

AZ-500

Tag 4

Microsoft Azure Security Technologies

Guten Morgen!



Agenda

1 Manage identity and access

2 Secure networking

3 Secure compute, storage, and databases

4 Manage security operations

SIEH

Monitoring

Defender Cloud

Microsoft Sentinel

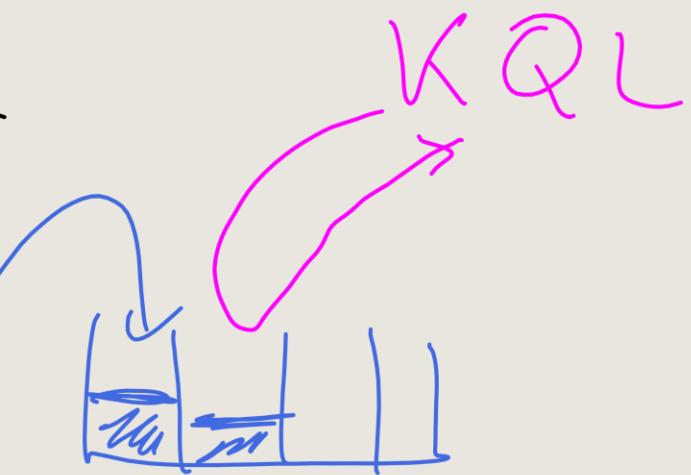
Lab 8

LA Workspace

Datalake

Blob

Lab 7



Table

30 Tage

Workbook

Kusto Query Lang

Dashboard

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

C Sentinel

B Defender

A Monitoring

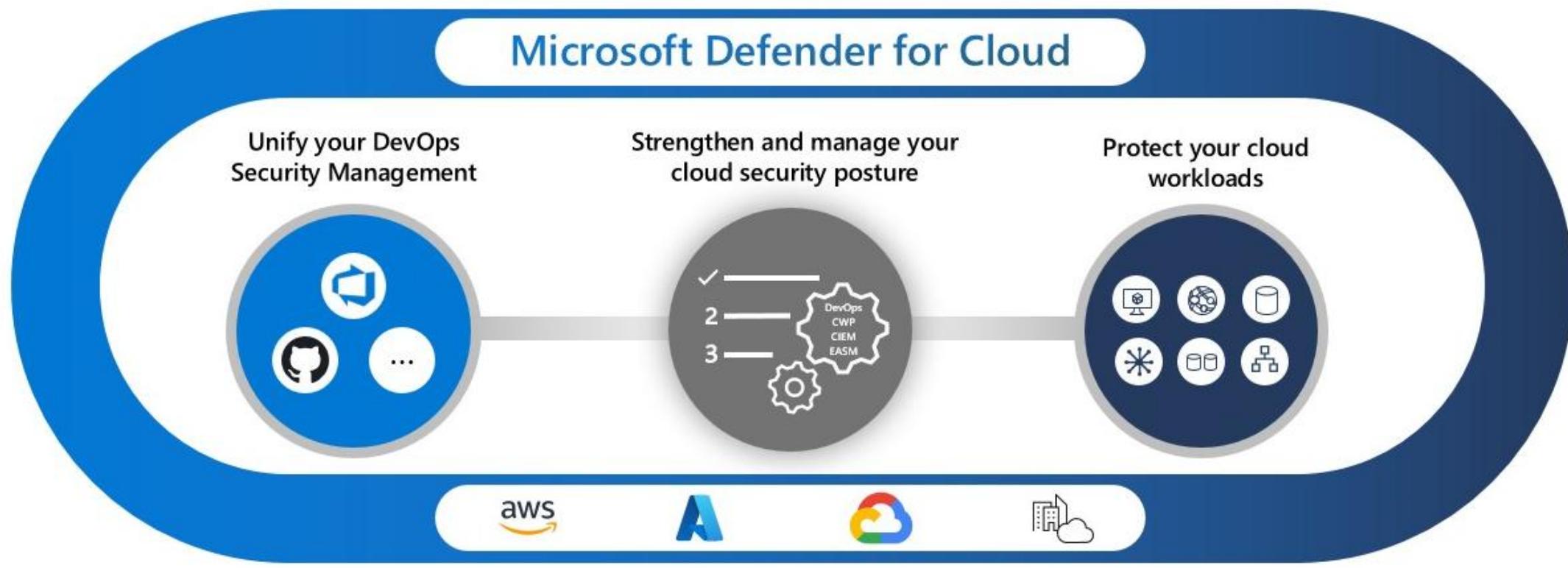
Sentinel

Azure

LA

Manage security posture by using Microsoft Defender for Cloud

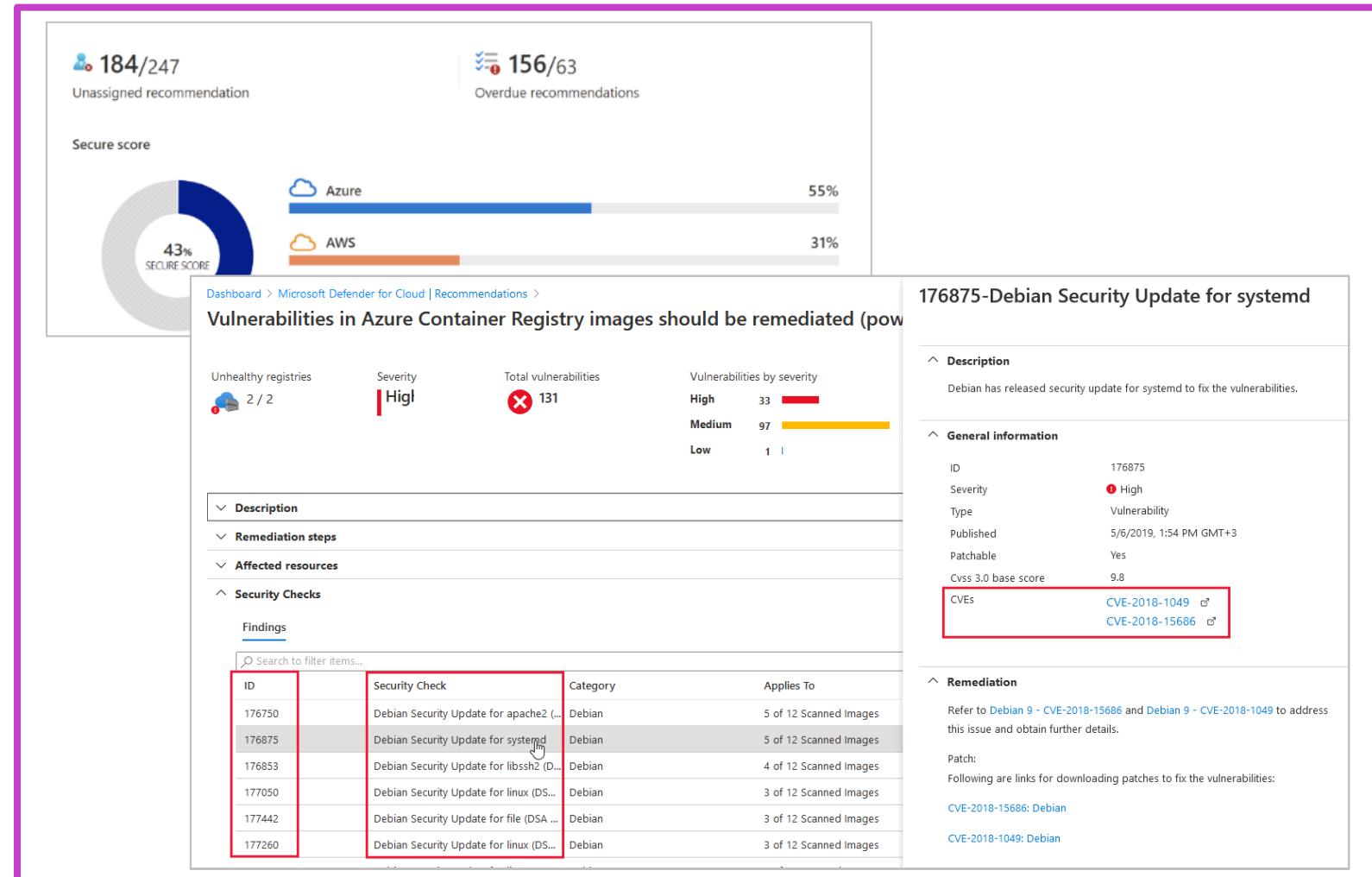
Implement Microsoft Defender for Cloud



- 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

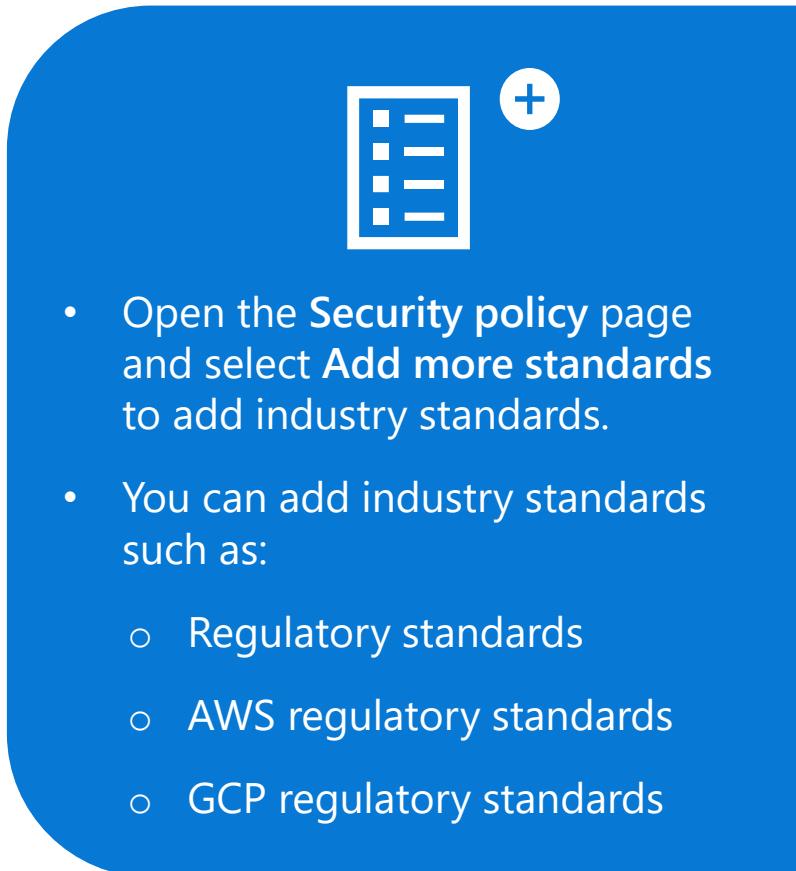


- Visit the regulatory compliance dashboard for overall scores and assessment results.
- View controls, associated assessments, and their status.
- Check both automated and manual assessments under the "**Your Actions**" tab.

The screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard. It includes a sidebar with navigation links like Overview, Getting started, Recommendations, Security alerts, Inventory, Workbooks, Community, and Diagnose and solve problems. The main area displays a summary of 2 subscriptions, with a callout '1' pointing to the NIST SP 800 53 R4 link. Below this, there's a section for 'AC. Access Control' with a callout '2' pointing to the 'Control details' for AC-2(1) through AC-2(7). To the right, a separate window titled 'AC.2.7 Role-based Schemes' shows a table of actions categorized by type (Automated, Manual) and action name, with a callout '3' pointing to the first row.

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

Manage compliance standards Microsoft Defender for Cloud



- 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

The screenshot shows the 'Settings | Security policy' page for the 'CyberSecSOC' subscription. It displays two main sections: 'Default initiative' and 'Industry & regulatory standards'.

Default initiative: This section shows the default initiative enabled on the subscription. It includes a table with columns: Assignment, Assigned On, Audit policies, Deny policies, Disabled policies, and Exempted policies. The table data is as follows:

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: This section lists various industry standards and their status. Each item has a 'Disable' button and a help icon (info symbol). The listed standards are:

- Azure Security Benchmark: Track Azure Security Benchmark controls in the Compliance Dashboard, based on a recommended set of policies and assessments. Status: Out of the box. Buttons: 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. Status: Out of the box. Buttons: Disable, ⓘ
- ISO 27001: Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments. Status: Out of the box. Buttons: Disable, ⓘ
- SOC TSP: Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments. Status: Out of the box. Buttons: 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. Status: Manually added. Buttons: Delete, ⓘ
- CMMC Level 3: Track CMMC Level 3 controls in the Compliance Dashboard, based on a recommended set of policies and assessments. Status: Manually added. Buttons: 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. Status: Manually added. Buttons: Delete, ⓘ

At the bottom of the page, there is a red-bordered button labeled '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 shows the Microsoft Defender for Cloud portal interface. On the left, a blue sidebar features a clipboard icon with a pencil and a plus sign, indicating the action to add a new initiative. The main area is titled "Add custom initiatives". It includes a "Create new" button highlighted with a red box, a "Refresh" button, and a search bar. Below these are two tables: one for "Custom policy initiative" and another for "Organizational policy". The "Organizational policy" table has a single row with columns for NAME (Organizational policy), DESCRIPTION (custom policy), STATUS (Not assigned), and an "Add" button also highlighted with a red box. To the right of these tables is the "Organizational policy" configuration blade, which is divided into tabs: Basics (selected), Parameters, Remediation, Non-compliance messages, and Review + create. The Basics tab 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"), and a large Description text area. At the bottom of the blade 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



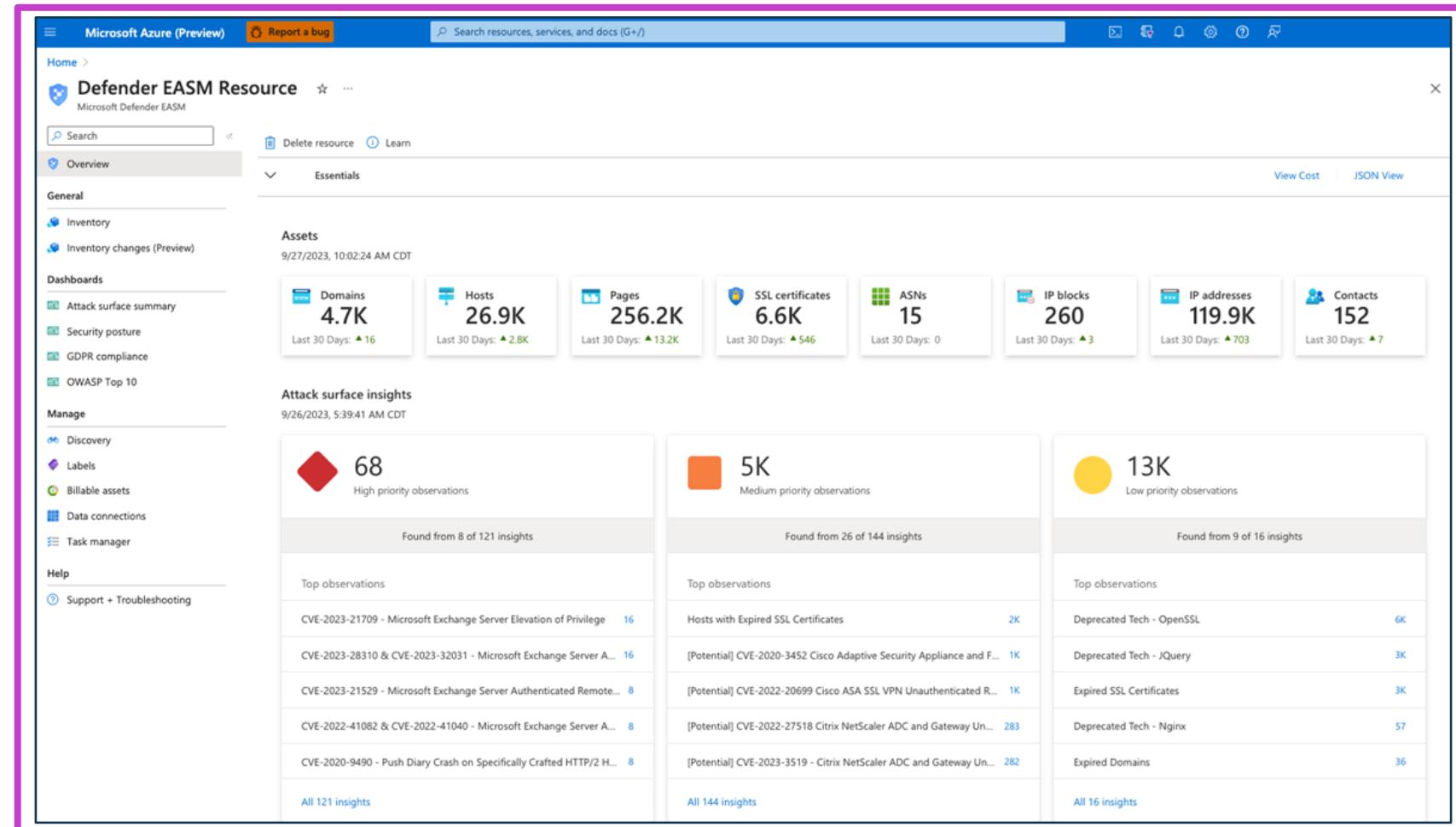
Connect multi-cloud environments

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.



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' (selected), 'Security policies', 'Email notifications', 'Workflow automation', and 'Continuous export'. The main content area has two sections: 'Cloud Security Posture Management (CSPM)' and 'Cloud Workload Protection (CWP)'. The CSPM section contains information about Microsoft Defender CSPM and a table with two rows: 'Foundational CSPM' (Free) and 'Defender CSPM' (\$5/Billable resource/Month). The CWP section contains information about Microsoft Defender for Cloud and a table with one row for 'Servers' (Plan 2 (\$15/Server/Month)). The 'Servers' row is highlighted with a red circle.

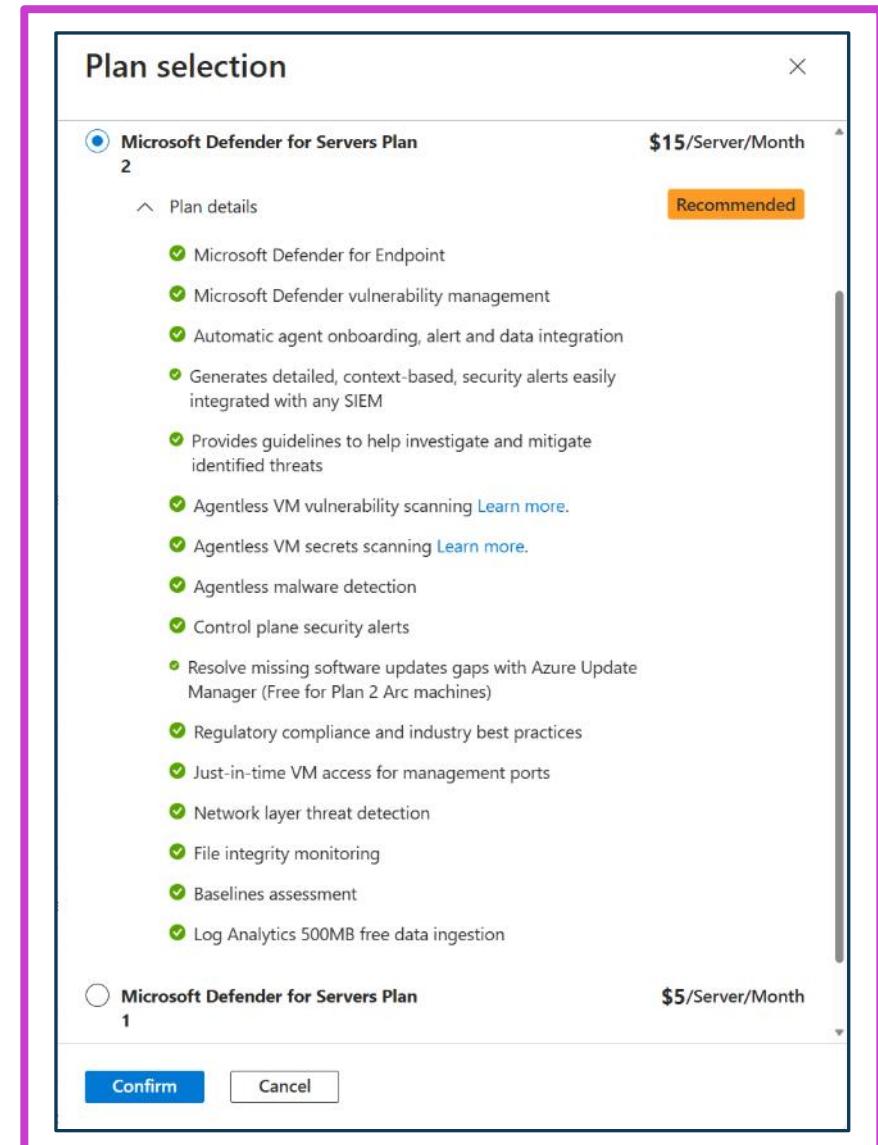
Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free Details >		Full	<button>Off</button> <button>On</button>
Defender CSPM	\$5/Billable resource/Month Details >	4 resources ⓘ		<button>Off</button> <button>On</button>

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

- 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.

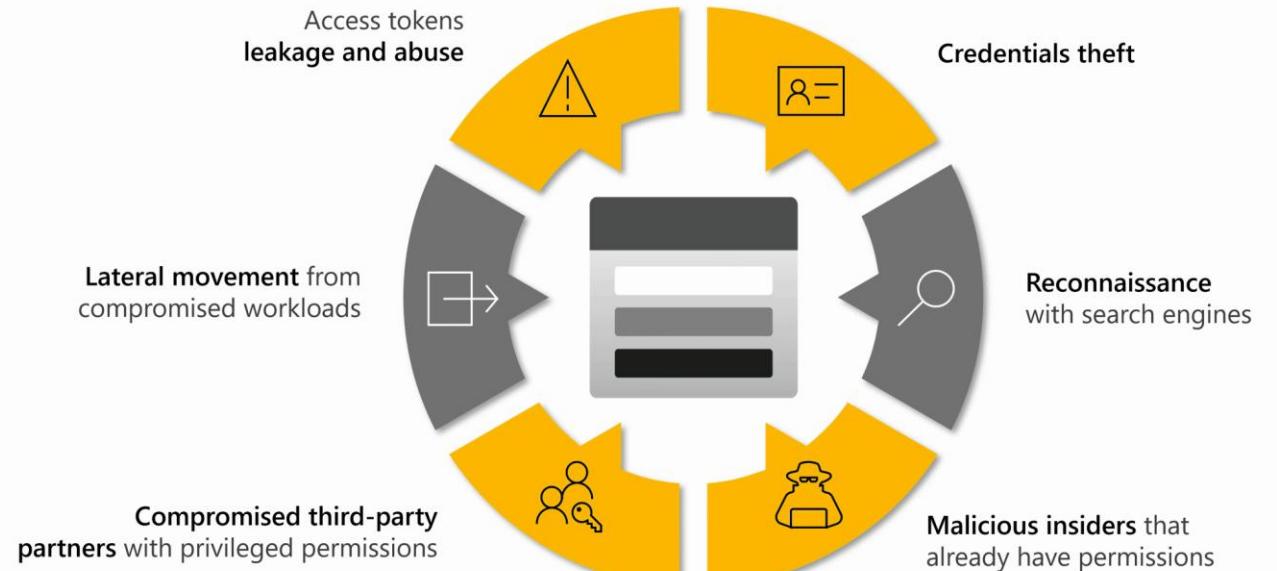
Microsoft Defender for Servers

- 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.
- Flexible deployment supports subscriptions and resources with integrated compliance and threat detection tools.



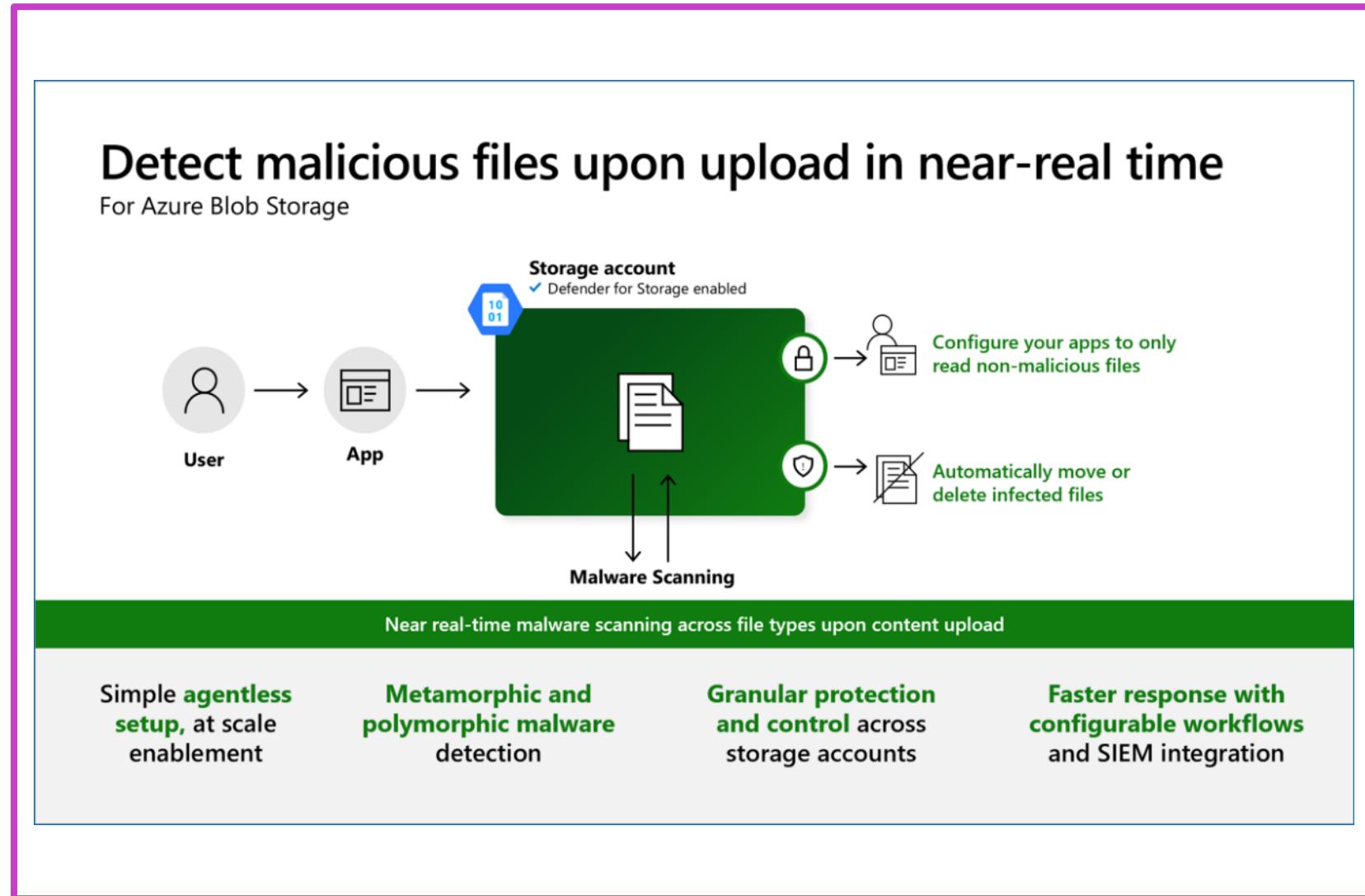
Microsoft Defender for Storage

- 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.



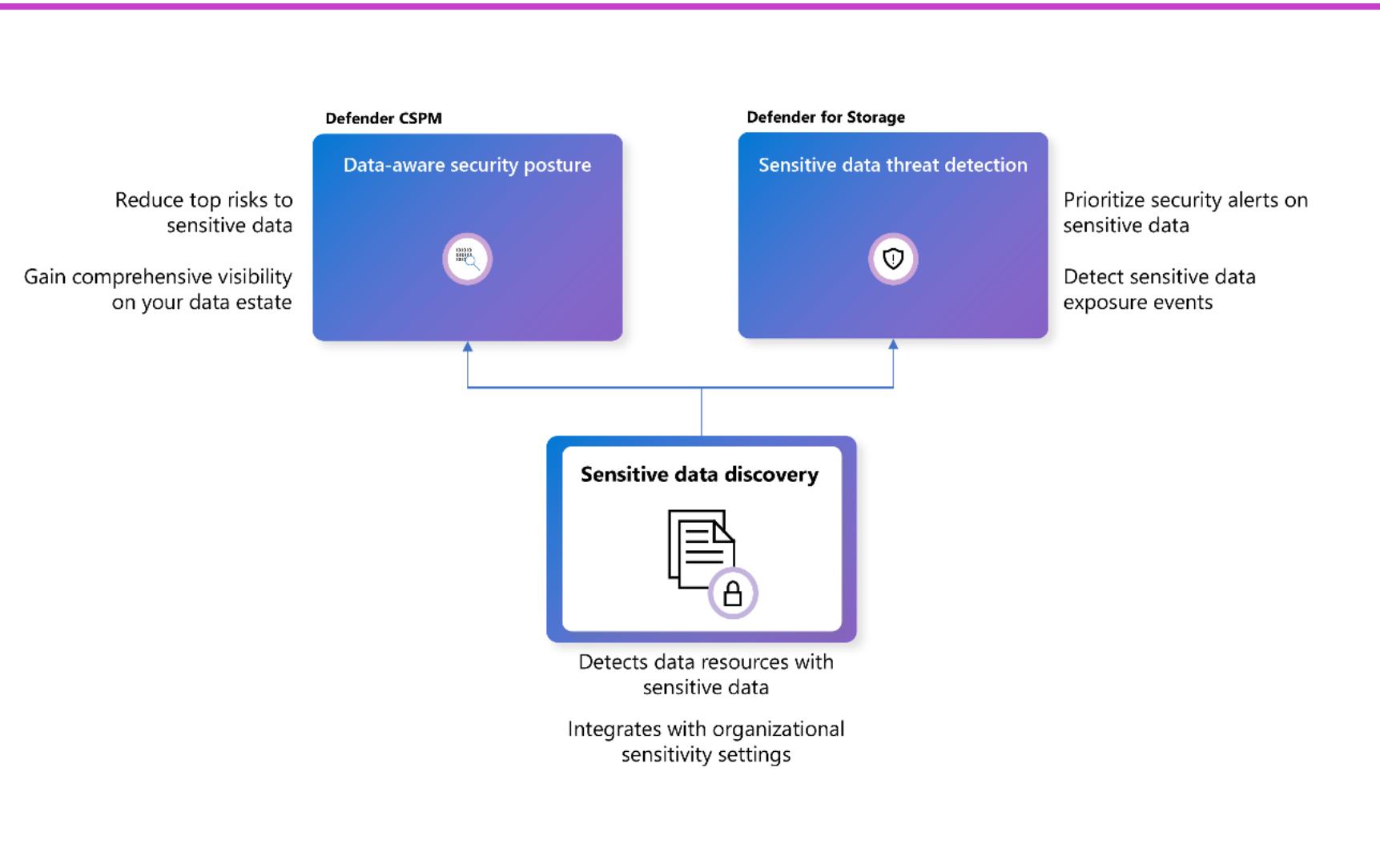
Malware scanning in Defender for Storage

- 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 URL [https://azuresdk.dev.fabricbot.ai/](#). The page is titled "Settings | Defender plans". On the left, there's a sidebar with "Search" and "Save" buttons, and a "Settings & monitoring" tab. The main content area has a "Enable all plans" button. It's 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: Full (On).
- Defender CSPM: \$5/Billable resource/Month, Details >. Resource quantity: 2 resources, Monitoring coverage: Full (On).

Cloud Workload Protection (CWP)

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



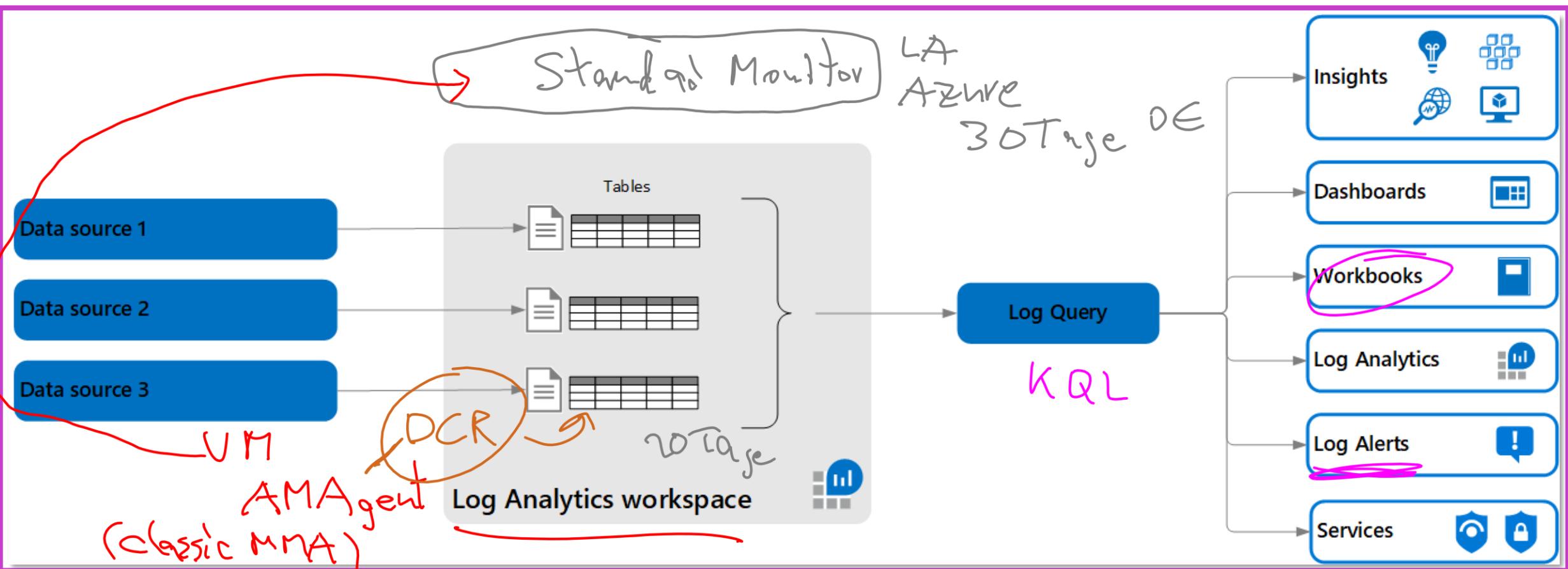
The screenshot shows the 'Settings & monitoring' section of the Microsoft Defender for Cloud interface. Under 'Cloud Workload Protection (CWP)', it displays the following configuration:

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

Below this, there is a section for 'Registry access' which enables agentless vulnerability assessment for registry images. It includes a status indicator and a toggle switch.

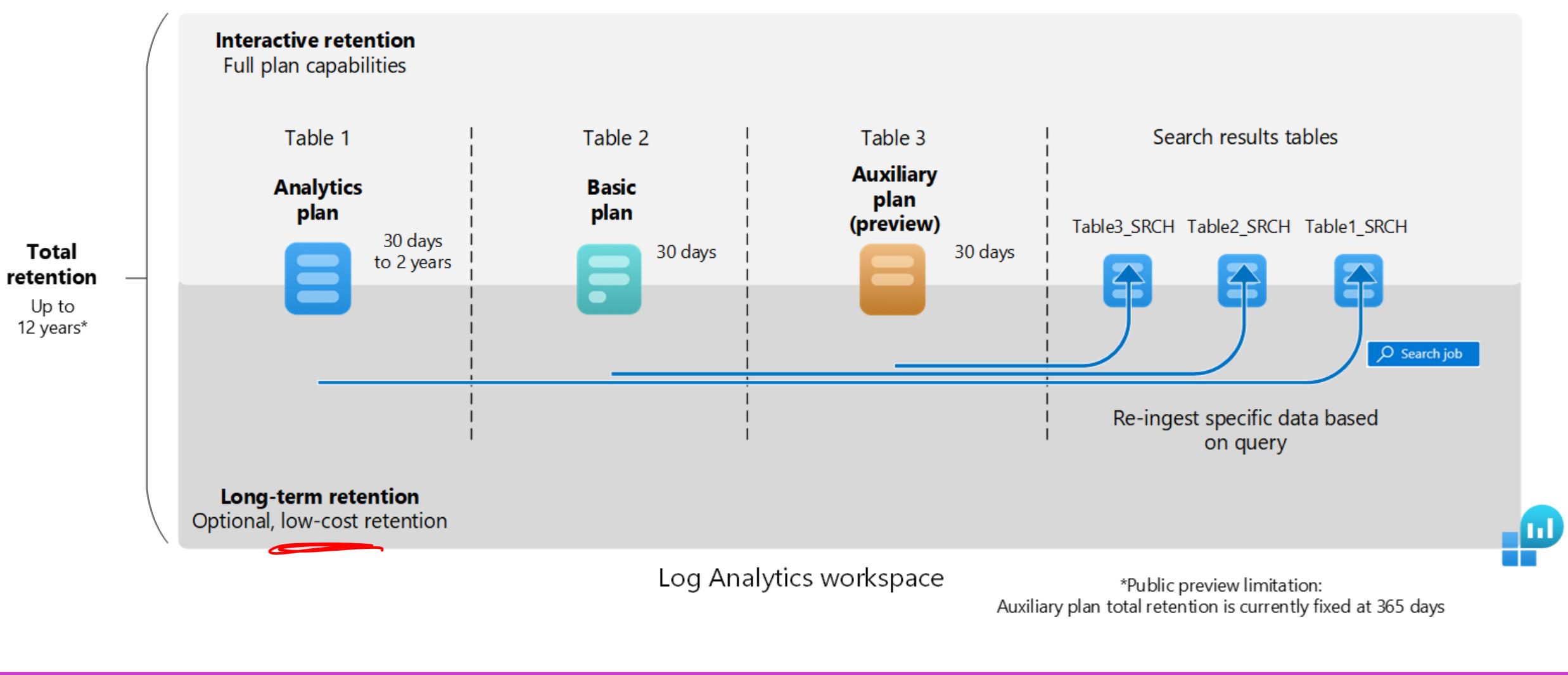
- Automatically scans ACR images for vulnerabilities without any agent deployment.
- Supports OS and language package scanning with continuous daily rescans.
- Provides detailed vulnerability reports and remediation recommendations for secure deployments.

Log Analytics workspace



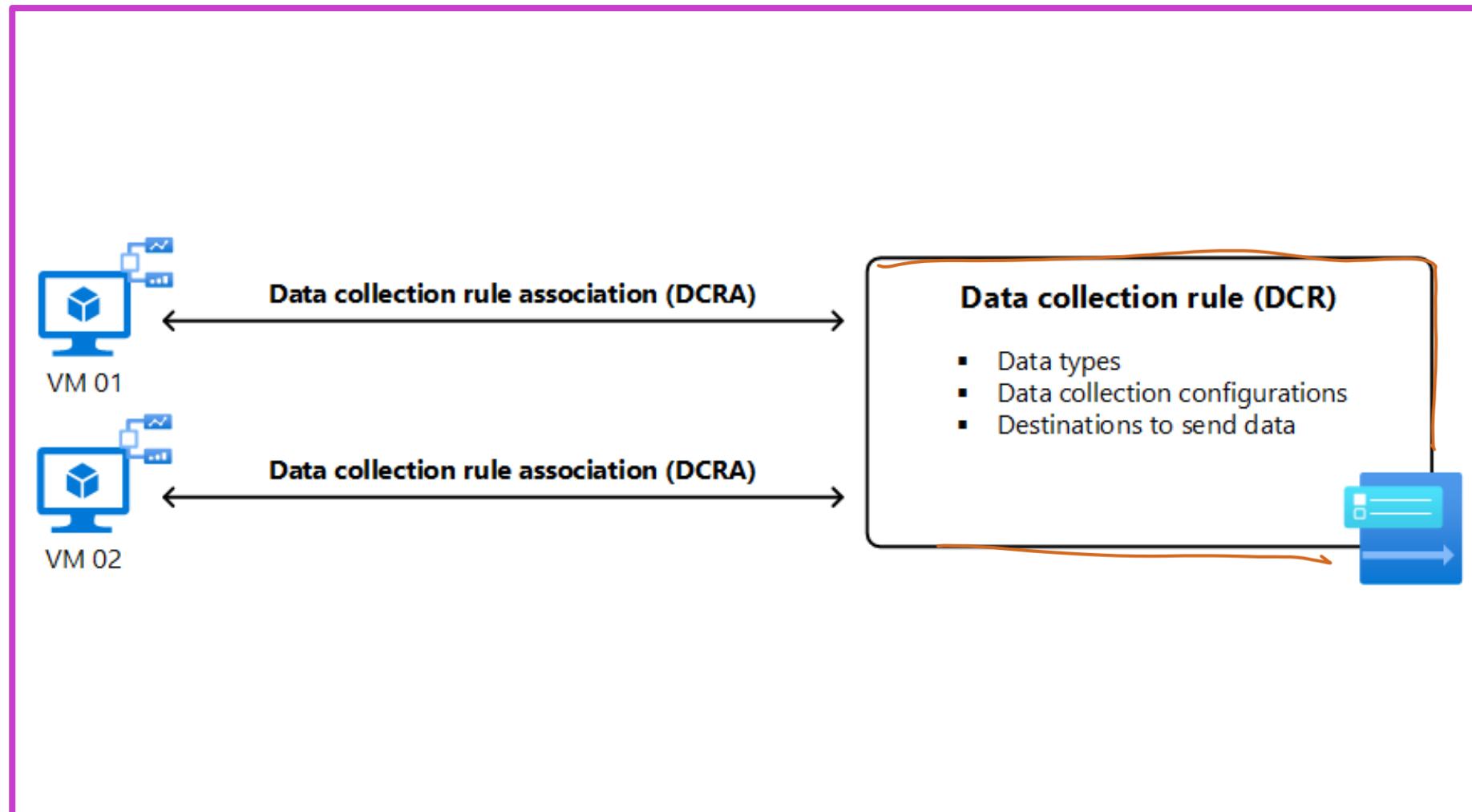
- A Log Analytics workspace is a centralized, configurable environment for Azure Monitor log data, allowing data collection and retention management across multiple Azure services.

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.



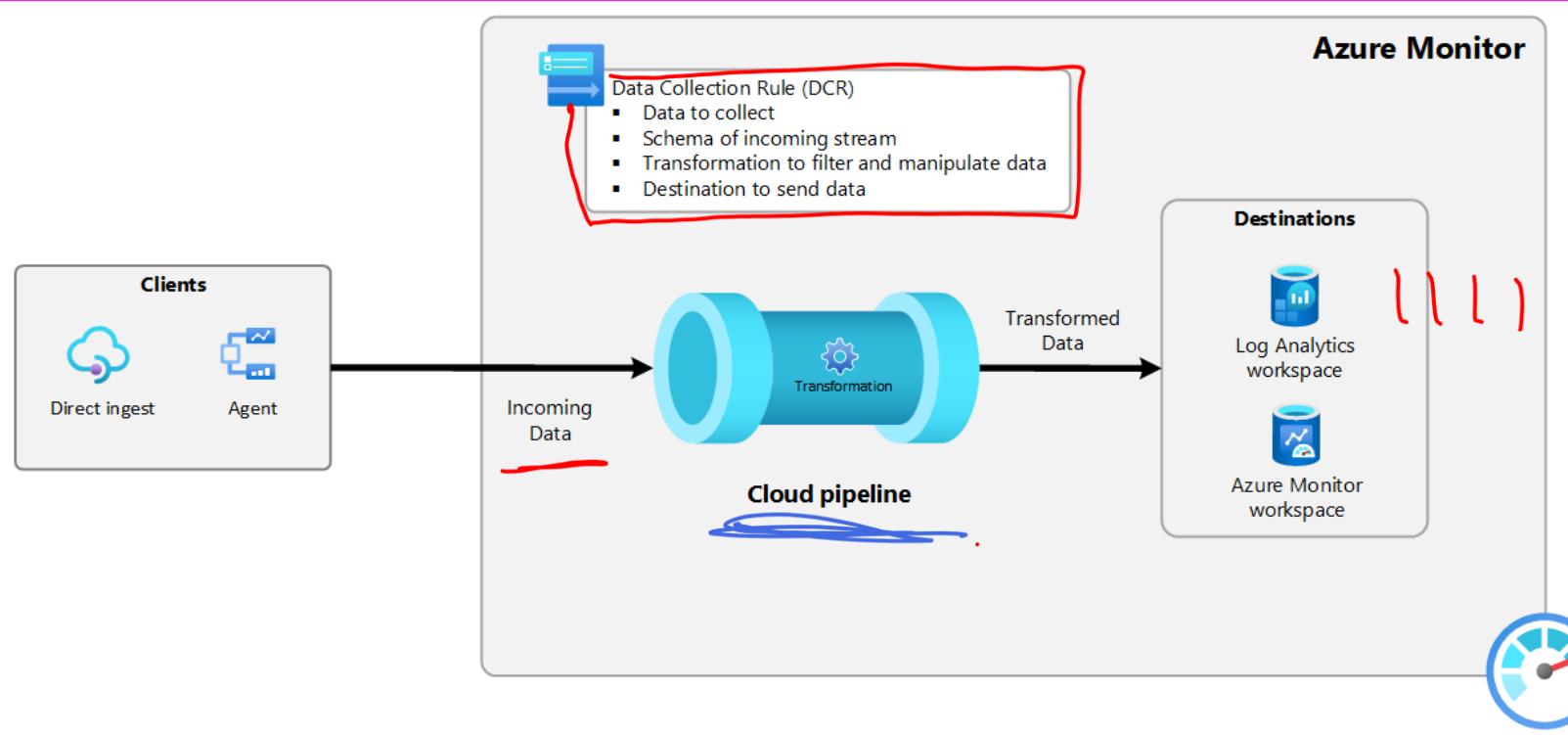
Collect data with Azure Monitor Agent

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 '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. The main content area is titled 'vm-1 | Extensions + applications' and shows a list of extensions. A yellow box highlights the message 'The Azure Monitor Agent is deployed'. A yellow arrow points from this message to the list of extensions. The list shows two items: 'AzureMonitorWindows...' and 'MDE.Windows'. The 'AzureMonitorWindows...' item has its status set to 'Disabled'.

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

- 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.

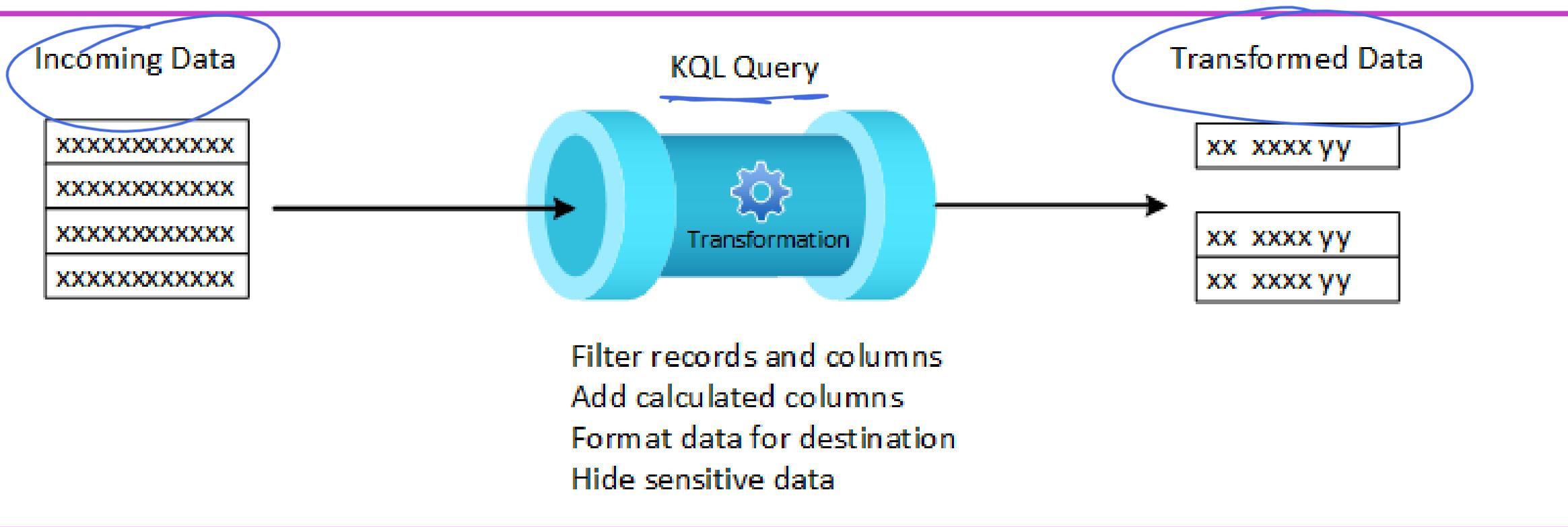
Data collection rules (DCRs) in Azure Monitor



- 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.

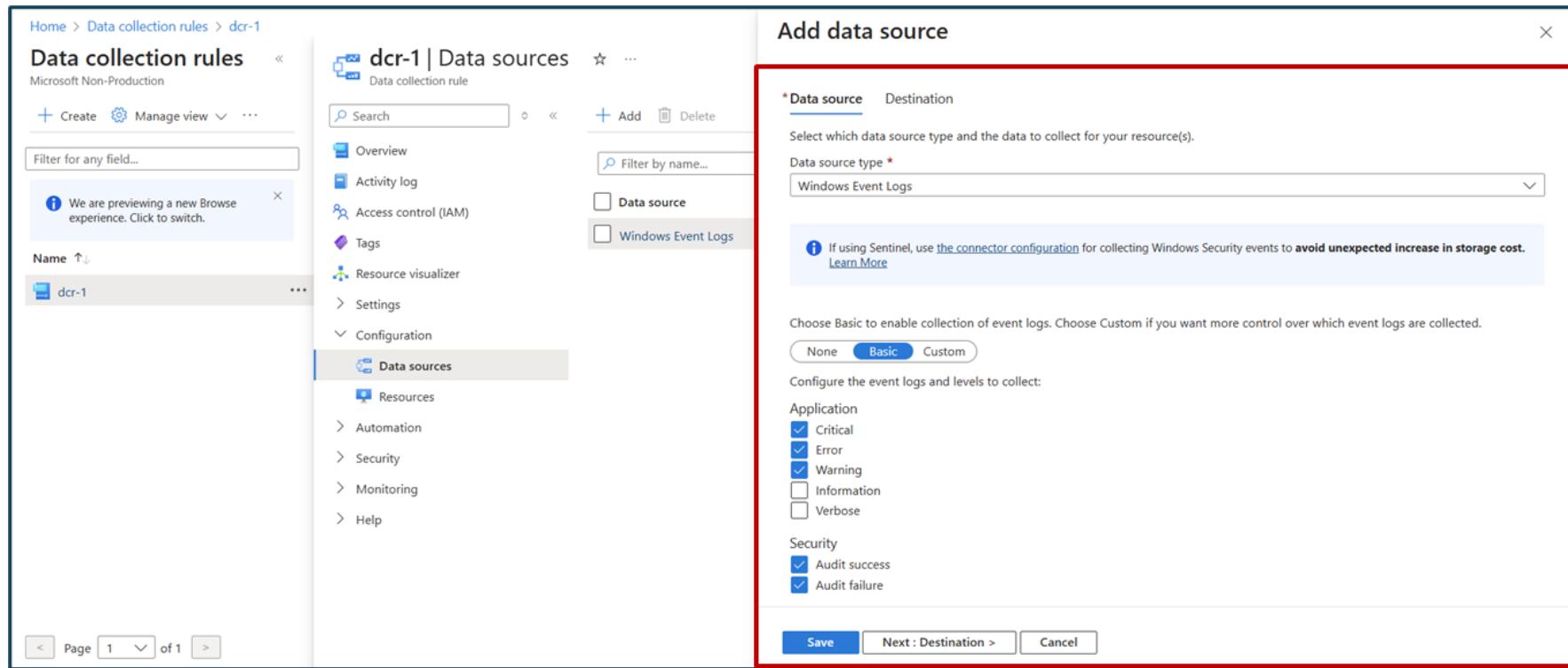
Transformations in Data collection rules (DCRs)

LA



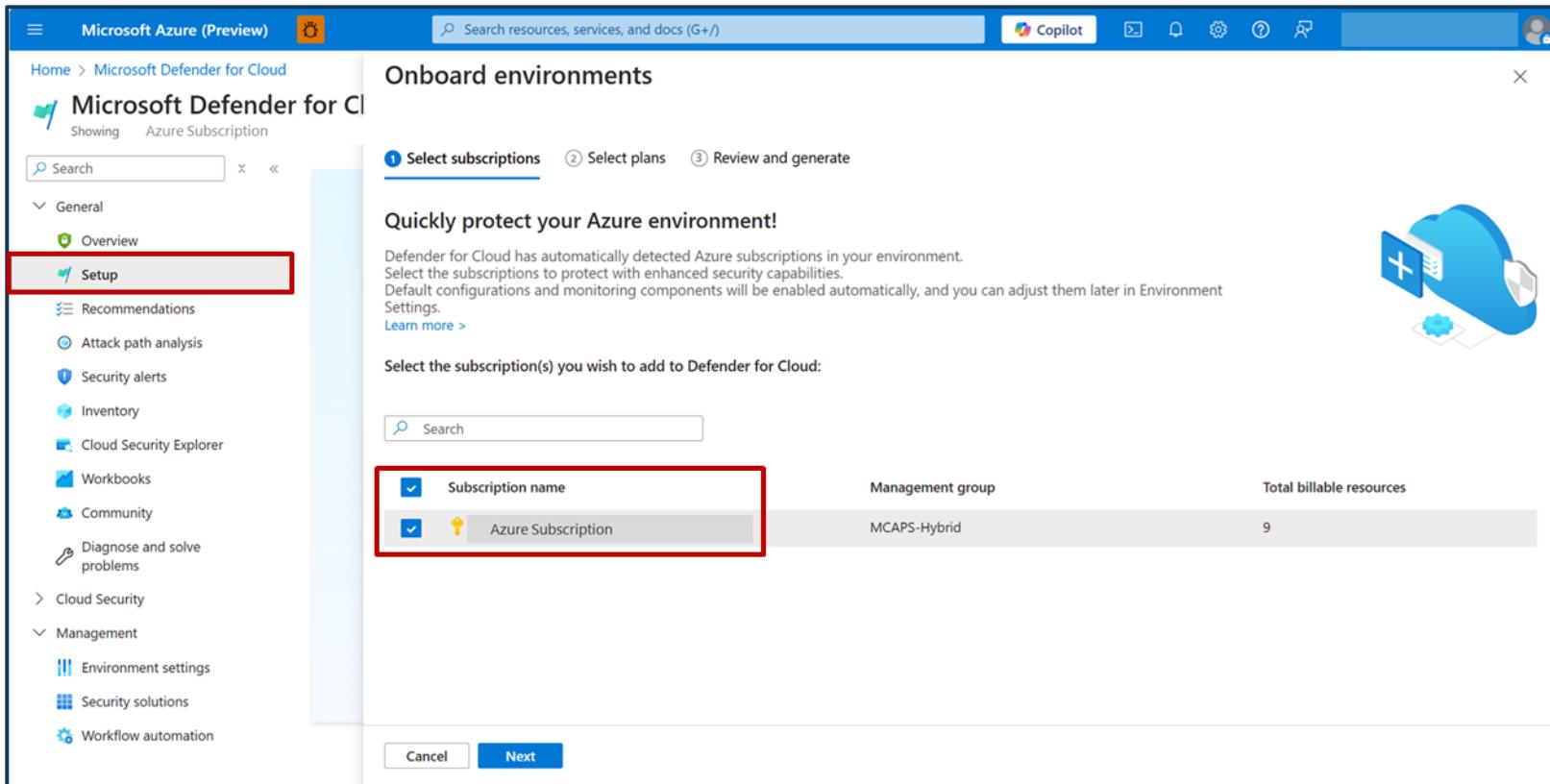
- Modify incoming data before storage or forwarding in Azure Monitor.
- Filter, remove sensitive data, or format data to match destination schema.
- Enable advanced scenarios like multi-destination routing and data enrichment.

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.

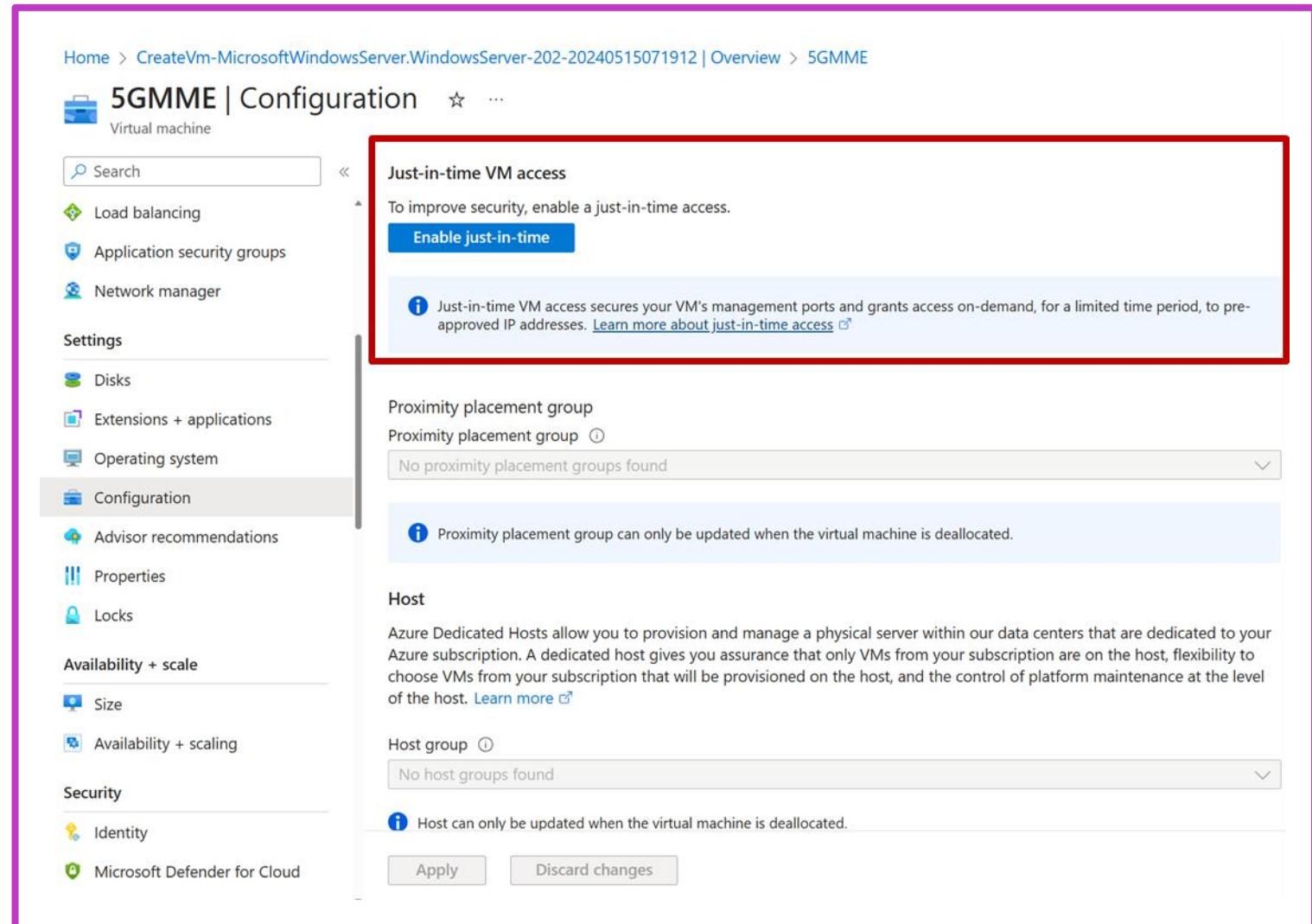
Connect your Azure subscriptions



- 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.

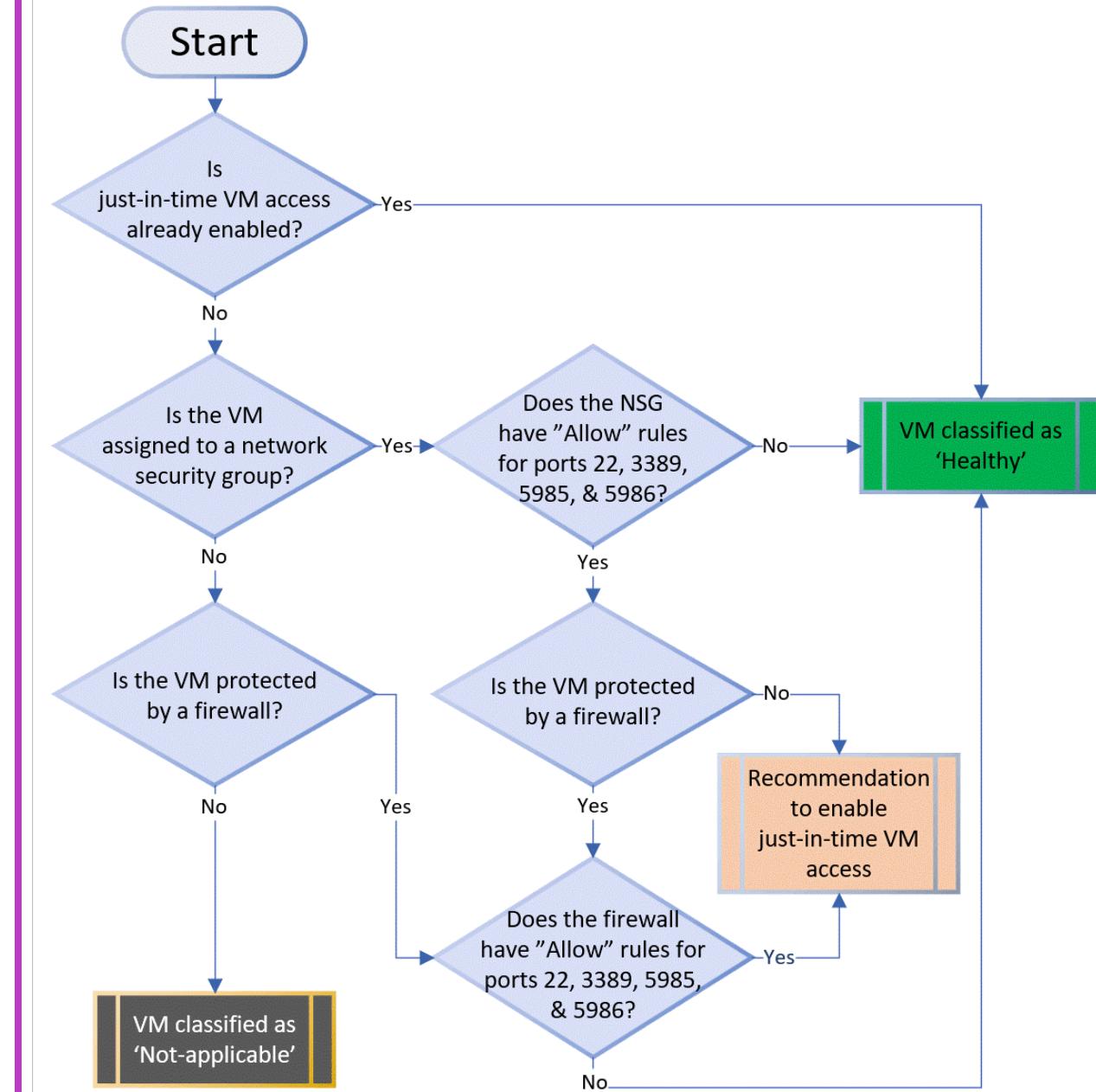
Understanding just-in-time VM access

- 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



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 message about subscriptions not having full protections enabled, with a link to upgrade. Below that, two links 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.' It shows 1 VM named 'romebuild' with 0 Requests, N/A for Last access, and a shield icon for Connection details. The 'Last user' column shows 'N/A'. A 'Request access' button is at the top right of the table area. A search bar is at the bottom left, and a three-dot menu is at the bottom right.

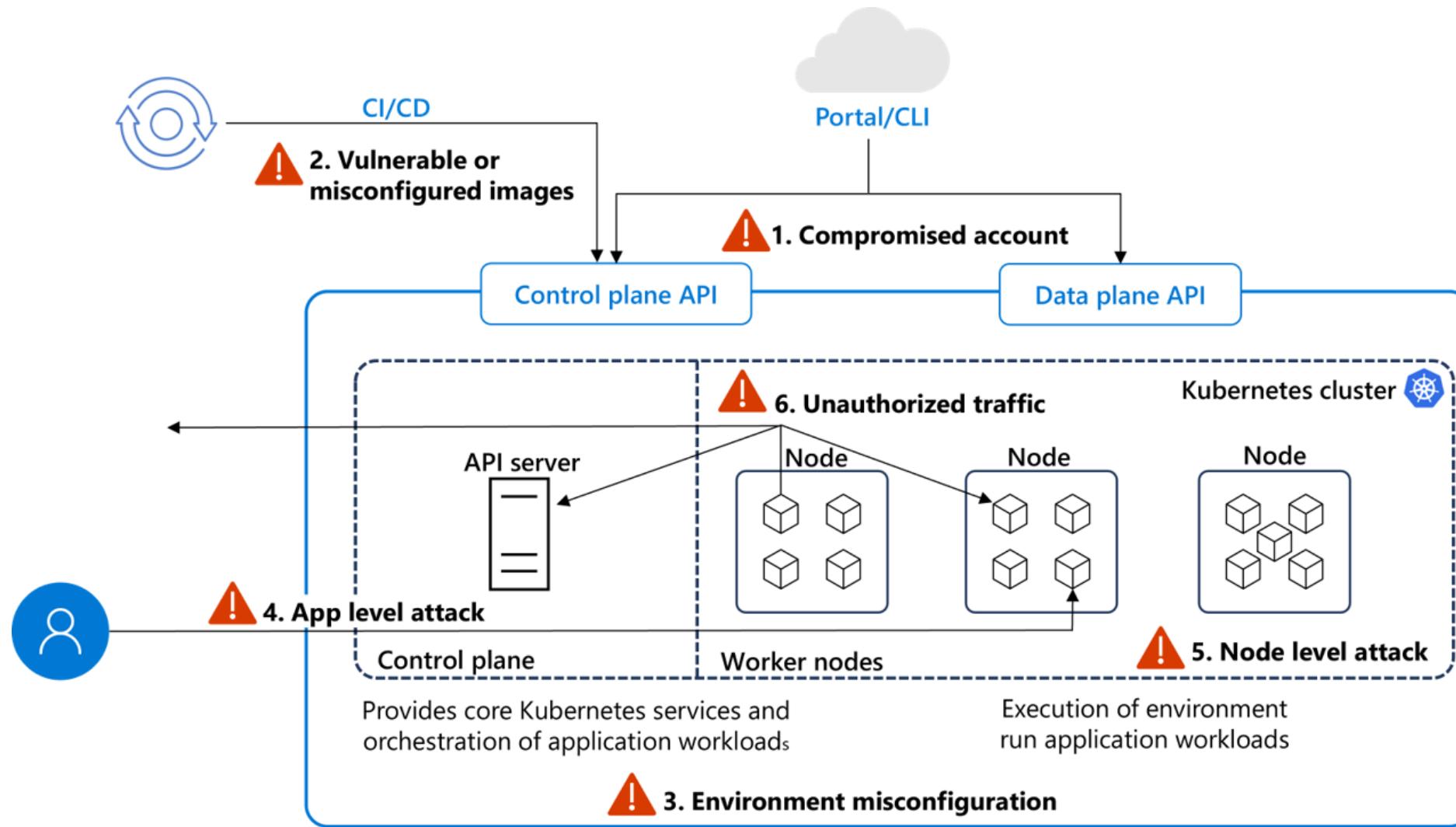
Virtual machine	Approved	Last access	Connection details	Last user
romebuild	0 Requests	N/A	shield icon	N/A

Container security in Microsoft Defender for Containers

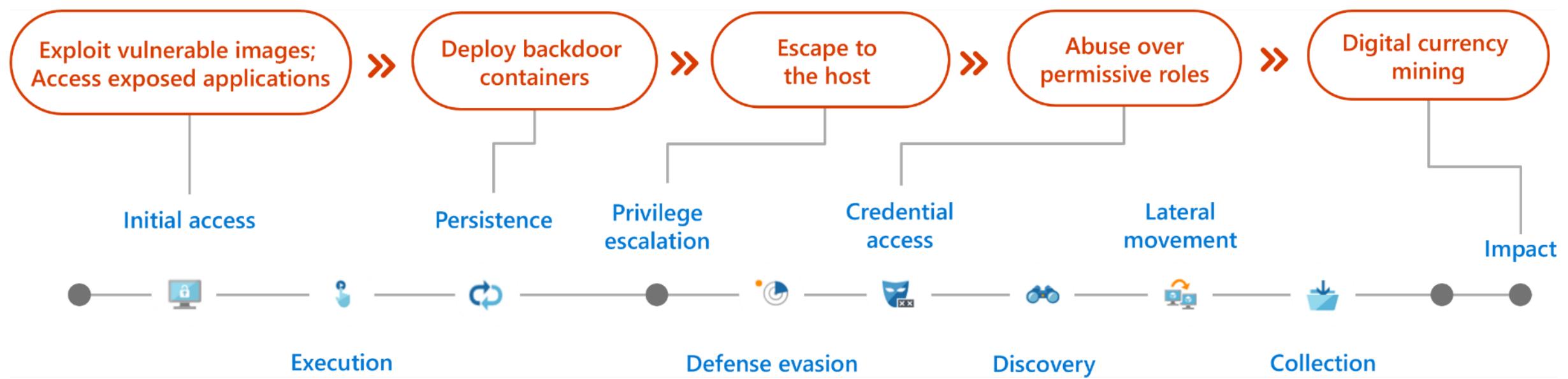
The screenshot shows the Microsoft Defender for Cloud Recommendations interface. On the left, a sidebar lists navigation options: General, Overview, Getting started, Recommendations (which is selected), Security alerts, Inventory, Workbooks, Community, Diagnose and solve problems, Cloud Security, Security 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). A search bar and filters for recommendation status, severity, and resource type are present. A red box highlights the 'Resource type == None' filter.

- 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

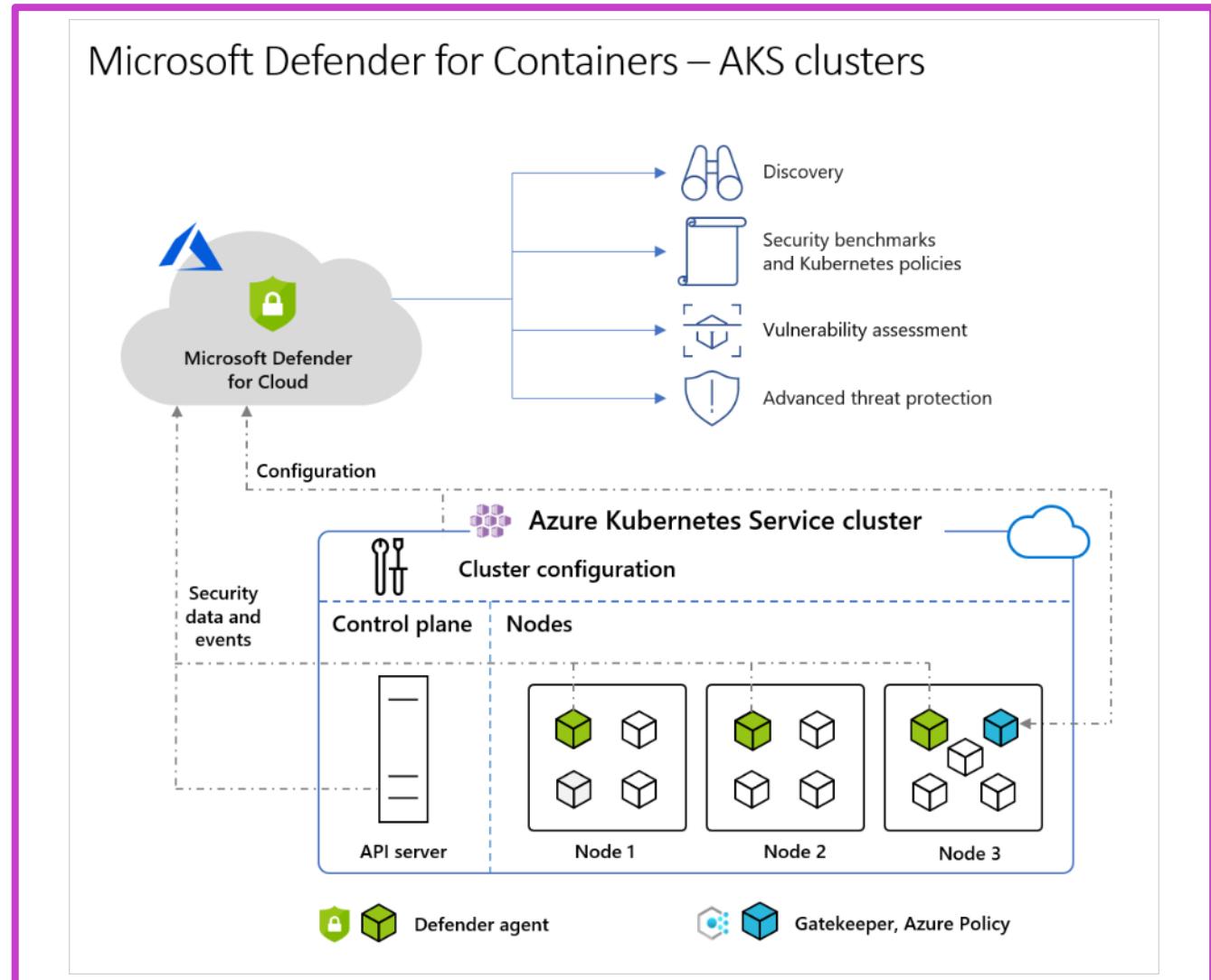


Common attack techniques



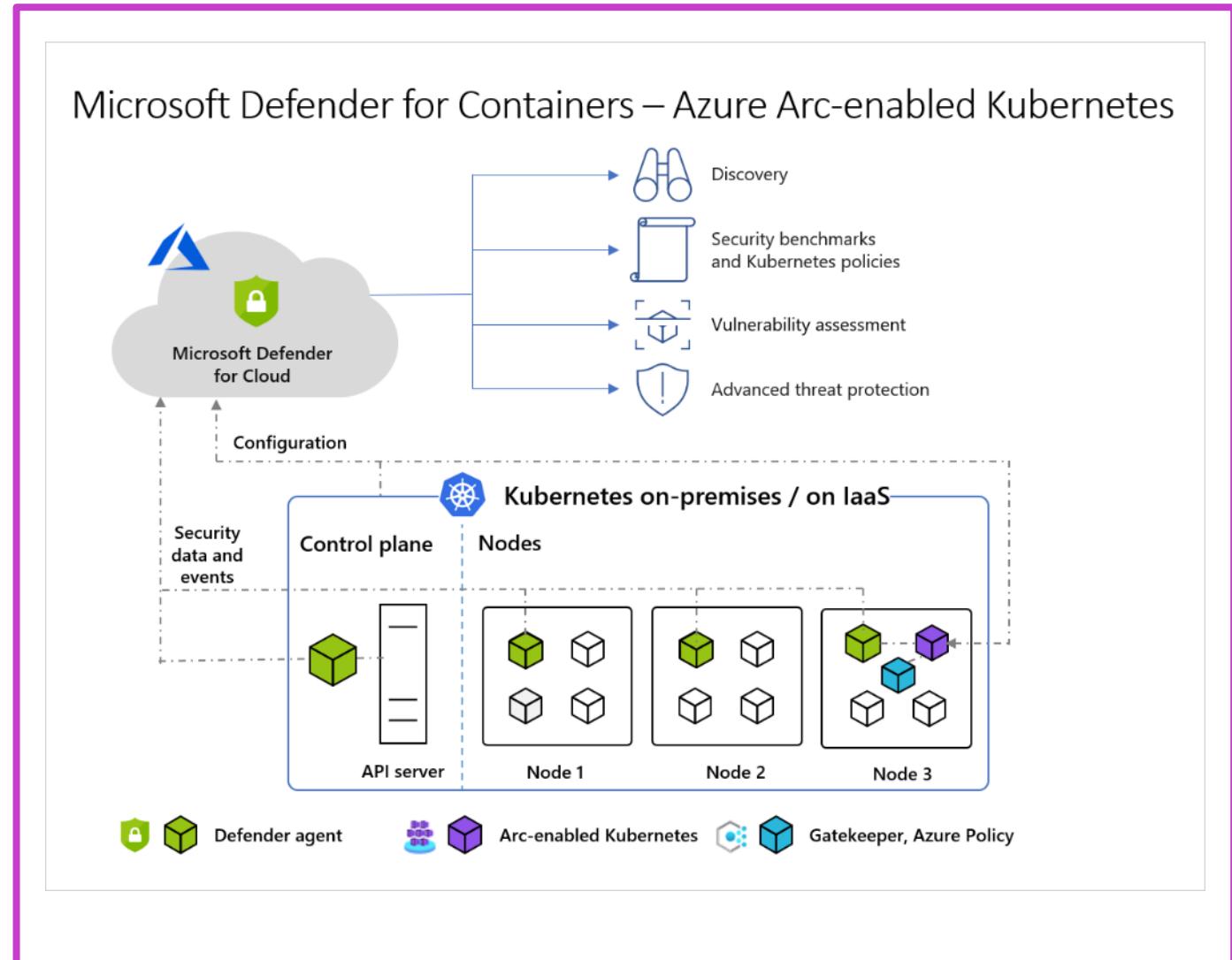
Architecture diagram of Defender for Cloud and AKS clusters

- 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.



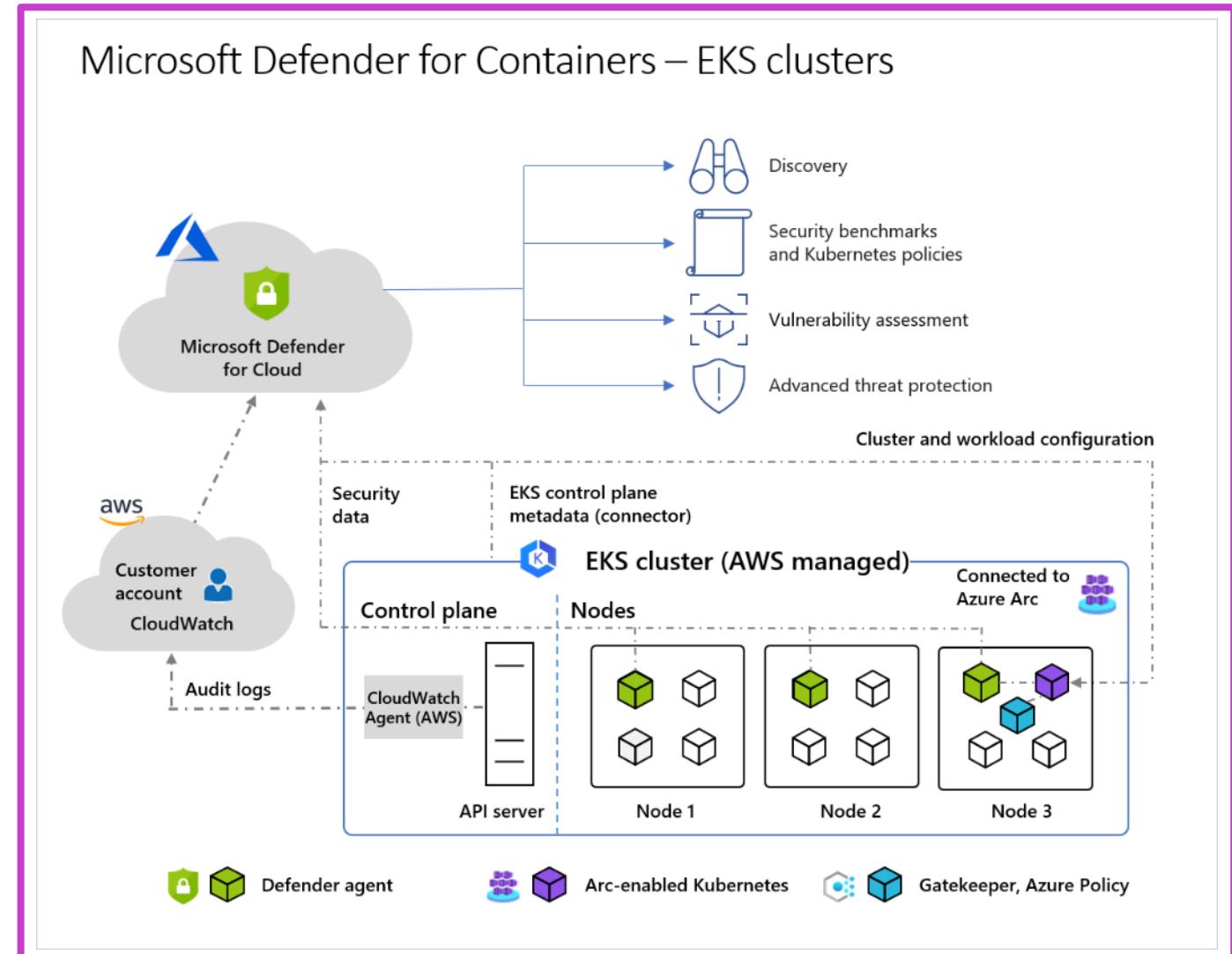
Architecture diagram of Defender for Cloud and Arc-enabled Kubernetes clusters

- 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.



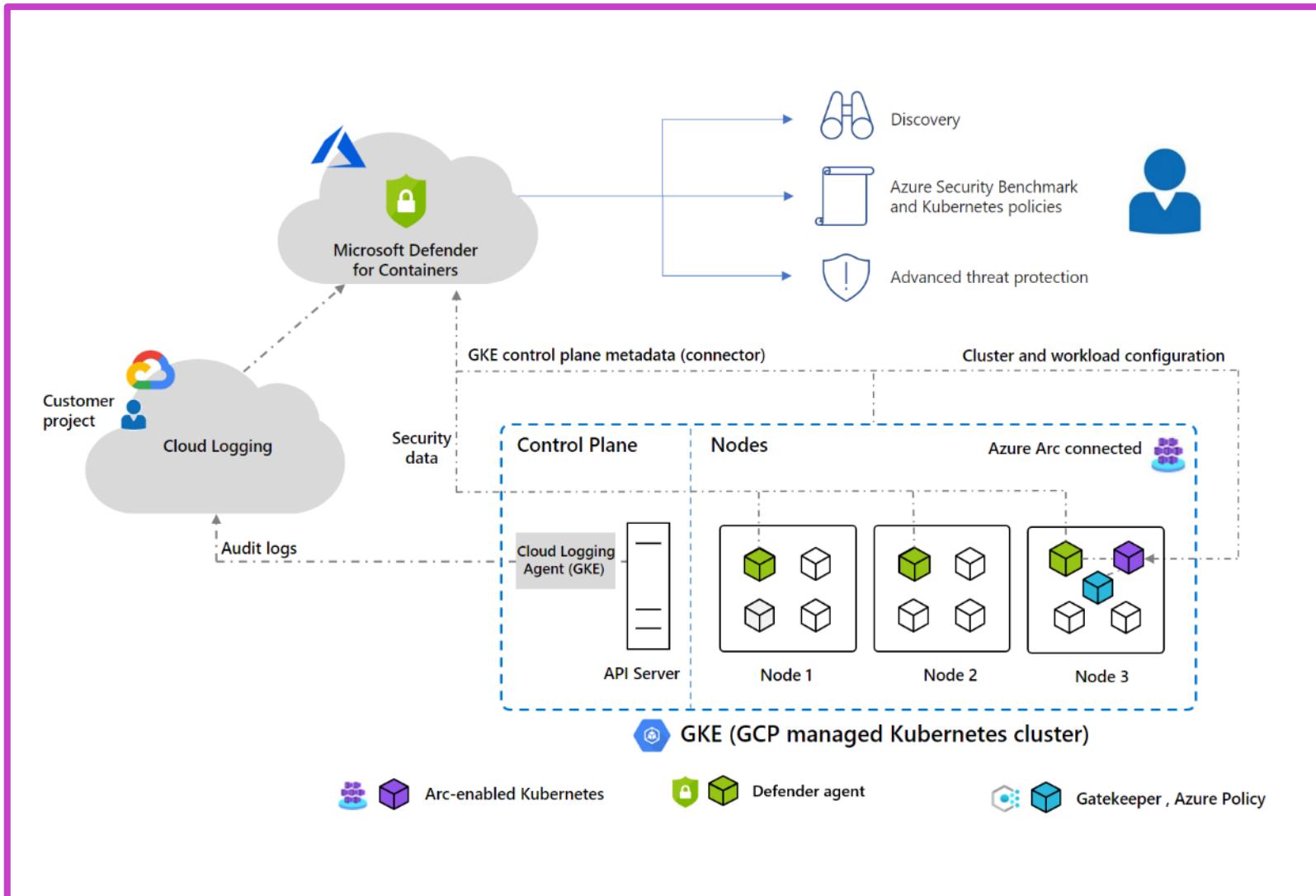
Architecture diagram of Defender for Cloud and EKS clusters

- 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

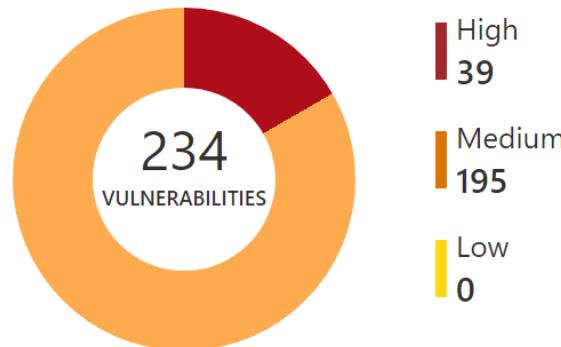
- Agentless audit log collection in GKE via GCP Cloud Logging.
- Azure Arc connects clusters to Defender for Cloud, enabling extensions.
- Extensions include Defender agent for runtime protection and Azure Policy for Kubernetes enforcement.



Defender for Cloud DevOps Security

Security Overview

DevOps security vulnerabilities ⓘ



DevOps security results

 **169**
Code scanning vulnerabilities

 **31**
OSS vulnerabilities

 **18**
Exposed Secrets

 **28**
Recommendations

DevOps coverage

 **1**
Github Connectors

30 Total

 Github repositories **27**

 Azure DevOps repositories **3**

 **1**
Azure DevOps Connectors

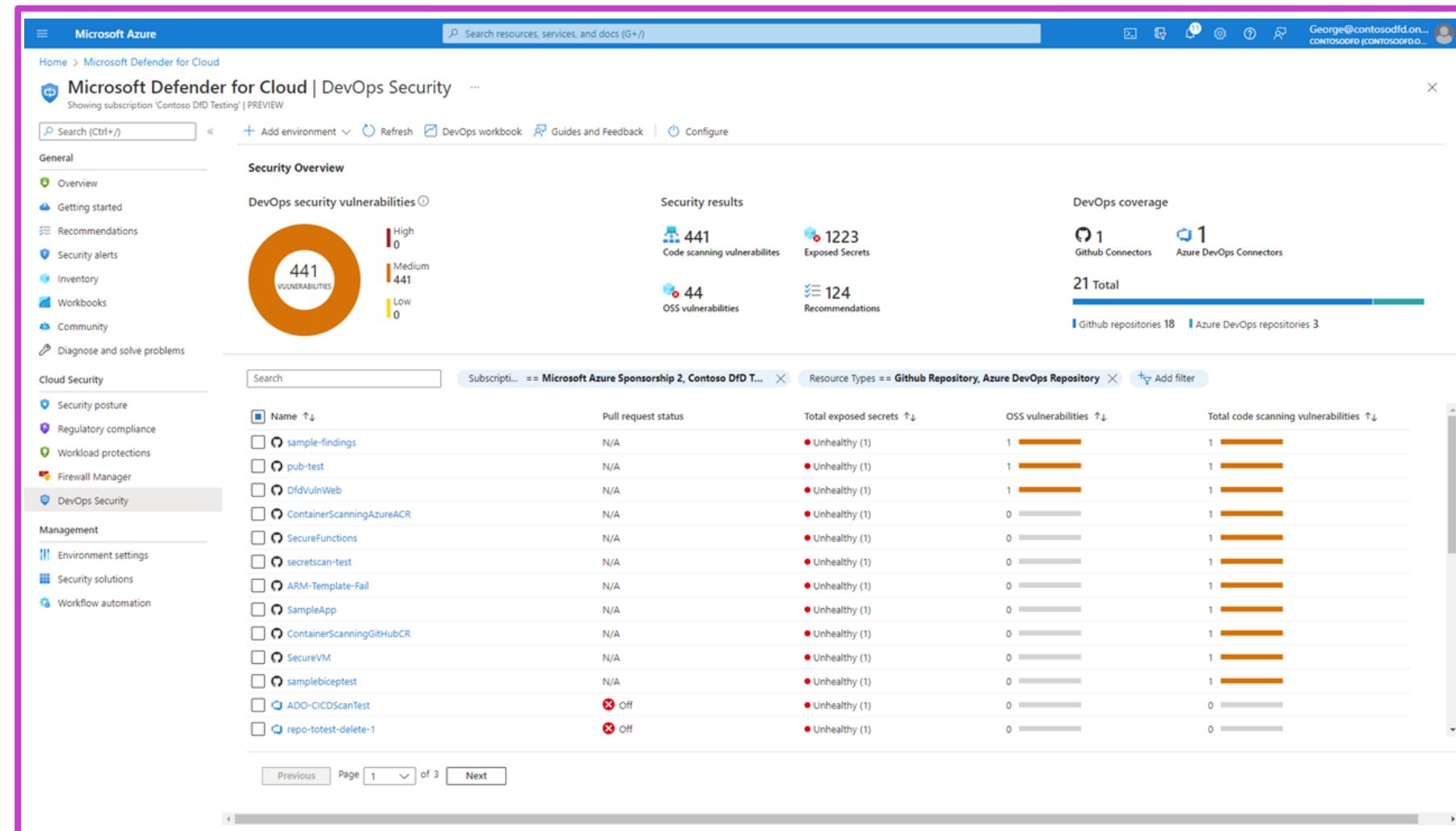
- Provides visibility, posture management, threat protection across Azure, AWS, GCP, on-premises.
- Centralizes DevOps security, integrates with Azure DevOps, GitHub, GitLab for application protection.
- Prioritizes code remediation with contextual insights, secures IaC templates, container images.

Defender for Cloud DevOps Security required permissions

Feature	Permissions
Connect DevOps environments to Defender for Cloud	<ul style="list-style-type: none">Azure: Subscription Contributor or Security AdminAzure DevOps: Project Collection Administrator on target OrganizationGitHub: Organization OwnerGitLab: Group Owner on target Group
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

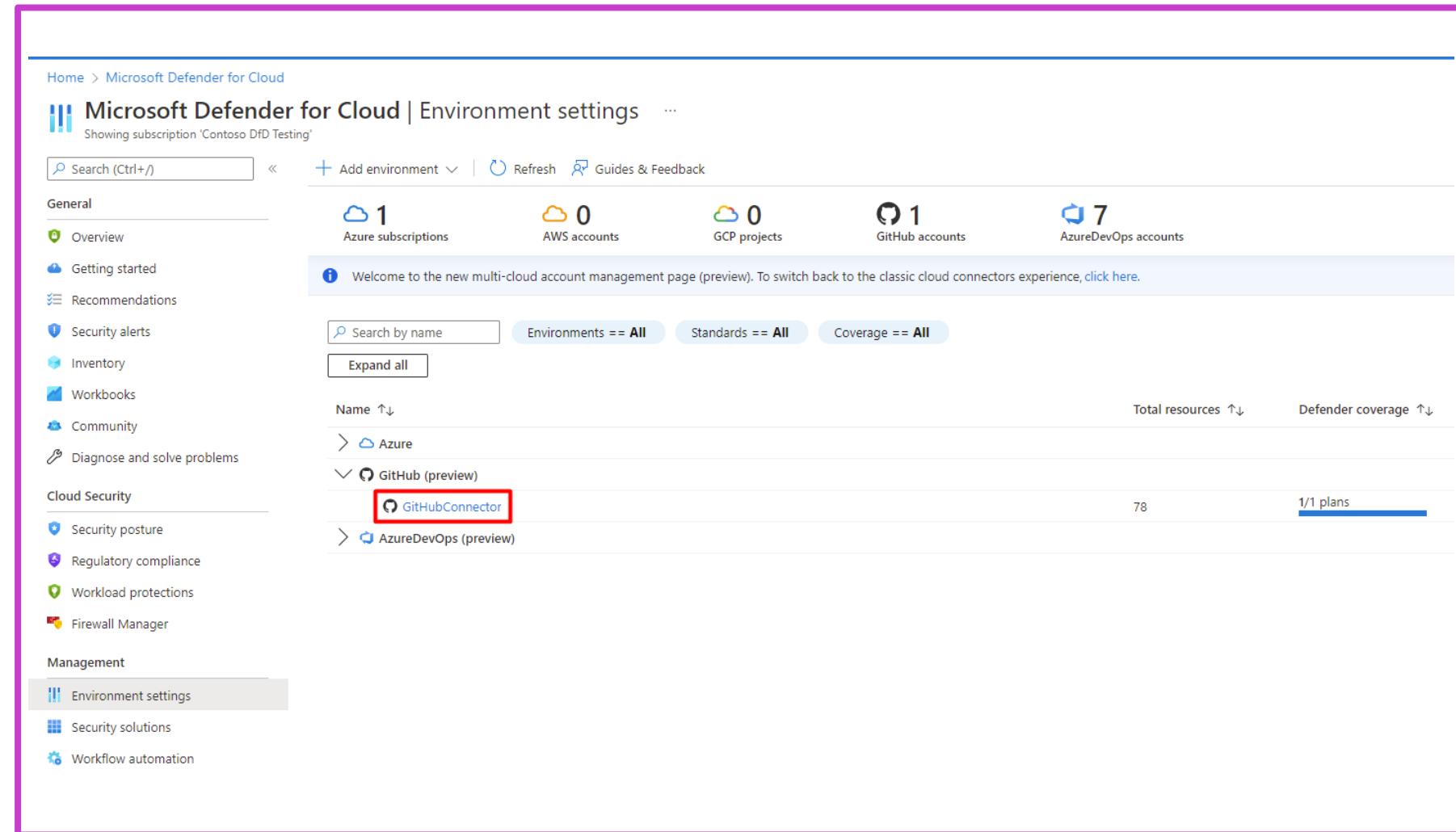
DevOps environment security posture

- 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.



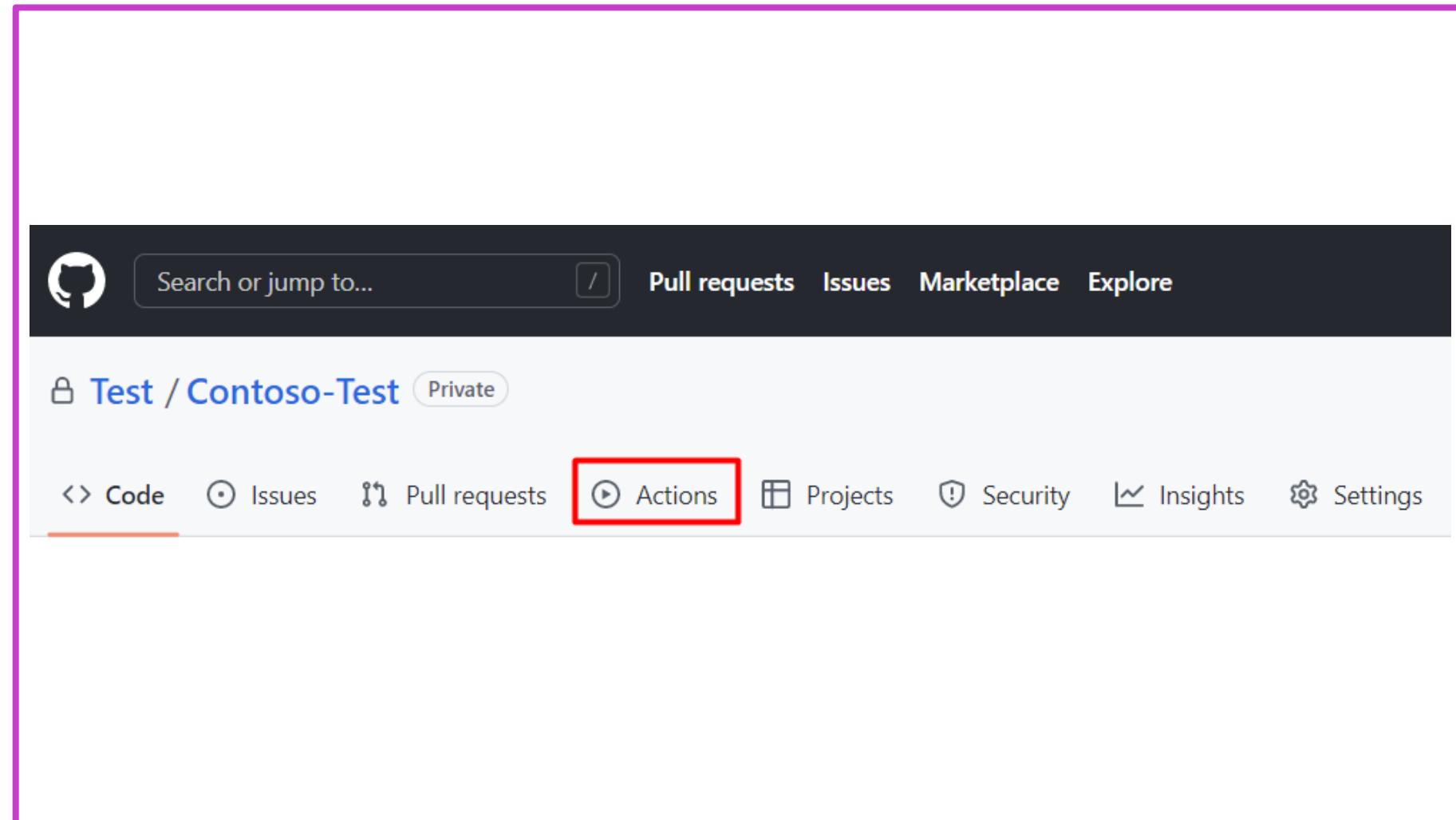
Connect your GitHub Environment to Defender for Cloud

- 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.



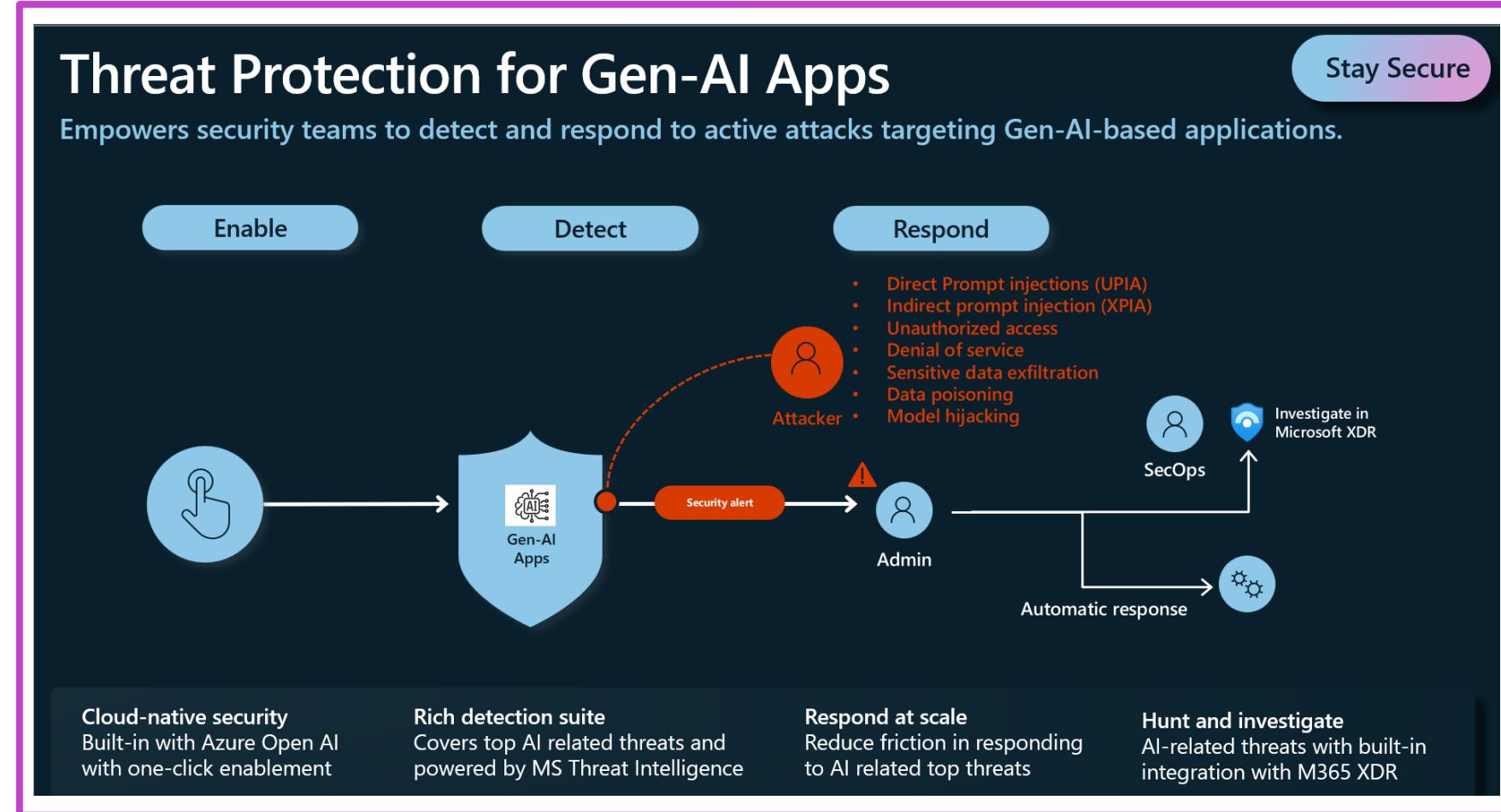
Configure the Microsoft Security DevOps GitHub action

- 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.

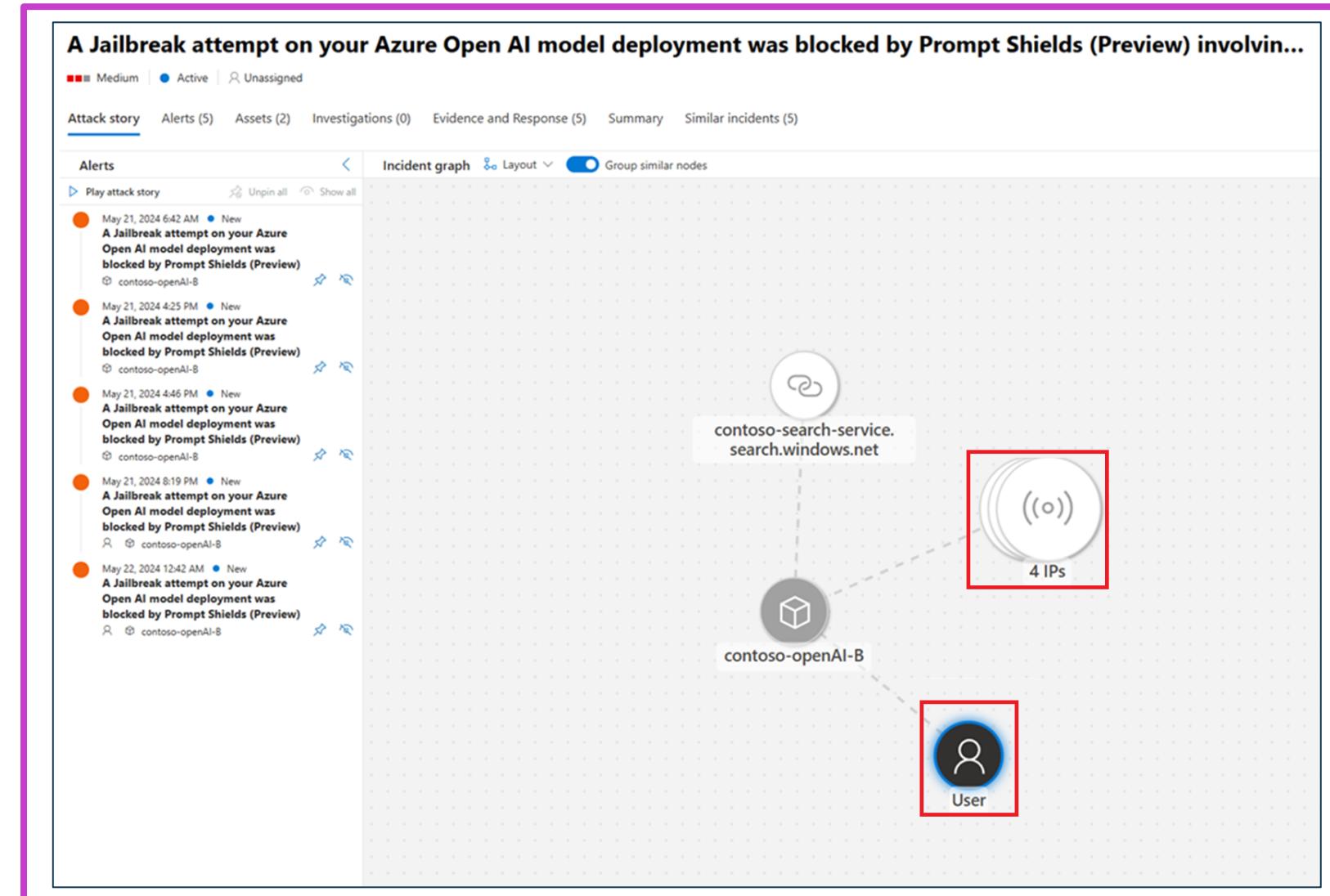
The screenshot shows the Microsoft Azure (Preview) portal with the URL [https://portal.azure.com/#blade/Microsoft_Azure_DefenderForCloud/EnvironmentSettingsBlade](#). The page is titled "Settings | Defender plans". On the left, there's a sidebar with "Settings" expanded, showing "Defender plans" selected. 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 table rows are:

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



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

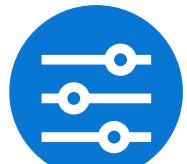
This section shows a list of security alerts with columns for Resource, Activity start time (UTC+2), and MITRE ATT&CK tactics. A modal dialog titled "Add filter" is open over the list, allowing users to refine their search by Alert name, Affected resource, Resource type, Tags, Creator, Owner, and environment.

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:



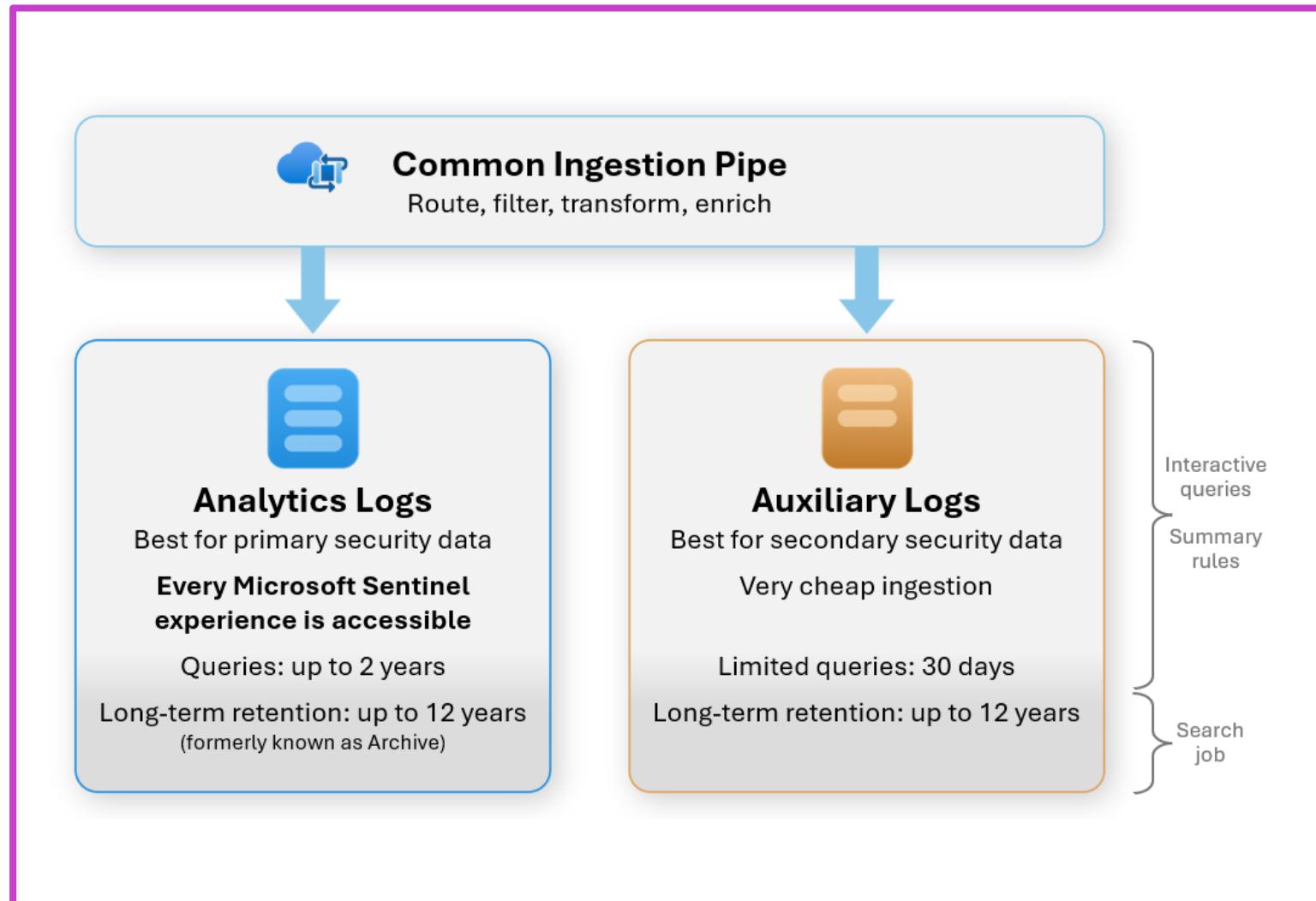
- Initiate a logic app in Defender for Cloud via **"Workflow automation."**
- Create, enable, or modify automation rules therein.
- Define a new workflow using **"Add workflow automation"** for details and triggers.
- Configure the Logic App through the **"Actions"** section.



- 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 Query Builder interface. The top navigation bar includes 'Home > Microsoft Sentinel' and 'Selected workspace: 'cybersoc''. The main area has a title 'Microsoft Sentinel | Logs' and a sub-section 'CyberSOC'. A query editor window titled 'New Query 1*' contains the following KQL code:

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

The 'Run' button is highlighted in blue. Below the query editor, there are tabs for 'Results' and 'Chart'. The 'Results' tab is selected, displaying a table with three columns: 'DataType', 'MBytes', and 'KBytes'. The table contains 11 rows of data. At the bottom of the results table, it says '6s 596ms | Display time (UTC+00:00) ▾' and 'Query details | 1 - 11 of 1342'.

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.

The screenshot shows the 'Analytics rule wizard - Create new rule' interface. The 'General' tab is selected and highlighted with a red box. The page includes fields for 'Name *', 'Description', 'Tactics and techniques' (with a dropdown showing '0 selected'), 'Severity' (set to 'Medium'), and 'Status' (set to 'Enabled'). At the bottom is a 'Next : Set rule logic >' button.

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

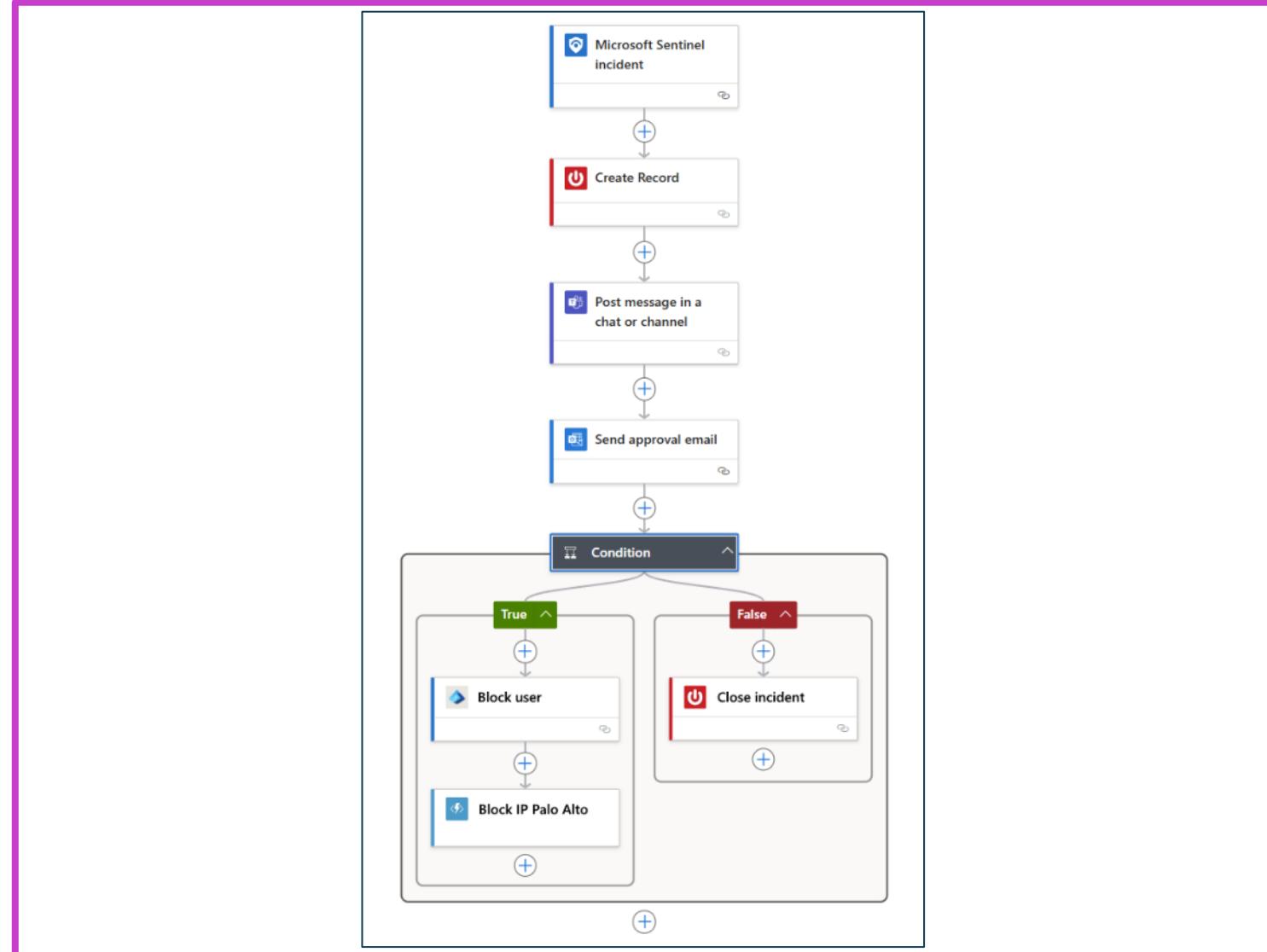
Using a playbook, you can:

- 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.



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



The screenshot shows the Azure Log Analytics workspace overview for 'law-1'. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs, Resource visualizer, Settings, Classic, Monitoring, Automation, and Help. The main content area displays workspace details: Resource group (az-rg-1), Status (Active), Location (East US), Subscription (Azure subscription), and Tags (Add tags). A note at the top states: '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.' Below this, there's a 'Get Started' section with three steps: 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), and 3. Monitor workspace health (Create alerts to proactively detect any issue that arise in your workspace). The right side of the screen shows workspace statistics: View Cost, JSON View, 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), and Operational issues (OK). A 'Useful links' section at the bottom right includes Documentation site and Community.

[Launch this Exercise in GitHub](#)

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.



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.

Plan selection

Defender for servers is offered in two plans.
Plan 1 provides a limited set of defenses with a focus on Defender for Endpoint's protections.
Plan 2 includes the full set of our enhanced security features for servers.
[Learn more](#)

Microsoft Defender for Servers Plan 2 \$15/Server/Month

Plan details

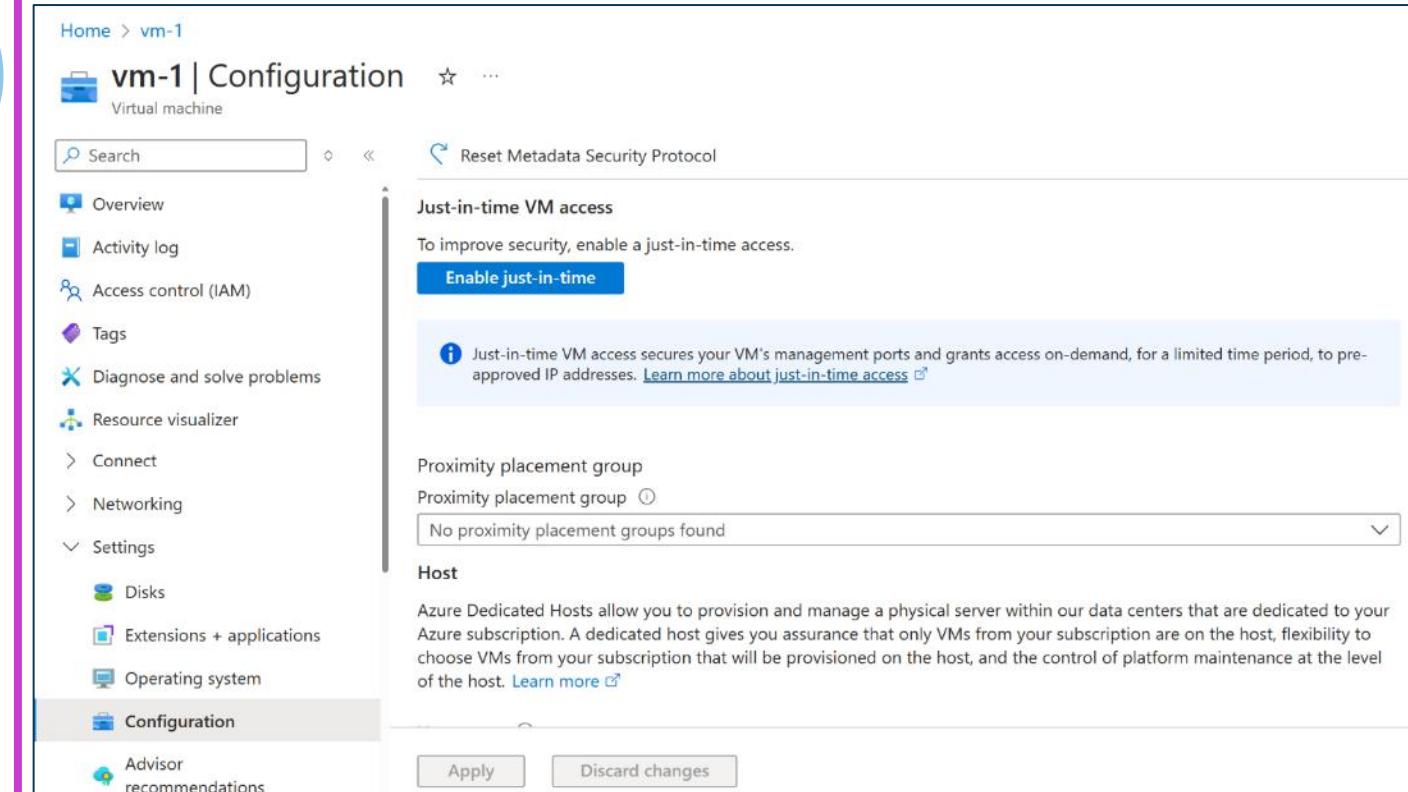
- Microsoft Defender for Endpoint
- Microsoft Defender vulnerability management
- Automatic agent onboarding, alert and data integration
- Generates detailed, context-based, security alerts easily integrated with any SIEM
- Provides guidelines to help investigate and mitigate identified threats
- Agentless VM vulnerability scanning [Learn more](#).
- Agentless VM secrets scanning [Learn more](#).
- Agentless malware detection (preview)
- Control plane security alerts
- Resolve missing software updates gaps with Azure Update Manager (Free for Plan 2 Arc machines)
- Regulatory compliance and industry best practices
- Just-in-time VM access for management ports
- Network layer threat detection
- File integrity monitoring
- Baselines assessment
- Log Analytics 500MB free data ingestion

[Launch this Exercise in GitHub](#)

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](#)



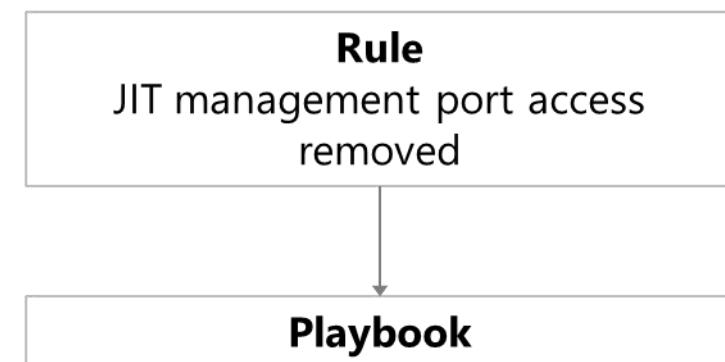
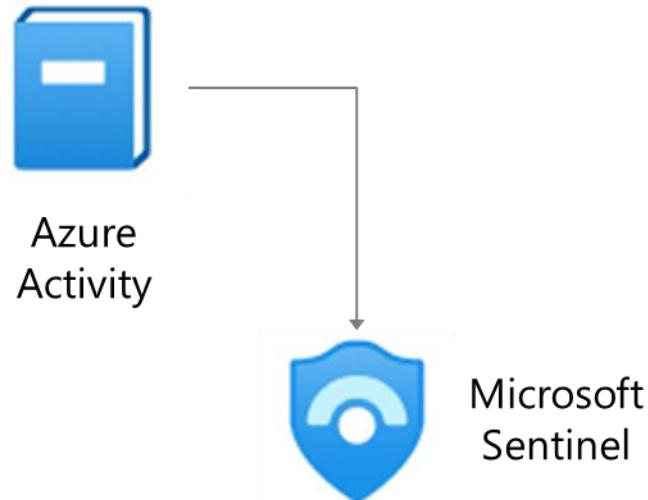
The screenshot shows the Azure portal interface for managing a virtual machine named 'vm-1'. On the left, there is a sidebar with various navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings (which is currently selected), Disks, Extensions + applications, Operating system, Configuration (which is also selected), and Advisor recommendations. The main content area displays the 'Configuration' tab for 'vm-1'. A prominent section titled 'Just-in-time VM access' contains the message: 'To improve security, enable a just-in-time access.' Below this is a blue 'Enable just-in-time' button. A tooltip 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](#)



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