WELCOME
TO

ESPC

JOIN THE
CONVERSATION
#ESPC24

AchieveMore

WITH
MICROSOFT
365

59° 16' 43'' N
18° 0' 55'' E

Stockholm24

The most complex product in Azure?

Mastering Cloud Security: A Deep Dive into Defender for Cloud for IT Pros and Developers

PIERRE THOOR

CYBERSECURITY, ONEVINN, SWEDEN

Introduction

Agenda

1. Defender for Cloud Overview
2. Securing Hybrid Environments
3. Enhancing DevOps Security
4. Protect ARM Deployment
5. Best Practices & Key Learning

Demos 

The importance of Cloud Security

Overview of Microsoft Defender for Cloud


DNS
SQL

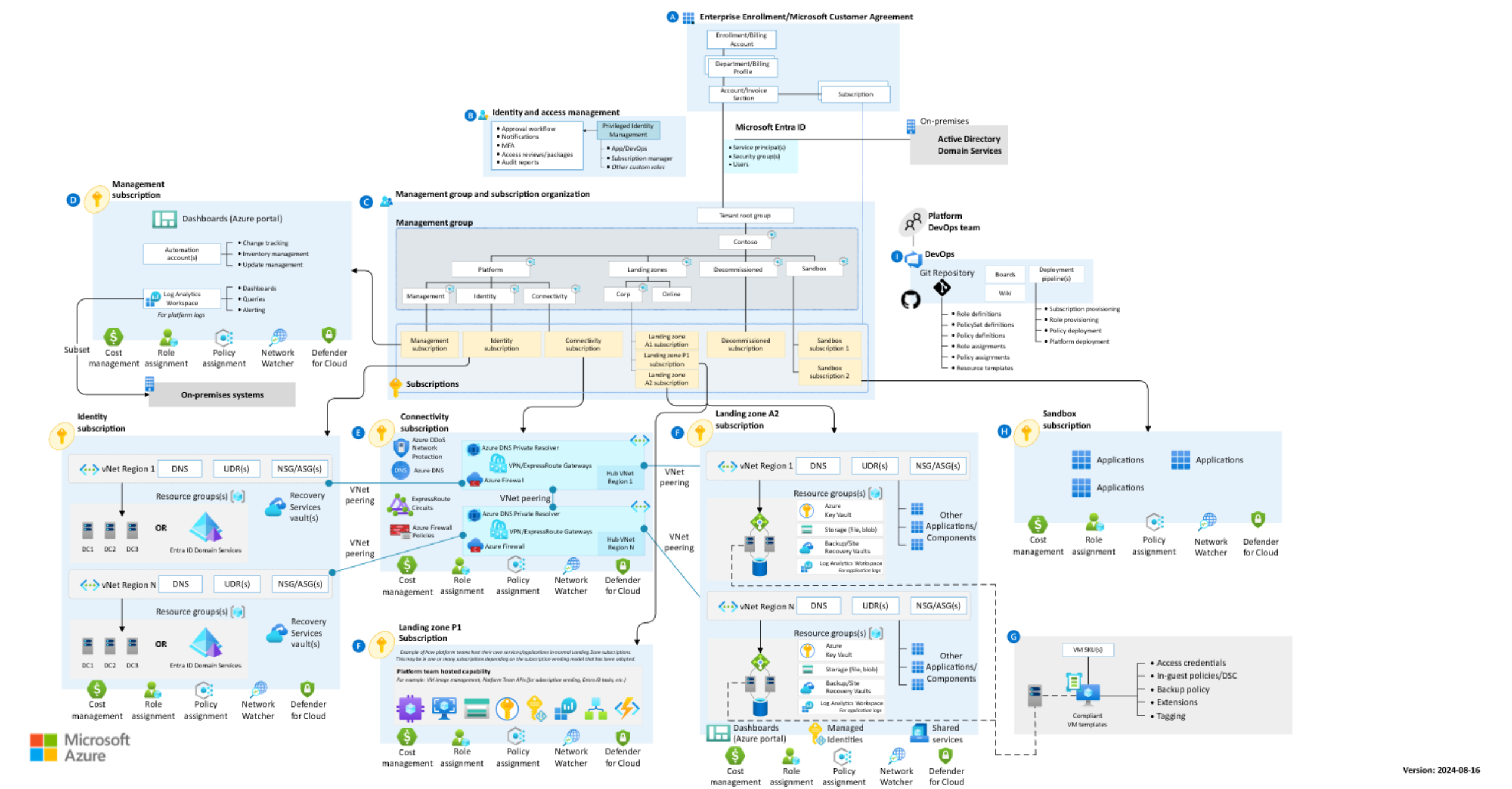
The most complex product in Azure?

Overview

Align with Azure Enterprise Scale Landing Zone concept

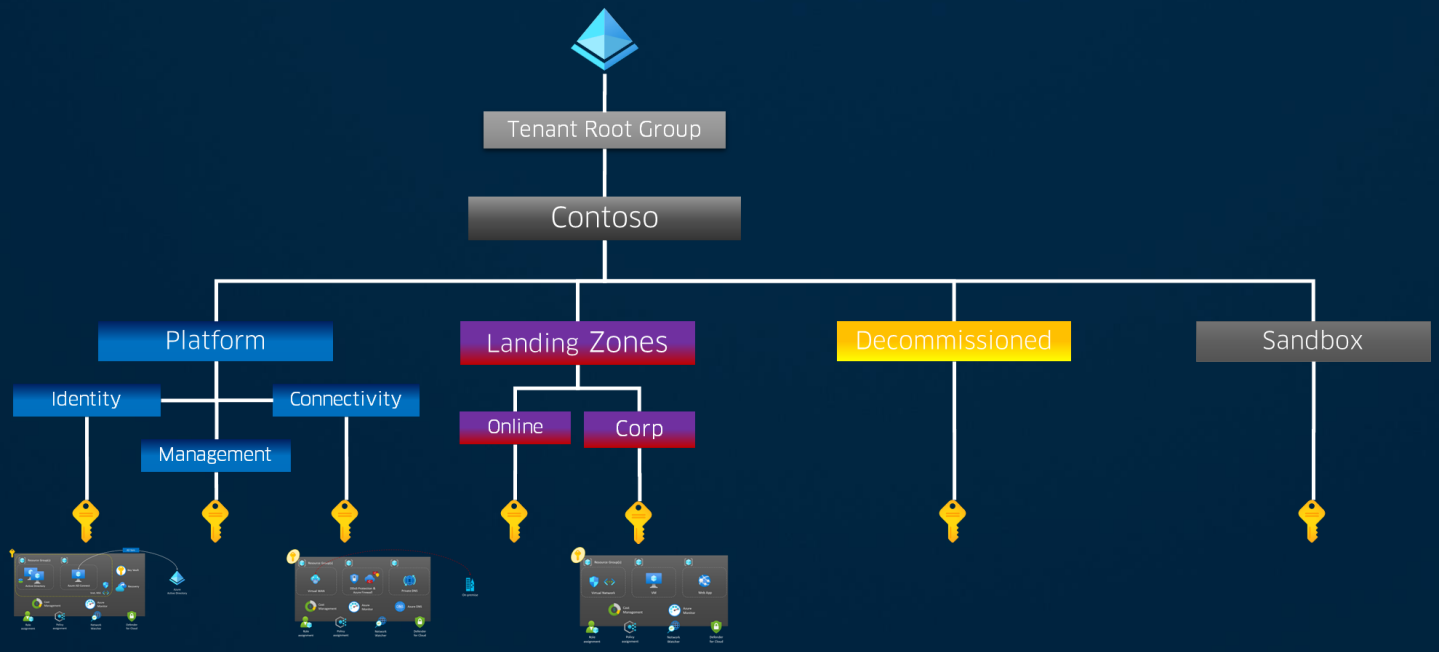
Azure Policy framework

Integrate with Defender XDR for correlation purposes

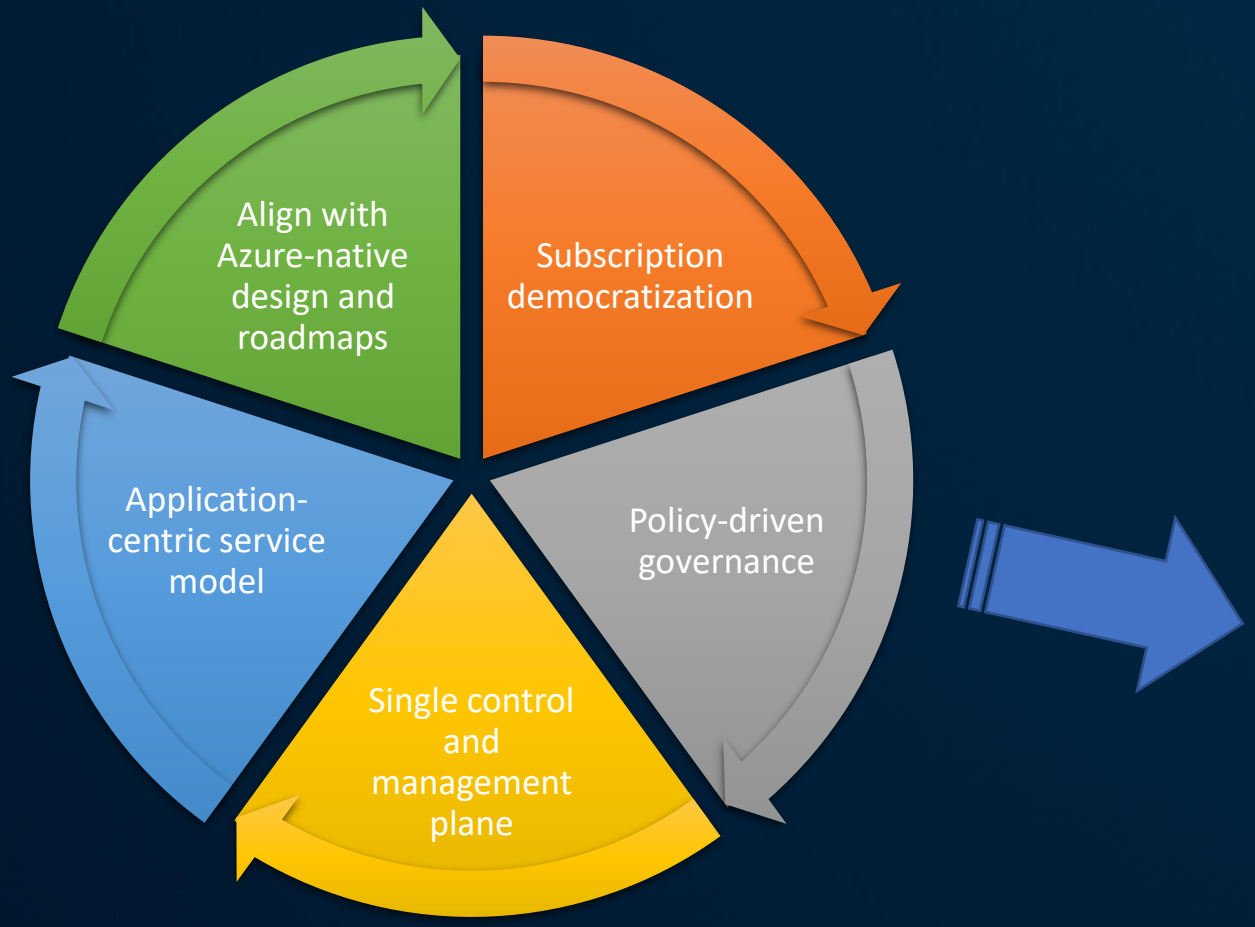

A Enterprise Enrollment/Microsoft Customer Agreement
Enrollment/Billing Account
Department/Billing Profile
Account/Invoice Section
Subscription
B Identity and access management
Approval workflow
Notifications
MFA
Access reviews/packages
Audit reports
Privileged Identity Management
App/DevOps
Subscription manager
Other custom roles
Microsoft Entra ID
Service principal(s)
Security group(s)
Users
On-premises
Active Directory Domain Services
D Management subscription
Dashboards (Azure portal)
Automation account(s)
Change tracking
Inventory management
Update management
Log Analytics Workspace
For platform logs
Dashboards
Queries
Alerting
Subset
Cost management
Role assignment
Policy assignment
Network Watcher
Defender for Cloud
On-premises systems
C Management group and subscription organization
Management group
Tenant root group
Contoso
Platform
Landing zones
Decommissioned
Sandbox
Management
Identity
Connectivity
Corp
Online
Management subscription
Identity subscription
Connectivity subscription
Landing zone A1 subscription
Landing zone P1 subscription
Landing zone A2 subscription
Decommissioned subscription
Sandbox subscription 1
Sandbox subscription 2
Subscriptions
Platform DevOps team
I DevOps
Git Repository
Boards
Wiki
Deployment pipeline(s)
Role definitions
PolicySet definitions
Policy definitions
Role assignments
Policy assignments
Resource templates
Subscription provisioning
Role provisioning
Policy deployment
Platform deployment
Identity subscription
vNet Region 1
DNS
UDR(s)
NSG/ASG(s)
Resource groups(s)
Recovery Services vault(s)
DC1
DC2
DC3
OR
Entra ID Domain Services
vNet Region N
E Connectivity subscription
Azure DDoS Network Protection
Azure DNS
ExpressRoute Circuits
Azure Firewall Policies
Azure DNS Private Resolver
VPN/ExpressRoute Gateways
Azure Firewall
Hub VNet Region 1
Hub VNet Region N
VNet peering
F Landing zone A2 subscription
Azure Key Vault
Storage (file, blob)
Backup/Site Recovery Vaults
Log Analytics Workspace
For application logs
Other Applications/ Components
Dashboards (Azure portal)
Managed Identities
Shared services
H Sandbox subscription
Applications
F Landing zone P1 Subscription
Example of how platform teams host their own services/applications in several Landing Zone subscriptions. This may be in one or many subscriptions depending on the subscription vending model that has been adopted
Platform team hosted capability
For example: VM image management, Platform Team APIs (for subscription vending, Entra ID tools, etc.)
G
VM SKU(s)
Compliant VM templates
Access credentials
In-guest policies/DSC
Backup policy
Extensions
Tagging
Microsoft Azure
Version: 2024-08-16

Prepare

- Use of Azure Policy within Enterprise Scale implementation
  - Organize Azure subscriptions into Management Groups
  - Enable Defender for Cloud on Management Group level

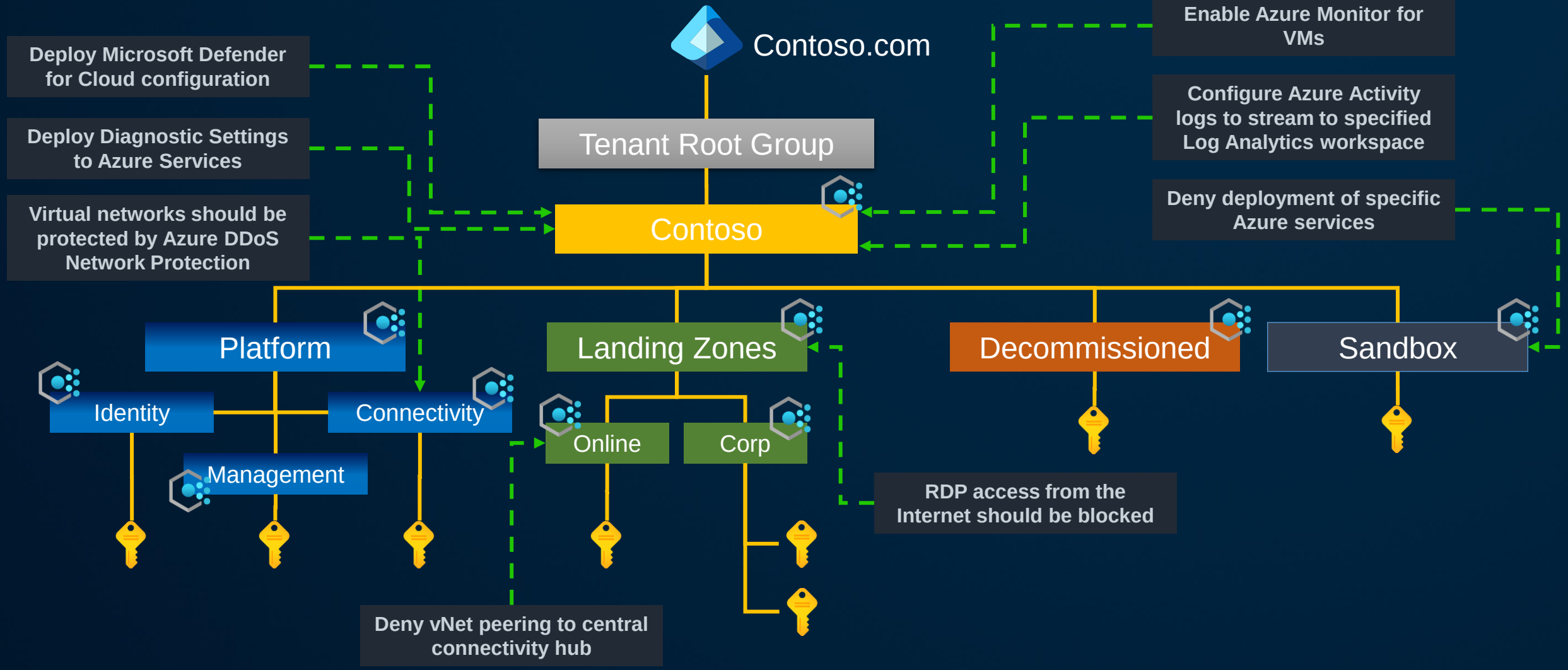


Design Principals



Azure Policy and `deployIfNotExist` enables autonomy in the platform, and reduces operational burden as you scale your deployments and subscriptions in the Azure landing zone architecture. The primary purpose is to ensure that subscriptions and resources are compliant, while empowering application teams to use their own preferred tools/clients to deploy.

Azure Policy (examples)



Prepare

main Microsoft-Defender-for-Cloud / Workbooks / Defender for Cloud Onboarding /

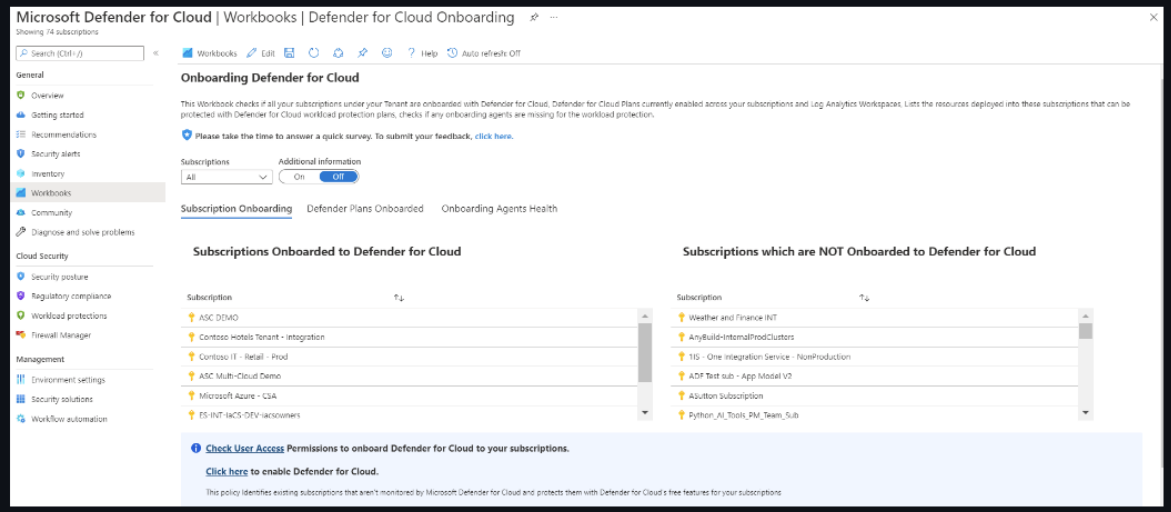
Defender for Cloud Onboarding Workbook

Author: Vasavi Pasula

This Onboarding Workbook checks if all your subscriptions under your Tenant are onboarded with Defender for Cloud, Defender for Cloud Plans currently enabled across your subscriptions and Log Analytics Workspaces, Lists the resources deployed into these subscriptions that can be protected with Defender for Cloud workload protection plans, checks if any onboarding agents are missing for the workload protection. The dashboard is powered by Azure Resource Graph (ARG) queries and divided into different sections. The workbook can be edited, and all queries can be modified to meet your needs.

The workbook provides different Tabs organized as:

- Subscription Onboarding
- Defender Plans Onboarded
- Onboarding Agents Health

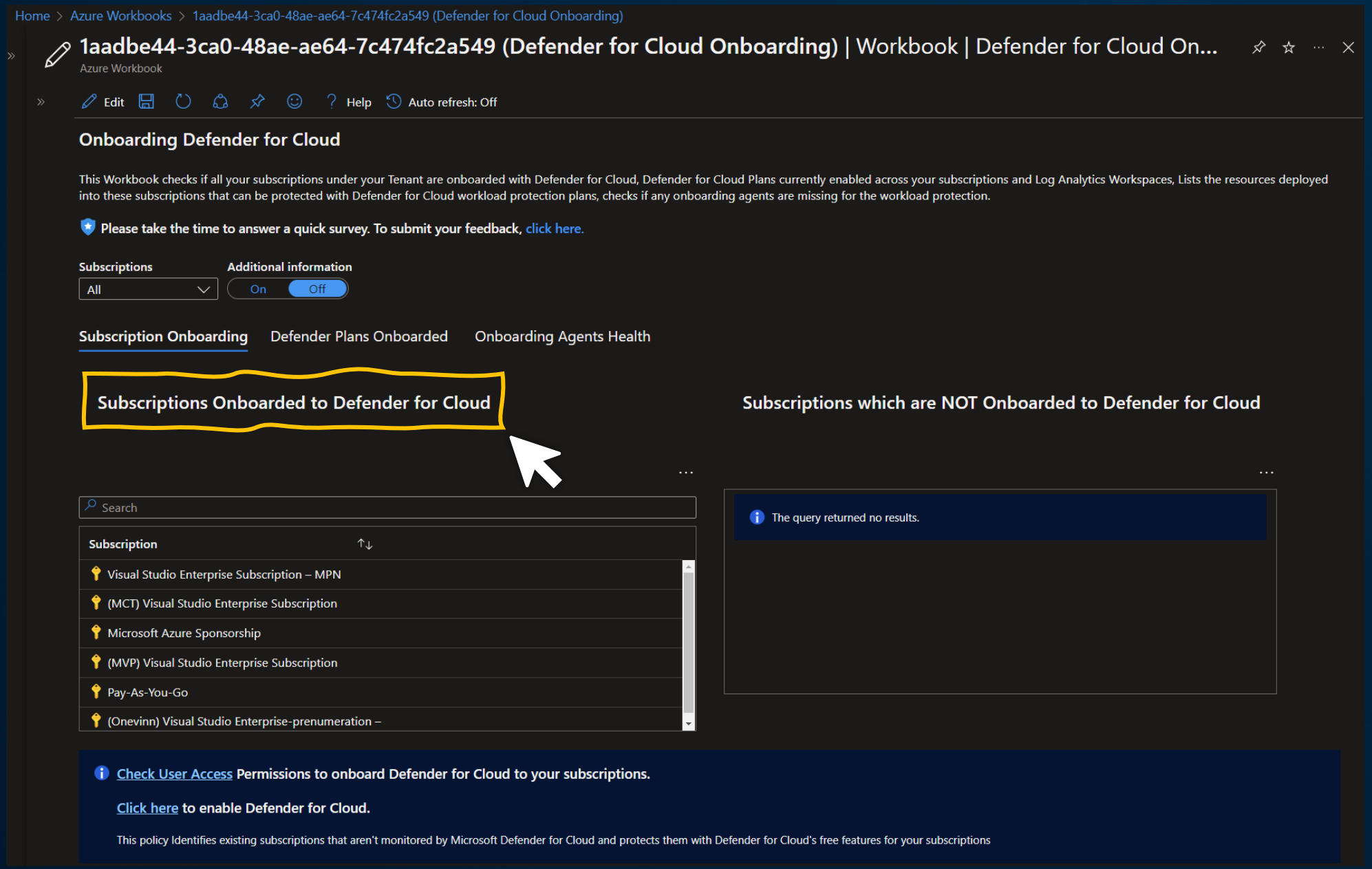


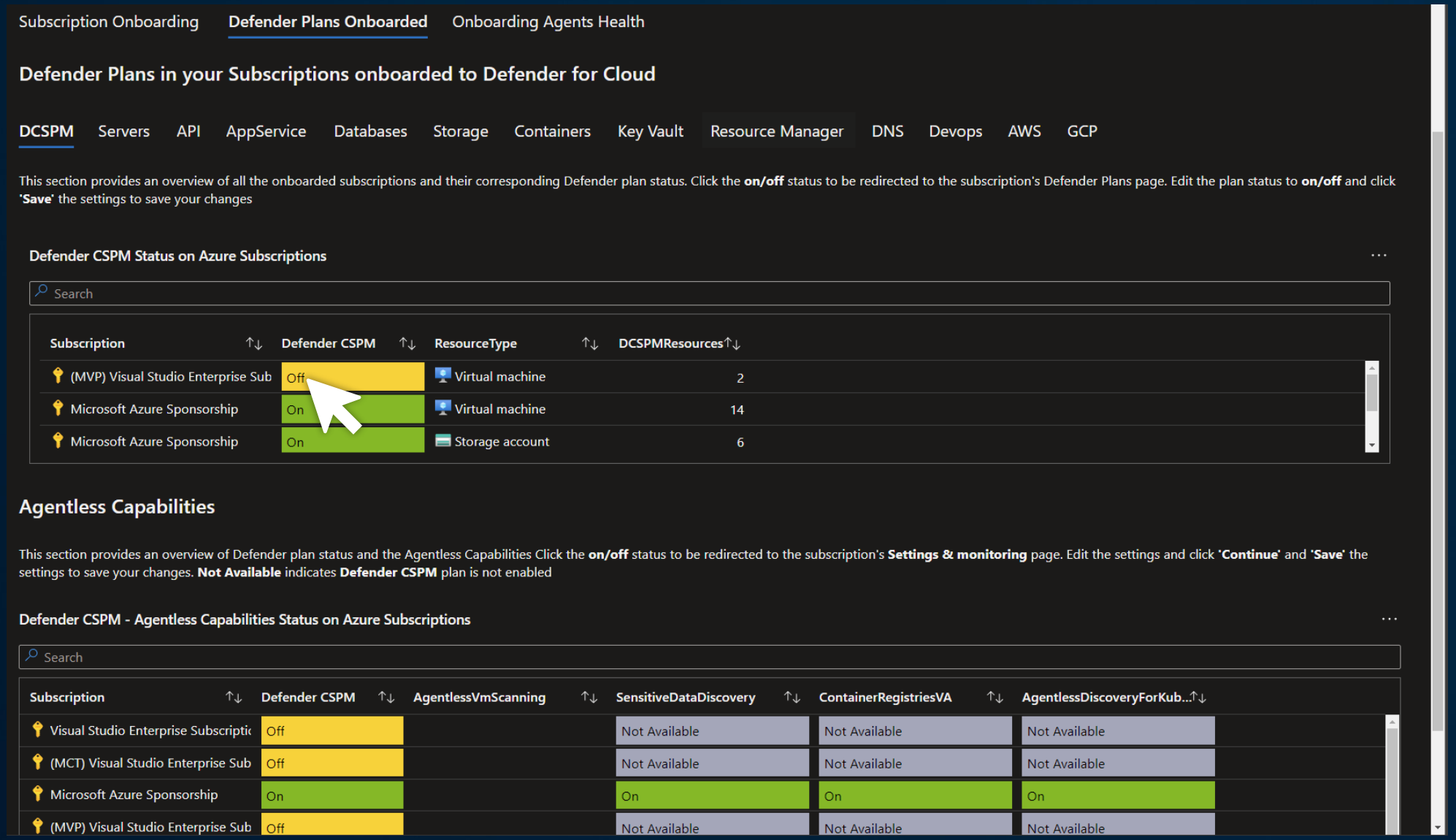
Try it on the Azure Portal

You can deploy the workbook by clicking on the buttons below:

Deploy to Azure | Deploy to Azure Gov

Checkout the blog ... learn more details about this workbook here


Home > Azure Workbooks > 1aadbe44-3ca0-48ae-ae64-7c474fc2a549 (Defender for Cloud Onboarding)
1aadbe44-3ca0-48ae-ae64-7c474fc2a549 (Defender for Cloud Onboarding) | Workbook | Defender for Cloud On...
Azure Workbook
Edit
Help
Auto refresh: Off
Onboarding Defender for Cloud
This Workbook checks if all your subscriptions under your Tenant are onboarded with Defender for Cloud, Defender for Cloud Plans currently enabled across your subscriptions and Log Analytics Workspaces, Lists the resources deployed into these subscriptions that can be protected with Defender for Cloud workload protection plans, checks if any onboarding agents are missing for the workload protection.
Please take the time to answer a quick survey. To submit your feedback, click here.
Subscriptions
All
Additional information
On
Off
Subscription Onboarding
Defender Plans Onboarded
Onboarding Agents Health
Subscriptions Onboarded to Defender for Cloud
Subscriptions which are NOT Onboarded to Defender for Cloud
Search
Subscription
Visual Studio Enterprise Subscription – MPN
(MCT) Visual Studio Enterprise Subscription
Microsoft Azure Sponsorship
(MVP) Visual Studio Enterprise Subscription
Pay-As-You-Go
(Onevinn) Visual Studio Enterprise-prenumeration –
The query returned no results.
Check User Access Permissions to onboard Defender for Cloud to your subscriptions.
Click here to enable Defender for Cloud.
This policy Identifies existing subscriptions that aren't monitored by Microsoft Defender for Cloud and protects them with Defender for Cloud's free features for your subscriptions


Subscription Onboarding
Defender Plans Onboarded
Onboarding Agents Health
Defender Plans in your Subscriptions onboarded to Defender for Cloud
DCSPM
Servers
API
AppService
Databases
Storage
Containers
Key Vault
Resource Manager
DNS
Devops
AWS
GCP
This section provides an overview of all the onboarded subscriptions and their corresponding Defender plan status. Click the on/off status to be redirected to the subscription's Defender Plans page. Edit the plan status to on/off and click 'Save' the settings to save your changes
Defender CSPM Status on Azure Subscriptions
Search
Subscription
Defender CSPM
ResourceType
DCSPMResources
(MVP) Visual Studio Enterprise Sub
Off
Virtual machine
2
Microsoft Azure Sponsorship
On
Virtual machine
14
Microsoft Azure Sponsorship
On
Storage account
6
Agentless Capabilities
This section provides an overview of Defender plan status and the Agentless Capabilities Click the on/off status to be redirected to the subscription's Settings & monitoring page. Edit the settings and click 'Continue' and 'Save' the settings to save your changes. Not Available indicates Defender CSPM plan is not enabled
Defender CSPM - Agentless Capabilities Status on Azure Subscriptions
Search
Subscription
Defender CSPM
AgentlessVmScanning
SensitiveDataDiscovery
ContainerRegistriesVA
AgentlessDiscoveryForKub...
Visual Studio Enterprise Subscriptic
Off
Not Available
Not Available
Not Available
(MCT) Visual Studio Enterprise Sub
Off
Not Available
Not Available
Not Available
Microsoft Azure Sponsorship
On
On
On
On
(MVP) Visual Studio Enterprise Sub
Off
Not Available
Not Available
Not Available

Home > Azure Workbooks > 1aadbe44-3ca0-48ae-ae64-7c474fc2a549 (Defender for Cloud Onboarding) | Workbook | Defender for Cloud Onboarding >

Defender plan

N/A

Save | Settings & monitoring

Enable all plans

Only Subscription Owners can fully enable DCSPM

Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at $15/Billable resource/month.
Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free Details >		Full	On Off
Defender CSPM	Based on subscription size, counting Compute and Data resources Defender CSPM is free until August 1st. When enabling Defender CSPM, automatic discount: Details >	In promotion		On Off

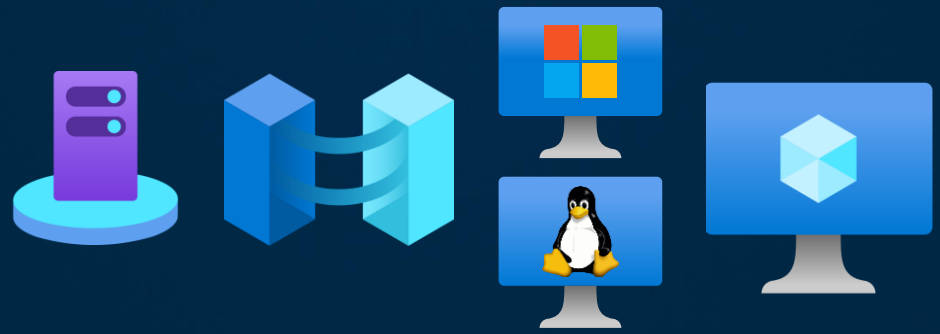
Cloud Workload Protection (CWP)

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 ($15/Server/Month) Change plan >	2 servers		On Off
App Service	$15/Instance/Month Details >	0 instances		On Off
Databases	Selected: 0/4 Select types >	Protected: 0/0 instances		On Off
Storage	$10/Storage account/month On-upload malware scanning ($0.15/GB) Details >	0 storage accounts		On Off
Containers	$7/VM core/Month Details >	0 container registries; 0 kubernetes cores		On Off
Key Vault	$0.02/10k transactions Details >	0 key vaults		On Off

Securing Hybrid Environments with Azure Arc and Defender for Servers

Azure Arc lab with Azure VMs



Try out Azure Arc with simple steps:

- Set environment variable:
  - `[System.Environment]::SetEnvironmentVariable("MSFT_ARC_TEST",'true',[System.EnvironmentVariableTarget]::Machine)`
- Remove all extensions from the Azure VM
  - `az vm extension list -g <rgName> --vm-name <vmName>`
  - `az vm extension delete -g <rgName> --vm-name <vmName> -n <extensionName>`
- Disable Azure VM guest agent
  - `Set-Service WindowsAzureGuestAgent -StartupType Disabled -Verbose`
  - `Stop-Service WindowsAzureGuestAgent -Force -Verbose`
- Firewall settings:
  - `New-NetFirewallRule -Name BlockAzureIMDS -DisplayName "Block access to Azure IMDS" -Enabled True -Profile Any -Direction Outbound -Action Block -RemoteAddress 169.254.169.254`
- Install Azure Arc connected machine agent via script, GPO or other with other tooling

Attacks from Azure

- Custom Script Extensions
- Run command

Attacks inside VM

- Mimikatz
- Atomic Red

DEMO 

Secure the Azure Arc agent

```
azcmagent config set incomingconnections.enabled false

azcmagent config set guestconfiguration.enabled false

azcmagent config set extensions.allowlist
“Microsoft.Azure.Monitor/AzureMonitorWindowsAgent,Micros
oft.Azure.AzureDefenderForServers/MDE.Windows”
```

Enhancing DevOps Security with Defender for DevOps

Feature	Foundational CSPM	Defender CSPM	Prerequisites
Connect Azure DevOps repositories	✅	✅	
Security recommendations to fix code vulnerabilities	✅	✅	GitHub Advanced Security for Azure DevOps for CodeQL findings, Microsoft Security DevOps extension
Security recommendations to discover exposed secrets	✅	✅	GitHub Advanced Security for Azure DevOps ($49 per month per active committer)
Security recommendations to fix open source vulnerabilities	✅	✅	GitHub Advanced Security for Azure DevOps ($49 per month per active committer)
Security recommendations to fix infrastructure as code misconfigurations	✅	✅	Microsoft Security DevOps extension (free extension from Marketplace) or Microsoft Security DevOps action
Security recommendations to fix DevOps environment misconfigurations	✅	✅	N/A
Pull request annotations		✅	
Code to cloud mapping for Containers		✅	Microsoft Security DevOps extension (free extension from Marketplace)
Code to cloud mapping for Infrastructure as Code templates		✅	Microsoft Security DevOps extension (free extension from Marketplace)
Attack path analysis		✅	Enable Defender CSPM on an Azure Subscription in the same tenant as the DevOps Connector
Cloud security explorer		✅	Enable Defender CSPM on an Azure Subscription in the same tenant as the DevOps Connector

Microsoft Security DevOps GitHub action

Trivy

Checkov

Template Analyzer

Example of misconfigured Bicep file

```
resource webApp 'Microsoft.Web/sites@2020-06-01' = {
  name: appName
  location: location
  kind: 'app'
  properties: {
    serverFarmId: appServicePlan.id
  }
}
```

DEMO 

I’m a developer and wants to deploy some Azure resources

Thinking about?

- Security
- Alignment of the bigger Azure environment
- Cost optimization

As the owner of the subscription, you are RESPONSIBLE

DEMO 

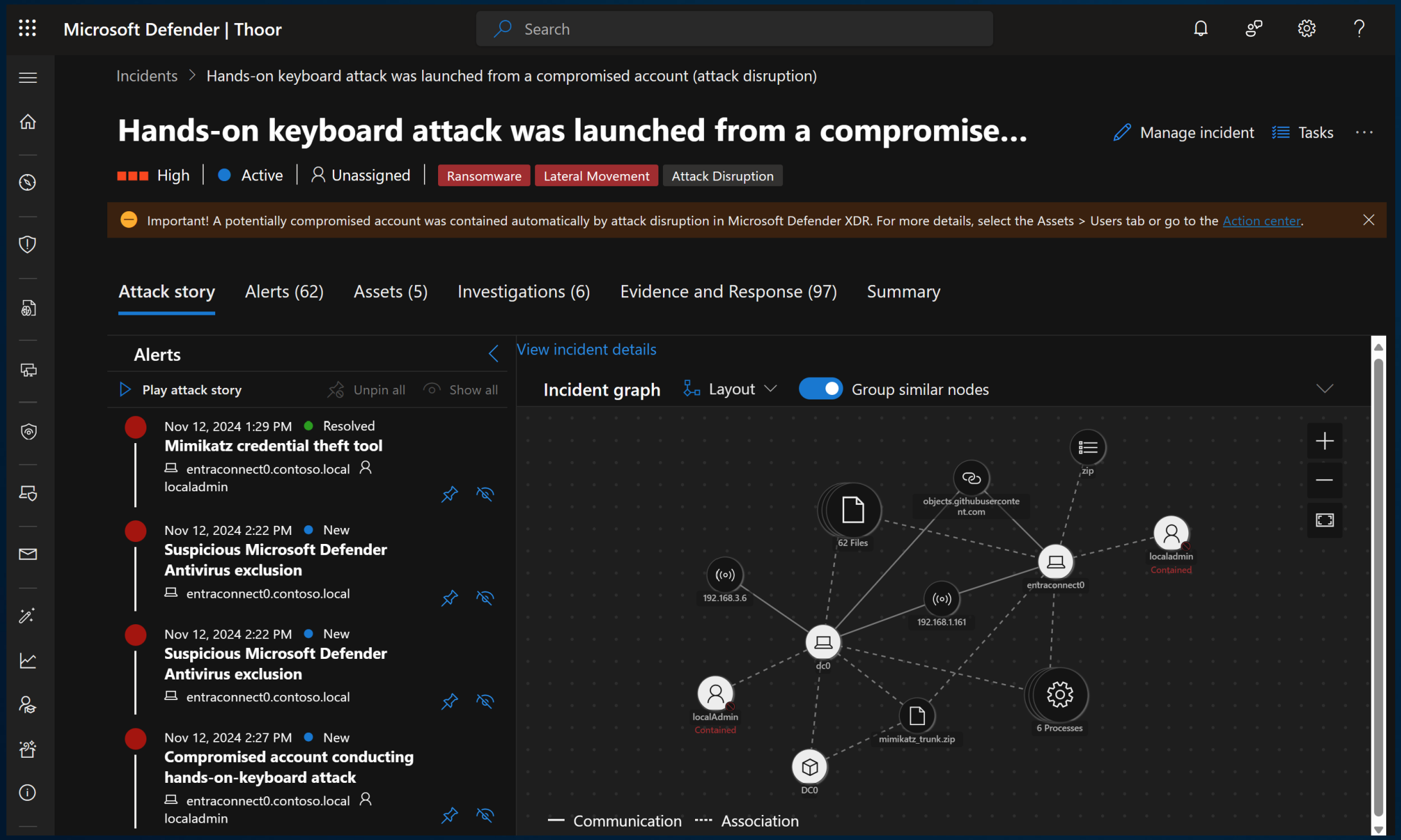
Cloud Security Posture Management: Defender CSPM

Microsoft Sentinel (SIEM) & Defender XDR

CSPM

- Find misconfigurations
- Get compliance issues
- Find security threats in our cloud environment

Correlation and integration


Microsoft Defender | Thoor
Search
Incidents > Hands-on keyboard attack was launched from a compromised account (attack disruption)
Hands-on keyboard attack was launched from a compromise...
Manage incident
Tasks
High | Active | Unassigned | Ransomware | Lateral Movement | Attack Disruption
Important! A potentially compromised account was contained automatically by attack disruption in Microsoft Defender XDR. For more details, select the Assets > Users tab or go to the Action center.
Attack story
Alerts (62)
Assets (5)
Investigations (6)
Evidence and Response (97)
Summary
Alerts
Play attack story
Unpin all
Show all
Nov 12, 2024 1:29 PM Resolved
Mimikatz credential theft tool
entraconnect0.contoso.local
localadmin
Nov 12, 2024 2:22 PM New
Suspicious Microsoft Defender Antivirus exclusion
entraconnect0.contoso.local
Nov 12, 2024 2:22 PM New
Suspicious Microsoft Defender Antivirus exclusion
entraconnect0.contoso.local
Nov 12, 2024 2:27 PM New
Compromised account conducting hands-on-keyboard attack
entraconnect0.contoso.local
localadmin
View incident details
Incident graph
Layout
Group similar nodes
zip
objects.githubusercontent.com
62 Files
localadmin
Contained
entraconnect0
192.168.3.6
192.168.1.161
dc0
localAdmin
Contained
6 Processes
mimikatz_trunk.zip
DC0
Communication
Association

Microsoft Sentinel | Data connectors

Selected workspace: 'thoorsentinel-v2'

Refresh | Guides & Feedback

17 Onboarded Connectors | 13 Connected | 0 Updates

More content at Content hub

Search by name or provider | Providers : **All** | Data Types : **All** | Status : **All**

Security Events via Legacy Agent Microsoft	**Solution** Windows Security Events	...
Subscription-based Microsoft Defender for Cloud (Legacy) Microsoft	**Solution** Microsoft Defender for Cloud	...
Syslog via Legacy Agent Microsoft	**Solution** Syslog	...
Tenant-based Microsoft Defender for Cloud (Preview) Microsoft	**Solution** Microsoft Defender for Cloud	...
Threat intelligence - TAXII Microsoft	**Solution** Threat Intelligence	...
Threat Intelligence Platforms - BEING DEPRECATED (Prev...	**Solution**	...

Microsoft Sentinel | Data connectors

Selected workspace: 'thoorsentinel-v2'

Refresh Guides & Feedback

17 Onboarded Connectors

13 Connected

0 Updates

More content at Content hub

Search by name or provider | Providers : **All** | Data Types : **All** | Status : **All**

Security Events via Legacy Agent Microsoft	**Solution** Windows Security Events	...
Subscription-based Microsoft Defender for Cloud (Legacy) Microsoft	**Solution** Microsoft Defender for Cloud	...
Syslog via Legacy Agent Microsoft	**Solution** Syslog	...
Tenant-based Microsoft Defender for Cloud (Preview) Microsoft	**Solution** Microsoft Defender for Cloud	...
Threat intelligence - TAXII Microsoft	**Solution** Threat Intelligence	...
Threat Intelligence Platforms - BEING DEPRECATED (Prev...	**Solution**	...

Best practices

(yes, we need to lean into something)

Guidelines/Best practices

- Align and scale at your pace with Enterprise Scale landing zones
- Use Azure Policy framework
- Tiering in Azure, least-privileges mindset
- Security first
- Do not expose Azure resources on the Internet

Do you think that MDC is the most complex product in Azure?

Key learning

- Defender for Cloud is **MASSIVE** and **COMPLEX**
- Continuous monitoring and visibility **IS** crucial
- Integrate **security** early in the development
- Help the SecOps team in **understanding your environment** better
- Participate in proactive **threat hunting** sessions with SecOps

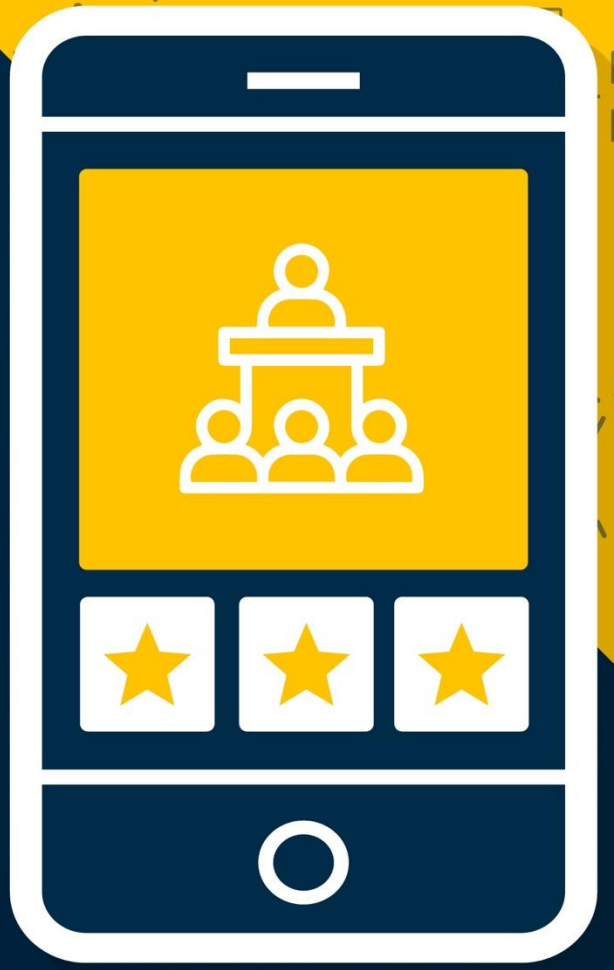
Thank you!

pierrethoor.bsky.social

@PierreThoor

https://github.com/pthoor/ESPC24

Please rate this session on the app



GET IT ON Google Play

Download on the App Store