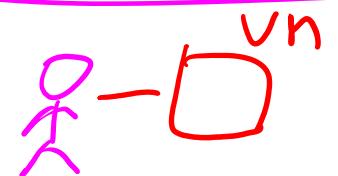


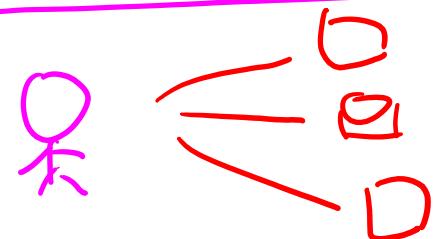
## System Assigned



1 : 1

der selbe Lifecycle

## User Assigned



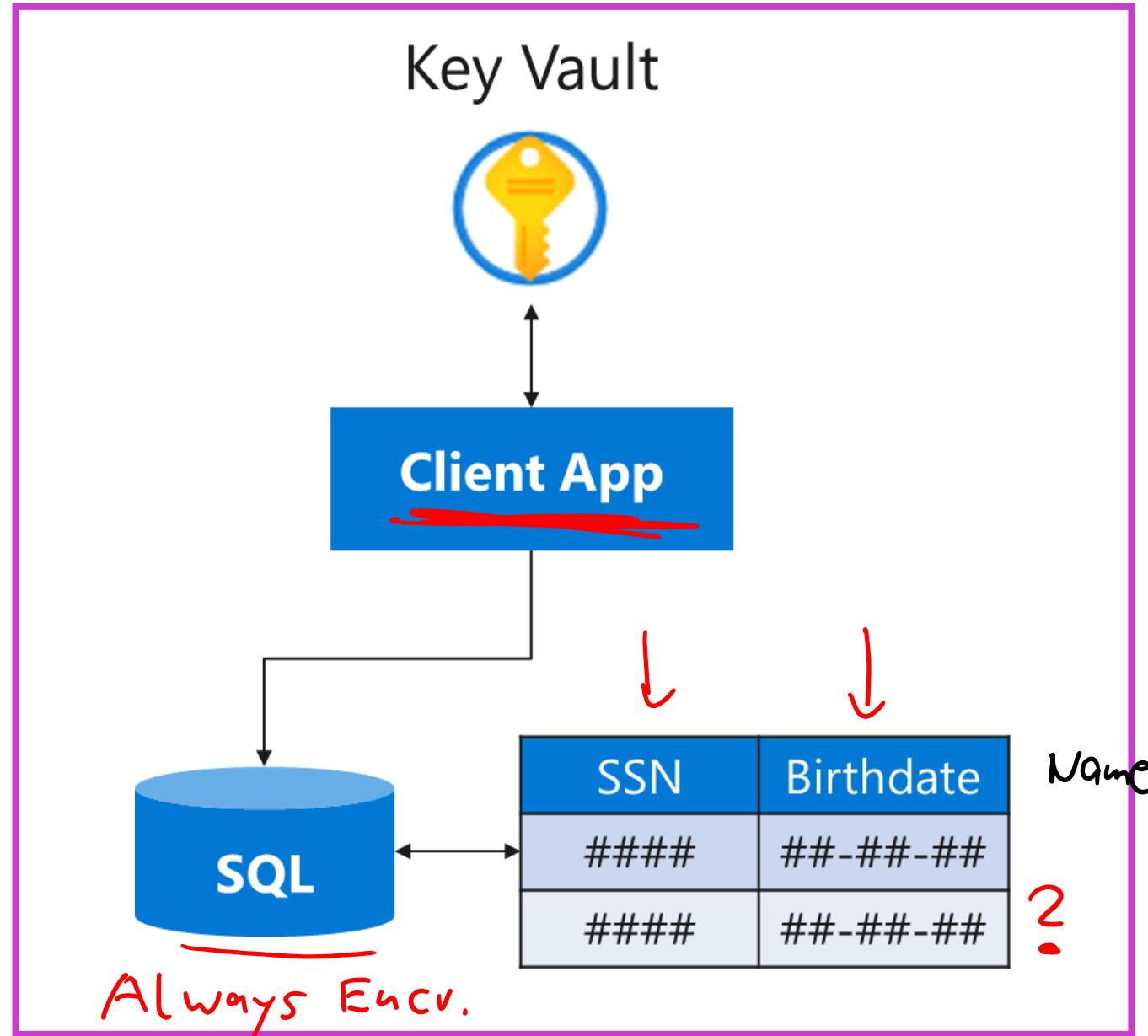
1 : N

Dauerhaft

z.B. vNSS  
scale set

# Lab 07 – Key Vault

- Create a Key Vault and configure permissions
- Add a key and a secret to the vault
- Register a client app that uses the key
- Create a SQL database
- Encrypt columns in a table
- Build a console app to test the encryption

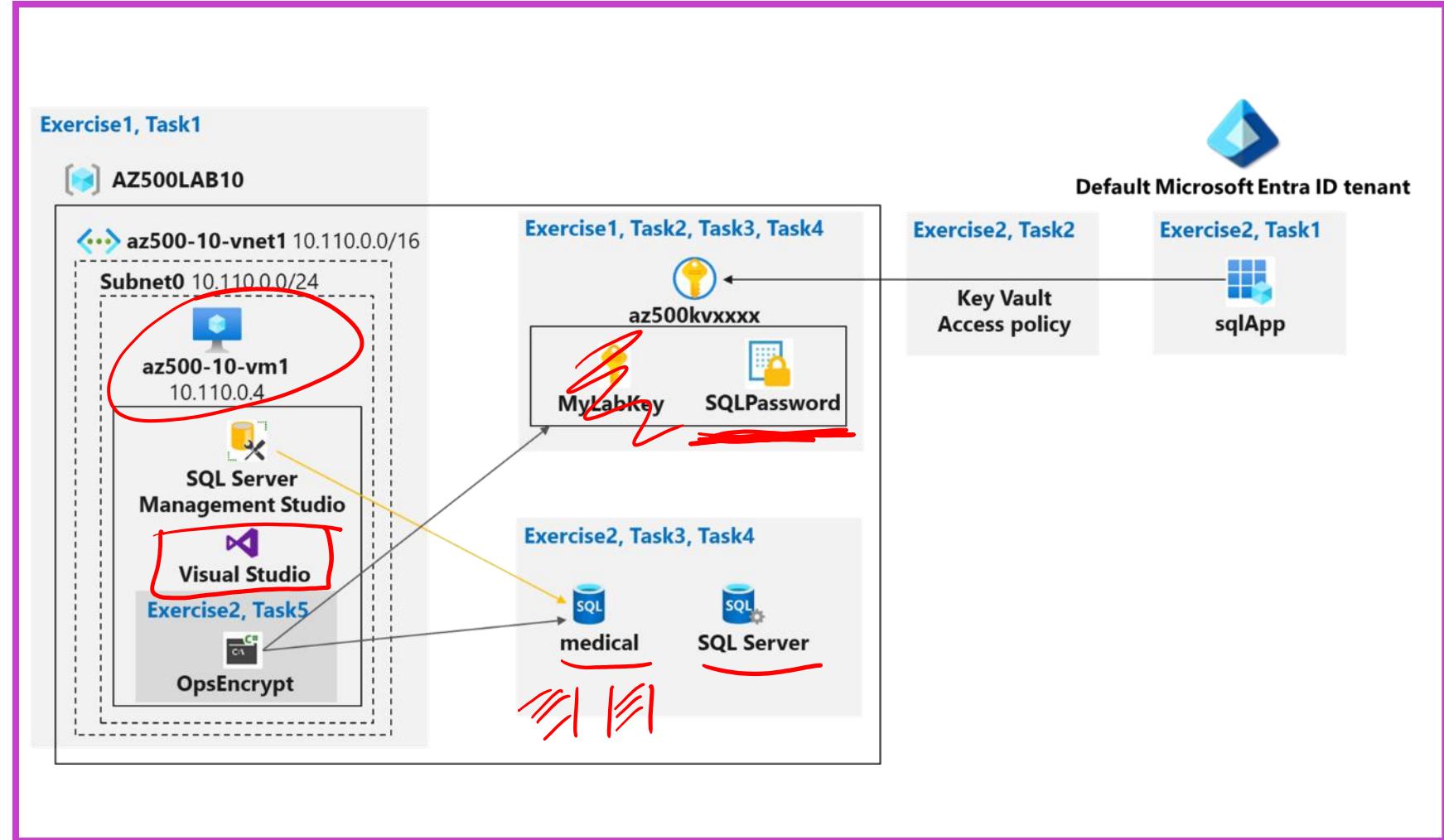


# Lab 07 – Key Vault



This exercise teaches students how to create an Azure Key Vault and store keys and secrets in the vault, create a SQL Database, and encrypt the content of columns in database tables by using Always Encrypted.

[Launch this Exercise in GitHub](#)



AZ-500

Tag 4

Secure cloud resources  
with Microsoft security  
technologies

Guten Morgen!



# Agenda

---

LP

- 1 Secure identity and access
- 2 Secure networking
- 3 Secure compute, storage, and databases
- 4 Secure Azure using Microsoft Defender for Cloud and Microsoft Sentinel

SC-200 - KQL

DCR  
AMA

Monitoring

# Learning Path: Secure Azure using Microsoft Defender for Cloud and Microsoft Sentinel

Manage security posture by using Microsoft Defender for Cloud

Configure and manage threat protection by using Microsoft Defender for Cloud

Configure and manage security monitoring and automation solutions

Module labs

# Learning Objectives

After completing this learning path, you will be able to:

- 1** Implement security operations, and deploy Azure policies, infrastructures, while securing keys and certificates.
- 2** Enhance Defender's security posture, ensure compliance, and monitor external threats.
- 3** Set up Defender for diverse threats, manage alerts, and leverage Sentinel for advanced security strategies.

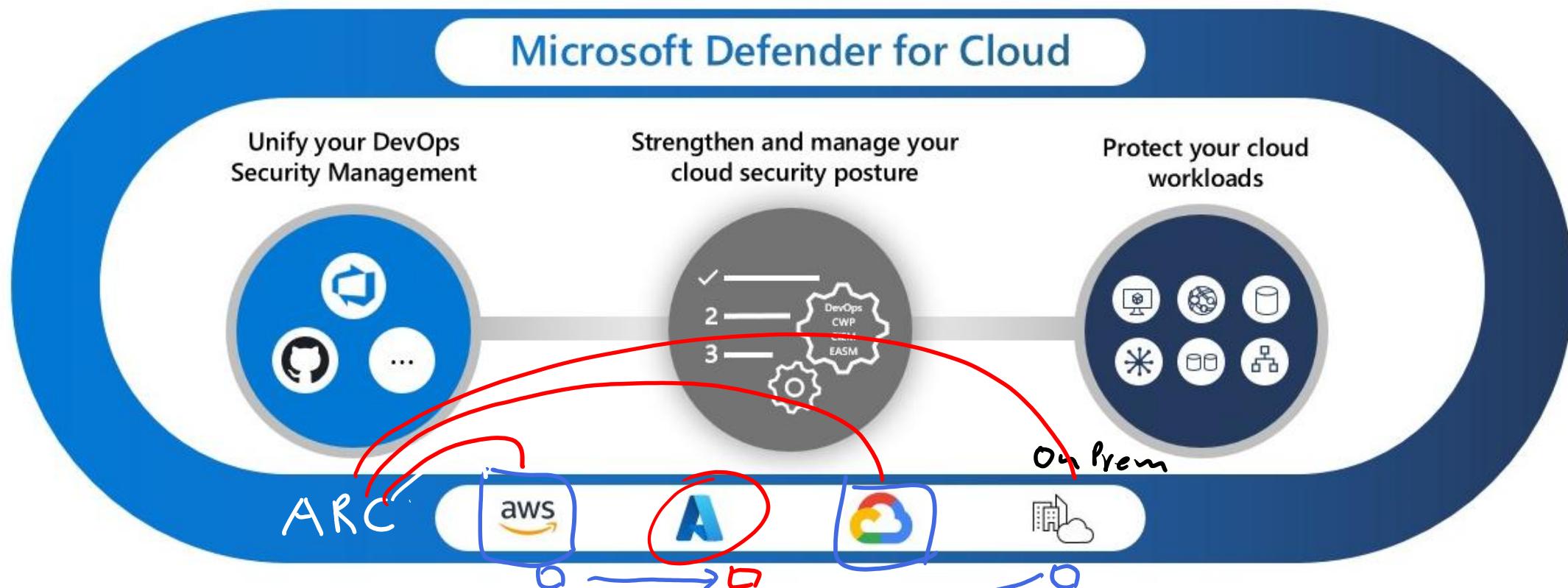
Def EP      Def Office      Def Cloud APP      Def Cloud ID  
↓            |            ↓            |  
Defender for M365

Manage security posture by using  
Microsoft Defender for Cloud

Azure  
GCP  
AWS

Github  
GitLab

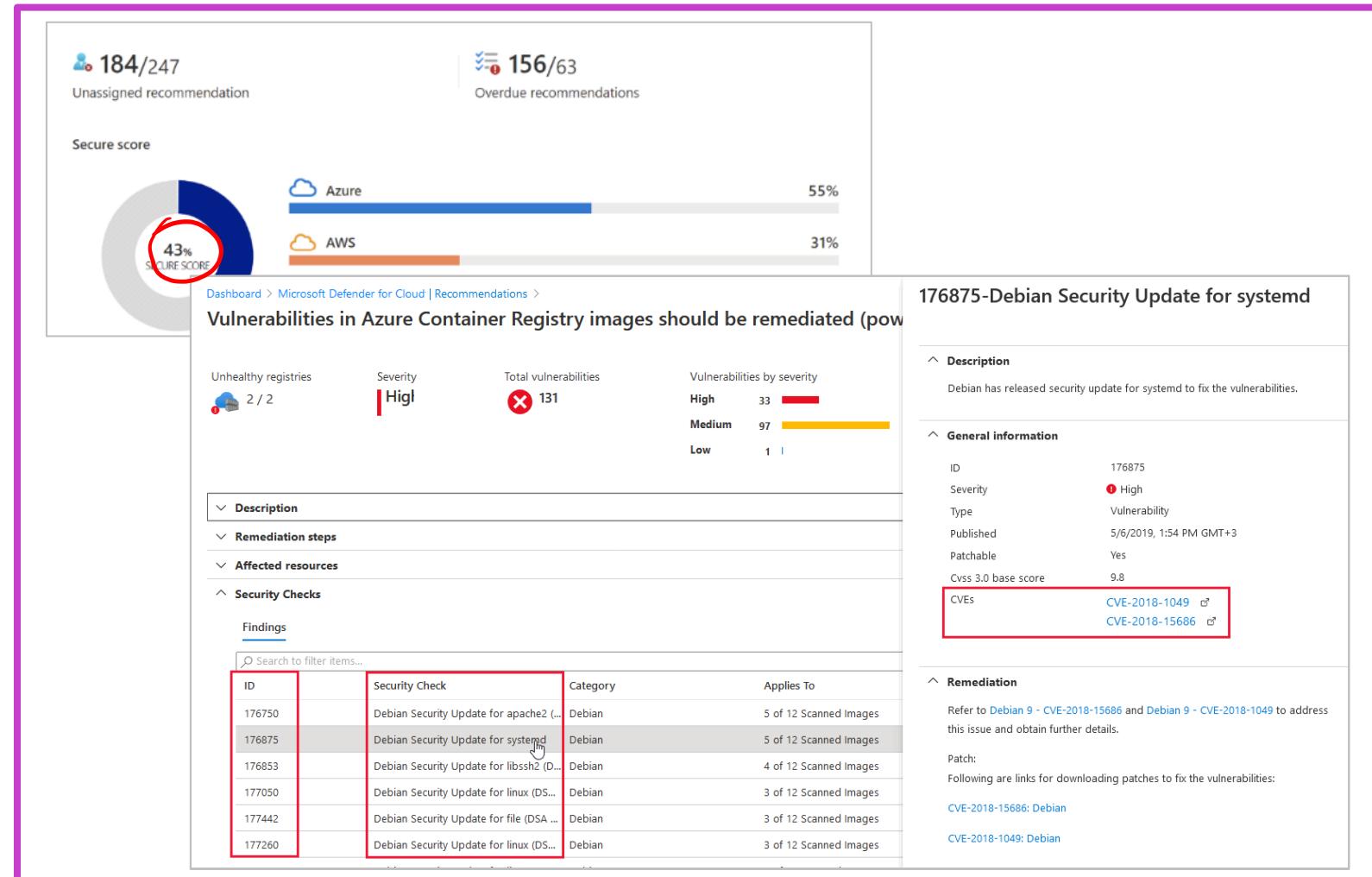
# Implement Microsoft Defender for Cloud



- Protect cloud apps and workloads: Secure resources with DevSecOps, CSPM, and CWPP solutions.
- Enhance security posture: Identify and remediate risks using Secure Score and compliance tools.
- Respond to threats: Detect, prioritize, and mitigate attacks with advanced threat detection capabilities.

# Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory

- Defender for Cloud evaluates cross-cloud resources for security threats.
- Secure Score aggregates findings to indicate the overall security status.
- Enhance security by following Defender's recommendations and using the Inventory page's filter for specific vulnerabilities.



# Assess compliance against security frameworks and Microsoft Defender for Cloud



- Visit the regulatory compliance dashboard for overall scores and assessment results.
- View controls, associated assessments, and their status.
- Check both automated and manual assessments under the "**Your Actions**" tab.

The screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard. The main interface includes a sidebar with navigation links like General, Cloud Security, and Management. The main content area displays various compliance standards (e.g., Azure Security Benchmark V3, ISO 27001, NIST SP 800 53 R4) and a section for "Regulatory compliance". A red circle highlights the "NIST SP 800 53 R4" tab. Below it, a list of controls is shown, with one control, "AC. Access Control", circled in red. To the right, a detailed view of the "AC.2.7 Role-based Schemes" section is displayed, showing a table of actions categorized by type (Automated, Manual) and action name.

Action Type	Action Name
Technical	Audit usage of custom RBAC rules
Technical	Service Fabric clusters should only use Azure Active Directory for client authentication
Technical	SQL servers should have an Azure Active Directory administrator provisioned
Operational	Audit privileged functions
Operational	Monitor account activity
Operational	Monitor privileged role assignment
Operational	Restrict access to privileged accounts
Operational	Revoke privileged roles as appropriate
Operational	Use privileged identity management

# Manage compliance standards Microsoft Defender for Cloud

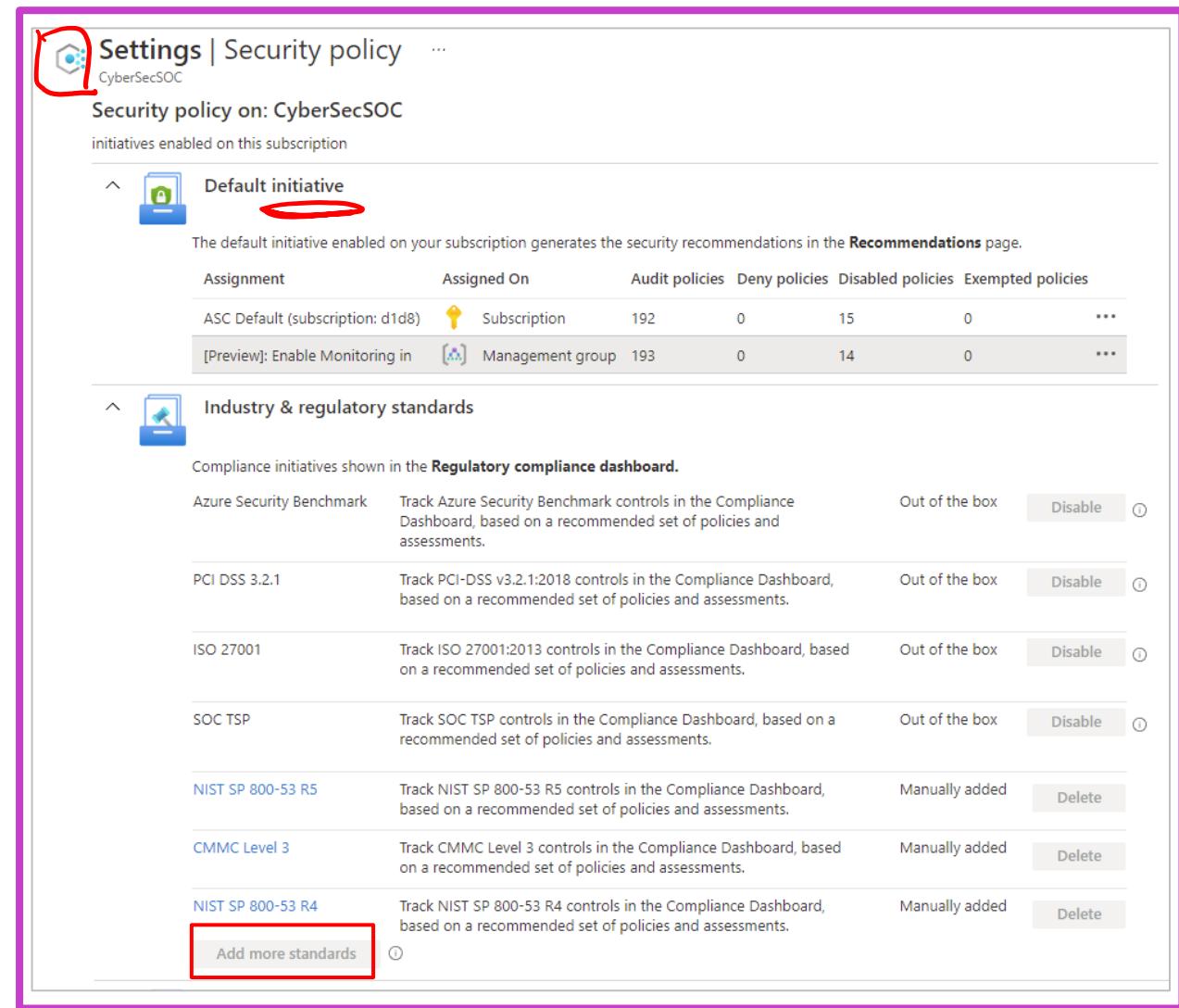
Azure  
Policies



- Open the **Security policy** page and select **Add more standards** to add industry standards.

You can add industry standards such as:

- Regulatory standards
- AWS regulatory standards
- GCP regulatory standards



Settings | Security policy

Security policy on: CyberSecSOC

initiatives enabled on this subscription

Default initiative

The default initiative enabled on your subscription generates the security recommendations in the [Recommendations](#) page.

Assignment	Assigned On	Audit policies	Deny policies	Disabled policies	Exempted policies
ASC Default (subscription: d1d8)	Subscription	192	0	15	0
[Preview]: Enable Monitoring in	Management group	193	0	14	0

Industry & regulatory standards

Compliance initiatives shown in the [Regulatory compliance dashboard](#).

Initiative	Description	Status	Action
Azure Security Benchmark	Track Azure Security Benchmark controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Disable
PCI DSS 3.2.1	Track PCI-DSS v3.2.1:2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Disable
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Disable
SOC TSP	Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Disable
NIST SP 800-53 R5	Track NIST SP 800-53 R5 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Manually added	Delete
CMMC Level 3	Track CMMC Level 3 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Manually added	Delete
NIST SP 800-53 R4	Track NIST SP 800-53 R4 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Manually added	Delete

Add more standards

# Add custom standards to Microsoft Defender for Cloud

- Open the **Security policy** page and select **Add a custom initiative**.
- Create a new custom initiative by selecting **Create new** and configure the policies and parameters

The screenshot illustrates the steps to add a custom standard to Microsoft Defender for Cloud. It features three main windows:

- Left Panel:** A blue sidebar with a clipboard icon and a plus sign, containing the instructions listed above.
- Middle Panel:** A modal titled "Add custom initiatives". It includes a "Create new" button (highlighted with a red box) and a "Refresh" button. Below is a table with one row:

NAME	DESCRIPTION	STATUS	Actions
Organizational policy	custom policy	Not assigned	<b>Add</b> (highlighted with a red box)
- Right Panel:** An "Organizational policy" configuration page. It has tabs for Basics, Parameters, Remediation, Non-compliance messages, and Review + create. The Basics tab is selected. It contains fields for Scope (with a link to "Learn more about setting the scope"), Exclusions (with a note to " Optionally select resources to exclude from the policy assignment"), Initiative definition (set to "Organizational policy"), Assignment name (set to "Organizational policy"), Description (empty), Policy enforcement (set to "Enabled" and "Disabled"), and Assigned by (empty). At the bottom are buttons for Review + create, Cancel, Previous, and Next.

# Connect hybrid cloud and multi-cloud environments to Microsoft Defender for Cloud including Amazon Web Services (AWS) and Google Cloud Platform (GCP)



## Connect hybrid cloud environments

You can connect your non-Azure computers in the following ways:

- Using Azure Arc-enabled servers (recommended)
- From Defender for Cloud's pages in the Azure portal



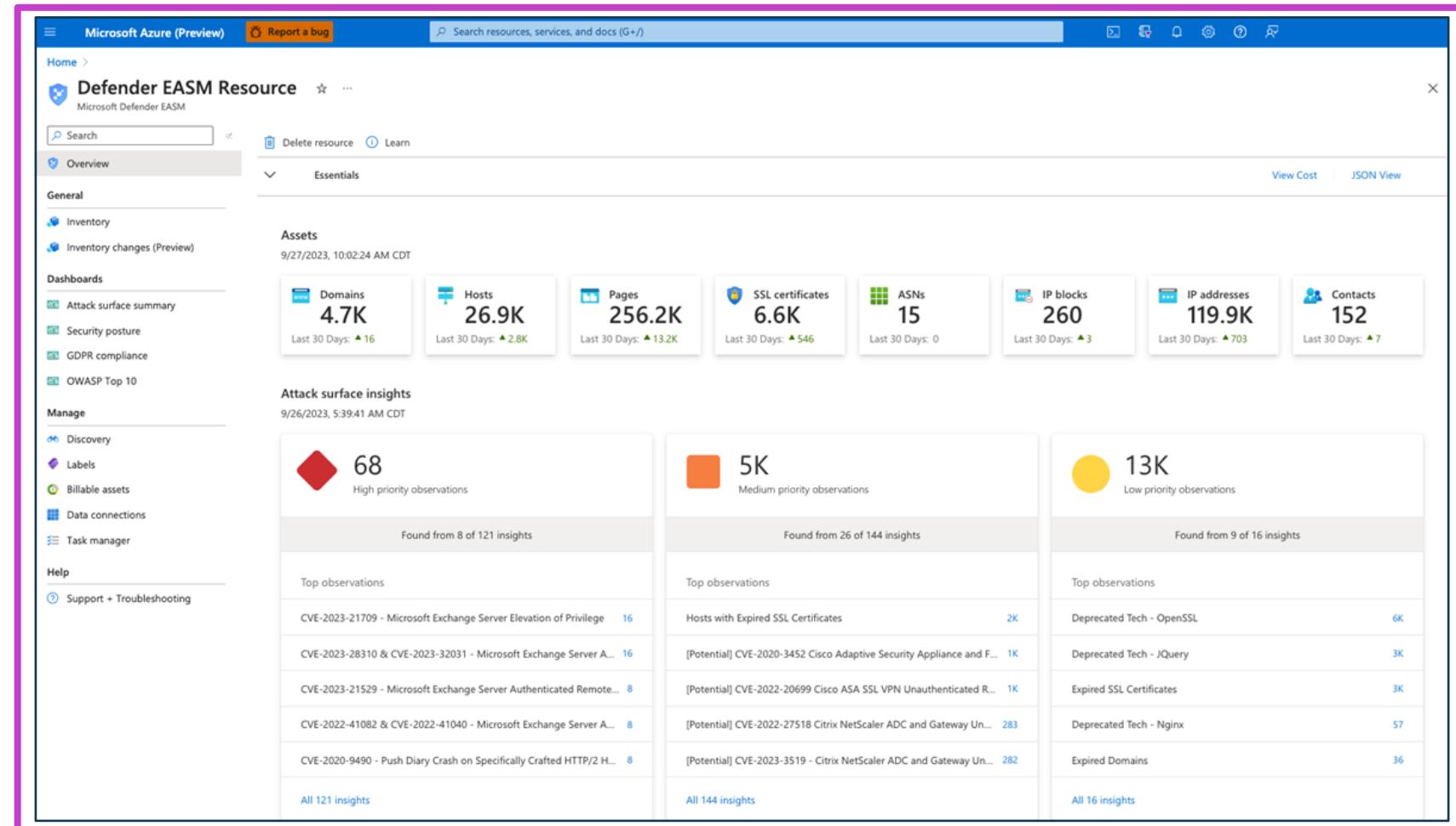
## Connect multi-cloud environments

You can connect multi-cloud environments through:

- Native cloud connector (recommended)
- Classic connector

# Implement and use Microsoft Defender External Attack Surface Management (EASM)

- Continuous Discovery: Defender EASM maps your attack surface, identifying unknown assets and potential vulnerabilities.
- Risk Insights: Dashboards highlight vulnerabilities, compliance gaps, and high-risk components for prioritized remediation.
- Dynamic Asset Management: Indexes and categorizes assets, enabling filtering for tailored risk assessment and action.



# Additional Study – Manage security posture by using Microsoft Defender for Cloud

Microsoft  
Learn Modules  
([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))



## Module Review Questions

- Identify and Remediate Security Risks: Use Secure Score and Inventory in Microsoft Defender for Cloud to assess and address security risks.
- Assess and Manage Compliance Standards: Evaluate compliance against security frameworks and manage compliance standards in Defender for Cloud.
- Add Custom Compliance Standards: Define and implement custom standards to tailor compliance requirements in Defender for Cloud.
- Connect Hybrid and Multi-Cloud Environments: Integrate AWS, GCP, and on-premises environments with Microsoft Defender for Cloud.
- Implement Microsoft Defender EASM: Use External Attack Surface Management (EASM) to monitor and reduce external security risks.

# Configure and manage threat protection by using Microsoft Defender for Cloud

# Enable workload protection services in Microsoft Defender for Cloud

The screenshot shows the 'Settings | Defender plans' page in the Microsoft Defender for Cloud Azure portal. The left sidebar includes 'Search', 'Save', 'Settings & monitoring', and sections for 'Settings', 'Defender plans' (which is selected), 'Security policies', 'Email notifications', 'Workflow automation', and 'Continuous export'. The main content area displays two sections: 'Cloud Security Posture Management (CSPM)' and 'Cloud Workload Protection (CWP)'. The CSPM section lists 'Foundational CSPM' (Free) and 'Defender CSPM' (\$5/Billable resource/Month). The CWP section lists 'Servers' (Plan 2 (\$15/Server/Month)). Status switches for each plan are shown as 'Off' or 'On'.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free Details >		Full	Off On
Defender CSPM	\$5/Billable resource/Month Details >	4 resources ⓘ		Off On

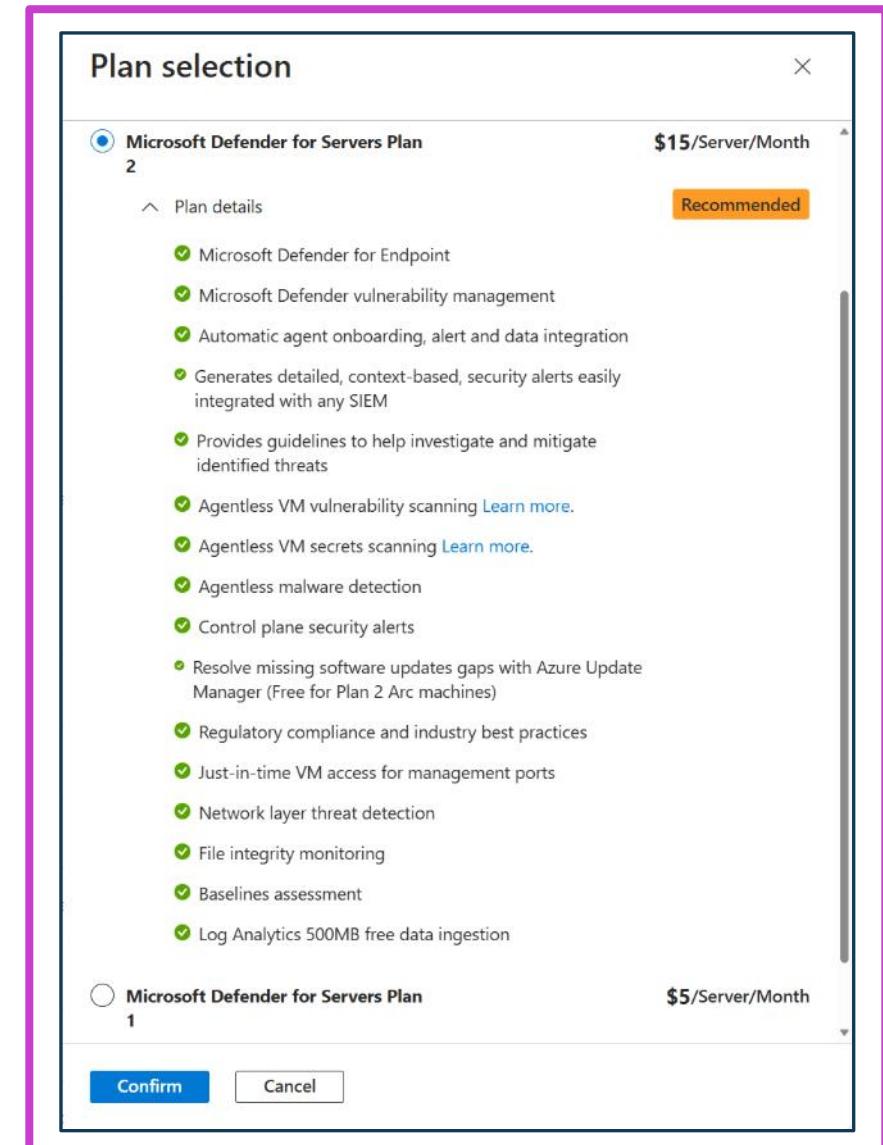
  

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month) Change plan >	2 servers	Full Settings >	Off On

- Comprehensive Protection: Defender for Servers safeguards Windows and Linux VMs in Azure, AWS, GCP, and on-premises.
- Security Enhancements: Provides recommendations to improve machine security posture and protect against threats.
- Flexible Deployment: Enable and configure the plan for specific environments via Azure portal.

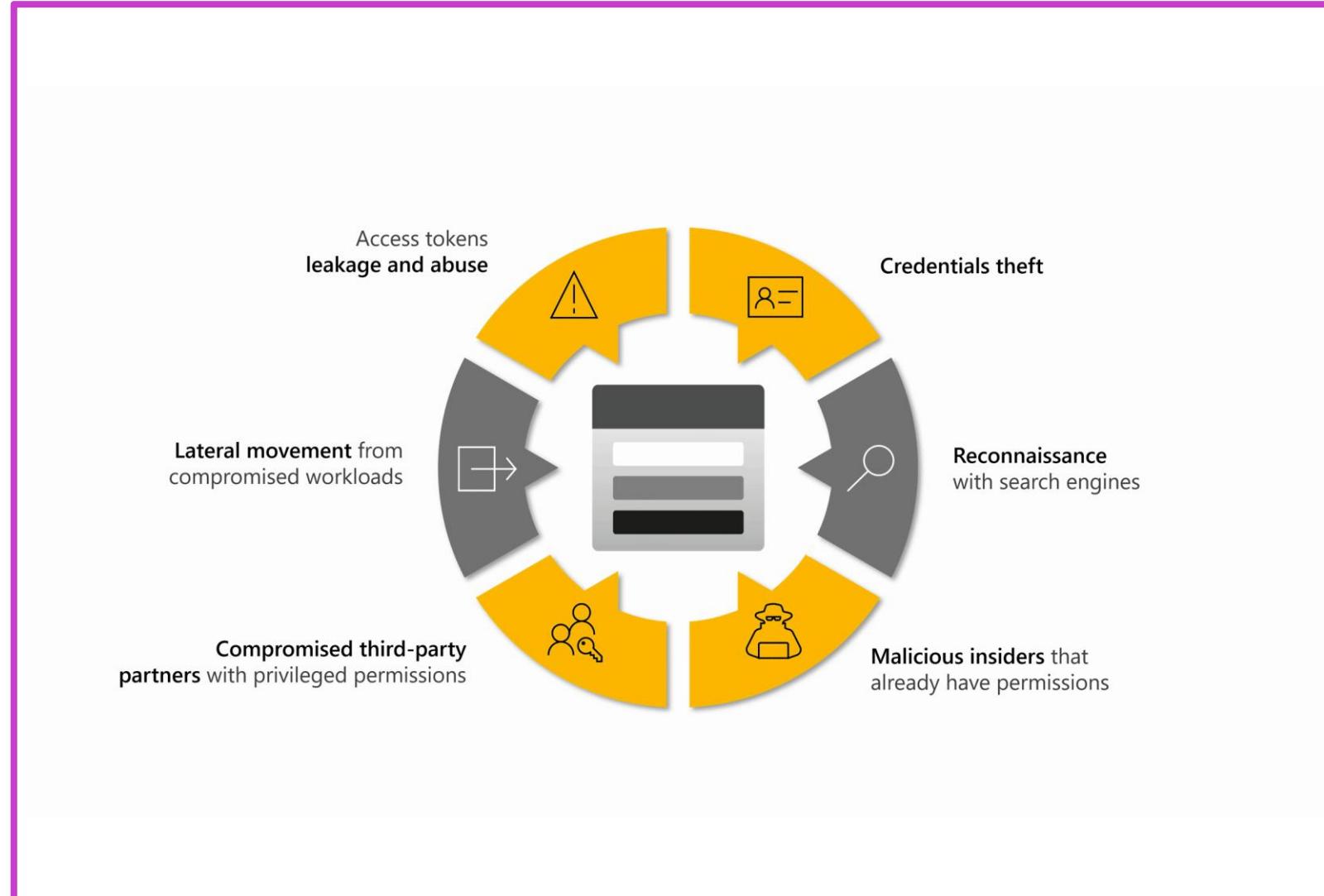
# Microsoft Defender for Servers

- Defender for Servers protects multicloud and on-premises machines, improving security posture and reducing risks.
- Plan 2 includes advanced features: agentless scanning, malware detection, and file integrity monitoring.  
  
Fin
- Flexible deployment supports subscriptions and resources with integrated compliance and threat detection tools.



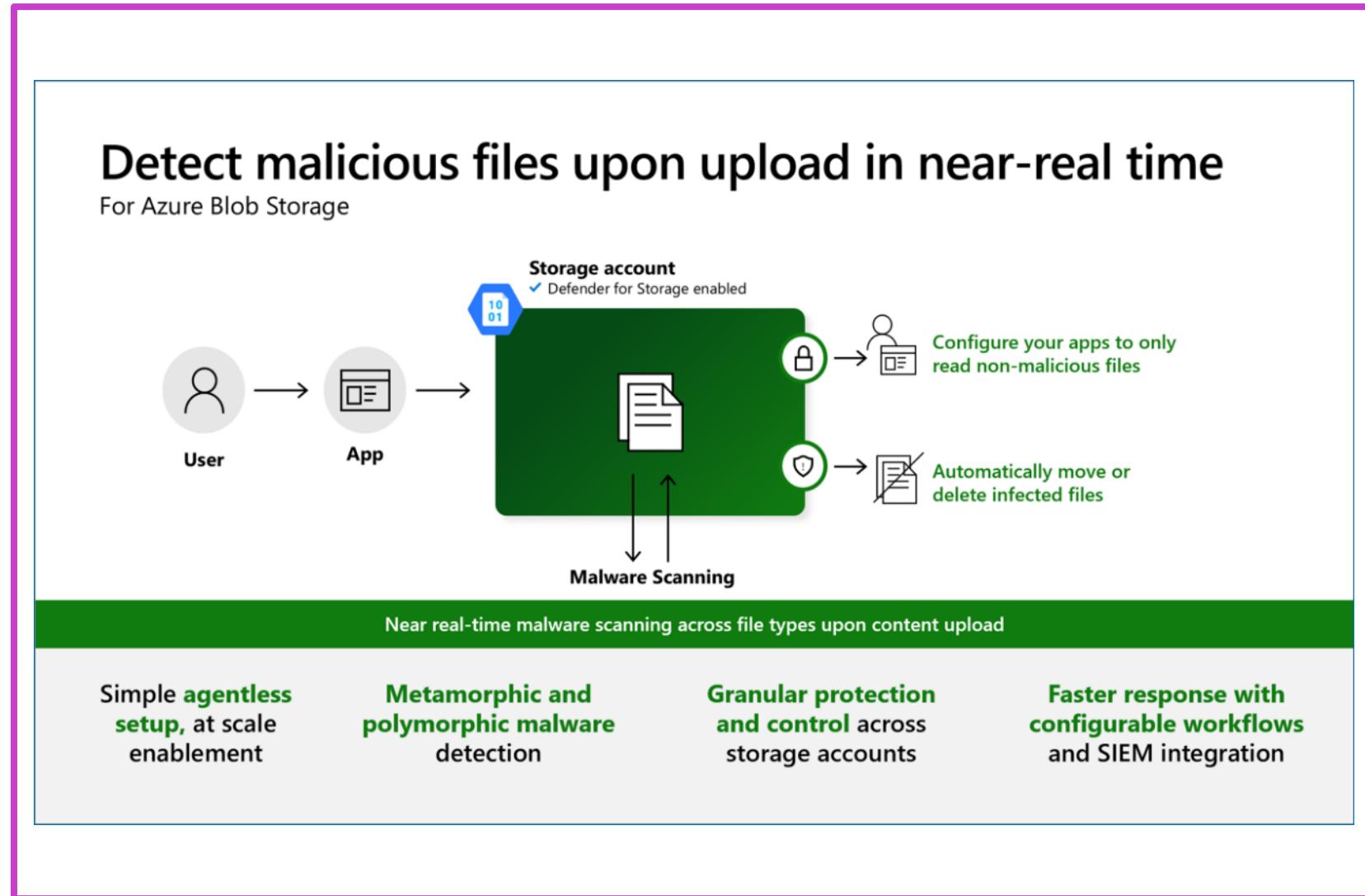
# Microsoft Defender for Storage

- Detects threats, prevents malicious uploads, data exfiltration, and corruption.
- Uses Microsoft Threat Intelligence, Defender Antivirus, Sensitive Data Discovery.
- Agentless, scales easily, protects Azure Blob, Files, Data Lake Storage.



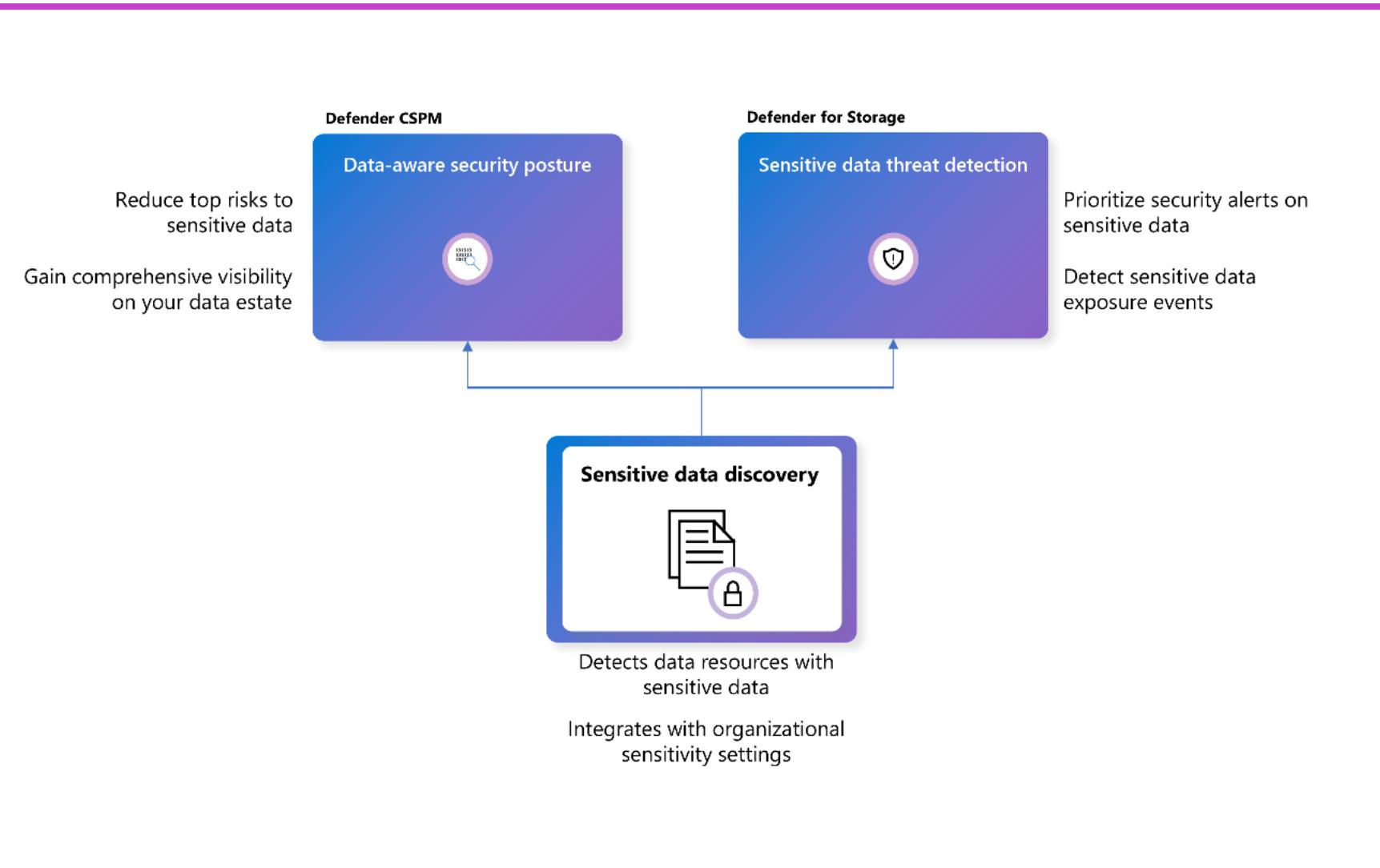
# Malware scanning in Defender for Storage

- Scans uploads in real-time for malware, supports all file types.
- Detects sensitive data threats, enhances data protection.
- Agentless, scalable setup; provides comprehensive security analytics.



# Detect threats to sensitive data

- Prioritizes alerts by data sensitivity, enhancing breach detection and prevention.
- Agentless scanning integrated with Microsoft Purview for policy alignment.
- Configurable without extra cost, automatic scans for new and existing storage.



# Enable and configure at scale with an Azure built-in policy

- Facilitates scalable, consistent security across all storage accounts via policy.
- Utilize Azure Policy dashboard to enable and configure Defender for Storage features.
- Assign policy for comprehensive or basic Defender for Storage capabilities, including customization.

The screenshot shows the Azure Policy Definitions interface. At the top, there's a search bar and navigation links for Overview, Getting started, Compliance, Remediation, and Events. Below that, a table lists policy definitions. The first row in the table is selected, showing its details in a modal window below.

**Policy | Definitions**

Name	Definition location	Policies	Type	Definition type	Category
Configure Microsoft Defender for Storage to be enabled			BuiltIn	Policy	Security Center
Configure basic Microsoft Defender for Storage to be enabled (Activity Monitoring only)			BuiltIn	Policy	Security Center

**Configure Microsoft Defender for Storage to be enabled**

**Policy definition**

**Assign** (button) Edit definition Duplicate definition Delete definition

**Essentials**

Name	: Configure Microsoft Defender for Storage to be enabled	Definition location	:
Description	: Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects potential thre...	Definition ID	:
Available Effects	: DeployIfNotExists, Disabled	Type	: Built-in
Category	: Security Center	Mode	: All

**Definition** Assignments (0) Parameters

```
1 {
2   "properties": {
3     "displayName": "Configure Microsoft Defender for Storage to be enabled",
4     "policyType": "BuiltIn",
5     "mode": "All",
6     "description": "Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects potential threats to your storage accounts.\r\n\r\nThis policy will enable all Defender for Storage features in your storage accounts.",
7     "metadata": {
8       "version": "1.0.2",
9       "category": "Security Center"
10    },
11    "parameters": {
12      "effect": {
13        "type": "String",
14        "metadata": {
15          "displayName": "Effect",
16          "description": "Enable or disable the execution of the policy"
17        }
18      }
19    }
20  }
```

# Configure Microsoft Defender for Servers, Microsoft Defender for Databases, and Microsoft Defender for Storage

The screenshot shows the Microsoft Defender for Cloud Settings page under the 'Defender plans' section. It displays the 'Cloud Workload Protection (CWP)' configuration for a specific environment. The table lists various resource types and their protection status.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month) Change plan >	2 servers	Full Settings >	Off On
App Service	\$15/Instance/Month Details >	0 instances		Off On
Databases	Selected: 0/4 Select types >	Protected: 0/0 instances	Full Settings >	Off On
Storage	\$10/Storage account/month \$0.15/GB scanned for On-Upload Malware Details >	2 storage accounts	Full Settings >	Off On
Containers	\$6.8693/VM core/Month Details >	0 container registries; 0 kubernetes clusters		Off On
Key Vault	\$0.25/Vault/Month Details >	1 key vaults		Off On

- Defender for Servers: Protects Azure VMs, improves security posture, and mitigates threats for cloud environments.
- Defender for Storage: Secures Azure storage accounts with malware scanning, sensitive data protection, and flexible configurations.
- Defender for Databases: Provides comprehensive protection for Azure SQL, Cosmos DB, and open-source databases.

# Implement and manage agentless scanning for virtual machines in Microsoft Defender for Servers

The screenshot shows the Microsoft Azure (Preview) interface with the title "Settings | Defender plans". The left sidebar shows "Defender plans" selected under "Settings". The main content area is divided into two sections: "Cloud Security Posture Management (CSPM)" and "Cloud Workload Protection (CWP)".

**Cloud Security Posture Management (CSPM):**

- Foundational CSPM: Free, Details >. Monitoring coverage is Full (On).
- Defender CSPM: \$5/Billable resource/Month, Details >. Resource quantity: 2 resources. Monitoring coverage is Full (On).

**Cloud Workload Protection (CWP):**

- Servers: Plan 2 (\$15/Server/Month), Change plan >. Resource quantity: 0 servers. Monitoring coverage is Full (On).
- App Service: \$15/Instance/Month, Details >. Resource quantity: 0 instances. Monitoring coverage is Full (On).

- Enhanced Security: Scans for vulnerabilities, malware, secrets, and software inventory across connected environments.
- Seamless Integration: No agents or connectivity needed, supports Azure, AWS, GCP, and Kubernetes nodes.
- Easy Enablement: Enabled by default in Defender CSPM or Servers Plan 2, with manual configuration options.

# Implement and manage Microsoft Defender Vulnerability Management for Azure

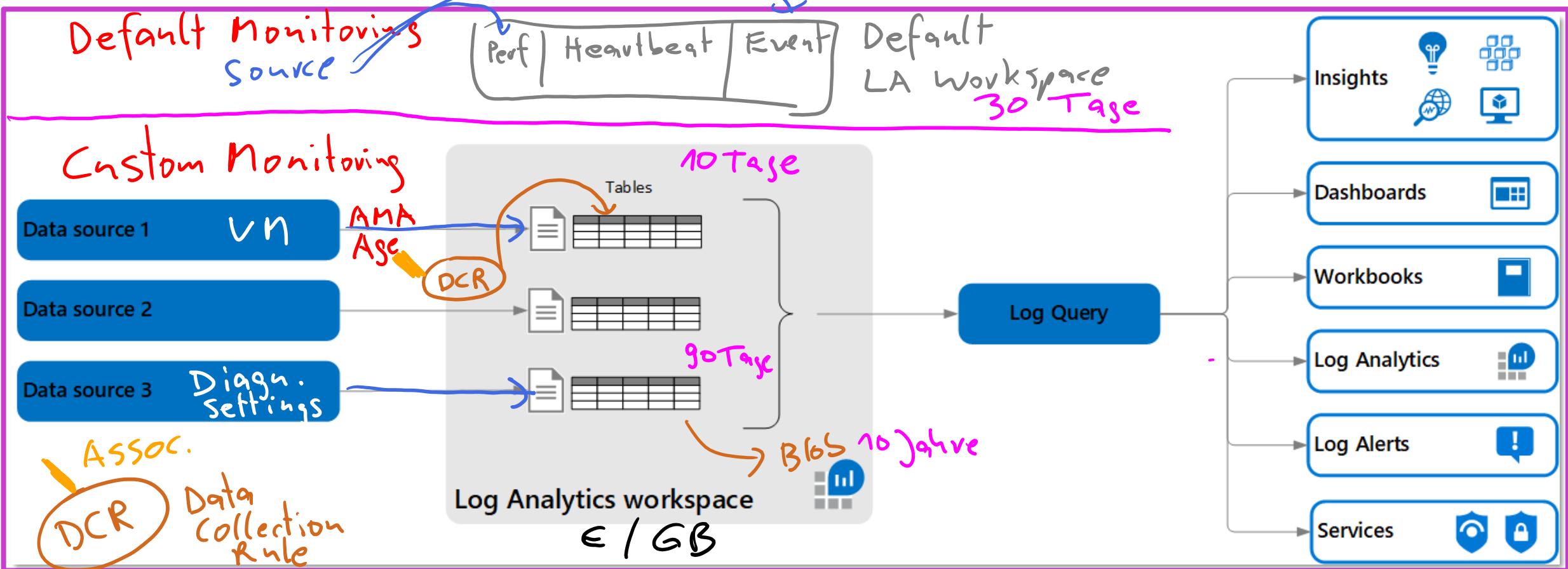
The screenshot shows the Microsoft Defender for Cloud Settings & monitoring page. At the top, there are 'Save' and 'Settings & monitoring' buttons. Below this, the 'Cloud Workload Protection (CWP)' section is expanded. A descriptive text states: 'Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.' A table summarizes the current configuration:

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month) <a href="#">Change plan &gt;</a>	8 servers	Full <a href="#">Settings &gt;</a>	<input type="button" value="Off"/> <input checked="" type="button" value="On"/>

Below the table, a 'Registry access' section is shown, which enables agentless vulnerability assessment for registry images. It includes a status indicator (blue/green icon), a 'Settings >' link, and a toggle switch set to 'On'.

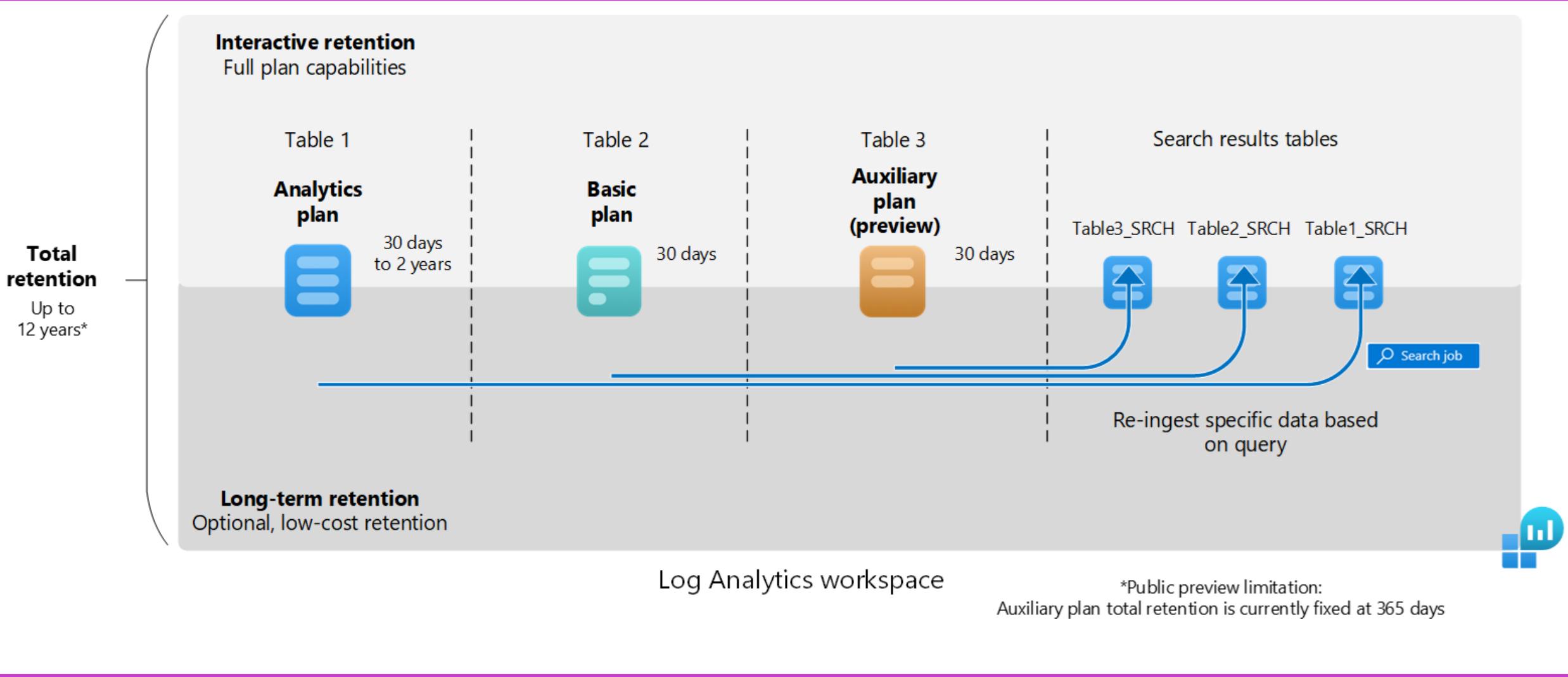
- Automatically scans ACR images for vulnerabilities without any agent deployment.
- Supports OS and language package scanning with continuous daily rescans.
- Provides detailed vulnerability reports and remediation recommendations for secure deployments.

# Log Analytics workspace



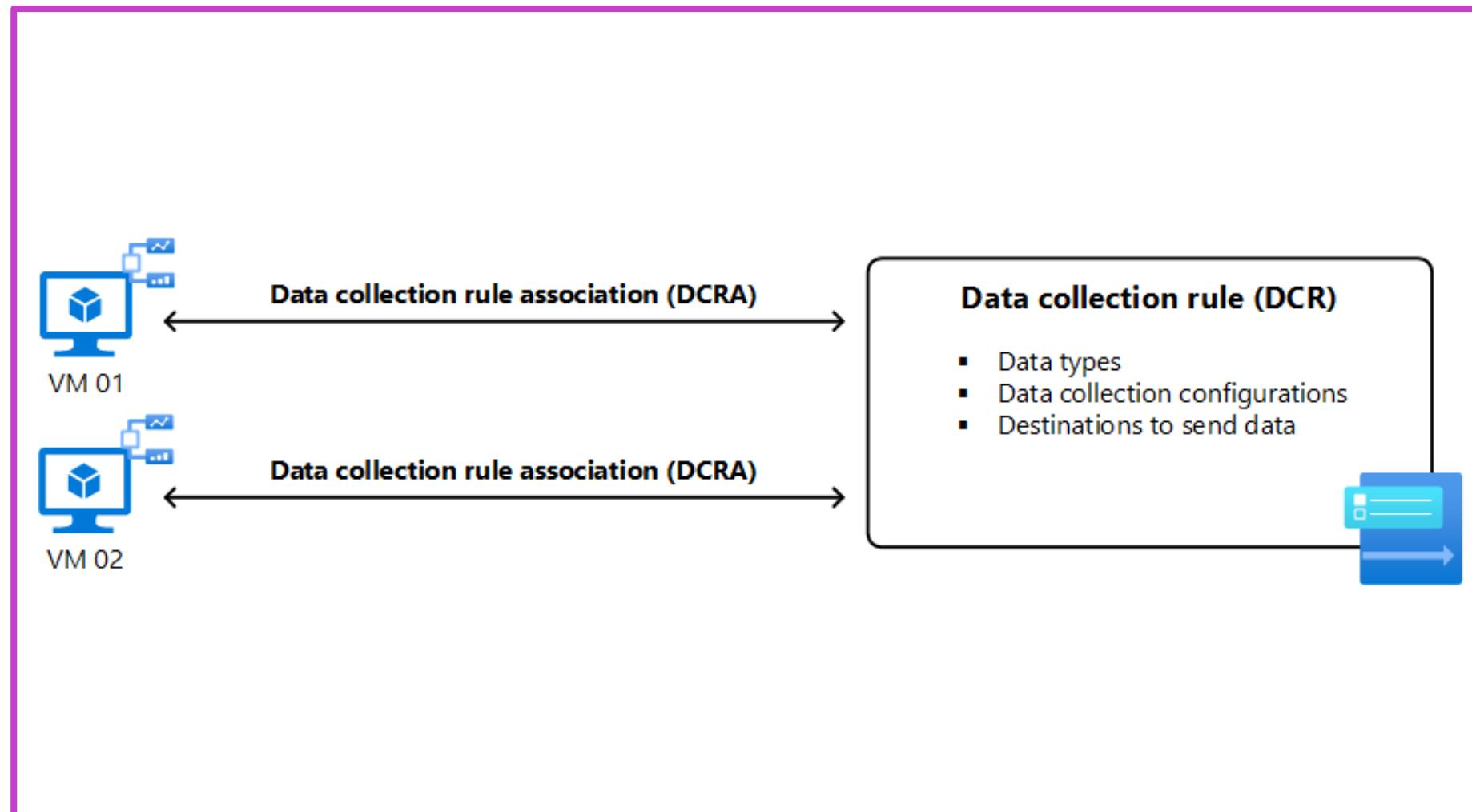
- A Log Analytics workspace is a centralized, configurable environment for Azure Monitor log data, allowing data collection and retention management across multiple Azure services.

# Manage data retention in a Log Analytics workspace



# Deploy the Azure Monitor Agent

- Azure Monitor Agent gathers data from guest operating systems across Azure, hybrid, and on-premises environments.
- Data Collection Rules (DCRs) manage data types, transformations, and destinations for flexible monitoring.
- Supports insights and services like Microsoft Sentinel and Defender for Cloud for enhanced security and compliance.



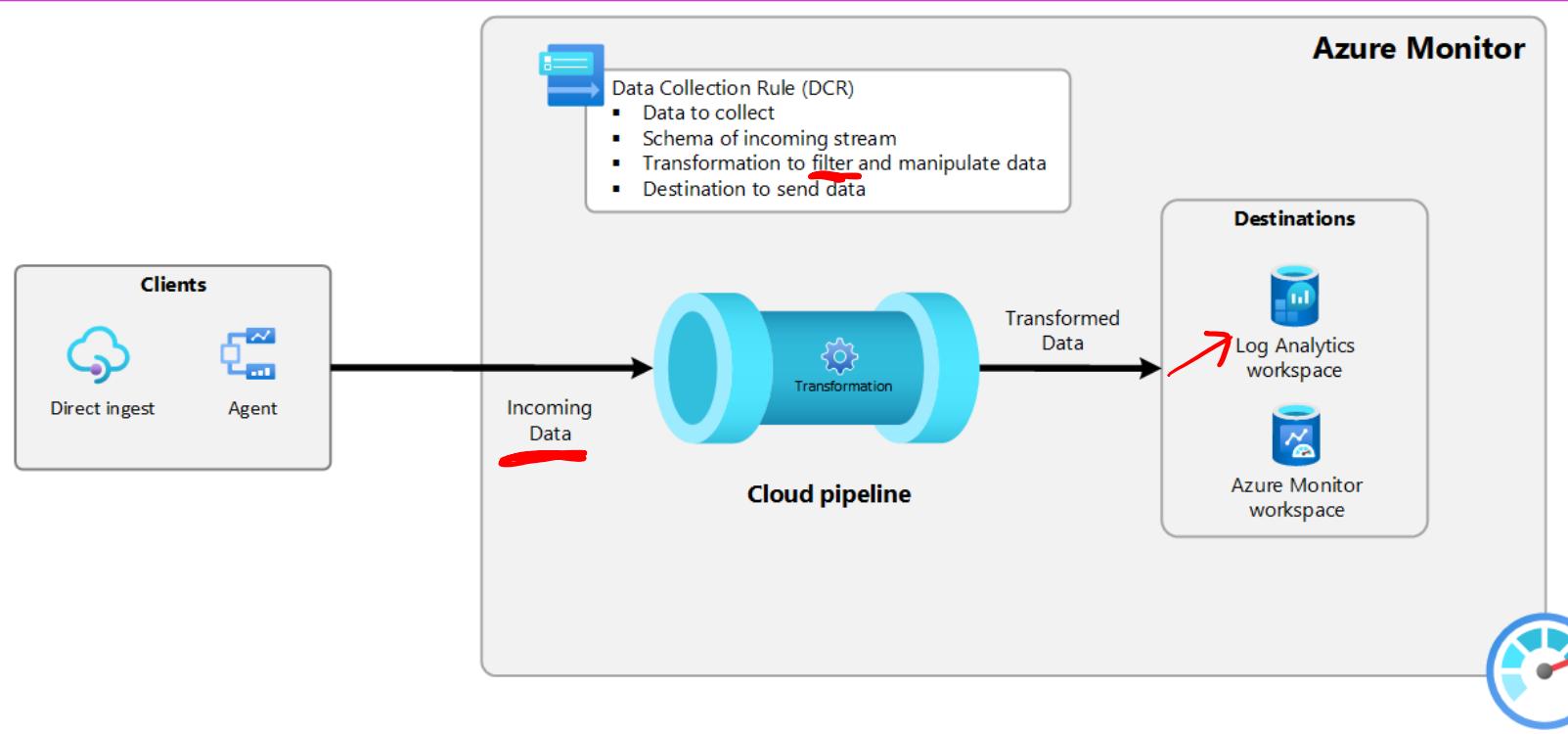
# Collect data with Azure Monitor Agent

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure (Preview)', a search bar, and various icons. Below the navigation bar, the URL path is visible: Home > Data collection rules > dcr-1 | Resources > vm-1. A yellow arrow points from the text 'Data collection rules > drc-1 for vm-1' to the URL path. On the left, a sidebar for 'vm-1 | Extensions + applications' is open, with 'Extensions + applications' highlighted by a red box. The main content area shows the 'Extensions' tab selected. A message box says 'The Azure Monitor Agent is deployed'. Below it, a table lists two items:

Name	Type	Version	Latest Version	Status	Automatic Upgrade
AzureMonitorWindows...	AzureMonitorWindows...	1.*	1.30.0.0	Enabled	Disabled
MDE.Windows	MDE.Windows	1.*	1.0.11.3	Not supported	Not supported

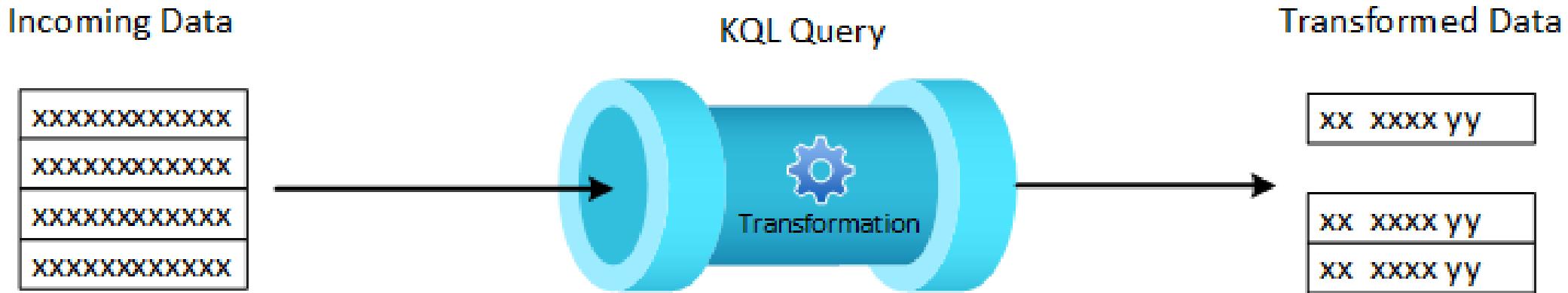
- Collects data from VMs, scale sets, and Arc-enabled servers.
- Uses Data Collection Rules (DCRs) to define and route data.
- Supports deployment via portal, CLI, PowerShell, or ARM templates.

# Data collection rules (DCRs) in Azure Monitor



- DCRs improve Azure Monitor data collection with scalable, configurable, and centralized management.
- DCRs replace legacy methods like Log Analytics agent and Data Collector API.
- Edge pipeline enables scalable, offline data collection for environments with connectivity challenges.

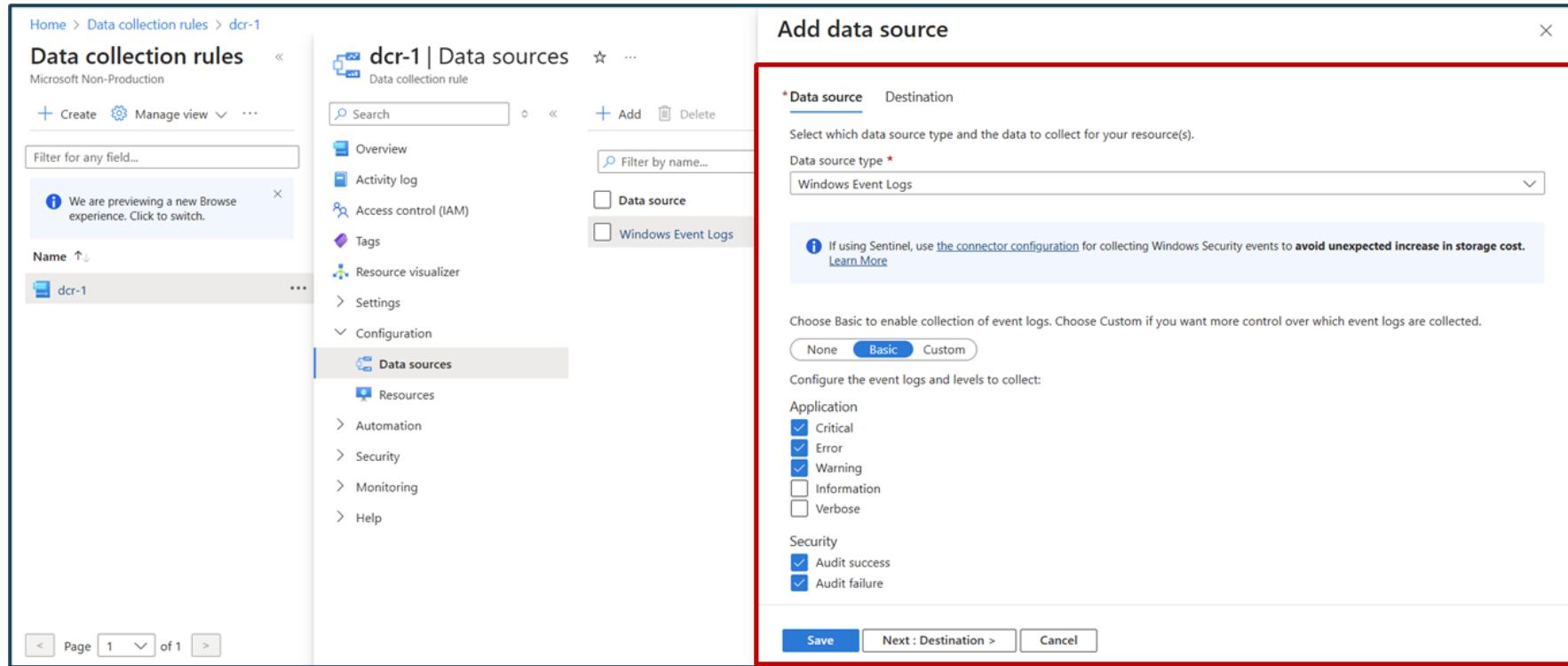
# Transformations in Data collection rules (DCRs)



Filter records and columns  
Add calculated columns  
Format data for destination  
Hide sensitive data

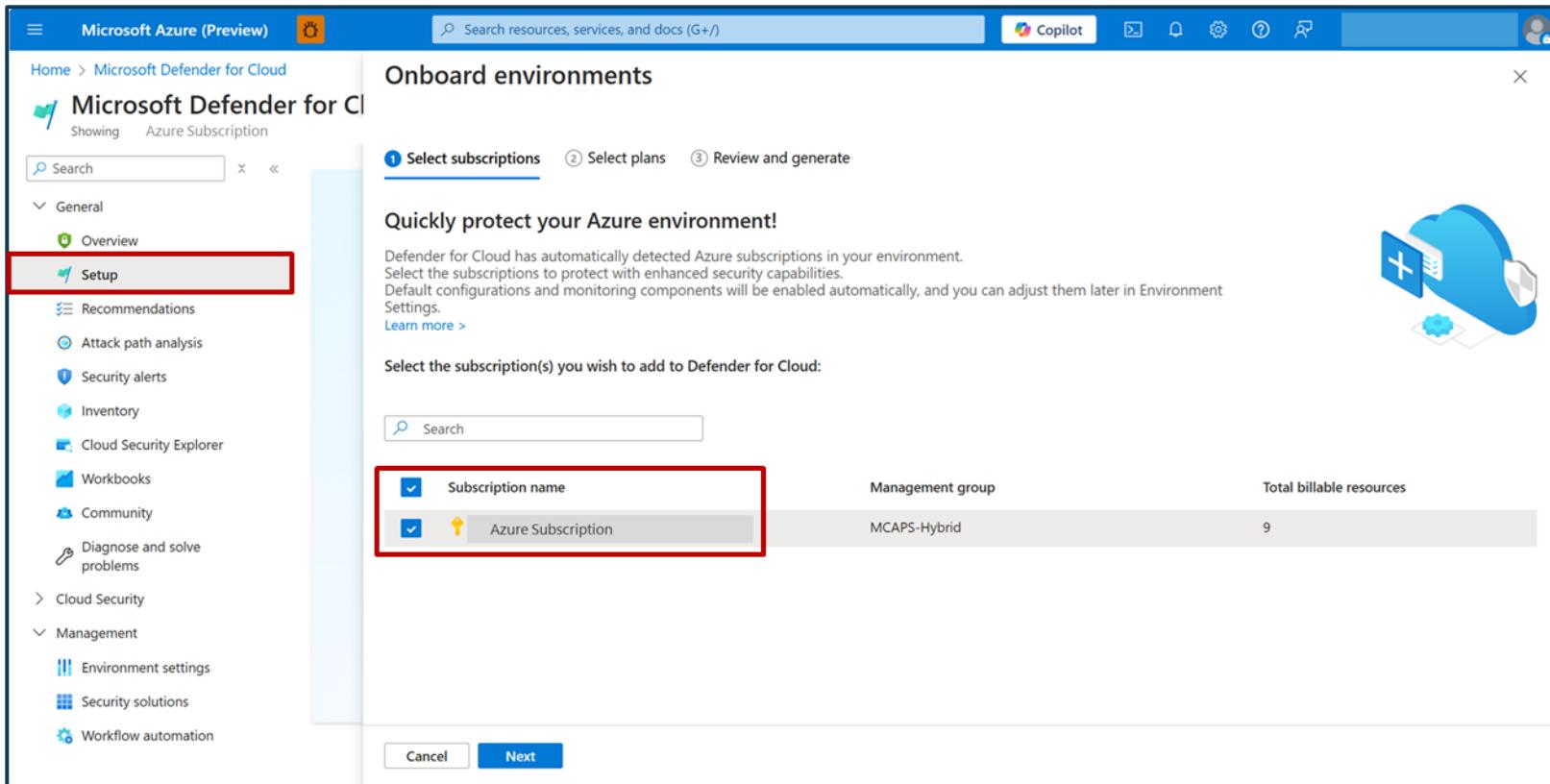
- Modify incoming data before storage or forwarding in Azure Monitor.
- Filter, remove sensitive data, or format data to match destination schema.
- Enable advanced scenarios like multi-destination routing and data enrichment.

# Monitor network security events and performance data by configuring data collection rules (DCRs) in Azure Monitor



- Data Collection and Management: Use Azure Monitor Agent with Data Collection Rules (DCR) for data collection and destinations.
- Configuration and Control: Define data sources, enforce security, and manage resources using Azure tools.
- Verification and Monitoring: Validate agent functionality and data flow using Log Analytics workspace queries.

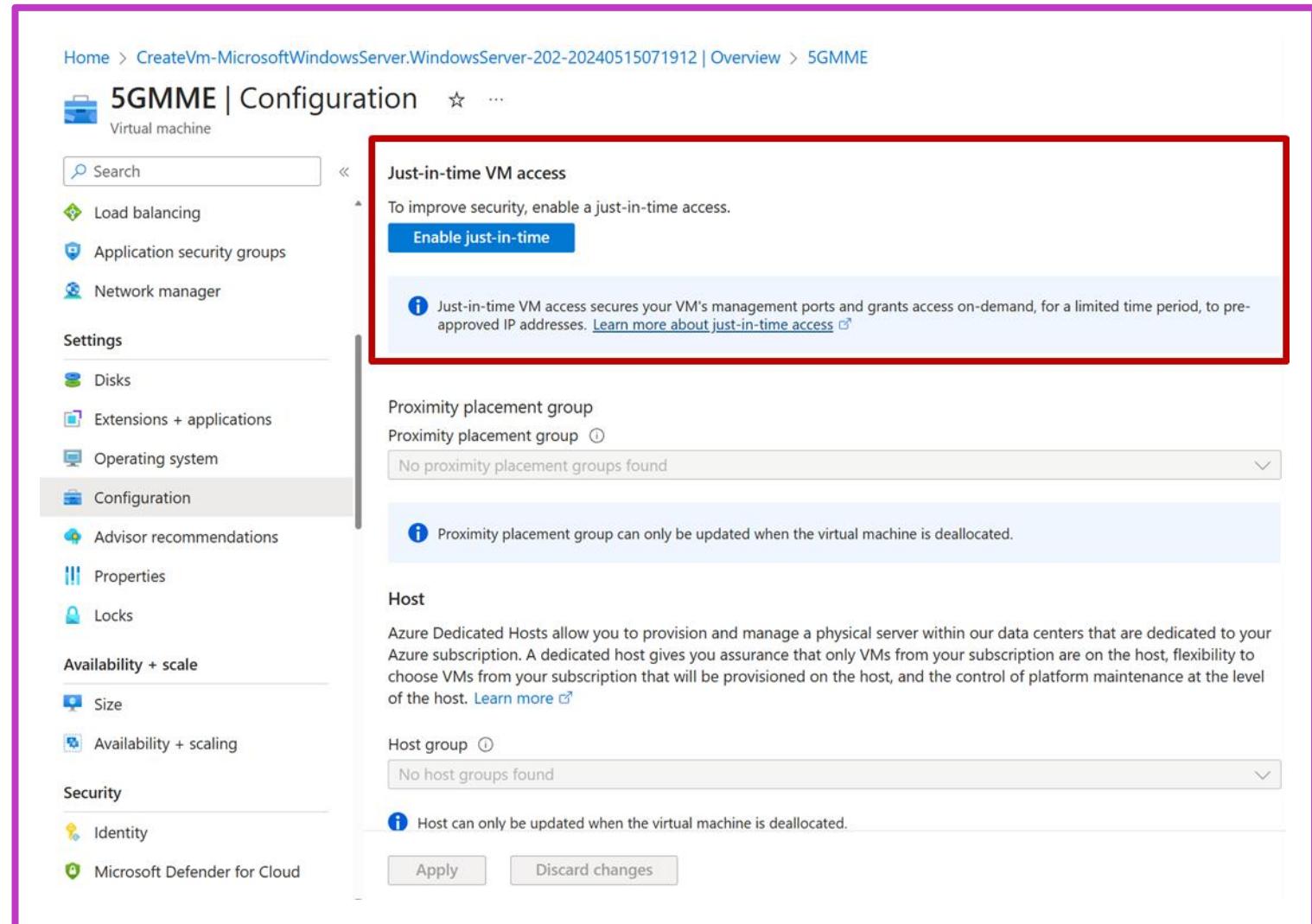
# Connect your Azure subscriptions



- Comprehensive protection: Combines DevSecOps, CSPM, and CWPP to secure cloud apps and workloads.
- Free foundational features: Includes Secure Score, asset inventory, and compliance tools with optional paid plans.
- Streamlined threat management: Detect vulnerabilities, block threats, and respond quickly with integrated analytics.

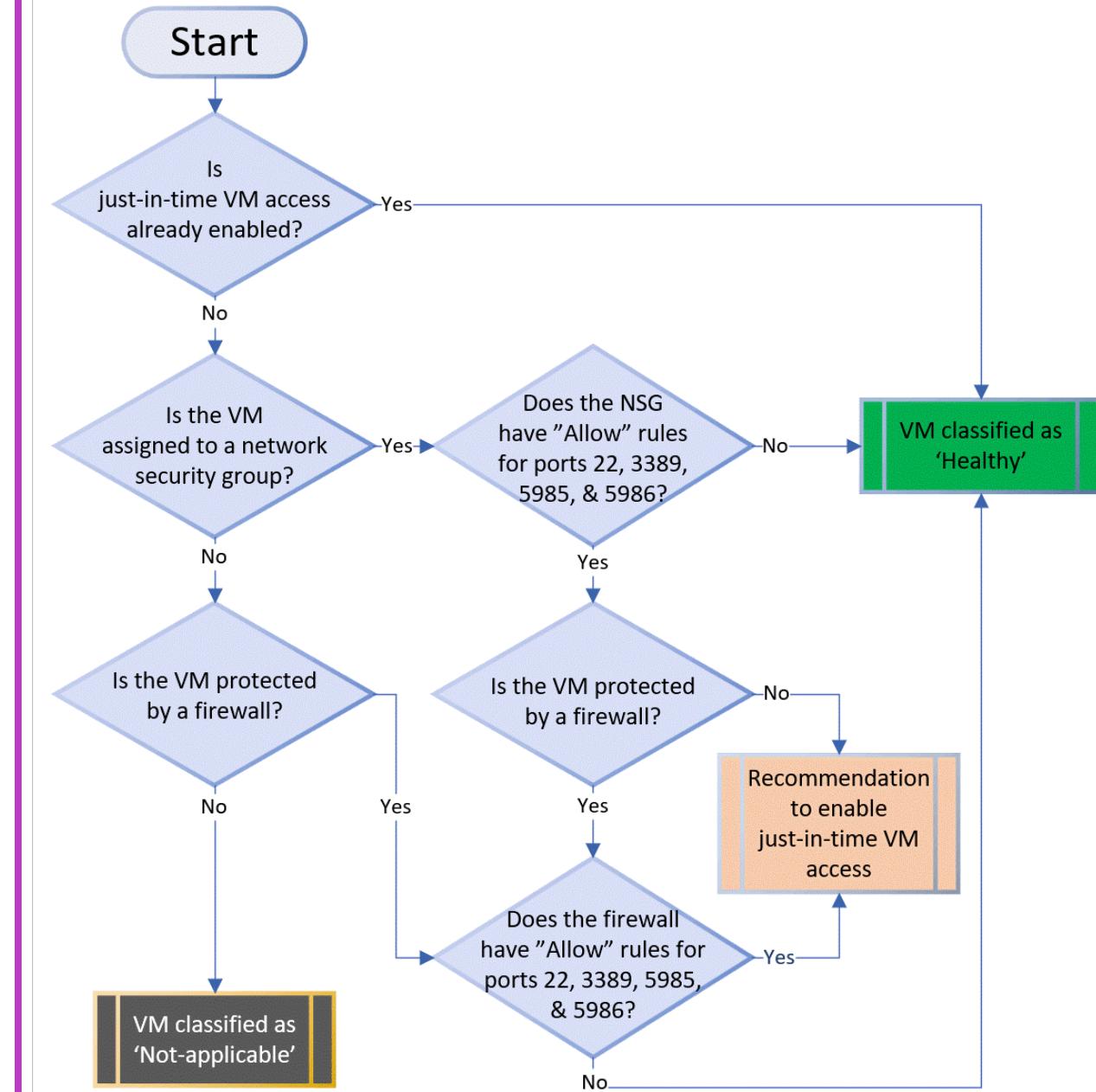
# Understanding just-in-time VM access

- Open management ports on VMs are targets for attacks; successful breaches can lead to further resource compromises.
- JIT VM access in Defender for Cloud reduces attack surfaces by limiting open ports while allowing legitimate access when needed.
- JIT manages inbound traffic on Azure and AWS, ensuring security rules are prioritized and access is controlled and temporary.



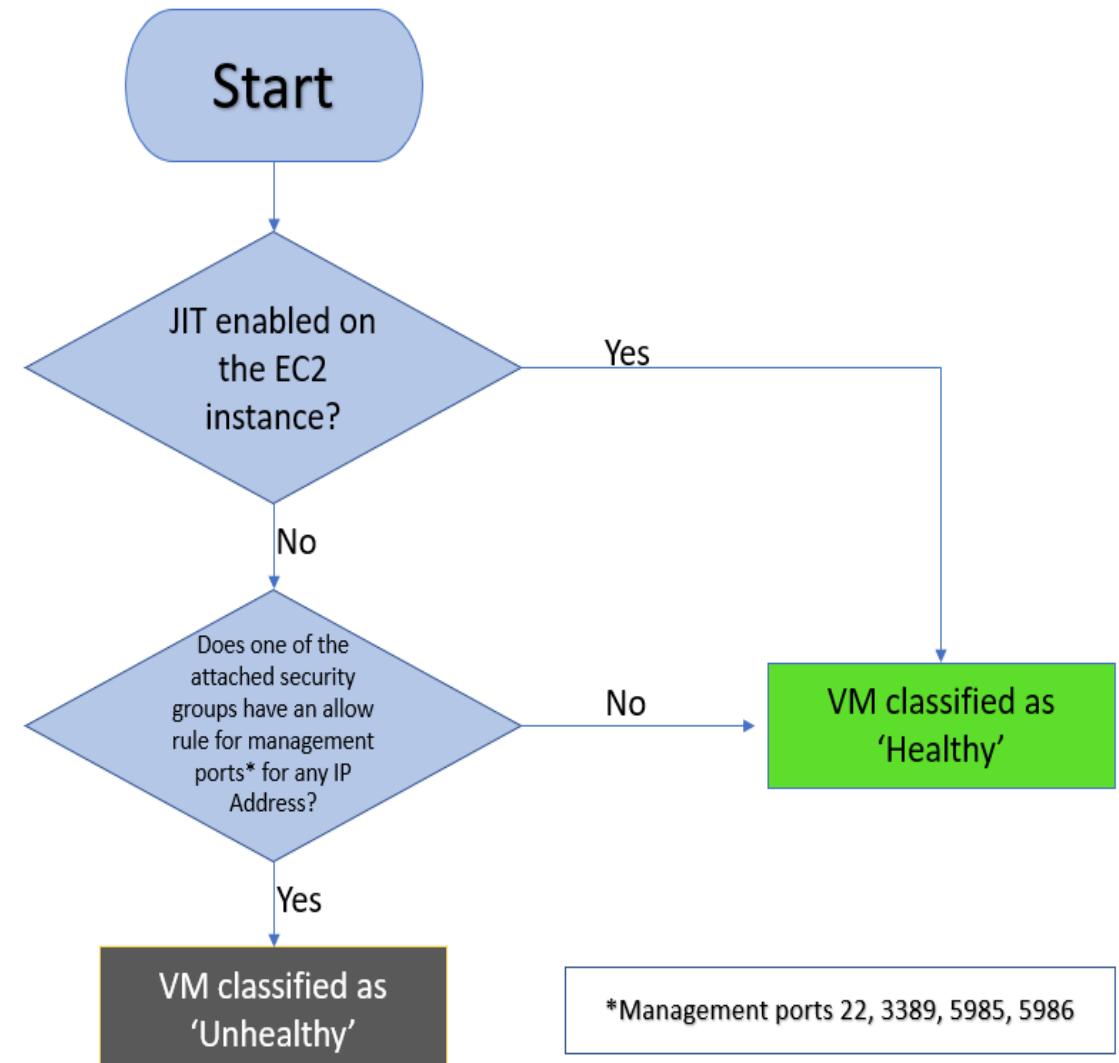
# Just-in-time VM is enabled an Azure Virtual Machine

**Example:** Azure Virtual Machine



# Just-in-time VM is enabled on the AWS EC2 Instance

**Example:** AWC EC2 Instance



# Added to the recommendation's Unhealthy resources tab

When Defender for Cloud finds a machine that can benefit from JIT, it adds that machine to the recommendation's Unhealthy resources tab.

**Example: Affected resources**

Dashboard > Microsoft Defender for Cloud | Recommendations >

Management ports of virtual machines should be protected with just-in-time network access control

^ Description  
Microsoft Defender for Cloud has identified some overly-permissive inbound rules for management ports in your Network Security Group. Enable just-in-time access control to protect your VM from internet-based brute-force attacks. [Learn more](#).

▼ Remediation steps

^ Affected resources

Unhealthy resources (78)    Healthy resources (112)    Not applicable resources (66)

conto

Name	Subscription
ContosoWeb2	Contoso IT - demo
ContosoWeb1	Contoso IT - demo
ContosoSQLSvr3	Contoso IT - demo
ContosoSQLSvr3	Contoso IT - demo
ContosoSQLSrv2	Contoso IT - demo

# Enable just-in-time access on VMs

- Protect Azure VMs from unauthorized access using JIT in Defender for Cloud.
- Enable and manage JIT via Defender for Cloud, Azure portal, PowerShell, or REST API.
- Prerequisites: Microsoft Defender for Servers Plan 2, Reader/Security Reader roles.

The screenshot shows the 'Just-in-time VM access' page in the Microsoft Defender for Cloud interface. At the top, there's a navigation bar with 'Home > Microsoft Defender for Cloud | Workload protections >'. Below it is a header 'Just-in-time VM access' with a refresh icon and three dots. A status message 'Last week' is displayed. A purple banner at the top indicates that some subscriptions don't have full protections enabled, with a link to upgrade. Two collapsed sections are shown: 'What is just-in-time VM access?' and 'How does it work?'. The main section is titled 'Virtual machines' and includes tabs for 'Configured' (which is selected), 'Not Configured', and 'Unsupported'. A note says 'VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.' Below this, it shows '1 VMs' and a table with one row. The table has columns: 'Virtual machine' (with a checkbox and a blue shield icon), 'Approved' (0 Requests), 'Last access' (N/A), 'Connection details' (blue shield icon), and 'Last user' (N/A). A 'Request access' button is located in the top right corner of the main content area.

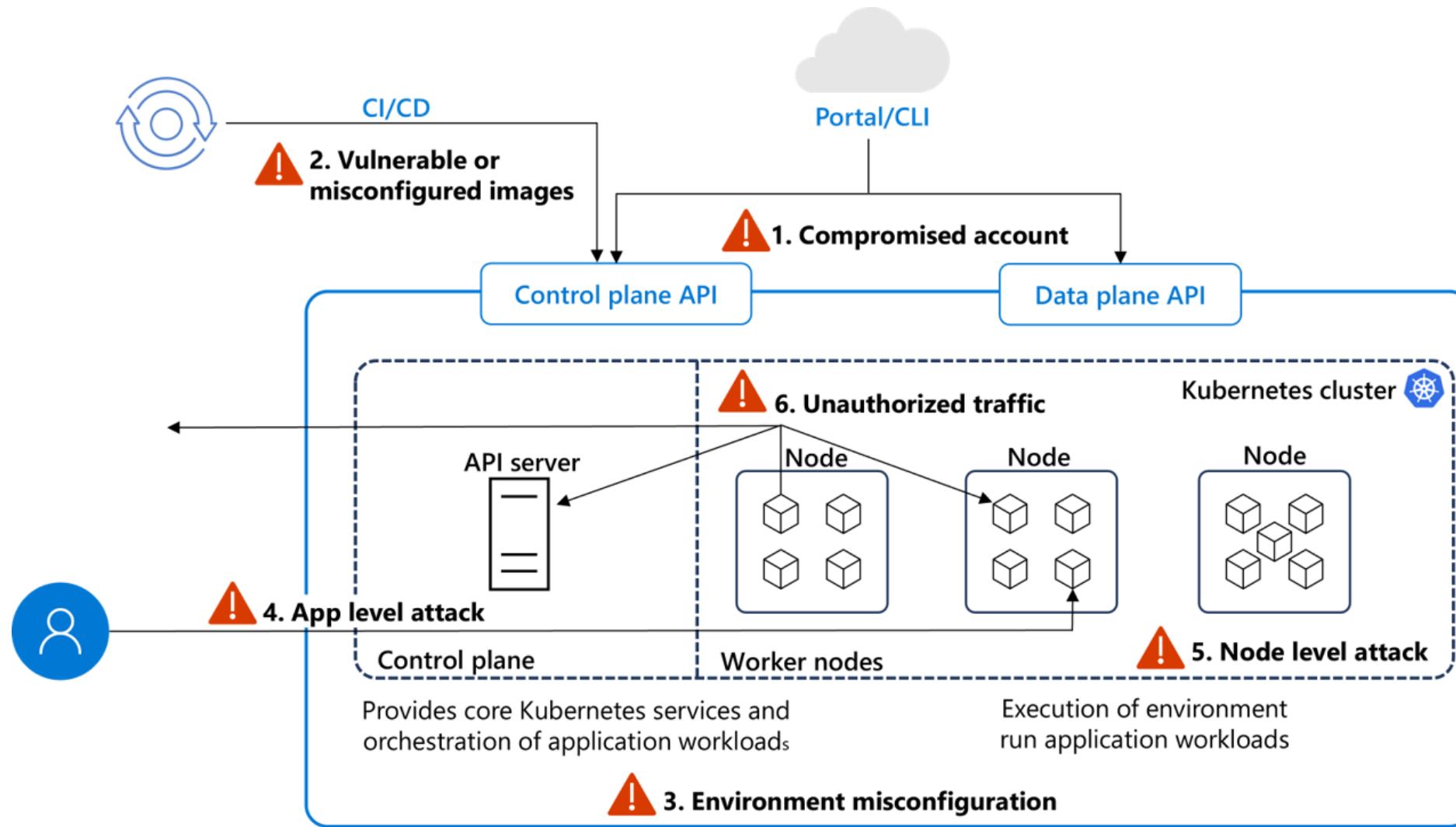
Virtual machine	Approved	Last access	Connection details	Last user
<input type="checkbox"/> romebuild	0 Requests	N/A		N/A

# Container security in Microsoft Defender for Containers

The screenshot shows the Microsoft Defender for Cloud Recommendations interface. On the left, a sidebar lists navigation options: General, Overview, Getting started, Recommendations (which is selected), Security alerts, Inventory, Workbooks, Community, Diagnose and solve problems, Cloud Security, Security posture, and Regulatory compliance. The main area displays a secure score of 44%, active items (15/15 controls, 216/287 recommendations), and resource health (2282 unhealthy, 1018 healthy, 532 not applicable). Below this, there's a search bar for recommendations and filters for recommendation status, severity, and resource type (the latter is highlighted with a red box). A progress bar at the bottom indicates a current score of 6.26 and a potential score increase of +7%.

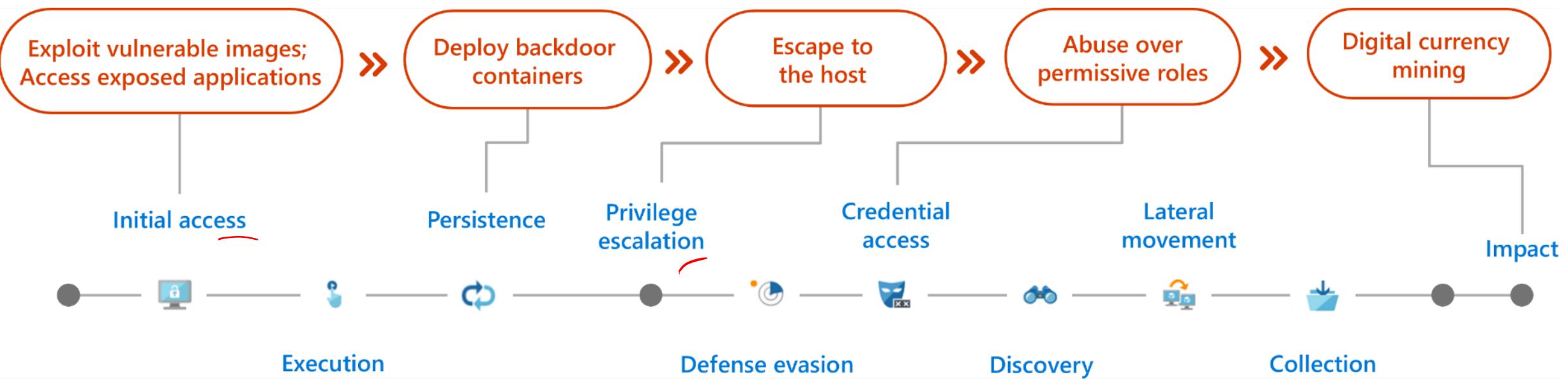
- Microsoft Defender for Containers: Cloud-native solution for container security across multicloud and on-premises environments.
- Four core domains: Security posture management, vulnerability assessment, run-time threat protection, deployment & monitoring.
- Features: Agentless capabilities, agent-based capabilities, vulnerability assessment, run-time protection with MITRE ATT&CK framework.

# Managed Kubernetes threat factors



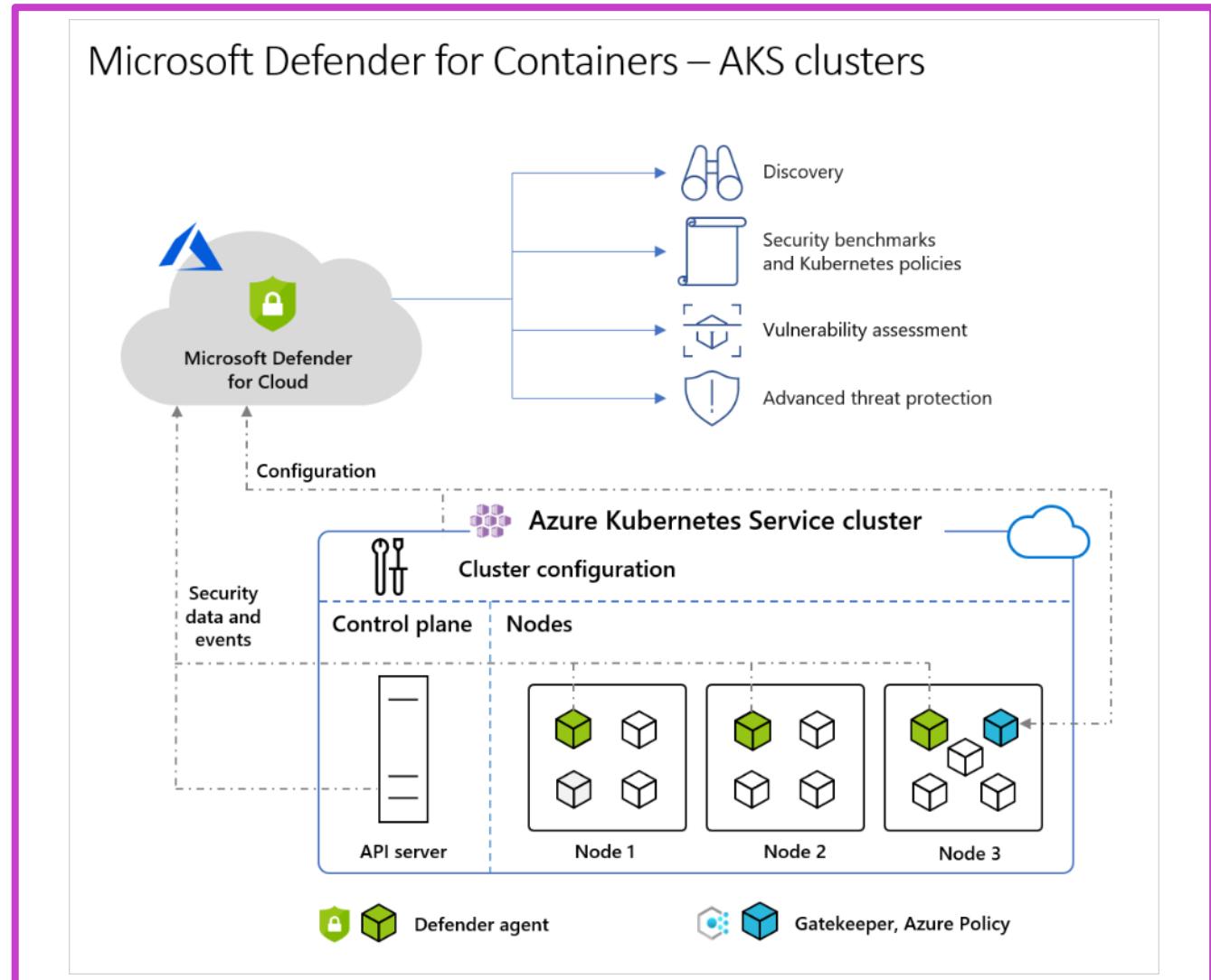
# Common attack techniques

MITRE Giver kill chain



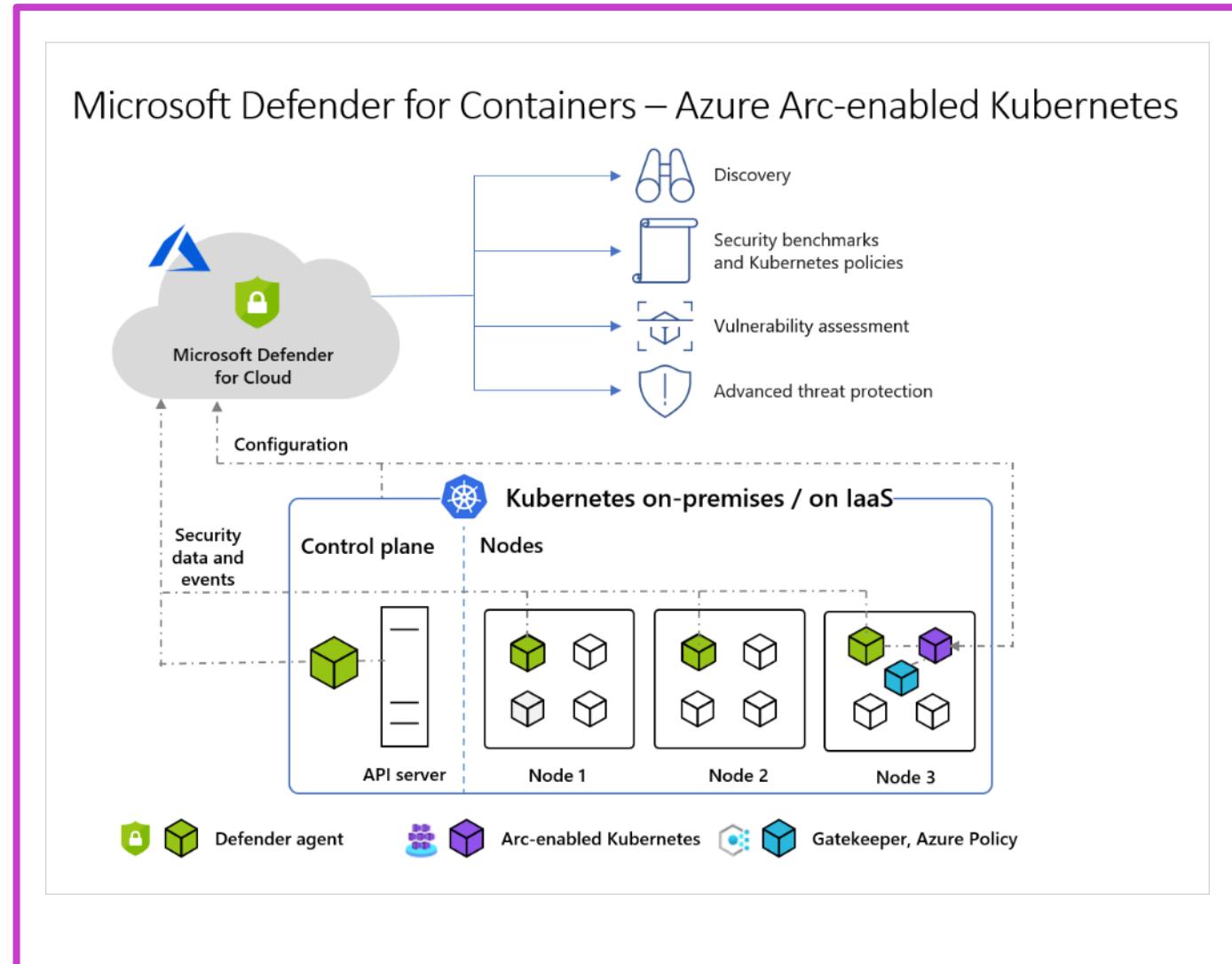
# Architecture diagram of Defender for Cloud and AKS clusters

- Agentless audit log collection in AKS; automatic, no extra cost or setup.
- Defender agent for runtime protection, Azure Policy for Kubernetes for enforcement.
- Agentless discovery creates, assigns roles, discovers, and binds to AKS clusters.



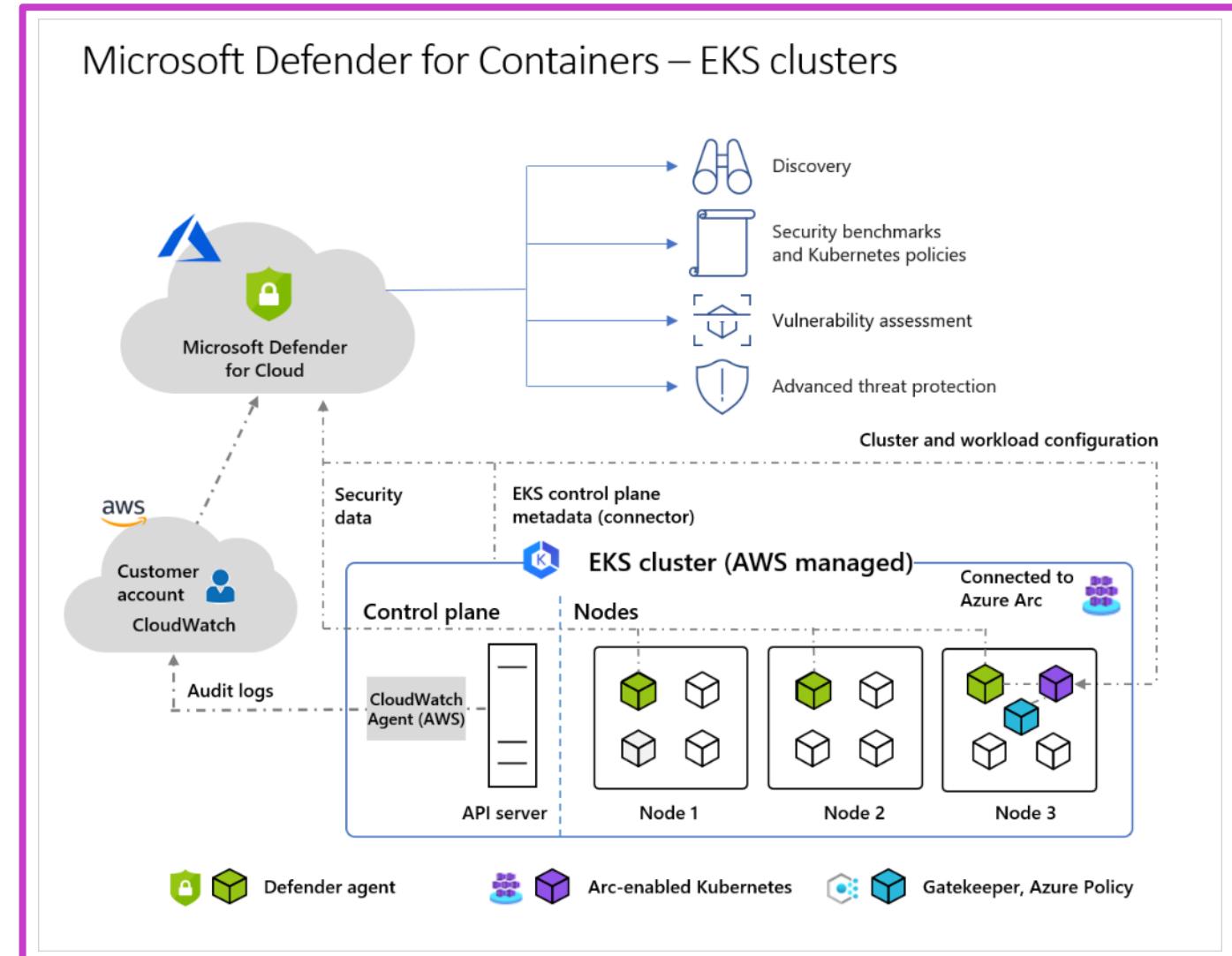
# Architecture diagram of Defender for Cloud and Arc-enabled Kubernetes clusters

- Azure Arc connects clusters to Defender for Cloud; requires one node installation.
- Defender agent provides runtime protection, collects signals and audit logs as Arc extension.
- Azure Policy for Kubernetes enforces policies centrally as an Arc-enabled extension, one node required.



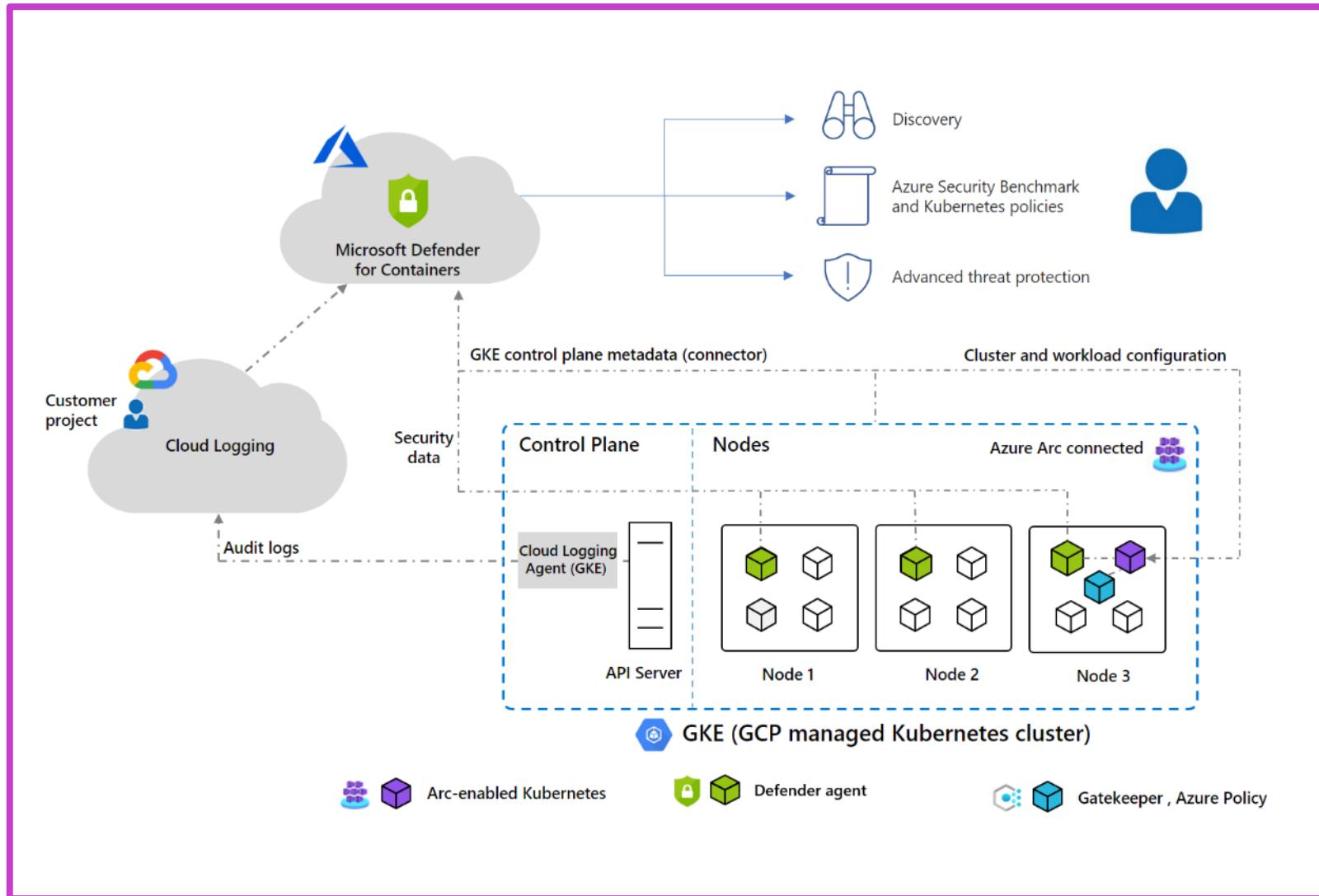
# Architecture diagram of Defender for Cloud and EKS clusters

- Defender for Cloud and EKS: Audit logs collected agentlessly, Arc-enabled Kubernetes with Defender agent, Azure Policy.
- AWS discovery snapshots: Role assignment, API-based cluster discovery by Defender for Cloud.
- Components include CloudWatch, Arc-enabled Kubernetes, Defender agent, and Azure Policy.



# Architecture diagram of Defender for Cloud and GKE clusters

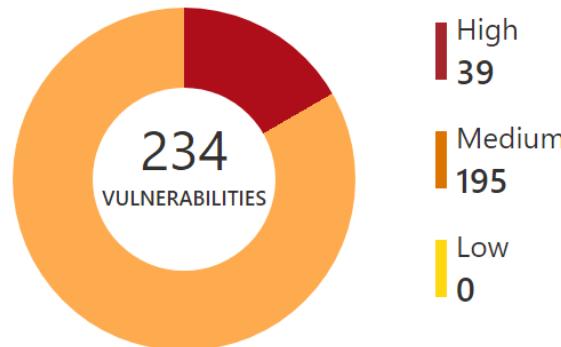
- Agentless audit log collection in GKE via GCP Cloud Logging.
- Azure Arc connects clusters to Defender for Cloud, enabling extensions.
- Extensions include Defender agent for runtime protection and Azure Policy for Kubernetes enforcement.



# Defender for Cloud DevOps Security

## Security Overview

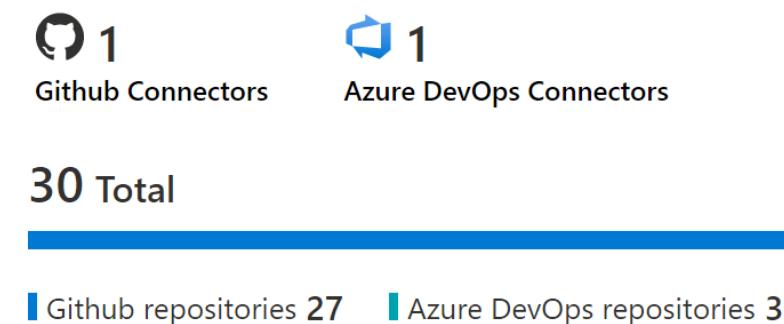
### DevOps security vulnerabilities ⓘ



### DevOps security results



### DevOps coverage



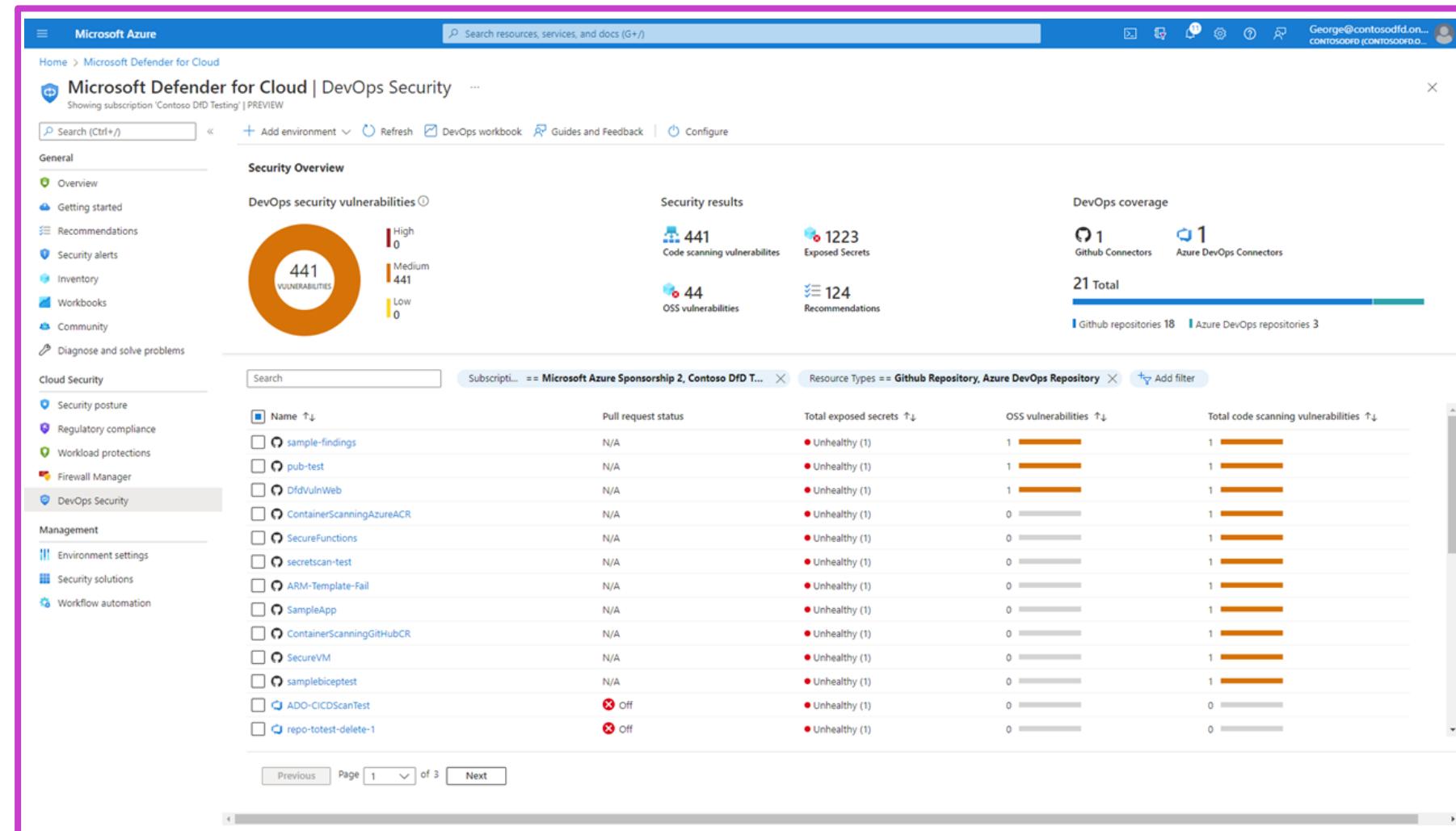
- Provides visibility, posture management, threat protection across Azure, AWS, GCP, on-premises.
- Centralizes DevOps security, integrates with Azure DevOps, GitHub, GitLab for application protection.
- Prioritizes code remediation with contextual insights, secures IaC templates, container images.

# Defender for Cloud DevOps Security required permissions

Feature	Permissions
Connect DevOps environments to Defender for Cloud	<ul style="list-style-type: none"><li>• Azure: Subscription Contributor or Security Admin</li><li>• Azure DevOps: Project Collection Administrator on target Organization</li><li>• GitHub: Organization Owner</li><li>• GitLab: Group Owner on target Group</li></ul>
Review security insights and findings	Security Reader
Configure pull request annotations	Subscription Contributor or Owner
Install the Microsoft Security DevOps extension in Azure DevOps	Azure DevOps Project Collection Administrator
Install the Microsoft Security DevOps action in GitHub	GitHub Write

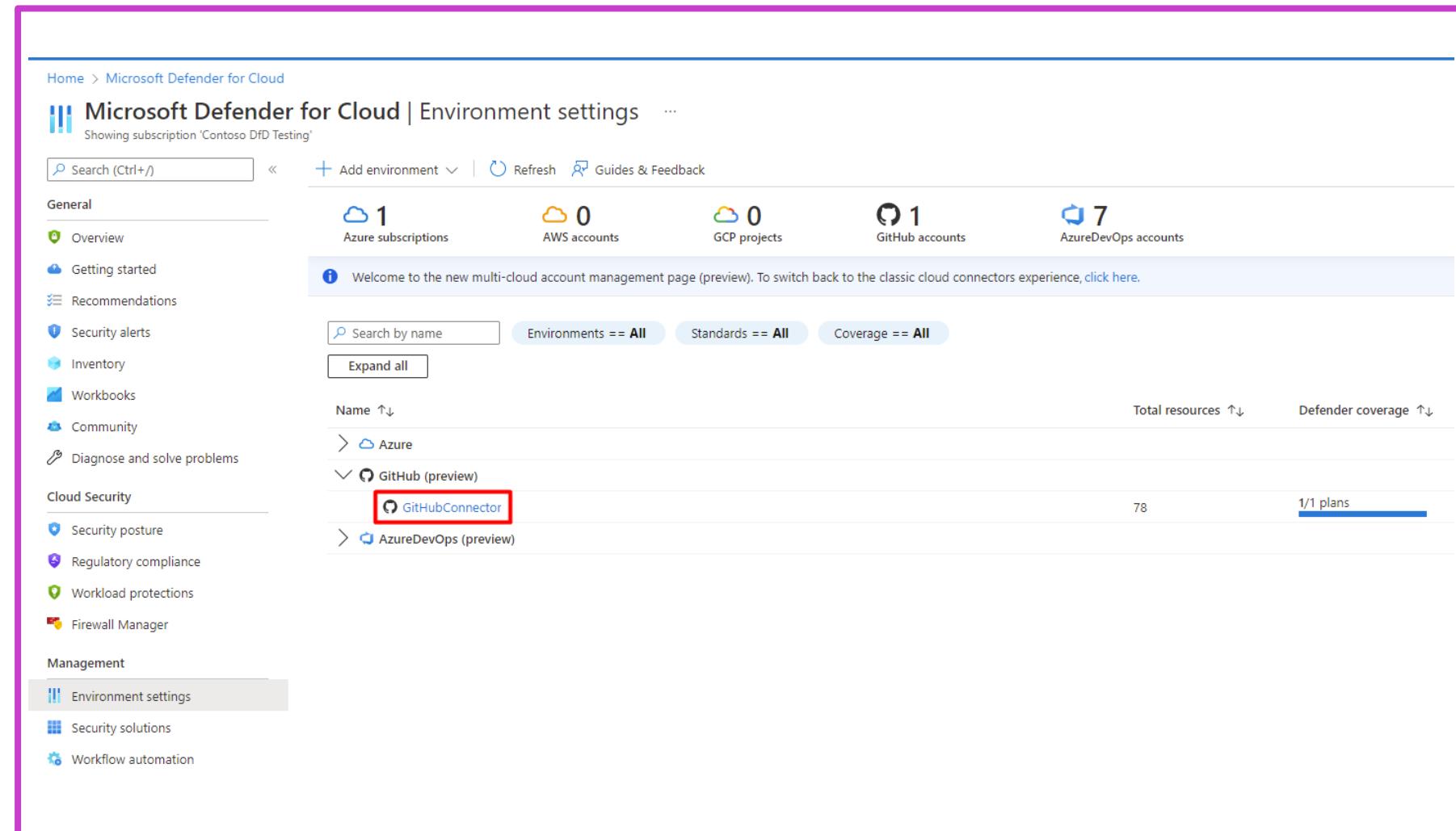
# DevOps environment security posture

- Enhances security across DevOps lifecycle, identifies risks in CI/CD pipelines and source code management.
- Uses scanners for Azure DevOps, GitHub; auto-scans every 24 hours for vulnerabilities, misconfigurations.
- Offers actionable recommendations to reduce attack surface, prioritize fixes, integrate real-time alerts for compliance.



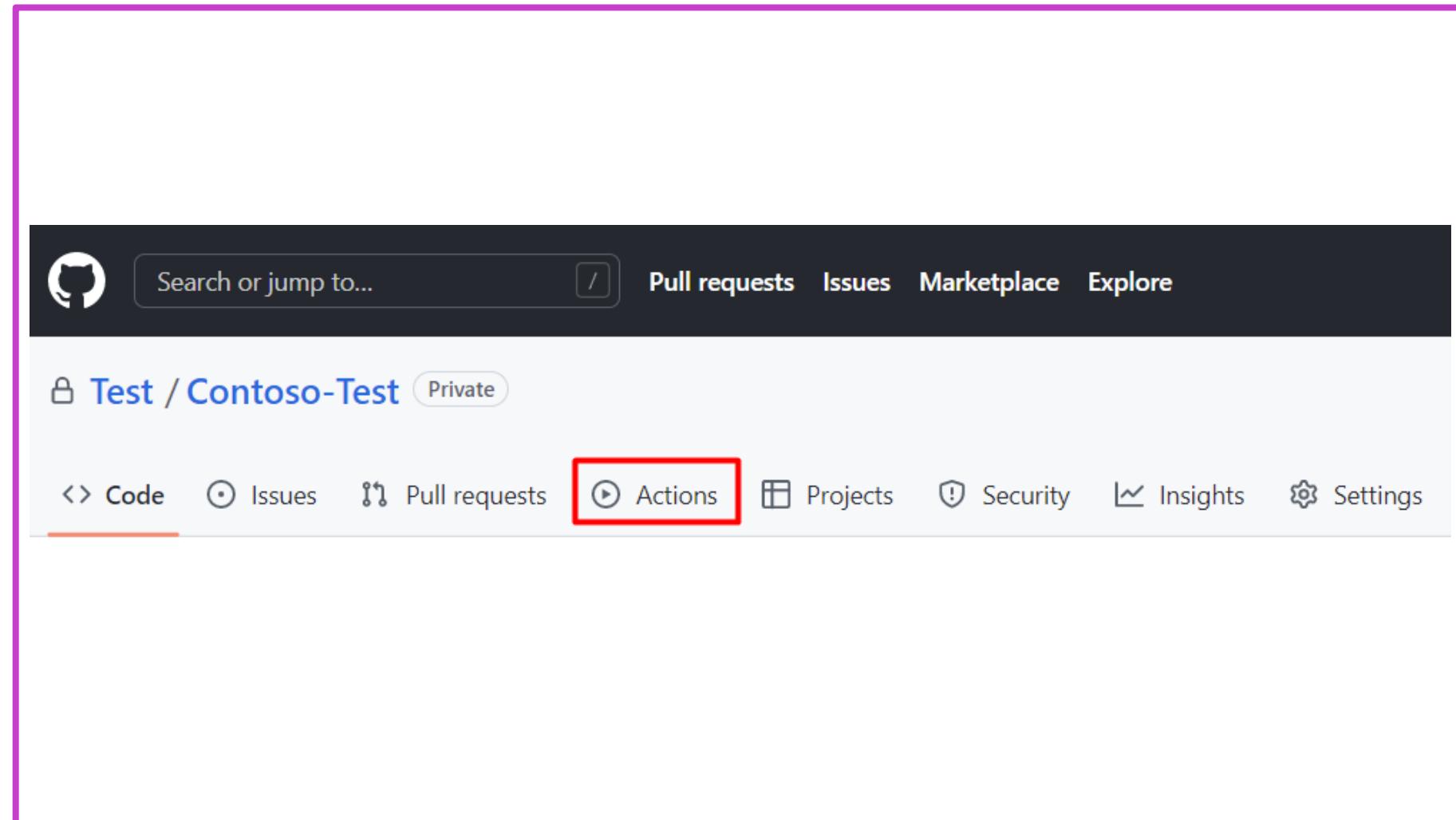
# Connect your GitHub Environment to Defender for Cloud

- Connect GitHub organizations in Defender for Cloud for autodiscovery and enhanced security.
- Extends security with CSPM features and contextualized risk assessments for GitHub resources.
- Requires Azure account, GitHub Enterprise with Advanced Security, and authorization steps.



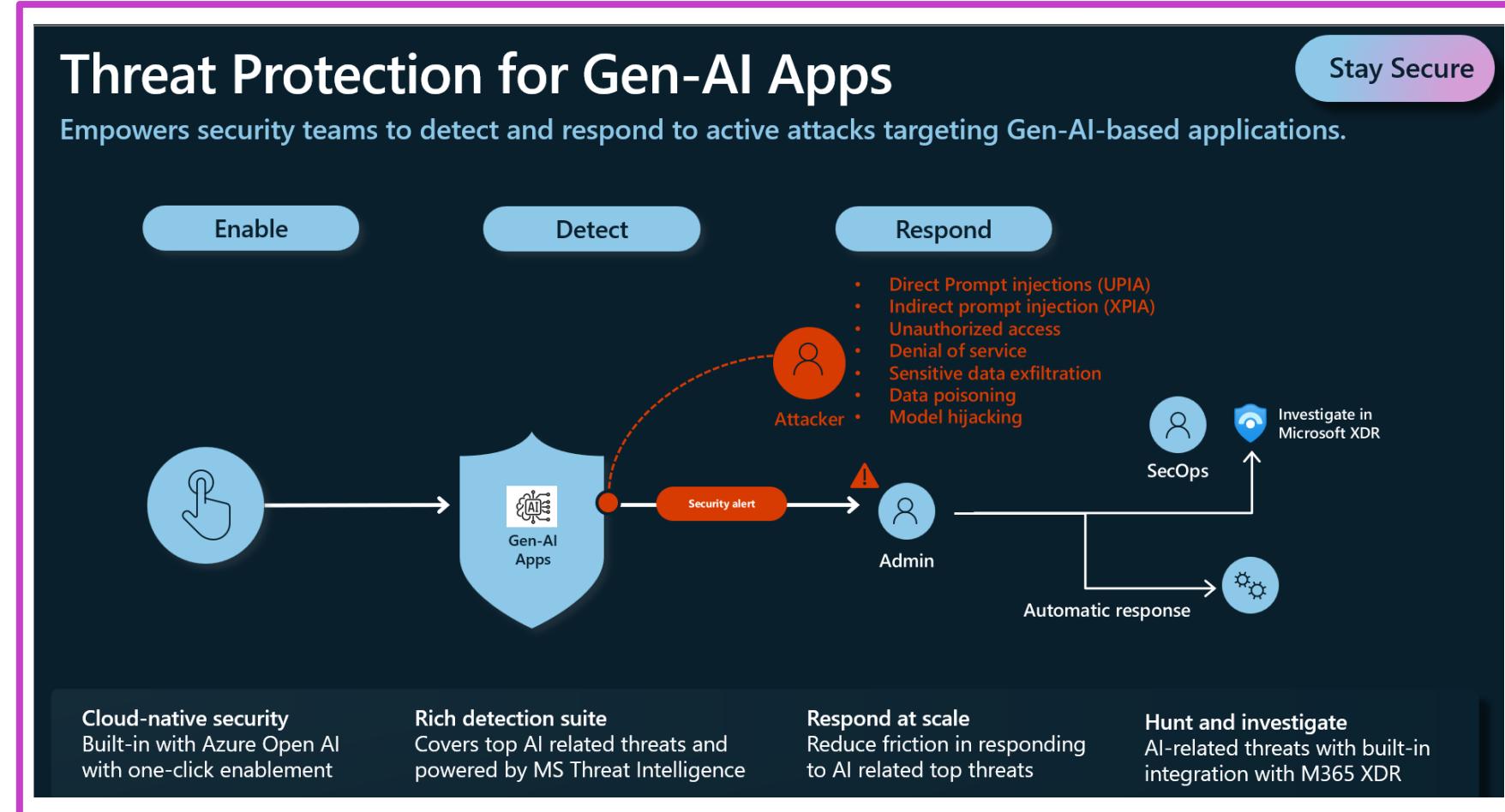
# Configure the Microsoft Security DevOps GitHub action

- Integrates static analysis tools into development with Security DevOps command line application.
- Requires Azure subscription, GitHub repositories connection, and GitHub Advanced Security setup.
- Set up GitHub action for workflow, commit, and view scan results in Defender for Cloud.



# Defender for Cloud AI threat protection

- Monitors generative AI threats in real time with Defender for Cloud.
- Integrates with Defender XDR and Azure AI Content Safety for alerts on data leakage, poisoning, jailbreak, and credential theft.
- Currently in preview; supports text tokens only with Azure OpenAI models and requires specific roles.



# Enable threat protection for AI workloads

- Monitors Azure AI workloads to detect vulnerabilities and threats such as data leakage and manipulation.
- Currently in preview; activate through Microsoft Defender for Cloud enabling AI workloads in Azure portal.
- Collects user prompt evidence from AI interactions, aiding alert triage and thorough incident investigation procedures.

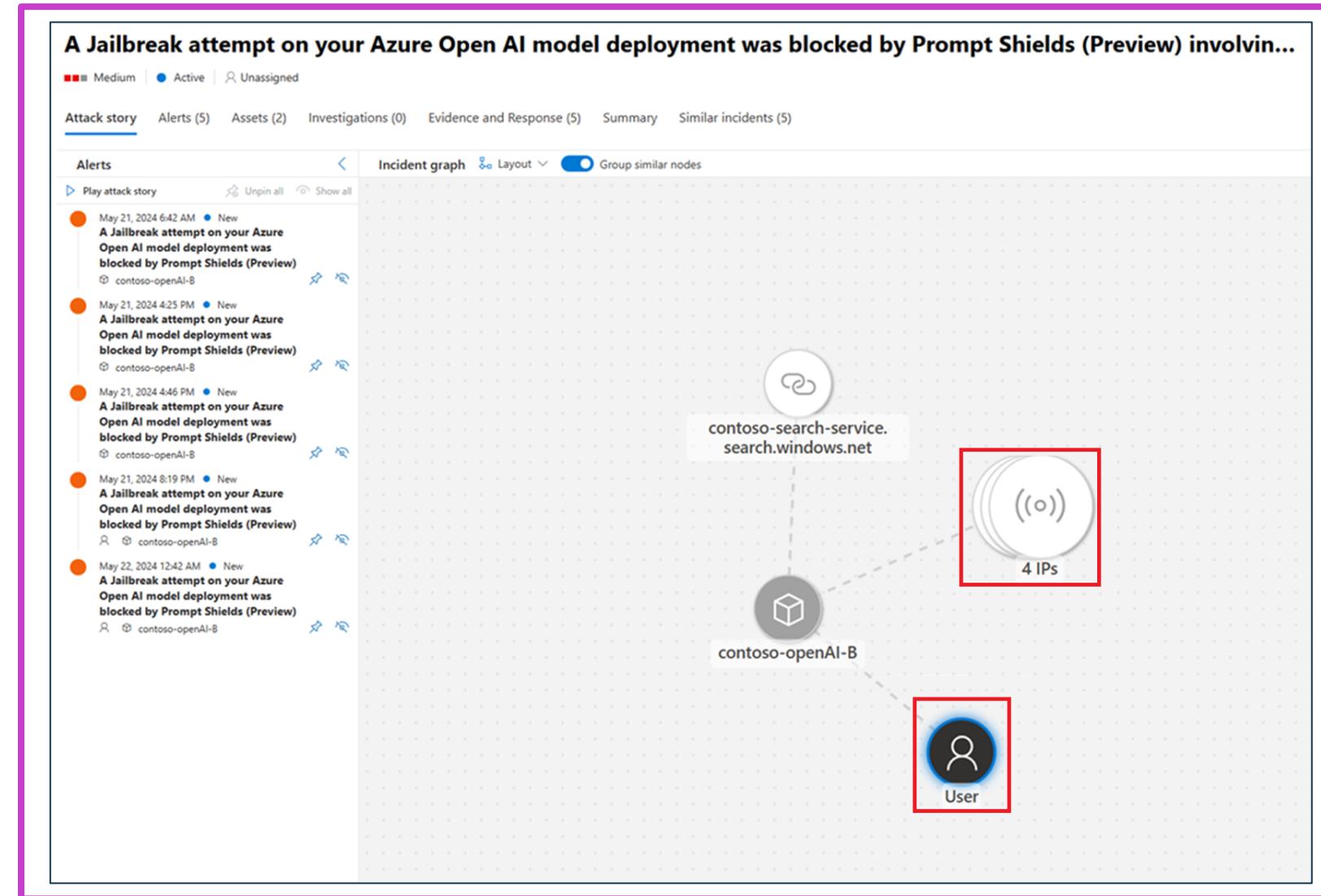
The screenshot shows the Microsoft Azure (Preview) portal with the URL [https://portal.azure.com/#blade/Microsoft\\_Azure\\_DefenderForCloud/EnvironmentSettingsBlade](#). The page is titled "Settings | Defender plans". On the left, there's a sidebar with "Settings" expanded, showing "Defender plans" selected. The main content area is titled "Cloud Workload Protection (CWP)". It says "Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments." Below this is a table with columns: Plan, Pricing\*, Resource quantity, Monitoring coverage, and Status. The rows represent different resource types:

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (/Server/Month)	201 servers	Full	Off → On
App Service	/Instance/Month	36 instances	Full	Off → On
Databases	Selected: 4/4 Action required	Protected: 17/17 instances	Partial	Off → On
Storage	/10K transactions	152 storage accounts	Full	Off → On
Containers	/VM core/Month	3 container registries; 60 kubernetes cores	Full	Off → On
Key Vault	/10k transactions	41 key vaults	Full	Off → On
Resource Manager	/1M API calls	4 Azure API Management services	Full	Off → On
APIs	Plan 1 (/1M API calls/Month)	4 Azure API Management services	Action required	Off → On
AI workloads	Details >		Full	Off → On

\* The price displayed represents the list price prior to any discounts or special offers being applied.  
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.  
\*\* Malware Scanning in Defender for Storage is not included for free in the first 30 days and will be charged from the first day in accordance with the pricing scheme.  
For more information on Defender for Cloud pricing, visit the [pricing page](#).

# Gain application and end-user context for AI alerts

- Enhances AI alerts with end-user and application context for better incident correlation.
- Enables blocking and prioritizing using IP, identity, and application details.
- Improves triage and investigation by adding user security parameters.



# Additional Study – Configure and manage threat protection by using Microsoft Defender for Cloud

Microsoft  
Learn Modules  
([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))



## Module Review Questions

- Enable Workload Protection Services: Activate threat protection for workloads using Microsoft Defender for Cloud.
- Configure Threat Protection for Servers, Databases, and Storage: Set up Microsoft Defender for Servers, Databases, and Storage for enhanced security monitoring.
- Implement Agentless Scanning for Virtual Machines: Enable agentless vulnerability scanning for Azure VMs using Microsoft Defender for Servers.
- Use Microsoft Defender Vulnerability Management: Manage and remediate vulnerabilities for Azure VMs with Microsoft Defender.
- Integrate DevOps Security Tools: Connect and configure GitHub, Azure DevOps, and GitLab with Microsoft Defender for Cloud DevOps Security.

Microsoft Sentinel

SIEM  
SOAR

SPLUNK

Configure and manage security  
monitoring and automation  
solutions

# Manage and respond to security alerts in Microsoft Defender for Cloud

## Manage security alerts

- From Defender for Cloud's overview, choose "**Security alerts**."
- Use and add filters to refine alert display.

## Respond to security alerts

- Choose an alert and click "**View full details**."
- Investigate and mitigate threats using "Alert details" and "Take action" tabs.

The screenshot illustrates the Microsoft Defender for Cloud interface for managing and responding to security alerts.

**Left Panel: Manage security alerts**

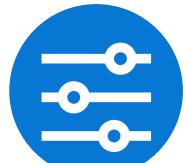
This section shows a list of security alerts with columns for Resource, Activity start time (UTC+2), and MITRE ATT&CK® tactics. A modal dialog titled "Add filter" is open over the list, allowing users to refine their search by Alert name, Affected resource, Resource type, Tags, Creator, Owner, and environment.

**Right Panel: Respond to security alerts**

This section shows a detailed view of a specific security alert titled "Potential SQL Injection". The alert is categorized as High Severity, Active, and occurred on 06/11/20, 1... Activity time. The alert description states: "Potential SQL injection was detected on your database Demo on server R-DEV\SQLEXPRESS". The affected resource is listed as "R-DEV Azure Arc machine Env: Development" and "DS-ThreatDetection\_Demo Subscription". The intent is identified as "Pre-attack". The "Alert details" tab is selected, showing client information like IP Address (127.0.0.1) and Oms Workspace ID (61d507e7). The "Take action" tab is also present. The alert is detected by Microsoft, and the vulnerable statement is shown as: "SELECT \* FROM sqli\_users WHERE ...".

# Configure workflow automation by using Microsoft Defender for Cloud

To configure workflow automation, you can:



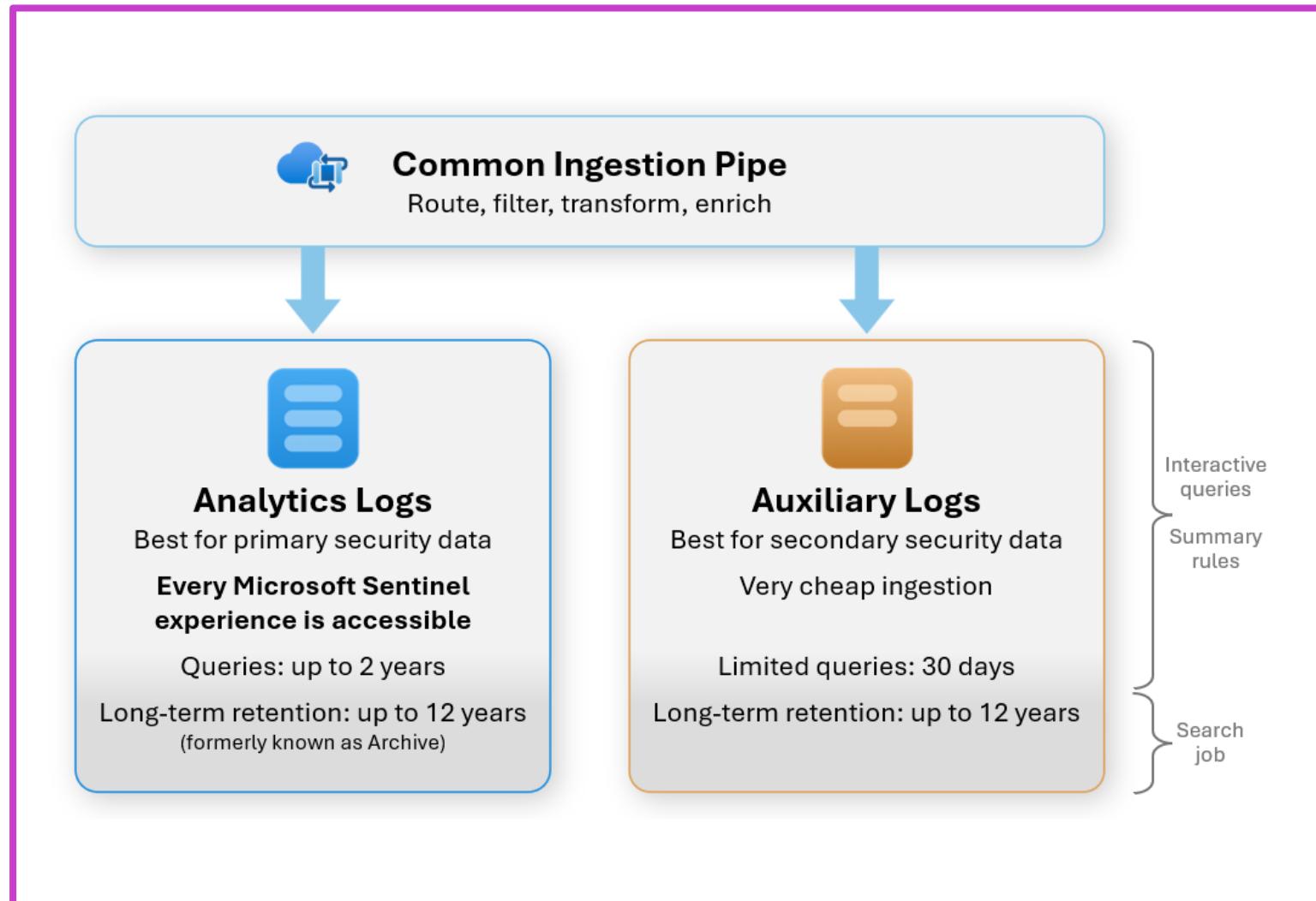
- Initiate a logic app in Defender for Cloud via **"Workflow automation."**
- Create, enable, or modify automation rules therein.
- Define a new workflow using **"Add workflow automation"** for details and triggers.
- Configure the Logic App through the **"Actions"** section.



- Implement large-scale workflow automation with provided policies.
- Use policy for Defender for Cloud alerts automation.
- Employ policy for Defender for Cloud recommendations automation.
- Utilize policy for Defender for Cloud regulatory compliance automation.

# Log retention plans in Microsoft Sentinel

- Log Collection Balance: Maximize security coverage while minimizing ingestion and retention costs with strategic planning.
- Data Categories: Classify logs into primary (critical) and secondary (contextual) for effective storage and accessibility.
- Retention Plans: Use Analytics, Auxiliary, or Basic plans for tailored performance and long-term retention needs.



# Understand how to use Query Builder for Kusto Query Language (KQL) in Sentinel

- Learn to filter, sort, and summarize log data using intuitive query steps.
- Use operators like project, extend, join, and summarize for deep data insights.
- Simplify complex queries with evaluate, let, and reusable expressions for better performance.

The screenshot shows the Microsoft Sentinel interface with a highlighted query in the 'Logs' section. A red oval highlights the KQL code in the 'New Query 1\*' pane:

```
1 Usage
2 | where QuantityUnit == 'MBytes'
3 | extend KBytes = Quantity * 1024
4 | project DataType, MBytes=Quantity, KBytes
```

The results pane below shows a table with three columns: 'DataType', 'MBytes', and 'KBytes'. The data includes various log types and their corresponding byte counts. A red arrow points from the 'KBytes' column header in the table back to the 'KBytes' part of the query code.

DataType	MBytes	KBytes
> DataverseActivity	0.003042	3.115008
> EmailAttachmentInfo	0.000927	0.949248
> ABAP_AGR_1251_CL	35.99145	36855.2448
> ABAP_USR05_CL	0.00049	0.50176
> ABAPSpoolLog_CL	0.000836	0.856064
> ABAP_AGR_PROF_CL	0.505803	517.942272
> ContainerRegistryRepositoryEvents	0.000936	0.958464
> IntuneDeviceComplianceOrg	0.040621	41.595904
> ABAP_AGR_USERS_CL	0.00031	0.31744
> SecurityIncident	0.001053	1.078272

# Configure data connectors in Microsoft Sentinel



## Enable a data connector

- Select the connector and then select the **Open connector** page.
- Refer to the connector page to understand how to ingest the data.
- Review a summary of the data and the connectivity status.
- Go to the **Next steps** tab for more content for the specific data type.



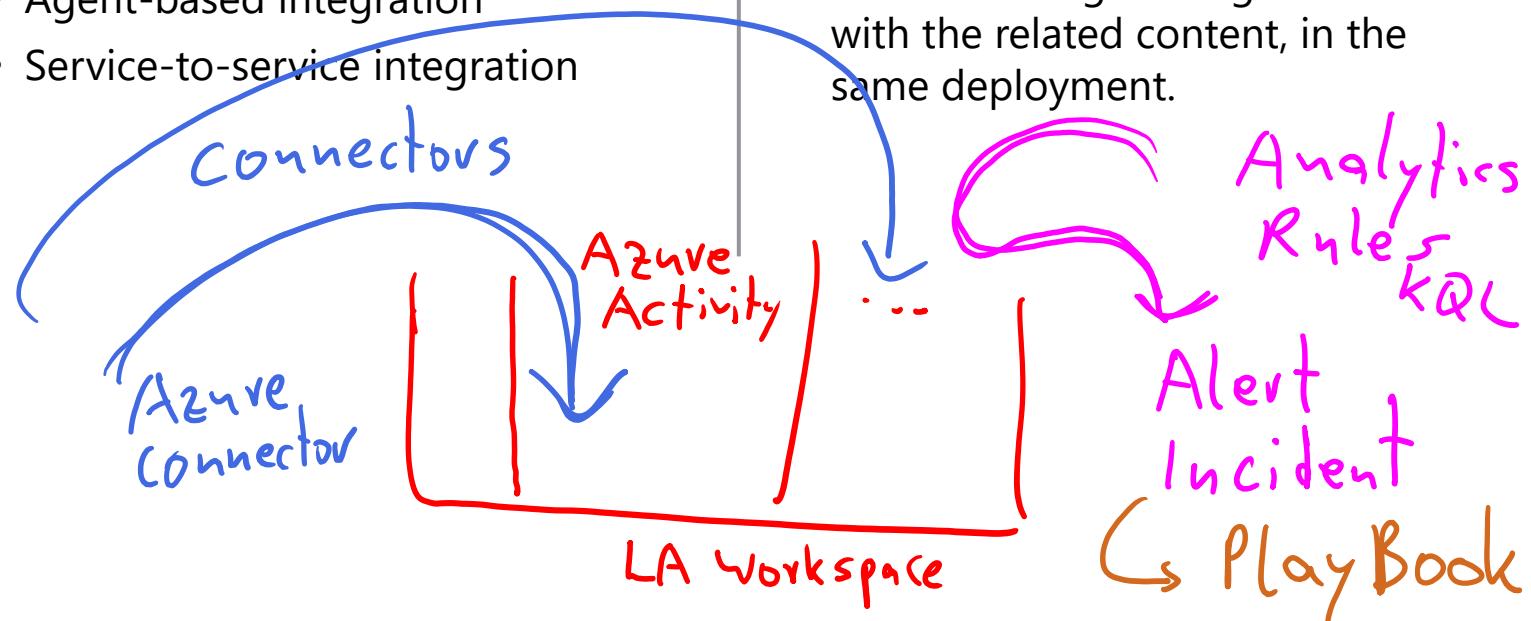
## Remember integrations for data connectors

- REST API integration
- Agent-based integration
- Service-to-service integration



## Deploy data connectors as part of a solution

Deploy a solution with a data connector to get it together with the related content, in the same deployment.



# Alerts and Incidents from Microsoft Sentinel

- Microsoft Sentinel Analytics Rules: Detect threats with scheduled, NRT, anomaly, and machine learning rules.
- Rule Management: Use templates for quick setup or customize rules via Kusto queries.
- Integration & Access: Supports cross-tenant scenarios, ARM templates, and Microsoft Defender integration.



# Enable analytics rules in Microsoft Sentinel

## Create a custom analytics rule with a scheduled query

- From the Microsoft Sentinel navigation menu, select **Analytics**.
- Select **+Create** and select **Scheduled query rule**.
- Configure the settings in the Analytics rule wizard's **General** tab.

## Define the rule query logic and configure settings

- Configure settings such as **Rule query**, **Alert enrichment**, **Query scheduling**, **Alert threshold**, and **Event grouping**.

## Configure the incident creation settings

- Choose whether and how Microsoft Sentinel turns alerts into actionable incidents using **Incident settings** and **Alert grouping** sections.

## Set automated responses and create the rule

- Set automation based on the alert generated by this analytics rule or on the incident created by the alerts.
- Review and create the rule.

Home > Microsoft Sentinel >

### Analytics rule wizard - Create new rule

**General** Set rule logic Incident settings (Preview) Automated response Review and create

Create an analytics rule that will run on your data to detect threats.

**Analytics rule details**

Name **\***

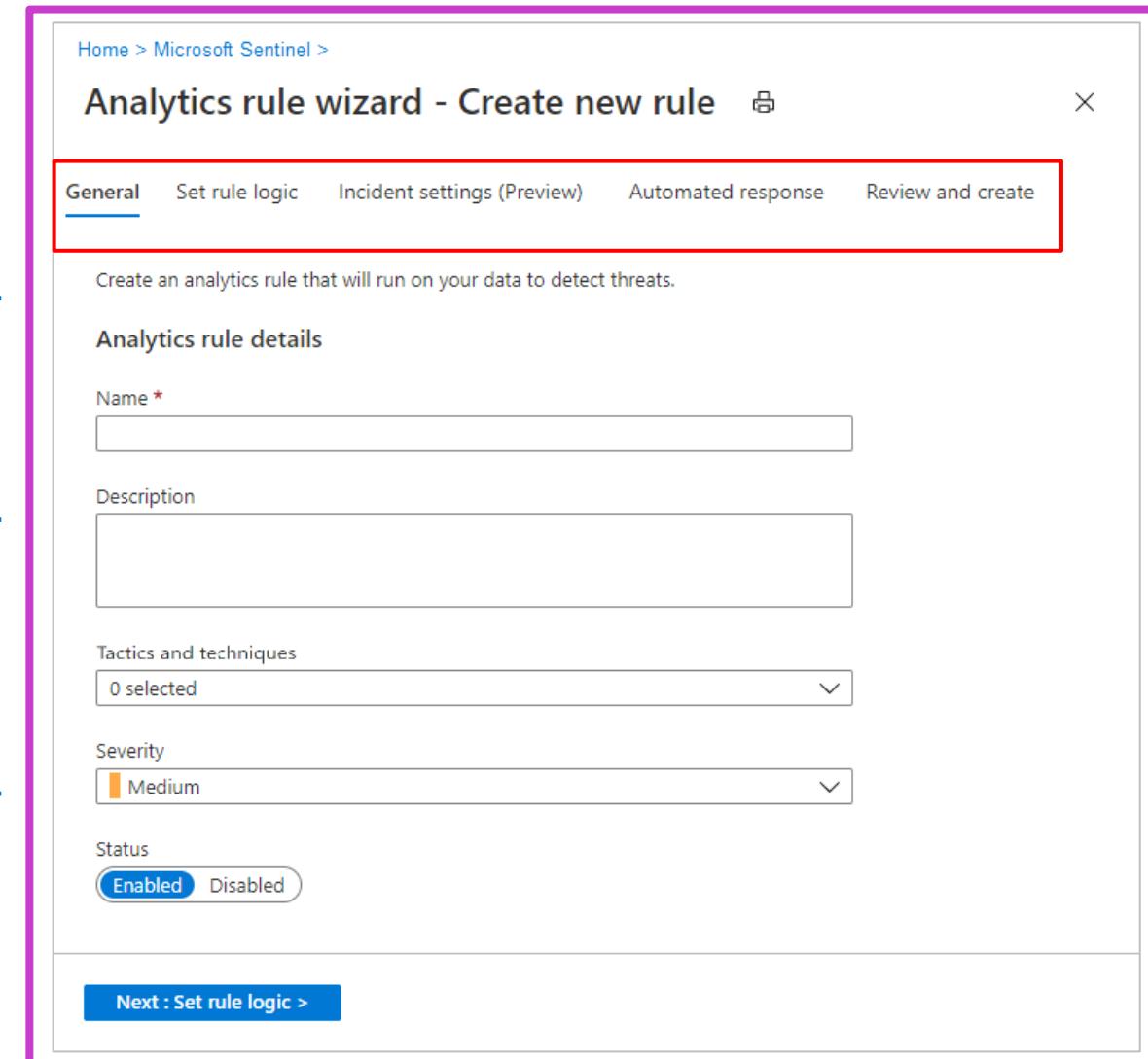
Description

Tactics and techniques

Severity

Status  Enabled  Disabled

**Next : Set rule logic >**



# Configure automation in Microsoft Sentinel

## Configure automation rules

By configuring automation rules, you can:

- Centrally manage the automation of incident handling
- Assign playbooks to incidents and alerts
- Automate responses for multiple analytics rules at once
- Tag, assign, or close incidents automatically without using playbooks
- Create lists of tasks for your analysts to perform
- Control the order of actions that are executed
- Apply automations when an incident is updated (now in Preview), as well as when it's created



## Automate using playbooks

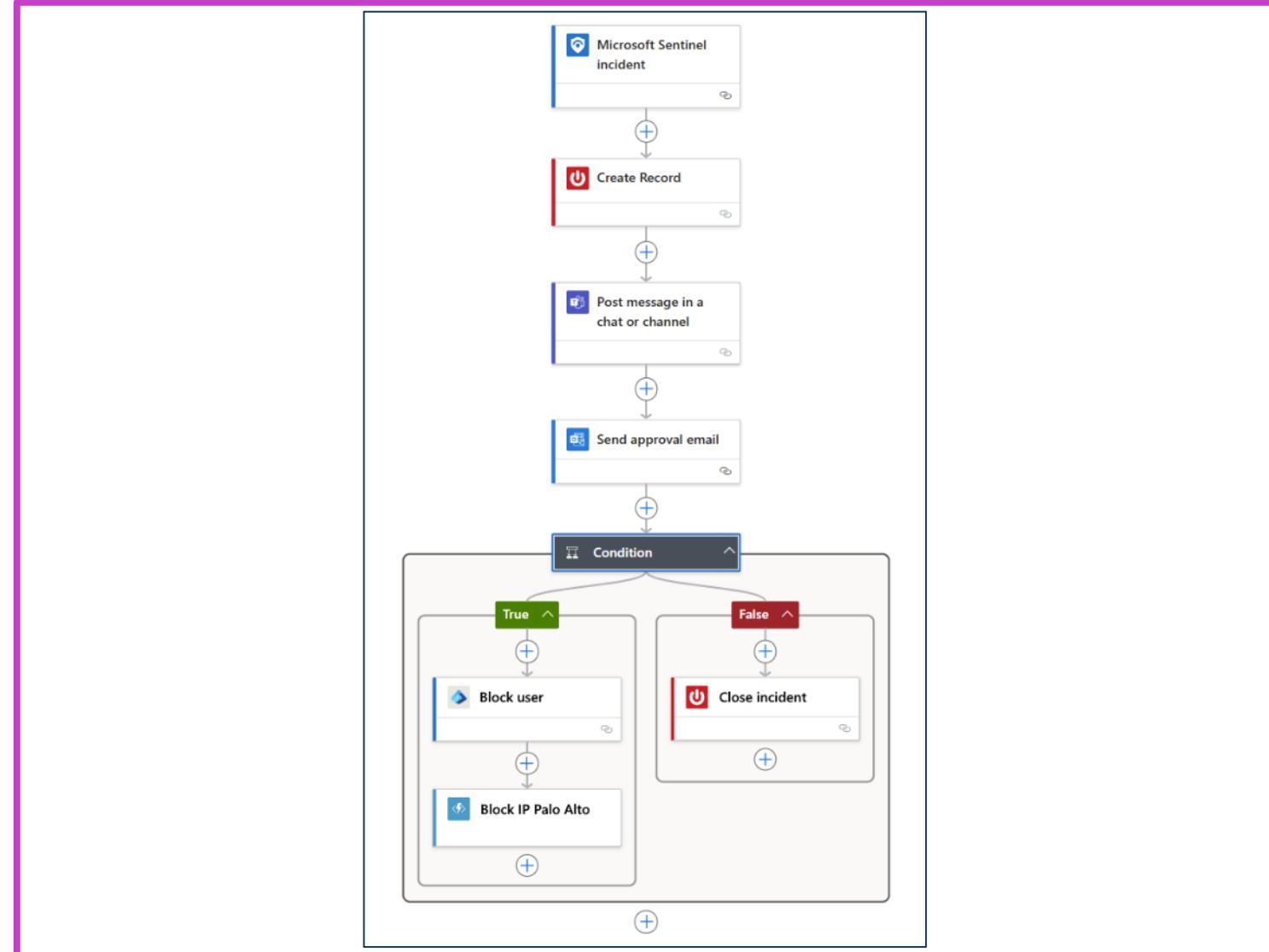
Using a playbook, you can:

- Automate and orchestrate your threat response
- Integrate with other systems, both internal and external
- Set playbooks to run automatically in response to specific alerts or incidents
- Benefit from the power and customization offered by Logic Apps in the form of:
  - Its integration and orchestration capabilities
  - Easy-to-use design tools
  - Scalability, reliability, and service level of a Tier 1 Azure service



# Automating Threat Response with Microsoft Sentinel

- Automate Incident Response: Use playbooks and automation rules in Microsoft Sentinel to remediate threats.
- Integration: Automation rules trigger playbooks for alerts, incidents, and ticketing system updates.
- Prerequisites: Roles like Contributor and Operator are required to manage and execute playbooks.



# Additional Study – Configure and manage security monitoring and automation solutions

Microsoft  
Learn Modules  
([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))



## Module Review Questions

- Manage and Respond to Security Alerts: Use Microsoft Defender for Cloud to detect, investigate, and respond to security alerts.
- Configure Workflow Automation: Automate threat response and remediation using workflows in Microsoft Defender for Cloud.
- Monitor Network Security with Azure Monitor: Configure data collection rules (DCRs) to monitor network events and performance data.
- Set Up Microsoft Sentinel Data Connectors: Integrate various data sources into Microsoft Sentinel for enhanced monitoring and analysis.
- Enable Analytics and Automation in Sentinel: Create analytics rules and configure automation workflows to respond to security incidents.

# Module Labs

# Lab 08 – Create a Log Analytics Workspace, Azure Storage Account, and Data Collection Rule (DCR)



This exercise teaches students how to create a Log Analytics Workspace, Azure Storage Account, and Data Collection Rule (DCR) to efficiently collect logs and data

[Launch this Exercise in GitHub](#)

The screenshot shows the Azure Log Analytics workspace overview for 'law-1'. The workspace is active and located in the East US region. It is connected to the 'az-rg-1' resource group and the 'Azure subscription'. The workspace has a workspace ID of 74672cccd-c990-48b5-9ef2-dc5dd5b6e5e2 and a pay-as-you-go pricing tier. The access control mode is set to 'Use resource or workspace permissions'. There are no operational issues. The 'Get Started' section provides links to connect a data source, configure monitoring solutions, and monitor workspace health. The 'Useful links' section includes links to the documentation site and community forums.

law-1 Log Analytics workspace

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Logs

Resource visualizer

Settings

Classic

Monitoring

Automation

Help

Search

Delete

The Log Analytics agents (MMA.OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. [Learn more about migrating to Azure Monitor Agent](#)

Essentials

Resource group (move) : az-rg-1

Status : Active

Location : East US

Subscription (move) : Azure subscription

Subscription ID

Tags (edit) : Add tags

Workspace Name : law-1

Workspace ID : 74672cccd-c990-48b5-9ef2-dc5dd5b6e5e2

Pricing tier : Pay-as-you-go

Access control mode : Use resource or workspace permissions

Operational issues : OK

View Cost | JSON View

Get Started Recommendations

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 Connect a data source  
Select one or more data sources to connect to the workspace  
Azure virtual machines (VMs)

2 Configure monitoring solutions  
Add monitoring solutions that provide insights for applications and services in your environment

3 Monitor workspace health  
Create alerts to proactively detect any issue that arise in your workspace

Useful links

Documentation site

Community

# Lab 09 – Configuring Microsoft Defender for Cloud Enhanced Security Features for Servers



This exercise teaches students how to configure Microsoft Defender for Cloud Enhanced Security Features for Servers Cloud Workload Protection plan.

[Launch this Exercise in GitHub](#)

Note: \*\*TO REVIEW ONLY\*\* select Change plan > to display the details of the recommended Microsoft Defender for Servers Plan 2, then click the X in the top-right corner of the plan selection details to close the template.

© Copyright Microsoft Corporation. All rights reserved.

# Lab 10 – Enable just-in-time access on VMs



This exercise teaches students how to use Microsoft Defender for Cloud's just-in-time (JIT) access to protect your Azure virtual machines (VMs) from unauthorized network access.

[Launch this Exercise in GitHub](#)

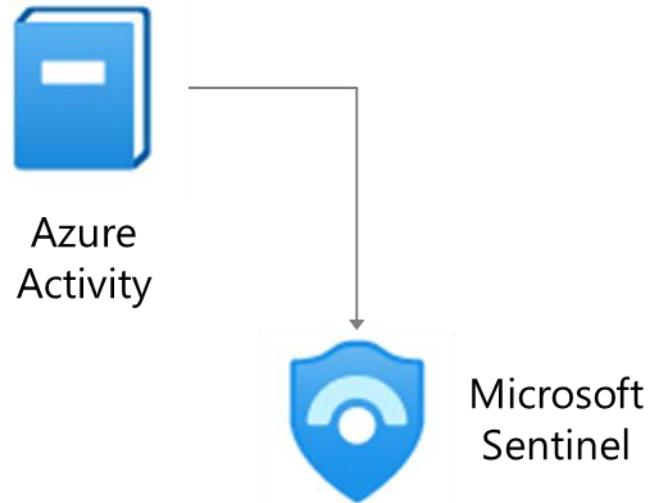
The screenshot shows the Azure portal interface for managing a virtual machine named 'vm-1'. On the left, there is a navigation sidebar with various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings (which is currently selected), Disks, Extensions + applications, Operating system, Configuration (which is also selected), and Advisor recommendations. The main content area is titled 'Just-in-time VM access' and contains the message: 'To improve security, enable a just-in-time access.' Below this is a blue 'Enable just-in-time' button. A callout box provides additional information: 'Just-in-time VM access secures your VM's management ports and grants access on-demand, for a limited time period, to pre-approved IP addresses. [Learn more about just-in-time access](#)'.

# Lab 11 – Microsoft Sentinel



This exercise teaches students how to onboard Microsoft Sentinel, automate threat detection, and respond with playbooks.

[Launch this Exercise in GitHub](#)



**Rule**  
JIT management port access removed

**Playbook**

# Knowledge check



## 1 What is the primary function of Data Collection Rules (DCRs) in Azure Monitor?

- To specify what data should be collected, how to transform that data, and where to send it
- To define the visual themes of Azure Monitor dashboards
- To manage user permissions in Azure Monitor

## 2 What is the purpose of Microsoft Defender for Cloud?

- To manage cloud billing and usage
- To protect cloud resources from threats
- To create virtual networks in Azure

## 3 How can you customize detection rules in Microsoft Sentinel?

- By predicting stock market trends
- By identifying potential security incidents
- By automating virtual machine deployments

# Learning Path Recap

## In this learning path, we:

Enabled effective performance tracking and real-time analytics through Azure Monitor configuration and management.

Fortified cloud security by enabling and managing Microsoft Defender for Cloud to counter various threats.

Set up and oversaw Microsoft Sentinel for centralized security data analysis and threat detection.

# End of presentation