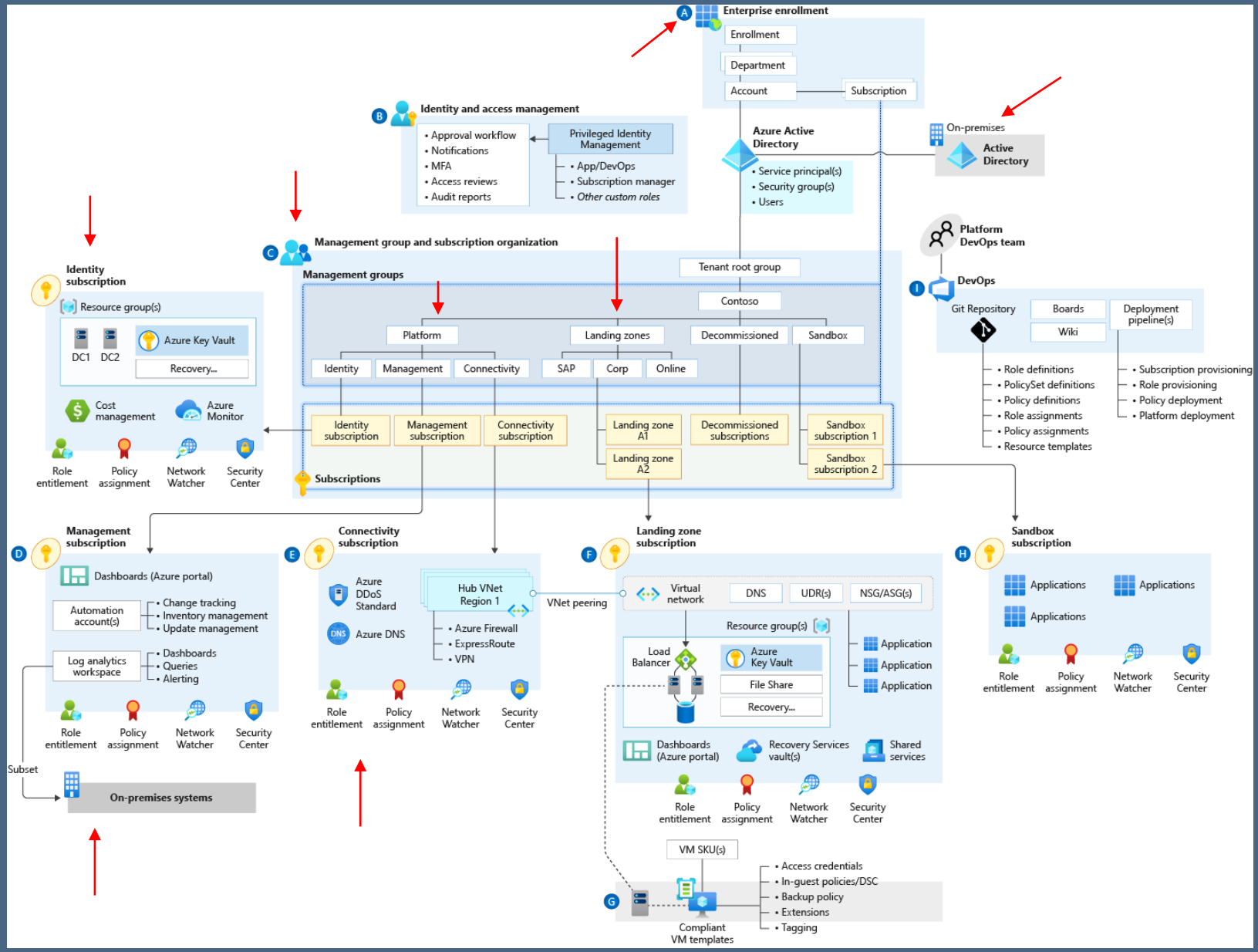
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)



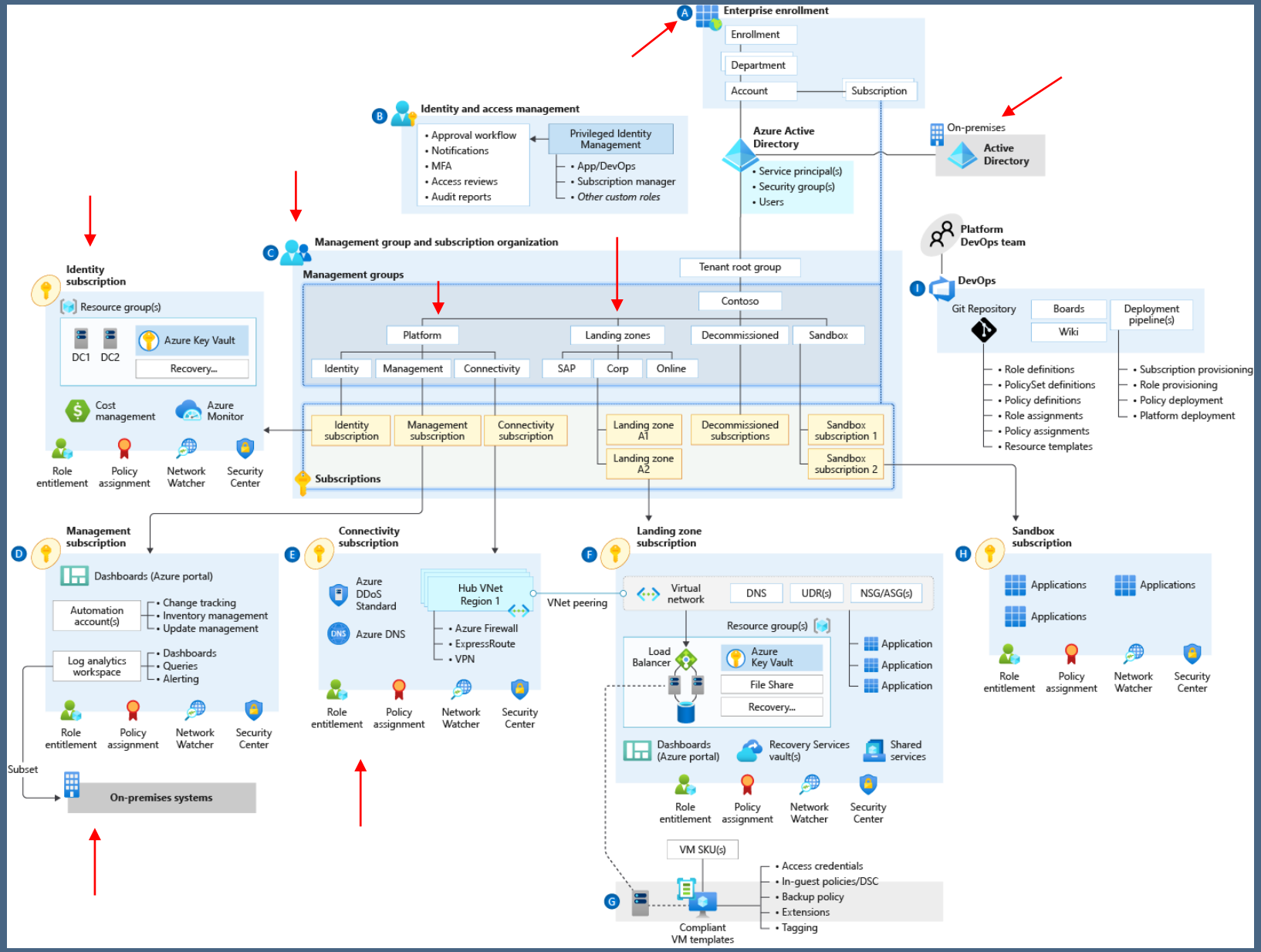
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)
- Management (Security, Governance, Operations)



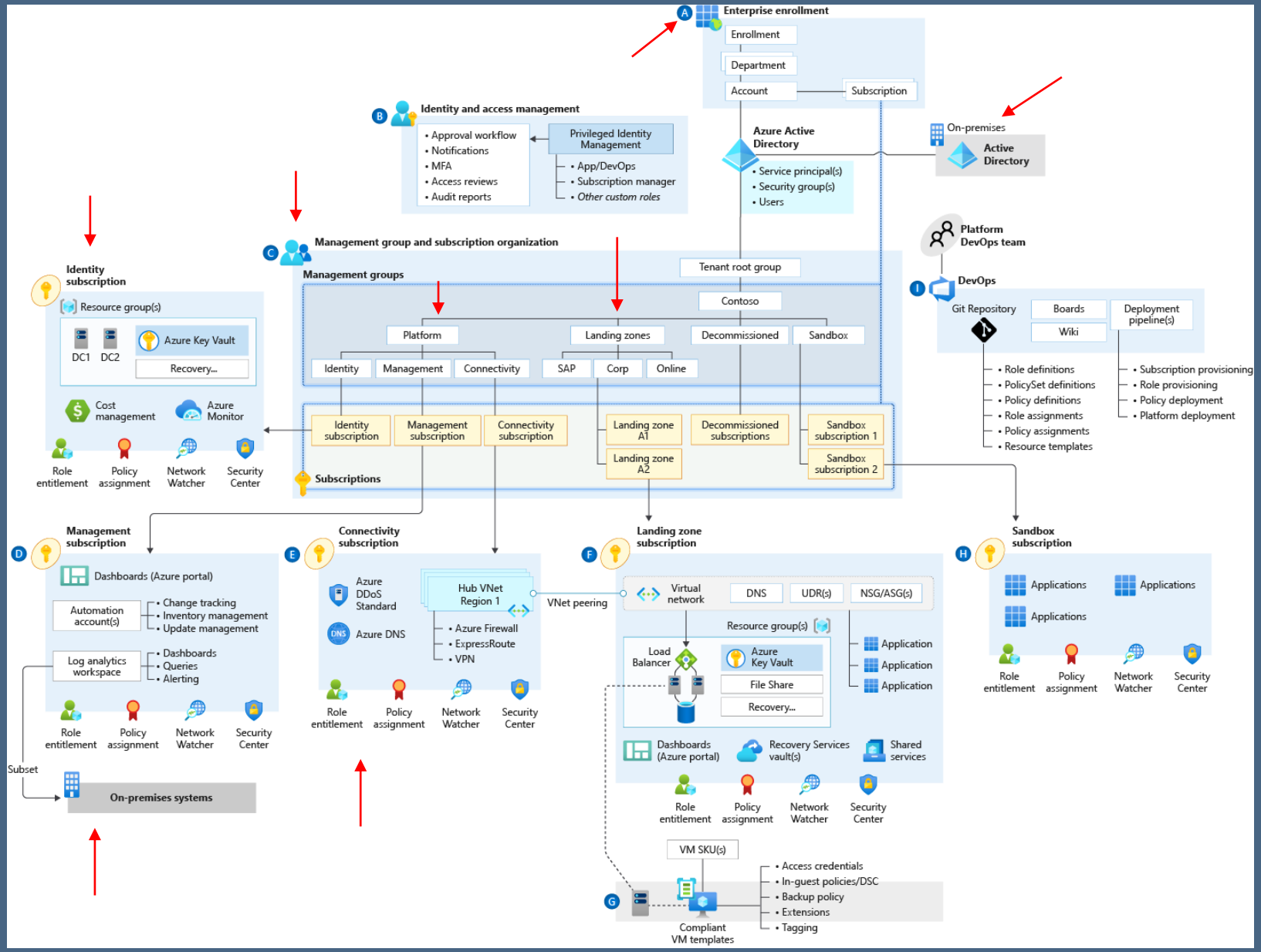
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)
- Management (Security, Governance, Operations)
- Multi-environment support for tenants including Prod, Dev, QA, Stage (not shown). In Prod, Blue/Green deployment model can be implemented



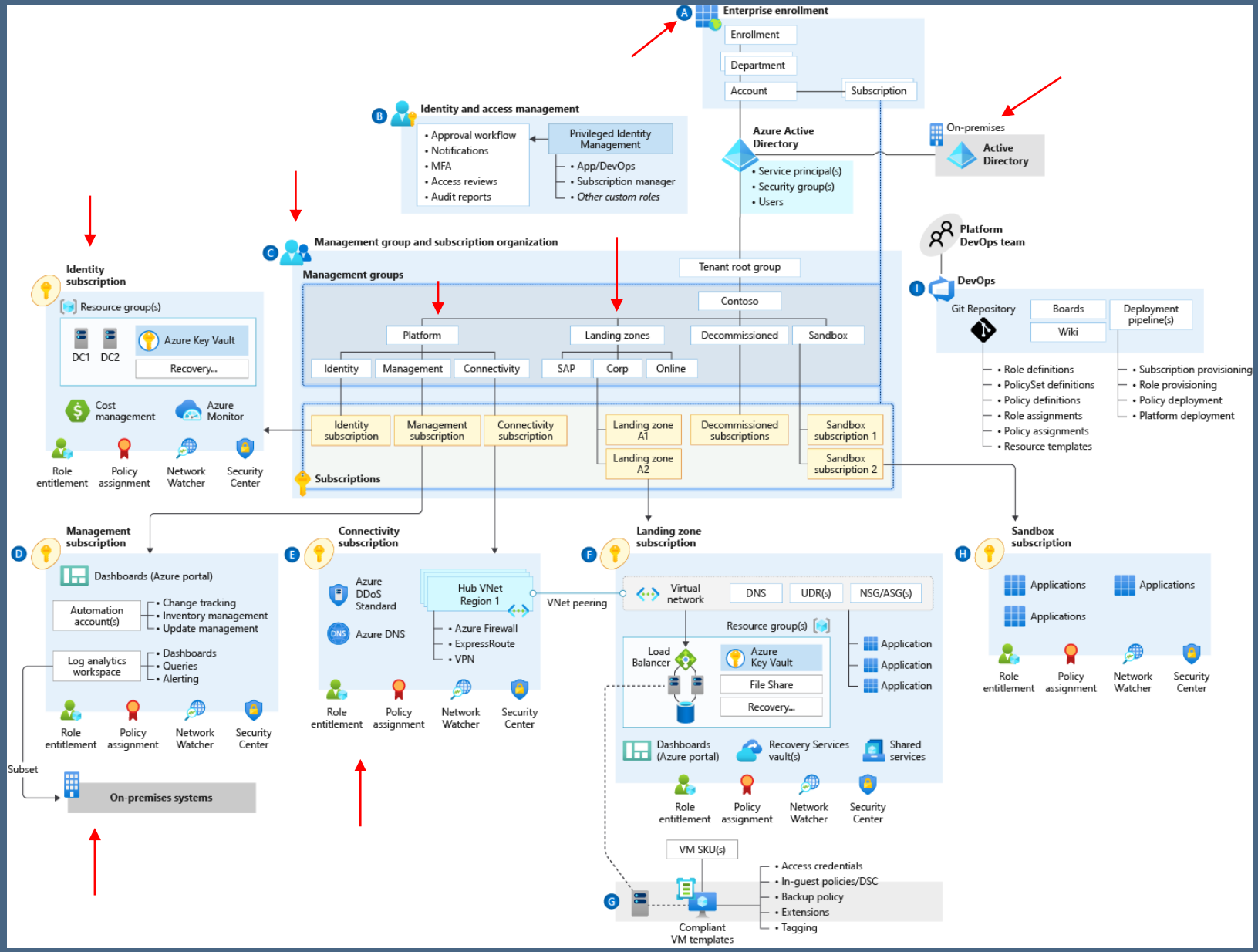
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)
- Management (Security, Governance, Operations)
- Multi-environment support for tenants including Prod, Dev, QA, Stage (not shown). In Prod, Blue/Green deployment model can be implemented
- Microservices and containerization (not shown)



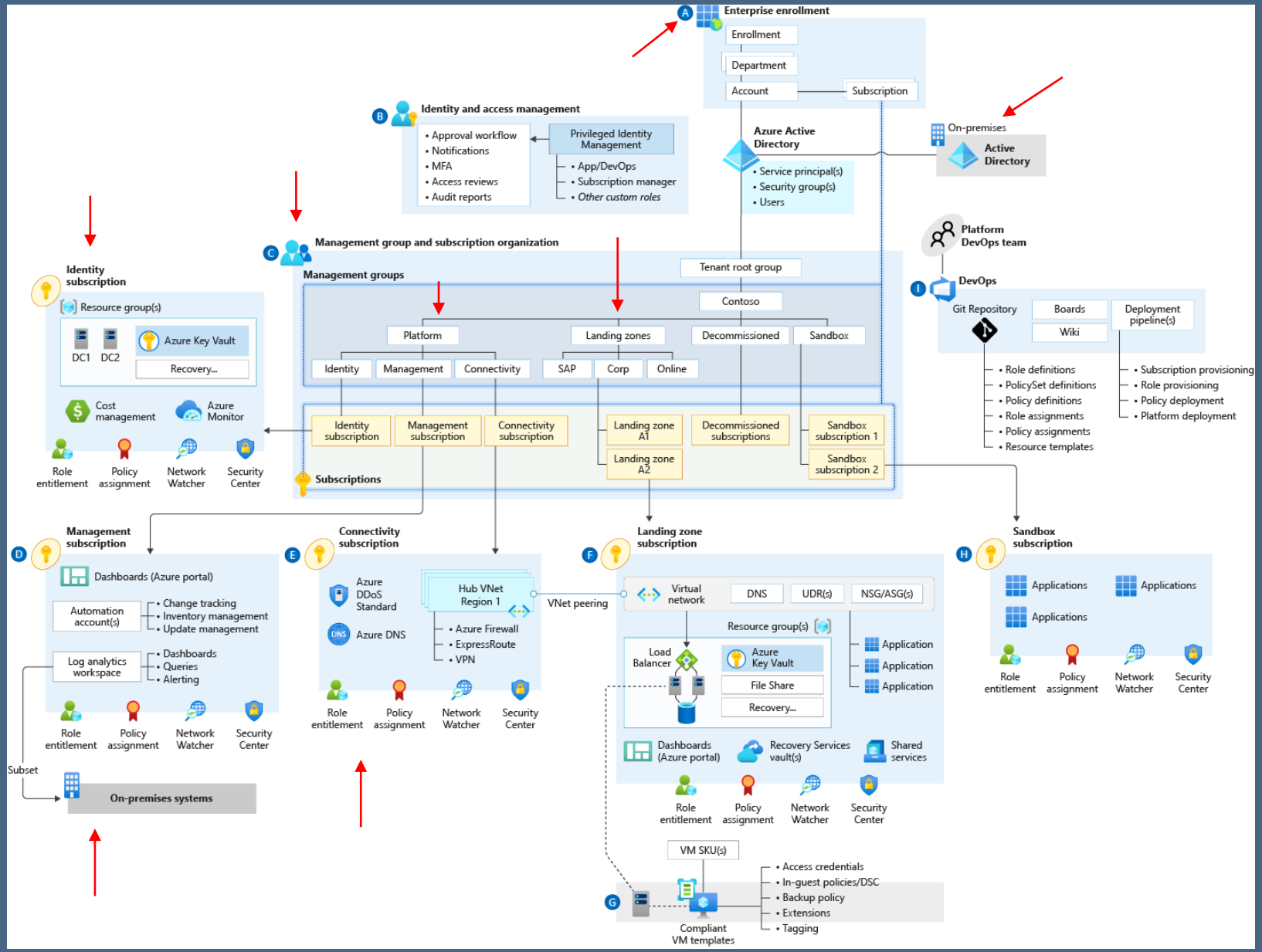
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)
- Management (Security, Governance, Operations)
- Multi-environment support for tenants including Prod, Dev, QA, Stage (not shown). In Prod, Blue/Green deployment model can be implemented
- Microservices and containerization (not shown)
- Data Loss Prevention – Azure Virtual Desktop for internal use (not shown)



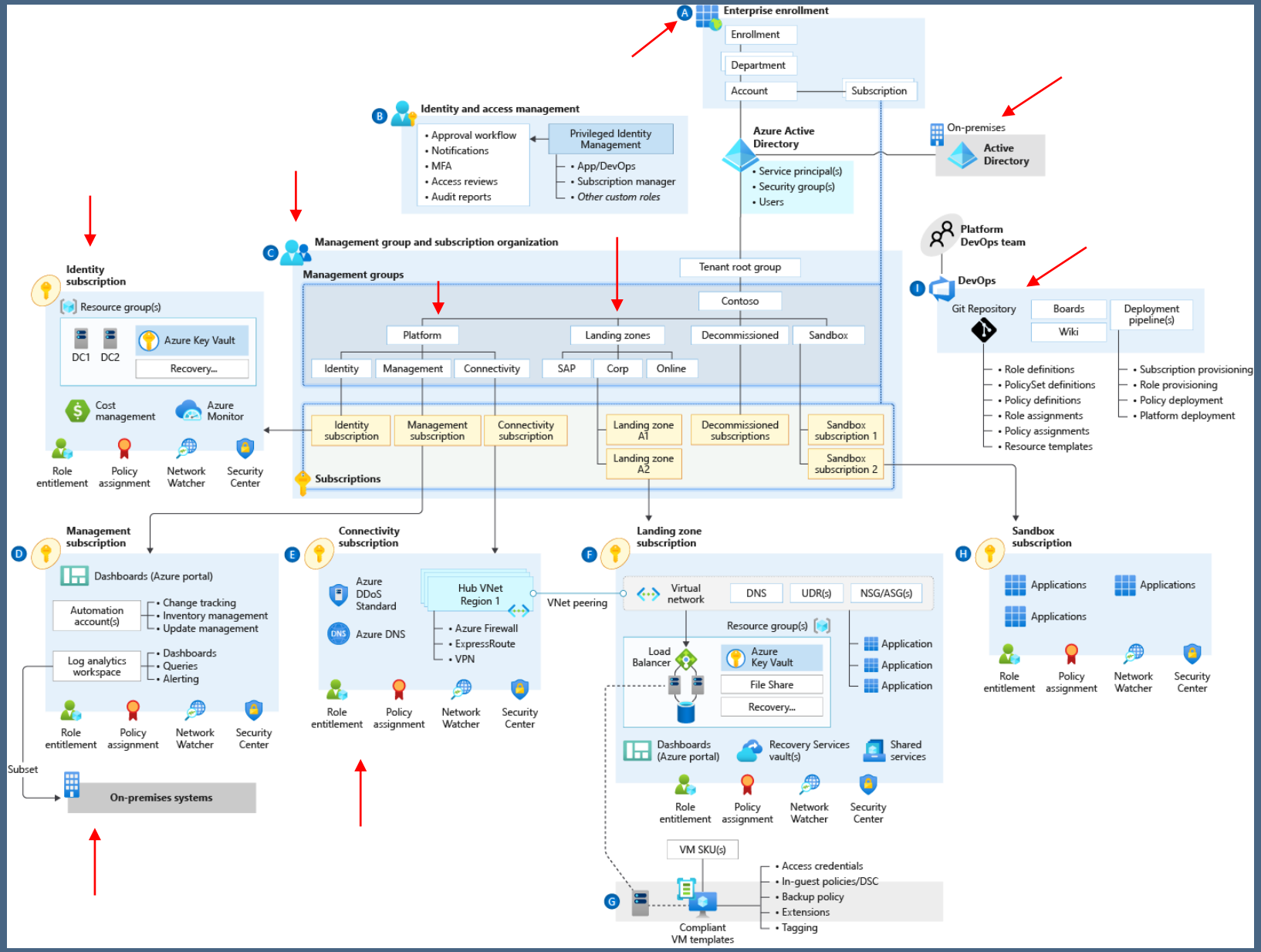
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)
- Management (Security, Governance, Operations)
- Multi-environment support for tenants including Prod, Dev, QA, Stage (not shown). In Prod, Blue/Green deployment model can be implemented
- Microservices and containerization (not shown)
- Data Loss Prevention – Azure Virtual Desktop for internal use (not shown)
- AAD B2C, CASB and the like for customer-facing applications and external use (not shown)



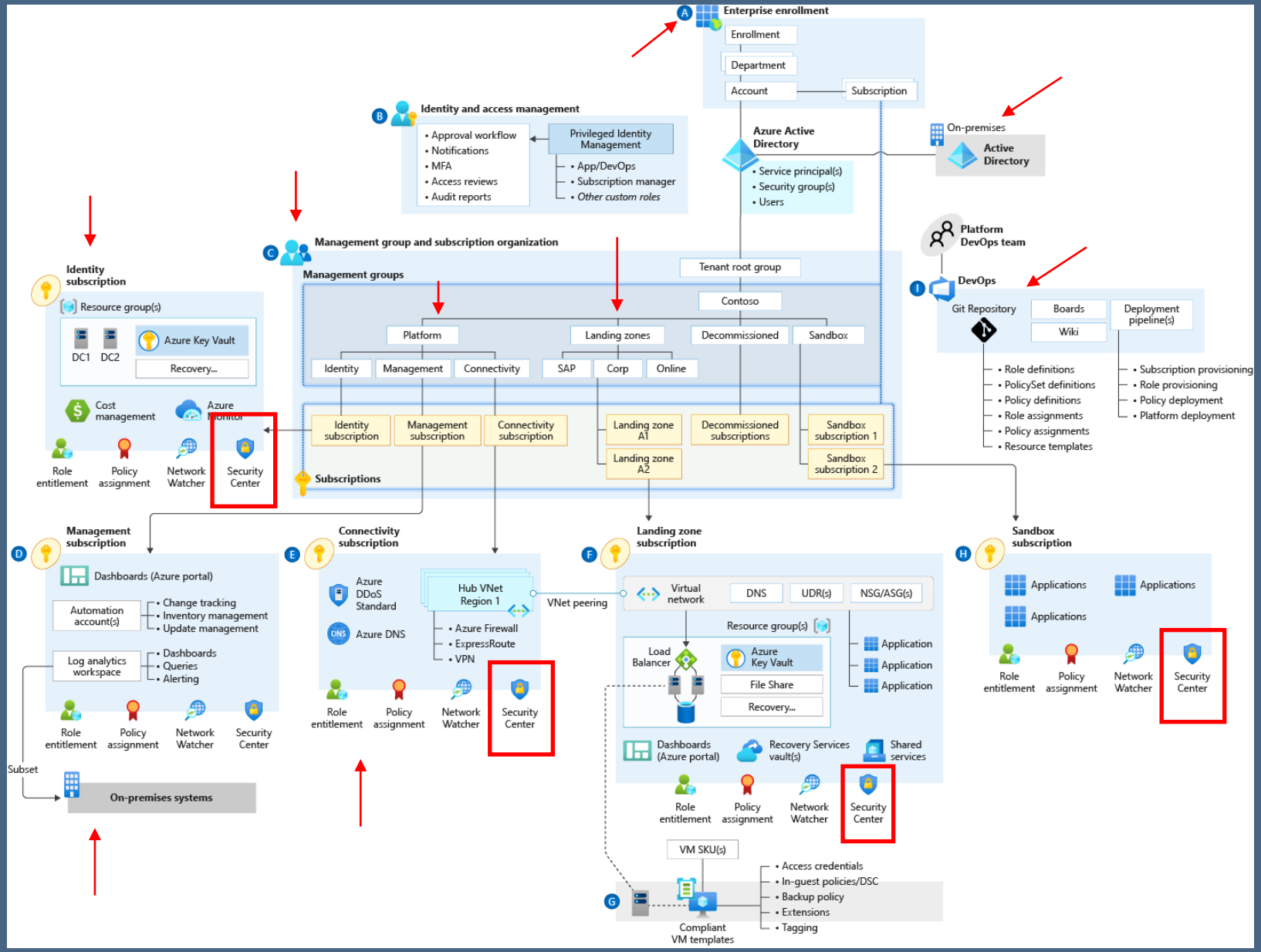
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)
- Management (Security, Governance, Operations)
- Multi-environment support for tenants including Prod, Dev, QA, Stage (not shown). In Prod, Blue/Green deployment model can be implemented
- Microservices and containerization (not shown)
- Data Loss Prevention – Azure Virtual Desktop for internal use (not shown)
- AAD B2C, CASB and the like for customer-facing applications and external use (not shown)
- DevOps with Pipelines from Non-Prod to Prod (I)



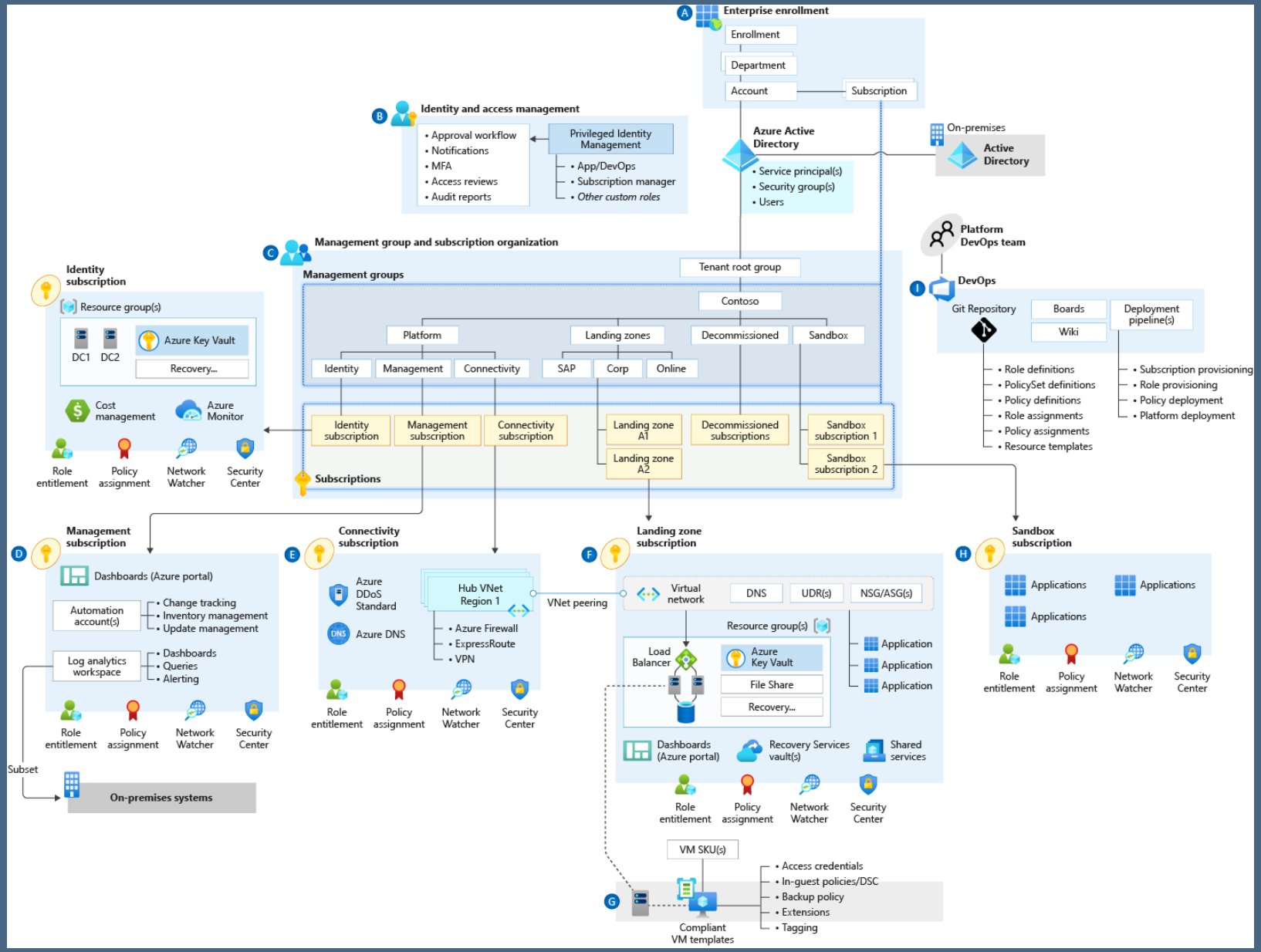
Putting it all together

- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)
- Management (Security, Governance, Operations)
- Multi-environment support for tenants including Prod, Dev, QA, Stage (not shown). In Prod, Blue/Green deployment model can be implemented
- Microservices and containerization (not shown)
- Data Loss Prevention – Azure Virtual Desktop for internal use (not shown)
- AAD B2C, CASB and the like for customer-facing applications and external use (not shown)
- DevOps with Pipelines from Non-Prod to Prod (I)
- Defender for Cloud shown as Security Center in use in distributed fashion



Summary

- Building Security as Code
- Building Security with standardization
- Building Security with automation
- Enhance Security by leveraging native tools such as DFC
- Keep Security with constant monitoring and quick response



Q&A