



# Azure Cloud Security Design

FOR INSURANCE INDUSTRY

# 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



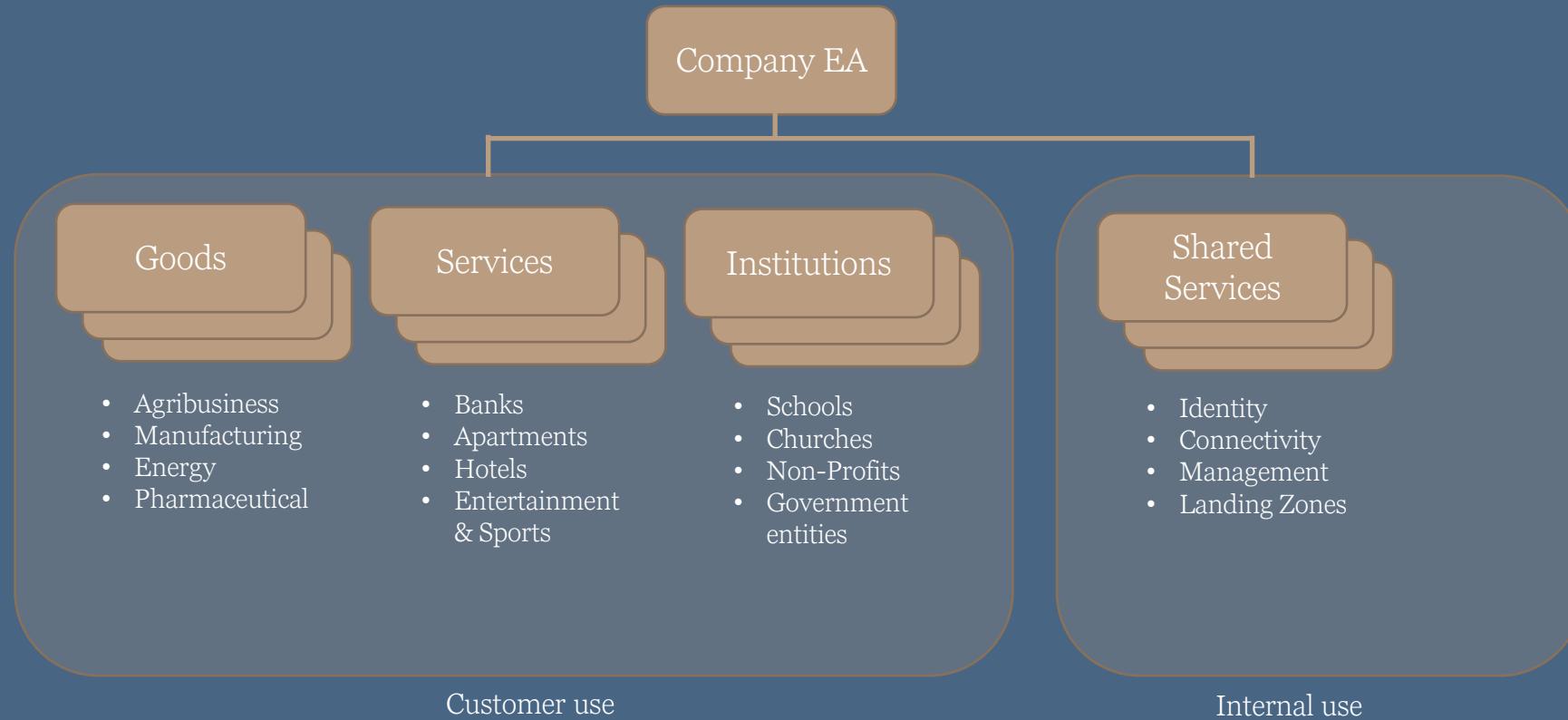






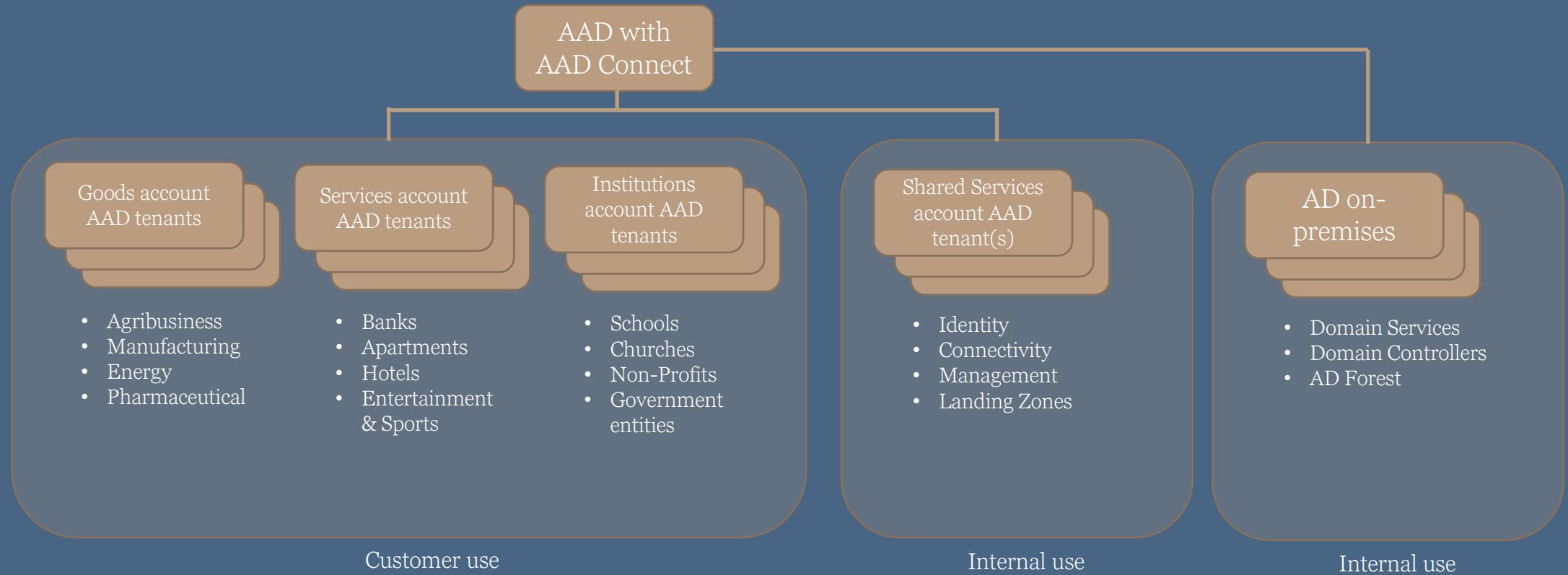


# Design Component – Enterprise Agreement Enrollment



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 components
- ALZ automates tenant creation
- ALZ is implemented via

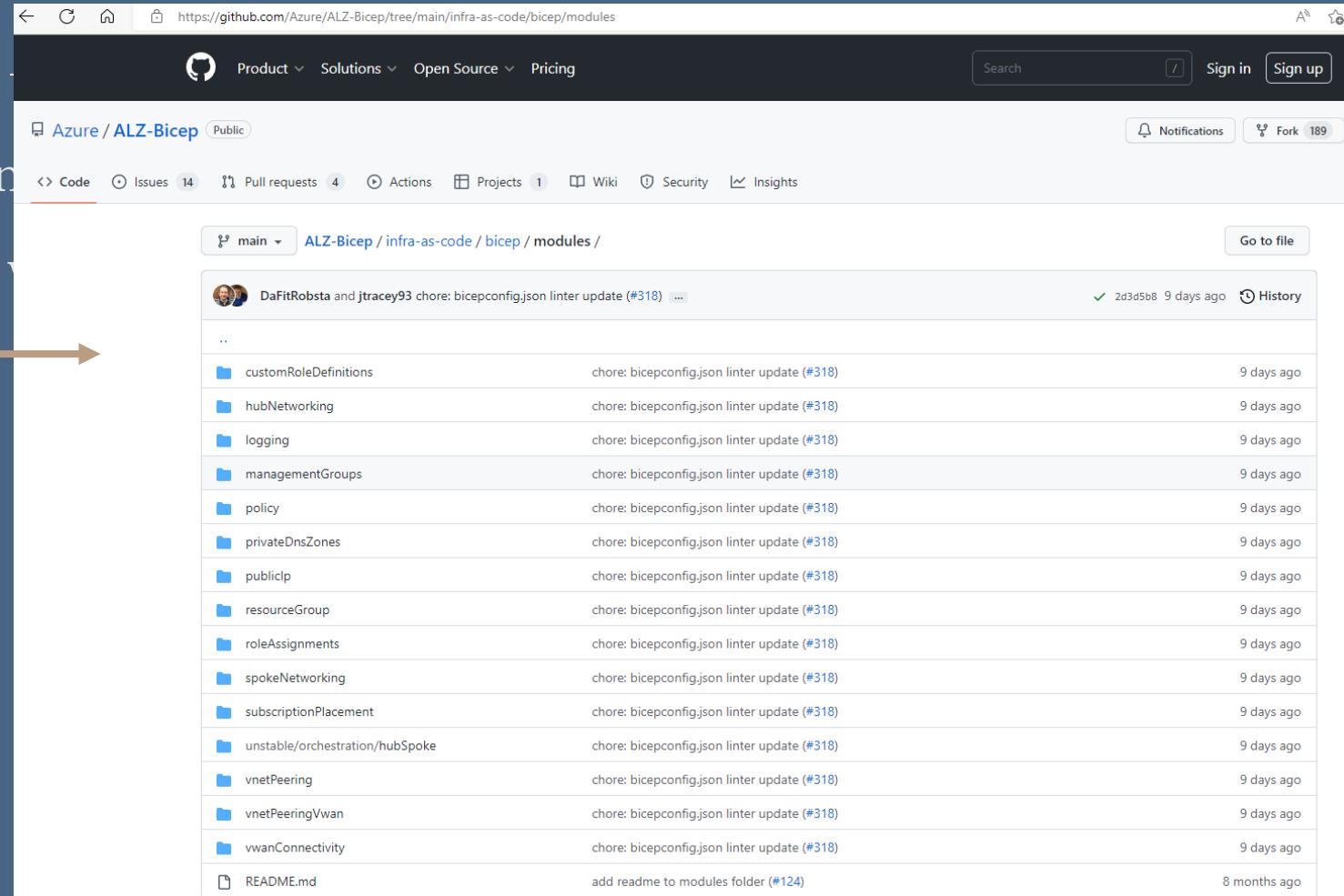
*Bicep*

*Terraform*

*Blueprints*

*Azure CLI*

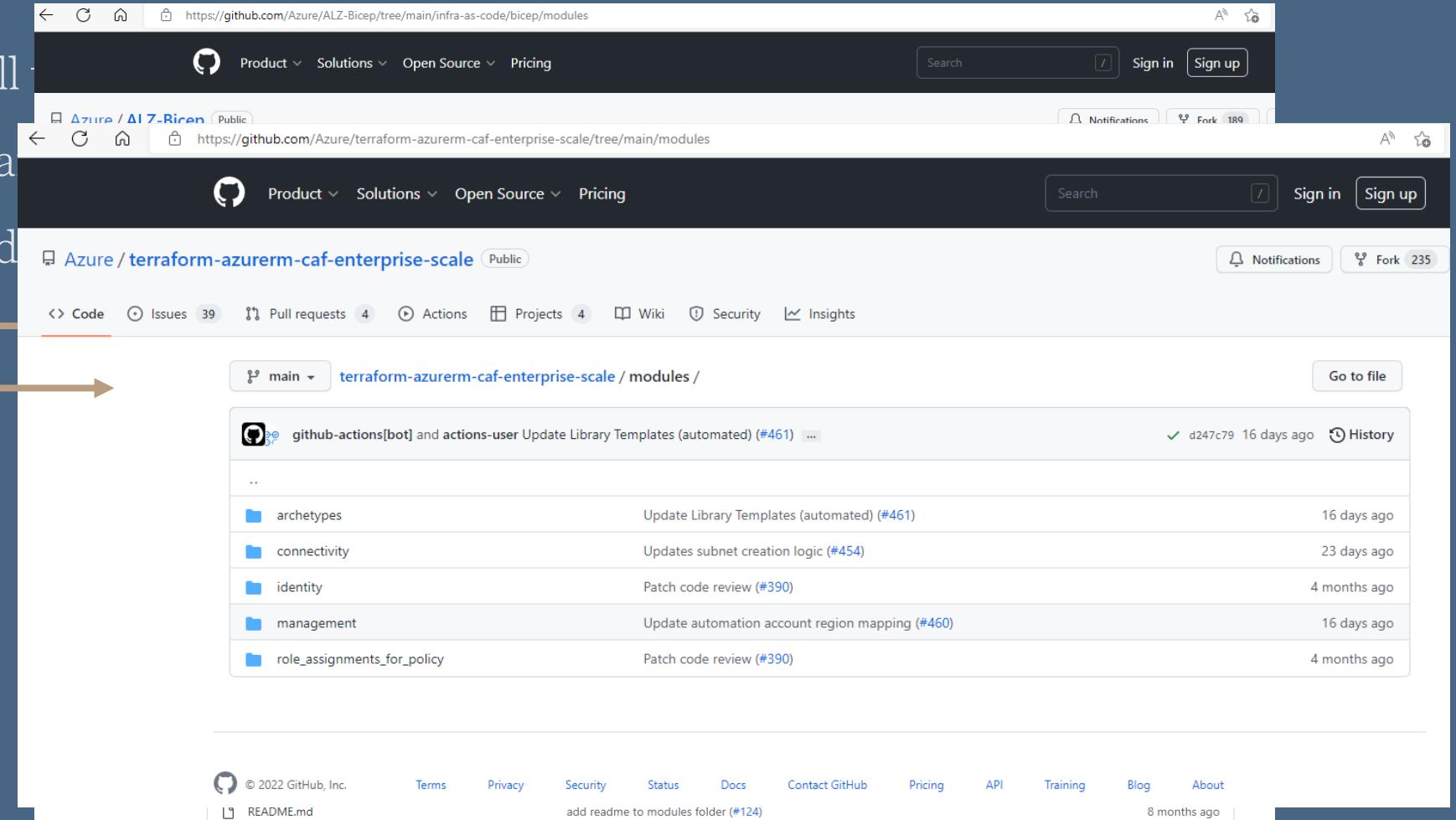
*Azure PowerShell*



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

# Design Component – Landing Zones (ALZ)

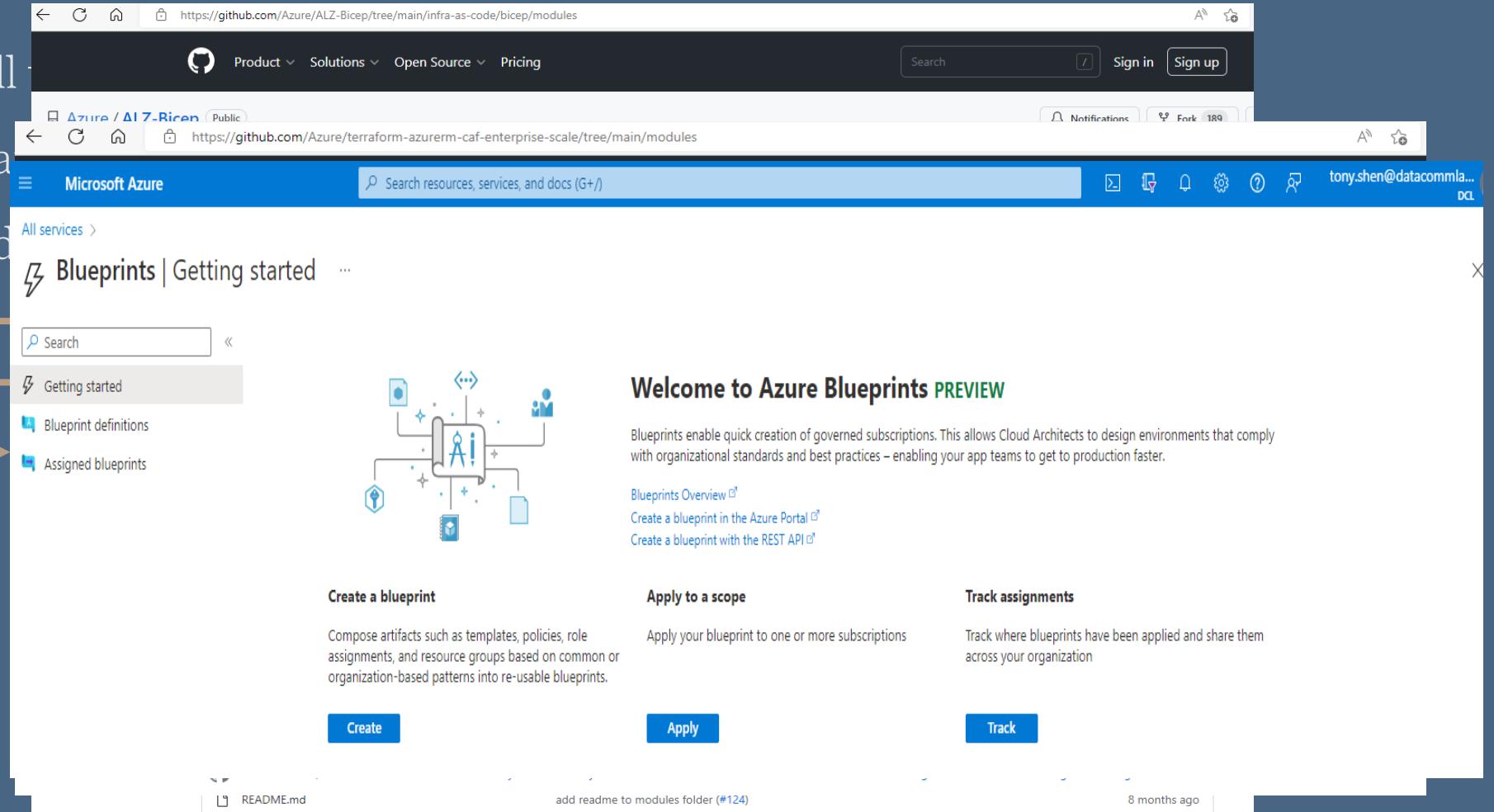
- ALZ standardizes all components
- ALZ automates tenant creation
- ALZ is implemented using:
  - Bicep*
  - Terraform*
  - Blueprints*
  - Azure CLI*
  - Azure PowerShell*



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

# Design Component – Landing Zones (ALZ)

- ALZ standardizes all components
- ALZ automates tenant setup
- ALZ is implemented via:
  - 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 components
- ALZ automates tenant creation
- ALZ is implemented in multiple ways

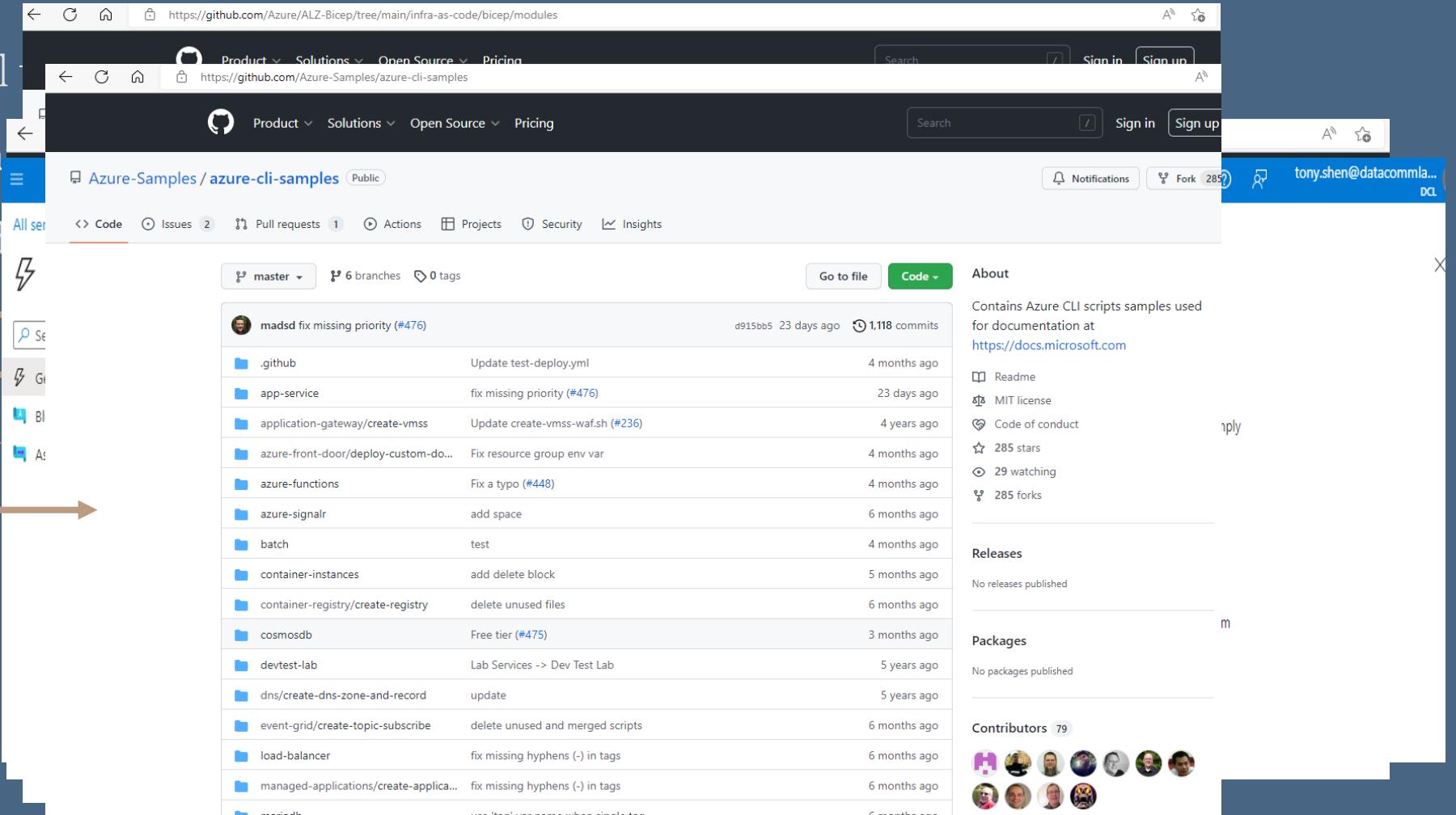
*Bicep*

*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 components
- ALZ automates tenant setup
- ALZ is implemented using

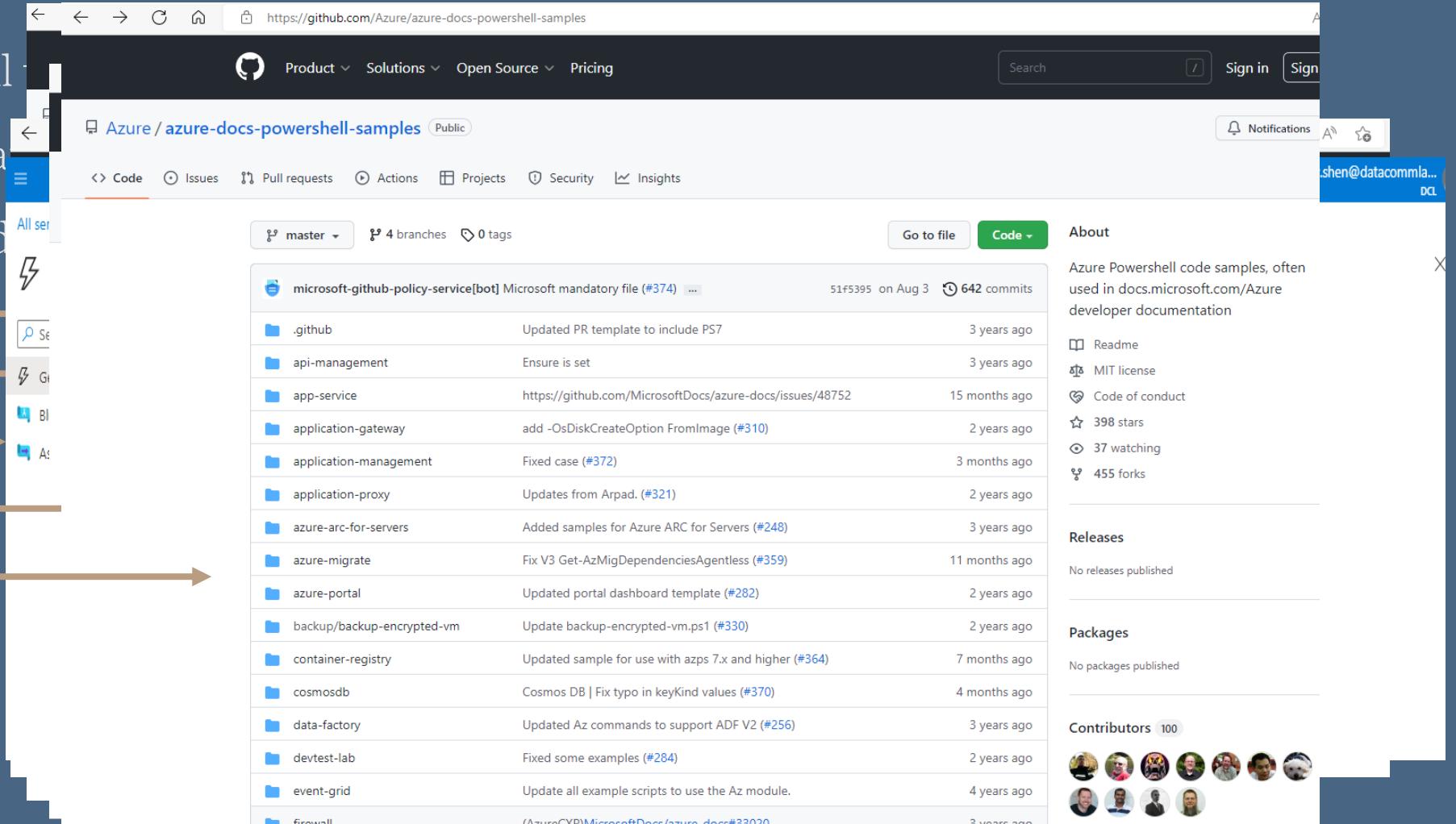
*Bicep*

*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

All services >

## Microsoft Defender for Cloud | Overview

Showing subscription 'DCL Pearland 2020'

Search (Ctrl+ /) Subscriptions What's new

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Firewall Manager

Management

- Environment settings
- Security solutions
- Workflow automation

**1** Azure subscriptions **6** Assessed resources **11** Active recommendations **--** Security alerts

### Security posture

11/11 Unassigned recommendation 0/0 Overdue recommendations

Secure score: 44% SECURE SCORE

Azure	44%
AWS	-
GCP	-

Explore your security posture >

### Regulatory compliance

Azure Security Benchmark New 27 of 43 passed controls

Lowest compliance regulatory standards by passed controls

ISO 27001	12/20
PCI DSS 3.2.1	35/43
SOC TSP	13/13

Improve your compliance >

### Workload protections

### Firewall Manager

# Design Component – Defender for Cloud

All services > Microsoft Defender for Cloud

## Microsoft Defender for Cloud | Recommendations

Showing subscription 'DCL Pearland 2020'

Search (Ctrl+ /) Refresh Download CSV report Open query Governance report (preview) Guides & Feedback

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Secure score recommendations All recommendations

Secure score 44% Active items Resource health Governance (preview)

Controls 3/7 Recommendations 11/27

Resource health: Unhealthy (3) Healthy (0) Not applicable (2)

Azure AWS GCP

Overdue recommendations 0/0 Unassigned recommendations 11/11

Show my items only (preview): Off

Search recommendations Recommendation status == None Severity == None Resource type == None Add filter

More (2)

Name	Max score	Current score	Potential score increase	Status	Unhealthy resources	Insights
Enable MFA	10	0.00	+ 56%	Unassigned	1 of 1 resources	<div style="width: 56%; background-color: red;"></div>
Encrypt data in transit	4	4.00	<div style="width: 100%; background-color: blue;"></div>	Completed	0 of 1 resources	<div style="width: 100%; background-color: green;"></div>
Manage access and permissions	4	4.00	<div style="width: 100%; background-color: blue;"></div>	Completed	0 of 2 resources	<div style="width: 50%; background-color: green;"></div>
Enable enhanced security features	Not scored	Not scored		Unassigned	1 of 1 resources	<div style="width: 0%; background-color: red;"></div>
Implement security best practices	Not scored	Not scored		Unassigned	2 of 2 resources	<div style="width: 0%; background-color: red;"></div>
Restrict unauthorized network access	Not scored	Not scored		Unassigned	0 of 1 resources	<div style="width: 0%; background-color: grey;"></div>
Remediate security configurations	Not scored	Not scored		Completed	0 of 1 resources	<div style="width: 0%; background-color: grey;"></div>

# Design Component – Defender for Cloud

All services > Microsoft Defender for Cloud

## Microsoft Defender for Cloud | Security alerts

Showing subscription 'DCL Pearland 2020'

Search (Ctrl+ /) Refresh Change status Open query Suppression rules Security alerts map Sample alerts Alerts workbook Download CSV report Guides & Feedback

General

- Active alerts: 0
- Affected resources: 0

Search by ID, IP, title, or affected resource

Subscription == All Status == Active Severity == Low, Medium, High Add filter

No grouping

Severity Alert title Affected resource Resource Group Activity start time (UTC-5) MITRE ATT&CK® tactics Status

No alerts found

< Previous Page 1 of 0 Next >

# Design Component – Defender for Cloud

All services > Microsoft Defender for Cloud

## Microsoft Defender for Cloud | Inventory

Showing subscription 'DCL Pearland 2020'

Search (Ctrl+ /) Refresh Add non-Azure servers Open query Assign tags Download CSV report Trigger logic app Learn more Guides & Feedback

General

Filter by name Subscriptions == All Resource Groups == All Resource types == All Defender for Cloud == All Monitoring agent == All Environment == All

Recommendations == All Installed applications == All Add filter

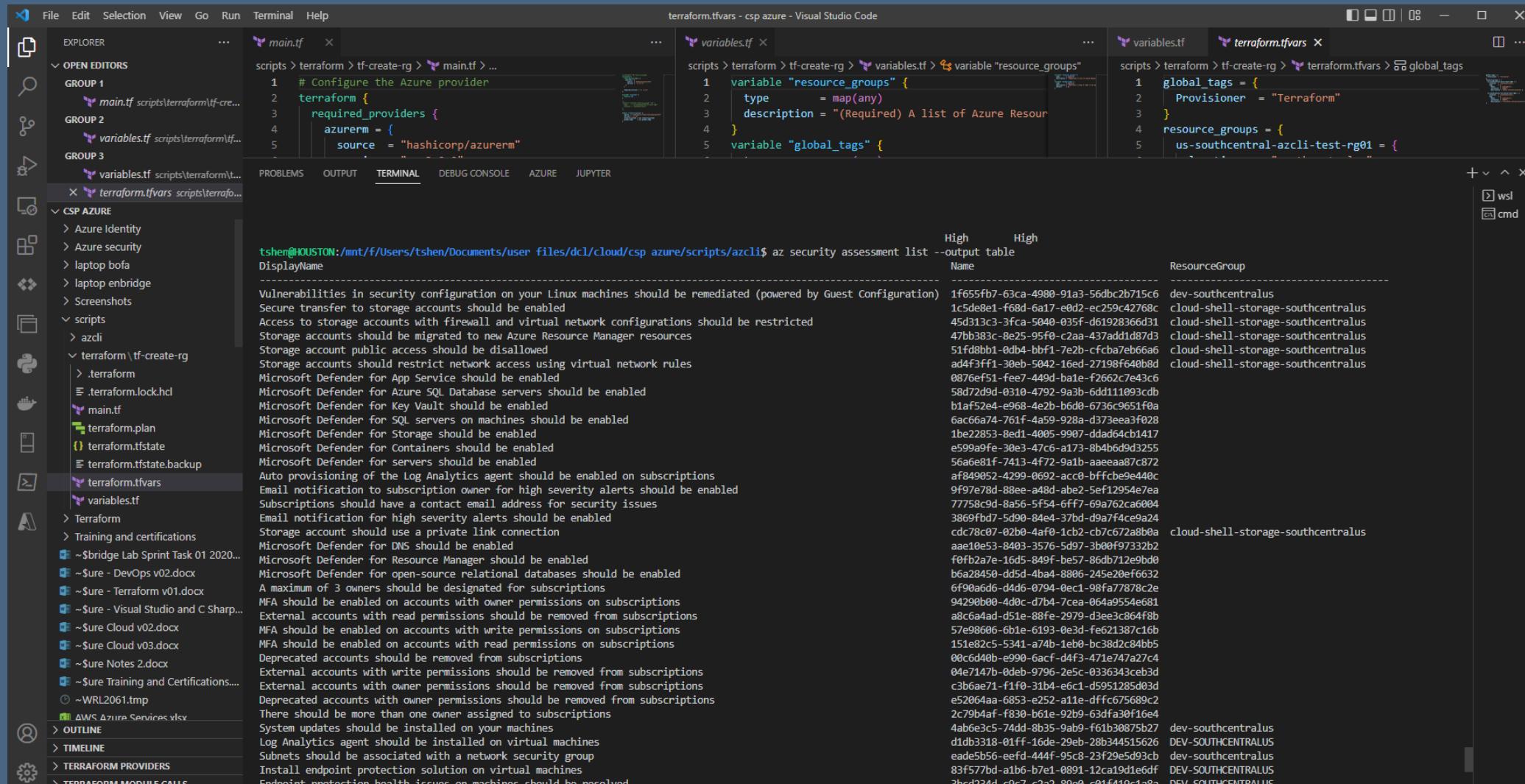
Total resources: 6 Unhealthy resources: 4 Unmonitored resources: 0 Unregistered subscriptions: 0

Resource name ↑↓	Resource type ↑↓	Subscription ↑↓	Monitoring agent ↑↓	Defender for Cloud ↑↓	Recommendations ↑↓
<input type="checkbox"/> DCL Pearland 2020	Subscription	DCL Pearland 2020	Partial	<div style="width: 20%; background-color: red;"></div>	<div style="width: 80%; background-color: green;"></div> ...
<input type="checkbox"/> ubun2001	Virtual machines	DCL Pearland 2020	Installed	<div style="width: 100%; background-color: red;"></div>	<div style="width: 0%; background-color: green;"></div> ...
<input type="checkbox"/> cs710032000a6ae30e3	Storage accounts	DCL Pearland 2020	Off	<div style="width: 20%; background-color: red;"></div>	<div style="width: 80%; background-color: green;"></div> ...
<input type="checkbox"/> loganalyticsworkspace01ussc	Log Analytics workspaces	DCL Pearland 2020	On	<div style="width: 100%; background-color: red;"></div>	<div style="width: 0%; background-color: green;"></div> ...
<input type="checkbox"/> dev-southcentralus-vnet	Virtual networks	DCL Pearland 2020	Off	<div style="width: 80%; background-color: green;"></div>	<div style="width: 20%; background-color: red;"></div> ...
<input type="checkbox"/> default	Subnets	DCL Pearland 2020	On	<div style="width: 0%; background-color: green;"></div>	<div style="width: 100%; background-color: red;"></div> ...

Previous Page 1 of 1 Next

**Download CSV report** (highlighted with a red box)

# Design Component – Defender for Cloud

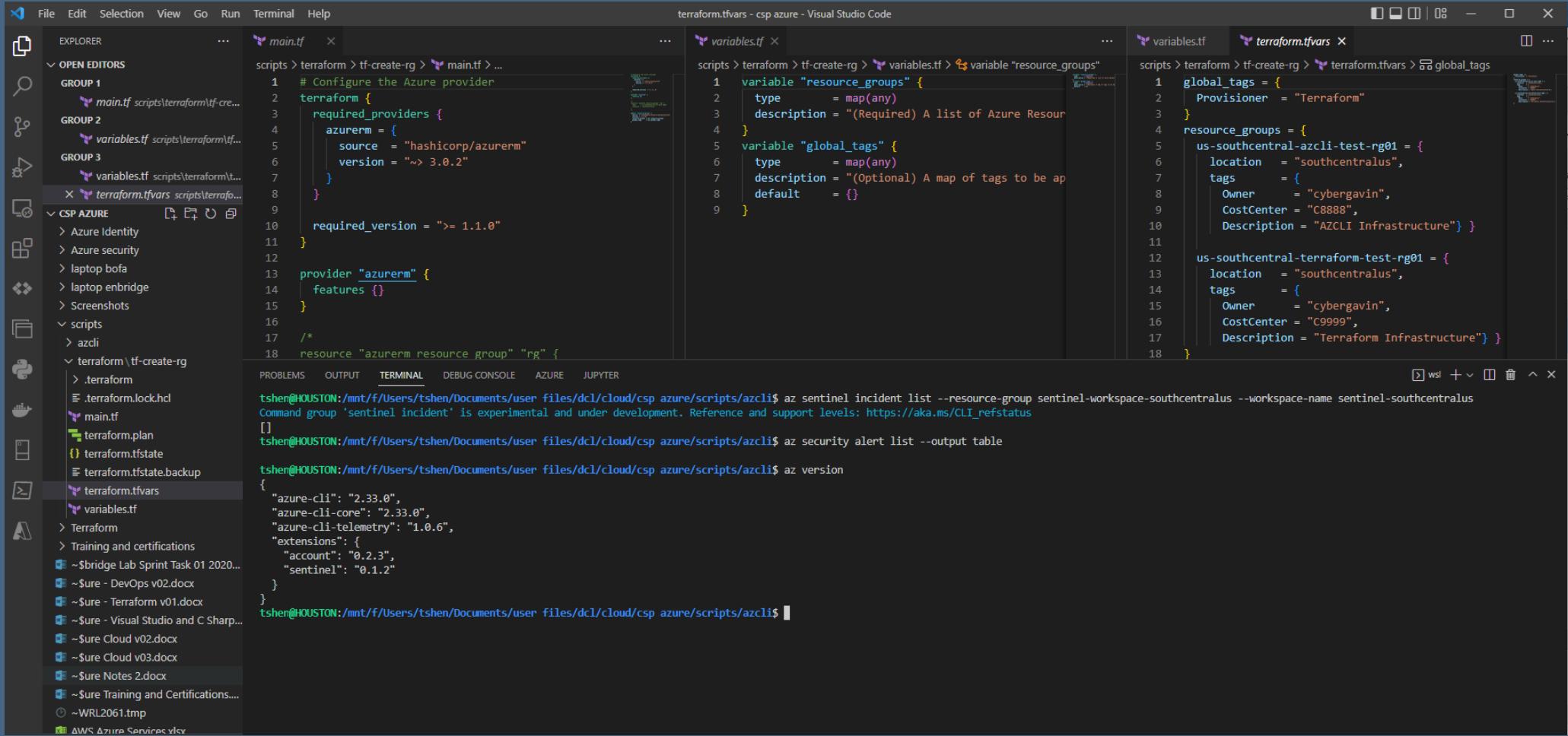


The screenshot shows a Visual Studio Code interface with several tabs open:

- EXPLORER**: Shows the file structure, including `main.tf`, `variables.tf`, and `terraform.tfvars`.
- main.tf**: Terraform configuration for the Azure provider.
- variables.tf**: Terraform configuration for resource groups and global tags.
- terraform.tfvars**: Terraform variable file.
- TERMINAL**: An Azure CLI terminal showing the output of the command `az security assessment list --output table`. The output lists various security recommendations across different Azure resources and their corresponding resource groups.

High	High	
DisplayName	Name	ResourceGroup
Vulnerabilities in security configuration on your Linux machines should be remediated (powered by Guest Configuration)	1f655fb7-63ca-4980-91a3-56dbc2b715c6	dev-southcentralus
Secure transfer to storage accounts should be enabled	1c5de8e1-f68d-6a17-e0d2-ec259c42768c	cloud-shell-storage-southcentralus
Access to storage accounts with firewall and virtual network configurations should be restricted	45d313c3-3fca-5040-035f-d61928366d31	cloud-shell-storage-southcentralus
Storage accounts should be migrated to new Azure Resource Manager resources	47bb383c-8e25-95f0-c2a3-437add1d87d3	cloud-shell-storage-southcentralus
Storage account public access should be disallowed	51fd8bb1-0d4b-bbf1-7e2b-cfcba7eb6a6	cloud-shell-storage-southcentralus
Storage accounts should restrict network access using virtual network rules	ad4f3ff1-30eb-5042-16ed-27198f640b8d	cloud-shell-storage-southcentralus
Microsoft Defender for App Service should be enabled	ad76ef51-fe07-449d-ba1e-f2662c7e43c6	
Microsoft Defender for Azure SQL Database servers should be enabled	5872d9d-0310-4792-9a3b-6dd111093cd8	
Microsoft Defender for Key Vault should be enabled	b1af52e4-e968-4e2b-b6d0-6736c9651f0a	
Microsoft Defender for SQL servers on machines should be enabled	6ac66a74-761f-4a59-928a-d373ea3f028	
Microsoft Defender for Storage should be enabled	1be2853-8ed1-4085-9907-dad64cb1417	
Microsoft Defender for Containers should be enabled	e599a9fe-30e3-47c6-a173-8b4b6d9d3255	
Microsoft Defender for servers should be enabled	56a6e81f-7413-4f72-9a1b-aeeaa87c872	
Auto provisioning of the Log Analytics agent should be enabled on subscriptions	af849052-4299-0692-ac08-bfffcbe9e440c	
Email notification to subscription owner for high severity alerts should be enabled	9f97e78d-88ee-a48d-abef-5ef12954e7ea	
Subscriptions should have a contact email address for security issues	77758c9d-8a56-5f54-6fff-69a762ca0004	
Email notification for high severity alerts should be enabled	3869fb7d-5d90-84e4-37bd-d9a7f4ce9a24	
Storage account should use a private link connection	cdc78c07-02b0-4af0-1cb2-cb7c672a8b0a	cloud-shell-storage-southcentralus
Microsoft Defender for DNS should be enabled	aae10e53-8403-3576-5d97-3b00f9732b2b	
Microsoft Defender for Resource Manager should be enabled	f0fb2a7e-16d5-849f-be57-86db712e9bd0	
Microsoft Defender for open-source relational databases should be enabled	b6a28450-dd5d-4ba4-8866-245e20ef6632	
A maximum of 3 owners should be designated for subscriptions	6f90a6d6-d4d6-0794-0ec1-98fa77878c2e	
MFA should be enabled on accounts with owner permissions on subscriptions	94290b00-4d8c-d7b4-7cea-064a9554e681	
External accounts with read permissions should be removed from subscriptions	a8c6a4ad-d51e-88fe-2979-d3ee3c864f8b	
MFA should be enabled on accounts with write permissions on subscriptions	57e98e06-6b1e-6193-0e3d-fe621387c16b	
MFA should be enabled on accounts with read permissions on subscriptions	151e82c5-5341-a74b-1eb0-bc38d2c84bb5	
Deprecated accounts should be removed from subscriptions	00c6d40b-e990-6acf-d4f3-471e747a27c4	
External accounts with write permissions should be removed from subscriptions	04e7147b-0deb-9796-2e5c-033634ceb3d	
External accounts with owner permissions should be removed from subscriptions	c3b2ae71-f1f0-31b4-e6c1-d5951285d03d	
Deprecated accounts with owner permissions should be removed from subscriptions	e52064aa-6853-e252-a11e-dffcc675689c2	
There should be more than one owner assigned to subscriptions	2c79b4af-f830-b61e-92b9-63dfa30f16e4	
System updates should be installed on your machines	4ab6e3c5-74dd-8b35-9ab9-f61b30875b27	dev-southcentralus
Log Analytics agent should be installed on virtual machines	d1db3318-01ff-16de-29eb-28b34515626	DEV-SOUTHCENTRALUS
Subnets should be associated with a network security group	eade5b56-eefd-444f-95c8-23f29e5d93cb	dev-southcentralus
Install endpoint protection solution on virtual machines	83f577bd-a1b6-b7e1-0891-12ca19d1e6df	DEV-SOUTHCENTRALUS
Endpoint protection health issues on machines should be resolved	3bcd234d-c9c7-c2a2-89e0-c01f419c1a8a	DEV-SOUTHCENTRALUS

# Design Component – Defender for Cloud



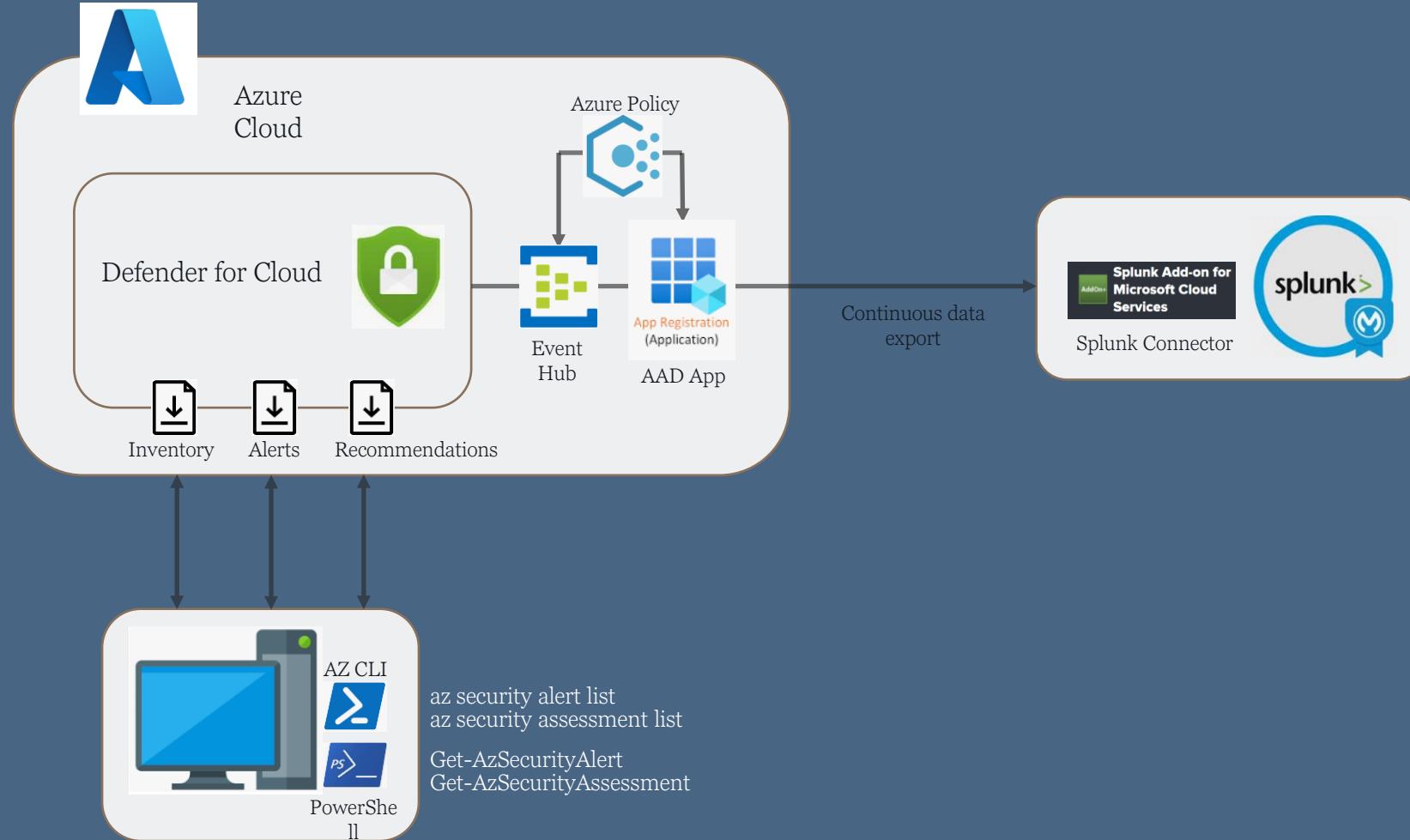
The screenshot shows a Visual Studio Code interface with four tabs open:

- main.tf**: Terraform configuration for creating a resource group. It includes provider declarations for Azure and azurerm, and a resource block for an azurerm resource group.
- variables.tf**: Terraform variable definitions for resource groups and global tags.
- variables.tf**: Another Terraform variable definition for global tags.
- terraform.tfvars**: Terraform variable file containing global tags and resource group configurations.

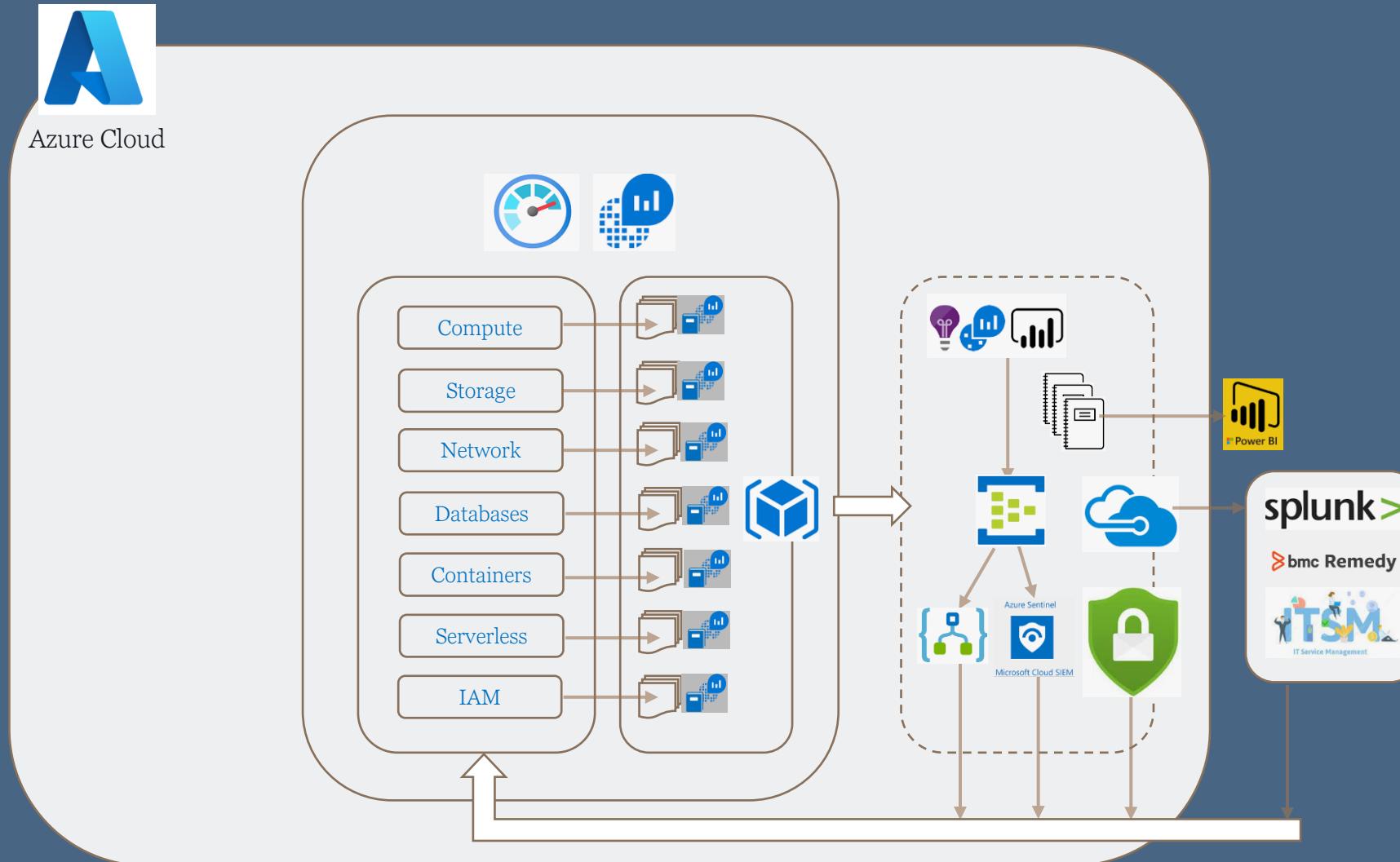
The terminal tab shows Azure CLI commands being run:

```
tschen@HOUSTON:/mnt/f/Users/tshen/Documents/user_files/dcl/cloud/csp_azure/scripts/azcli$ az sentinel incident list --resource-group sentinel-workspace-southcentralus --workspace-name sentinel-southcentralus
Command group 'sentinel incident' is experimental and under development. Reference and support levels: https://aka.ms/CLI\_refstatus
[]
tschen@HOUSTON:/mnt/f/Users/tshen/Documents/user_files/dcl/cloud/csp_azure/scripts/azcli$ az security alert list --output table
tschen@HOUSTON:/mnt/f/Users/tshen/Documents/user_files/dcl/cloud/csp_azure/scripts/azcli$ az version
{
  "azure-cli": "2.33.0",
  "azure-cli-core": "2.33.0",
  "azure-cli-telemetry": "1.0.6",
  "extensions": {
    "account": "0.2.3",
    "sentinel": "0.1.2"
  }
}
tschen@HOUSTON:/mnt/f/Users/tshen/Documents/user_files/dcl/cloud/csp_azure/scripts/azcli$
```

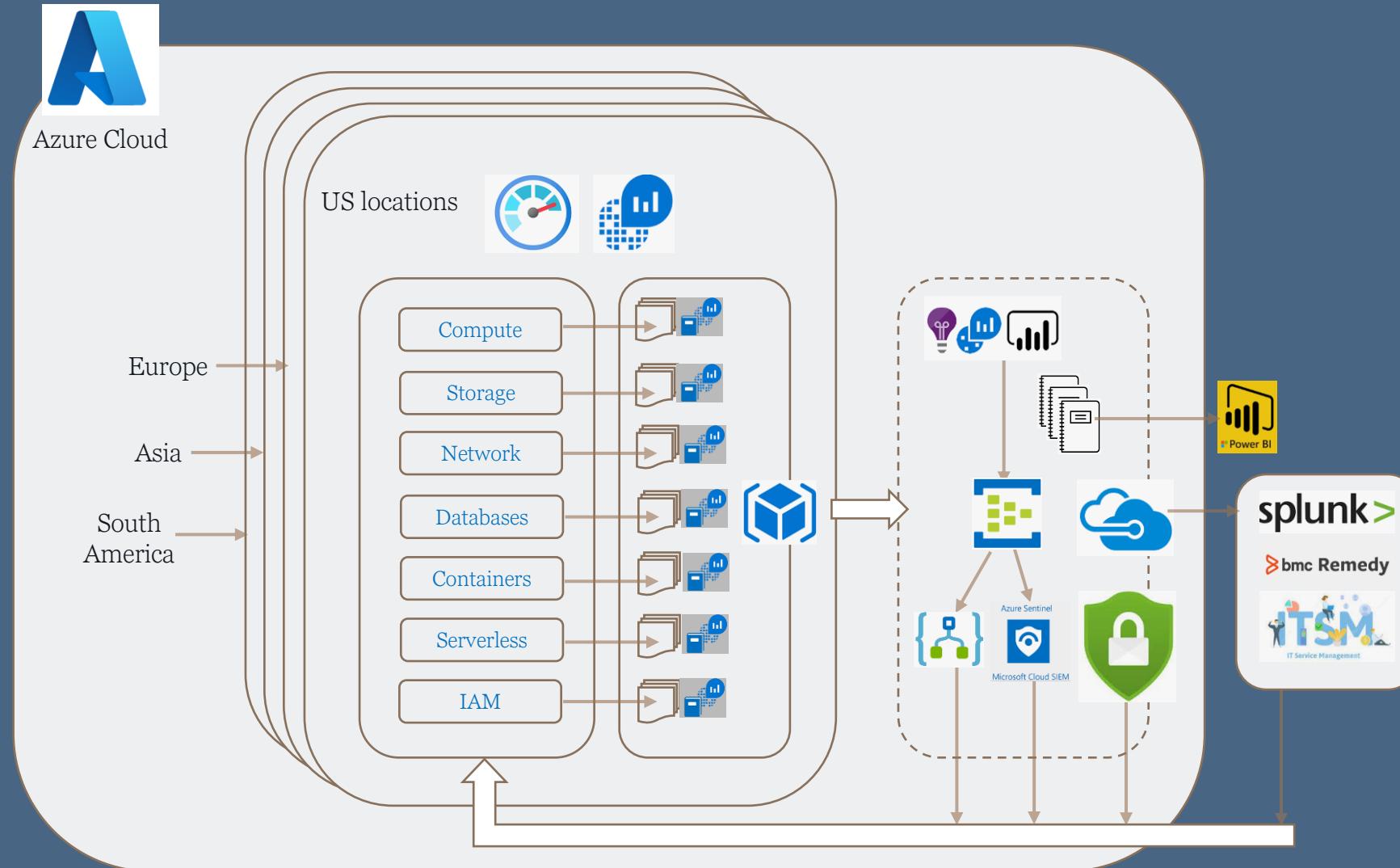
# Design Component – Defender for Cloud



# Design Component – Defender for Cloud



# Design Component – Defender for Cloud



# 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

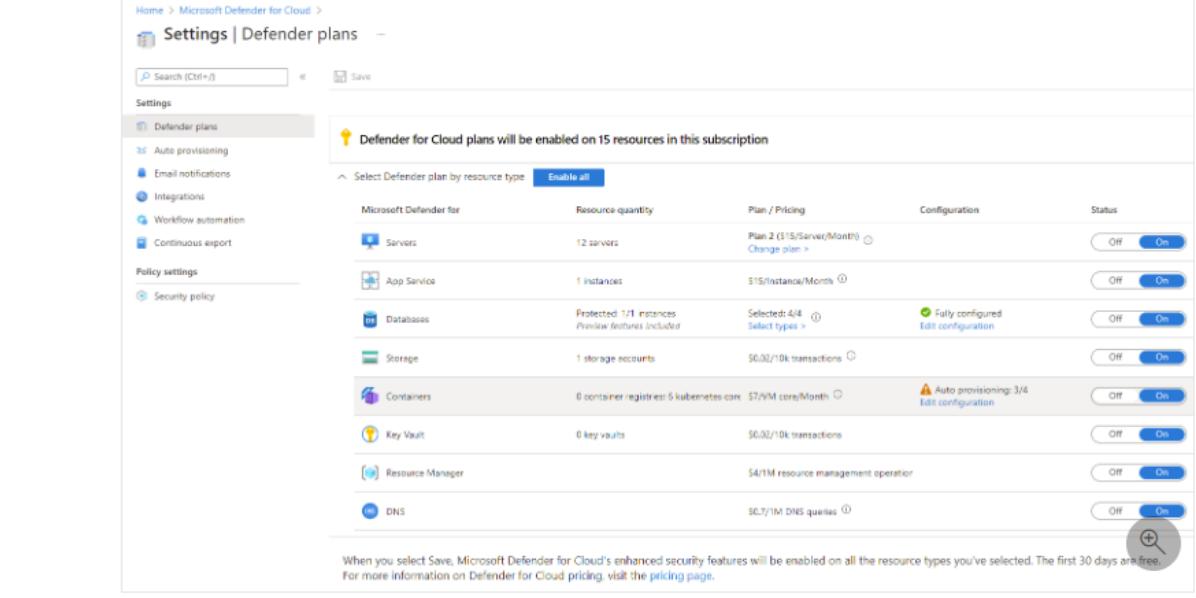
- Microsoft Defender for Endpoint - Microsoft Defender for Servers includes [Microsoft Defender for Endpoint](#) for comprehensive endpoint detection and response (EDR). Learn more about the benefits of using Microsoft Defender for Endpoint together with Defender for Cloud in [Use Defender for Cloud's 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**.



Home > Microsoft Defender for Cloud > Settings | Defender plans

Defender for Cloud plans will be enabled on 15 resources in this subscription

Select Defender plan by resource type: **Enable all**

Microsoft Defender for	Resource quantity	Plan / Pricing	Configuration	Status
Servers	12 servers	Plan 2 (\$15/Server/Month) <a href="#">Change plan &gt;</a>	<span>Off</span> <span>On</span>	
App Service	1 instances	\$15/instance/Month	<span>Off</span> <span>On</span>	
Databases	Protected: 1/1 instances Preview features included	Selected: 4/4 <a href="#">Select types &gt;</a>	<span>Fully configured</span> <a href="#">Edit configuration</a>	<span>Off</span> <span>On</span>
Storage	1 storage accounts	\$0.00/10k transactions	<span>Off</span> <span>On</span>	
Containers	0 container registries: 6 kubernetes core	\$7/VM core/Month <a href="#">Edit configuration</a>	<span>Auto provisioning: 3/4</span>	<span>Off</span> <span>On</span>
Key Vault	0 key vaults	\$0.00/10k transactions	<span>Off</span> <span>On</span>	
Resource Manager	0 resource management operations	\$4/1M resource management operation	<span>Off</span> <span>On</span>	
DNS	0.7/1M DNS queries	\$0.7/1M DNS queries	<span>Off</span> <span>On</span>	

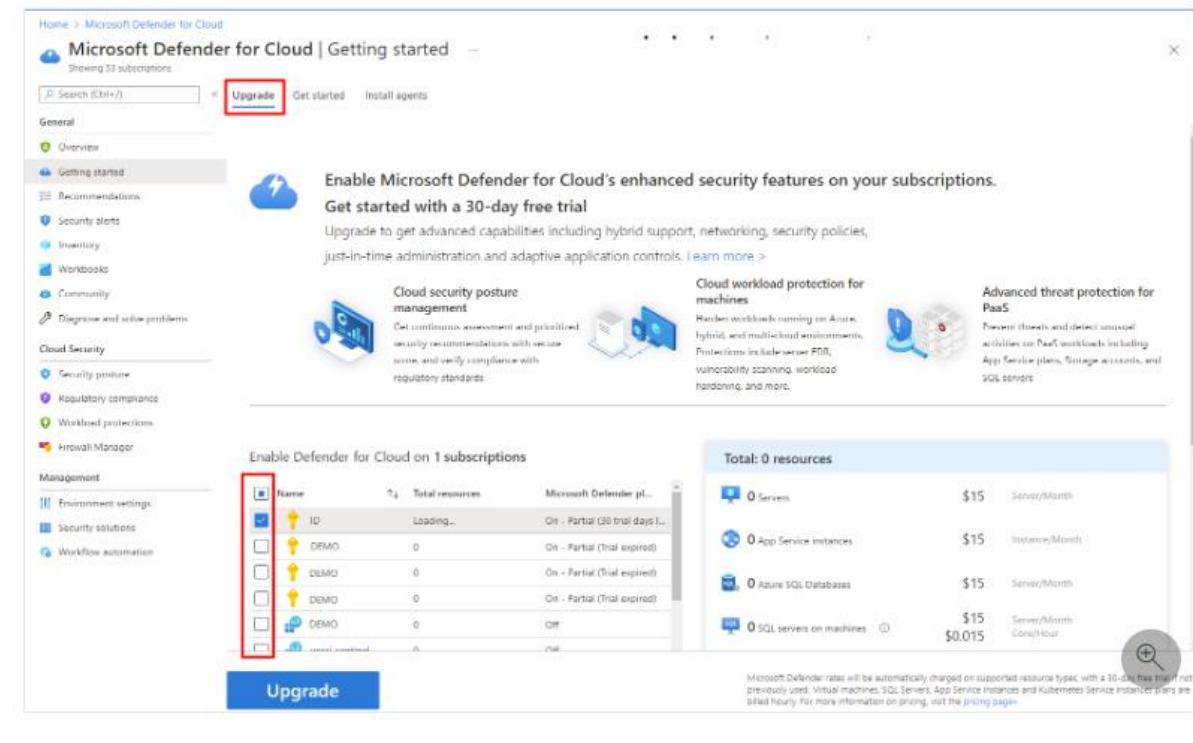
When you select Save, Microsoft Defender for Cloud's enhanced security features will be enabled on all the resource types you've selected. The first 30 days are free. For more information on Defender for Cloud pricing, visit the [pricing page](#).

# 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.



The screenshot shows the Microsoft Defender for Cloud interface. The left sidebar has a 'Getting started' tab selected, indicated by a red box. The main content area is titled 'Enable Microsoft Defender for Cloud's enhanced security features on your subscriptions.' It features a '30-day free trial' offer and three service highlights: 'Cloud security posture management', 'Cloud workload protection for machines', and 'Advanced threat protection for PaaS'. Below this, a table lists '1 subscriptions' with a red box highlighting the first row. The table columns are 'Name', 'Total resources', and 'Microsoft Defender pl...'. The first row shows 'ID' with 'Loading...' under 'Total resources' and 'On - Partial (30 trial days left)' under 'Microsoft Defender pl...'. The 'Upgrade' button at the bottom is also highlighted with a red box.

Name	Total resources	Microsoft Defender pl...
ID	Loading...	On - Partial (30 trial days left)
DEMO	0	On - Partial (Trial expired)
DEMO	0	On - Partial (Trial expired)
DEMO	0	On - Partial (Trial expired)
DEMO	0	Off
DEMO	0	Off

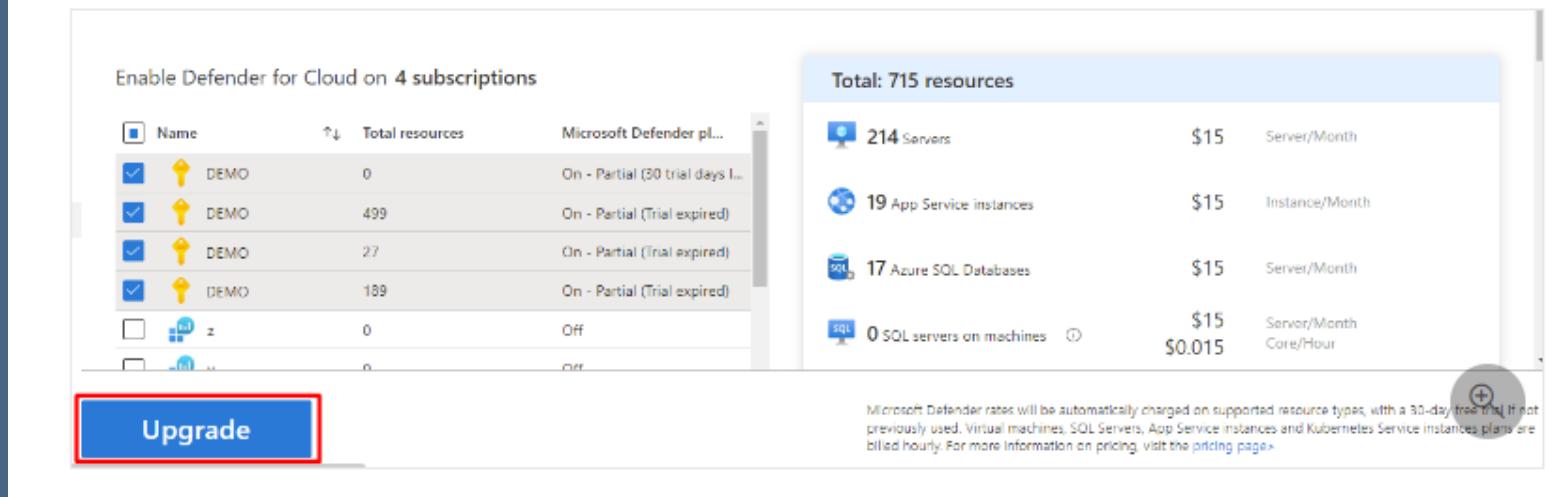
**Upgrade**

# 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.



The screenshot shows the 'Enable Defender for Cloud on 4 subscriptions' interface. On the left, a table lists four subscriptions named 'DEMO' with varying resource counts (0, 499, 27, 189) and Microsoft Defender protection status (On - Partial or Off). An 'Upgrade' button is highlighted with a red box. On the right, a summary table shows 'Total: 715 resources' with details for 214 servers, 19 App Service instances, 17 Azure SQL Databases, and 0 SQL servers on machines. Pricing is listed as \$15 per Server/Month for servers and \$15 per Instance/Month for App Service instances. A note at the bottom states: 'Microsoft Defender rates will be automatically charged on supported resource types, with a 30-day free trial if not previously used. Virtual machines, SQL Servers, App Service instances and Kubernetes Service instances plans are billed hourly. For more information on pricing, visit the [pricing page](#).<sup>1</sup>'

Name	Total resources	Microsoft Defender pl...
DEMO	0	On - Partial (30 trial days l...
DEMO	499	On - Partial (Trial expired)
DEMO	27	On - Partial (Trial expired)
DEMO	189	On - Partial (Trial expired)
z	0	Off
u	0	Off

**Upgrade**

Total: 715 resources

Resource Type	Count	Price	Unit
214 Servers	\$15	Server/Month	
19 App Service instances	\$15	Instance/Month	
17 Azure SQL Databases	\$15	Server/Month	
0 SQL servers on machines	\$0.015	Server/Month Core/Hour	

Microsoft Defender rates will be automatically charged on supported resource types, with a 30-day free trial if not previously used. Virtual machines, SQL Servers, App Service instances and Kubernetes Service instances plans are billed hourly. For more information on pricing, visit the [pricing page](#).<sup>1</sup>

# Design Component – Defender for Cloud

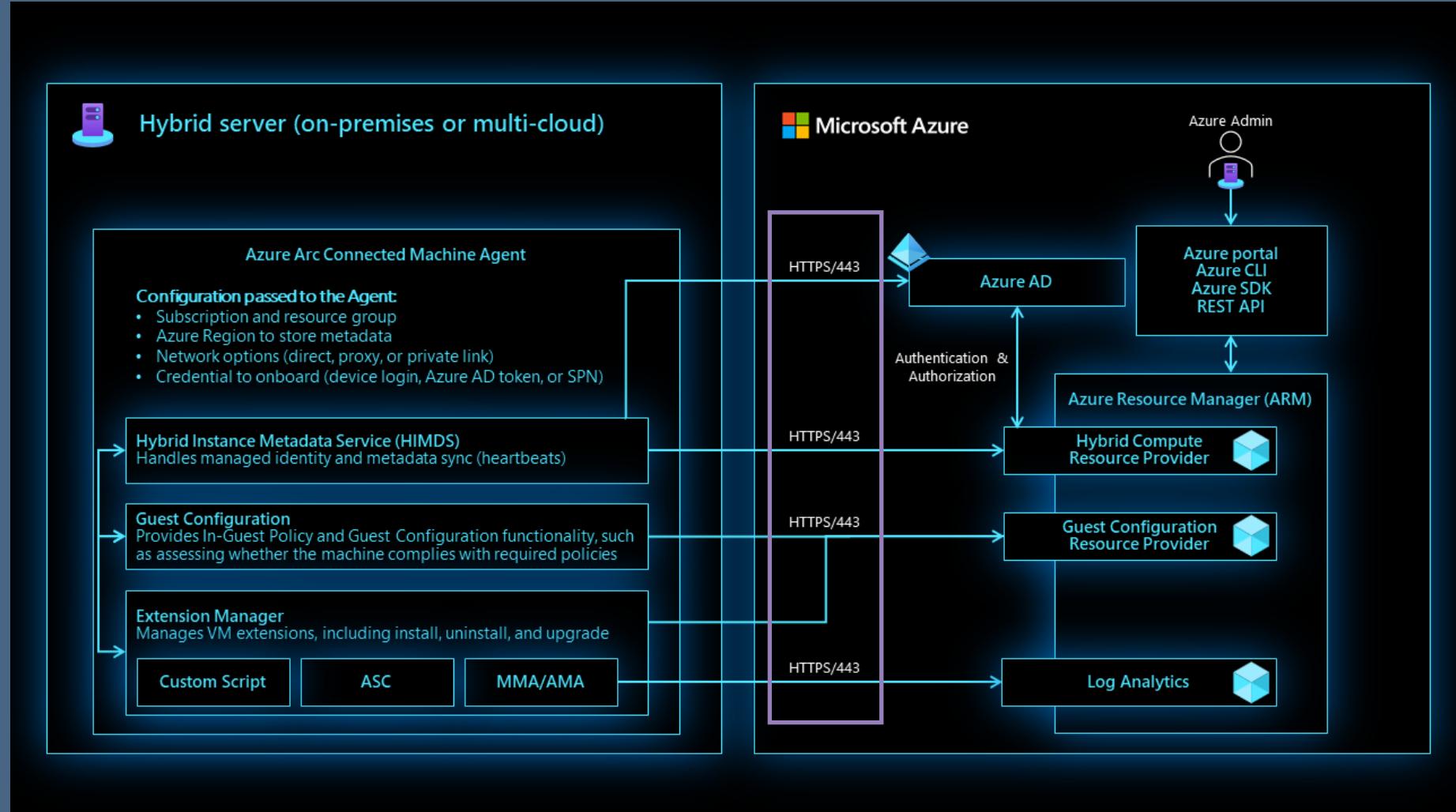
DFC covers non-Azure servers by agents

Arc-Enabled Servers



# Design Component – Defender for Cloud

DFC communicates with agents and supporting services via HTTPS/443

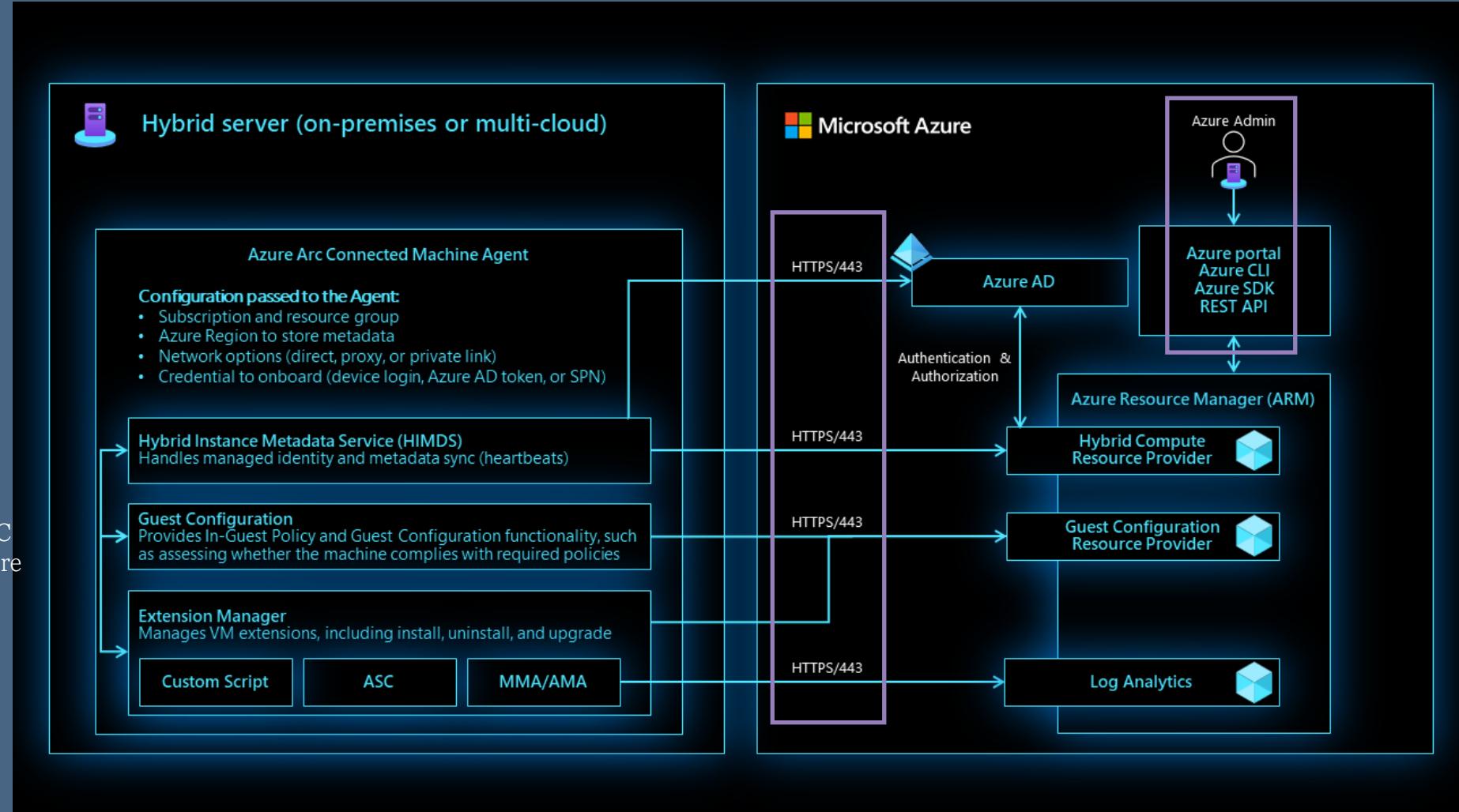


DFC covers non-Azure servers by agents

# 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



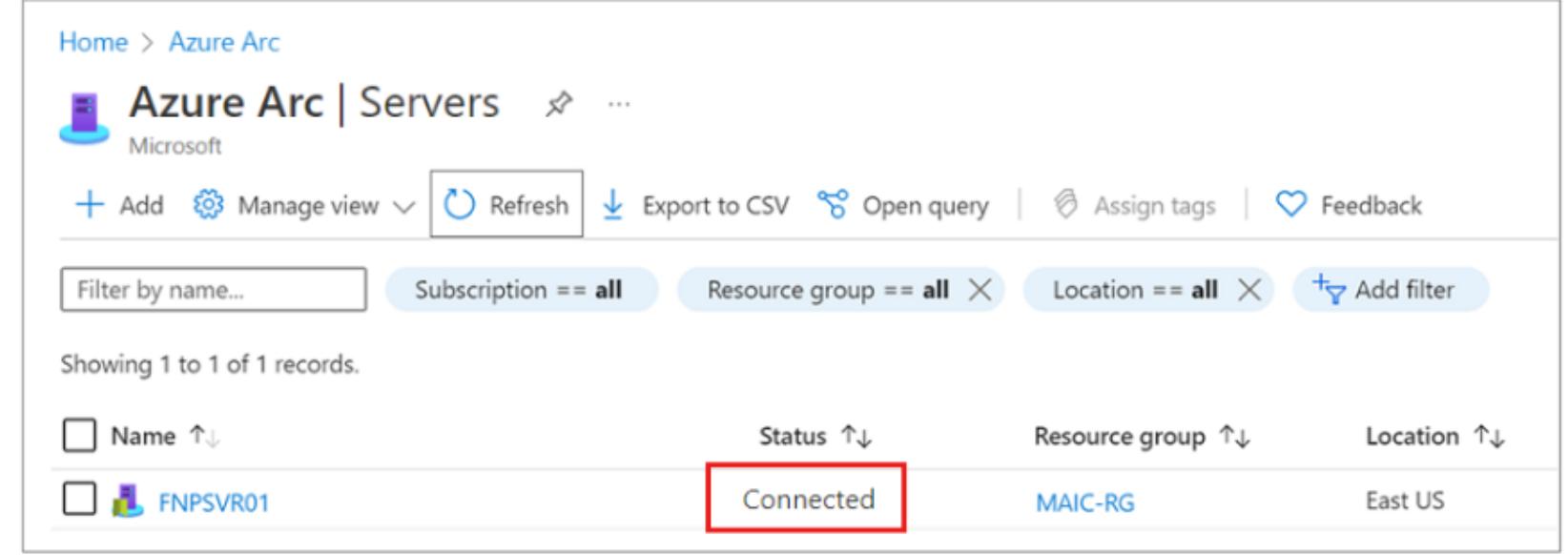
DFC covers non-Azure servers by agents

# Design Component – Defender for Cloud

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

## Verify the connection with Azure Arc

After you install the agent and configure it to connect to Azure Arc-enabled servers, go to the Azure portal to verify that the server has successfully connected. View your machine in the [Azure portal](#).



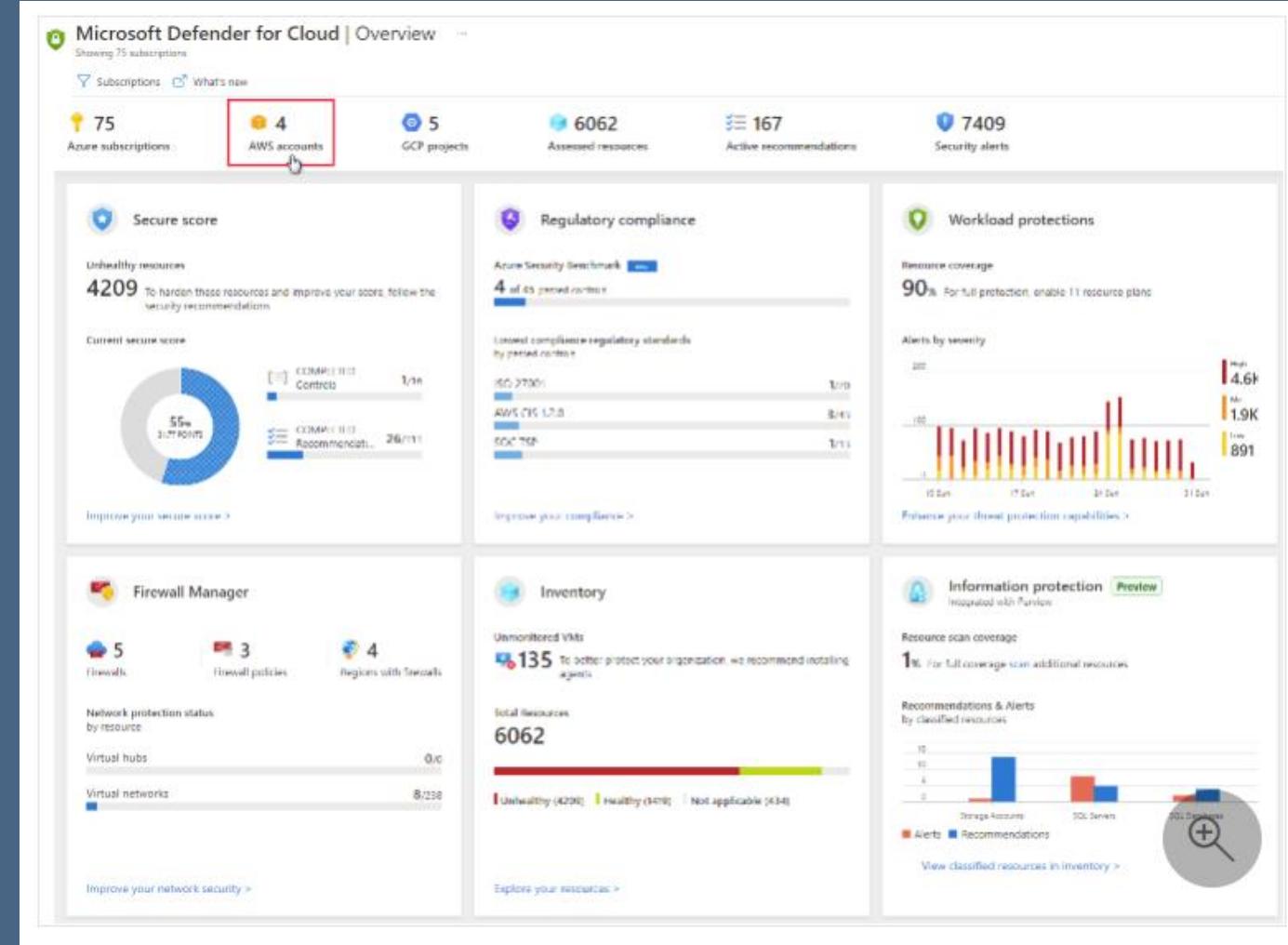
The screenshot shows the Azure Arc | Servers blade in the Azure portal. The top navigation bar includes 'Home > Azure Arc' and the 'Azure Arc | Servers' title. Below the title are buttons for 'Add', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', and 'Feedback'. There are also filters for 'Filter by name...', 'Subscription == all', 'Resource group == all', and 'Location == all'. The main table displays one record: 'FNPSVR01'. The 'Status' column for this record is highlighted with a red box and contains the value 'Connected'. The 'Resource group' column shows 'MAIC-RG' and the 'Location' column shows 'East US'.

Name	Status	Resource group	Location
FNPSVR01	Connected	MAIC-RG	East US

DFC covers non-Azure servers by agents

# Design Component – Defender for Cloud

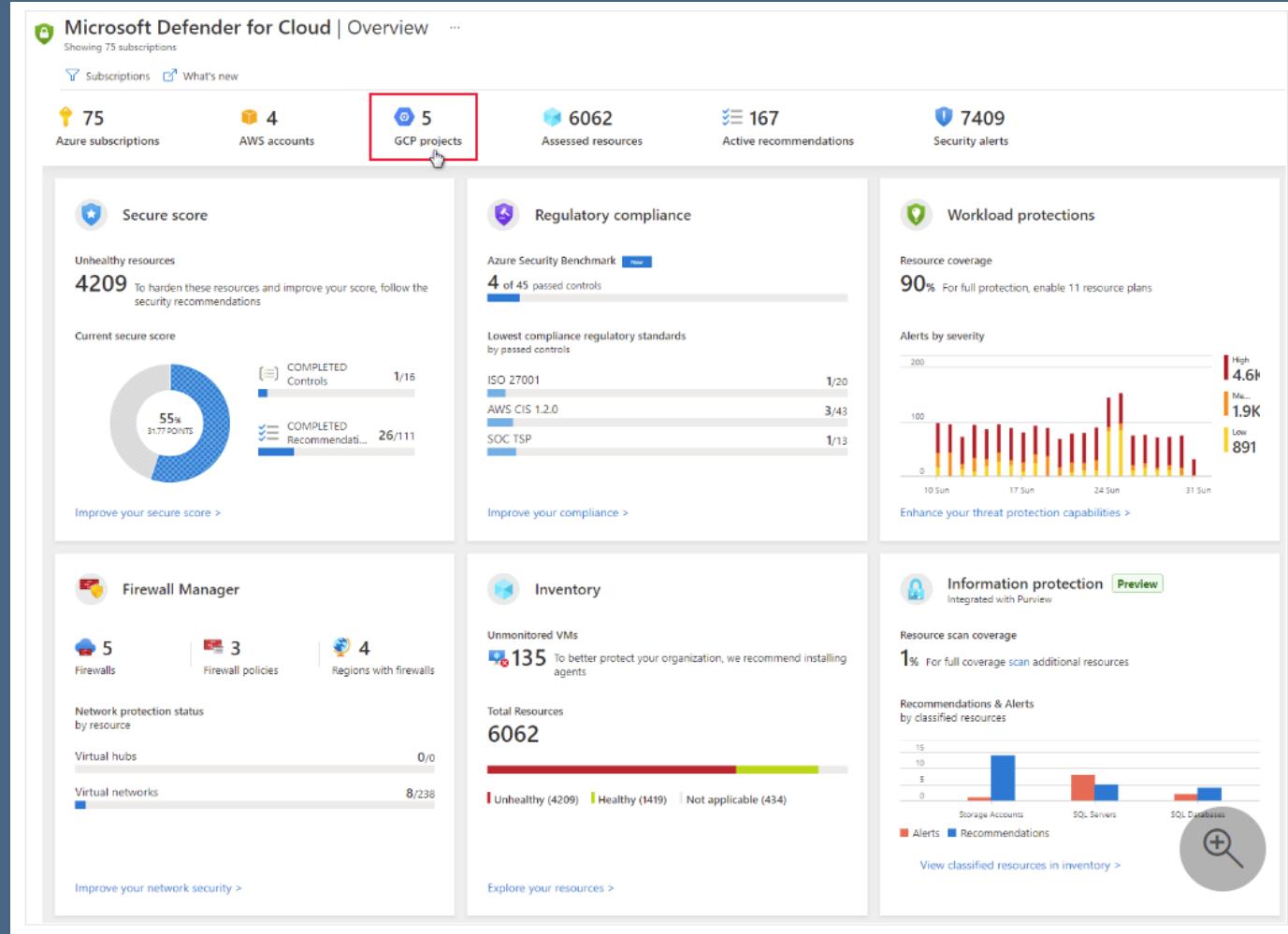
Example of AWS inventory



DFC covers non-Azure servers by agents

# Design Component – Defender for Cloud

Example of GCP inventory



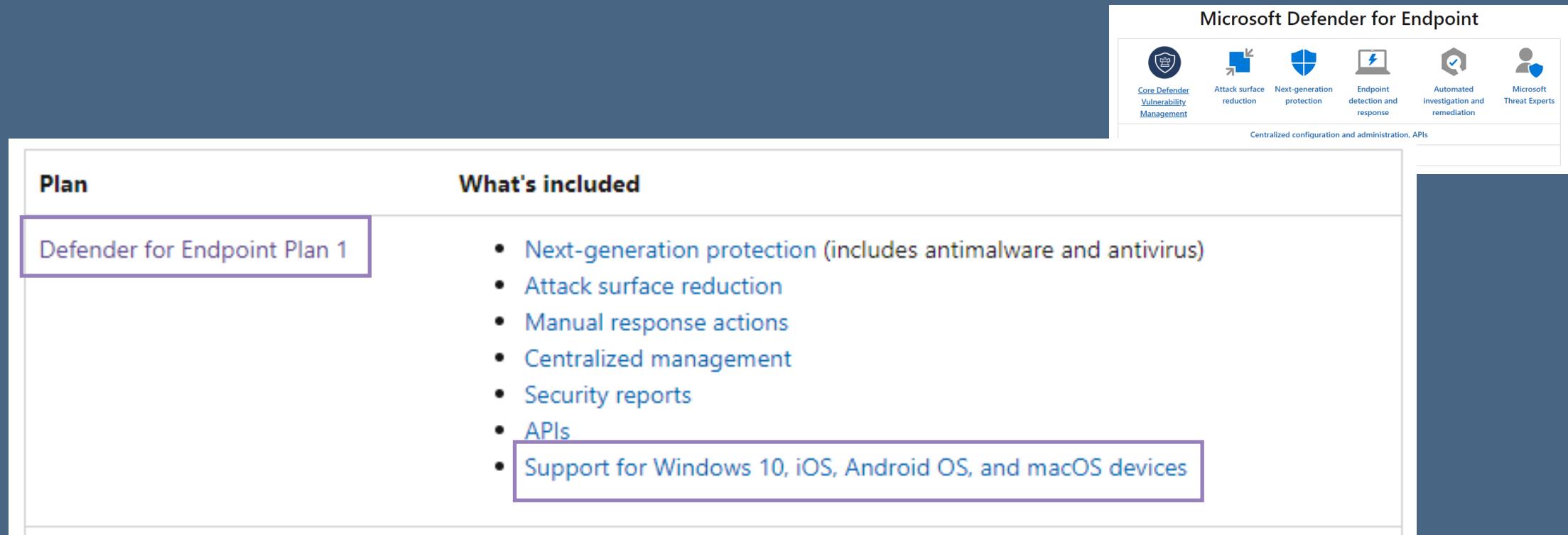
DFC covers non-Azure servers by agents

# Design Component – Defender for Cloud



MDE is device/server centric

# Design Component – Defender for Cloud



The screenshot shows the Microsoft Defender for Endpoint service page. At the top, there is a navigation bar with icons for Core Defender, Vulnerability Management, Attack surface reduction, Next-generation protection, Endpoint detection and response, Automated investigation and remediation, and Microsoft Threat Experts. Below the navigation bar, a sub-header reads "Centralized configuration and administration, APIs". The main content area is divided into two sections: "Plan" and "What's included". The "Plan" section is currently selected and displays "Defender for Endpoint Plan 1". The "What's included" section lists the following features:

- 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



The screenshot shows a Microsoft Azure documentation page. The URL in the address bar is [Azure / Security / Microsoft Defender for Cloud /](#). The main title is **Overview of Microsoft Defender for Servers**. Below the title, the text reads: "Article • 06/27/2022 • 8 minutes to read • 5 contributors". There are like and dislike buttons on the right. A callout box highlights: "Microsoft Defender for Servers is one of the enhanced security features of Microsoft Defender for Cloud. Use it to add threat detection and advanced defenses to your Windows and Linux machines whether they're running in Azure, AWS, GCP, and on-premises environment." Below this, a section discusses protecting hybrid and multicloud environments using Azure Arc, with links to quickstarts for non-Azure and AWS connections. The text states: "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".

Azure / Security / Microsoft Defender for Cloud /

## Overview of Microsoft Defender for Servers

Article • 06/27/2022 • 8 minutes to read • 5 contributors

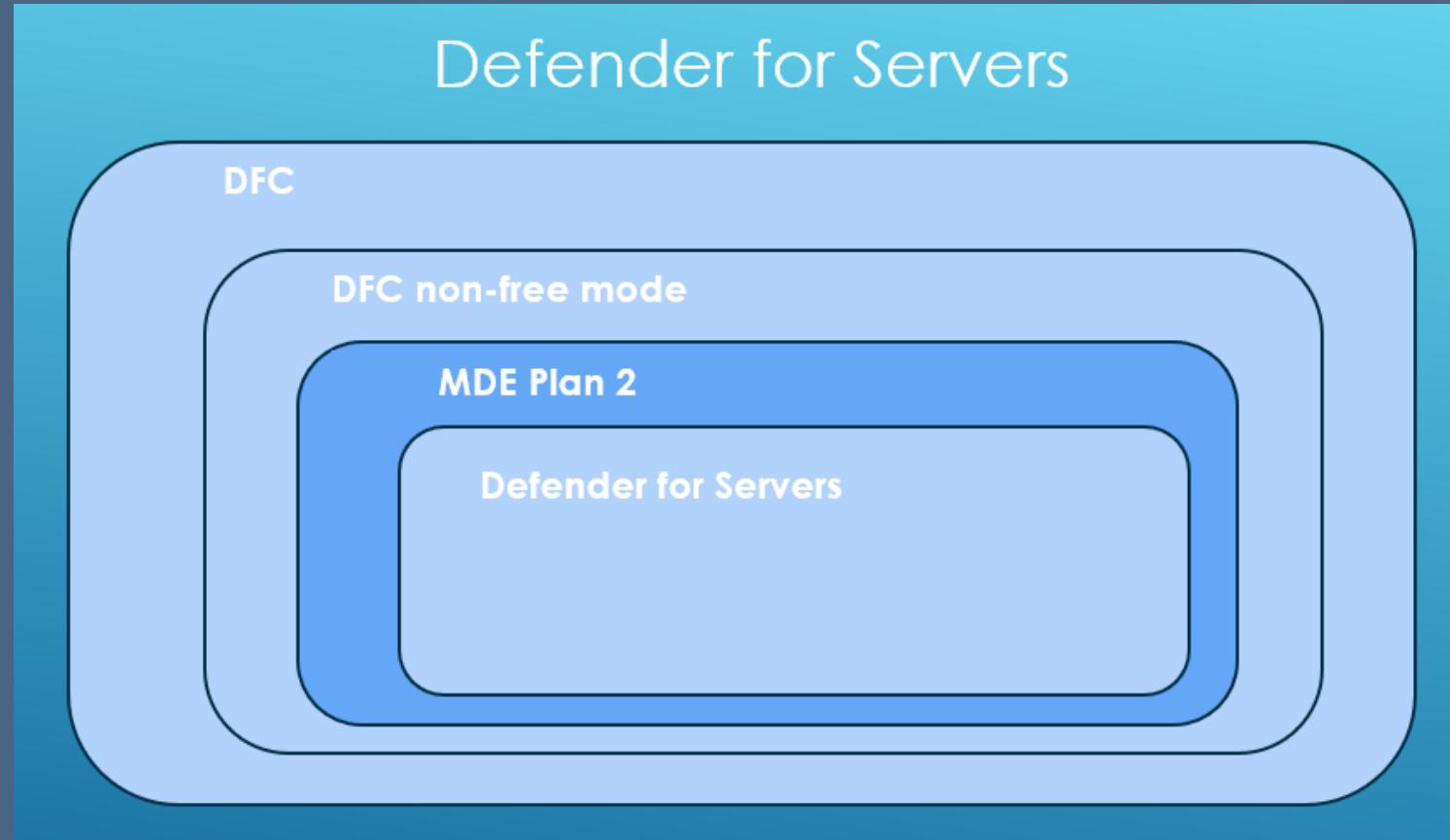
Microsoft Defender for Servers is one of the enhanced security features of Microsoft Defender for Cloud. Use it to add threat detection and advanced defenses to your Windows and Linux machines whether they're running in Azure, AWS, GCP, and on-premises environment.

To protect machines in hybrid and multicloud environments, Defender for Cloud uses [Azure Arc](#). Connect your hybrid and multicloud machines as explained [in the relevant quickstart](#):

- [Connect your non-Azure machines to Microsoft Defender for Cloud](#)
- [Connect your AWS accounts to Microsoft Defender for Cloud](#)

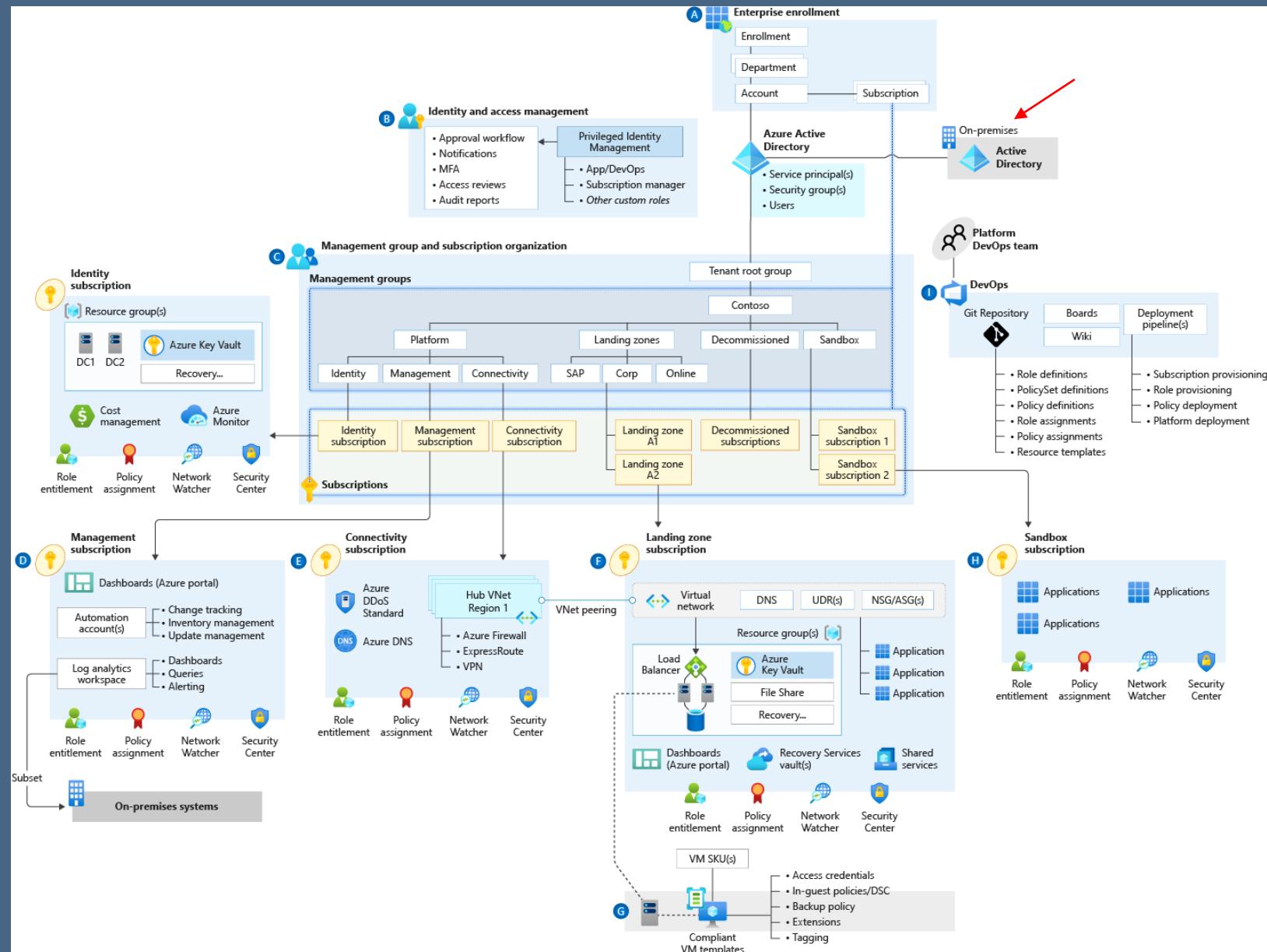
Defender for Servers supports security for servers in a hybrid and multi-cloud environment. Defender for Servers and MDE Plan 2 overlap in protecting servers

# Design Component – Defender for Cloud



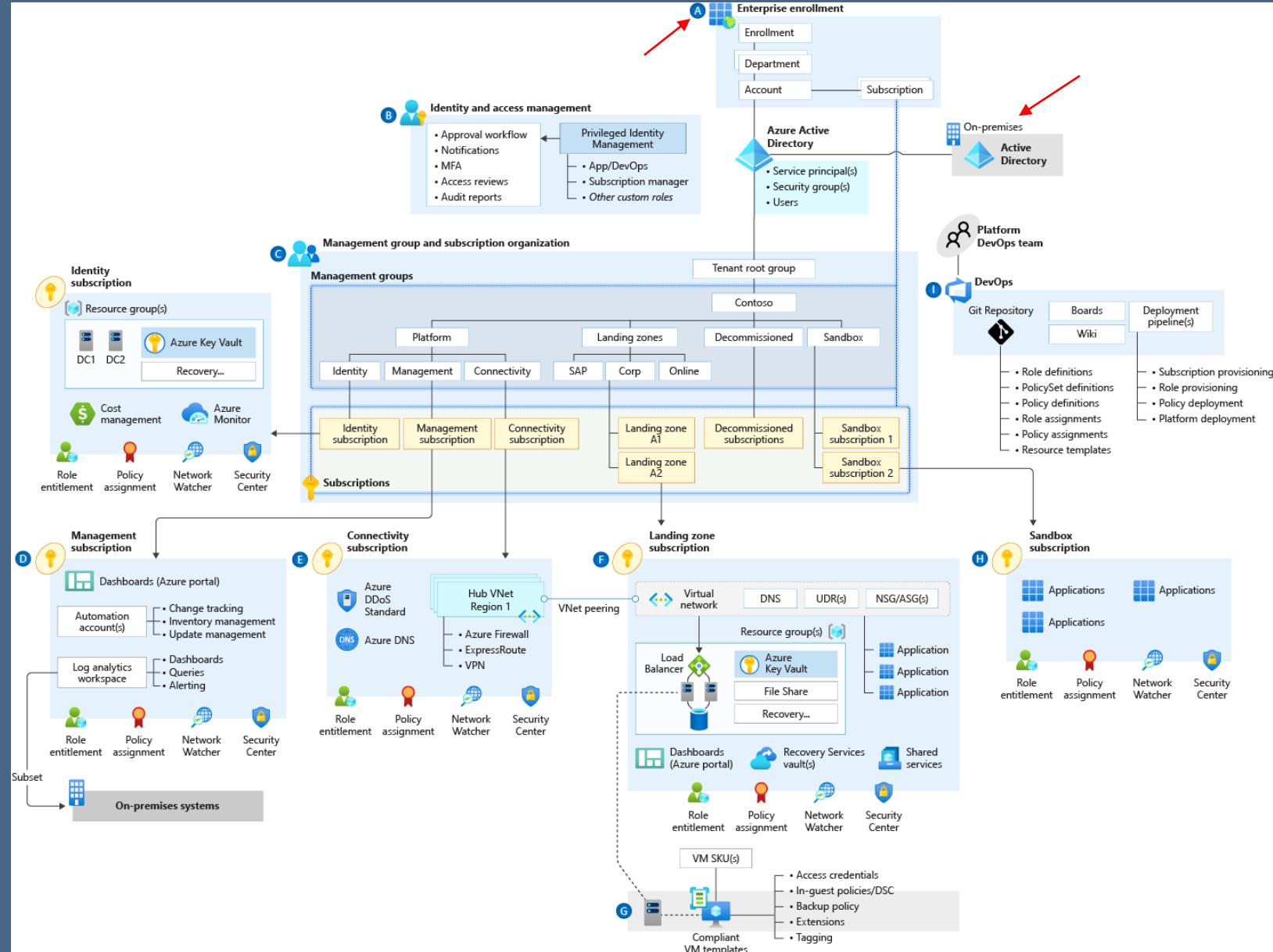
# Putting it all together

- Hybrid including both Azure and on-prem



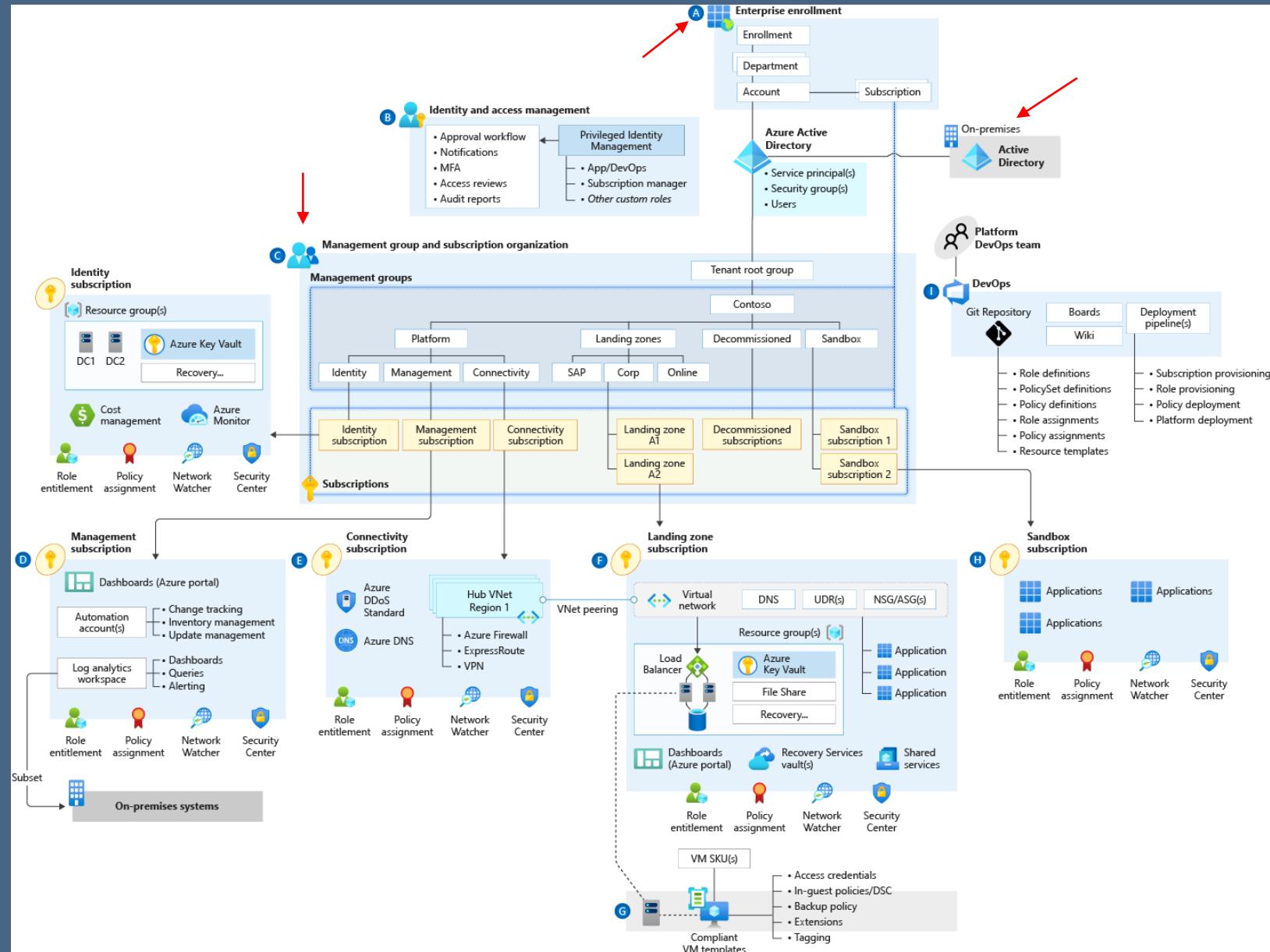
# Putting it all together

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



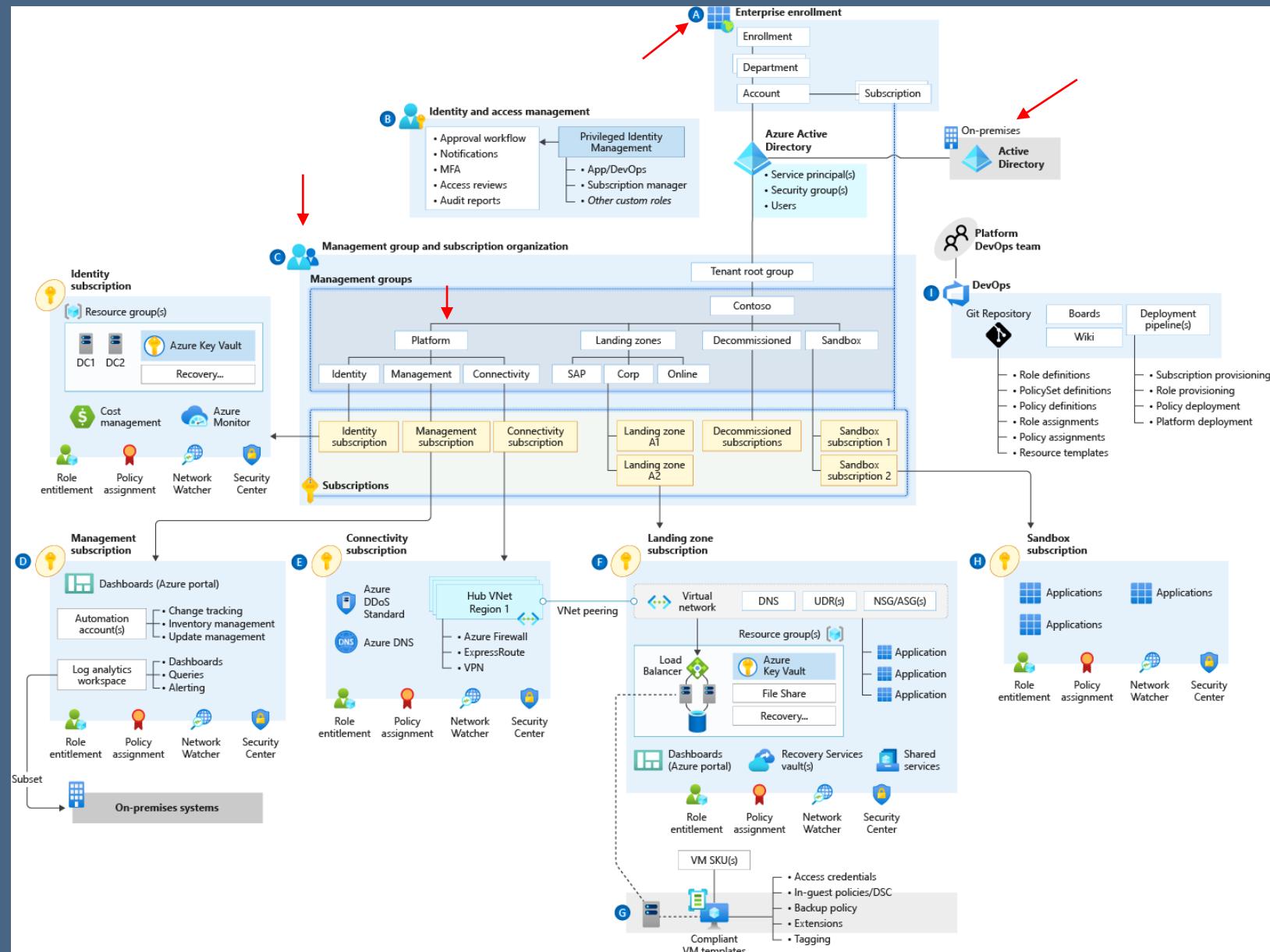
# Putting it all together

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



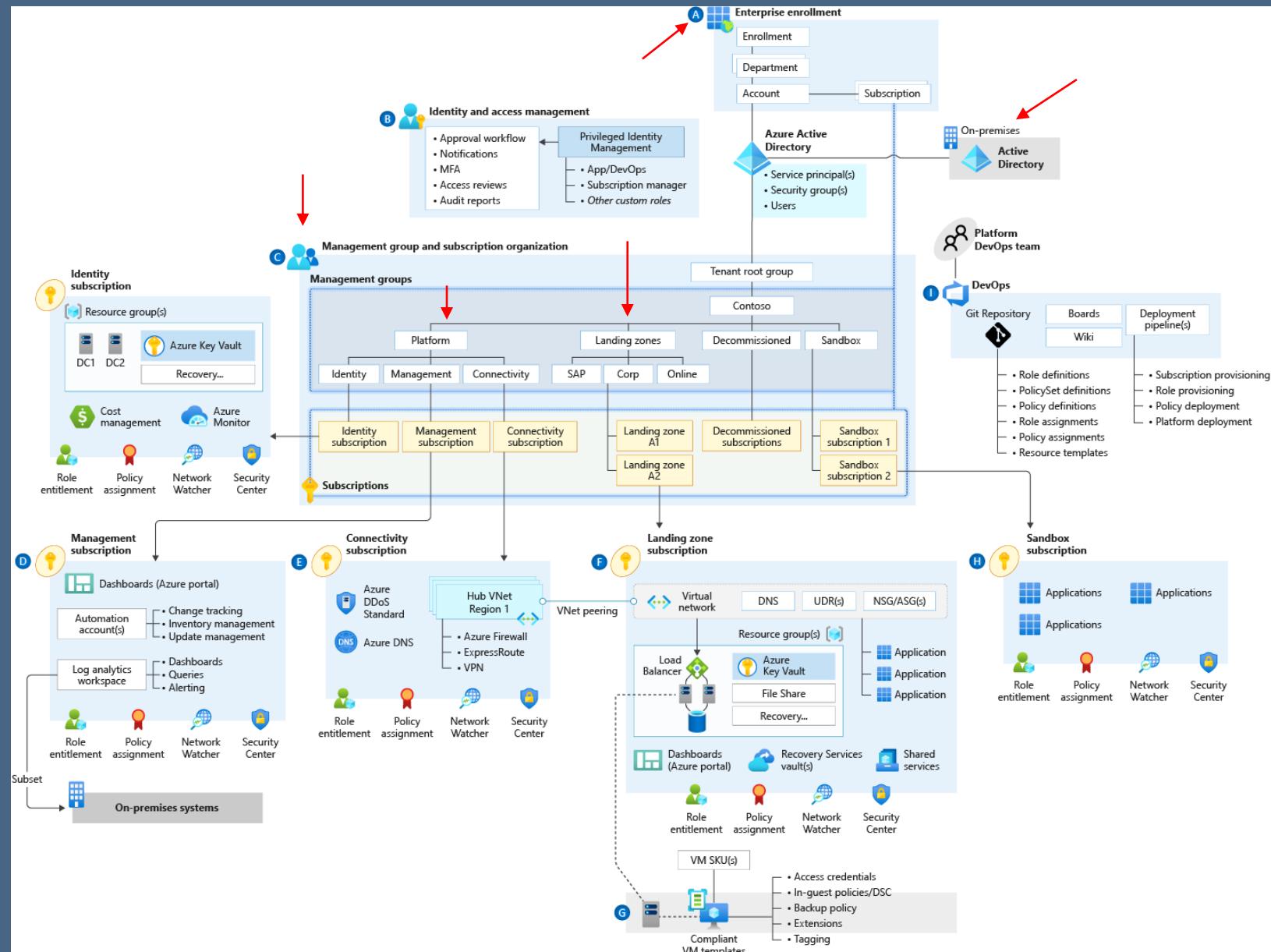
# Putting it all together

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



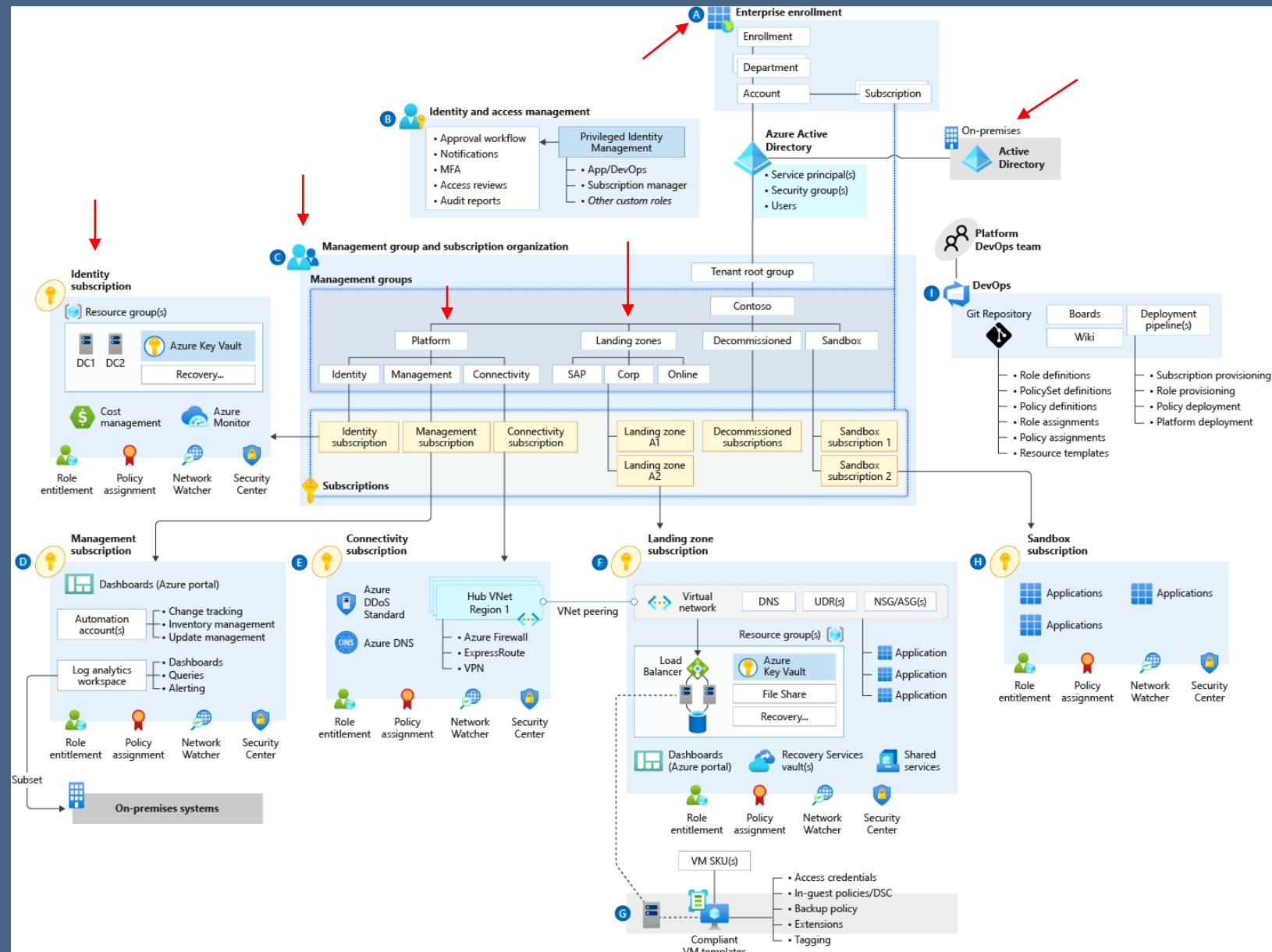
# Putting it all together

- 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



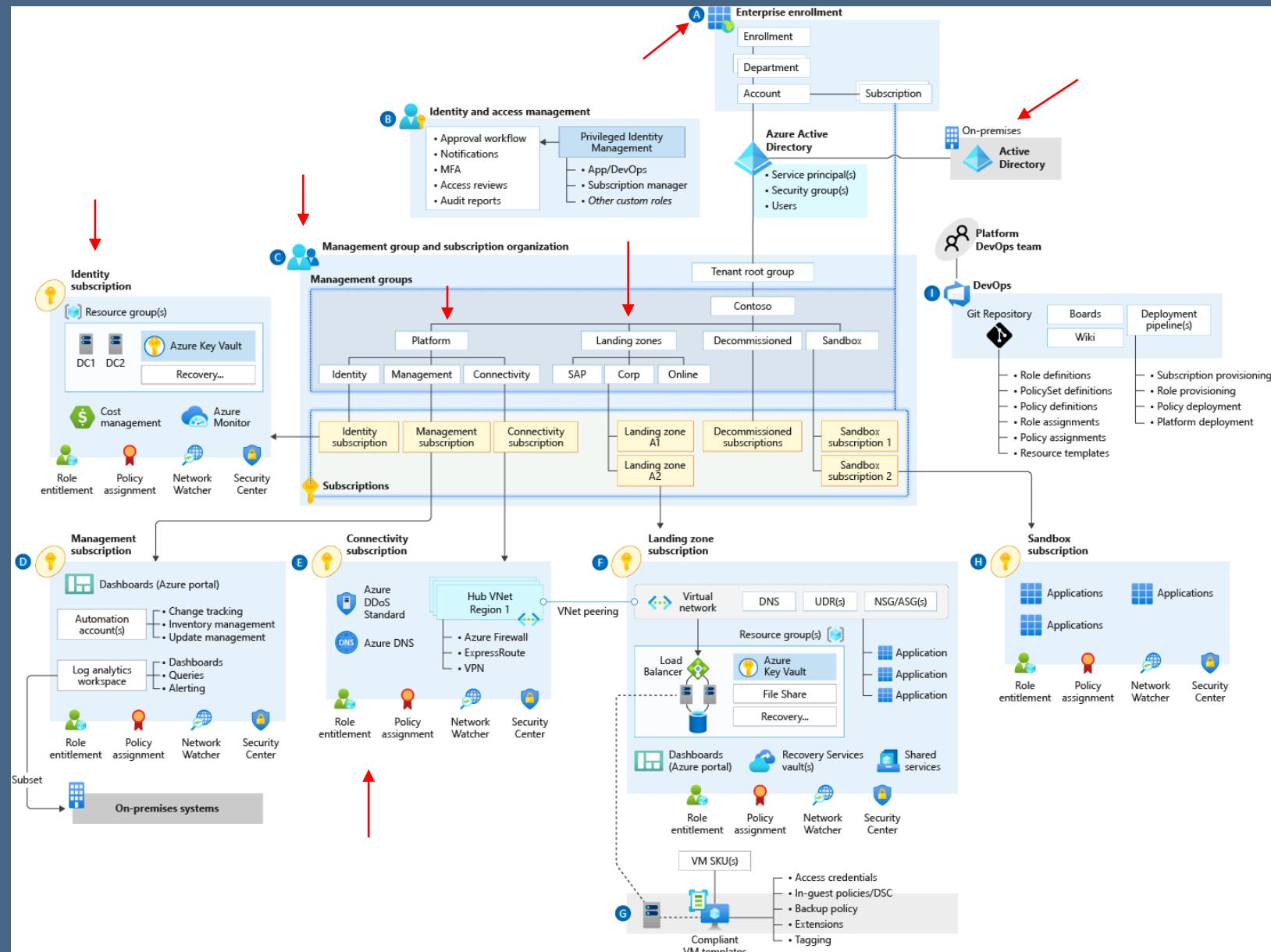
# Putting it all together

- 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)



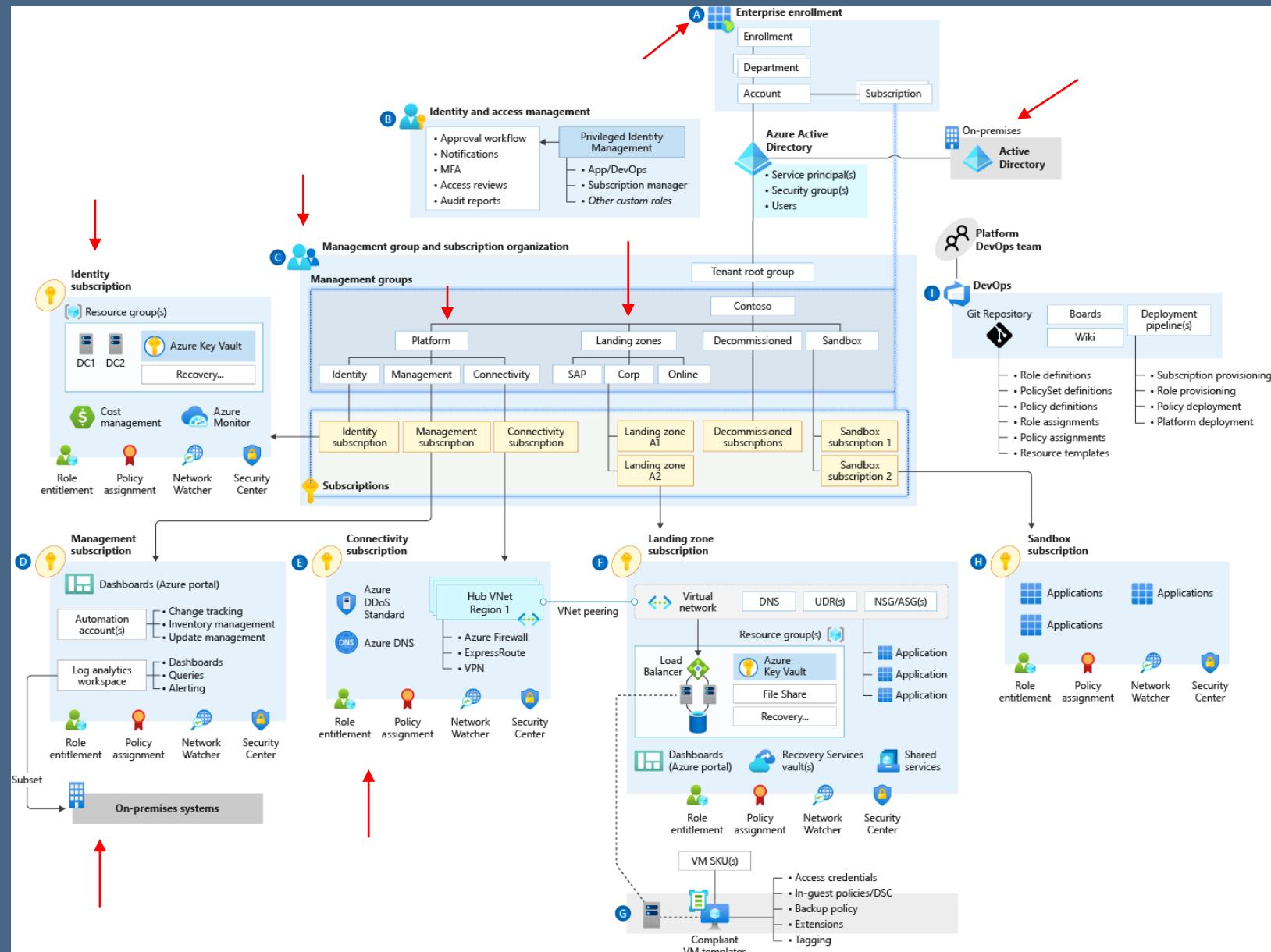
# Putting it all together

- 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)



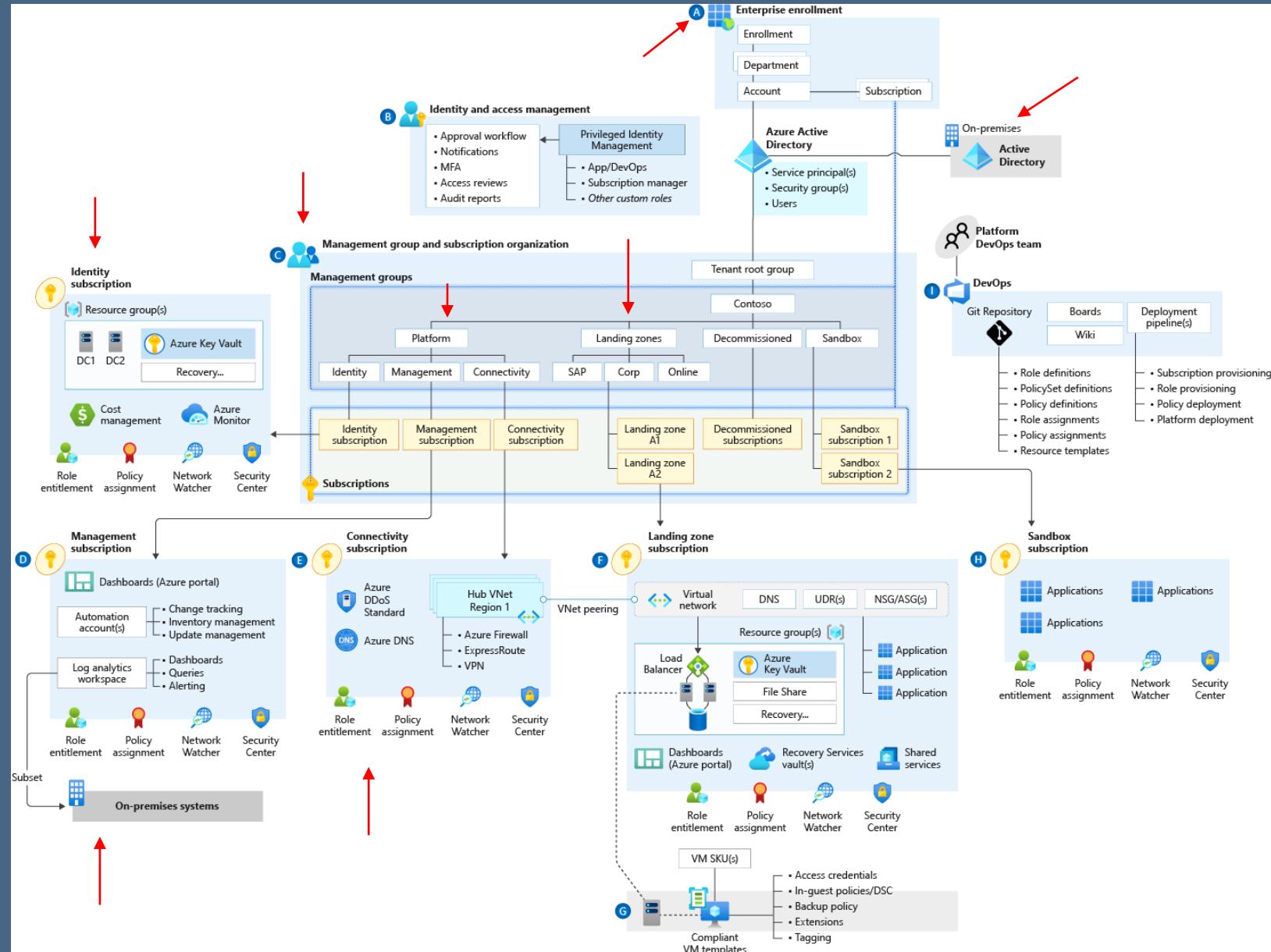
# Putting it all together

- 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)



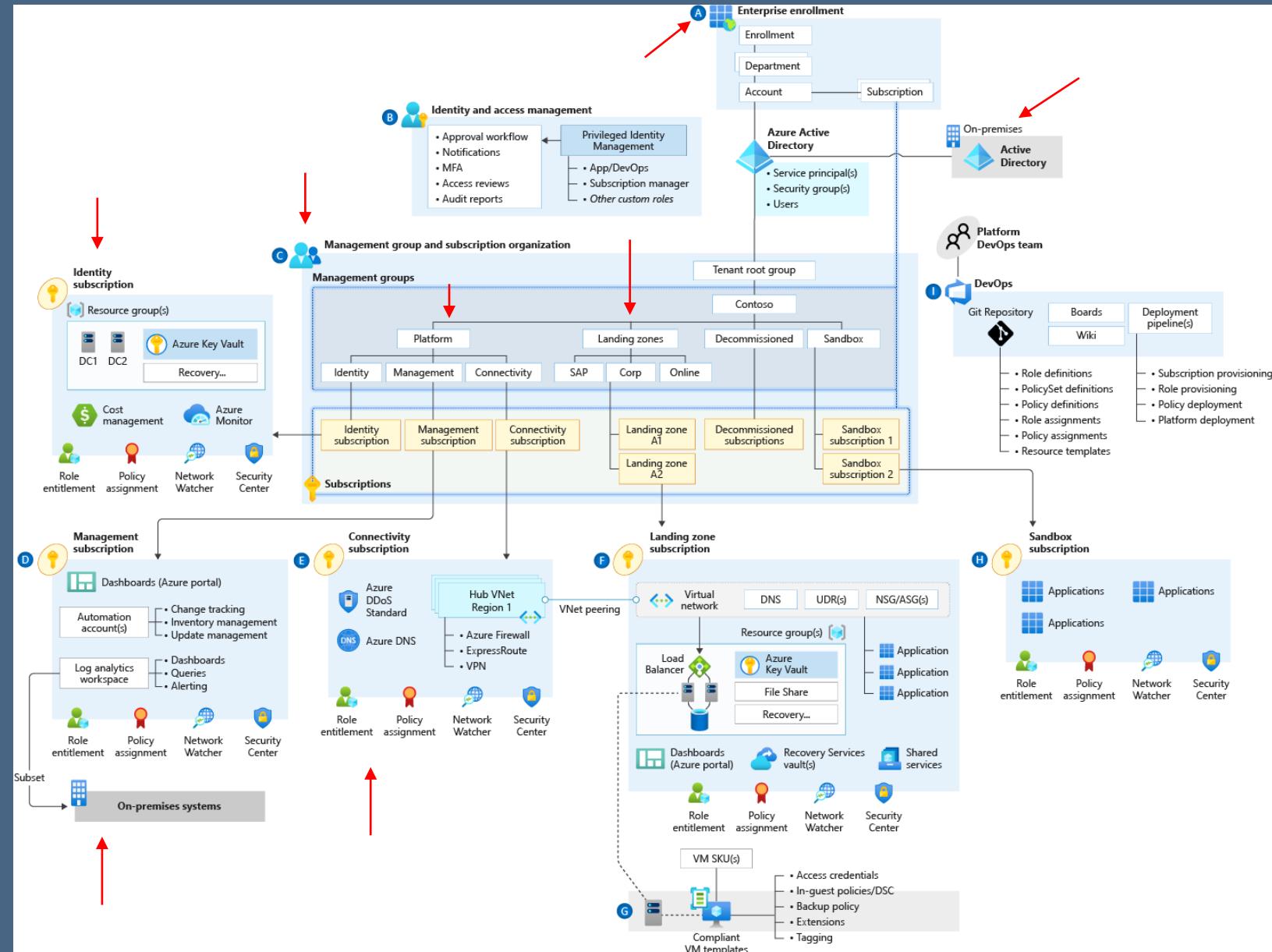
# Putting it all together

- 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



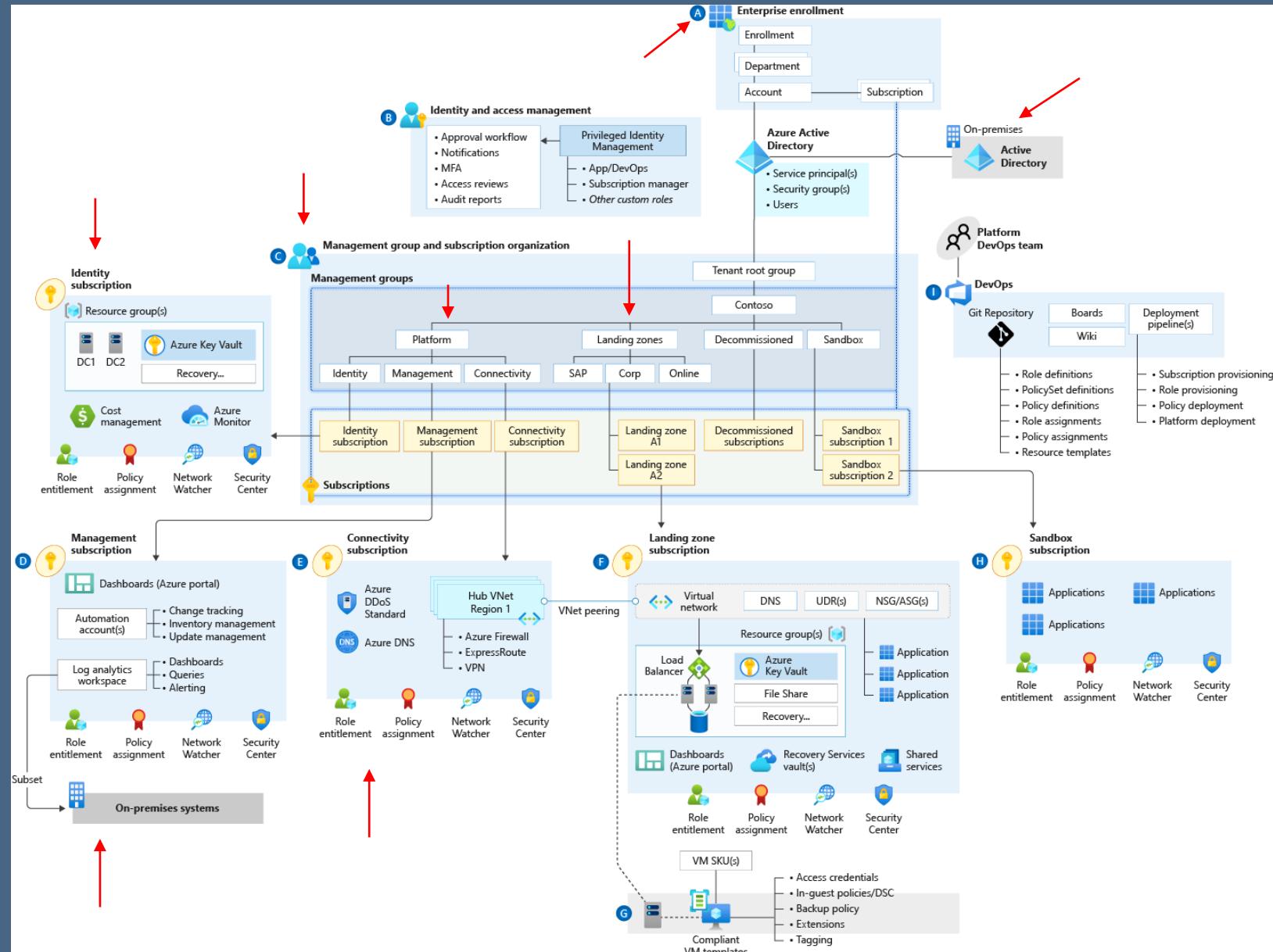
# Putting it all together

- 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)



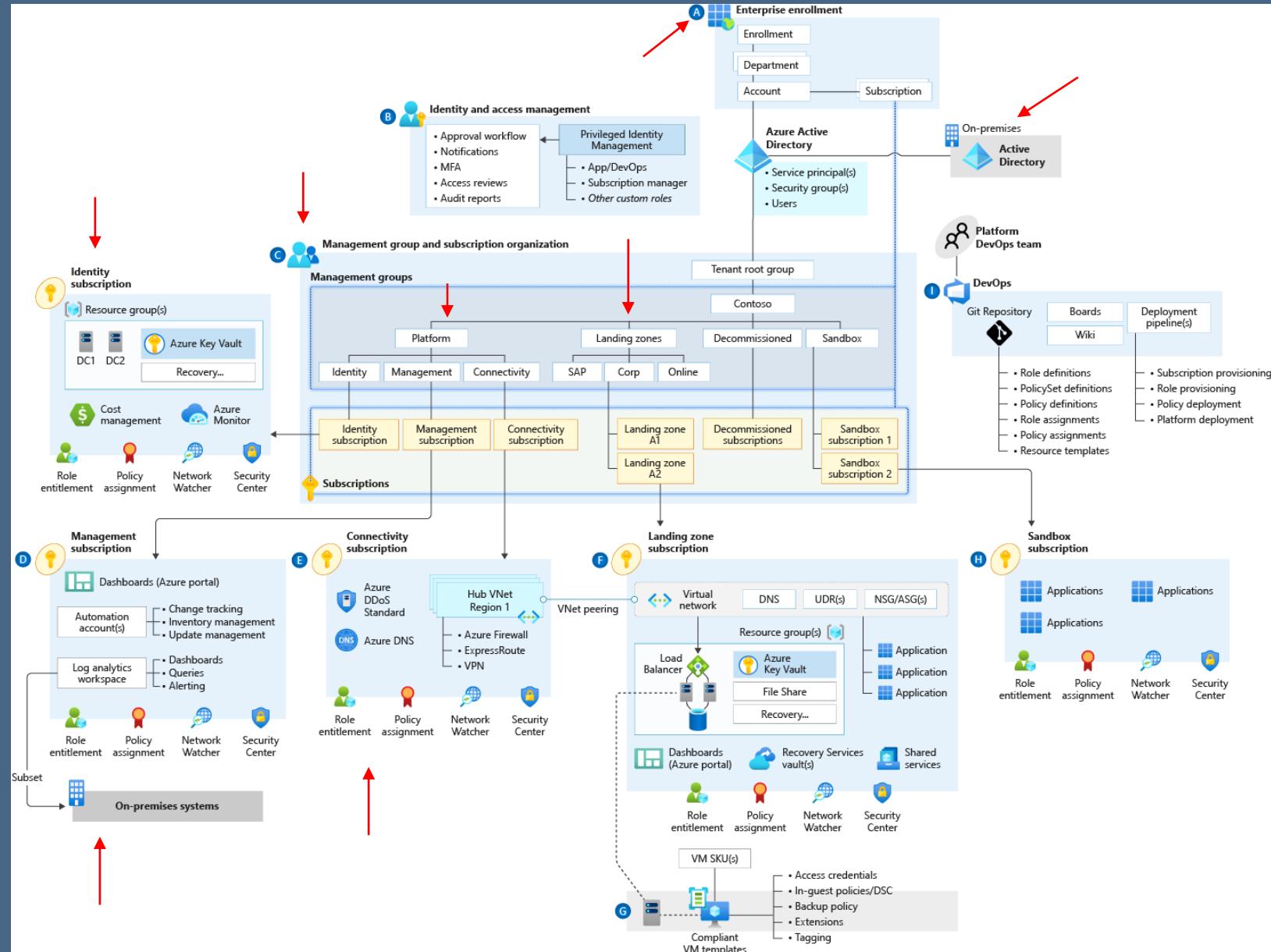
# Putting it all together

- 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)



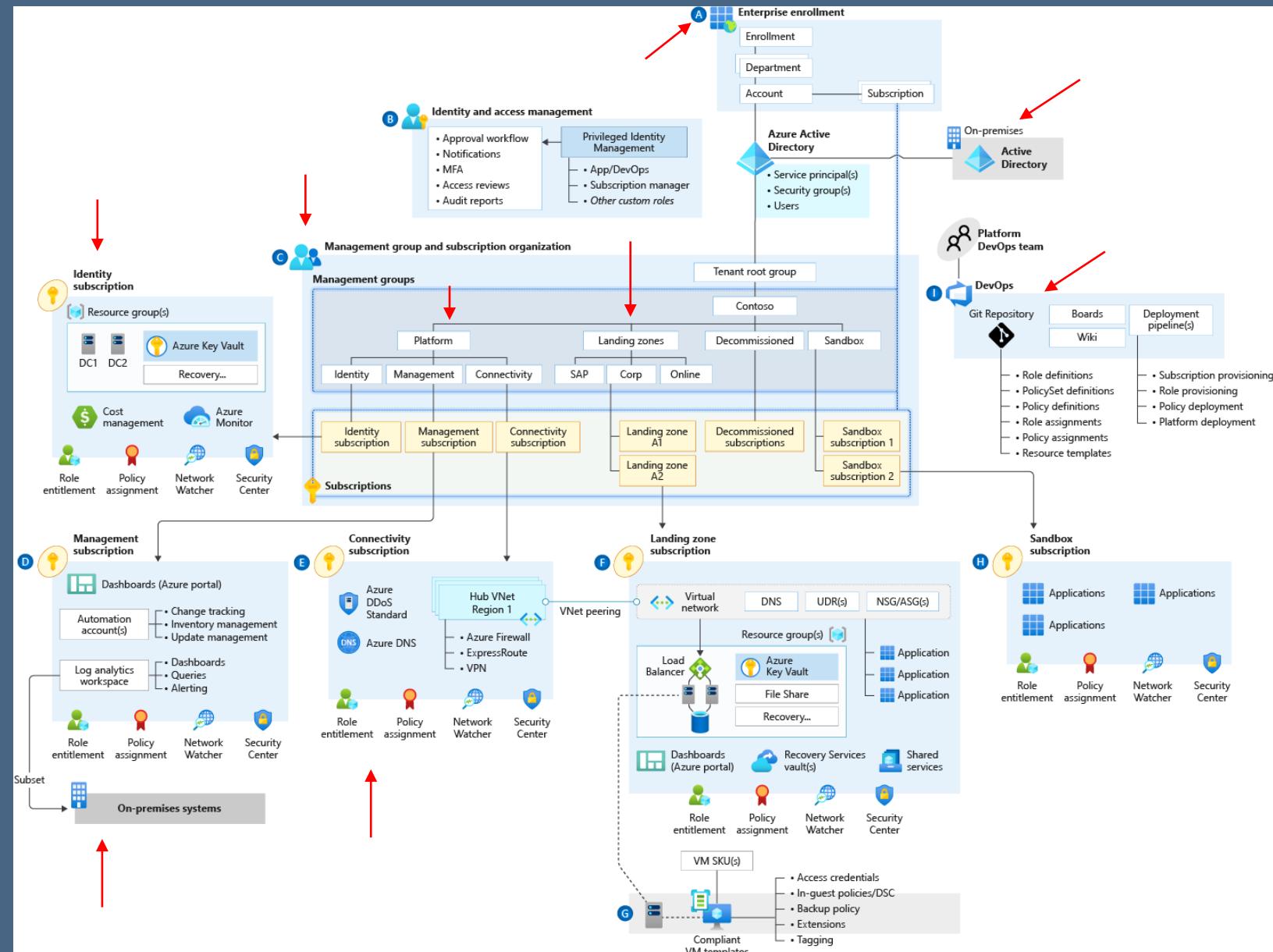
# Putting it all together

- 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)



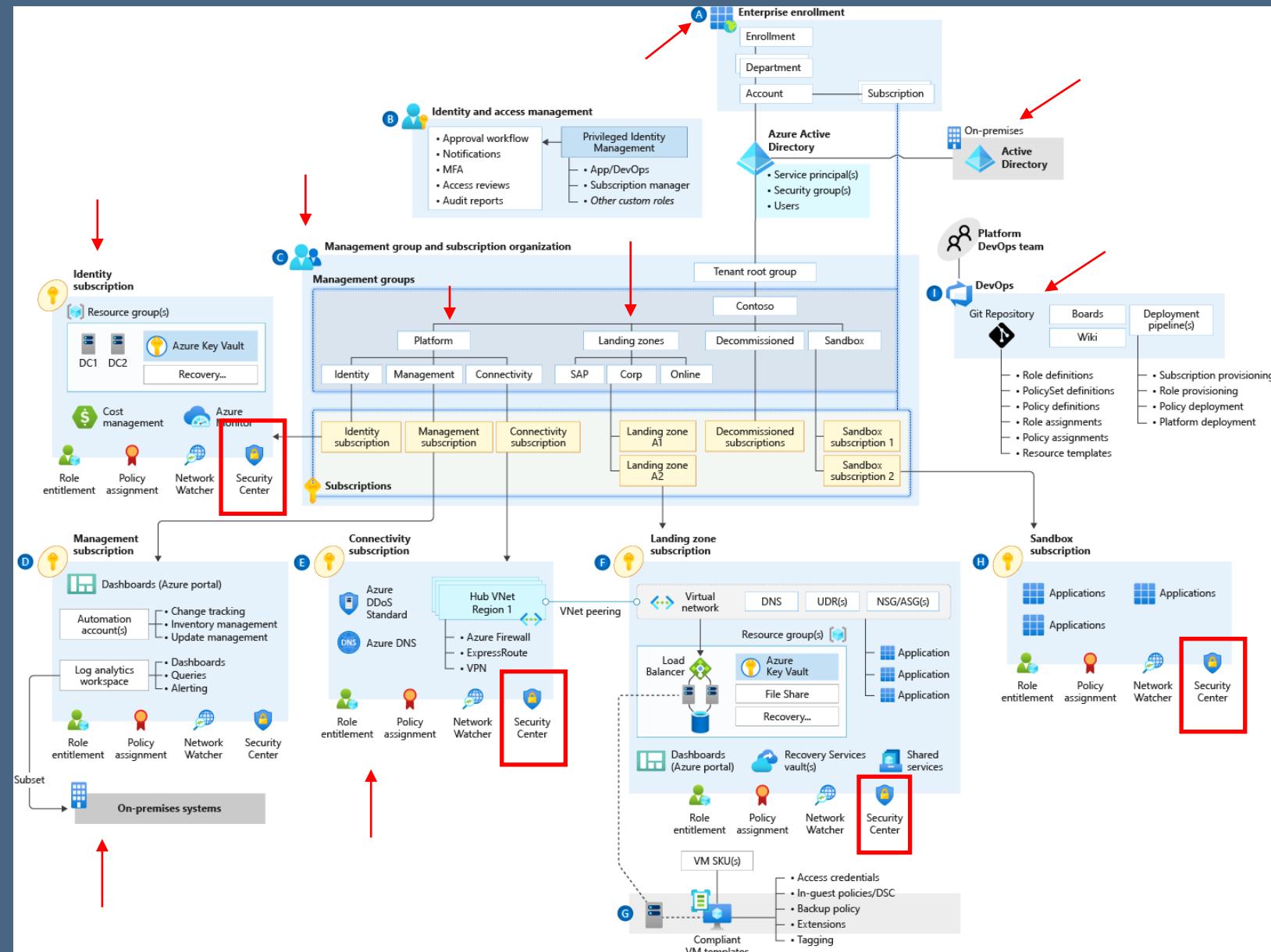
# Putting it all together

- 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)



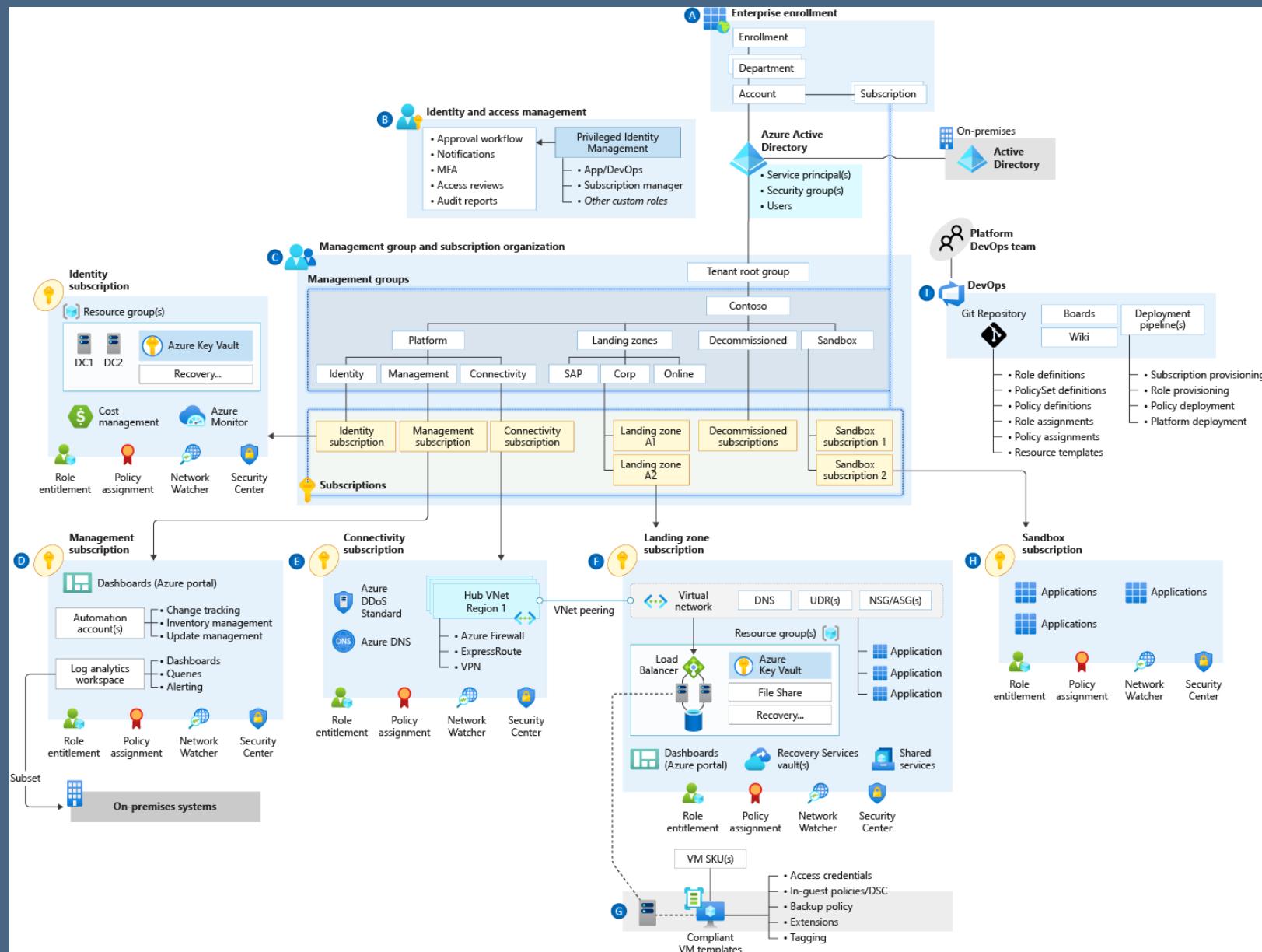
# Putting it all together

- 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