



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

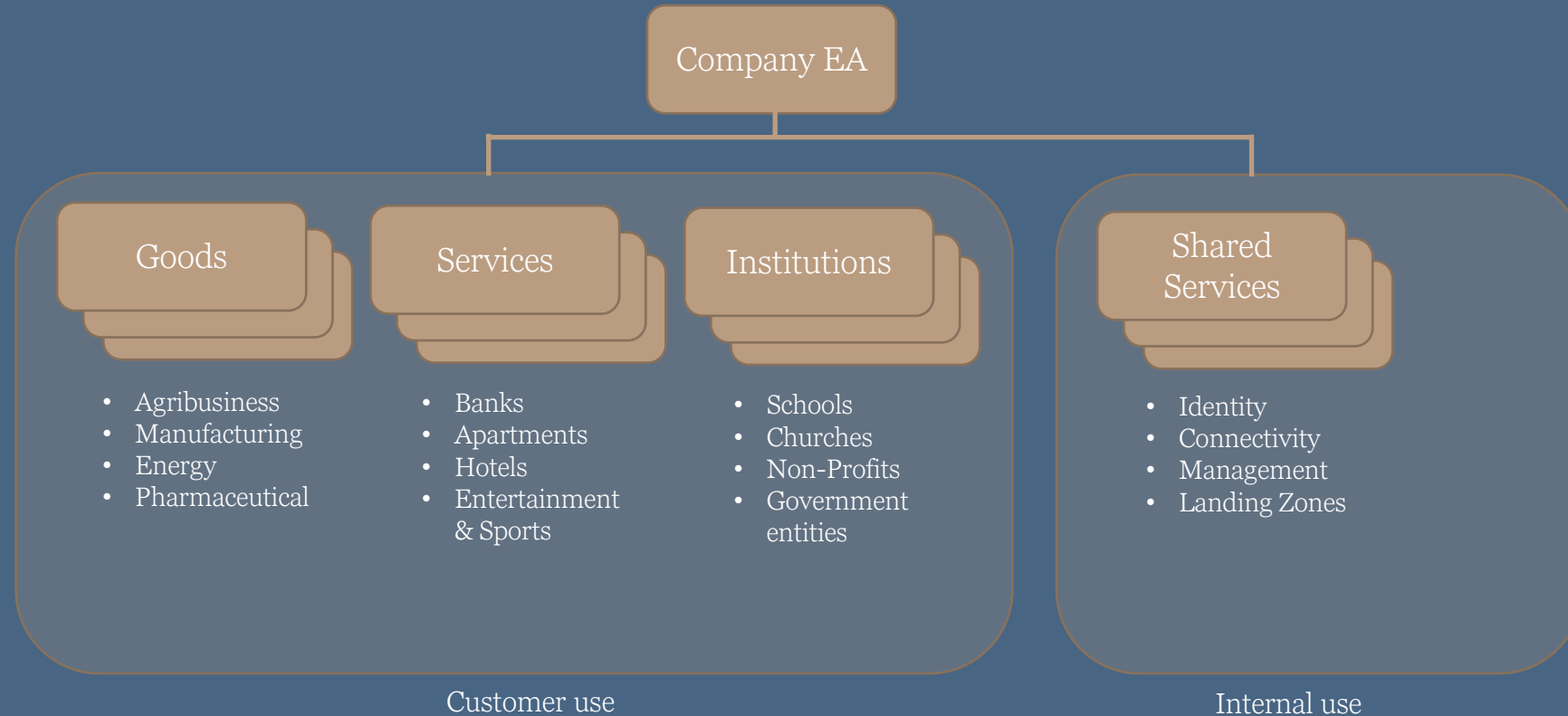
Azure Cloud Security Design for Insurance – Design Principles

- 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 Features

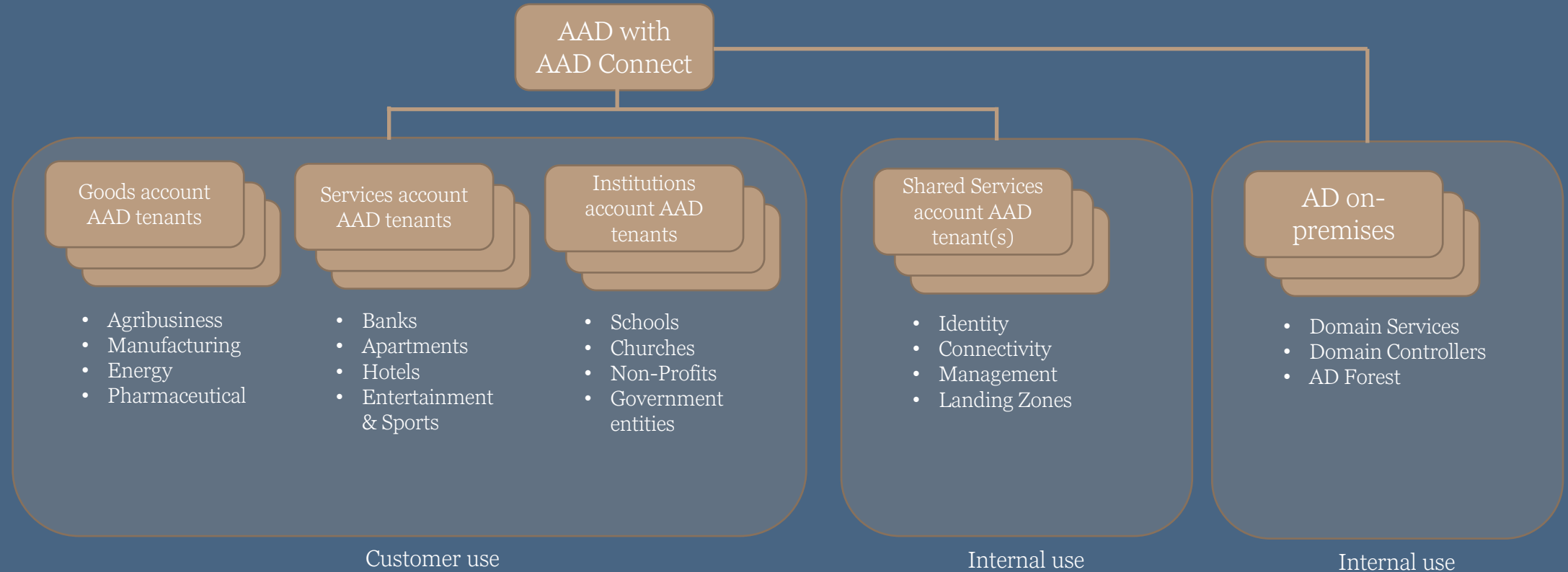
- Hybrid – Certain assets that must reside and operate on-prem
- Dedicated connectivity – ExpressRoutes
- Microservices and containerization
- Data Loss Prevention – Azure Virtual Desktop for internal use
- CASB and the like for customer-facing applications and external use

Design 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

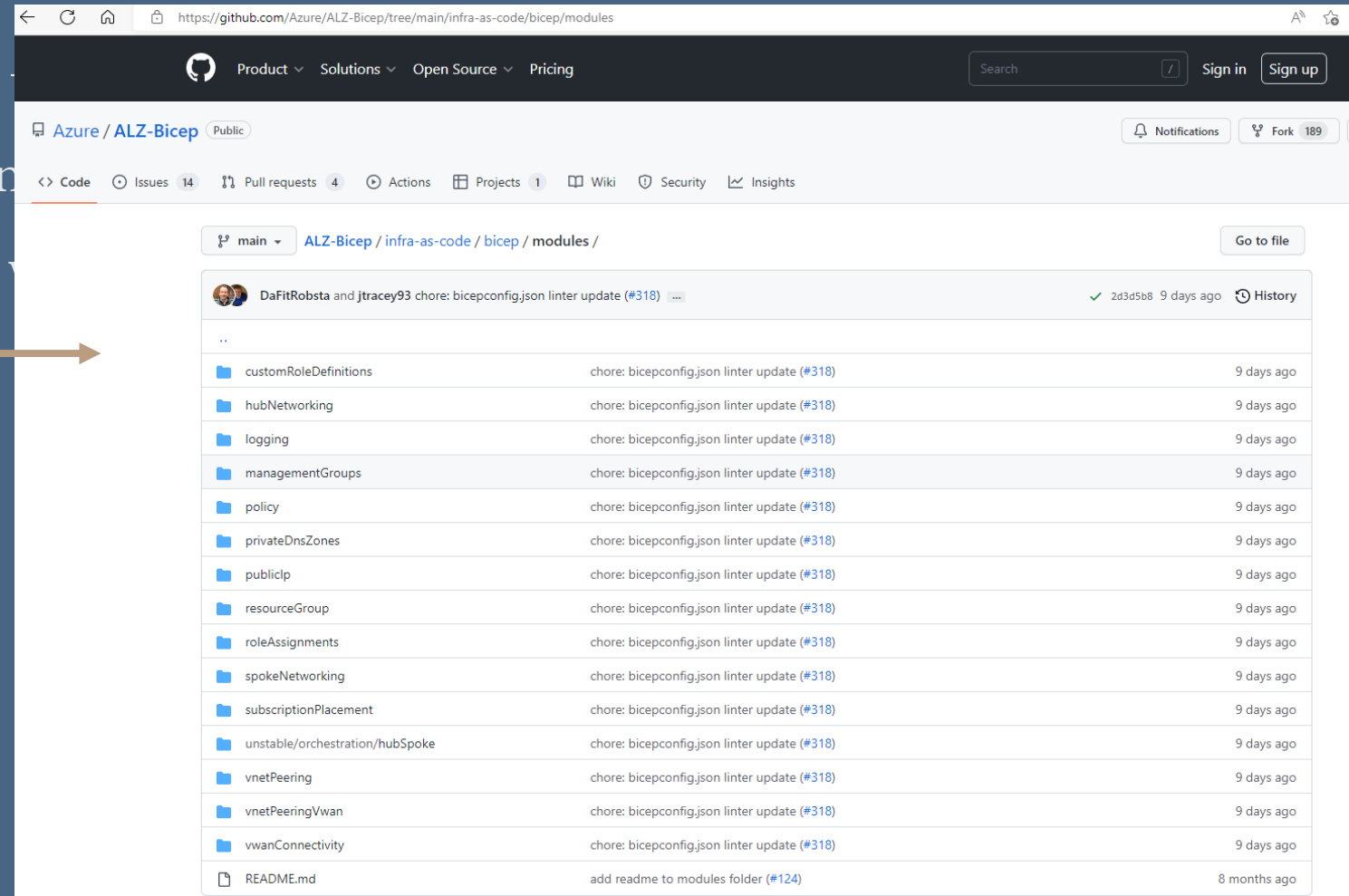
Bicep

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

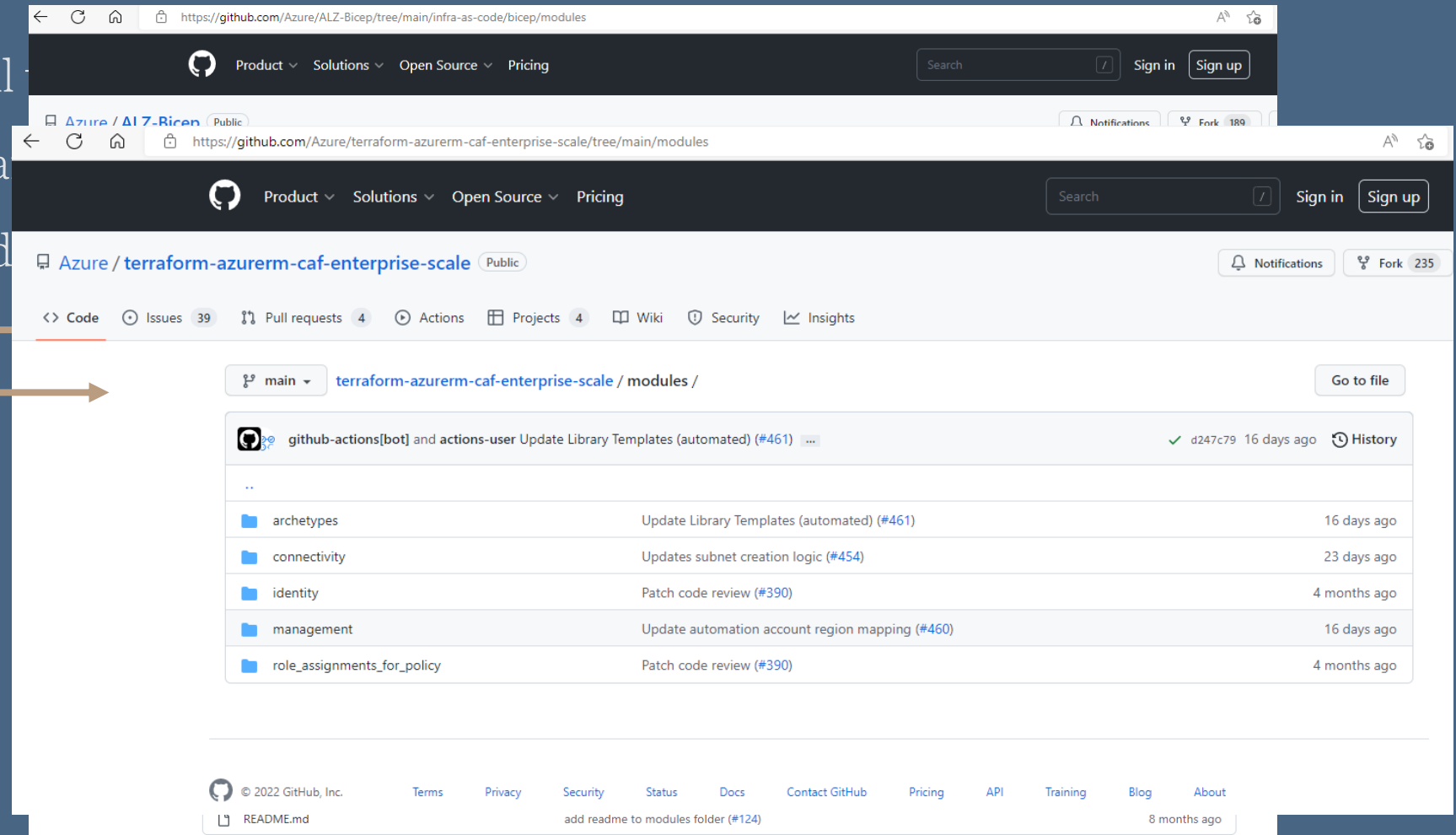
Bicep

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

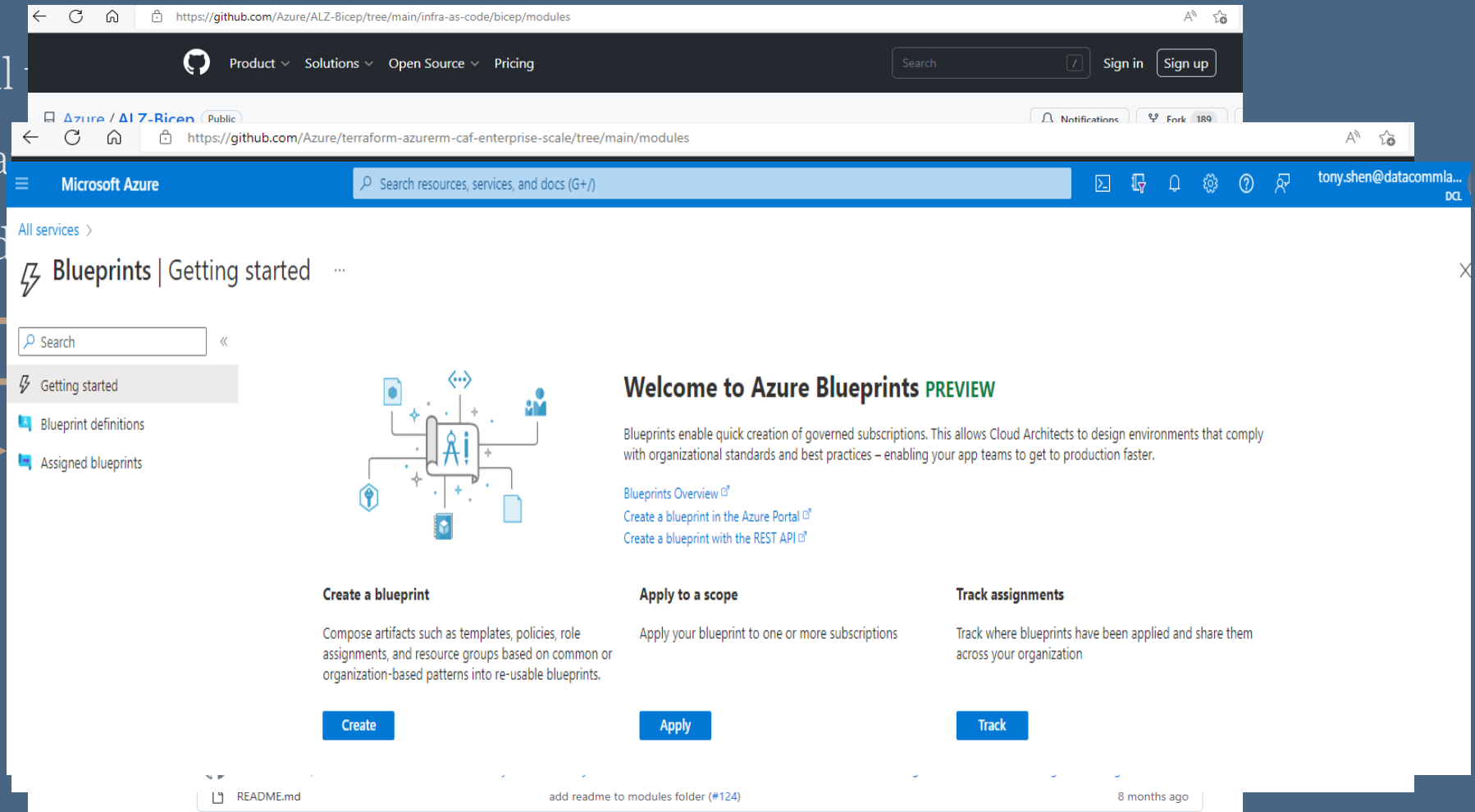
Bicep

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

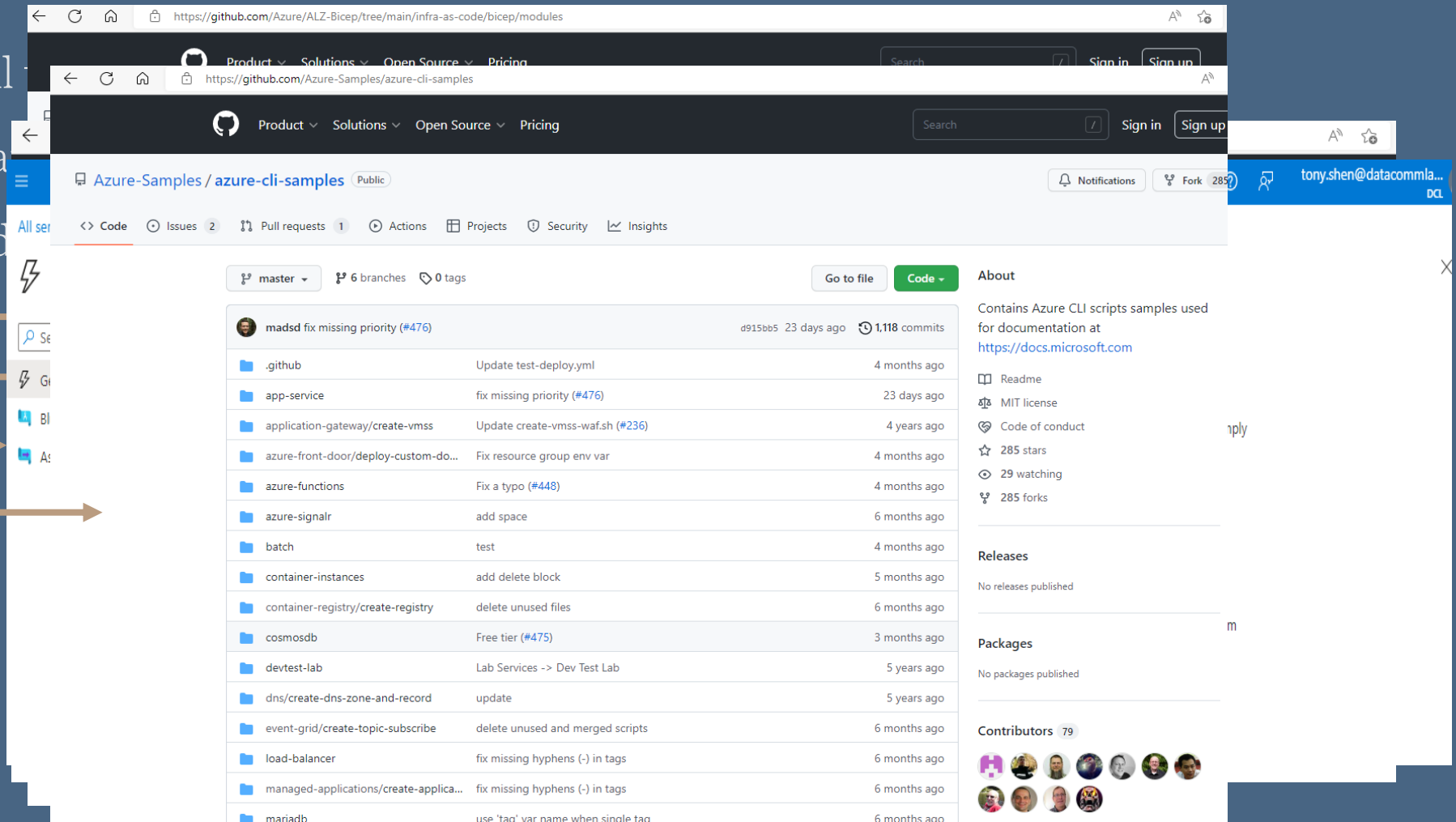
Bicep

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

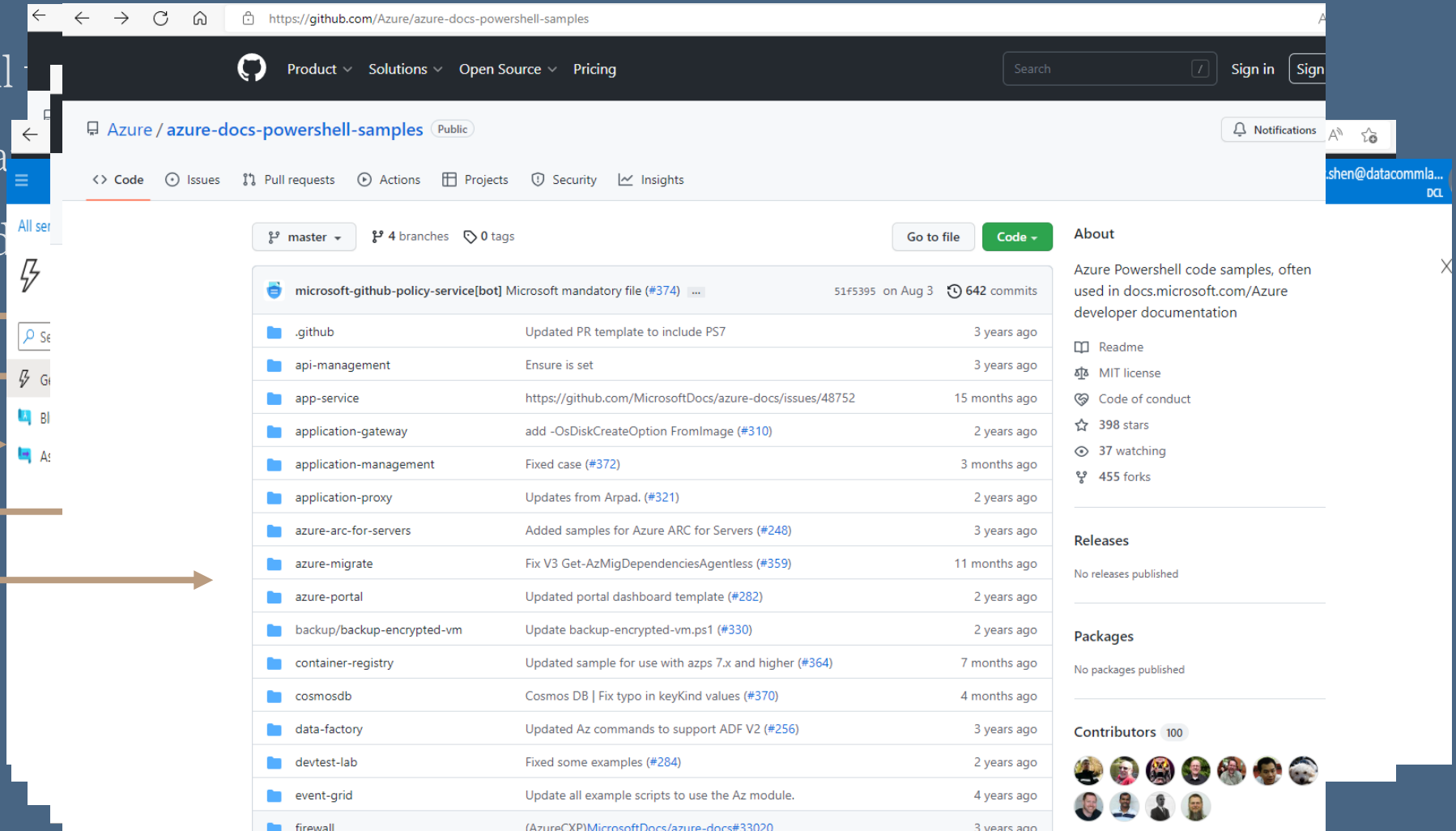
Bicep

Terraform

Blueprints

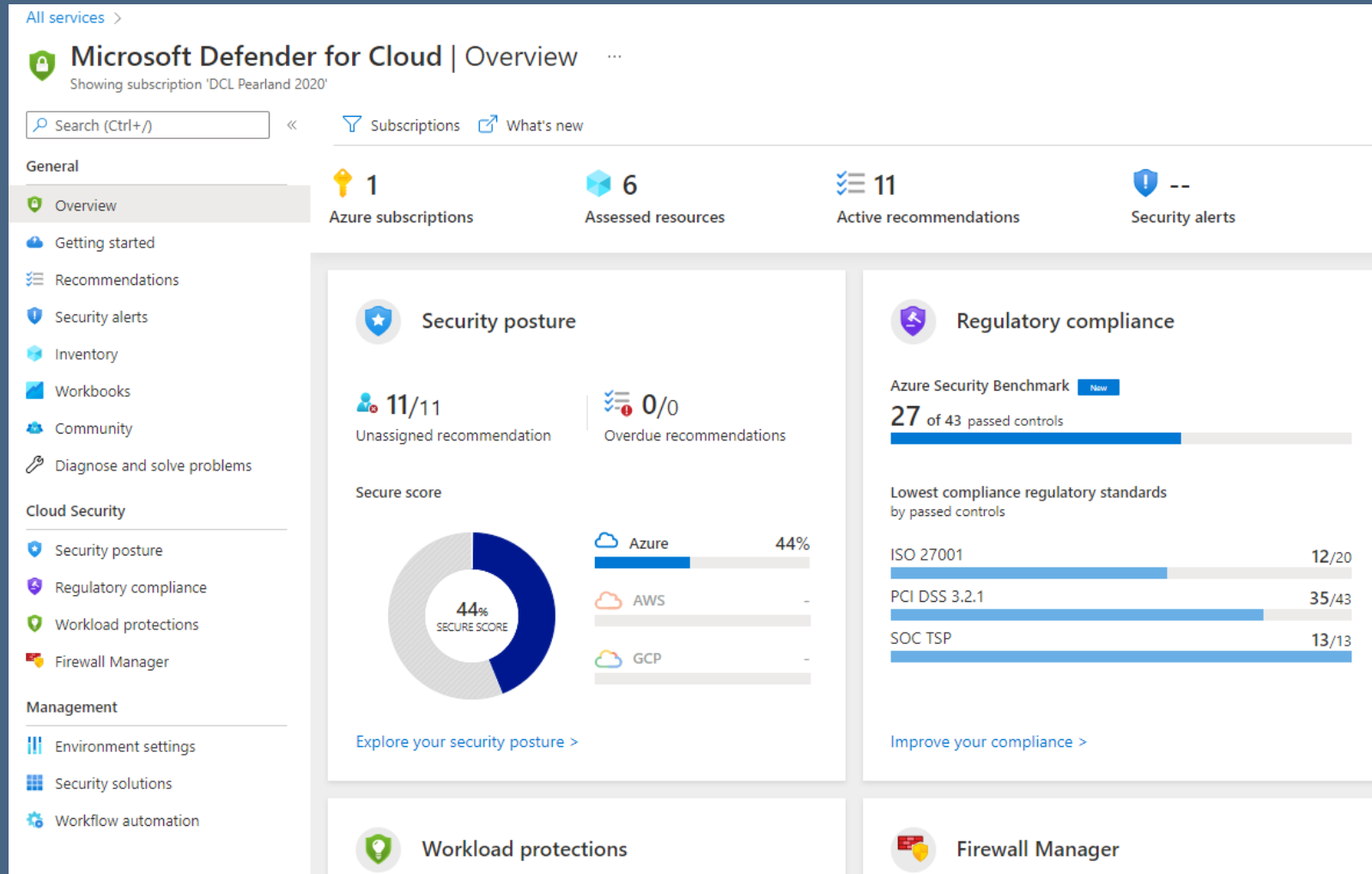
Azure CLI

Azure PowerShell



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

Design Component – Defender for Cloud



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

Cloud Security

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

Management

- Environment settings
- Security solutions
- Workflow automation

Secure score recommendations All recommendations

Secure score 44%

Active items

- Controls 3/7
- Recommendations 11/27

Resource health

Unhealthy (3) Healthy (0) Not applicable (2)

Governance (preview)

Overdue recommendations 0/0

Unassigned recommendations 11/11

Search recommendations

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

Show my items only (preview): Off

Name	Max score	Current score	Potential score increase	Status	Unhealthy resources	Insights
Enable MFA	10	0.00	+ 56%	Unassigned	1 of 1 resources	
Encrypt data in transit	4	4.00		Completed	0 of 1 resources	
Manage access and permissions	4	4.00		Completed	0 of 2 resources	
Enable enhanced security features	Not scored	Not scored		Unassigned	1 of 1 resources	
Implement security best practices	Not scored	Not scored		Unassigned	2 of 2 resources	
Restrict unauthorized network access	Not scored	Not scored		Unassigned	0 of 1 resources	
Remediate security configurations	Not scored	Not scored		Completed	0 of 1 resources	

Design Component – Defender for Cloud

The screenshot shows the Microsoft Defender for Cloud Security alerts page. The interface includes a left-hand navigation pane with sections for General, Cloud Security, and Management. The main content area displays the 'Security alerts' view for the subscription 'DCL Pearlant 2020'. At the top, there are statistics for 'Active alerts' (0) and 'Affected resources' (0). Below these, there is a search bar and filter options for Subscription, Status, and Severity. The 'Download CSV report' button is highlighted with a red box. The main area shows a message 'No alerts found' with a shield icon.

All services > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Security alerts

Showing subscription 'DCL Pearlant 2020'

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

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

0 Active alerts 0 Affected resources

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 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

<input type="checkbox"/> Resource name ↑↓	Resource type ↑↓	Subscription ↑↓	Monitoring agent ↑↓	Defender for Cloud ↑↓	Recommendations ↑↓
<input type="checkbox"/> DCL Pearland 2020	Subscription	DCL Pearland 2020		Partial	...
<input type="checkbox"/> ubun2001	Virtual machines	DCL Pearland 2020	✓ Installed	On	...
<input type="checkbox"/> cs710032000a6ae30e3	Storage accounts	DCL Pearland 2020		Off	...
<input type="checkbox"/> loganalyticsworkspace01ussc	Log Analytics workspaces	DCL Pearland 2020			...
<input type="checkbox"/> dev-southcentralus-vnet	Virtual networks	DCL Pearland 2020			...
<input type="checkbox"/> <> default	Subnets	DCL Pearland 2020			...

Previous Page 1 of 1 Next

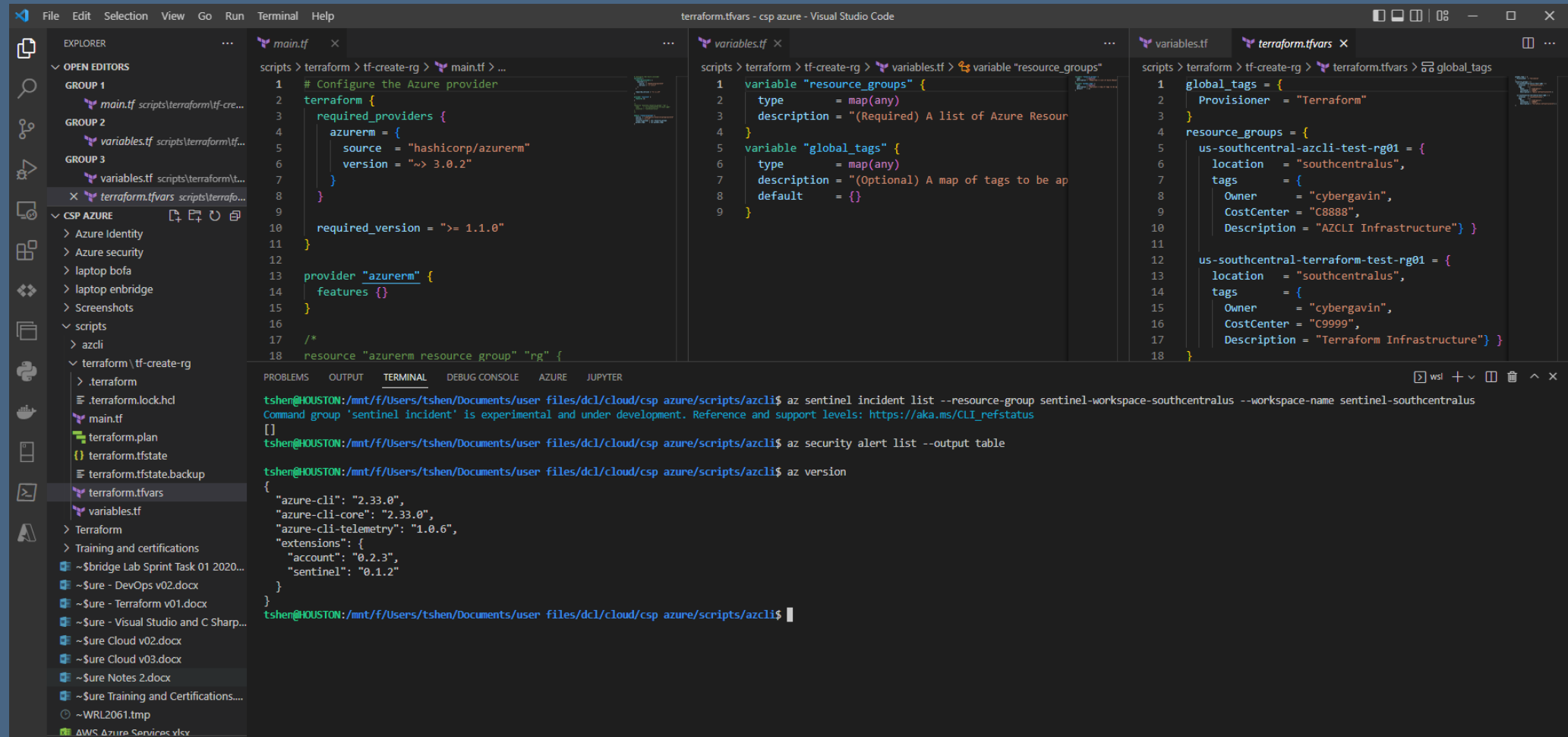
Design Component – Defender for Cloud

The screenshot shows a Visual Studio Code editor with several Terraform files open: `main.tf`, `variables.tf`, and `terraform.tfvars`. The `main.tf` file contains configuration for the Azure provider and required providers. The `variables.tf` file defines variables for resource groups and global tags. The `terraform.tfvars` file sets values for these variables.

The terminal window shows the output of the command `az security assessment list --output table`. The output is a table with columns: Name, ResourceGroup, and a list of security recommendations. The recommendations include various security alerts and their severity levels.

Name	ResourceGroup
Vulnerabilities in security configuration on your Linux machines should be remediated (powered by Guest Configuration)	dev-southcentralus
Secure transfer to storage accounts should be enabled	cloud-shell-storage-southcentralus
Access to storage accounts with firewall and virtual network configurations should be restricted	cloud-shell-storage-southcentralus
Storage accounts should be migrated to new Azure Resource Manager resources	cloud-shell-storage-southcentralus
Storage account public access should be disallowed	cloud-shell-storage-southcentralus
Storage accounts should restrict network access using virtual network rules	cloud-shell-storage-southcentralus
Microsoft Defender for App Service should be enabled	
Microsoft Defender for Azure SQL Database servers should be enabled	
Microsoft Defender for Key Vault should be enabled	
Microsoft Defender for SQL servers on machines should be enabled	
Microsoft Defender for Storage should be enabled	
Microsoft Defender for Containers should be enabled	
Microsoft Defender for servers should be enabled	
Auto provisioning of the Log Analytics agent should be enabled on subscriptions	
Email notification to subscription owner for high severity alerts should be enabled	
Subscriptions should have a contact email address for security issues	
Email notification for high severity alerts should be enabled	
Storage account should use a private link connection	cloud-shell-storage-southcentralus
Microsoft Defender for DNS should be enabled	
Microsoft Defender for Resource Manager should be enabled	
Microsoft Defender for open-source relational databases should be enabled	
A maximum of 3 owners should be designated for subscriptions	
MFA should be enabled on accounts with owner permissions on subscriptions	
External accounts with read permissions should be removed from subscriptions	
MFA should be enabled on accounts with write permissions on subscriptions	
MFA should be enabled on accounts with read permissions on subscriptions	
Deprecated accounts should be removed from subscriptions	
External accounts with write permissions should be removed from subscriptions	
External accounts with owner permissions should be removed from subscriptions	
Deprecated accounts with owner permissions should be removed from subscriptions	
There should be more than one owner assigned to subscriptions	
System updates should be installed on your machines	dev-southcentralus
Log Analytics agent should be installed on virtual machines	DEV-SOUTHCENTRALUS
Subnets should be associated with a network security group	dev-southcentralus
Install endpoint protection solution on virtual machines	DEV-SOUTHCENTRALUS
Endpoint protection health issues on machines should be resolved	DEV-SOUTHCENTRALUS

Design Component – Defender for Cloud



The screenshot displays the Visual Studio Code interface with a Terraform project. The Explorer sidebar on the left shows the file structure, including a 'scripts' directory and a 'terraform' directory. The main editor area shows three Terraform files: 'main.tf', 'variables.tf', and 'terraform.tfvars'. The 'main.tf' file contains the configuration for the Azure provider and the 'azurerm_resource_group' resource. The 'variables.tf' file defines the 'resource_groups' variable. The 'terraform.tfvars' file defines the 'global_tags' variable. The terminal at the bottom shows the execution of the 'az' CLI commands to list incidents and security alerts, and the 'az version' command.

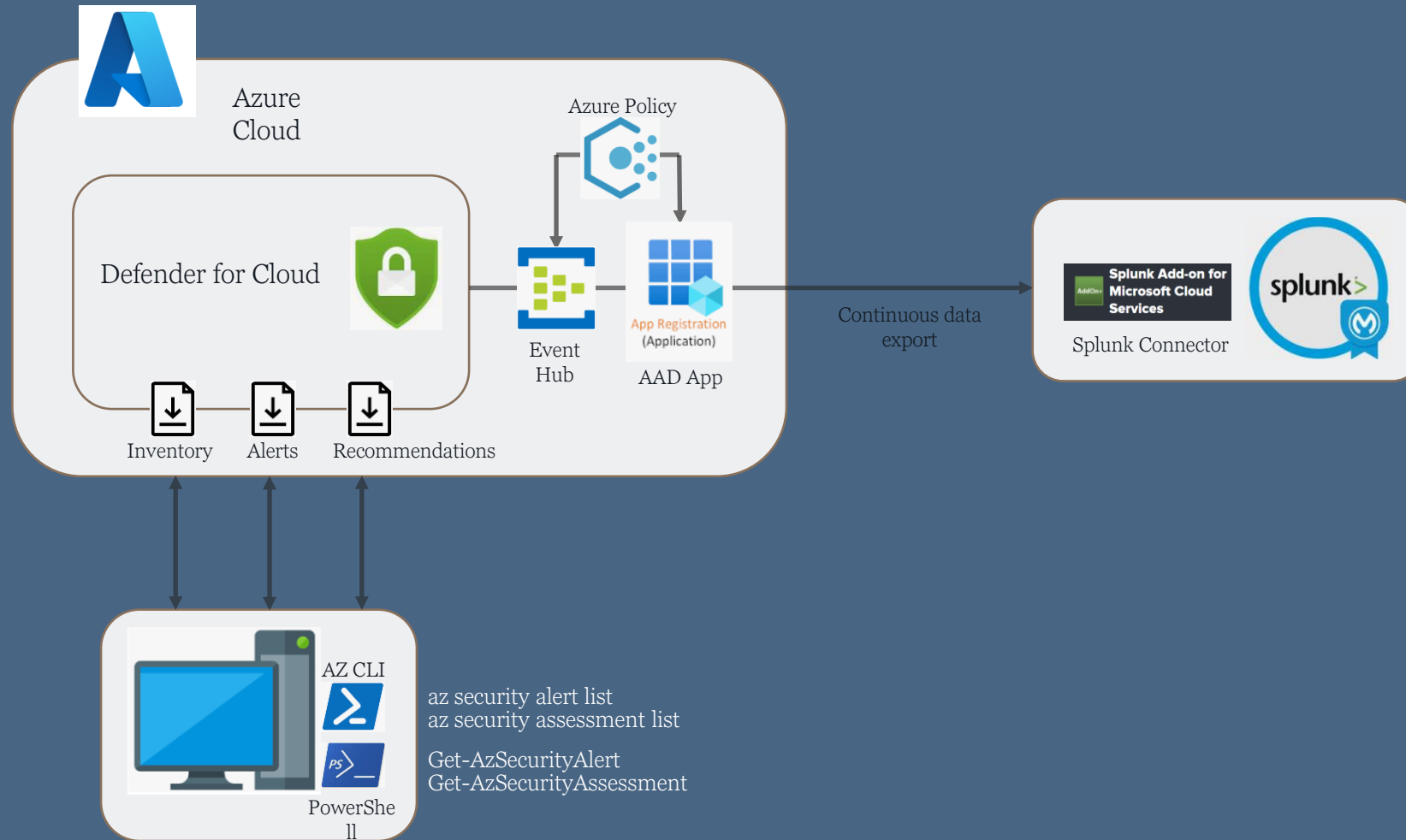
```
main.tf
1 # Configure the Azure provider
2 terraform {
3   required_providers {
4     azurerm = {
5       source = "hashicorp/azurerm"
6       version = "~> 3.0.2"
7     }
8   }
9   required_version = ">= 1.1.0"
10 }
11
12
13 provider "azurerm" {
14   features {}
15 }
16
17 /*
18 resource "azurerm_resource_group" "rg" {
```

```
variables.tf
1 variable "resource_groups" {
2   type = map(any)
3   description = "(Required) A list of Azure Resour
4 }
5
6 variable "global_tags" {
7   type = map(any)
8   description = "(Optional) A map of tags to be ap
9   default = {}
10 }
```

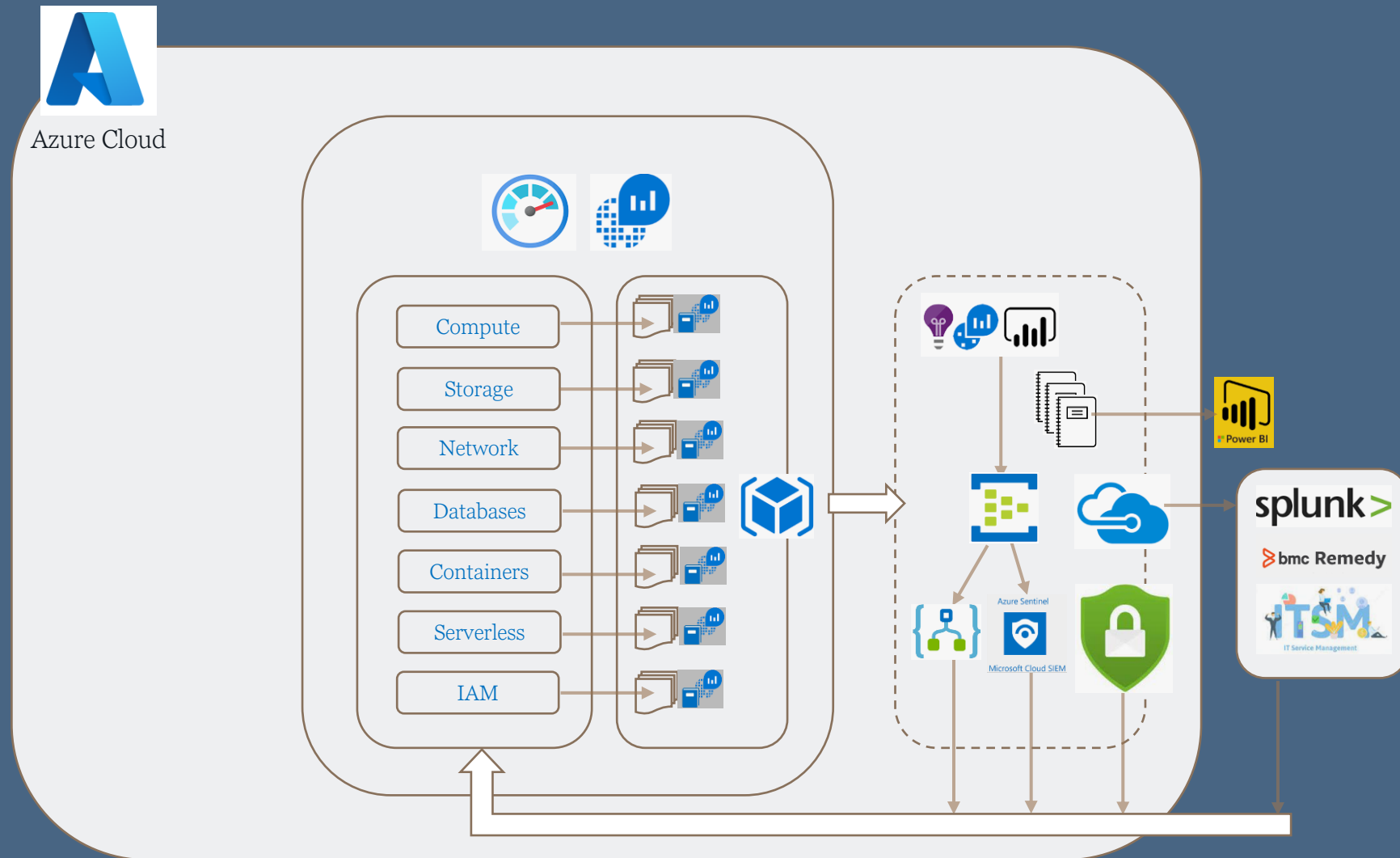
```
terraform.tfvars
1 global_tags = {
2   Provisioner = "Terraform"
3 }
4
5 resource_groups = {
6   us-southcentral-azcli-test-rg01 = {
7     location = "southcentralus",
8     tags = {
9       Owner = "cybergavin",
10      CostCenter = "C8888",
11      Description = "AZCLI Infrastructure" } }
12
13   us-southcentral-terraform-test-rg01 = {
14     location = "southcentralus",
15     tags = {
16       Owner = "cybergavin",
17       CostCenter = "C9999",
18       Description = "Terraform Infrastructure" } }
19 }
```

```
terminal
tshen@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
[]
tshen@HOUSTON:/mnt/f/Users/tshen/Documents/user_files/dcl/cloud/csp_azure/scripts/azcli$ az security alert list --output table
tshen@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"
  }
}
tshen@HOUSTON:/mnt/f/Users/tshen/Documents/user_files/dcl/cloud/csp_azure/scripts/azcli$
```

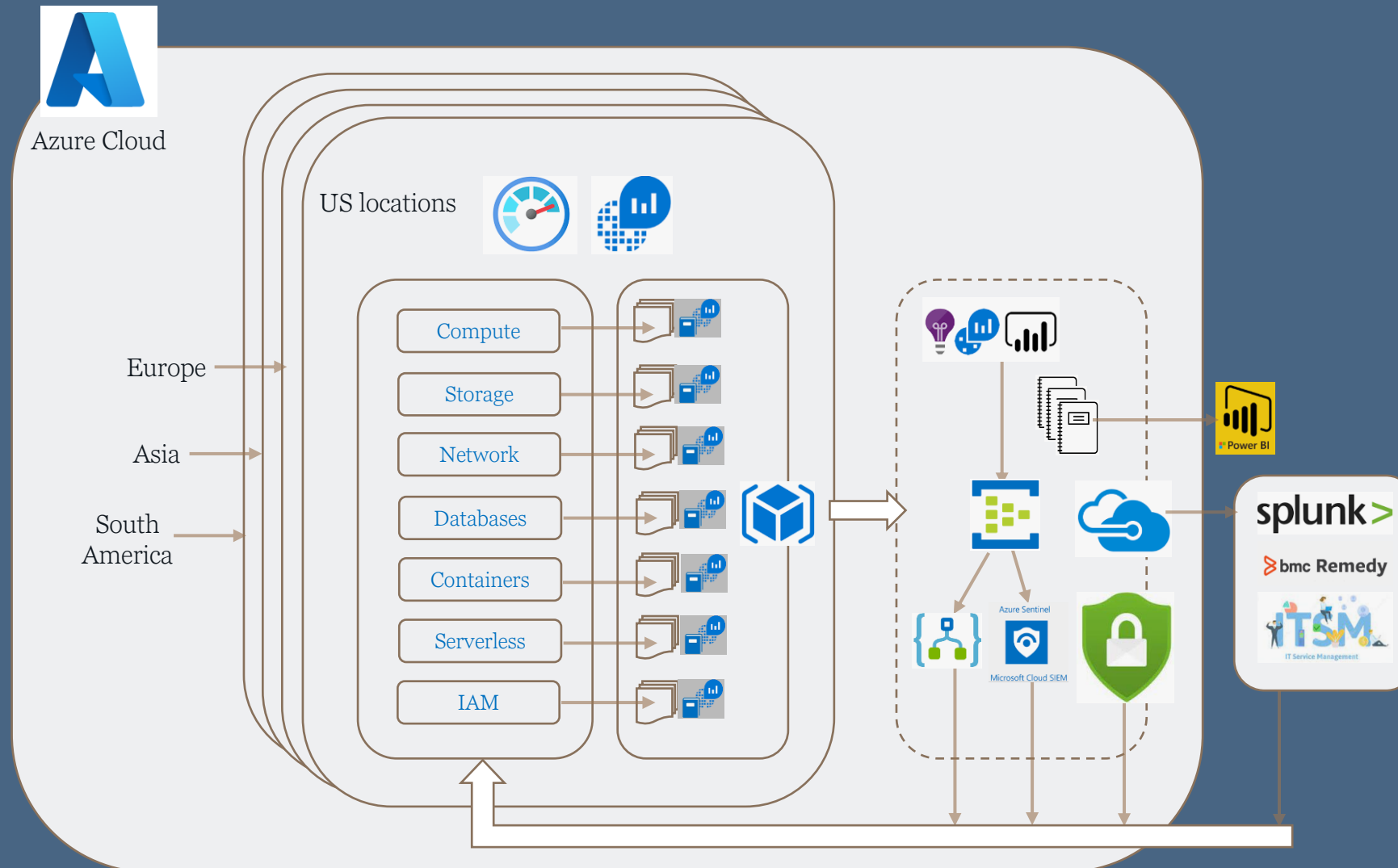
Design Component – Defender for Cloud



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

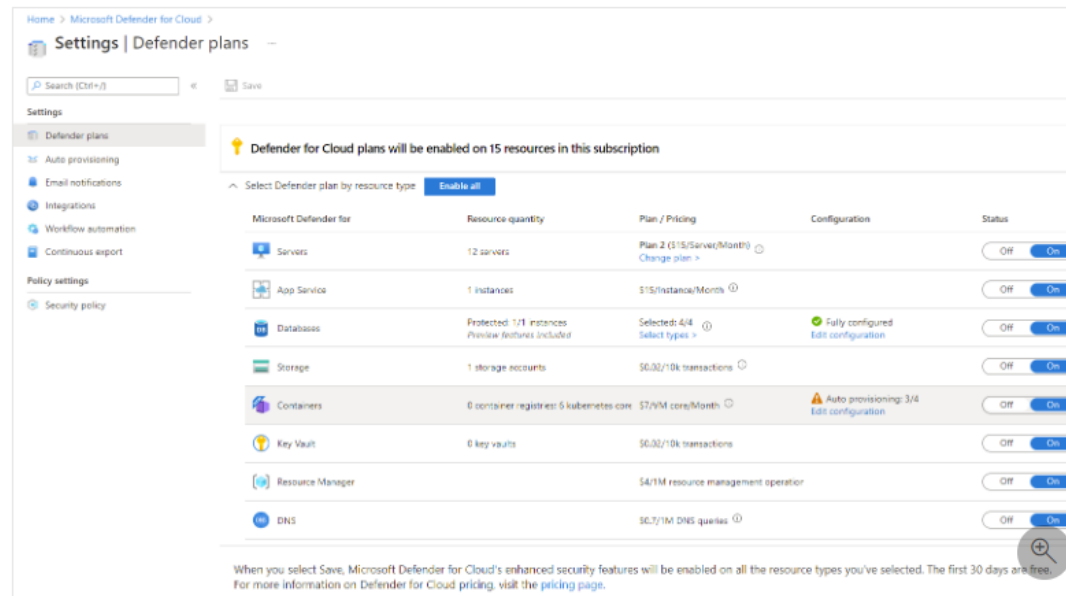
- **Microsoft Defender for Endpoint** - Microsoft Defender for Servers includes [Microsoft Defender for Endpoint](#) for comprehensive endpoint detection and response (EDR). Learn more about the benefits of using Microsoft Defender for Endpoint together with Defender for Cloud in [Use Defender for Cloud's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

Search (Ctrl+F) Save

Settings

- Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export

Policy settings

- Security policy

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) Change plan >		Off On
App Service	1 instances	\$15/Instance/Month ⓘ		Off On
Databases	Protected: 1/1 instances Preview features included	Selected: 4/4 ⓘ Select types >	Fully configured Edit configuration	Off On
Storage	1 storage accounts	\$6.02/10k transactions ⓘ		Off On
Containers	0 container registries: 5 kubernetes.com	\$7/VM core/Month ⓘ	Auto provisioning: 3/4 Edit configuration	Off On
Key Vault	0 key vaults	\$6.02/10k transactions		Off On
Resource Manager		\$4/1M resource management operations		Off On
DNS		\$0.7/1M DNS queries ⓘ		Off On

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 'Getting started' page. The 'Upgrade' tab is selected, which lists subscriptions and workspaces eligible for onboarding. The page includes a search bar, navigation tabs (Upgrade, Get started, Install agents), and a sidebar with various security features. The main content area displays a list of subscriptions and a summary of resources.

Enable Microsoft Defender for Cloud's enhanced security features on your subscriptions.
Get started with a 30-day free trial
Upgrade to get advanced capabilities including hybrid support, networking, security policies, just-in-time administration and adaptive application controls. [Learn more >](#)

Cloud security posture management
Get continuous assessment and prioritized security recommendations with secure score, and verify compliance with regulatory standards.

Cloud workload protection for machines
Makes workloads running on Azure, hybrid, and multi-cloud environments. Protections include secure FDR, vulnerability scanning, workload hardening, and more.

Advanced threat protection for PaaS
Protect clouds and detect unusual activities on PaaS workloads including App Service plans, Storage accounts, and SQL servers.

Enable Defender for Cloud on 1 subscriptions

Name	ID	Total resources	Microsoft Defender pl...
<input checked="" type="checkbox"/> ID		Loading...	On - Partial (30 trial days)
<input type="checkbox"/> DEMO		0	On - Partial (trial expired)
<input type="checkbox"/> DEMO		0	On - Partial (trial expired)
<input type="checkbox"/> DEMO		0	On - Partial (trial expired)
<input type="checkbox"/> DEMO		0	Off
<input type="checkbox"/> ...		0	Off

Total: 0 resources

Resource	Count	Price	Unit
0 Servers	0	\$15	Server/Month
0 App Service instances	0	\$15	Instance/Month
0 Azure SQL Databases	0	\$15	Server/Month
0 SQL servers on machines	0	\$0.015	Server/Month

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

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.

Enable Defender for Cloud on 4 subscriptions

<input type="checkbox"/>	Name	Total resources	Microsoft Defender pl...
<input checked="" type="checkbox"/>	DEMO	0	On - Partial (30 trial days l...
<input checked="" type="checkbox"/>	DEMO	499	On - Partial (Trial expired)
<input checked="" type="checkbox"/>	DEMO	27	On - Partial (Trial expired)
<input checked="" type="checkbox"/>	DEMO	189	On - Partial (Trial expired)
<input type="checkbox"/>	z	0	Off
<input type="checkbox"/>	u	0	Off

Upgrade

Total: 715 resources

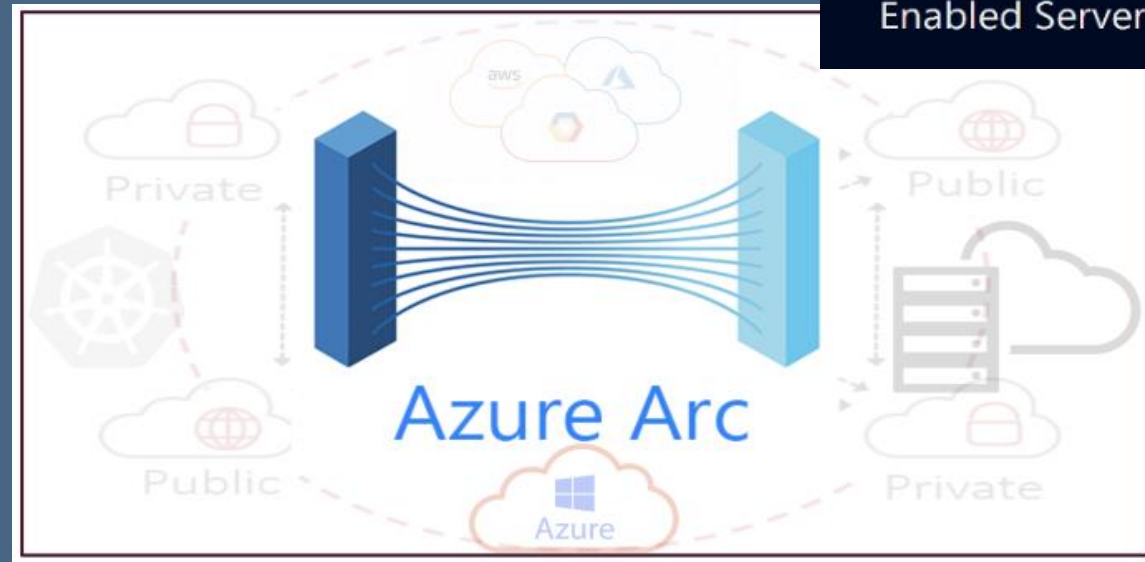
214 Servers	\$15	Server/Month
19 App Service instances	\$15	Instance/Month
17 Azure SQL Databases	\$15	Server/Month
0 SQL servers on machines	\$15	Server/Month
	\$0.015	Core/Hour

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](#).

Design Component – Defender for Cloud

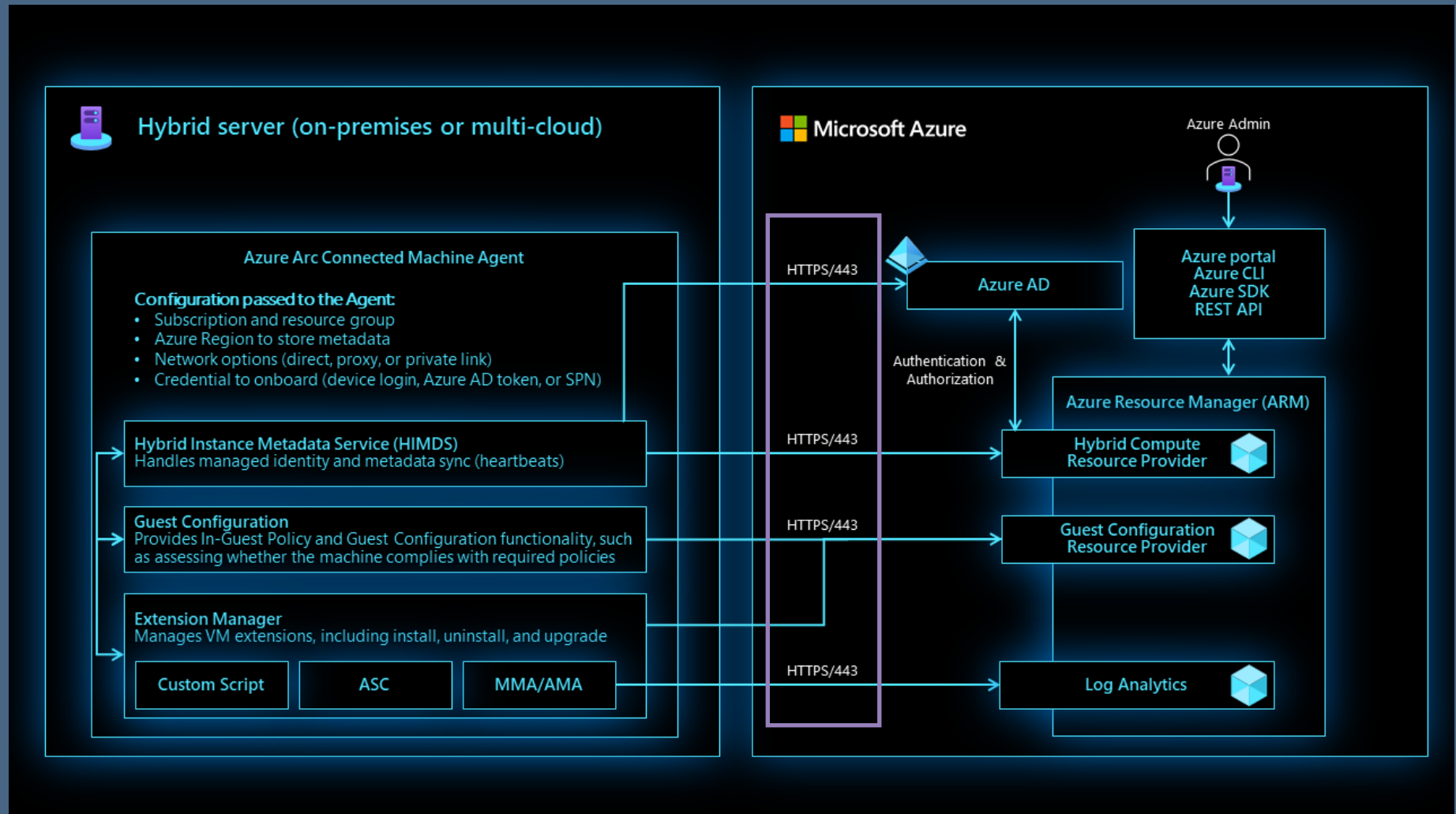
DFC covers non-Azure servers by agents

Arc-Enabled Servers



Design Component – Defender for Cloud

DFC communicates with agents and supporting services via HTTPS/443

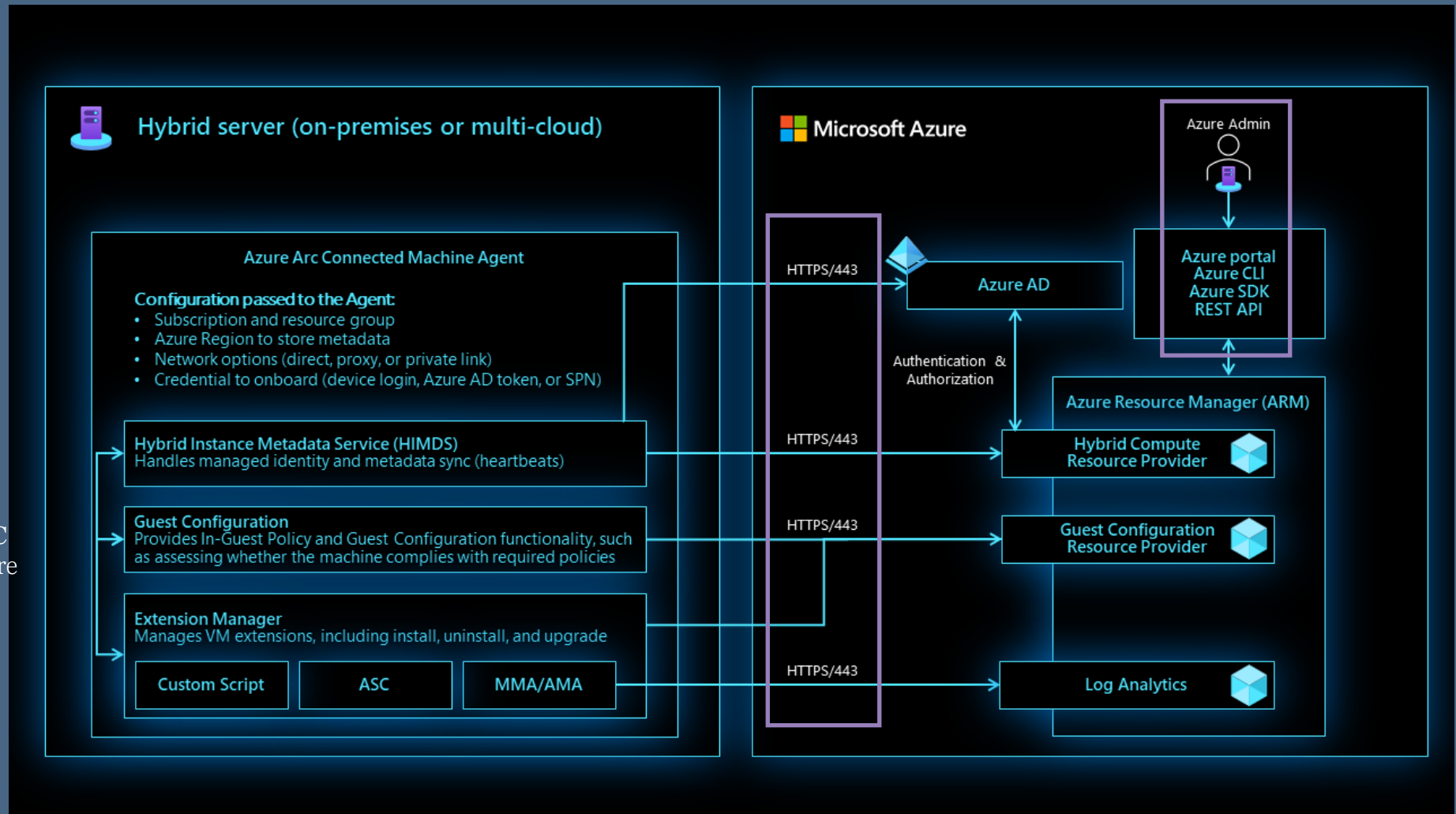


DFC covers non-Azure servers by agents

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



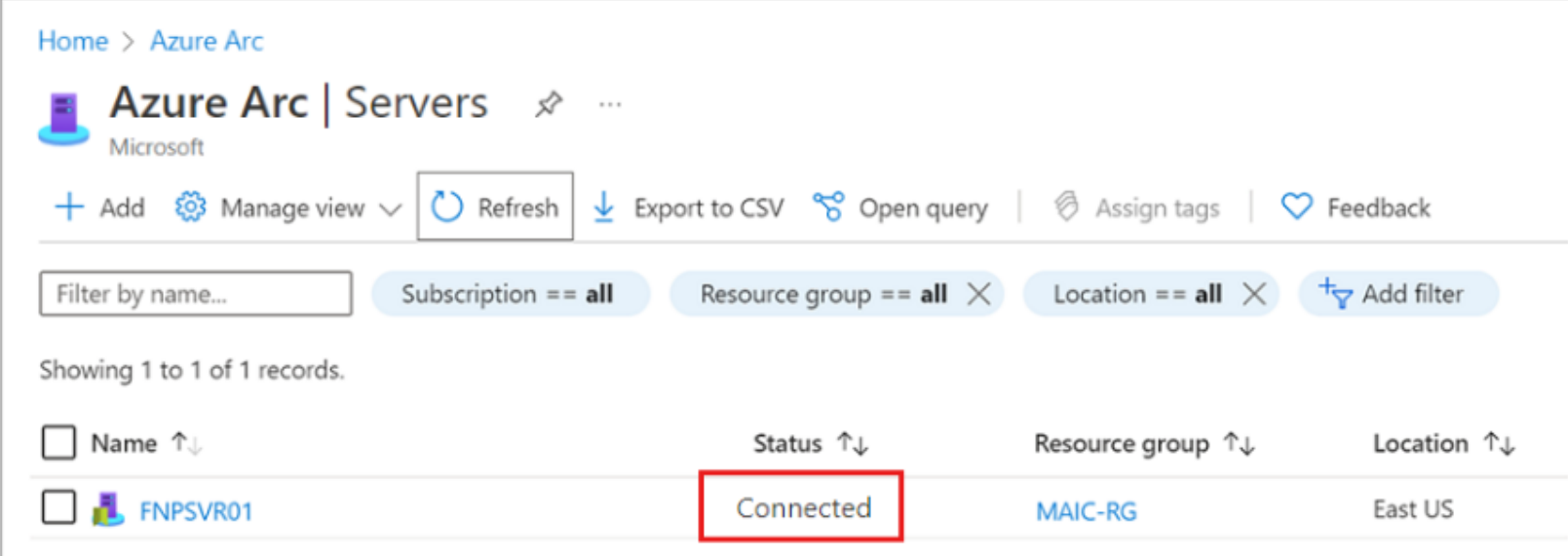
DFC covers non-Azure servers by agents

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](#).



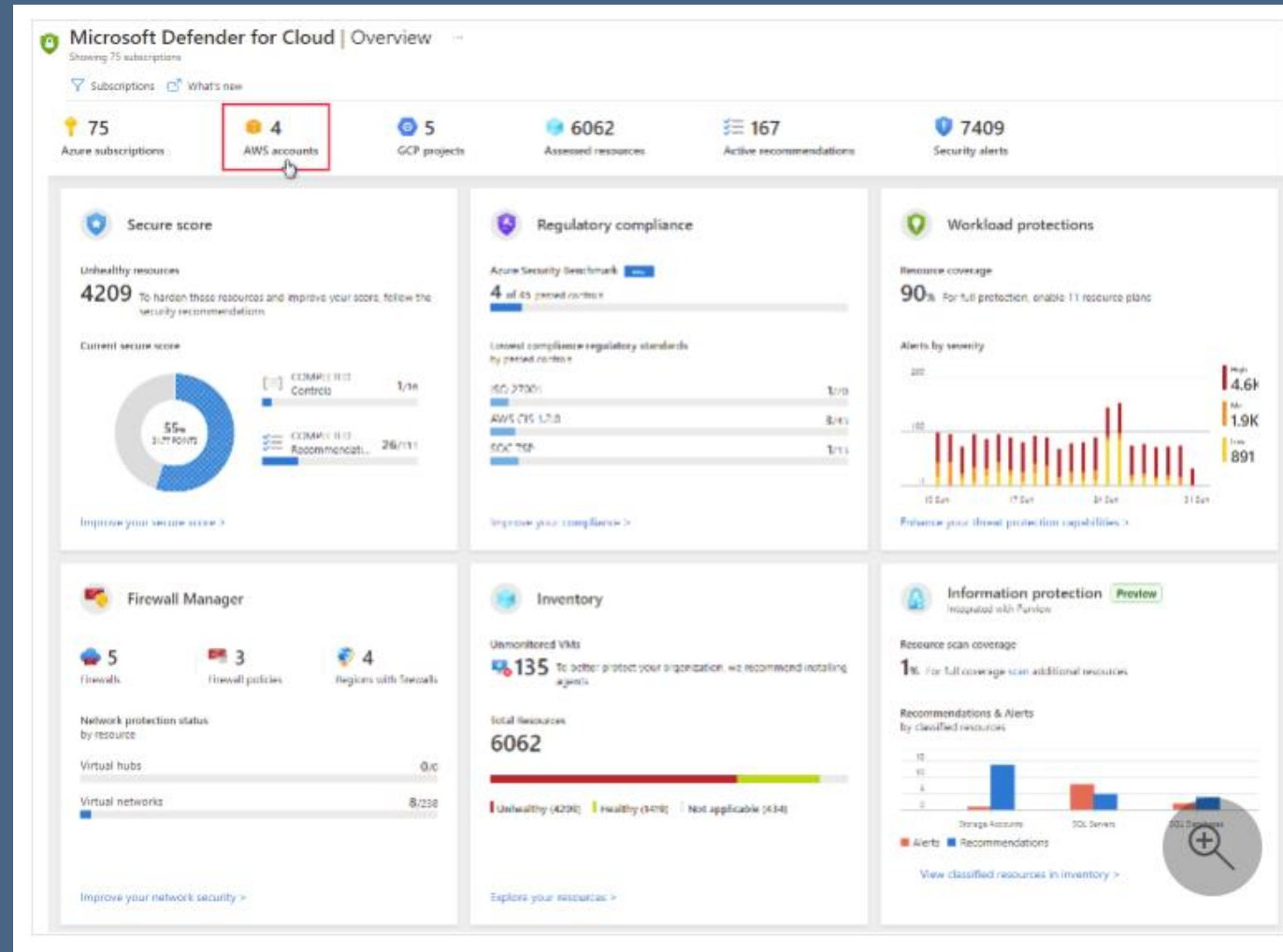
The screenshot shows the 'Azure Arc | Servers' page in the Azure portal. The page title is 'Azure Arc | Servers' with a Microsoft logo. Below the title, there are several action buttons: '+ Add', 'Manage view' (with a dropdown arrow), 'Refresh' (circled in red), 'Export to CSV', 'Open query', 'Assign tags', and 'Feedback'. Below these buttons, there is a filter bar with a text input 'Filter by name...', and three filter buttons: 'Subscription == all', 'Resource group == all' (with a close icon), and 'Location == all' (with a close icon). There is also an 'Add filter' button. Below the filter bar, it says 'Showing 1 to 1 of 1 records.' Below this, there is a table with columns: 'Name' (with a checkbox and sort icon), 'Status' (with a sort icon), 'Resource group' (with a sort icon), and 'Location' (with a sort icon). The table has one row with the following data: 'FNPSVR01' (with a checkbox and server icon), 'Connected' (circled in red), 'MAIC-RG', and 'East US'.

Name	Status	Resource group	Location
<input type="checkbox"/> FNPSVR01	Connected	MAIC-RG	East US

DFC covers non-Azure servers by agents

Design Component – Defender for Cloud

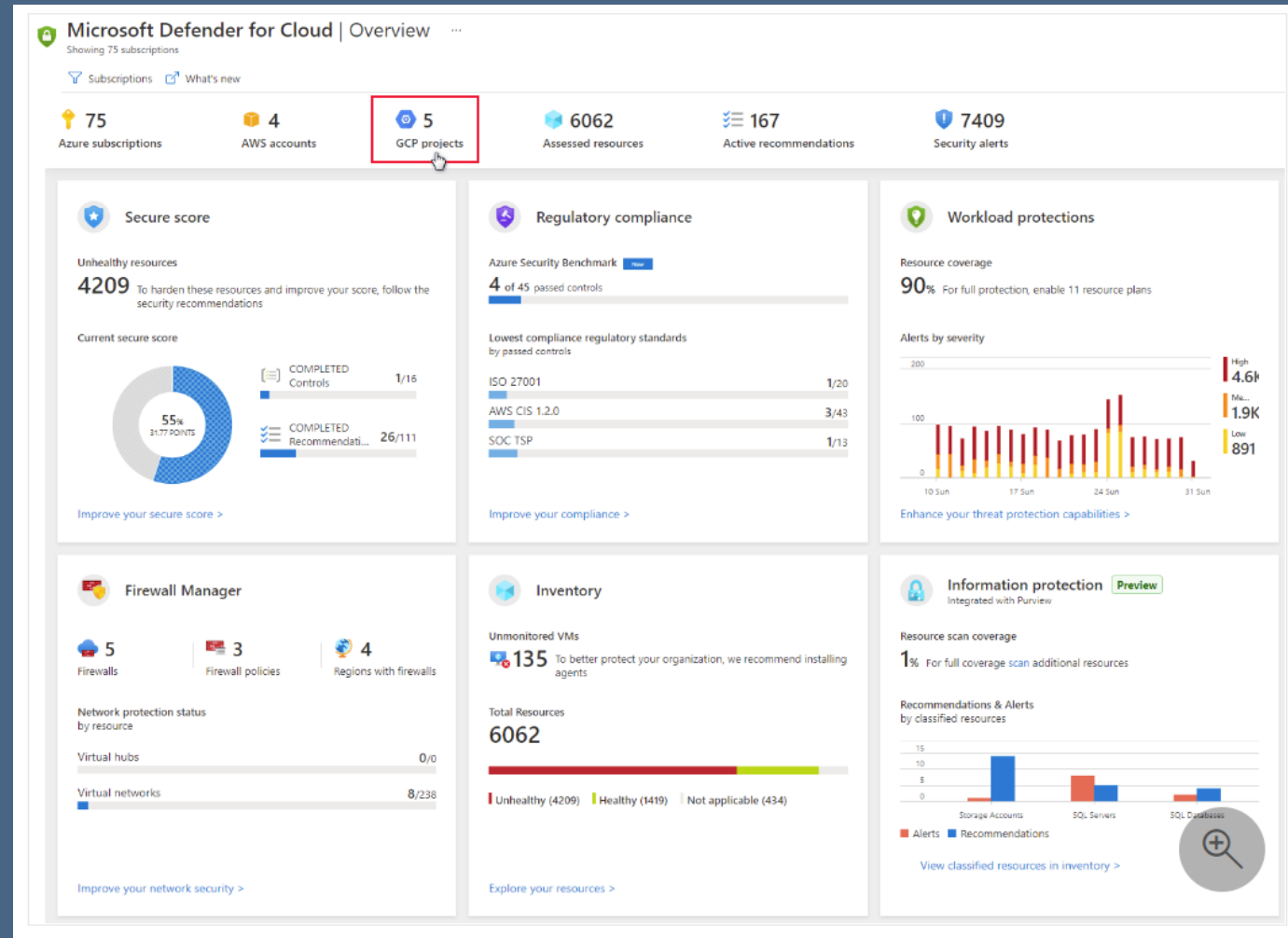
Example of AWS inventory



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


Microsoft Defender for Endpoint



Core Defender Vulnerability Management


Attack surface reduction


Next-generation protection


Endpoint detection and response


Automated investigation and remediation


Microsoft Threat Experts

Centralized configuration and administration, APIs

Plan	What's included
Defender for Endpoint Plan 1	<ul style="list-style-type: none">• 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

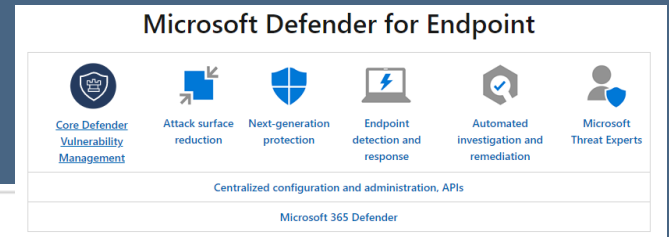
MDE has two plans. Plan 1 covers devices

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

Azure / Security / Microsoft Defender for Cloud /

Overview of Microsoft Defender for Servers

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

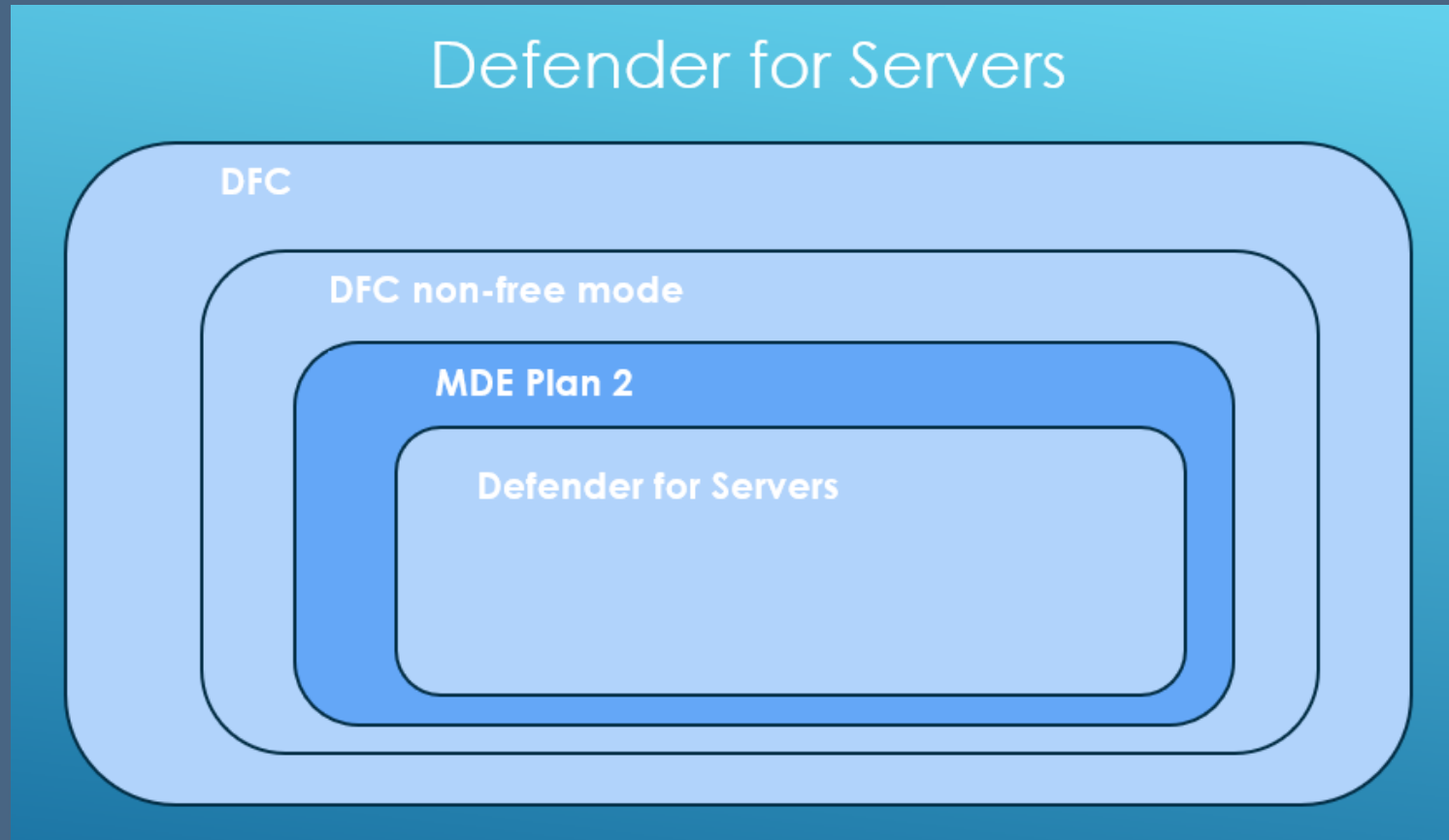
Microsoft Defender for Servers is one of the enhanced security features of Microsoft Defender for Cloud. Use it to add threat detection and advanced defenses to your Windows and Linux machines whether they're running in Azure, AWS, GCP, and on-premises environment.

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](#)

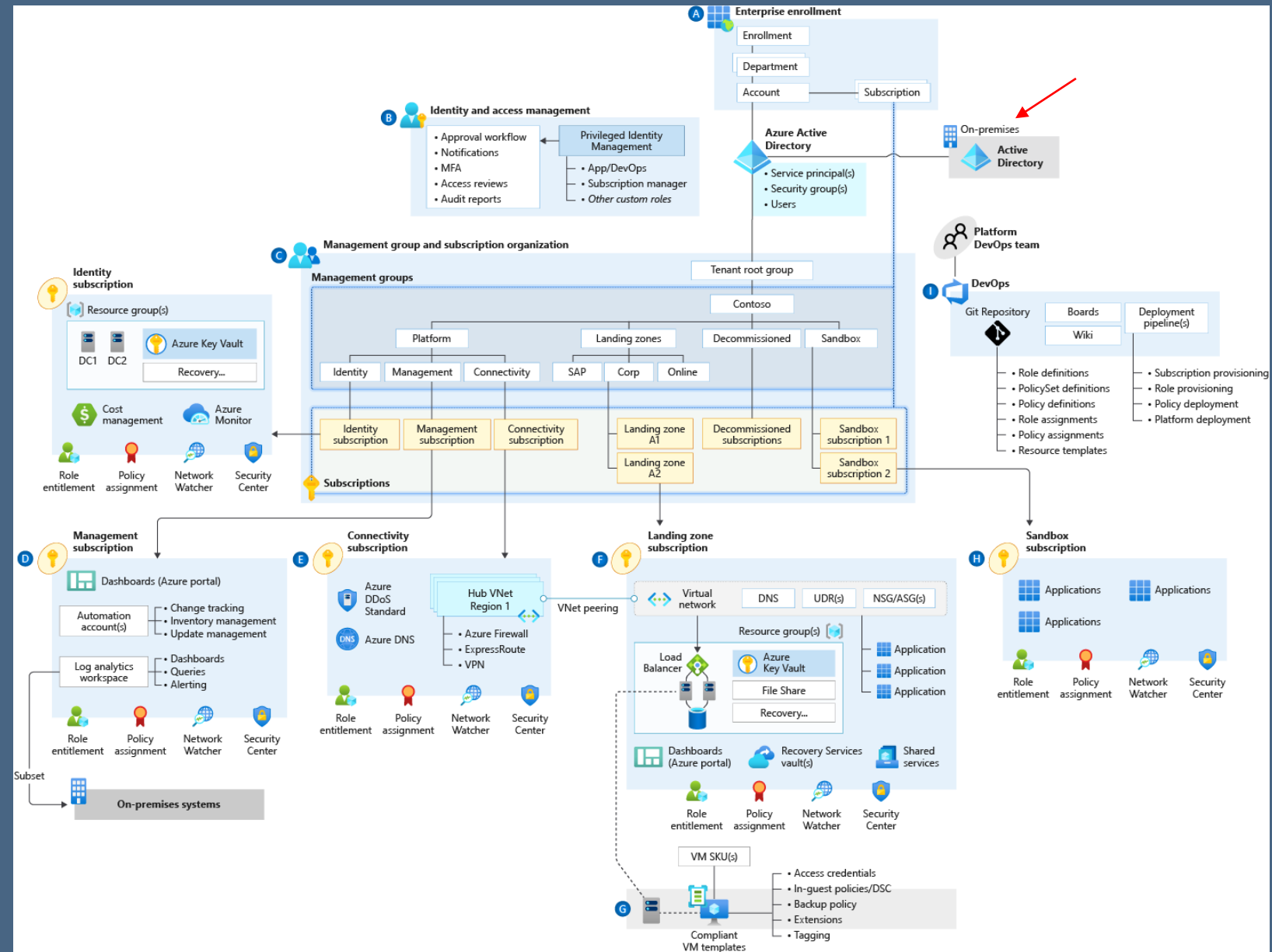
Defender for Servers supports security for servers in a hybrid and multi-cloud environment.
Defender for Servers and MDE Plan 2 overlap in protecting servers

Design Component – Defender for Cloud



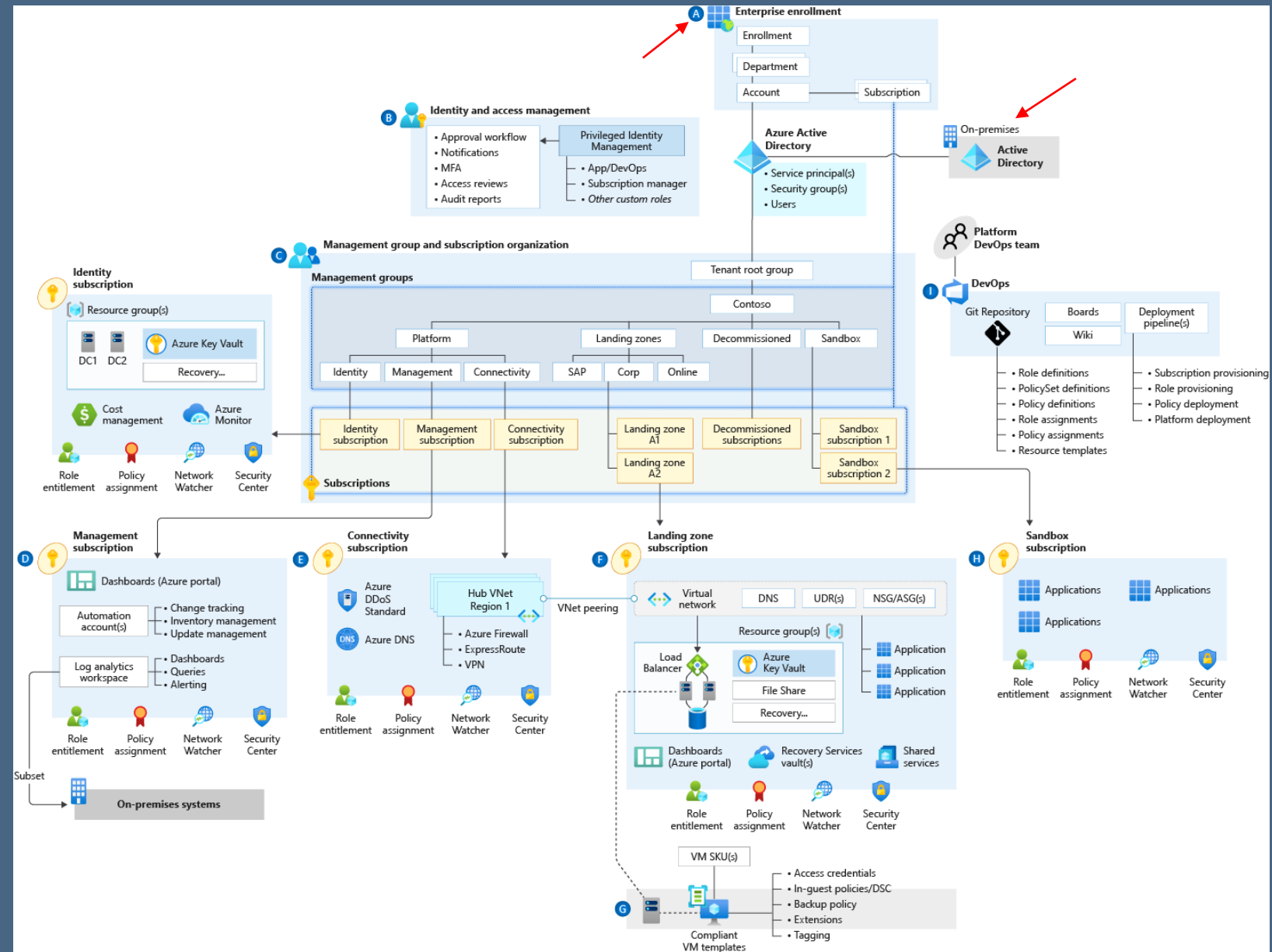
Putting it all together

- Hybrid including both Azure and on-prem



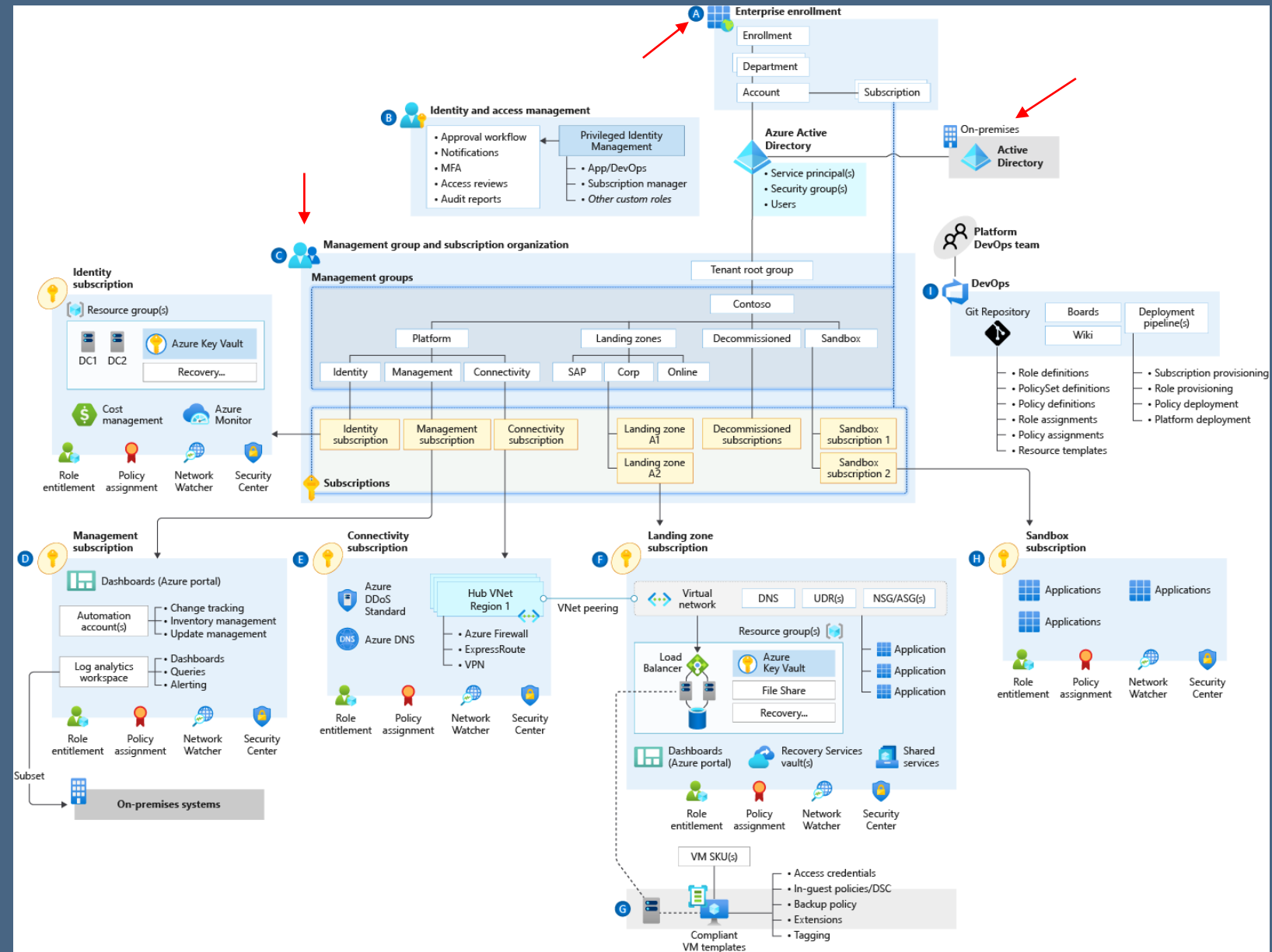
Putting it all together

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

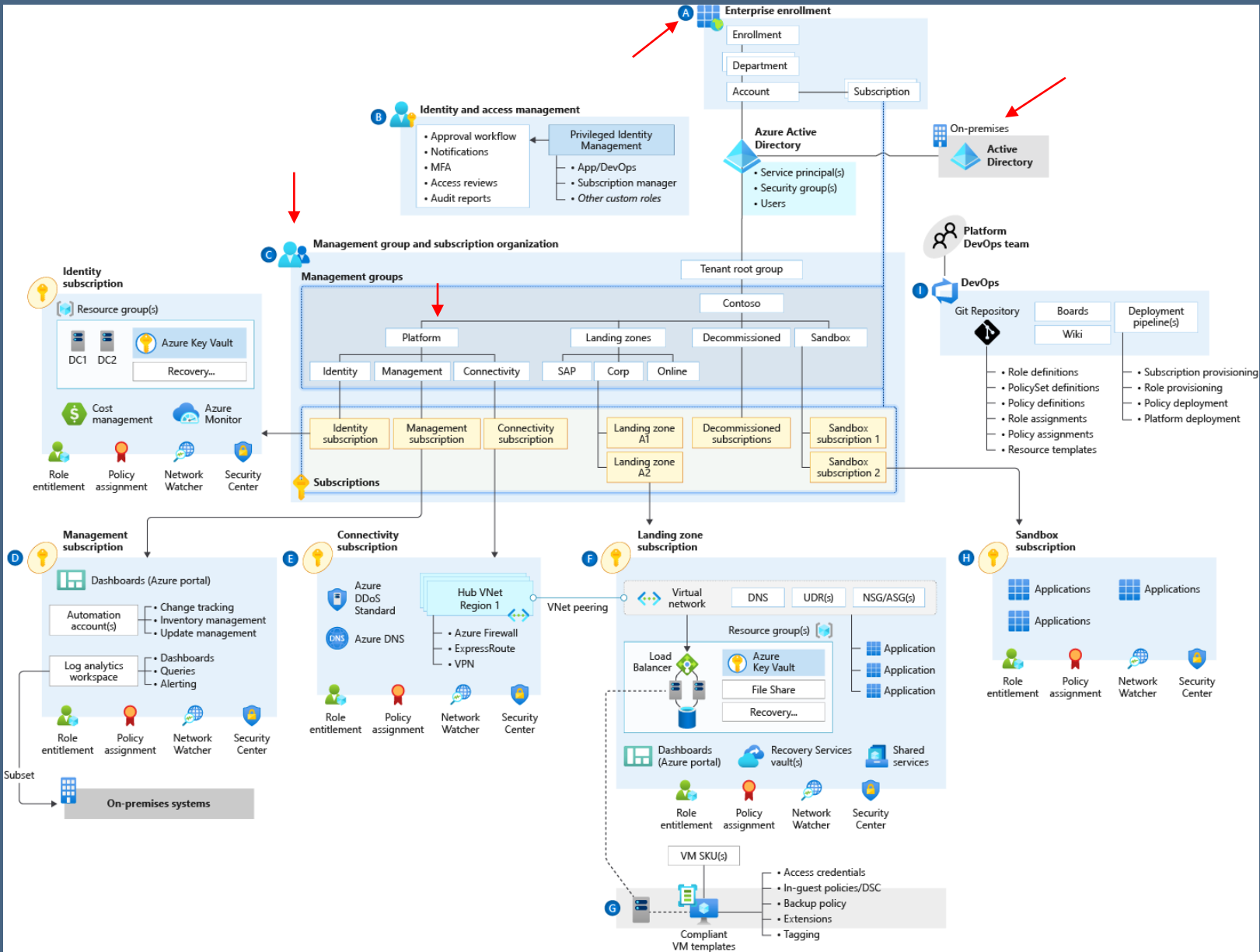


Putting it all together

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

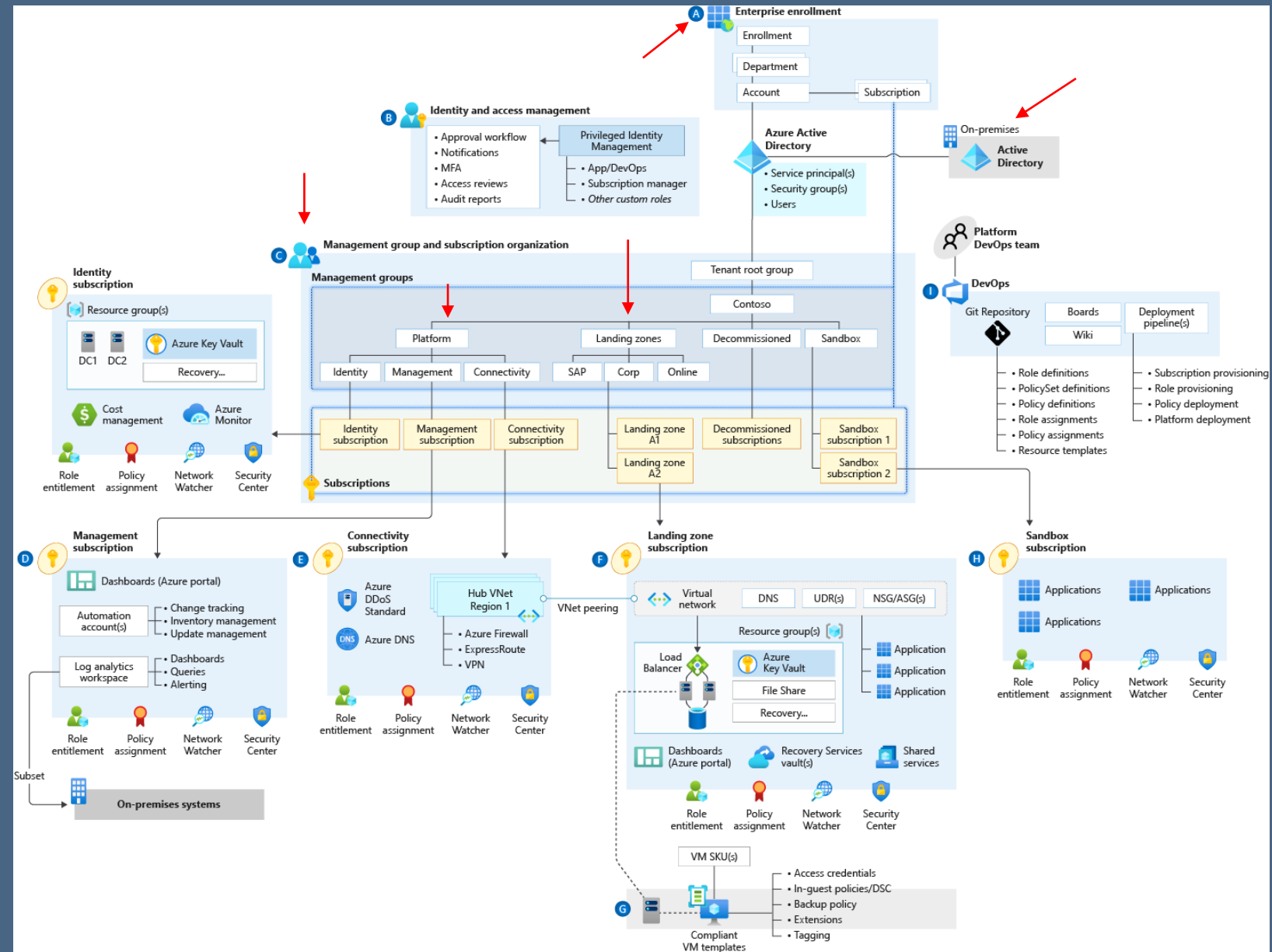


- Hybrid including both Azure and on-prem
- EA enrollment
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)



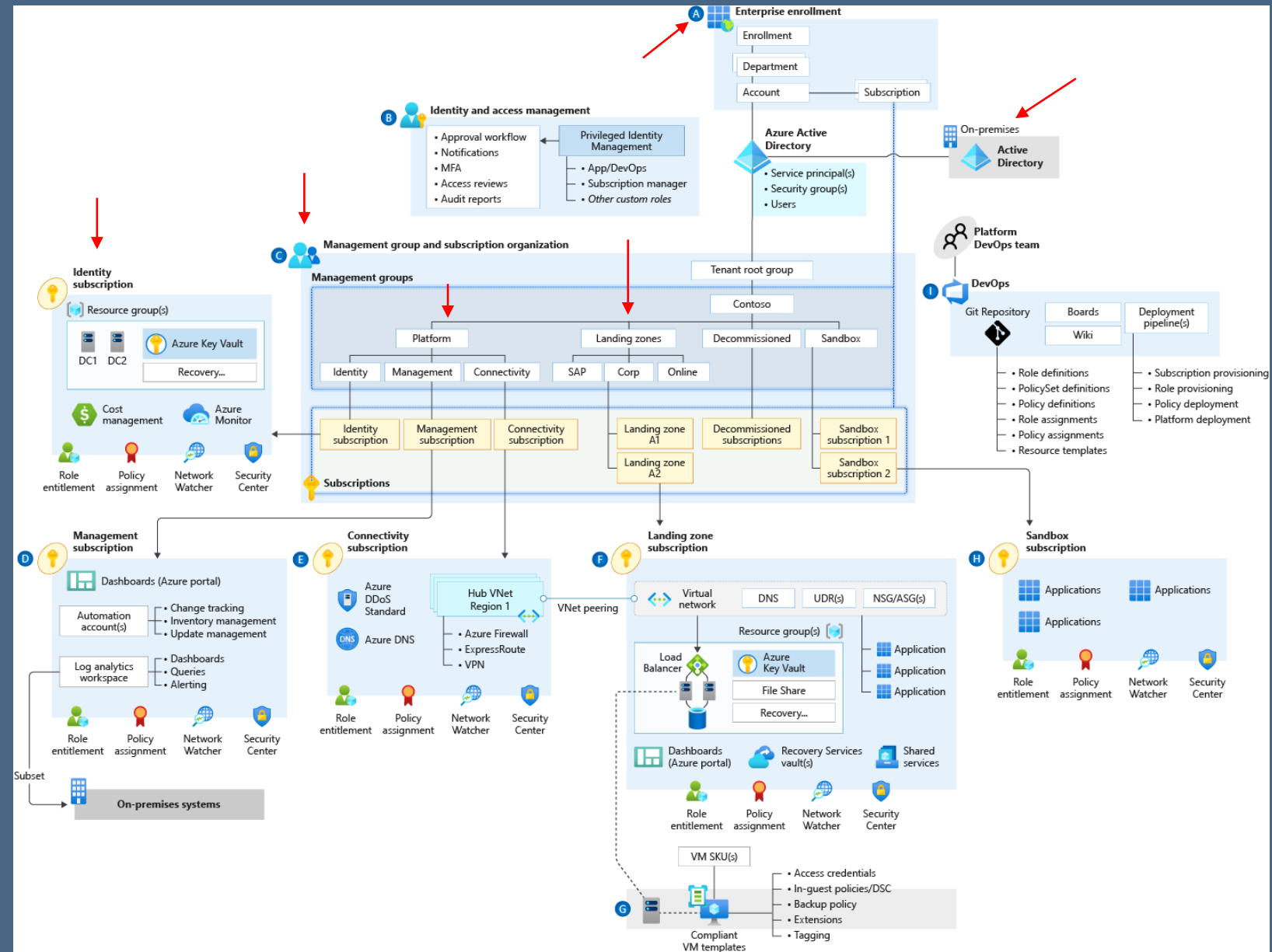
Putting it all together

- 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



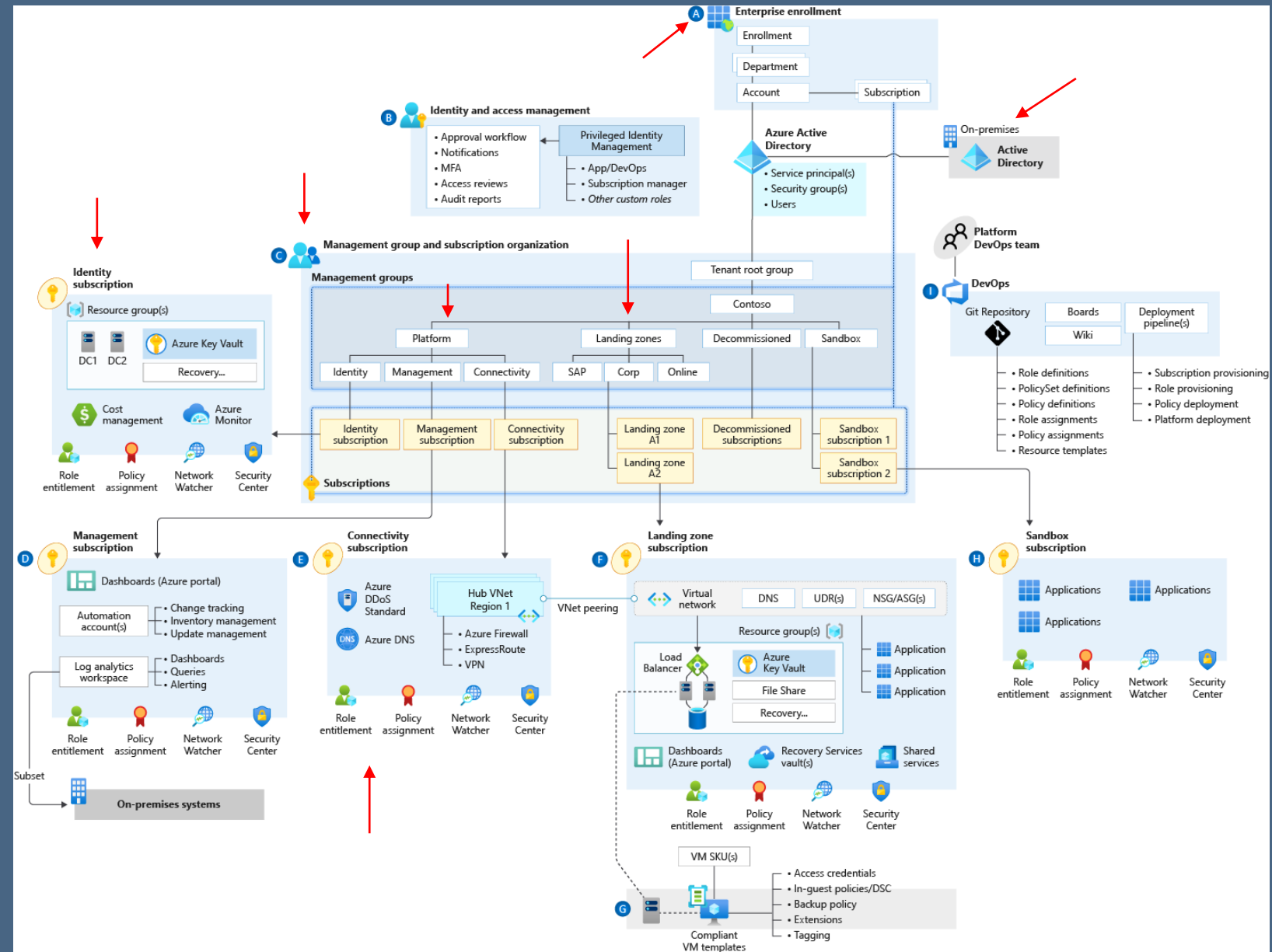
Putting it all together

- 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)



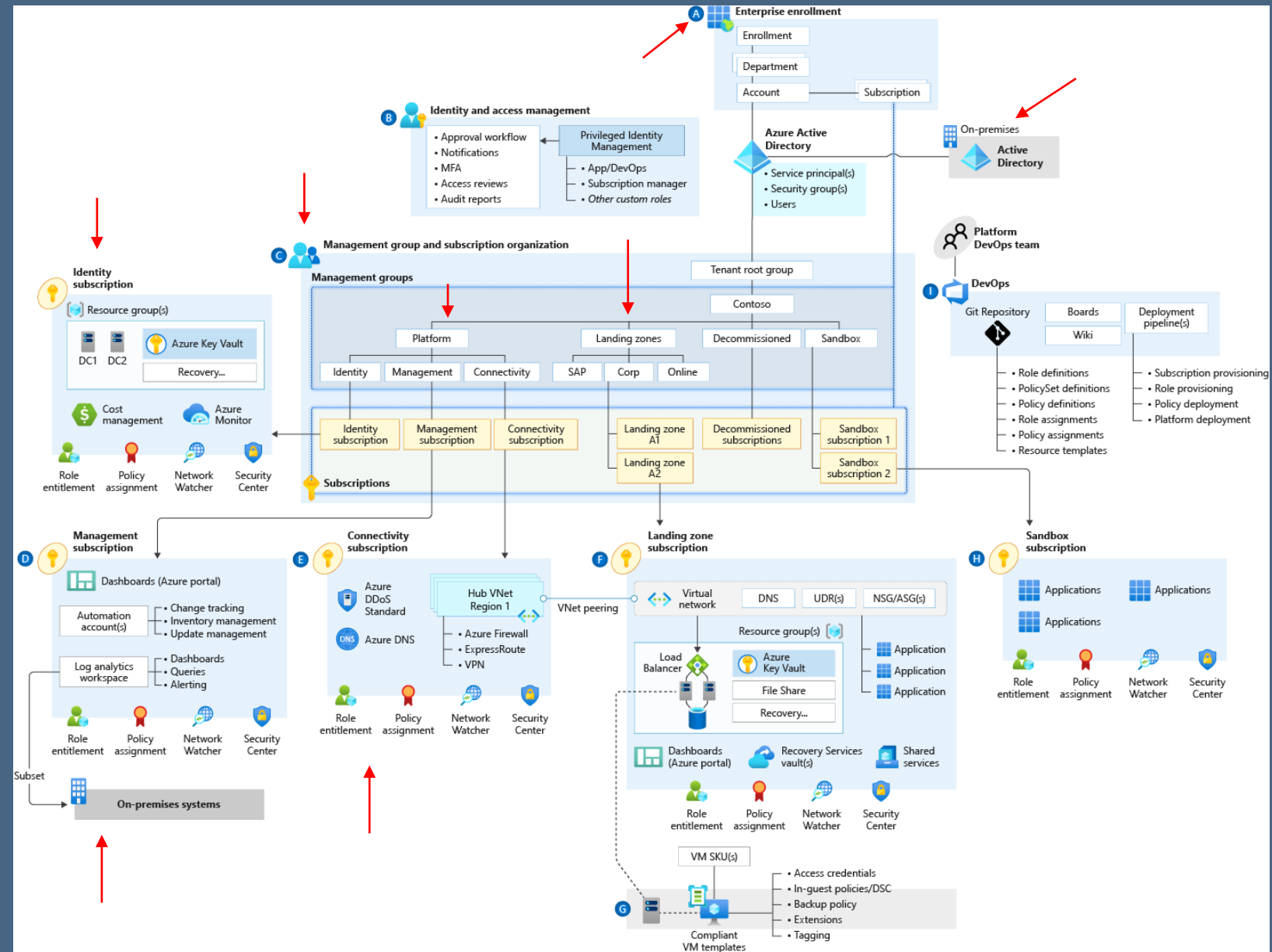
Putting it all together

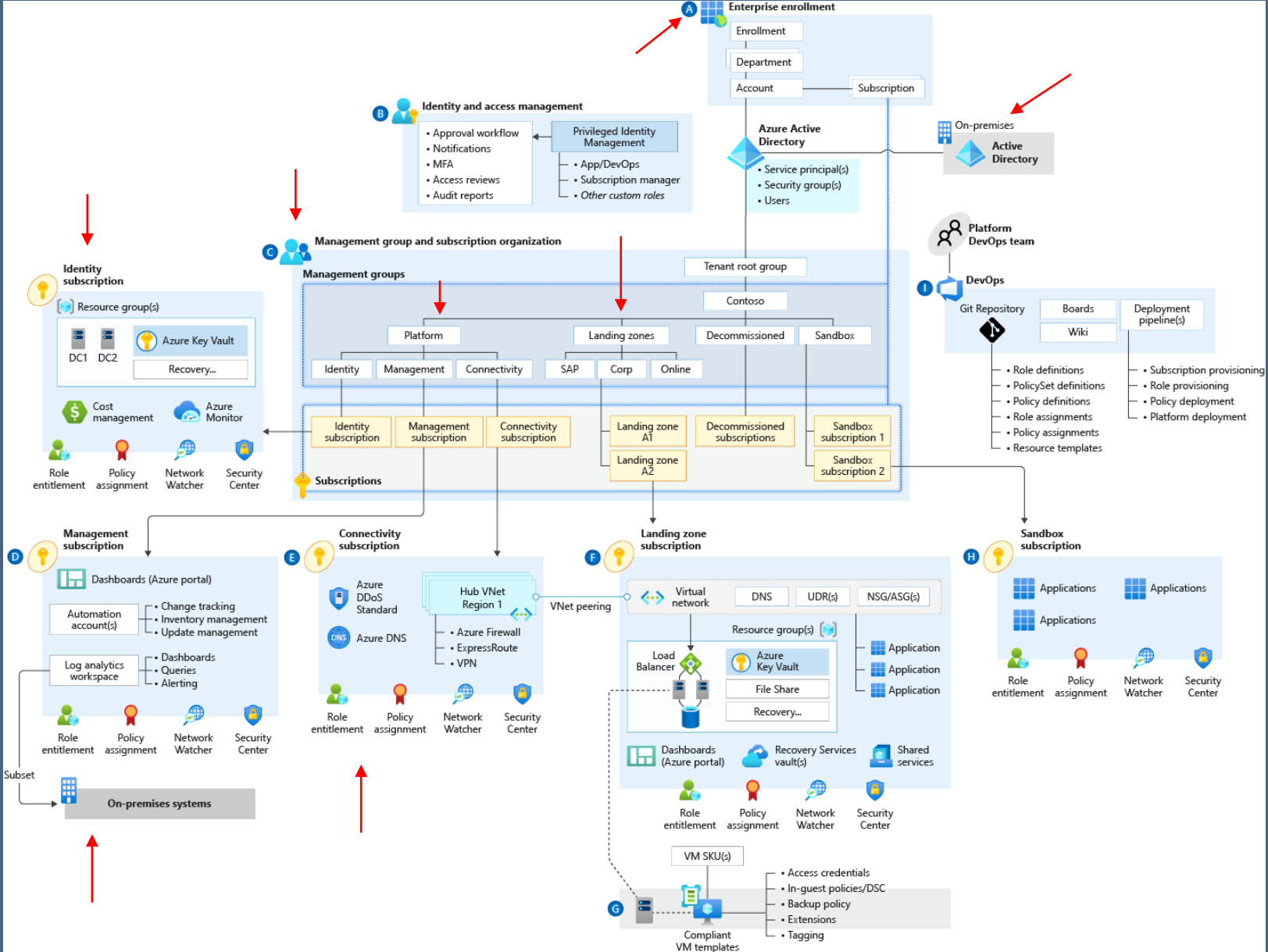
- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)



Putting it all together

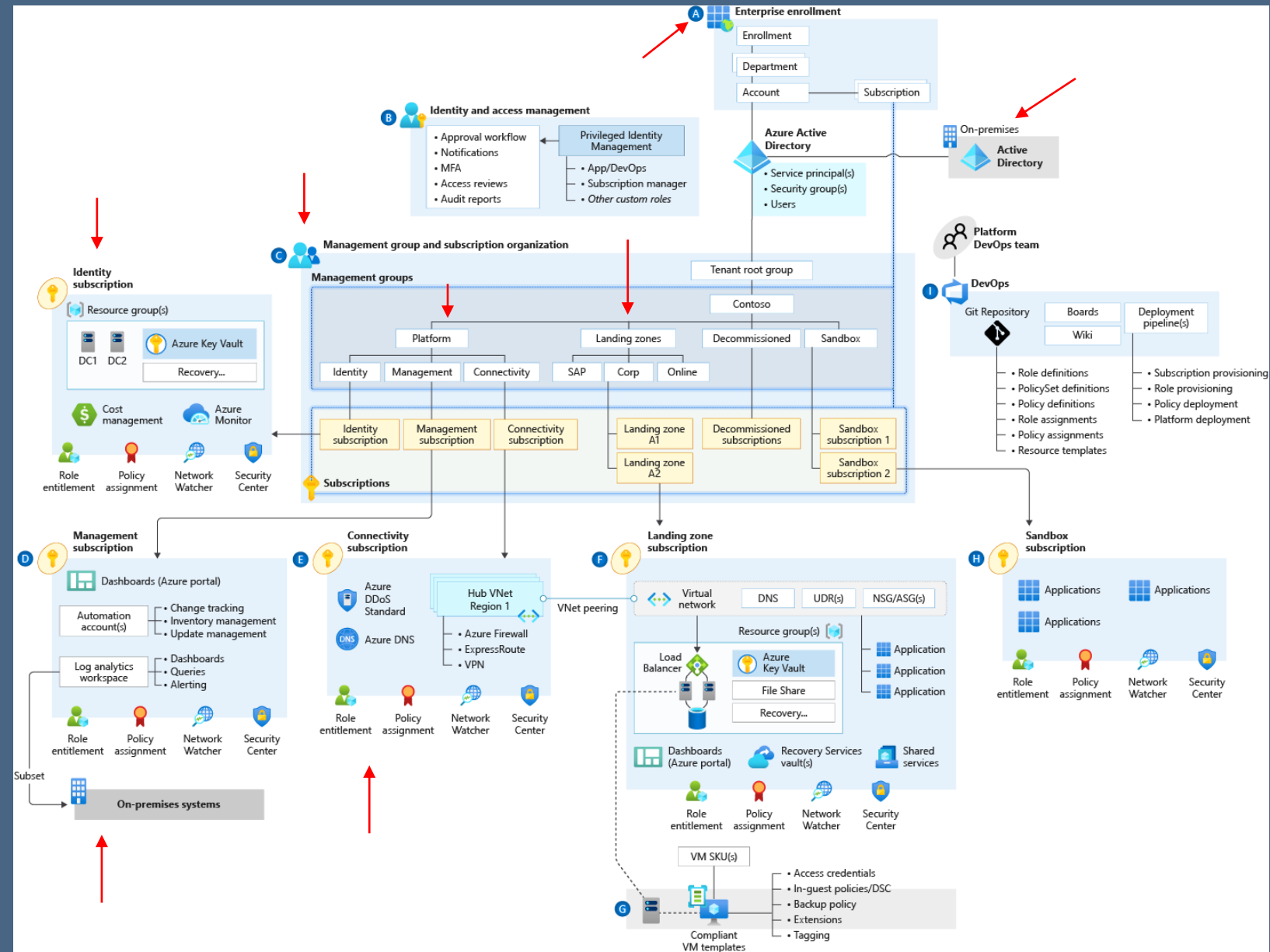
- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)
- Management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





Putting it all together

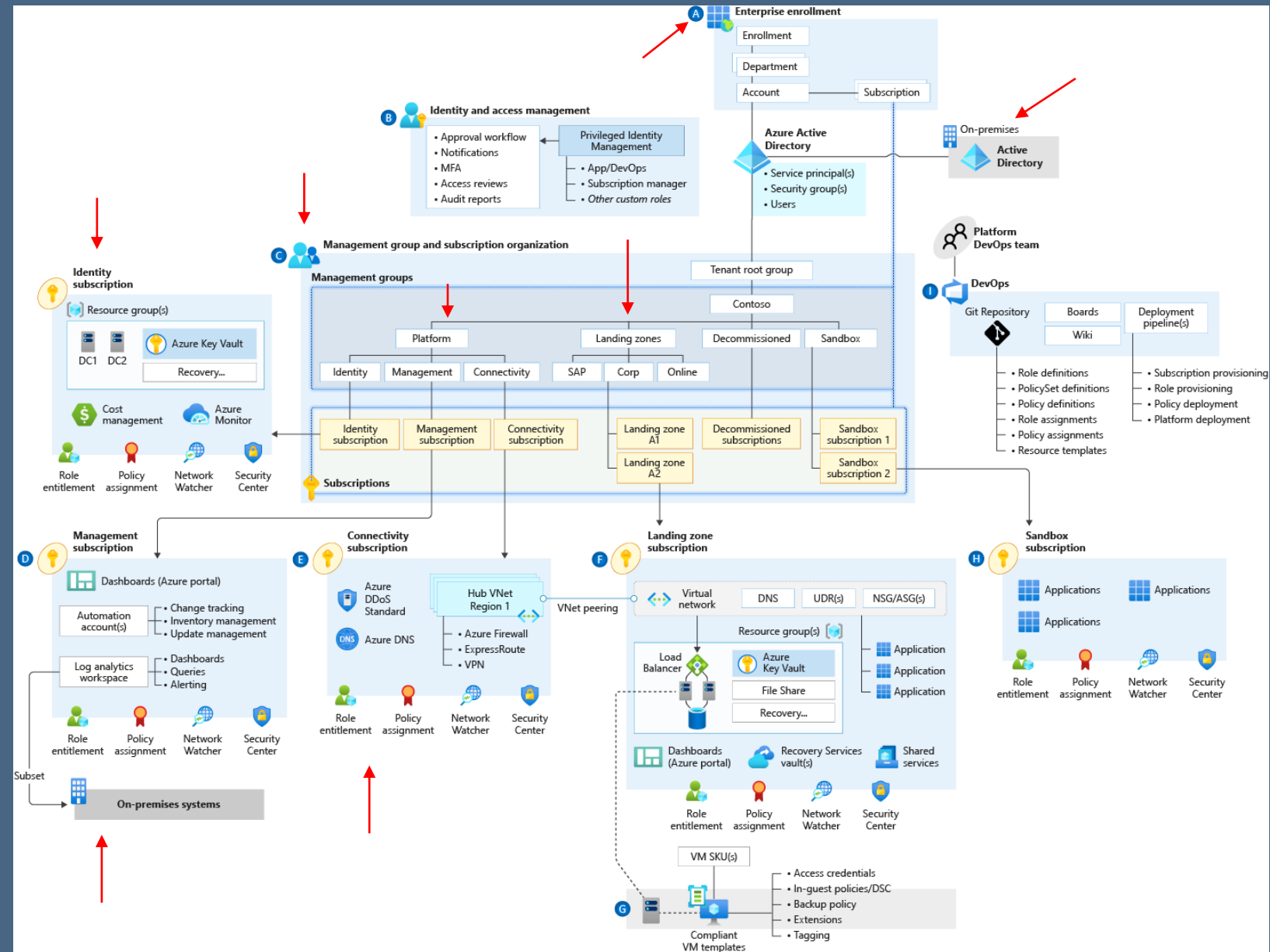
- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)
- Management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





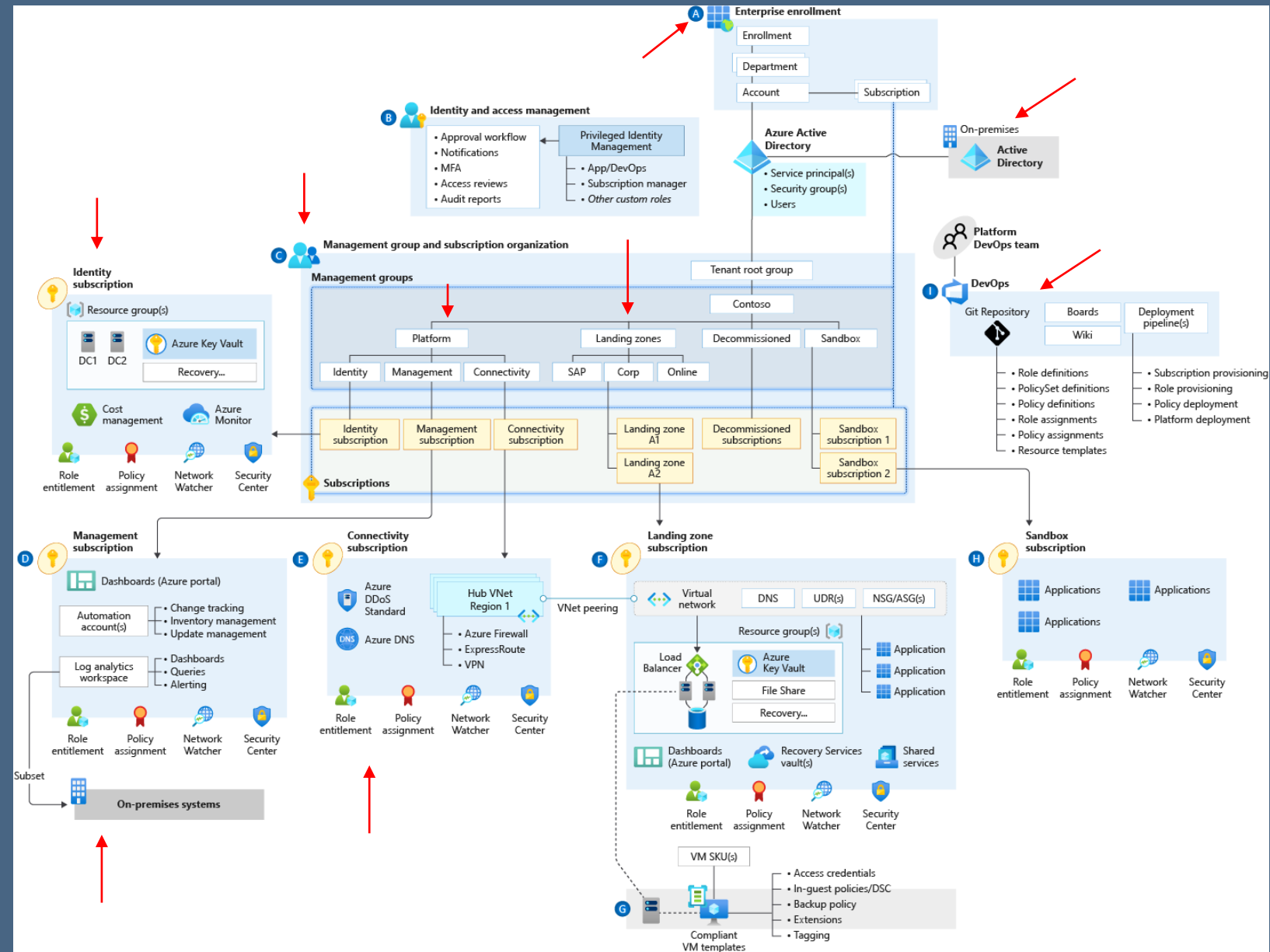
Putting it all together

- 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)
- AAD B2C, CASB and the like for customer-facing applications and external use (not shown)

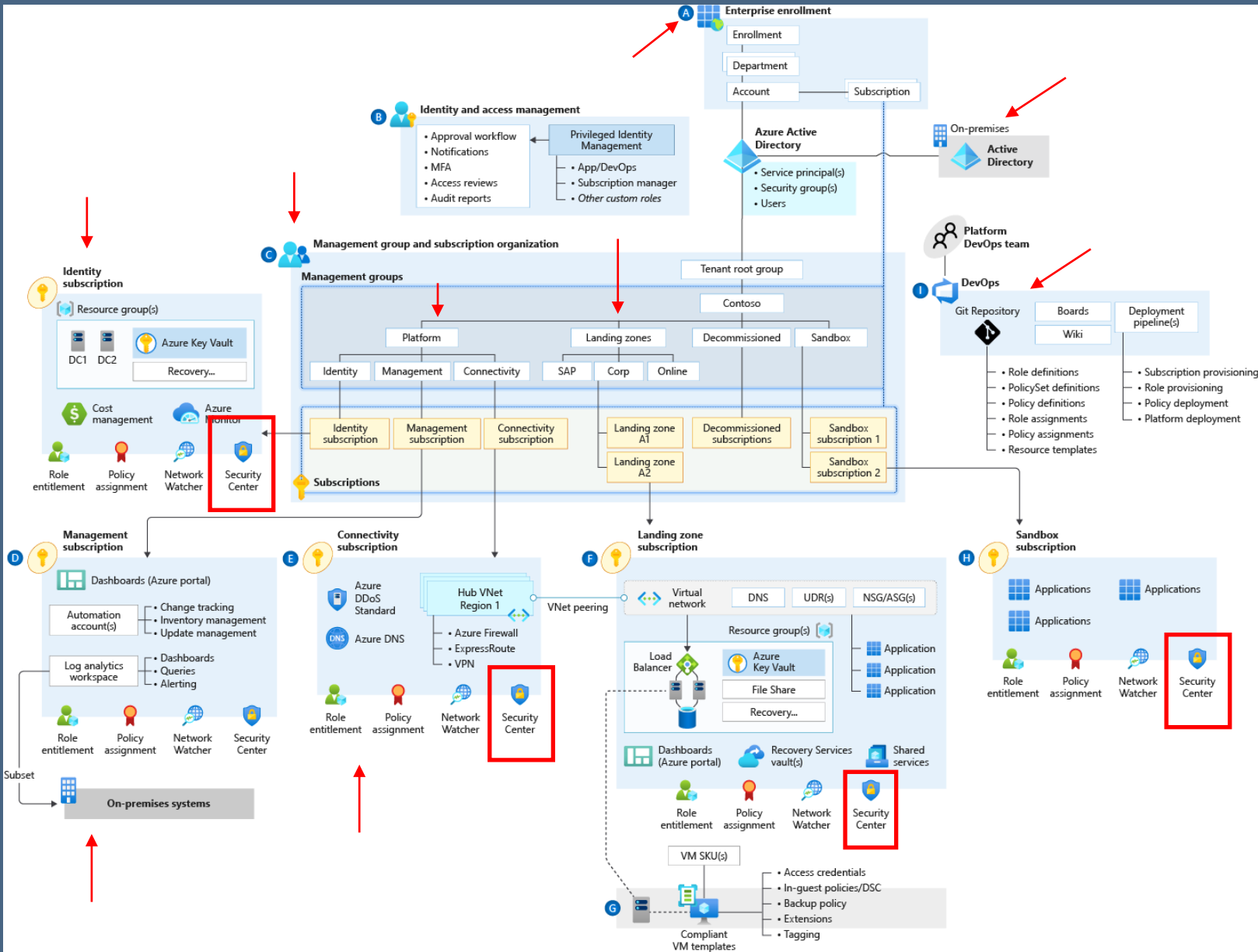


Putting it all together

- 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)

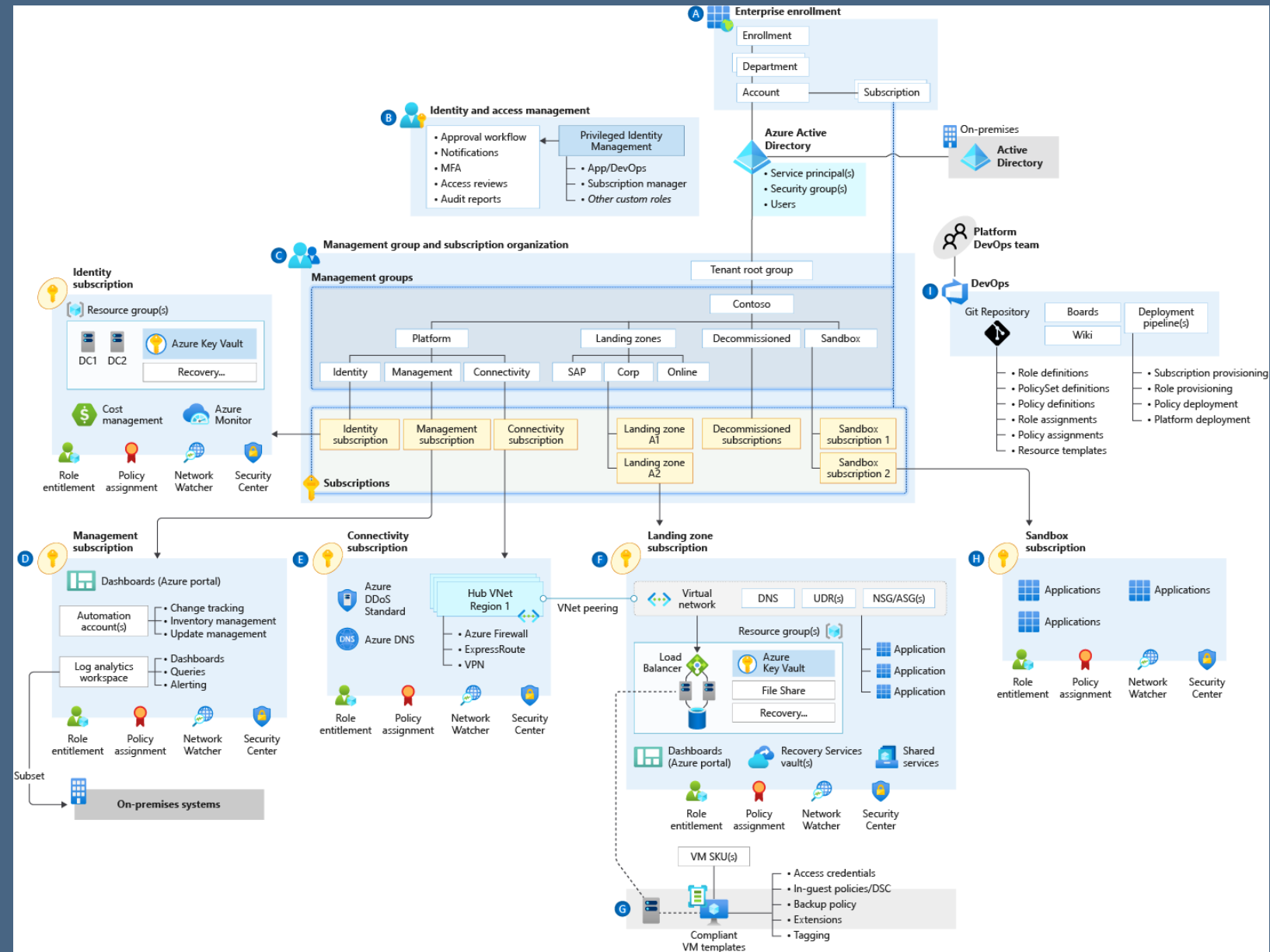


- Hybrid including both Azure and on-prem
- EA enrollment (A)
- Management Groups
- Platform MG for Shared Services (Identity, Connectivity, Management)
- Landing Zones MG for Tenant deployment
- Identity (AAD based IAM)
- Connectivity (Networking, including ExpressRoutes, DNS, UDRs, VPN, FWs)
- Management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