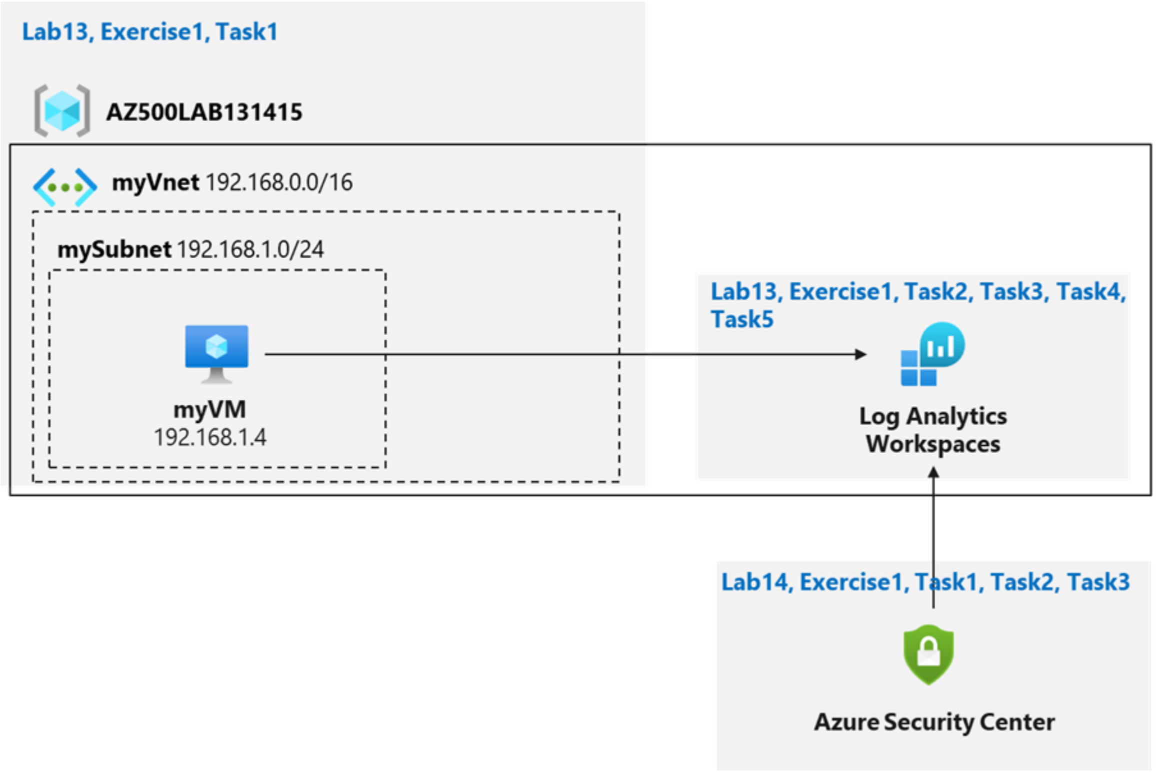
Lab 14: Microsoft Defender for Cloud



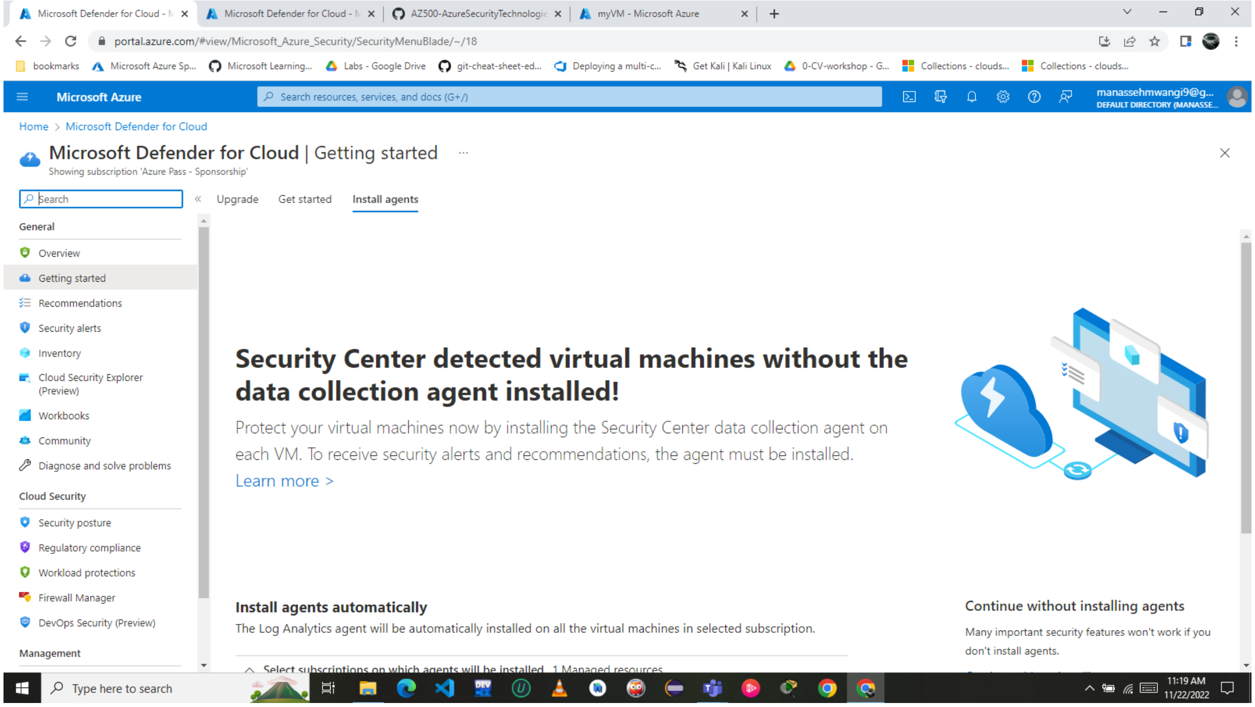
In this exercise, you will complete the following tasks:

- Task 1: Configure Microsoft Defender for Cloud
- Task 2: Review the Microsoft Defender for Cloud recommendations
- Task 3: Implement the Microsoft Defender for Cloud recommendation to enable Just in time VM Access

Task 1: Configure Microsoft Defender for Cloud

On the Microsoft Defender for Cloud | Getting started blade, click Upgrade**.**

In the Microsoft Defender for Cloud | Getting started blade, in the Install agents tab, scroll down and click Install agents.



Microsoft Defender for Cloud | Getting started

Showing subscription 'Azure Pass - Sponsorship'

Security Center detected virtual machines without the data collection agent installed!

Protect your virtual machines now by installing the Security Center data collection agent on each VM. To receive security alerts and recommendations, the agent must be installed.

Learn more >

Install agents automatically

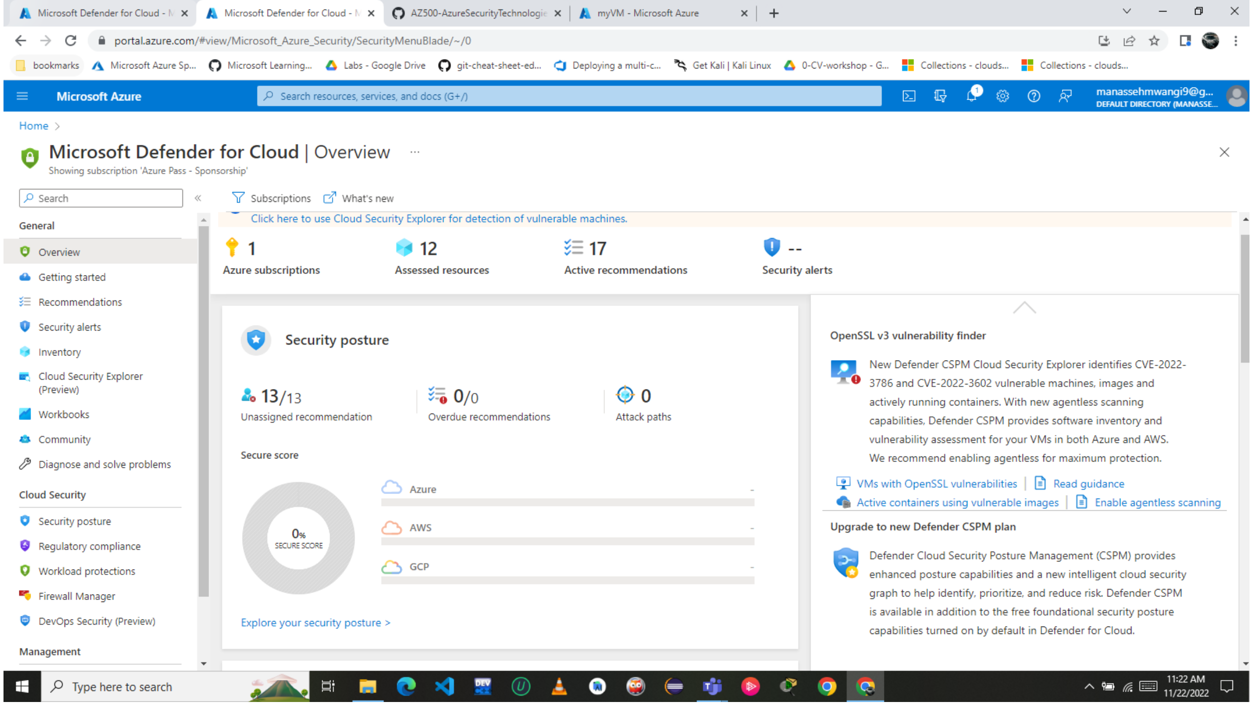
The Log Analytics agent will be automatically installed on all the virtual machines in selected subscription.

Select subscriptions on which agents will be installed 1 Managed resources

Continue without installing agents

Many important security features won't work if you don't install agents.

Review all the features that are available as part of Microsoft Defender plans.



Microsoft Defender for Cloud | Overview

Showing subscription 'Azure Pass - Sponsorship'

Click here to use Cloud Security Explorer for detection of vulnerable machines.

1 Azure subscriptions | 12 Assessed resources | 17 Active recommendations | -- Security alerts

Security posture

13/13 Unassigned recommendation | 0/0 Overdue recommendations | 0 Attack paths

Secure score

Explore your security posture >

OpenSSL v3 vulnerability finder

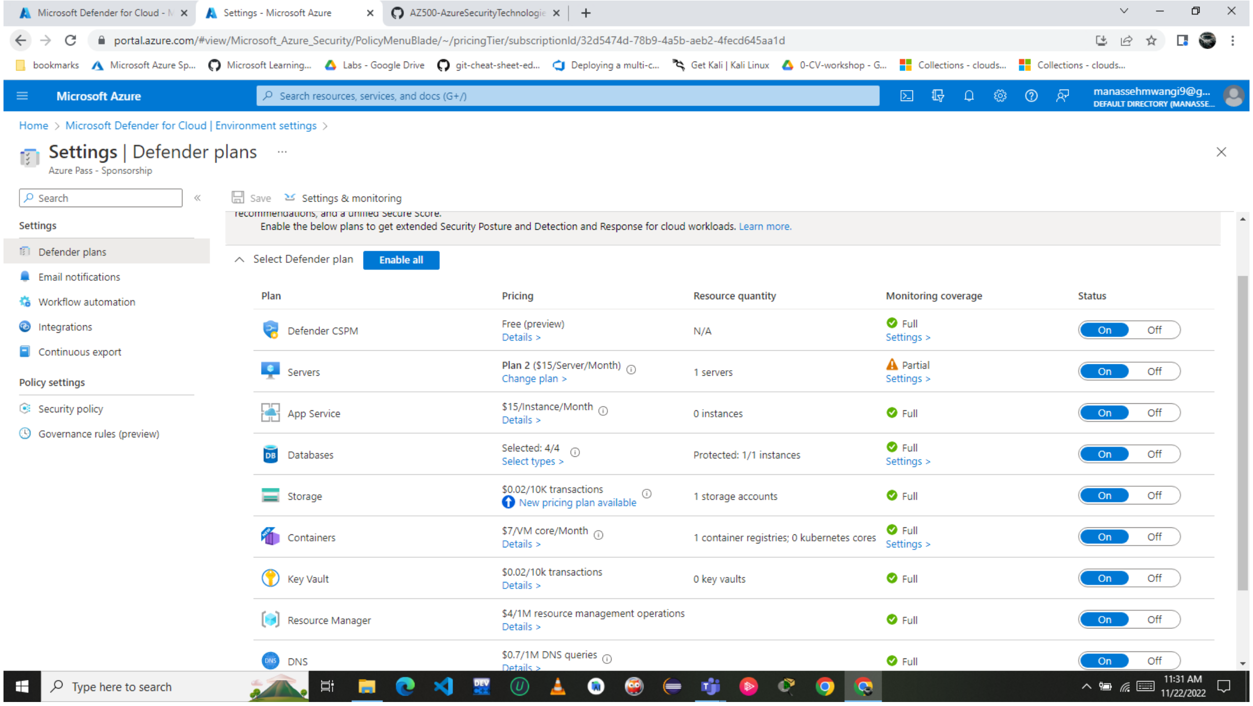
New Defender CSPM Cloud Security Explorer identifies CVE-2022-3786 and CVE-2022-3602 vulnerable machines, images and actively running containers. With new agentless scanning capabilities, Defender CSPM provides software inventory and vulnerability assessment for your VMs in both Azure and AWS. We recommend enabling agentless for maximum protection.

VMs with OpenSSL vulnerabilities | Read guidance
Active containers using vulnerable images | Enable agentless scanning

Upgrade to new Defender CSPM plan

Defender Cloud Security Posture Management (CSPM) provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize, and reduce risk. Defender CSPM is available in addition to the free foundational security posture capabilities turned on by default in Defender for Cloud.

Enable all Microsoft Defender for Cloud Plans and click Save.


Microsoft Defender for Cloud - M
Settings - Microsoft Azure
AZ500-AzureSecurityTechnologie
portal.azure.com/#view/Microsoft_Azure_Security/PolicyMenuBlade/~/pricingTier/subscriptionId/32d5474d-78b9-4a5b-aeb2-4fecd645aa1d
bookmarks
Microsoft Azure Sp...
Microsoft Learning...
Labs - Google Drive
git-cheat-sheet-ed...
Deploying a multi-c...
Get Kali | Kali Linux
0-CV-workshop - G...
Collections - clouds...
Collections - clouds...
Microsoft Azure
Search resources, services, and docs (G+/)
manassehmwangi9@g...
DEFAULT DIRECTORY (MANASSE...
Type here to search
11:31 AM
11/22/2022

Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans

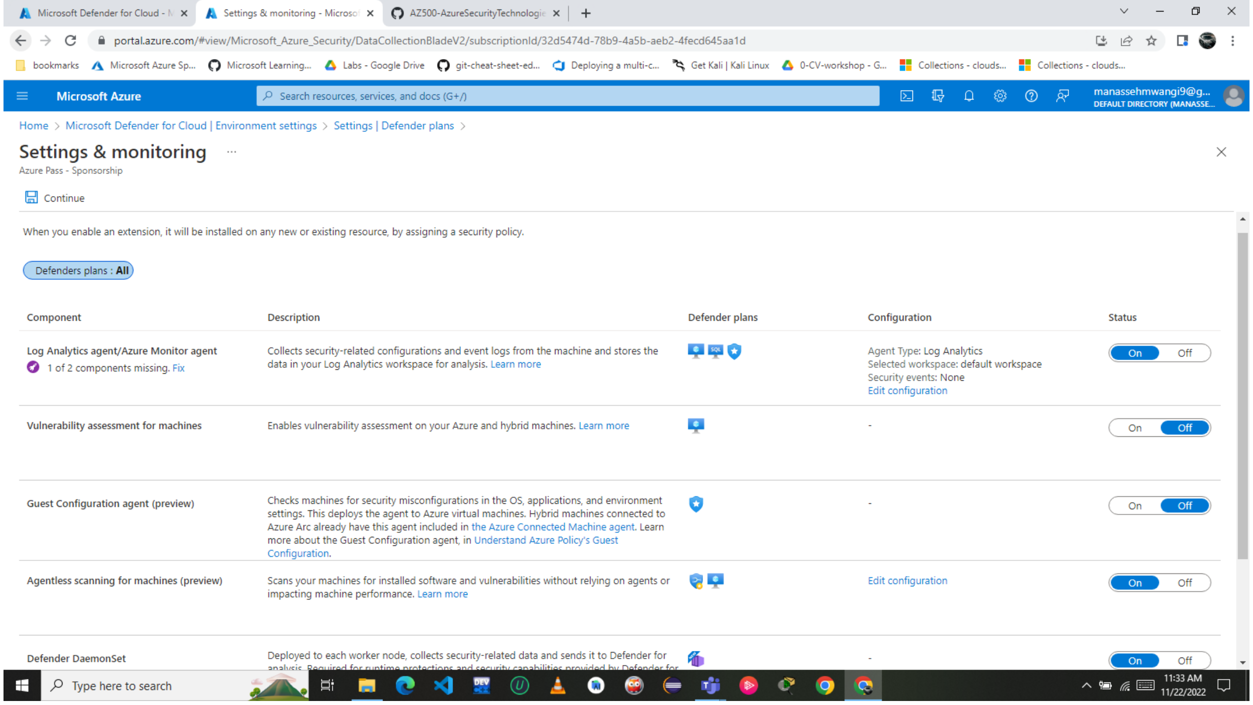
Azure Pass - Sponsorship

recommendations, and a unified secure score.
Enable the below plans to get extended Security Posture and Detection and Response for cloud workloads. Learn more.

Select Defender plan **Enable all**

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Defender CSPM	Free (preview) Details >	N/A	✓ Full Settings >	On
Servers	Plan 2 ($15/Server/Month) Change plan >	1 servers	⚠ Partial Settings >	On
App Service	$15/Instance/Month Details >	0 instances	✓ Full	On
Databases	Selected: 4/4 Select types >	Protected: 1/1 instances	✓ Full Settings >	On
Storage	$0.02/10K transactions New pricing plan available	1 storage accounts	✓ Full	On
Containers	$7/VM core/Month Details >	1 container registries; 0 kubernetes cores	✓ Full Settings >	On
Key Vault	$0.02/10k transactions Details >	0 key vaults	✓ Full	On
Resource Manager	$4/1M resource management operations Details >		✓ Full	On
DNS	$0.7/1M DNS queries Details >		✓ Full	On

make sure that Auto provisioning is set to on for the first item Log Analytics agent for Azure VMs.


Microsoft Defender for Cloud - M
Settings & monitoring - Microsof
AZ500-AzureSecurityTechnologie
portal.azure.com/#view/Microsoft_Azure_Security/DataCollectionBladeV2/subscriptionId/32d5474d-78b9-4a5b-aeb2-4fecd645aa1d
bookmarks
Microsoft Azure Sp...
Microsoft Learning...
Labs - Google Drive
git-cheat-sheet-ed...
Deploying a multi-c...
Get Kali | Kali Linux
0-CV-workshop - G...
Collections - clouds...
Collections - clouds...
Microsoft Azure
Search resources, services, and docs (G+/)
manassehmwangi9@g...
DEFAULT DIRECTORY (MANASSE...
Type here to search
11:33 AM
11/22/2022

Home > Microsoft Defender for Cloud | Environment settings > Settings | Defender plans >

Settings & monitoring

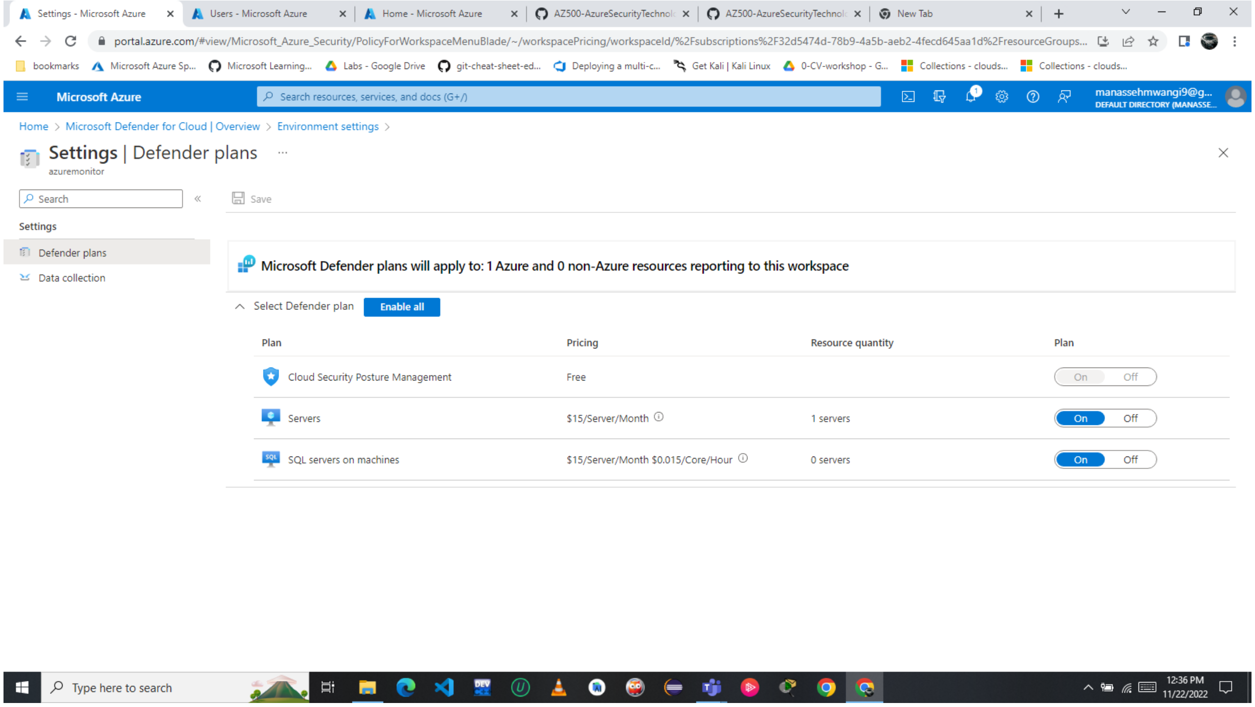
Azure Pass - Sponsorship

When you enable an extension, it will be installed on any new or existing resource, by assigning a security policy.

Defenders plans : **All**

Component	Description	Defender plans	Configuration	Status
Log Analytics agent/Azure Monitor agent 1 of 2 components missing. Fix	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. Learn more		Agent Type: Log Analytics Selected workspace: default workspace Security events: None Edit configuration	On
Vulnerability assessment for machines	Enables vulnerability assessment on your Azure and hybrid machines. Learn more		-	Off
Guest Configuration agent (preview)	Checks machines for security misconfigurations in the OS, applications, and environment settings. This deploys the agent to Azure virtual machines. Hybrid machines connected to Azure Arc already have this agent included in the Azure Connected Machine agent. Learn more about the Guest Configuration agent, in Understand Azure Policy's Guest Configuration.		-	Off
Agentless scanning for machines (preview)	Scans your machines for installed software and vulnerabilities without relying on agents or impacting machine performance. Learn more		Edit configuration	On
Defender DaemonSet	Deployed to each worker node, collects security-related data and sends it to Defender for analysis. Required for runtime protections and security capabilities provided by Defender for		-	On

Enable all Microsoft Defender for Cloud plans is selected and click Save.


Settings - Microsoft Azure
Users - Microsoft Azure
Home - Microsoft Azure
AZ500-AzureSecurityTechnolo
New Tab
portal.azure.com/#view/Microsoft_Azure_Security/PolicyForWorkspaceMenuBlade/~/workspacePricing/workspaceId/%2Fsubscriptions%2F32d5474d-78b9-4a5b-aeb2-4fecd645aa1d%2FresourceGroups...
Microsoft Azure
Search resources, services, and docs (G+/)
manassehmwangi9@g...
DEFAULT DIRECTORY (MANASSE...
Type here to search
12:36 PM
11/22/2022

Home > Microsoft Defender for Cloud | Overview > Environment settings >

Settings | Defender plans

azuremonitor

Search

Save

Settings

Defender plans

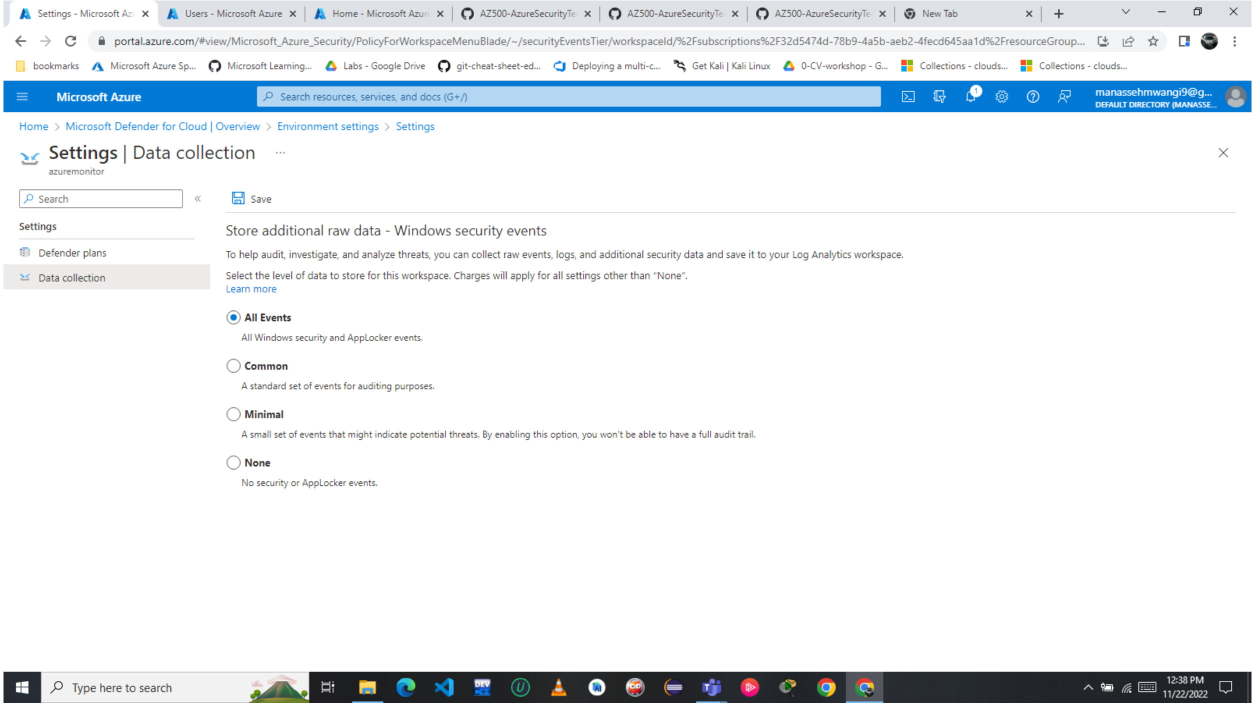
Data collection

Microsoft Defender plans will apply to: 1 Azure and 0 non-Azure resources reporting to this workspace

Select Defender plan **Enable all**

Plan	Pricing	Resource quantity	Plan
Cloud Security Posture Management	Free		On / Off
Servers	$15/Server/Month	1 servers	**On** / Off
SQL servers on machines	$15/Server/Month $0.015/Core/Hour	0 servers	**On** / Off

Data collection from the Microsoft Defender for Cloud Select All Events and Save.


Settings - Microsoft Az
Users - Microsoft Azure
Home - Microsoft Azur
AZ500-AzureSecurityTe
New Tab
portal.azure.com/#view/Microsoft_Azure_Security/PolicyForWorkspaceMenuBlade/~/securityEventsTier/workspaceId/%2Fsubscriptions%2F32d5474d-78b9-4a5b-aeb2-4fecd645aa1d%2FresourceGroup...
Microsoft Azure
Search resources, services, and docs (G+/)
manassehmwangi9@g...
DEFAULT DIRECTORY (MANASSE...
Type here to search
12:38 PM
11/22/2022

Home > Microsoft Defender for Cloud | Overview > Environment settings > Settings

Settings | Data collection

azuremonitor

Search

Save

Settings

Defender plans

Data collection

Store additional raw data - Windows security events

To help audit, investigate, and analyze threats, you can collect raw events, logs, and additional security data and save it to your Log Analytics workspace.

Select the level of data to store for this workspace. Charges will apply for all settings other than "None".
Learn more

● **All Events**
All Windows security and AppLocker events.

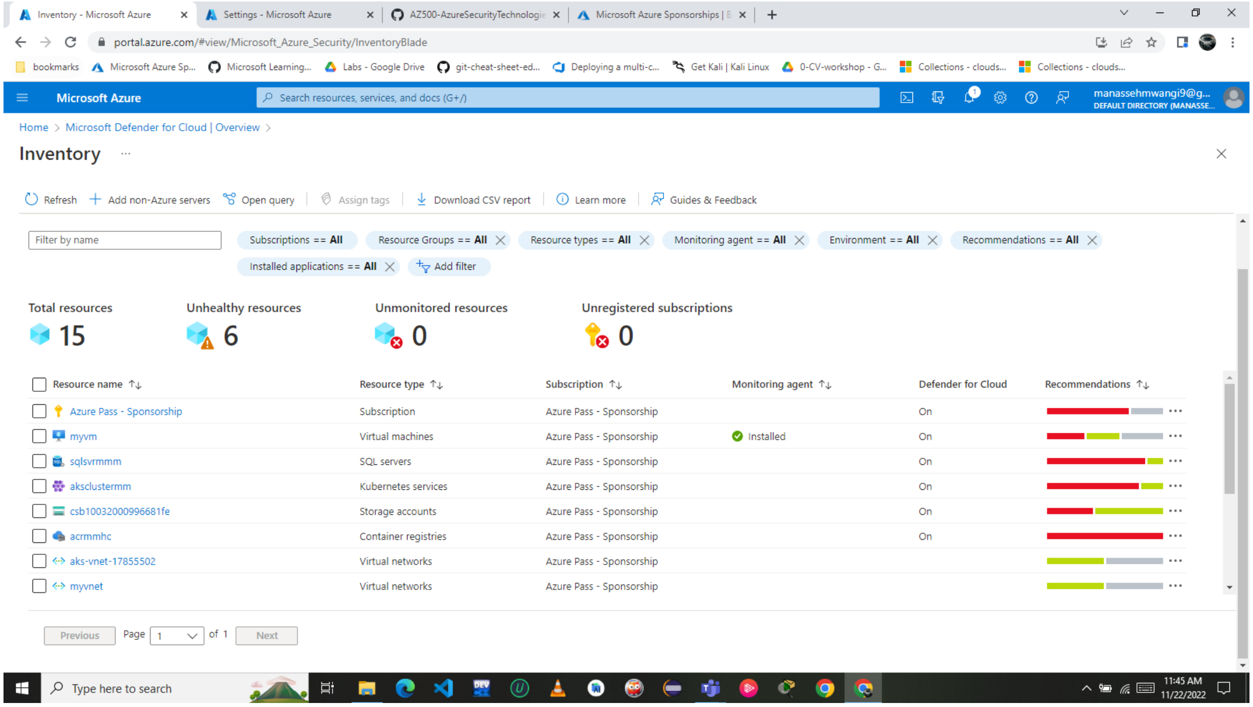
○ **Common**
A standard set of events for auditing purposes.

○ **Minimal**
A small set of events that might indicate potential threats. By enabling this option, you won't be able to have a full audit trail.

○ **None**
No security or AppLocker events.

Task 2: Review the Microsoft Defender for Cloud recommendation

On the Inventory blade, select the myVM entry.


Home > Microsoft Defender for Cloud | Overview >

Inventory

Refresh | Add non-Azure servers | Open query | Assign tags | Download CSV report | Learn more | Guides & Feedback

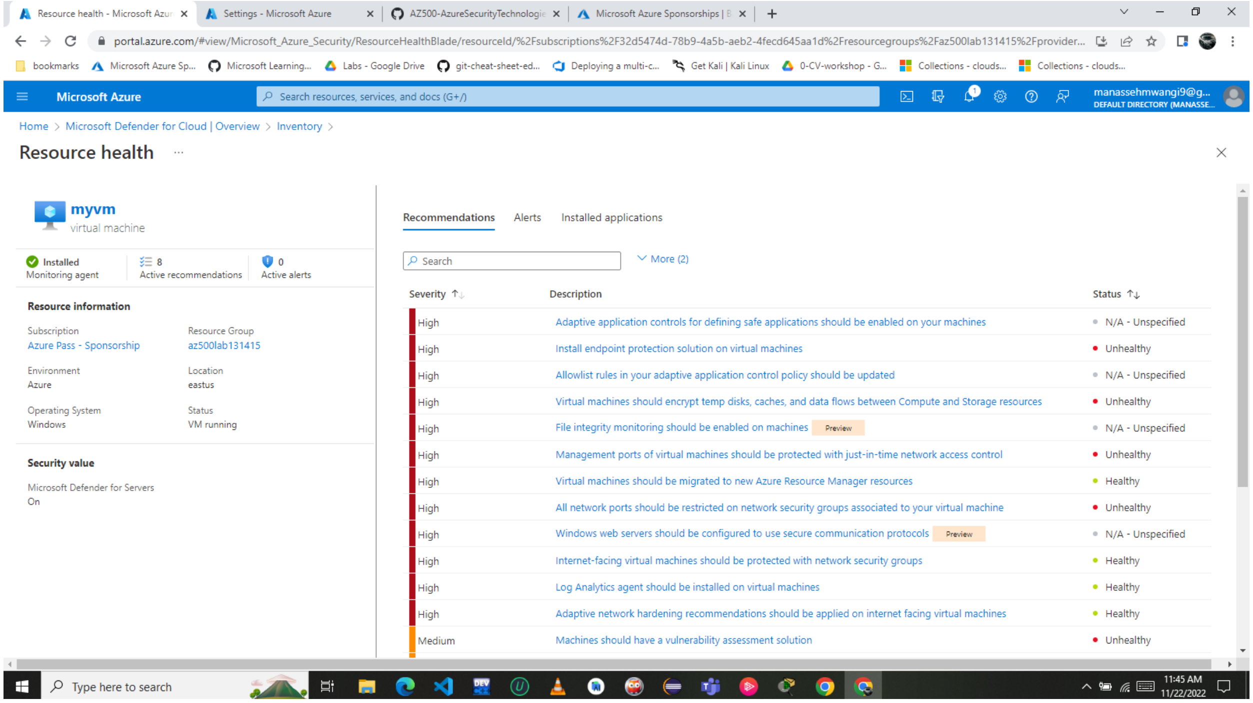
Filter by name | Subscriptions == **All** | Resource Groups == **All** | Resource types == **All** | Monitoring agent == **All** | Environment == **All** | Recommendations == **All** | Installed applications == **All** | Add filter

Total resources 15 | Unhealthy resources 6 | Unmonitored resources 0 | Unregistered subscriptions 0

Resource name	Resource type	Subscription	Monitoring agent	Defender for Cloud	Recommendations
Azure Pass - Sponsorship	Subscription	Azure Pass - Sponsorship		On	
myvm	Virtual machines	Azure Pass - Sponsorship	Installed	On	
sqlsvrmmm	SQL servers	Azure Pass - Sponsorship		On	
aksclustermm	Kubernetes services	Azure Pass - Sponsorship		On	
csb10032000996681fe	Storage accounts	Azure Pass - Sponsorship		On	
acrmmhc	Container registries	Azure Pass - Sponsorship		On	
aks-vnet-17855502	Virtual networks	Azure Pass - Sponsorship			
myvnet	Virtual networks	Azure Pass - Sponsorship			

Previous | Page 1 of 1 | Next

On the Resource health blade, on the Recommendations tab, review the list of recommendations for myVM.


Home > Microsoft Defender for Cloud | Overview > Inventory >

Resource health

myvm
virtual machine

Installed
Monitoring agent

8
Active recommendations

0
Active alerts

Resource information

Subscription: Azure Pass - Sponsorship

Resource Group: az500lab131415

Environment: Azure

Location: eastus

Operating System: Windows

Status: VM running

Security value

Microsoft Defender for Servers
On

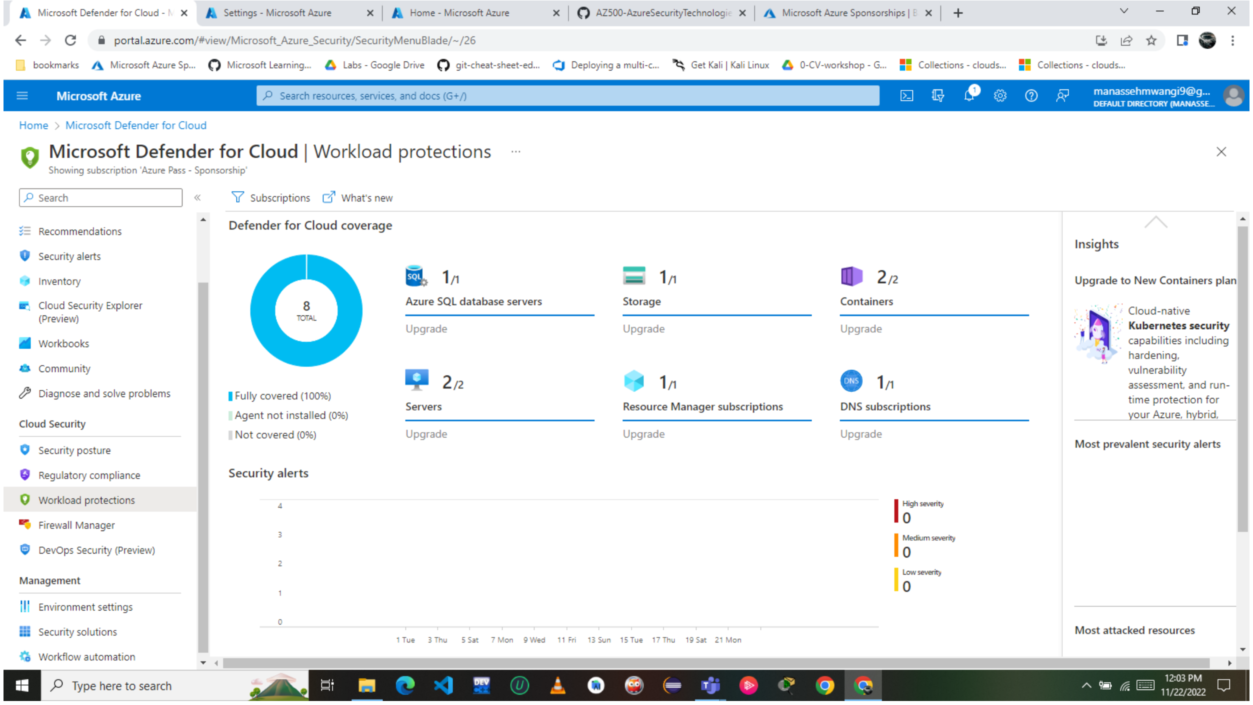
Recommendations | Alerts | Installed applications

Search | More (2)

Severity	Description	Status
High	Adaptive application controls for defining safe applications should be enabled on your machines	N/A - Unspecified
High	Install endpoint protection solution on virtual machines	Unhealthy
High	Allowlist rules in your adaptive application control policy should be updated	N/A - Unspecified
High	Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources	Unhealthy
High	File integrity monitoring should be enabled on machines Preview	N/A - Unspecified
High	Management ports of virtual machines should be protected with just-in-time network access control	Unhealthy
High	Virtual machines should be migrated to new Azure Resource Manager resources	Healthy
High	All network ports should be restricted on network security groups associated to your virtual machine	Unhealthy
High	Windows web servers should be configured to use secure communication protocols Preview	N/A - Unspecified
High	Internet-facing virtual machines should be protected with network security groups	Healthy
High	Log Analytics agent should be installed on virtual machines	Healthy
High	Adaptive network hardening recommendations should be applied on internet facing virtual machines	Healthy
Medium	Machines should have a vulnerability assessment solution	Unhealthy

Task 3: Implement the Microsoft Defender to enable Just in time VM Access

select the Workload protections under Cloud Security tile.



portal.azure.com/#view/Microsoft_Azure_Security/SecurityMenuBlade/~/26

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Workload protections

Showing subscription 'Azure Pass - Sponsorship'

Defender for Cloud coverage

8 TOTAL

- Fully covered (100%)
- Agent not installed (0%)
- Not covered (0%)

1/1 Azure SQL database servers Upgrade	1/1 Storage Upgrade	2/2 Containers Upgrade
2/2 Servers Upgrade	1/1 Resource Manager subscriptions Upgrade	1/1 DNS subscriptions Upgrade

Security alerts

Insights

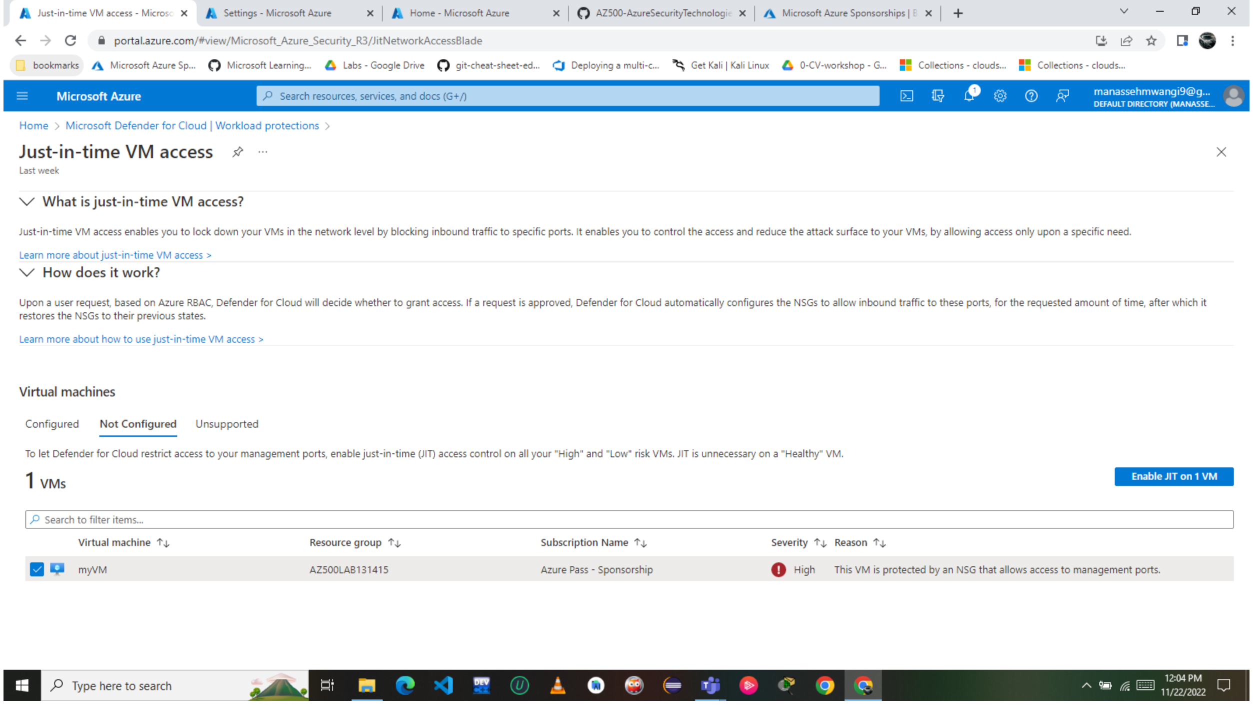
Upgrade to New Containers plan

Cloud-native **Kubernetes security** capabilities including hardening, vulnerability assessment, and run-time protection for your Azure, hybrid,

Most prevalent security alerts

Most attacked resources

Select Enable JIT on 1 VM



portal.azure.com/#view/Microsoft_Azure_Security_R3/JitNetworkAccessBlade

Home > Microsoft Defender for Cloud | Workload protections >

Just-in-time VM access

Last week

What is just-in-time VM access?

Just-in-time VM access enables you to lock down your VMs in the network level by blocking inbound traffic to specific ports. It enables you to control the access and reduce the attack surface to your VMs, by allowing access only upon a specific need.

Learn more about just-in-time VM access >

How does it work?

Upon a user request, based on Azure RBAC, Defender for Cloud will decide whether to grant access. If a request is approved, Defender for Cloud automatically configures the NSGs to allow inbound traffic to these ports, for the requested amount of time, after which it restores the NSGs to their previous states.

Learn more about how to use just-in-time VM access >

Virtual machines

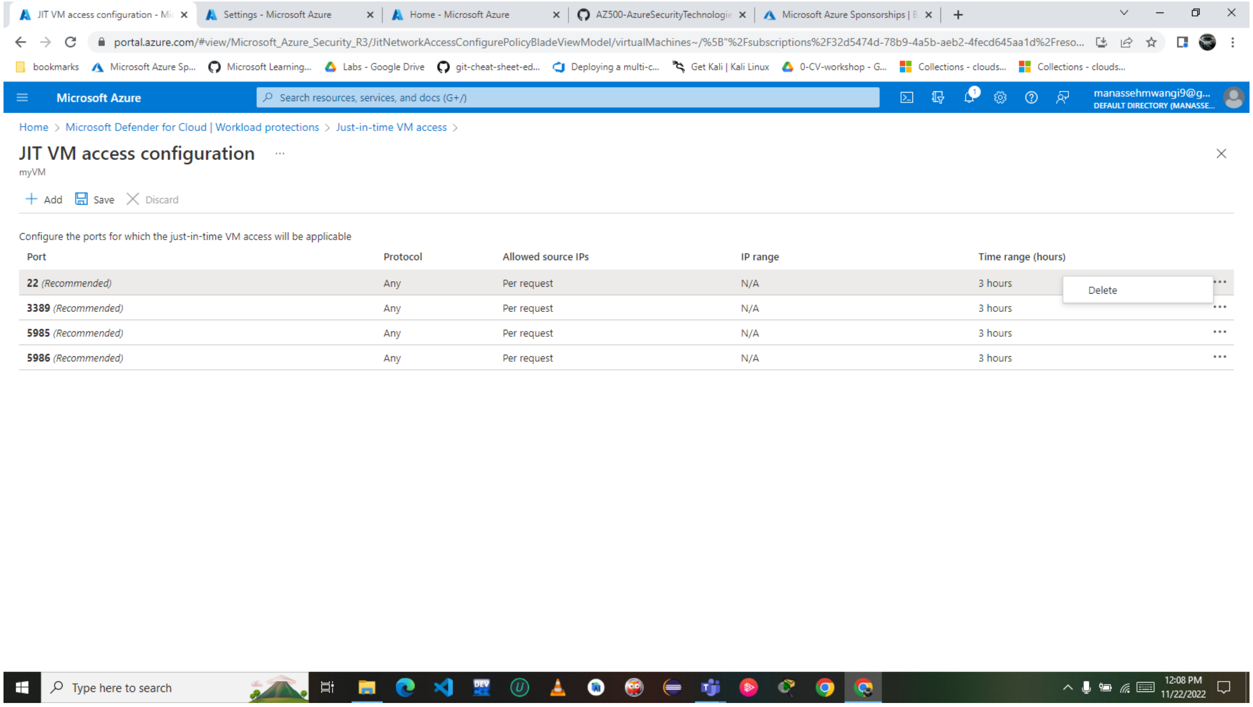
Configured | **Not Configured** | Unsupported

To let Defender for Cloud restrict access to your management ports, enable just-in-time (JIT) access control on all your "High" and "Low" risk VMs. JIT is unnecessary on a "Healthy" VM.

1 VMs

	Virtual machine	Resource group	Subscription Name	Severity	Reason
☑	myVM	AZ500LAB131415	Azure Pass - Sponsorship	High	This VM is protected by an NSG that allows access to management ports.

Referencing the port 22, click the ellipsis button and then click Delete. Click save



Home > Microsoft Defender for Cloud | Workload protections > Just-in-time VM access >

JIT VM access configuration

myVM

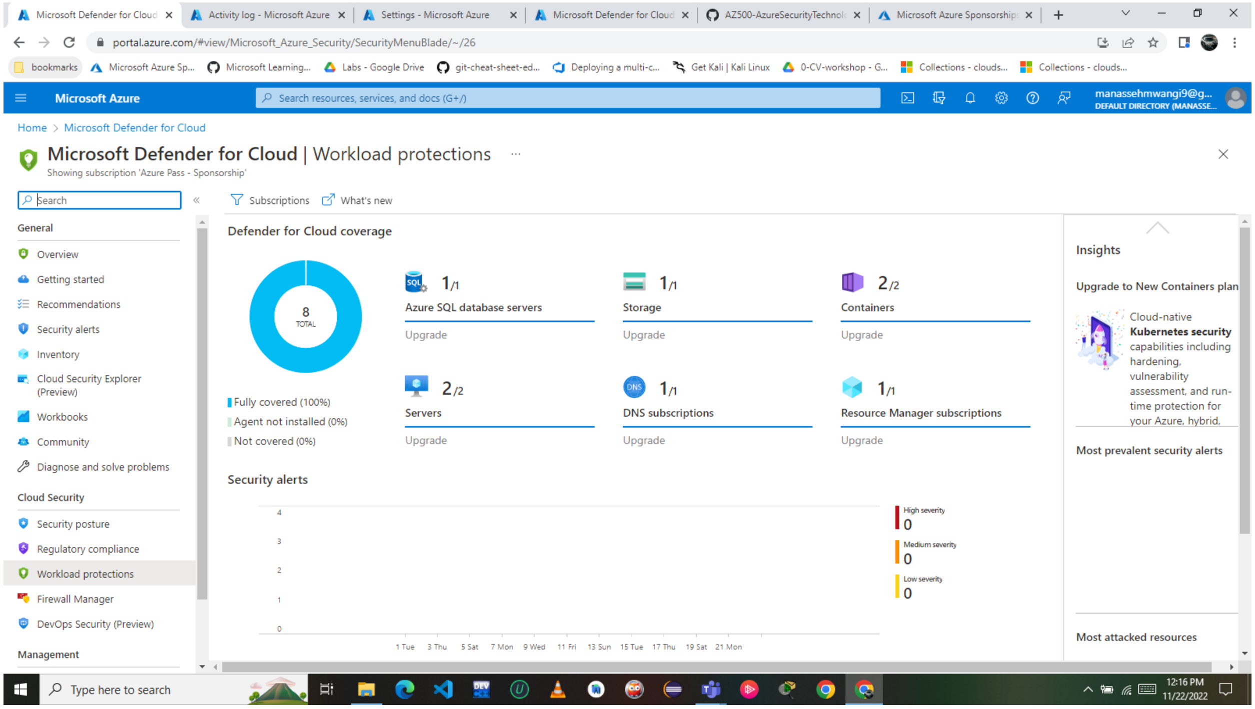
+ Add Save Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)
22 *(Recommended)*	Any	Per request	N/A	3 hours
3389 *(Recommended)*	Any	Per request	N/A	3 hours
5985 *(Recommended)*	Any	Per request	N/A	3 hours
5986 *(Recommended)*	Any	Per request	N/A	3 hours

Delete
portal.azure.com/#view/Microsoft_Azure_Security_R3/JitNetworkAccessConfigurePolicyBladeViewModel/virtualMachines~/%5B"%2Fsubscriptions%2F32d5474d-78b9-4a5b-aeb2-4fecd645aa1d%2Freso...
Microsoft Azure
Search resources, services, and docs (G+/)
manassehmwangi9@g...
DEFAULT DIRECTORY (MANASSE...
Type here to search
12:08 PM
11/22/2022

Check the Secure Score to determine the impact of implementing these features.



Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Workload protections

Showing subscription 'Azure Pass - Sponsorship'

Defender for Cloud coverage

8 TOTAL

Fully covered (100%)
Agent not installed (0%)
Not covered (0%)

1/1 Azure SQL database servers Upgrade	1/1 Storage Upgrade	2/2 Containers Upgrade
2/2 Servers Upgrade	1/1 DNS subscriptions Upgrade	1/1 Resource Manager subscriptions Upgrade

Security alerts

High severity 0
Medium severity 0
Low severity 0

Insights

Upgrade to New Containers plan

Cloud-native **Kubernetes security** capabilities including hardening, vulnerability assessment, and run-time protection for your Azure, hybrid,

Most prevalent security alerts

Most attacked resources