Microsoft

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

Dashboard

Workbook

Kusto Query Lang

Lab 7

KQL

Lab 8

LA Workspace

Monitoring

Defender Cloud

Datalake

SIEM Microsoft Sentinel Blob

Table

30 Tage

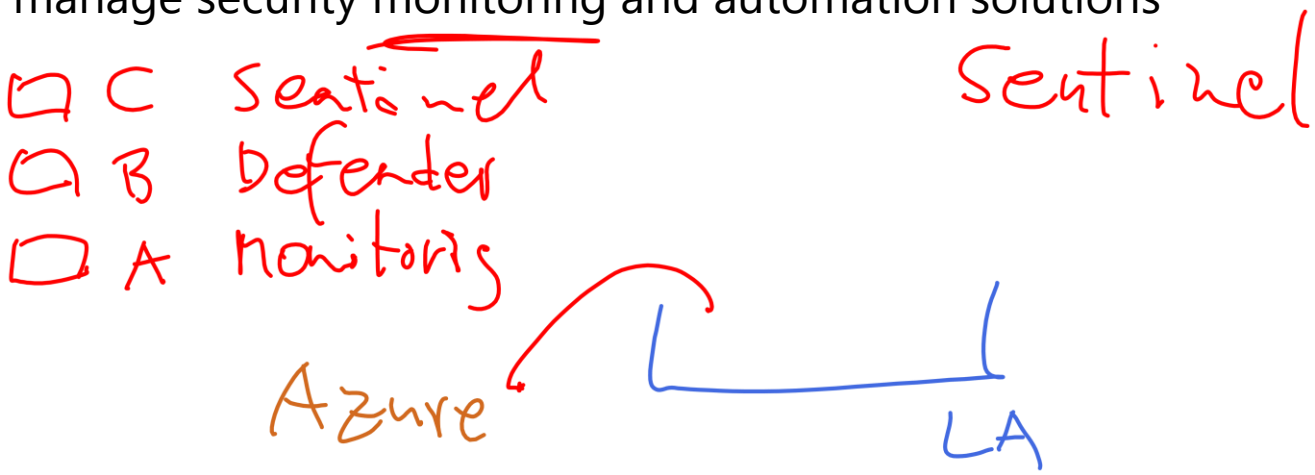
Learning Path: Secure Azure using Microsoft Defender for Cloud and Microsoft Sentinel

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



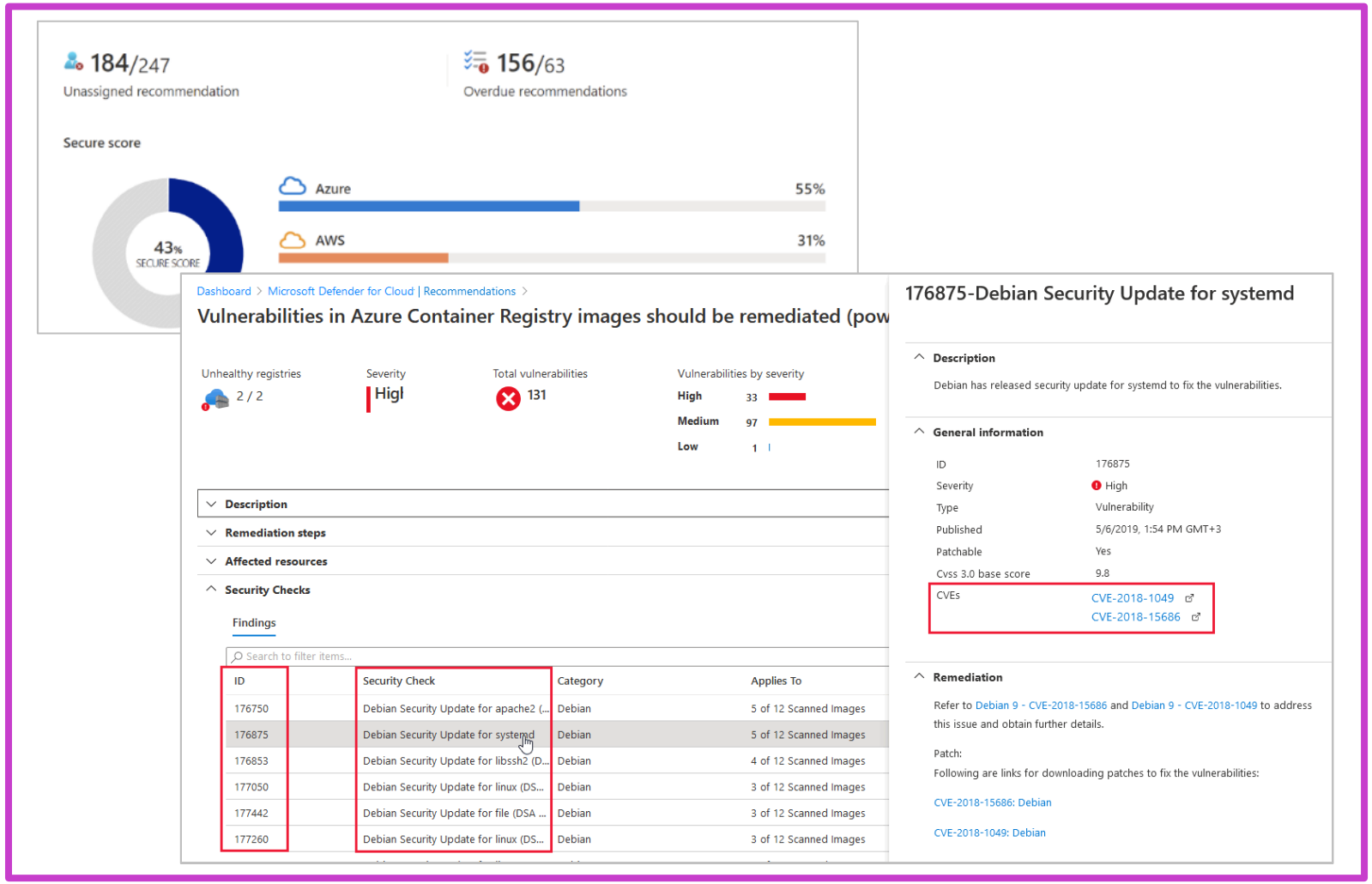
Manage security posture by using Microsoft Defender for Cloud

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.

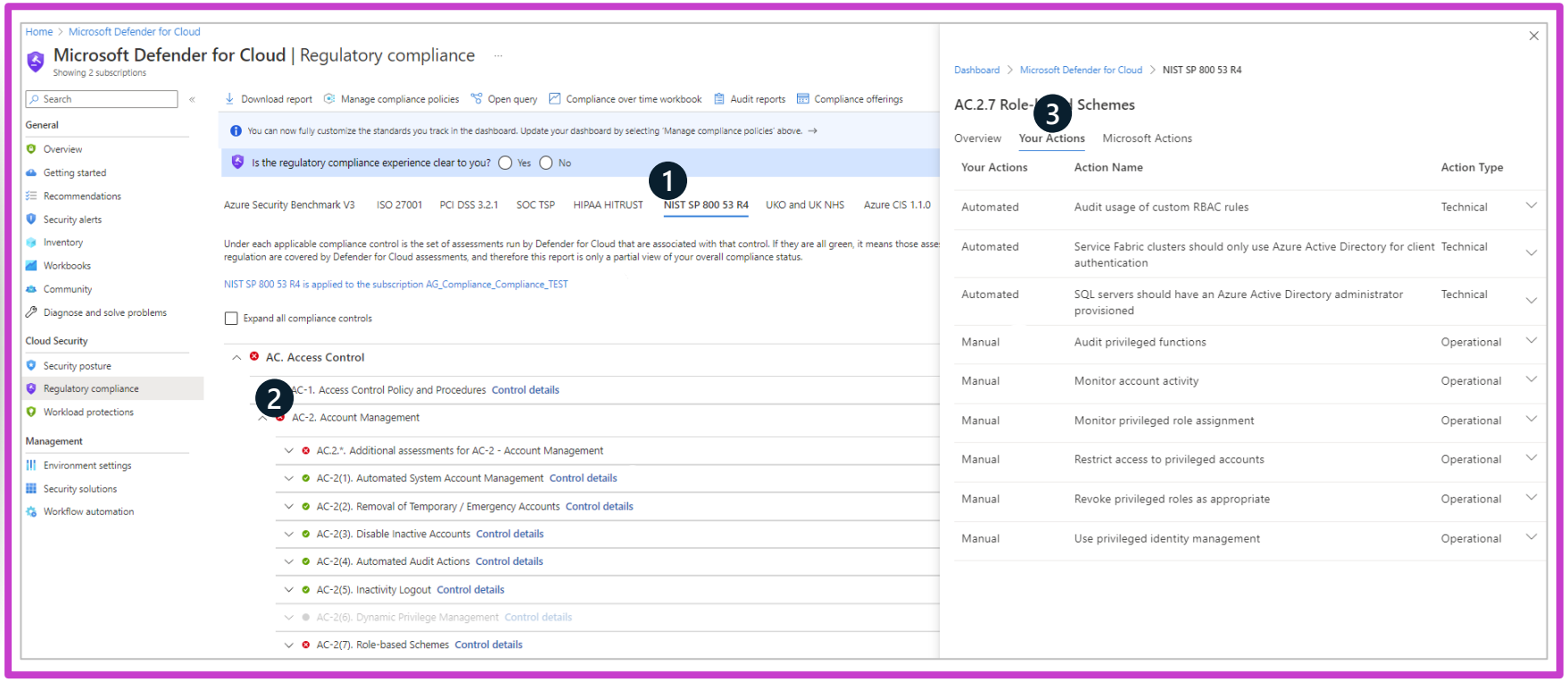
Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory

- 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.



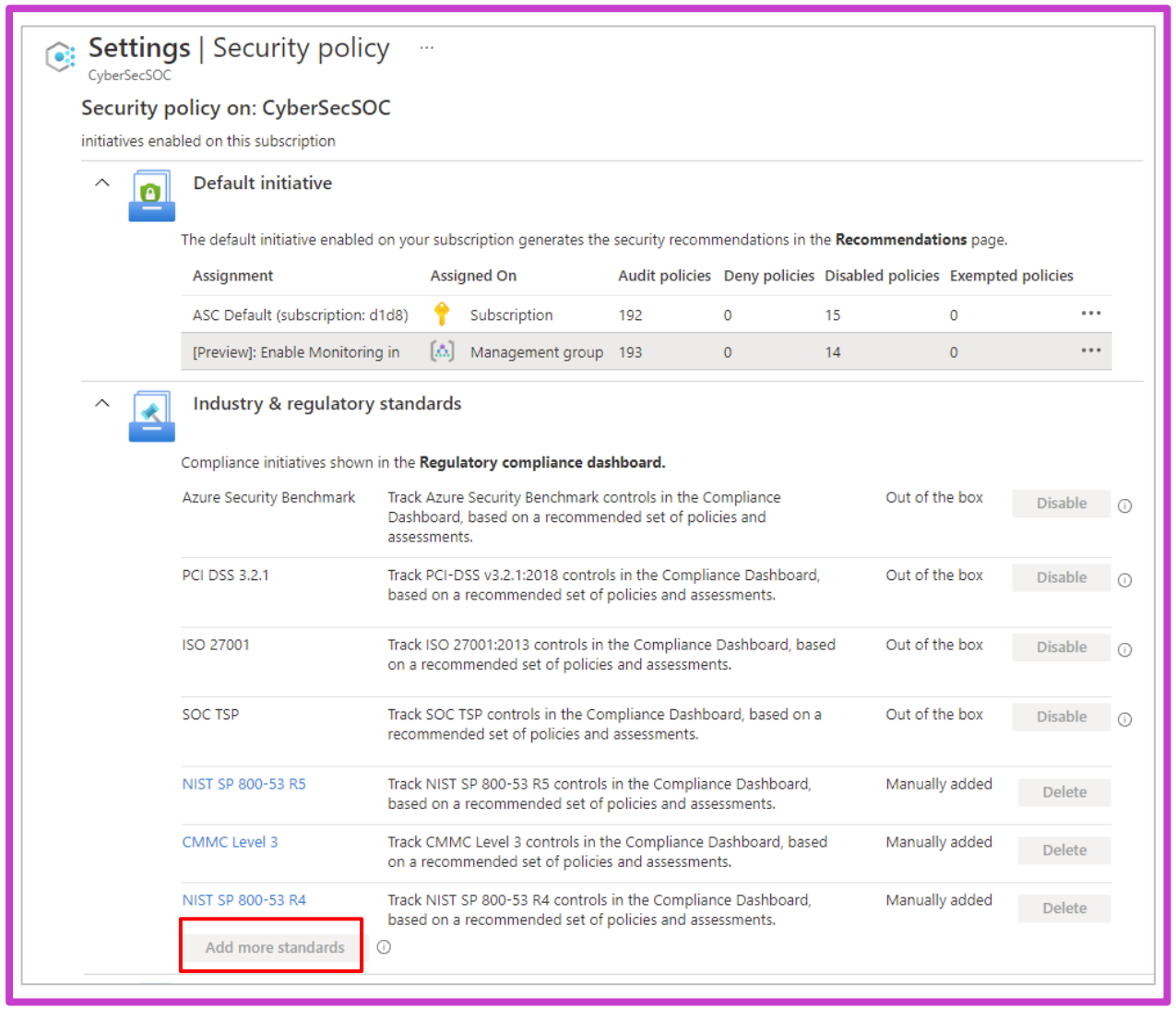
Assess compliance against security frameworks and Microsoft Defender for Cloud

- 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.



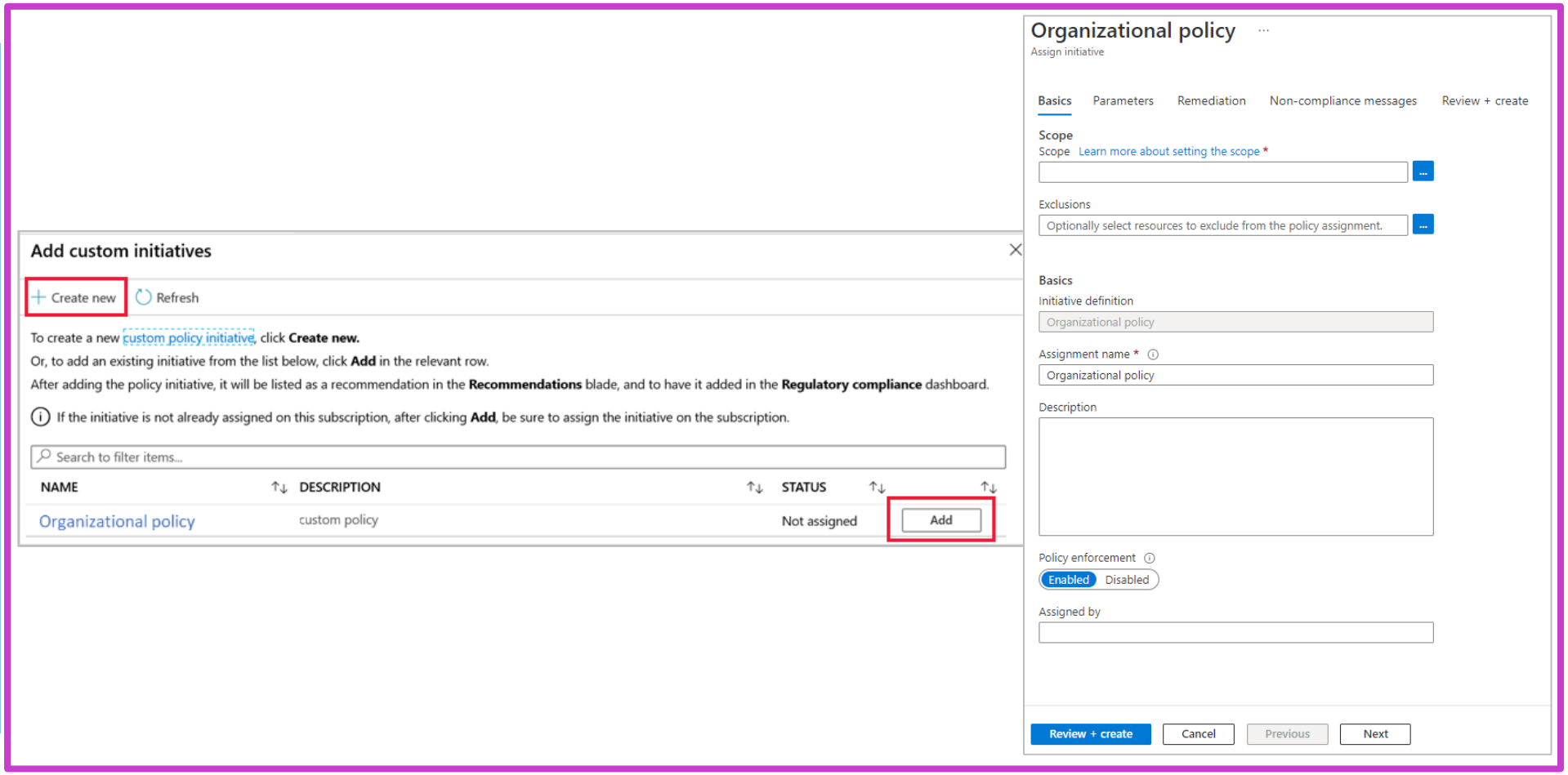
Manage compliance standards Microsoft Defender for Cloud

- 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



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



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:

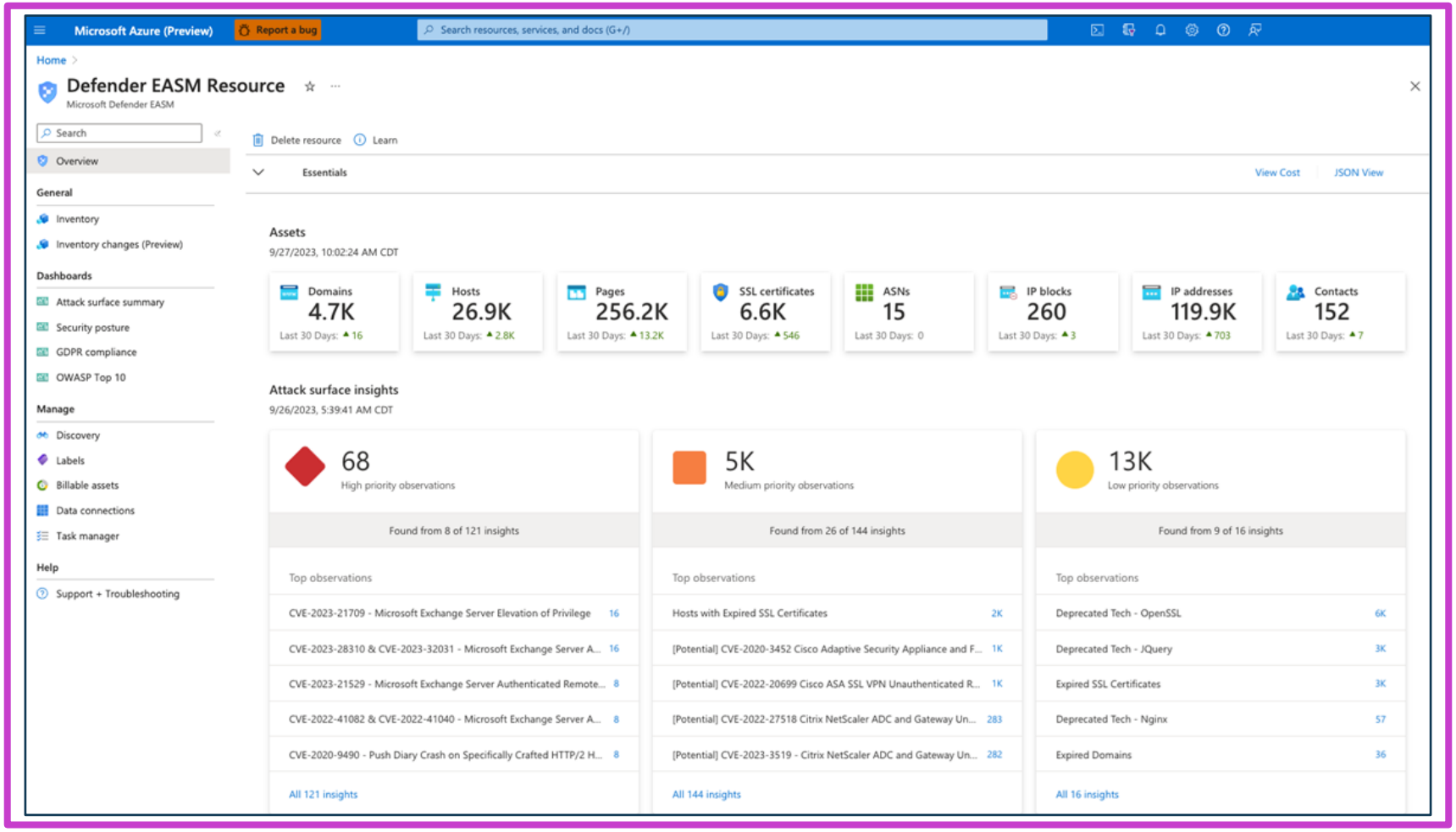
- Native cloud connector (recommended)
- Classic connector

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

- Continuous Discovery: Defender EASM maps your attack surface, identifying unknown assets and potential vulnerabilities.

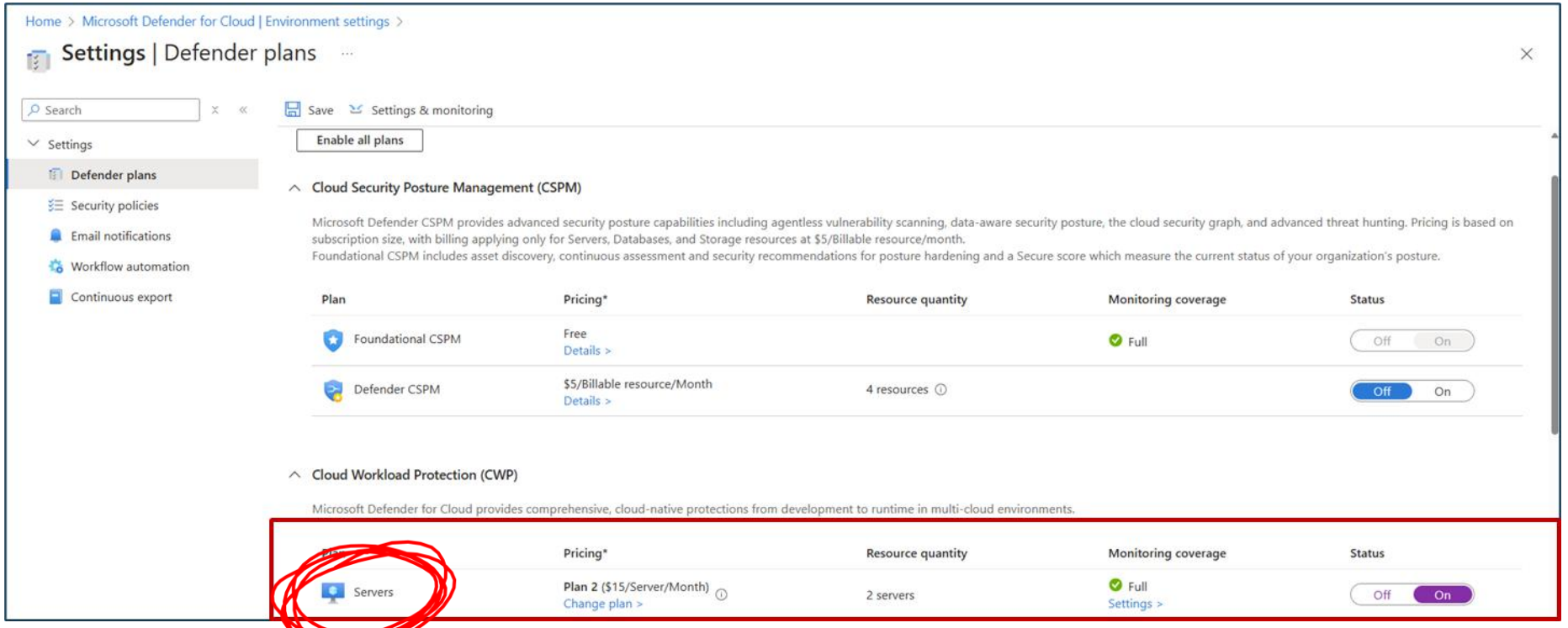
- Risk Insights: Dashboards highlight vulnerabilities, compliance gaps, and high-risk components for prioritized remediation.

- 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

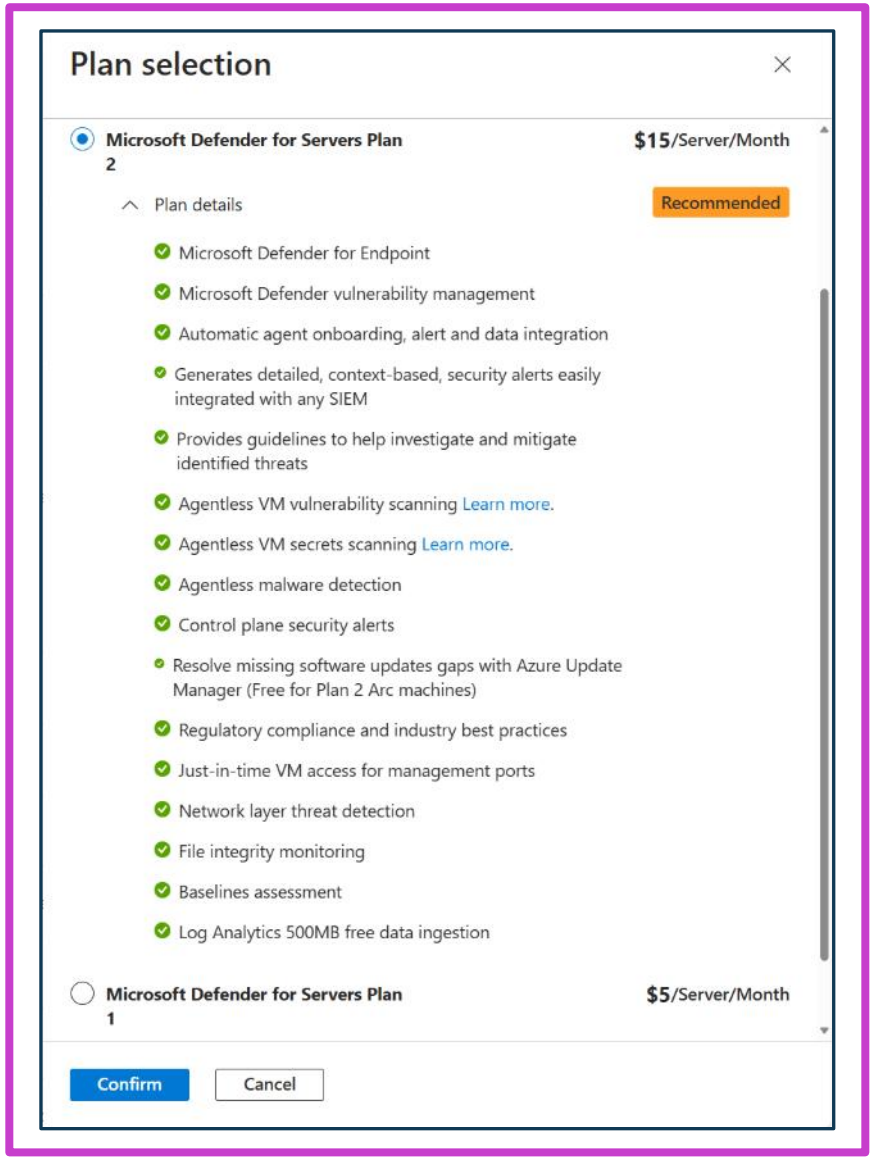
Enable workload protection services in Microsoft Defender for Cloud



- 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.

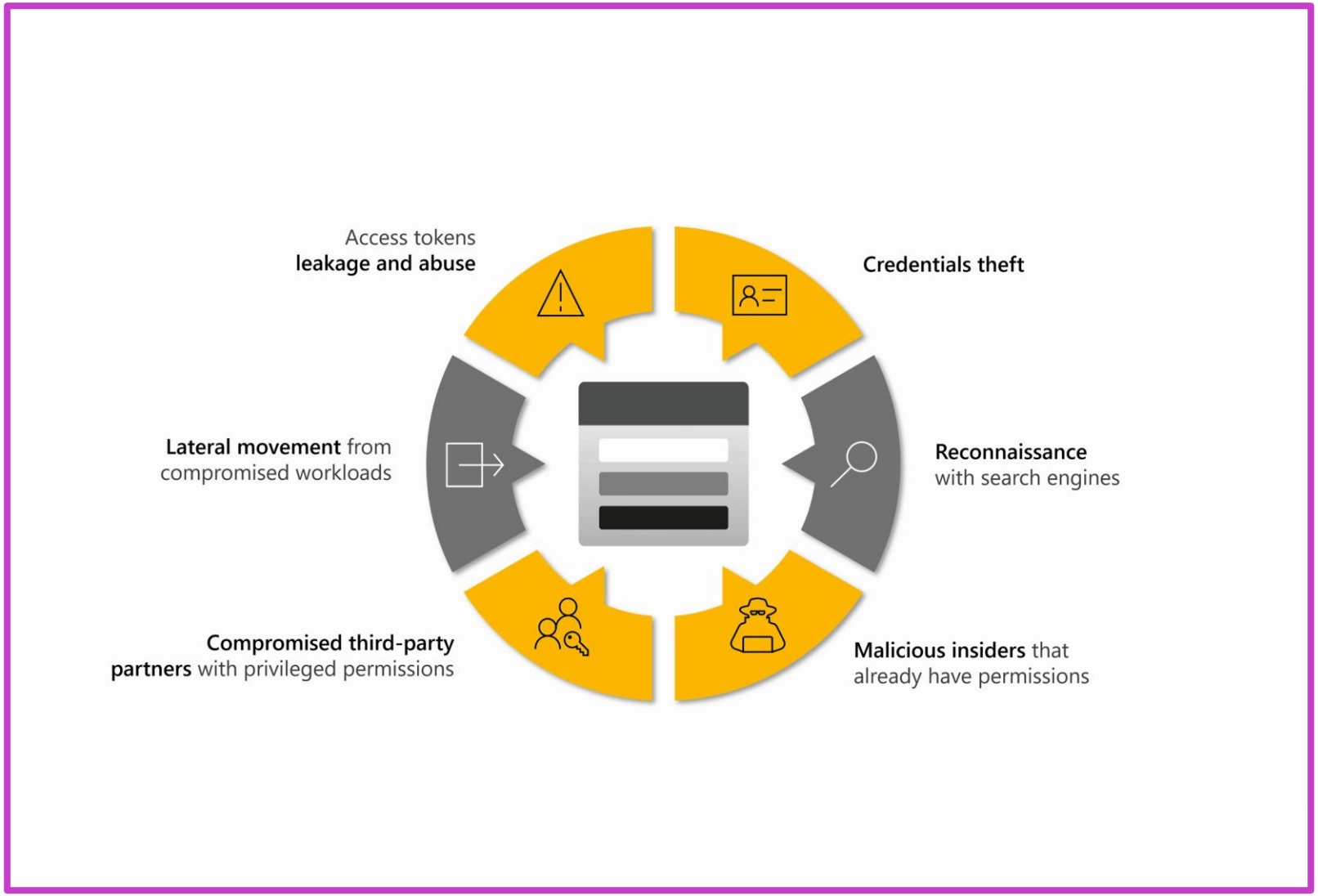
Microsoft Defender for Servers

- 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.



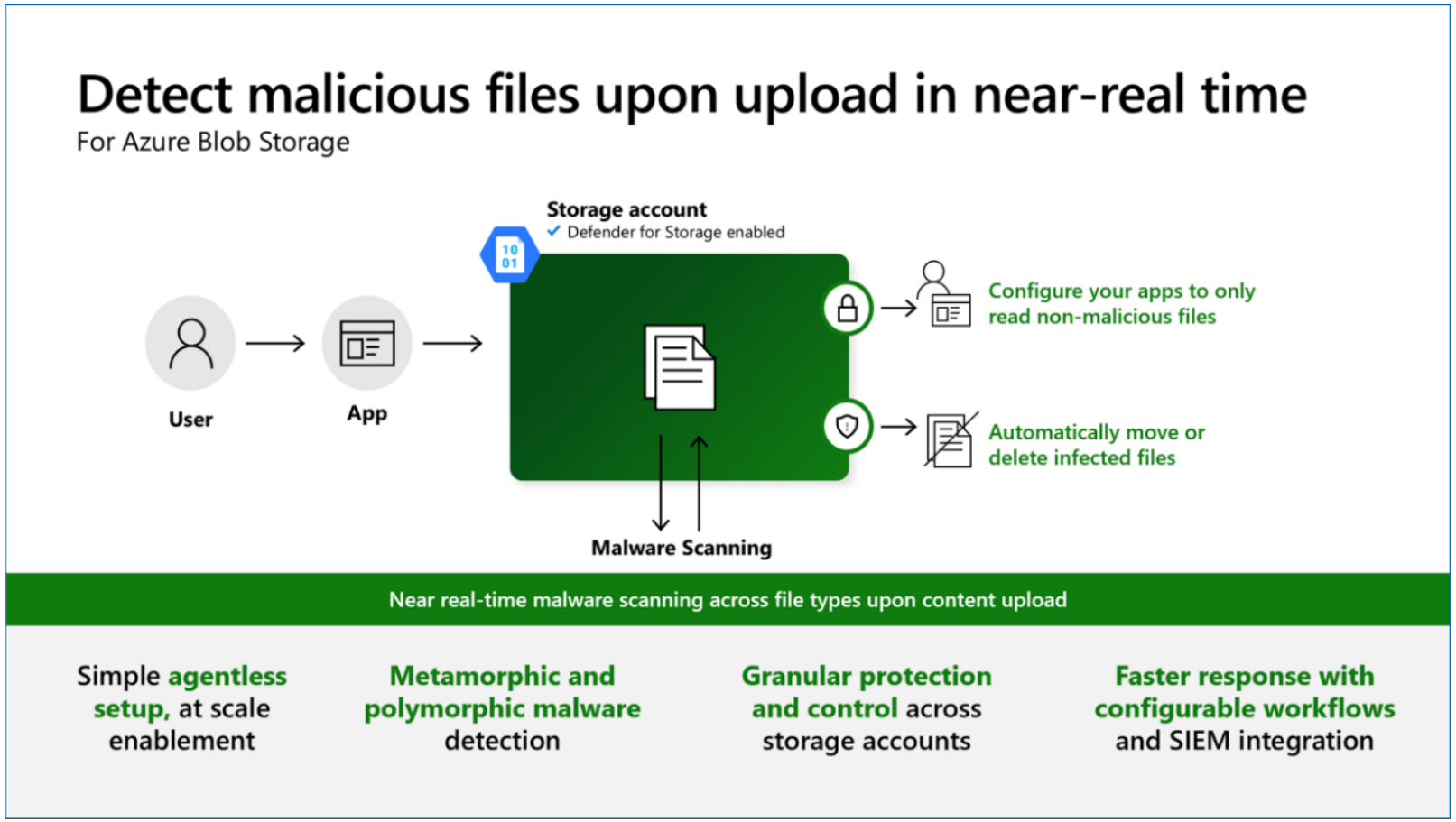
Microsoft Defender for Storage

- 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.



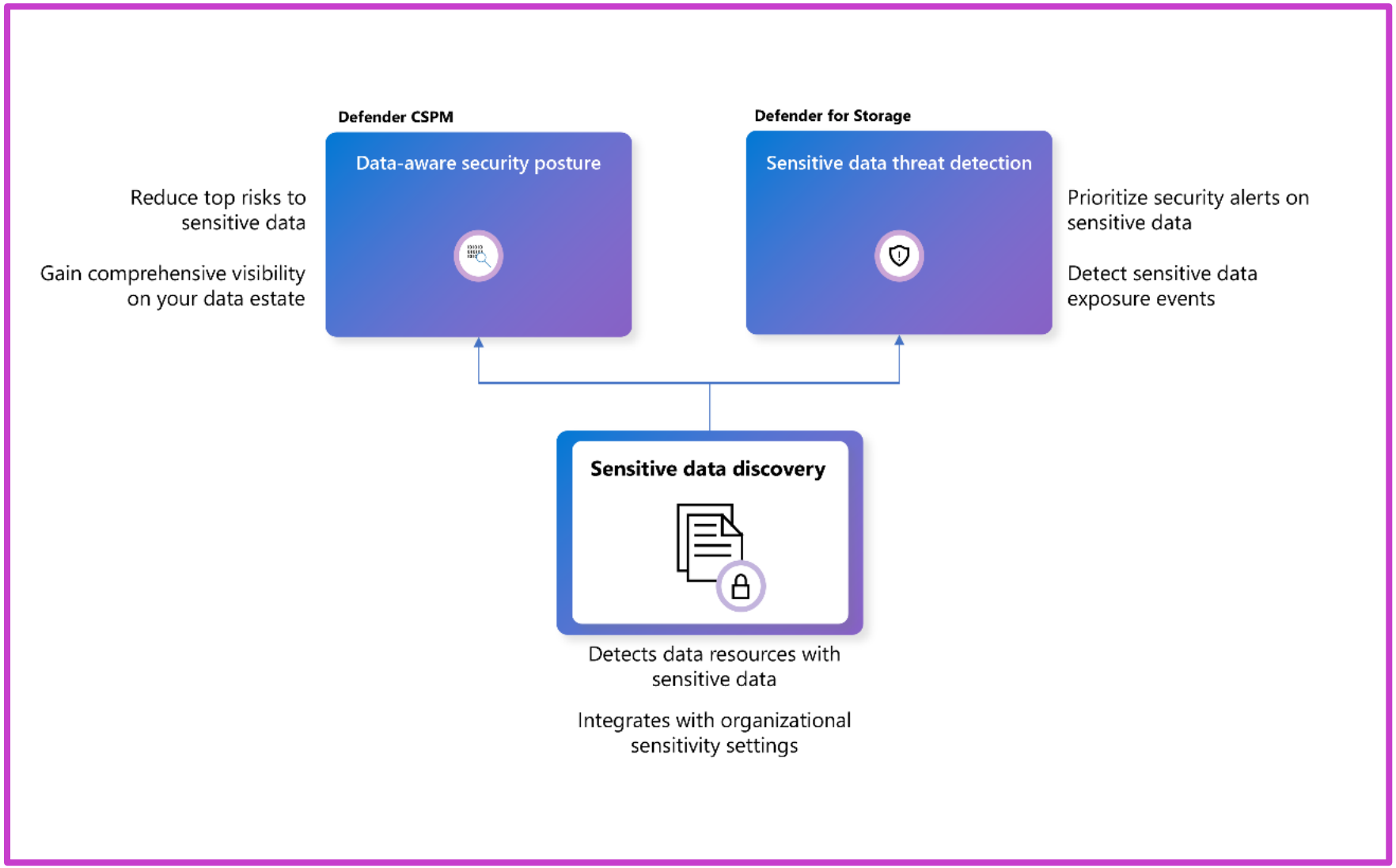
Malware scanning in Defender for Storage

- 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.



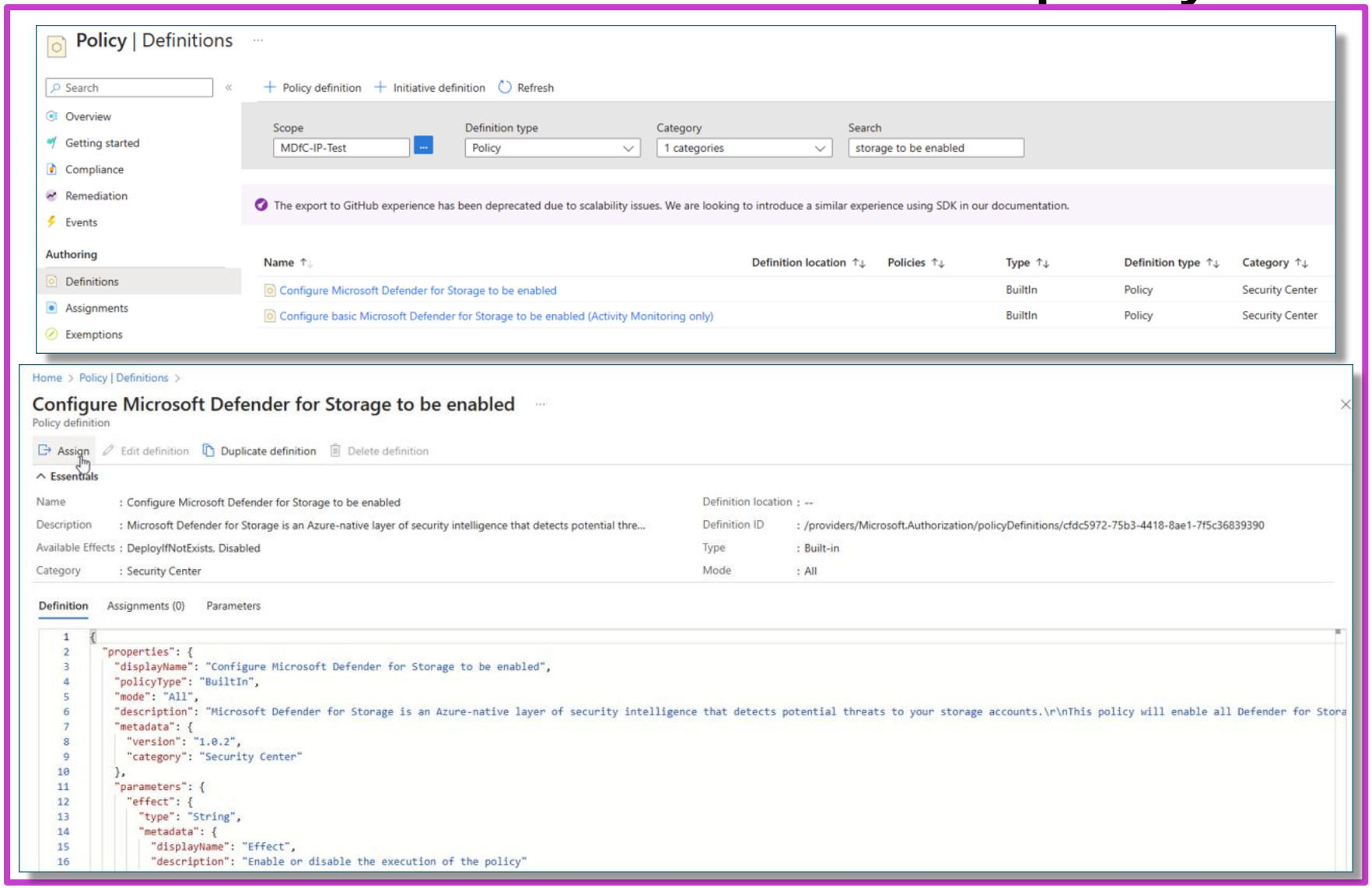
Detect threats to sensitive data

- 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.

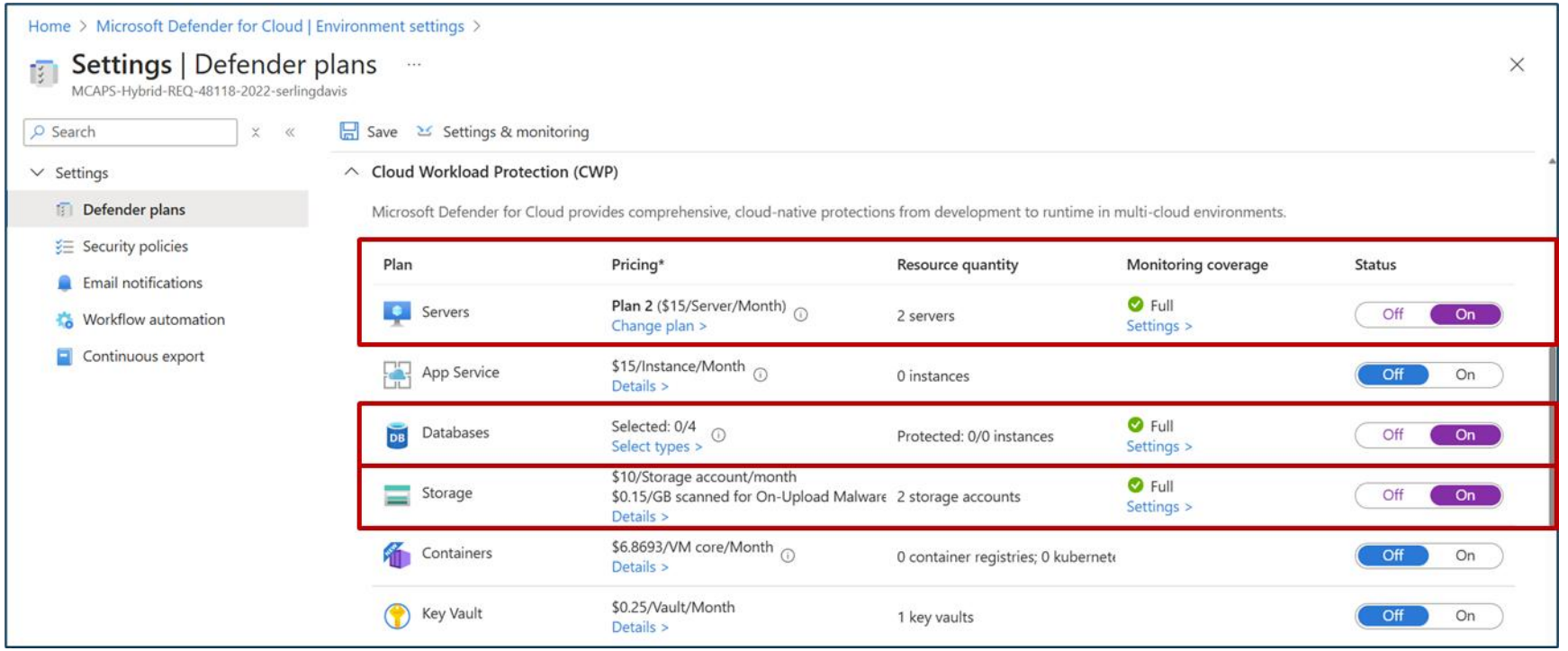


Enable and configure at scale with an Azure built-in policy

- 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.

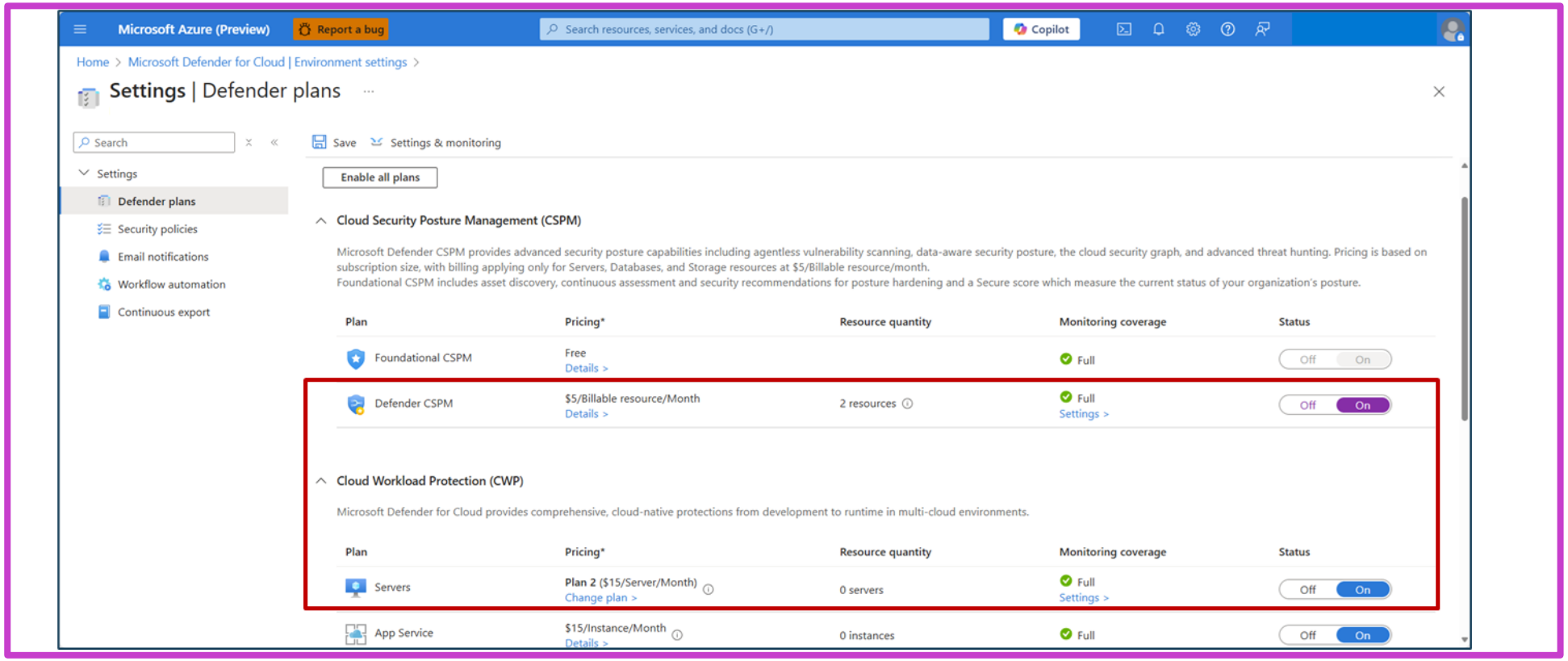


Configure Microsoft Defender for Servers, Microsoft Defender for Databases, and Microsoft Defender for Storage



- 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

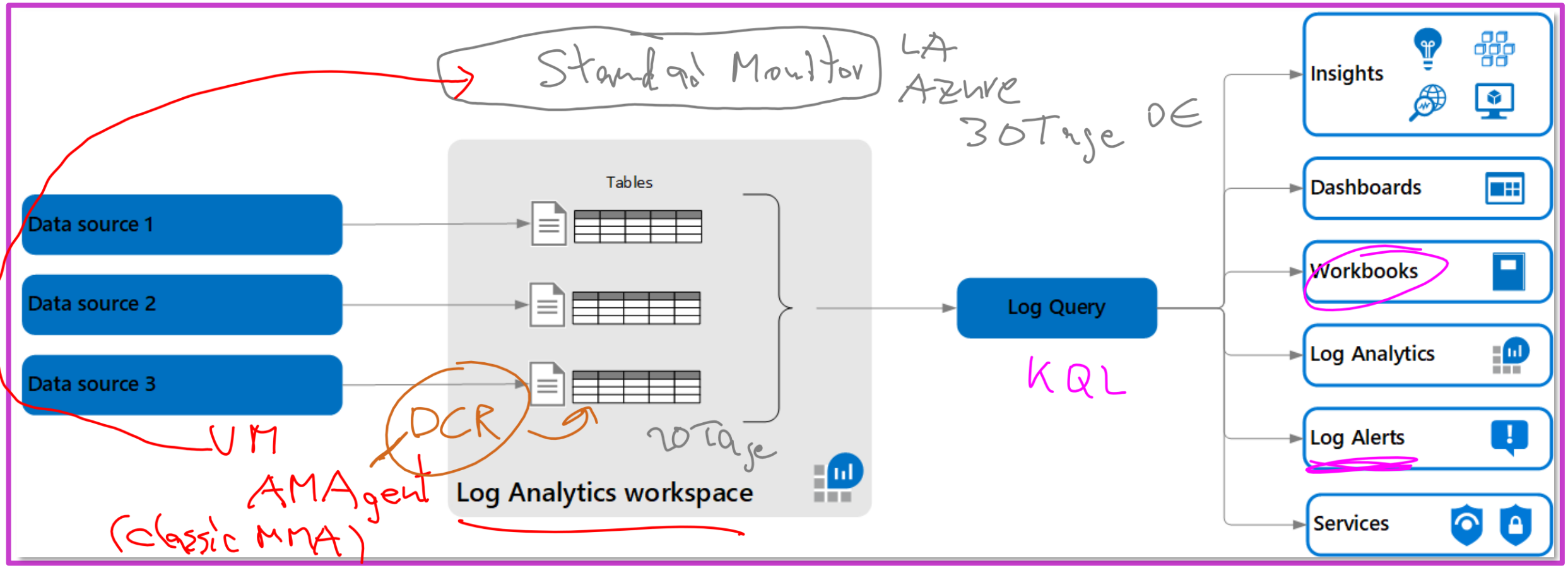


- Enhanced Security: Scans for vulnerabilities, malware, secrets, and software inventory across connected environments.
- Seamless Integration: No agents or connectivity needed, supports Azure, AWS, GCP, and Kubernetes nodes.
- Easy Enablement: Enabled by default in Defender CSPM or Servers Plan 2, with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

Implement and manage Microsoft Defender Vulnerability Management for Azure

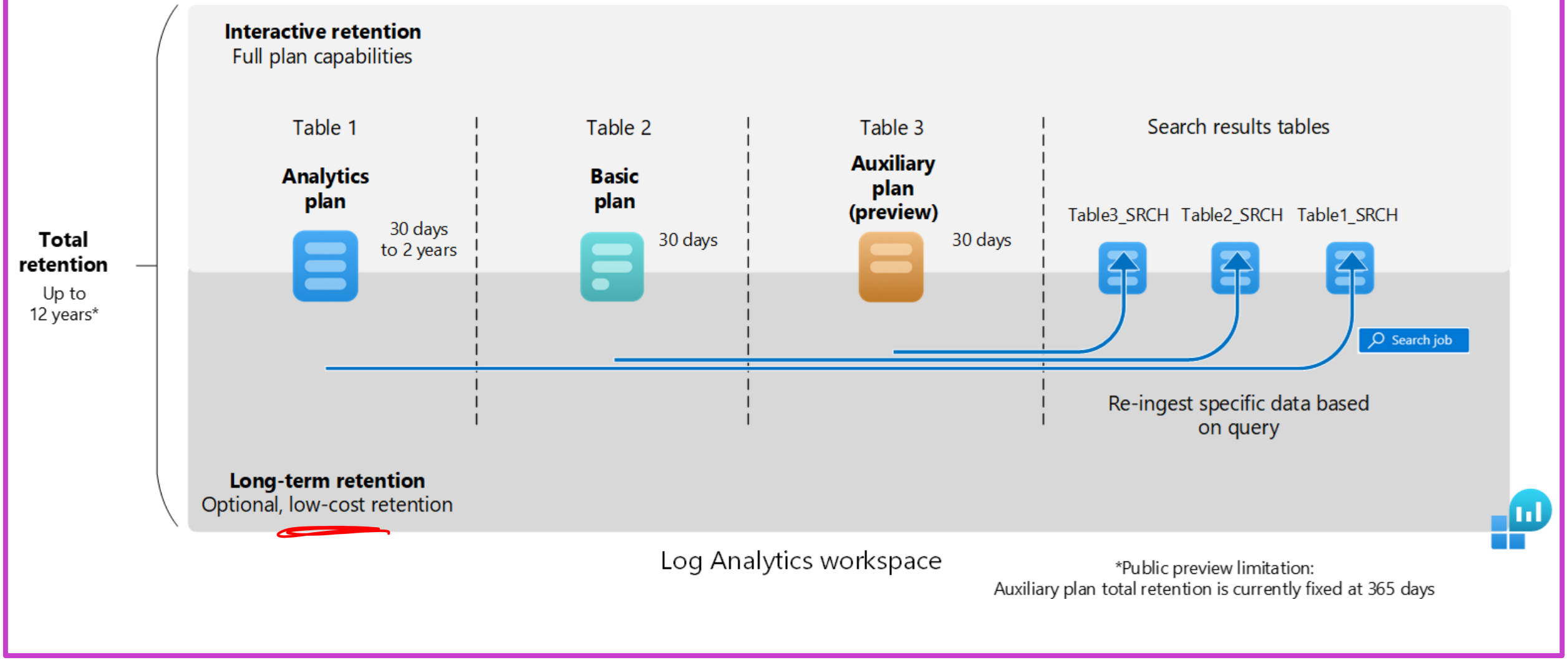
- Automatically scans ACR images for vulnerabilities without any agent deployment.
- Supports OS and language package scanning with continuous daily rescans.
- Provides detailed vulnerability reports and remediation recommendations for secure deployments.

Log Analytics workspace



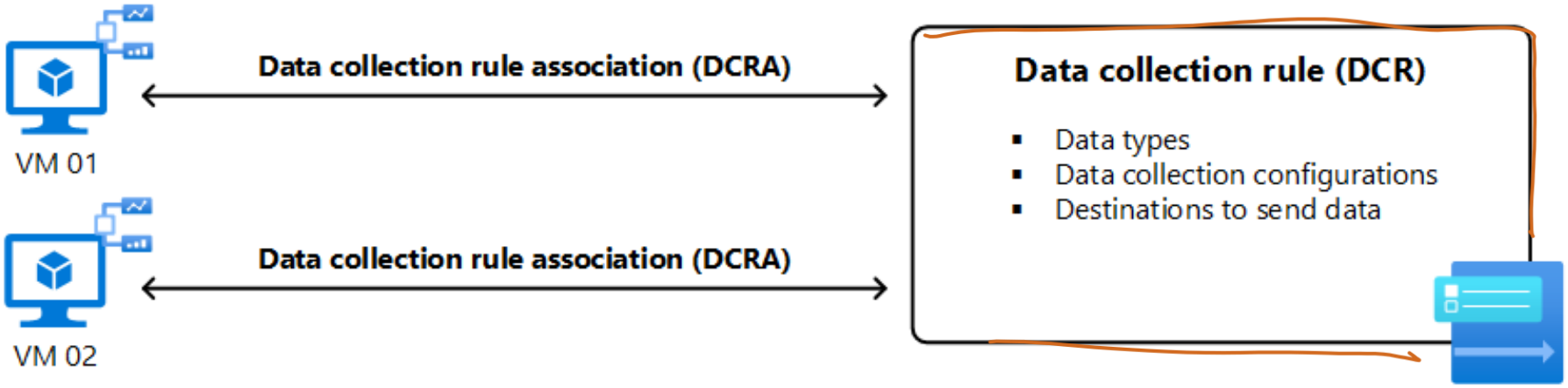
- A Log Analytics workspace is a centralized, configurable environment for Azure Monitor log data, allowing data collection and retention management across multiple Azure services.

Manage data retention in a Log Analytics workspace

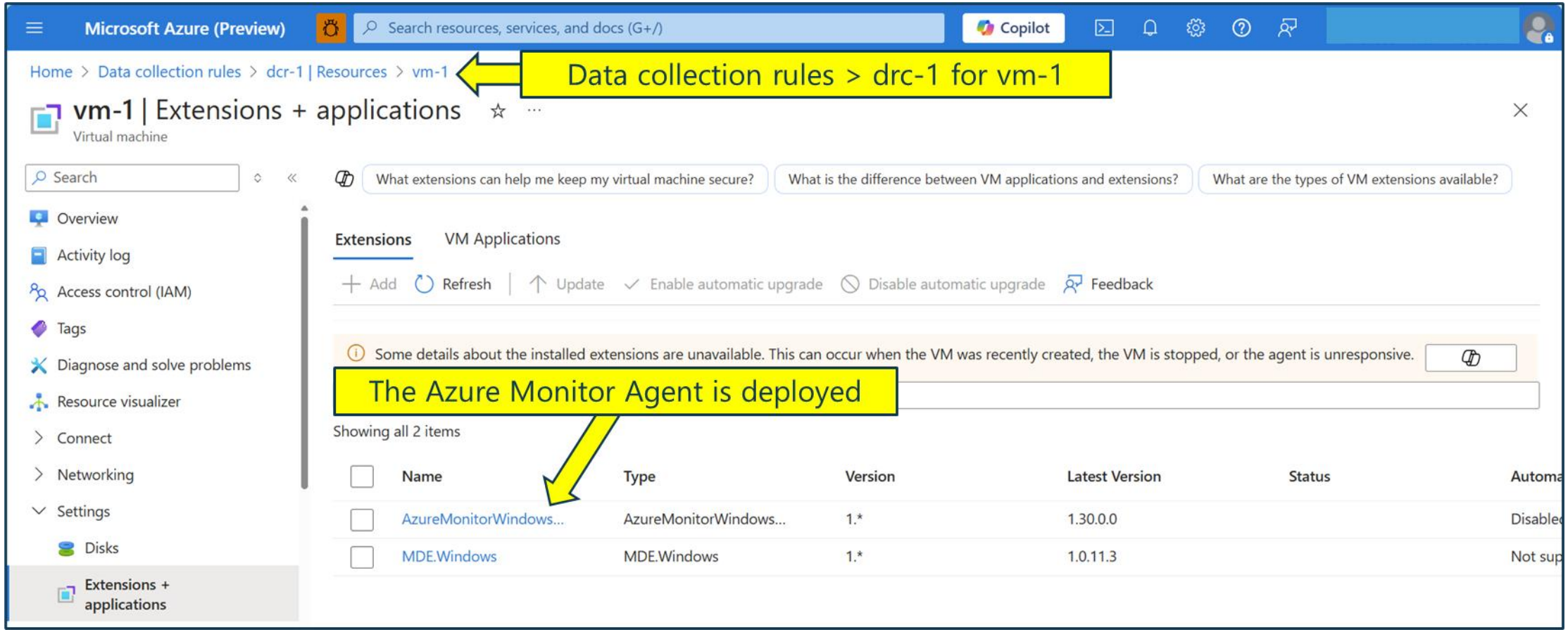


Deploy the Azure Monitor Agent

- 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.

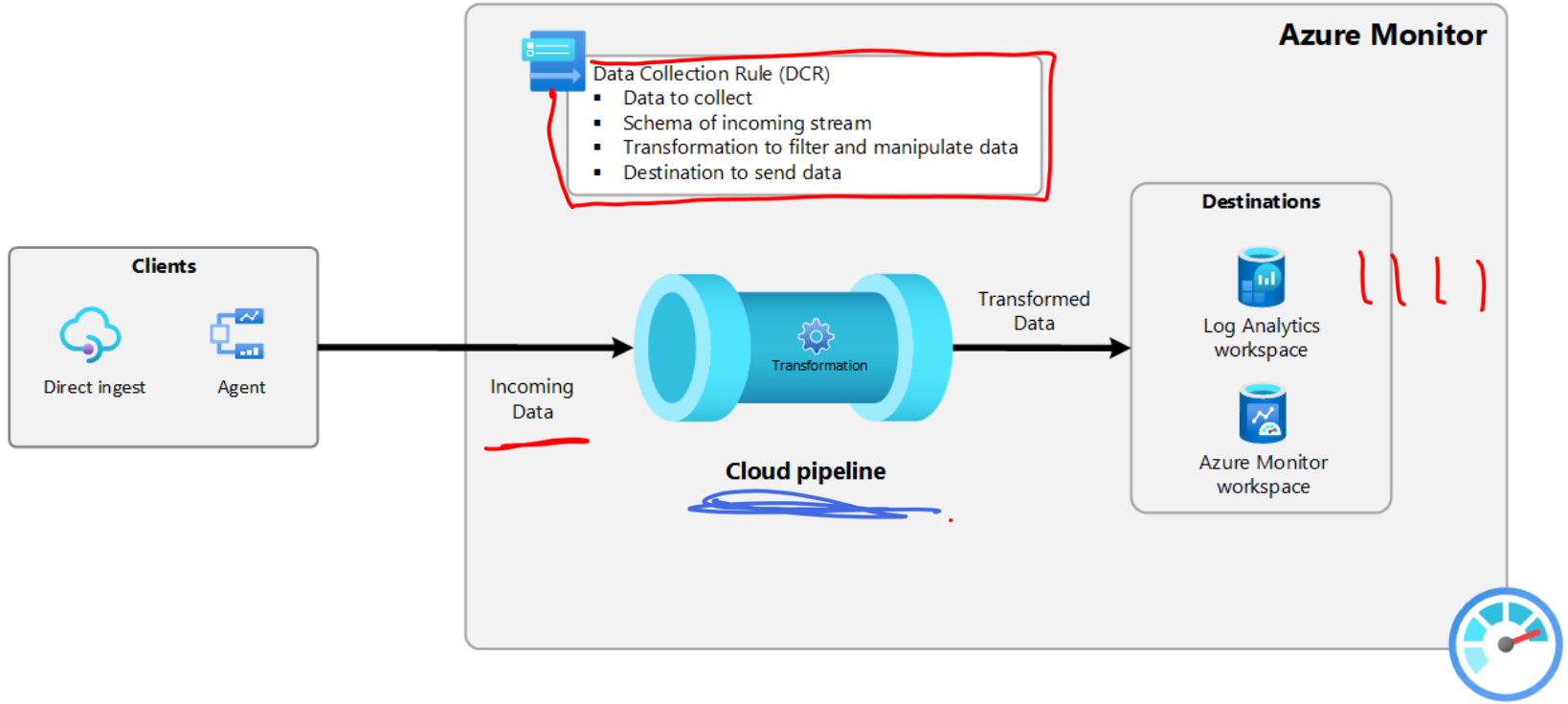


Collect data with Azure Monitor Agent



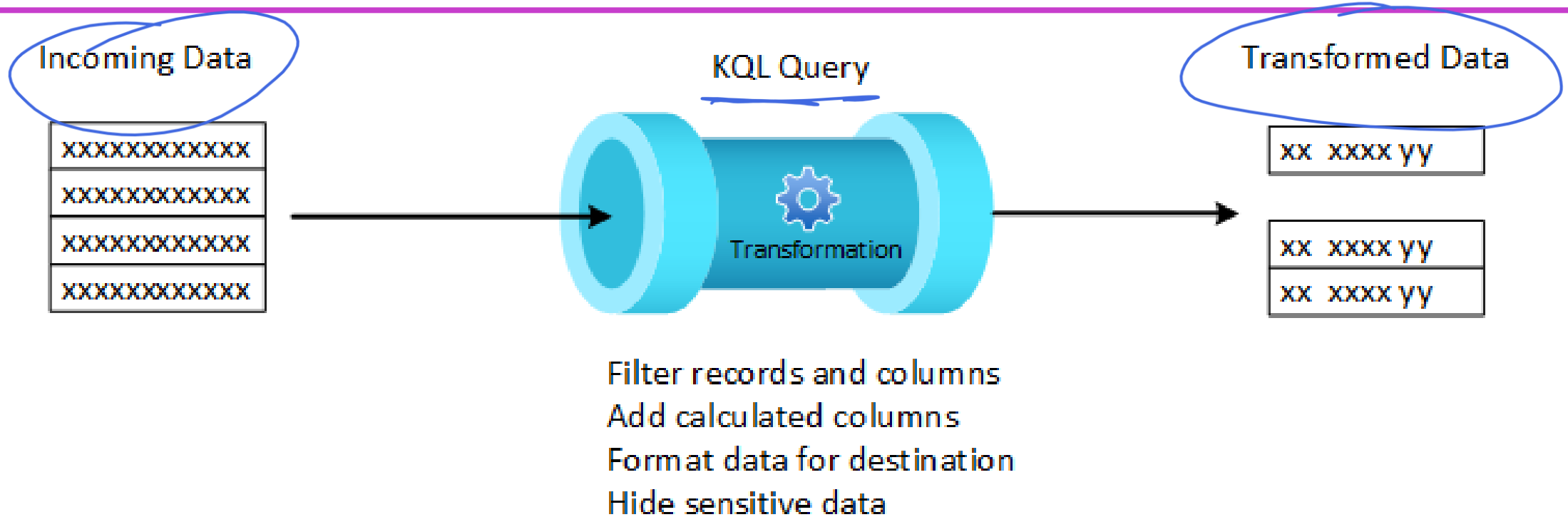
- Collects data from VMs, scale sets, and Arc-enabled servers.
- Uses Data Collection Rules (DCRs) to define and route data.
- Supports deployment via portal, CLI, PowerShell, or ARM templates.

Data collection rules (DCRs) in Azure Monitor



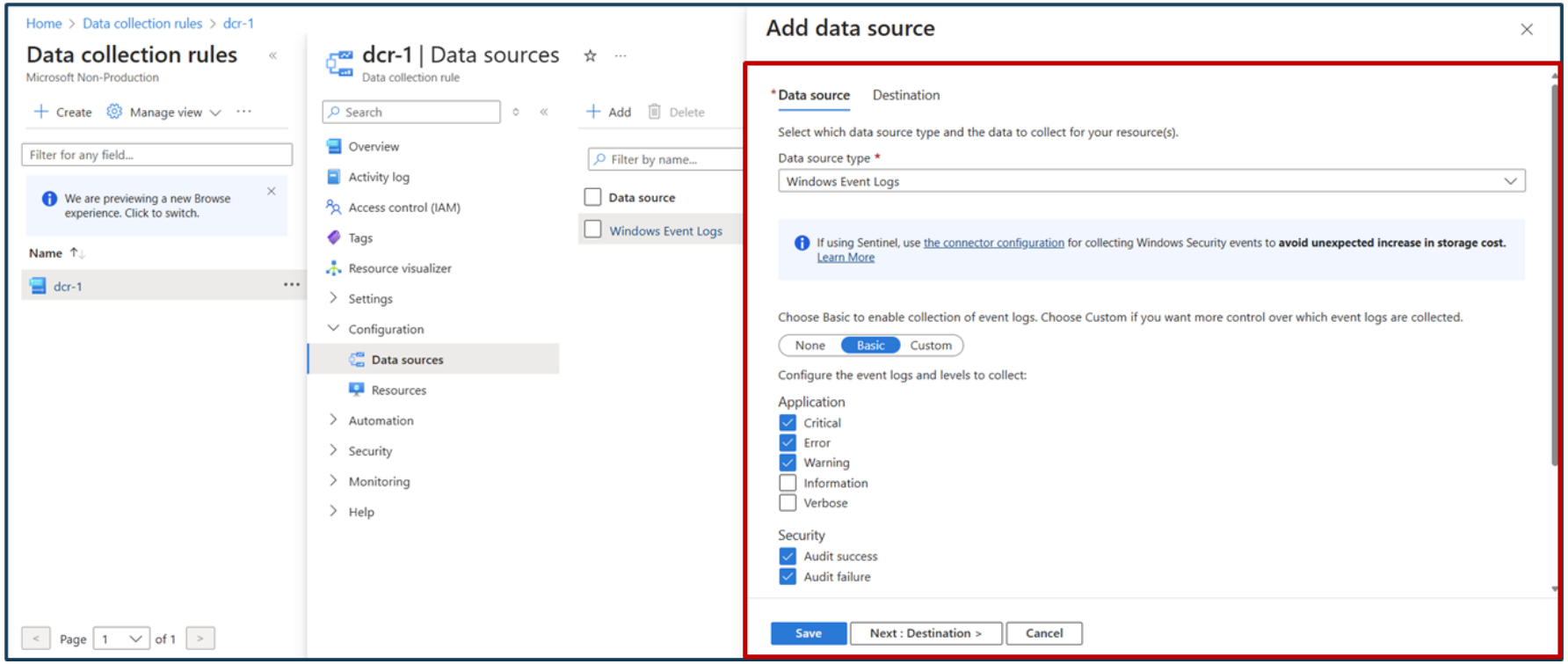
- DCRs improve Azure Monitor data collection with scalable, configurable, and centralized management.
- DCRs replace legacy methods like Log Analytics agent and Data Collector API.
- Edge pipeline enables scalable, offline data collection for environments with connectivity challenges.

Transformations in Data collection rules (DCRs)



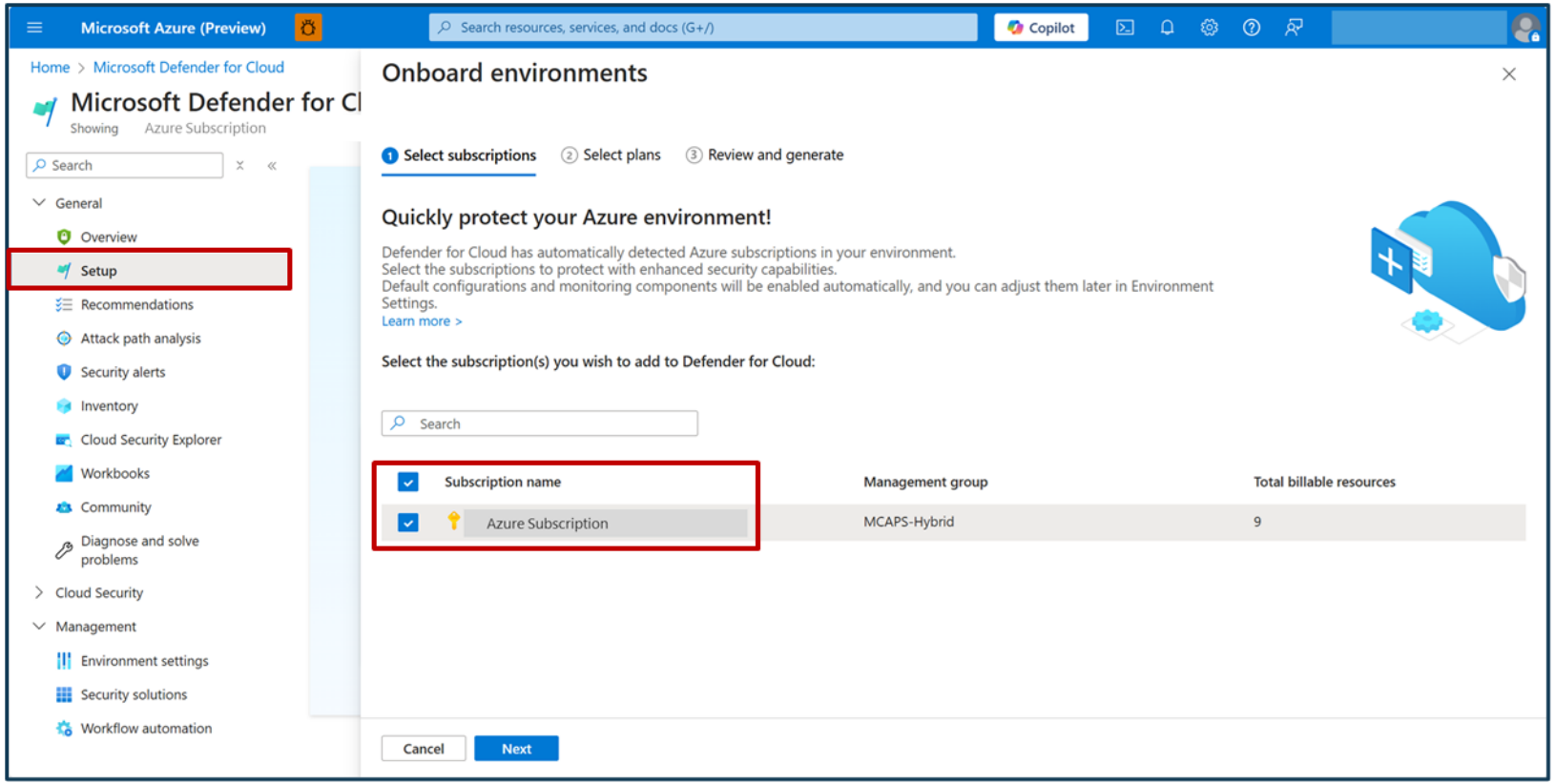
- Modify incoming data before storage or forwarding in Azure Monitor.
- Filter, remove sensitive data, or format data to match destination schema.
- Enable advanced scenarios like multi-destination routing and data enrichment.

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.

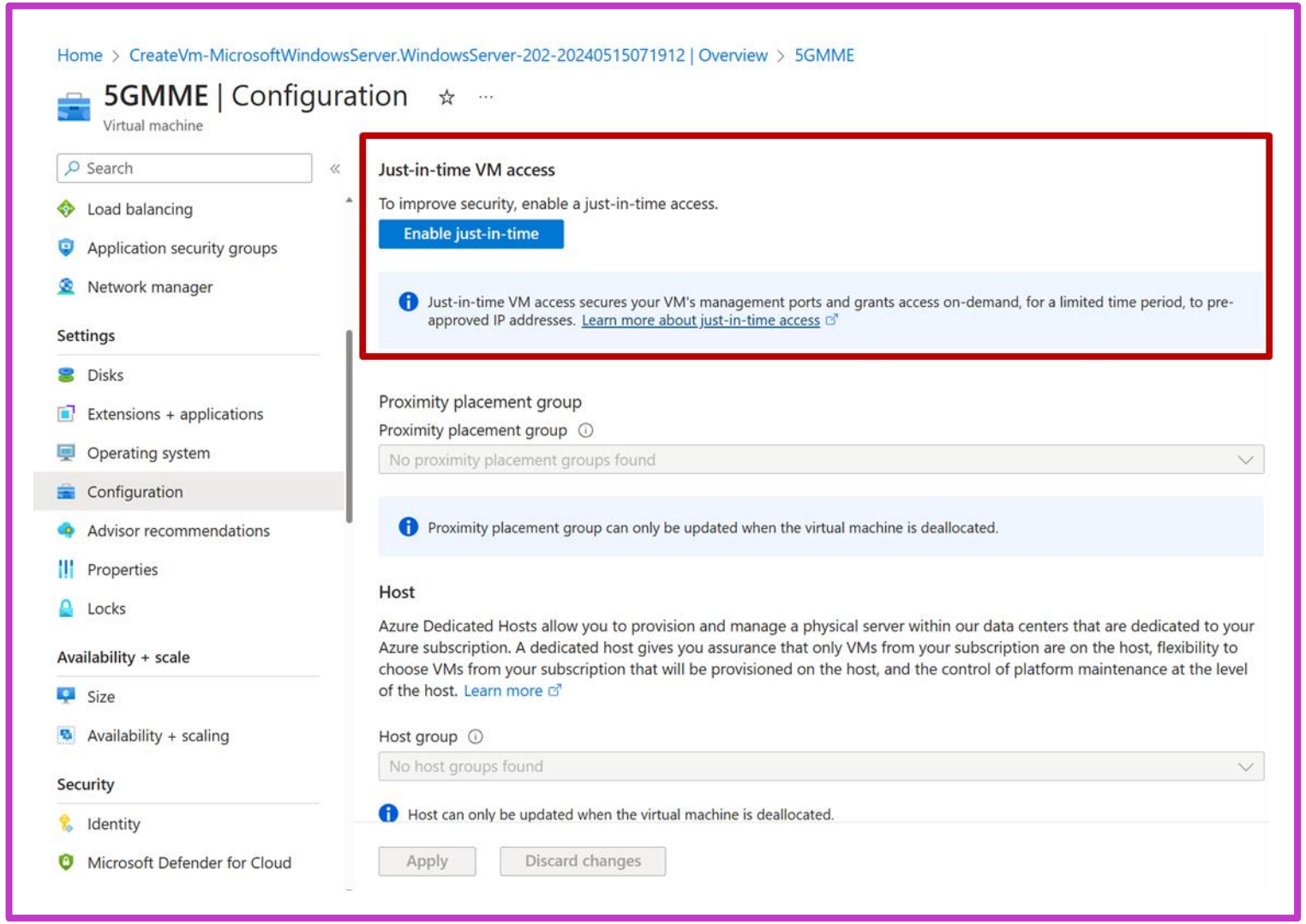
Connect your Azure subscriptions



- 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.

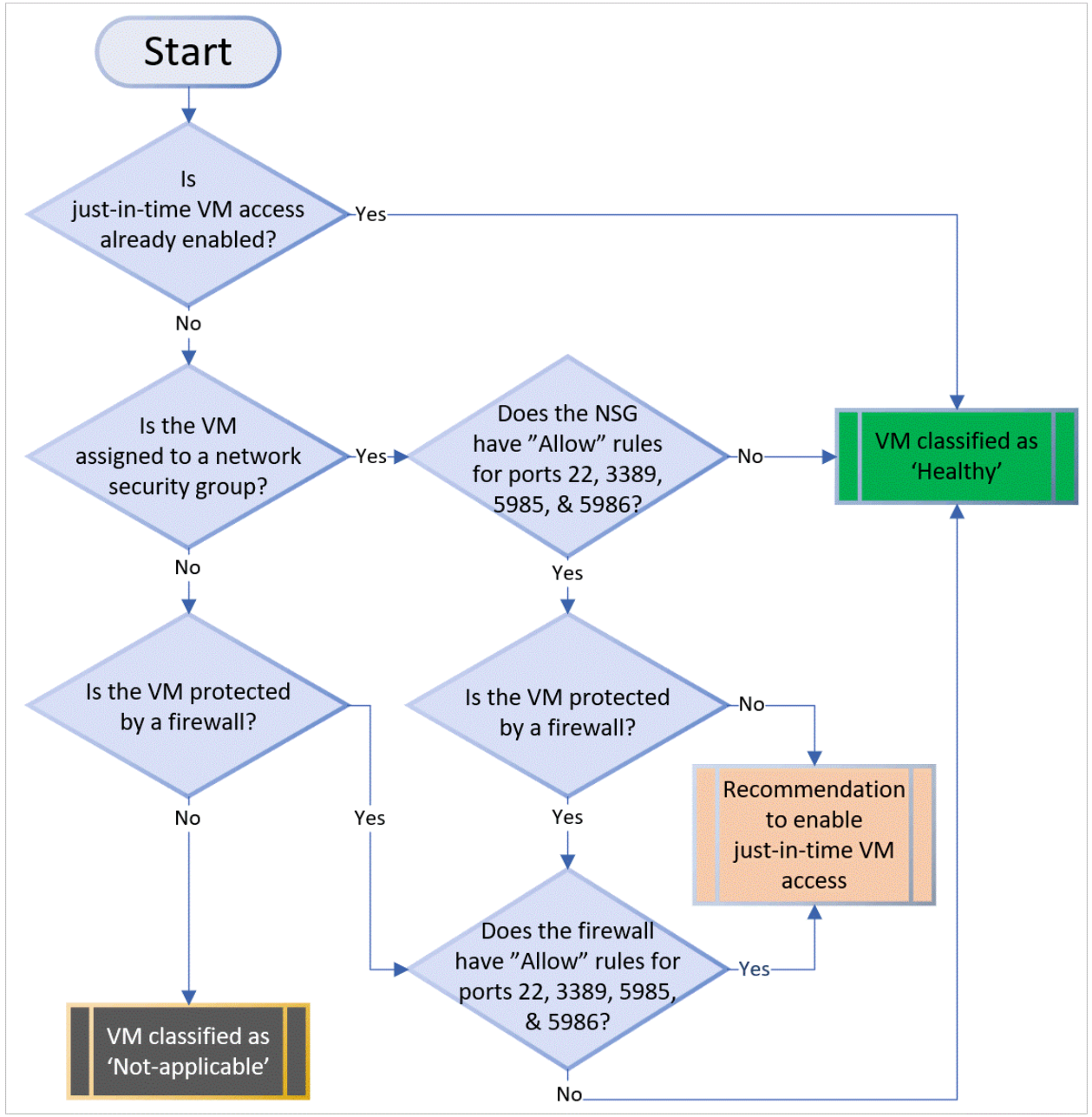
Understanding just-in-time VM access

- 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.



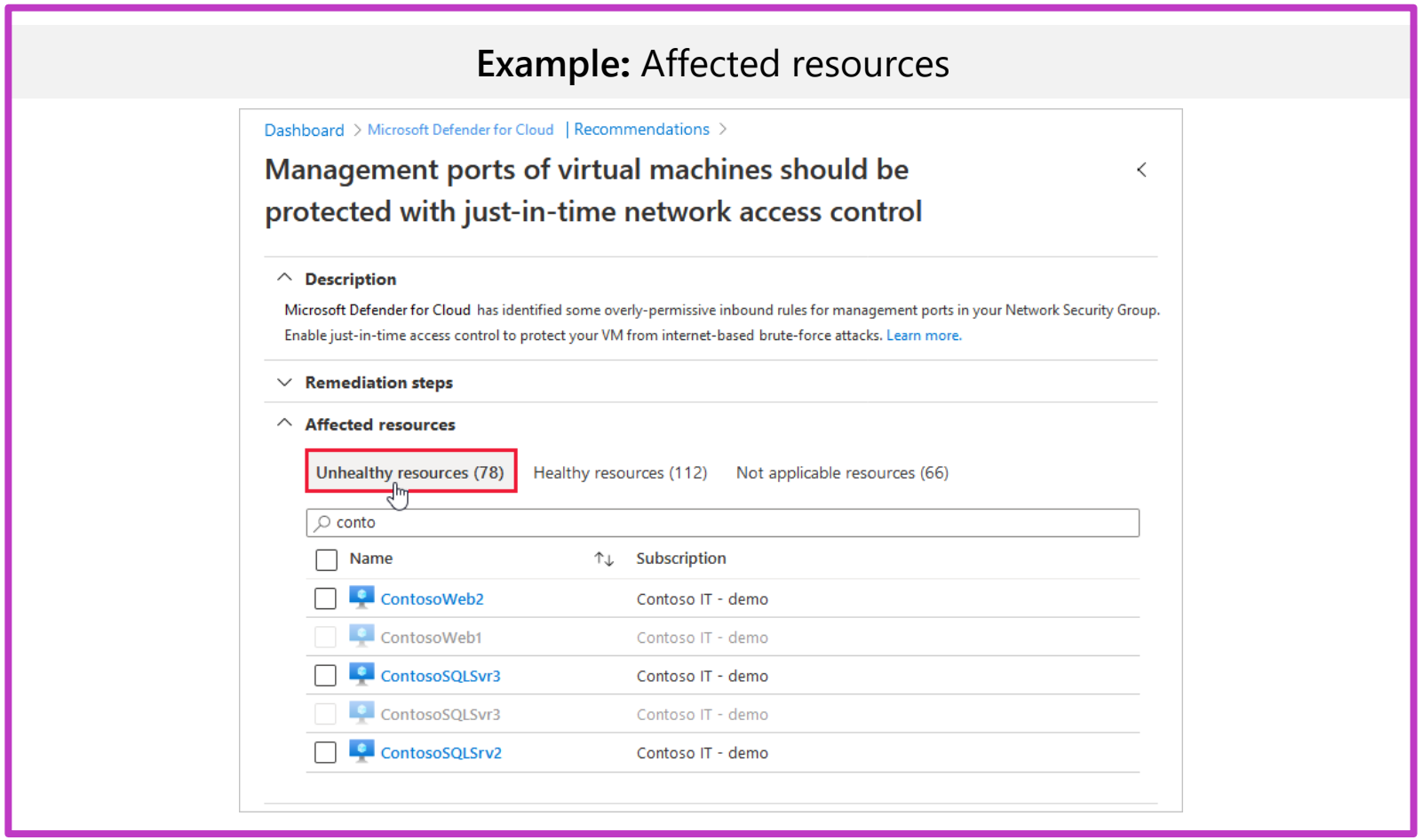
Just-in-time VM is enabled an Azure Virtual Machine

Example: Azure Virtual Machine



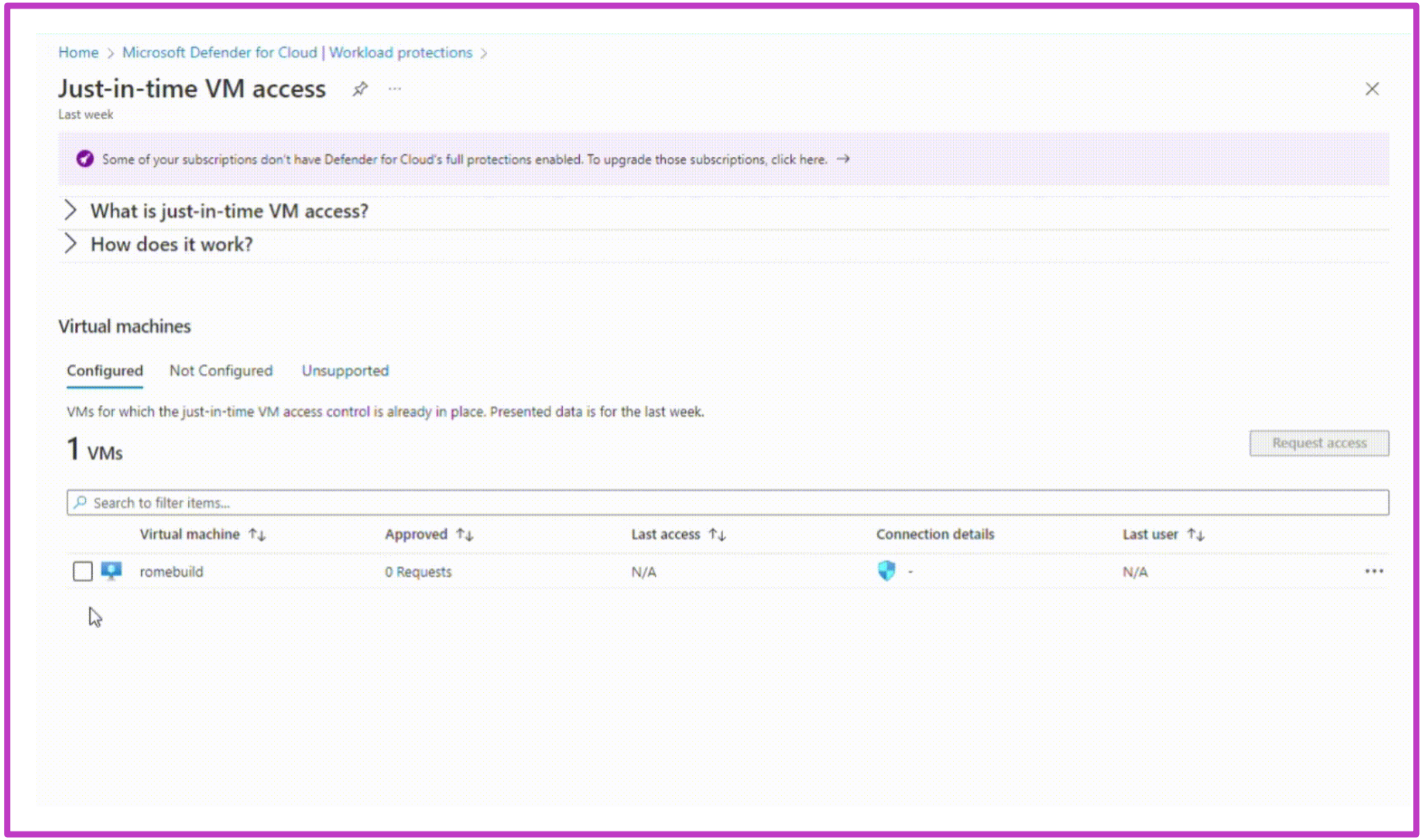
Added to the recommendation's Unhealthy resources tab

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

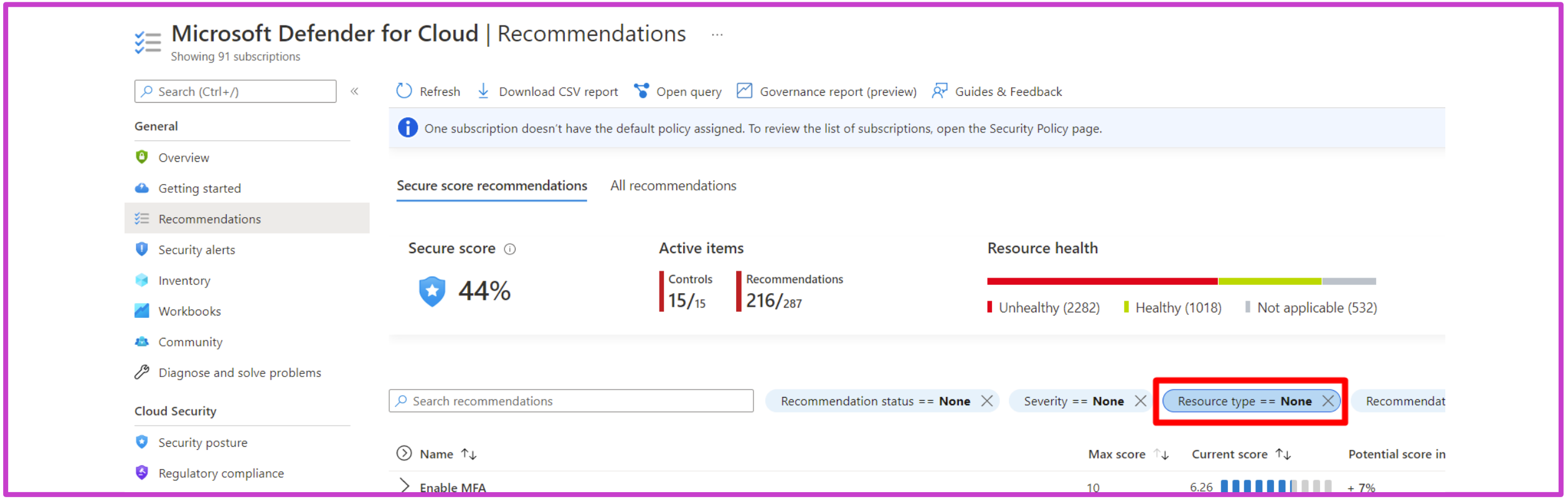


Enable just-in-time access on VMs

- 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.

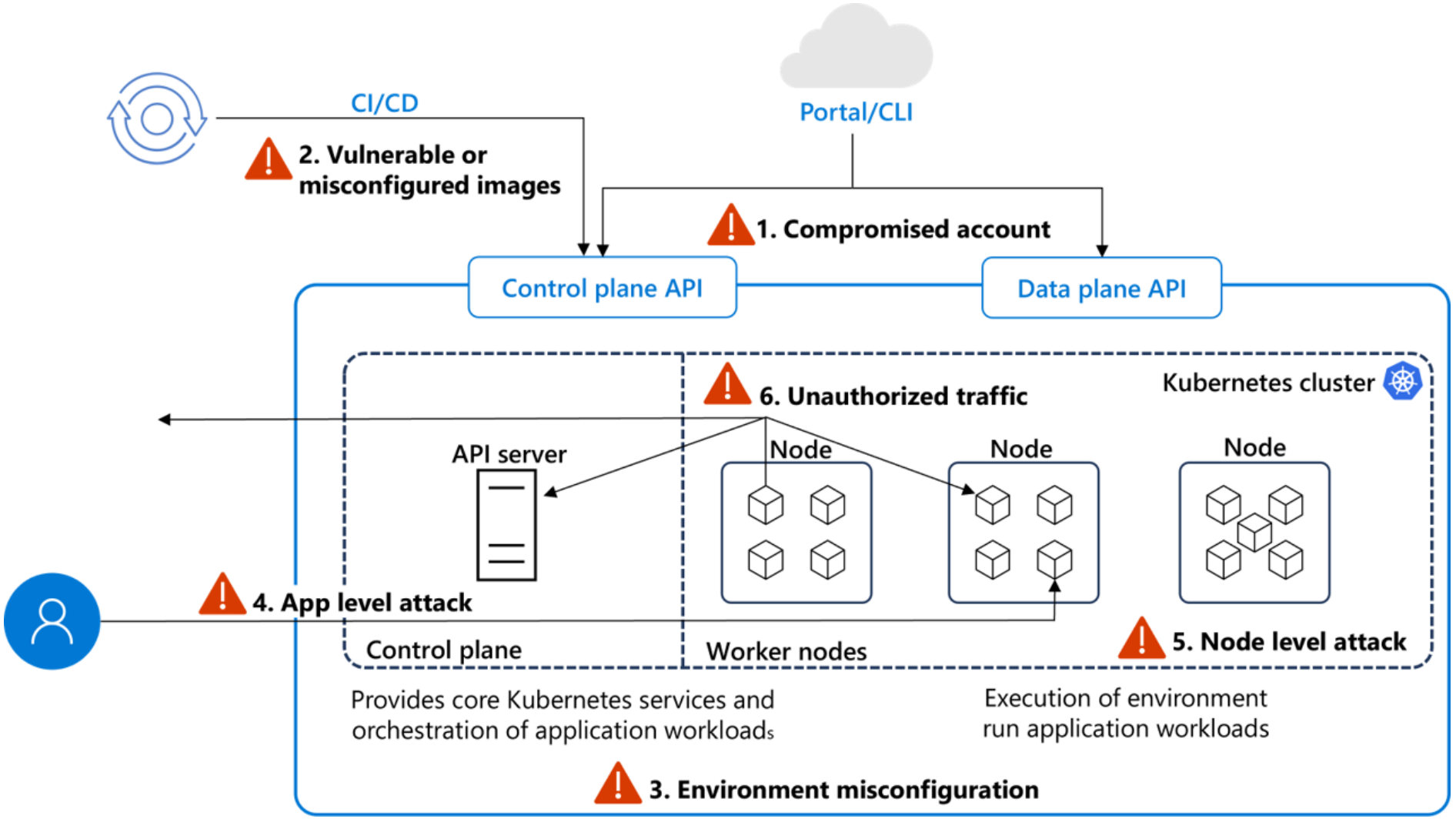


Container security in Microsoft Defender for Containers

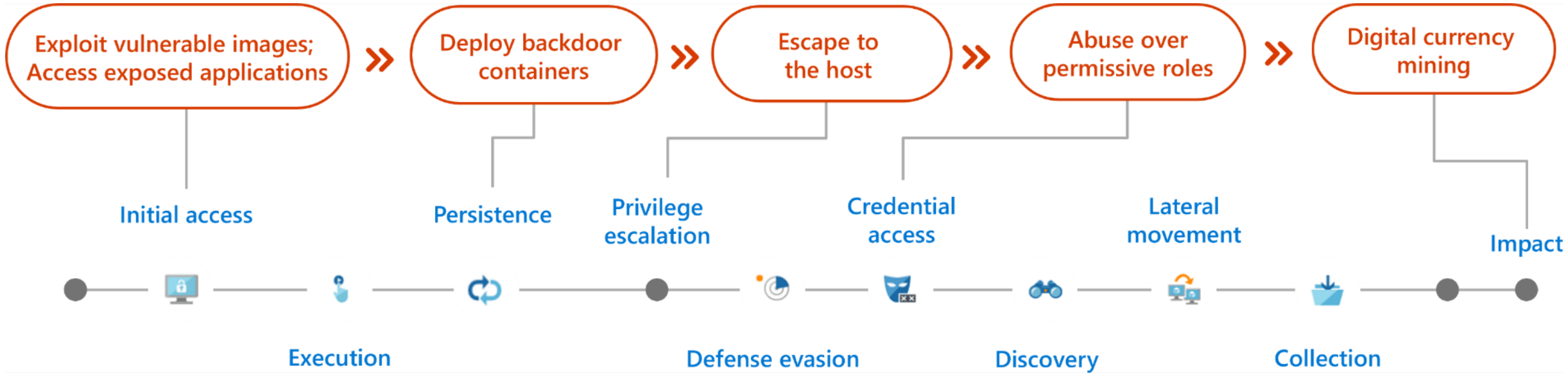


- Microsoft Defender for Containers: Cloud-native solution for container security across multicloud and on-premises environments.
- Four core domains: Security posture management, vulnerability assessment, run-time threat protection, deployment & monitoring.
- Features: Agentless capabilities, agent-based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

Managed Kubernetes threat factors

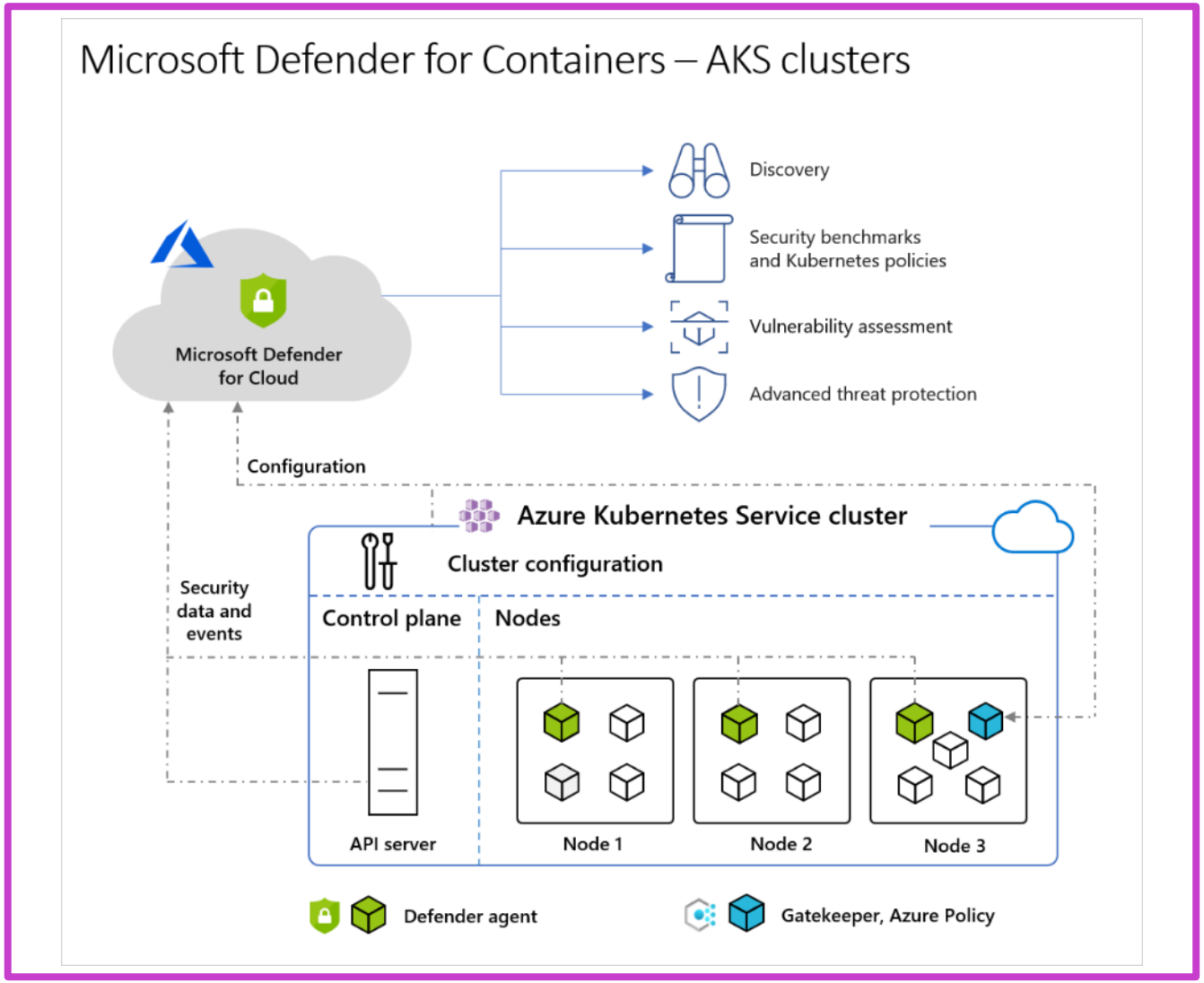


Common attack techniques



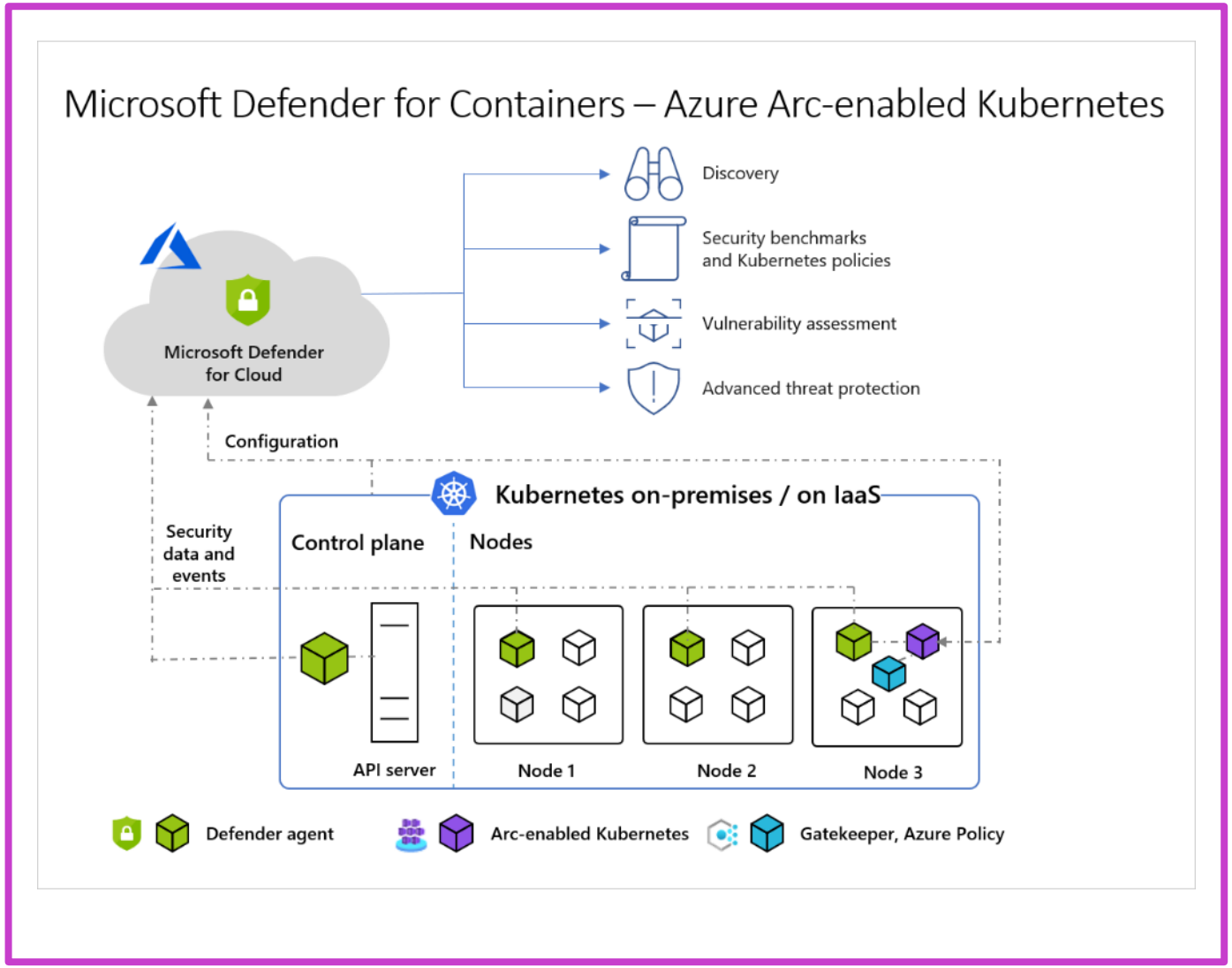
Architecture diagram of Defender for Cloud and AKS clusters

- 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.



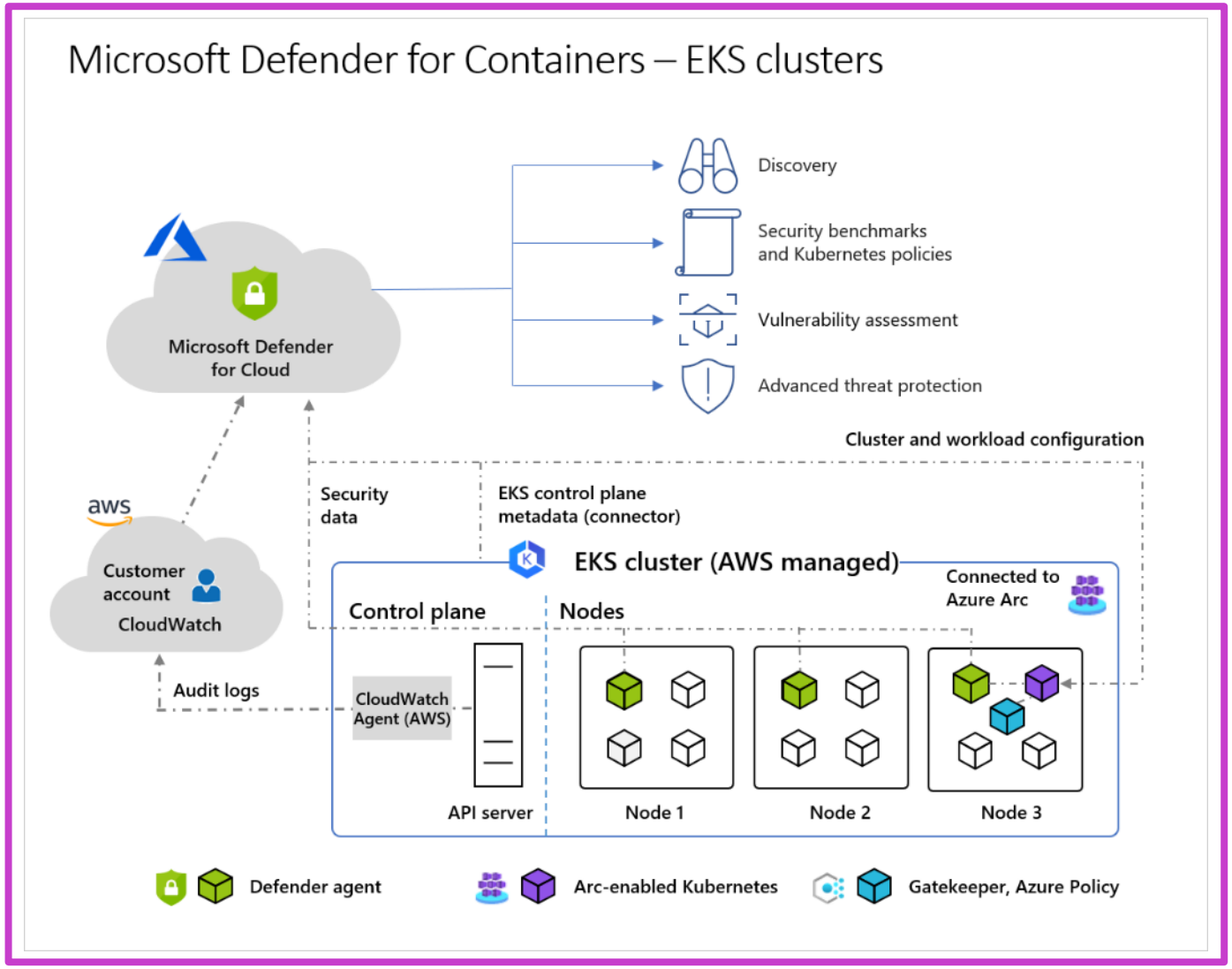
Architecture diagram of Defender for Cloud and Arc-enabled Kubernetes clusters

- 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.



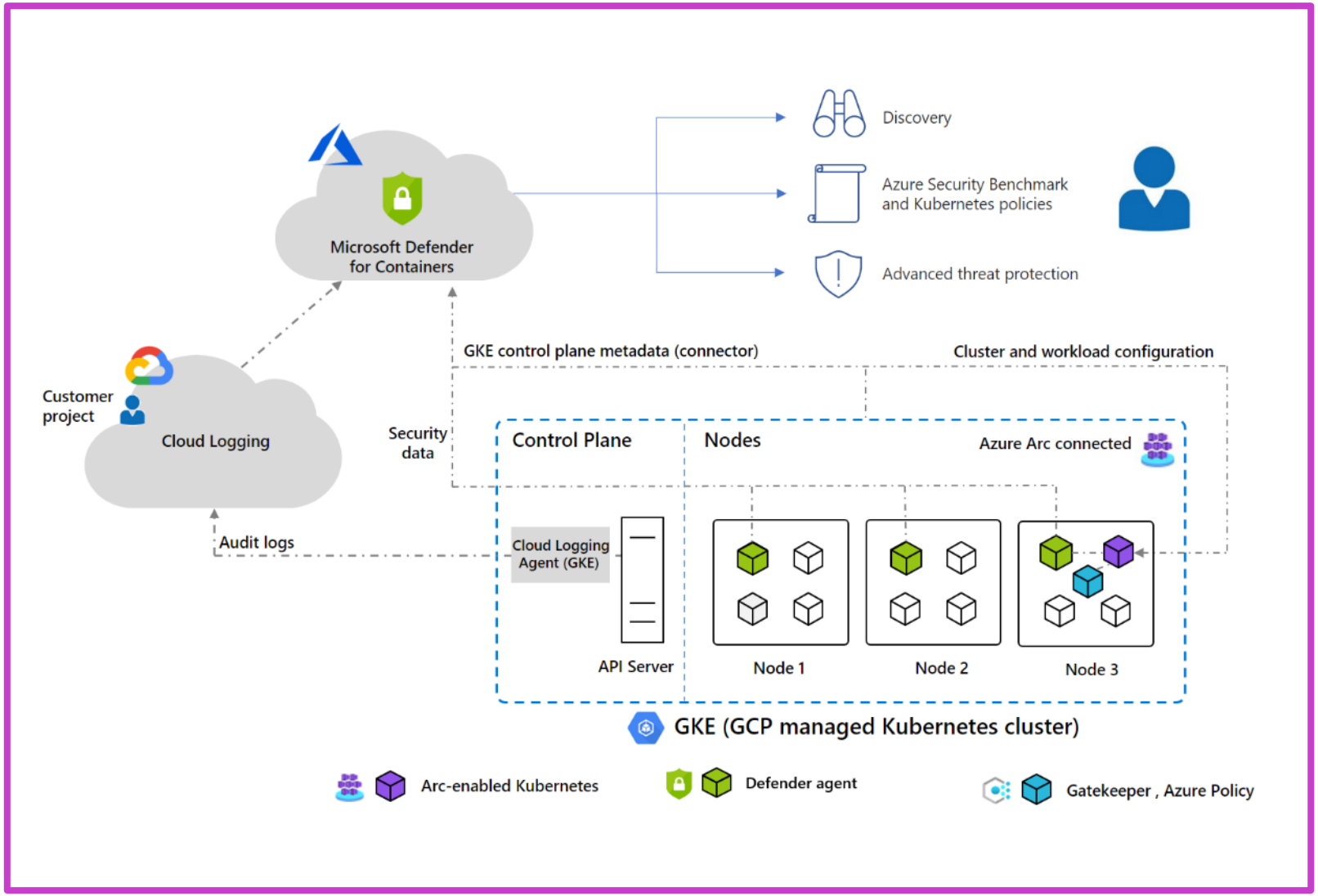
Architecture diagram of Defender for Cloud and EKS clusters

- 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.

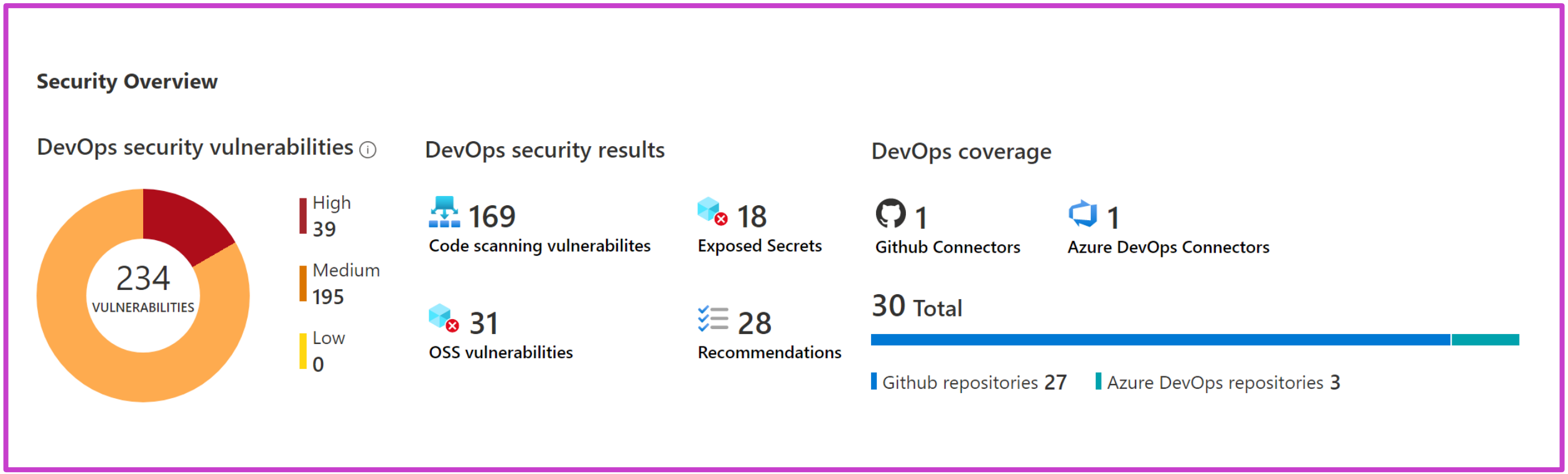


Architecture diagram of Defender for Cloud and GKE clusters

- 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



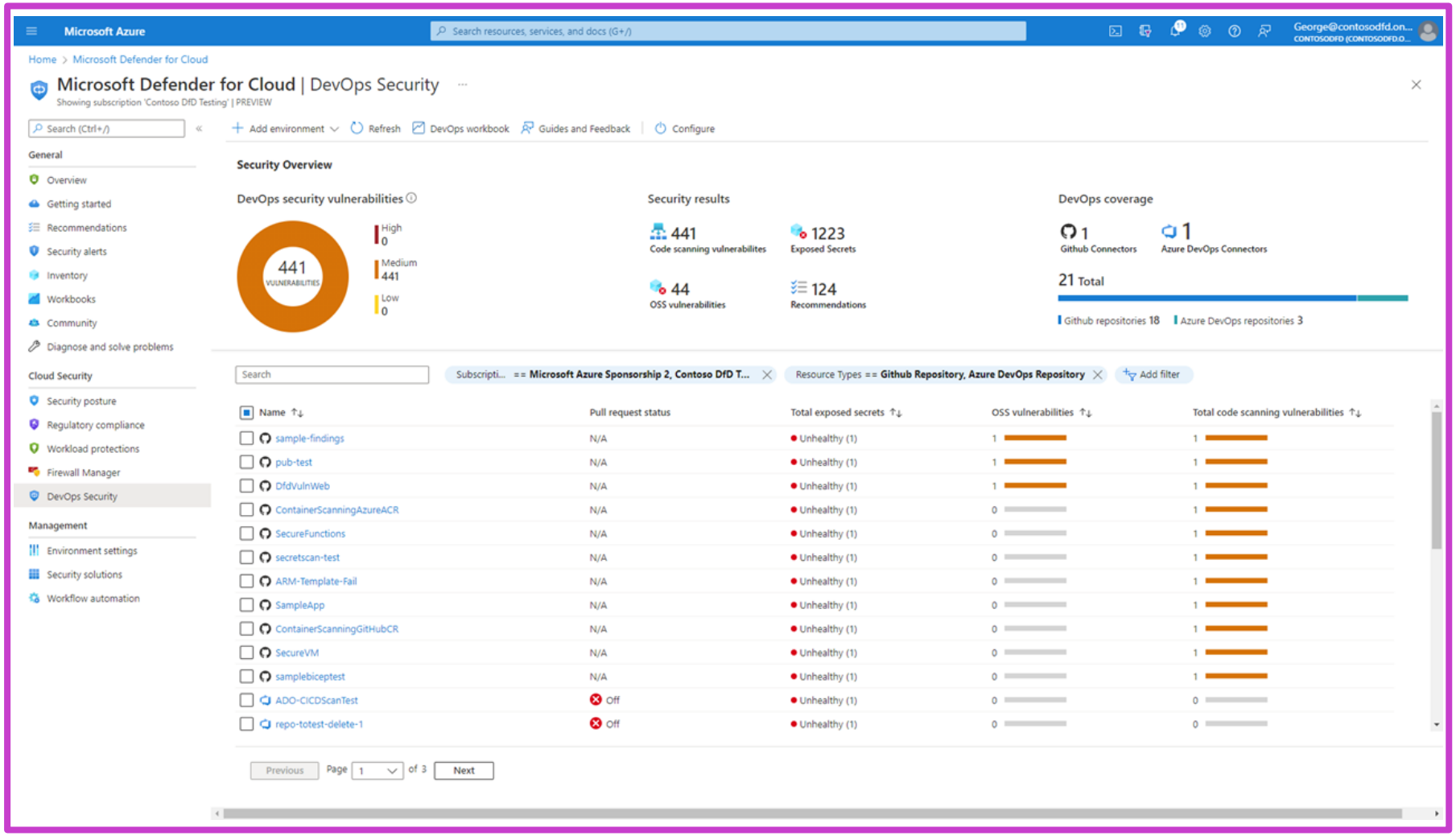
- Provides visibility, posture management, threat protection across Azure, AWS, GCP, on-premises.
- Centralizes DevOps security, integrates with Azure DevOps, GitHub, GitLab for application protection.
- Prioritizes code remediation with contextual insights, secures IaC templates, container images.

Defender for Cloud DevOps Security required permissions

Feature	Permissions
Connect DevOps environments to Defender for Cloud	• Azure: Subscription Contributor or Security Admin • Azure DevOps: Project Collection Administrator on target Organization • GitHub: Organization Owner • GitLab: 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

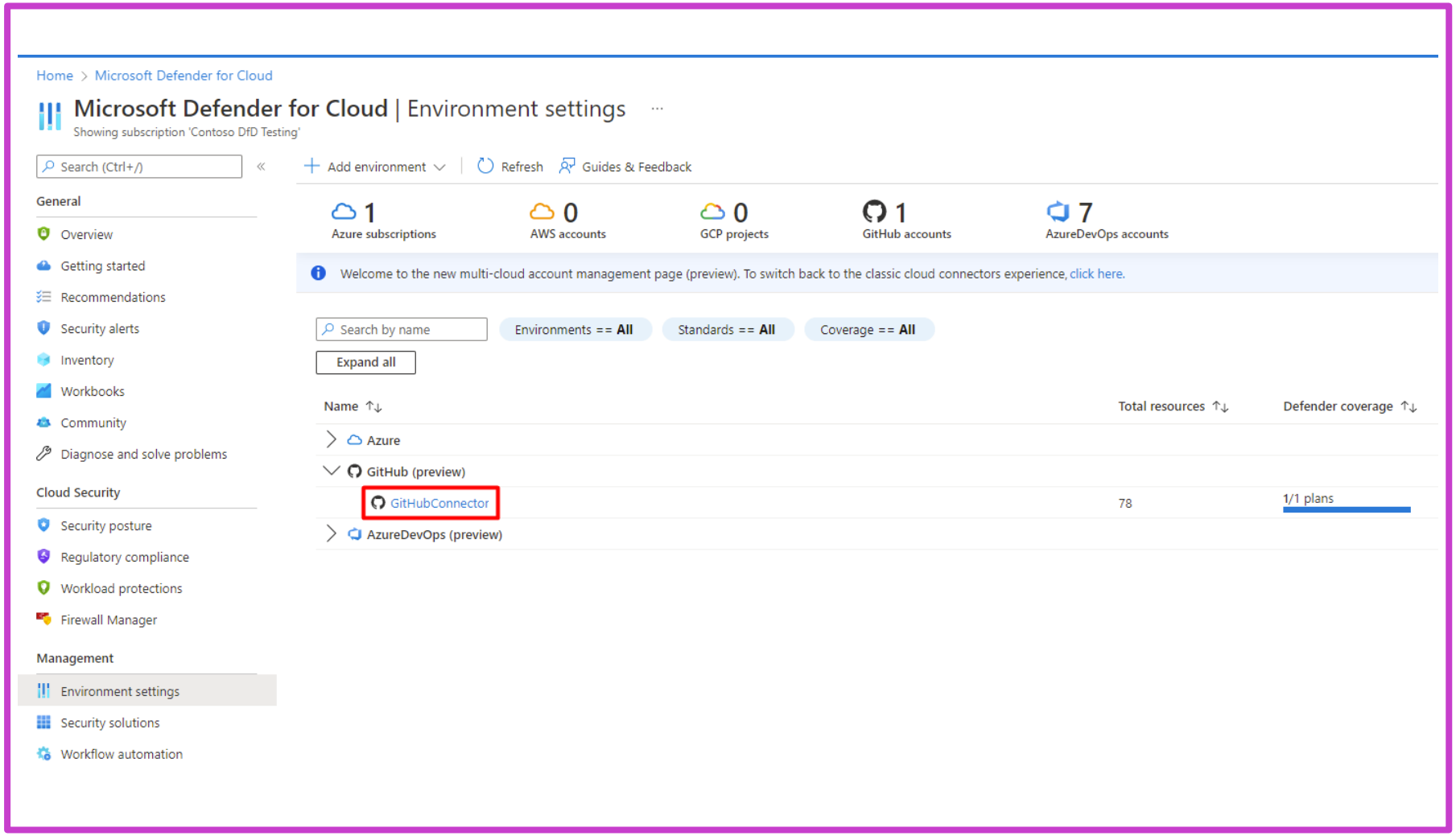
DevOps environment security posture

- 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.



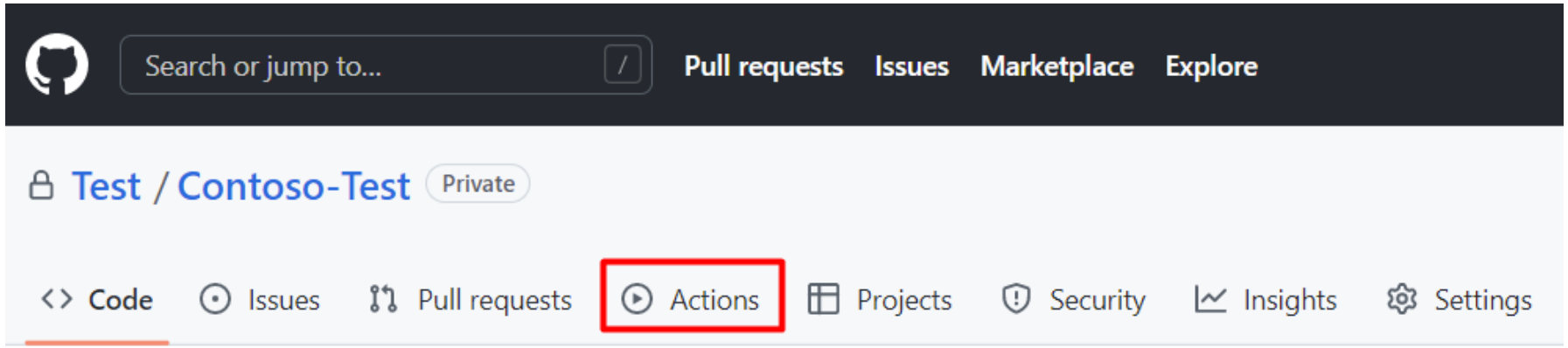
Connect your GitHub Environment to Defender for Cloud

- 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.



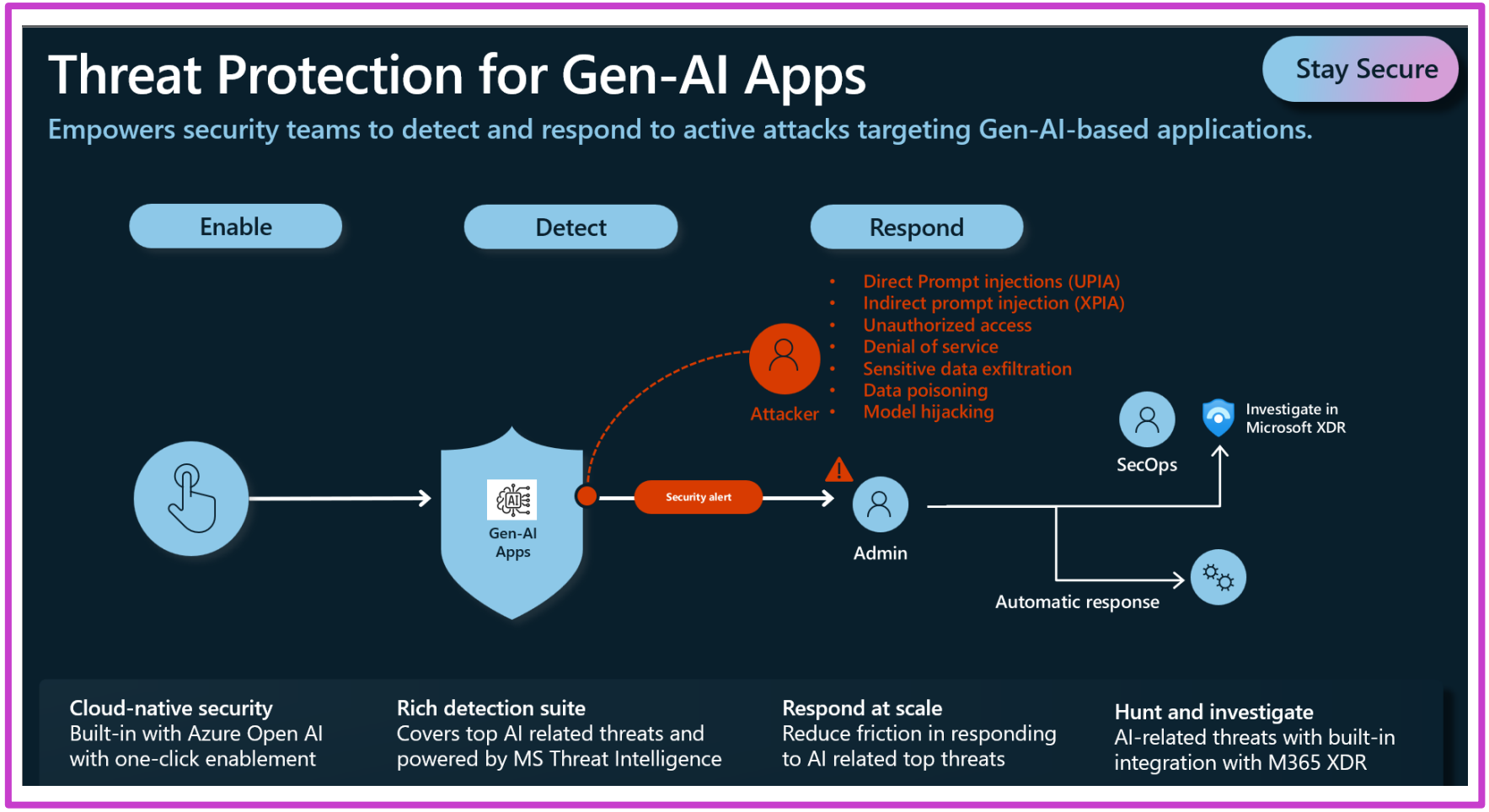
Configure the Microsoft Security DevOps GitHub action

- 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.



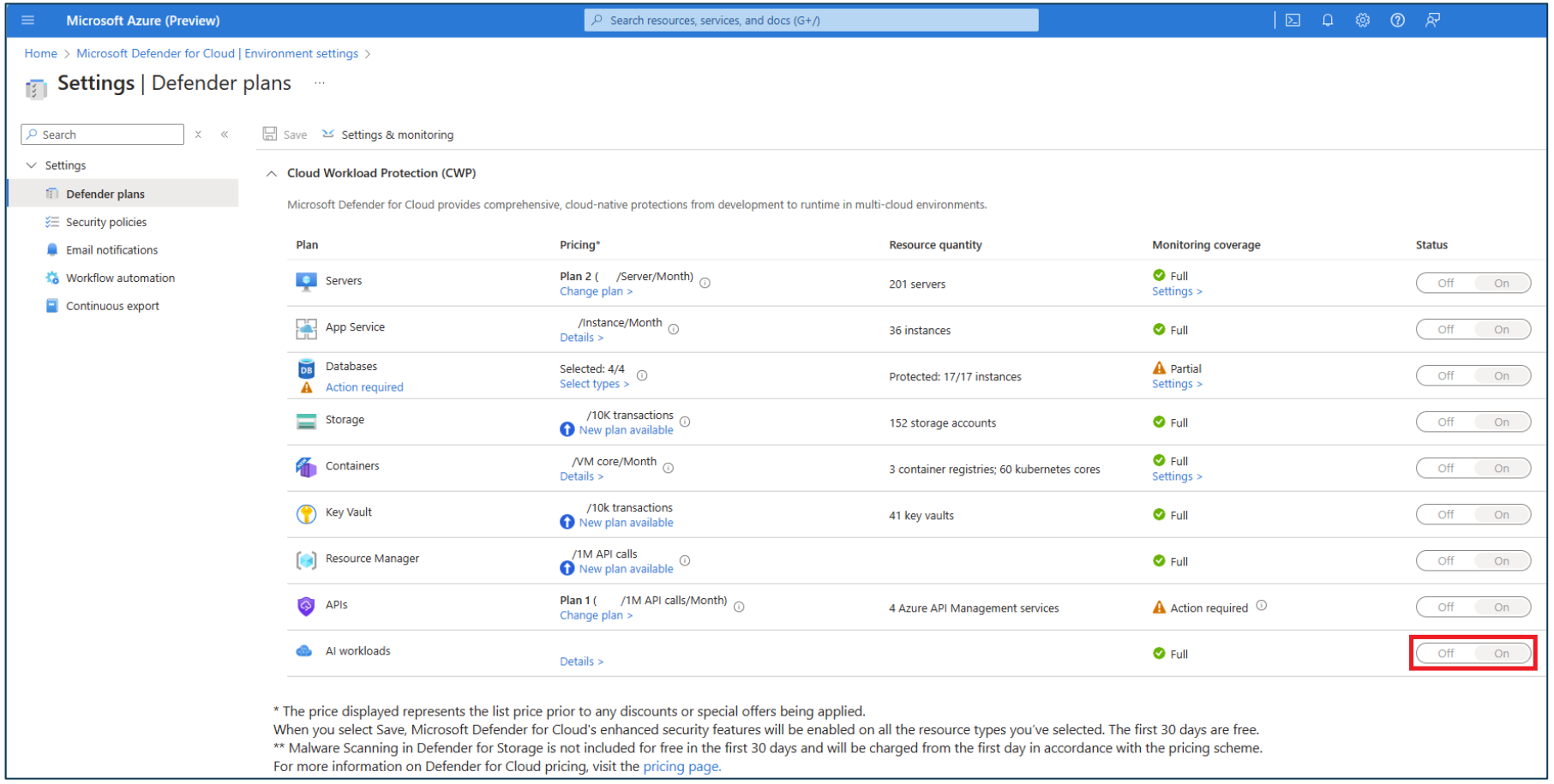
Defender for Cloud AI threat protection

- 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.



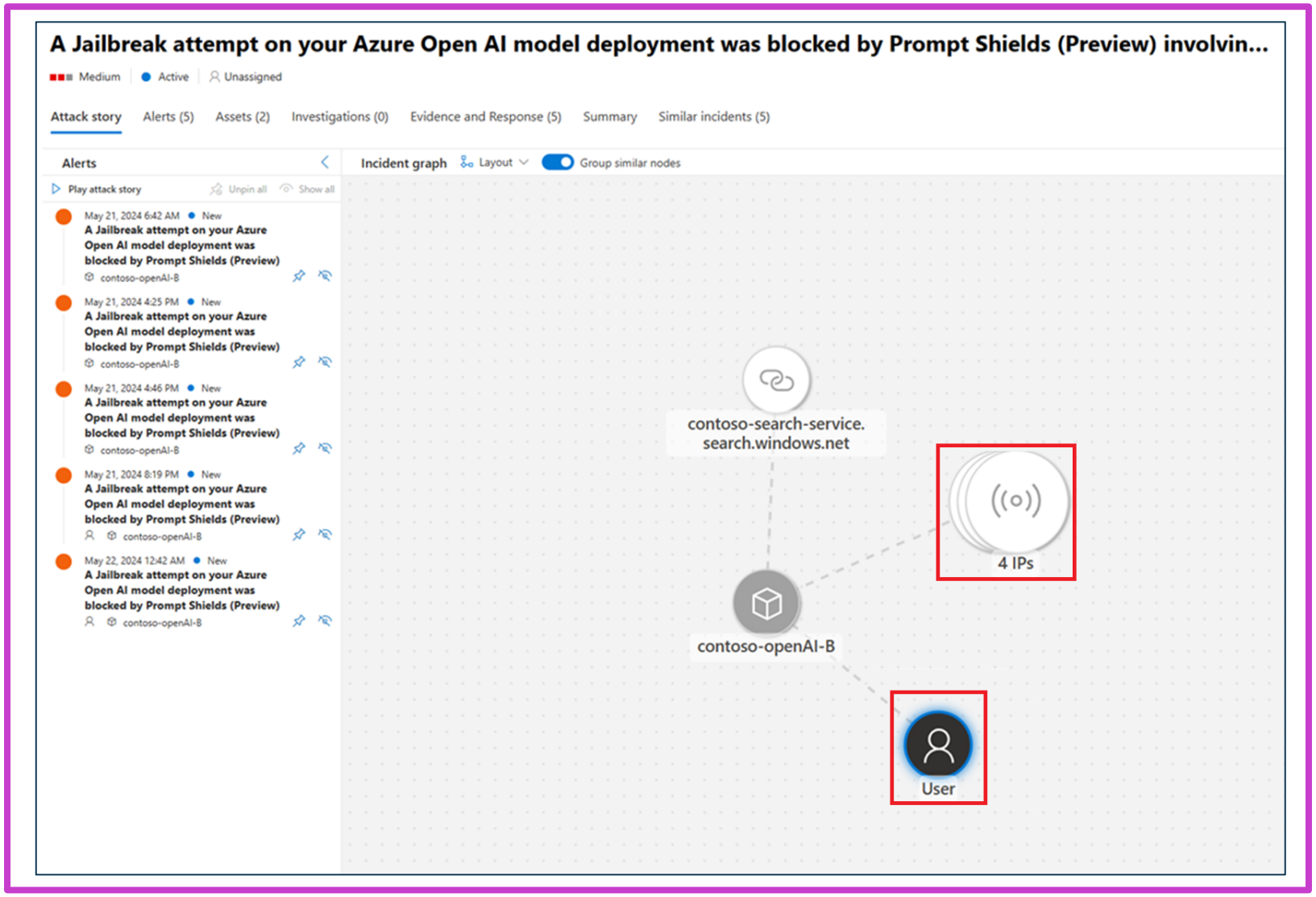
Enable threat protection for AI workloads

- 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.



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

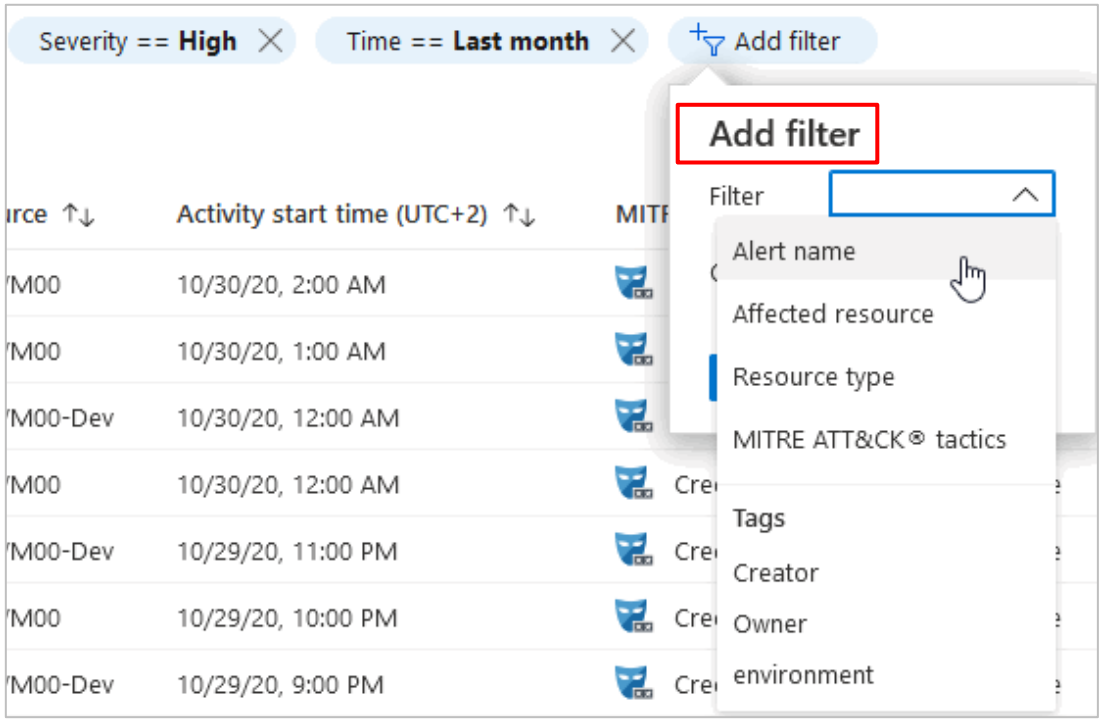
Manage security alerts

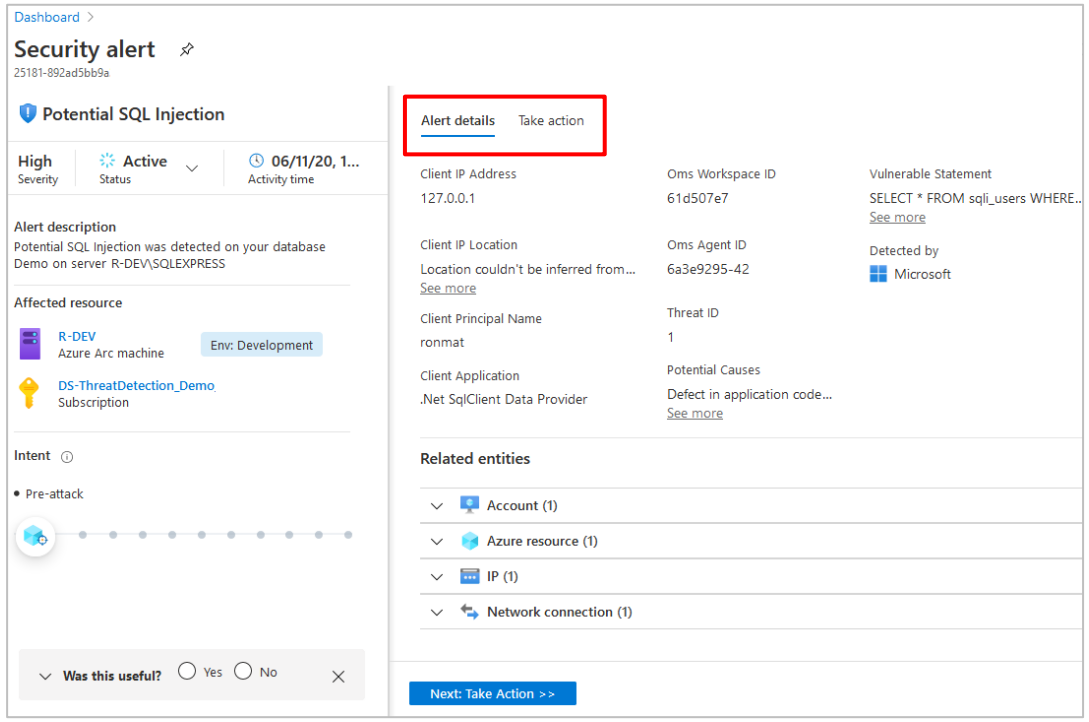
- From Defender for Cloud's overview, choose "**Security alerts**."
- Use and add filters to refine alert display.

Respond to security alerts

Choose an alert and click "**View full details**."

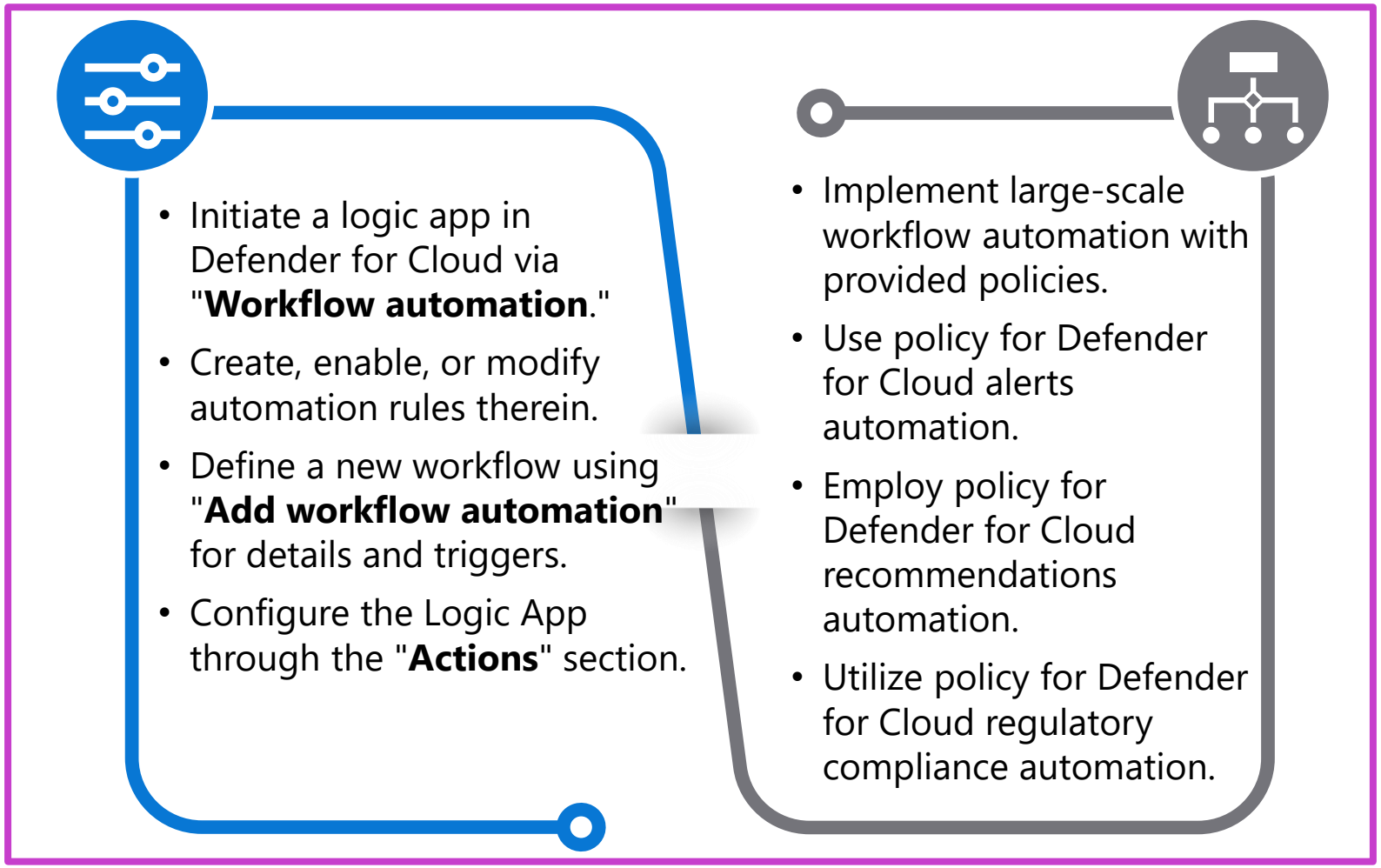
- Investigate and mitigate threats using "Alert details" and "Take action" tabs.





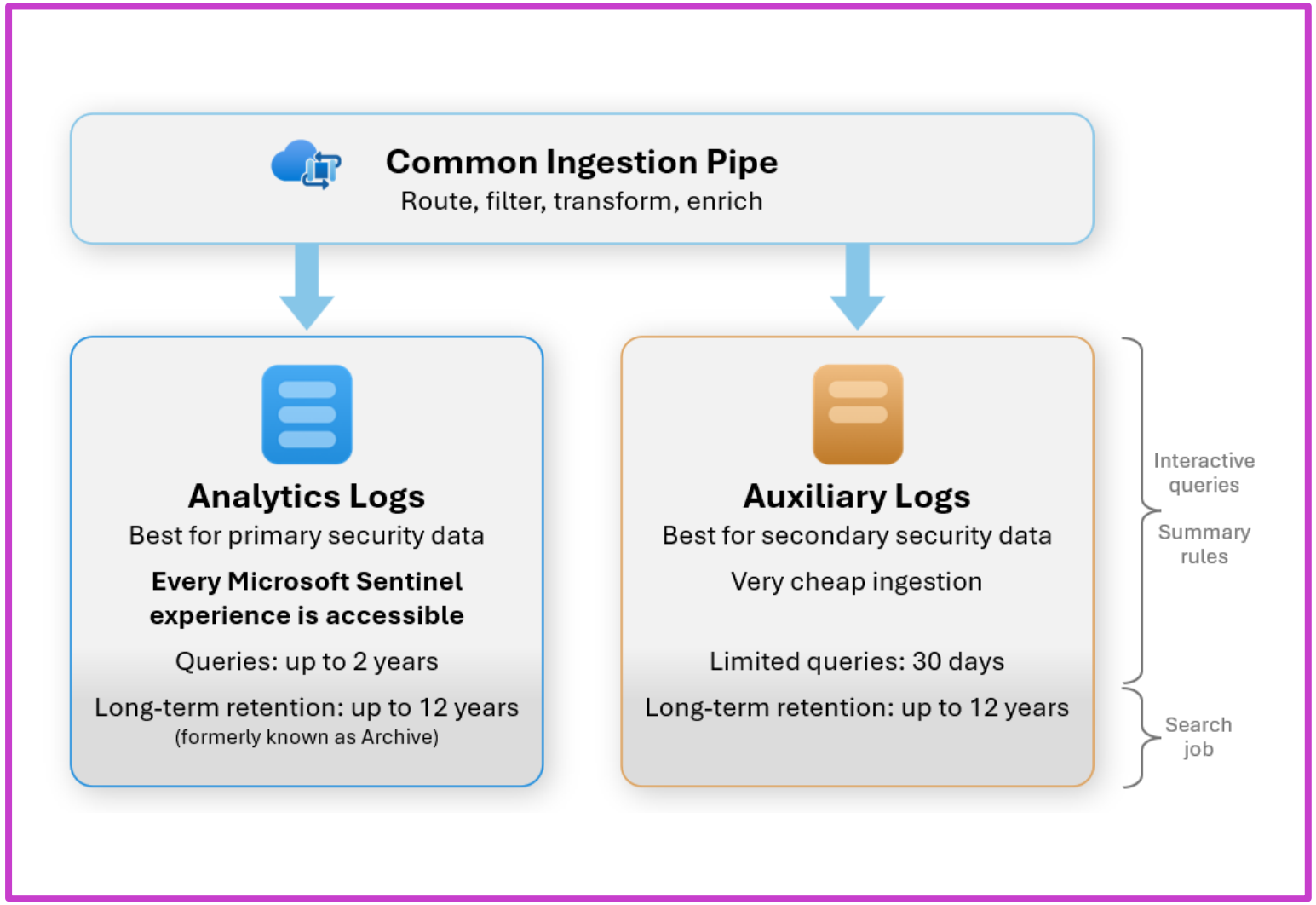
Configure workflow automation by using Microsoft Defender for Cloud

To configure workflow automation, you can:



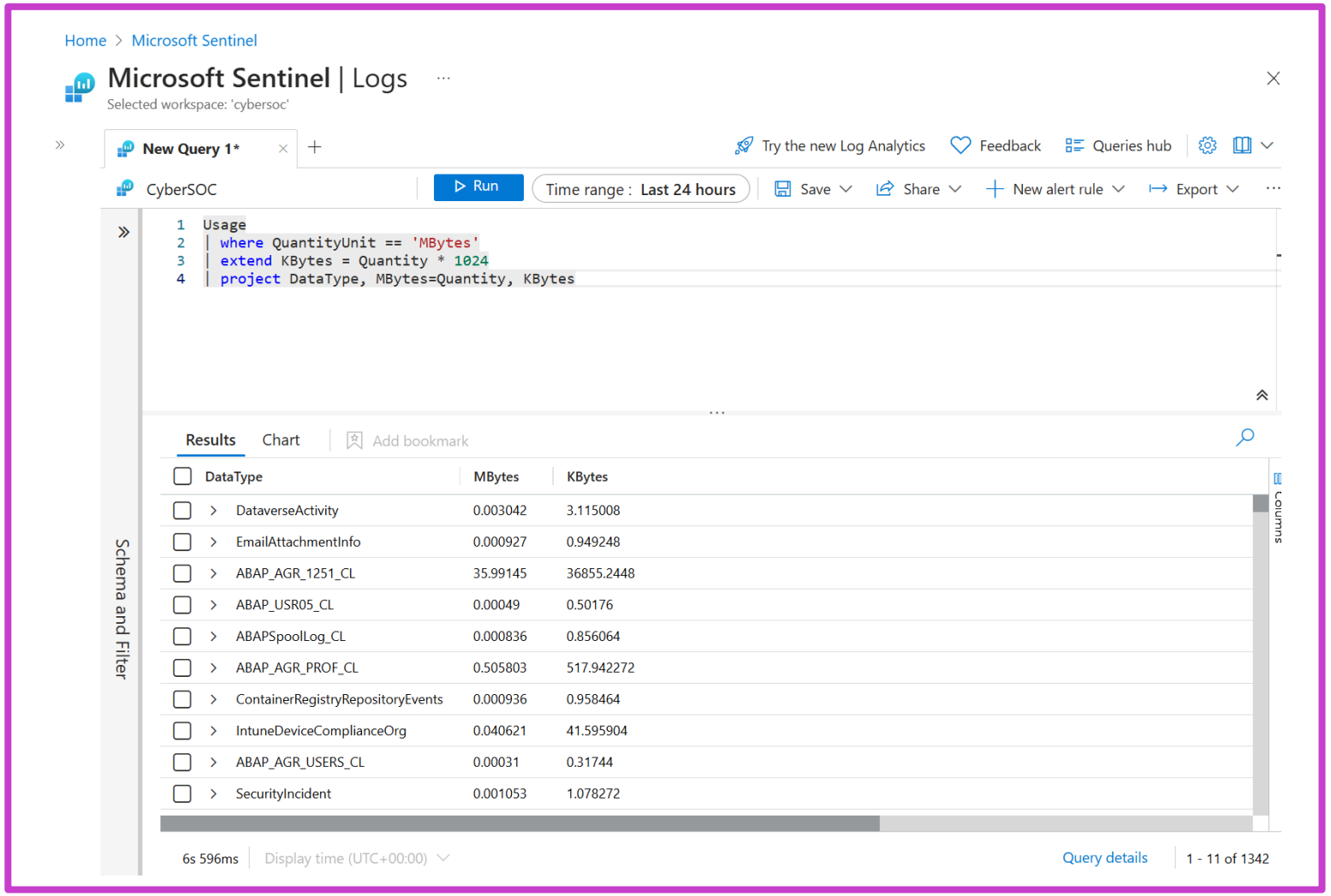
Log retention plans in Microsoft Sentinel

- 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.



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

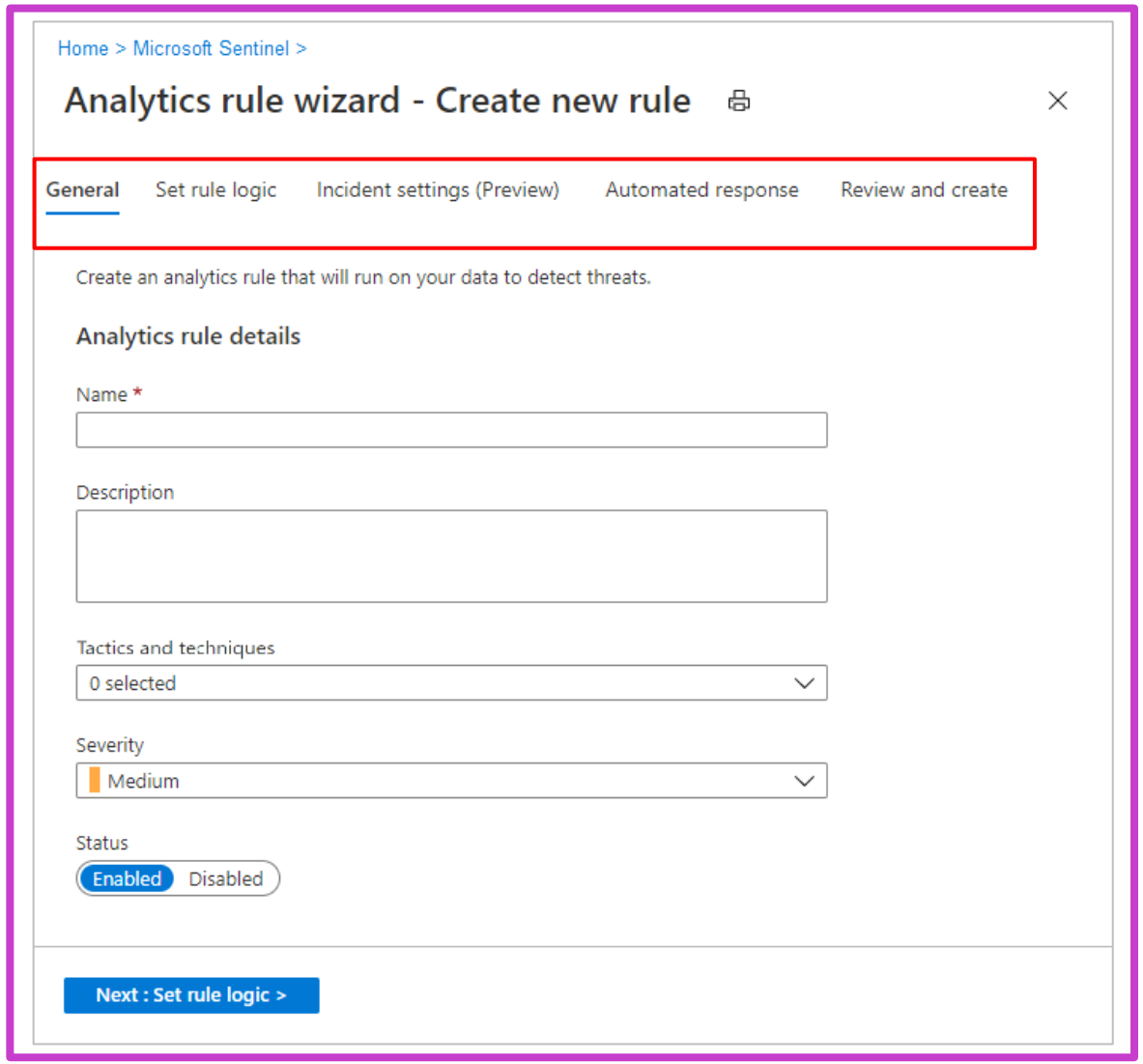
- Configure settings such as **Rule query**, **Alert enrichment**, **Query scheduling, Alert threshold,** and **Event grouping.**

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.



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

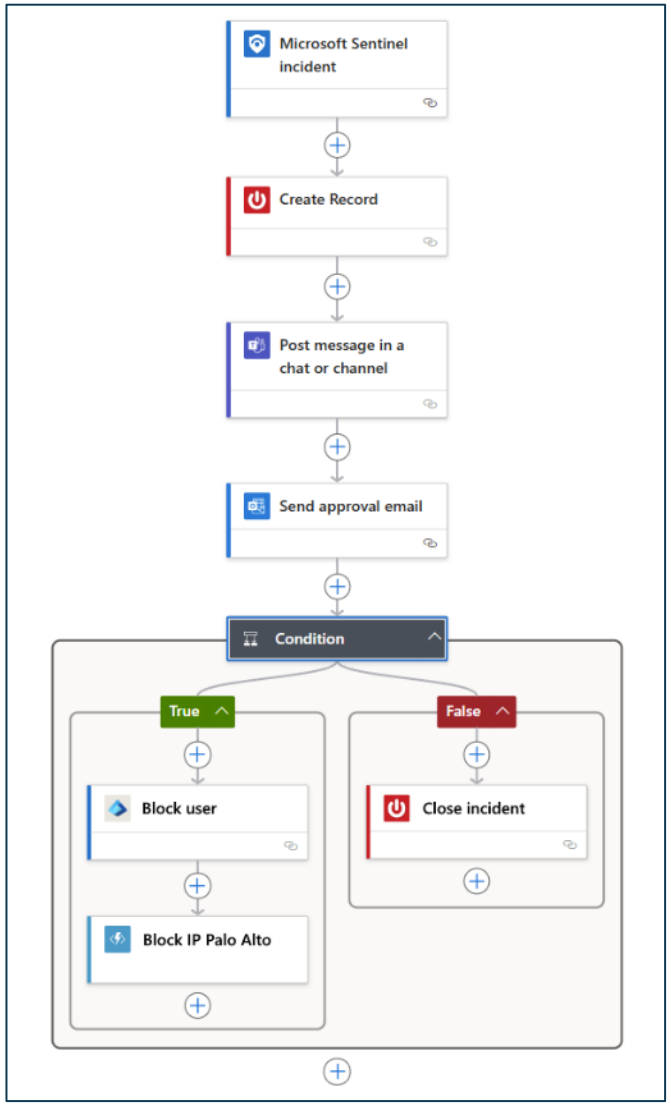
Automate using playbooks

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.

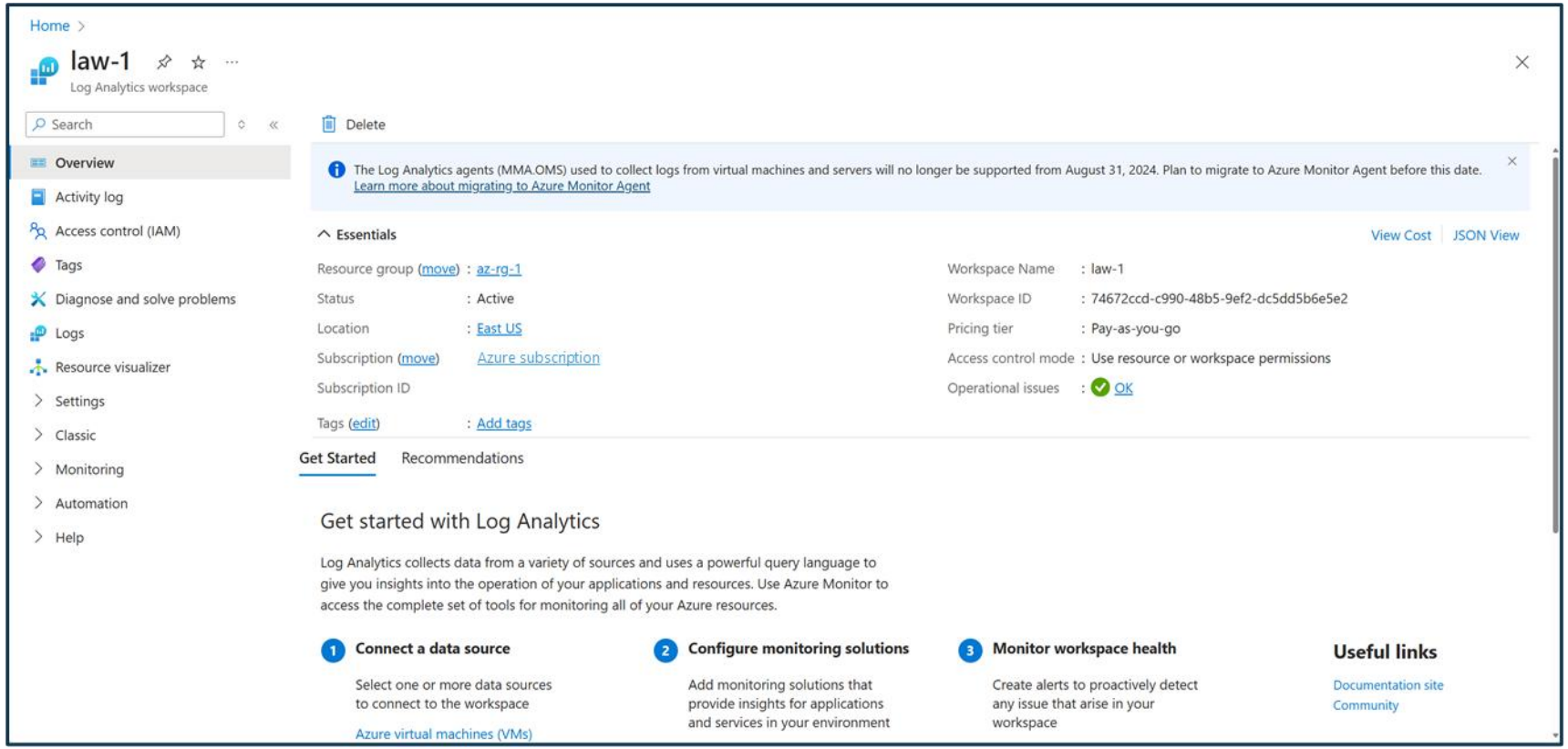


Module Labs

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

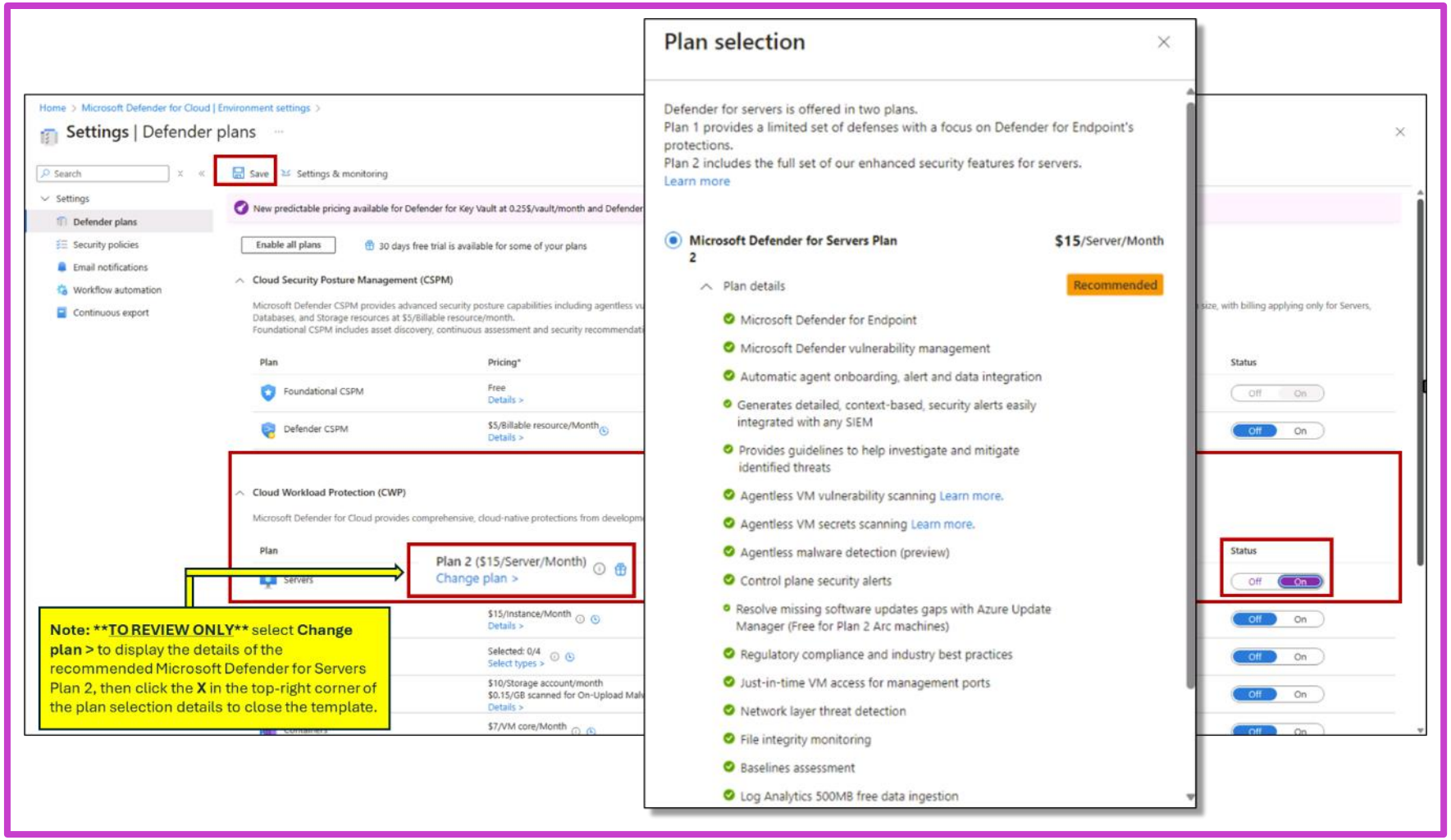
[Launch this Exercise in GitHub]



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.

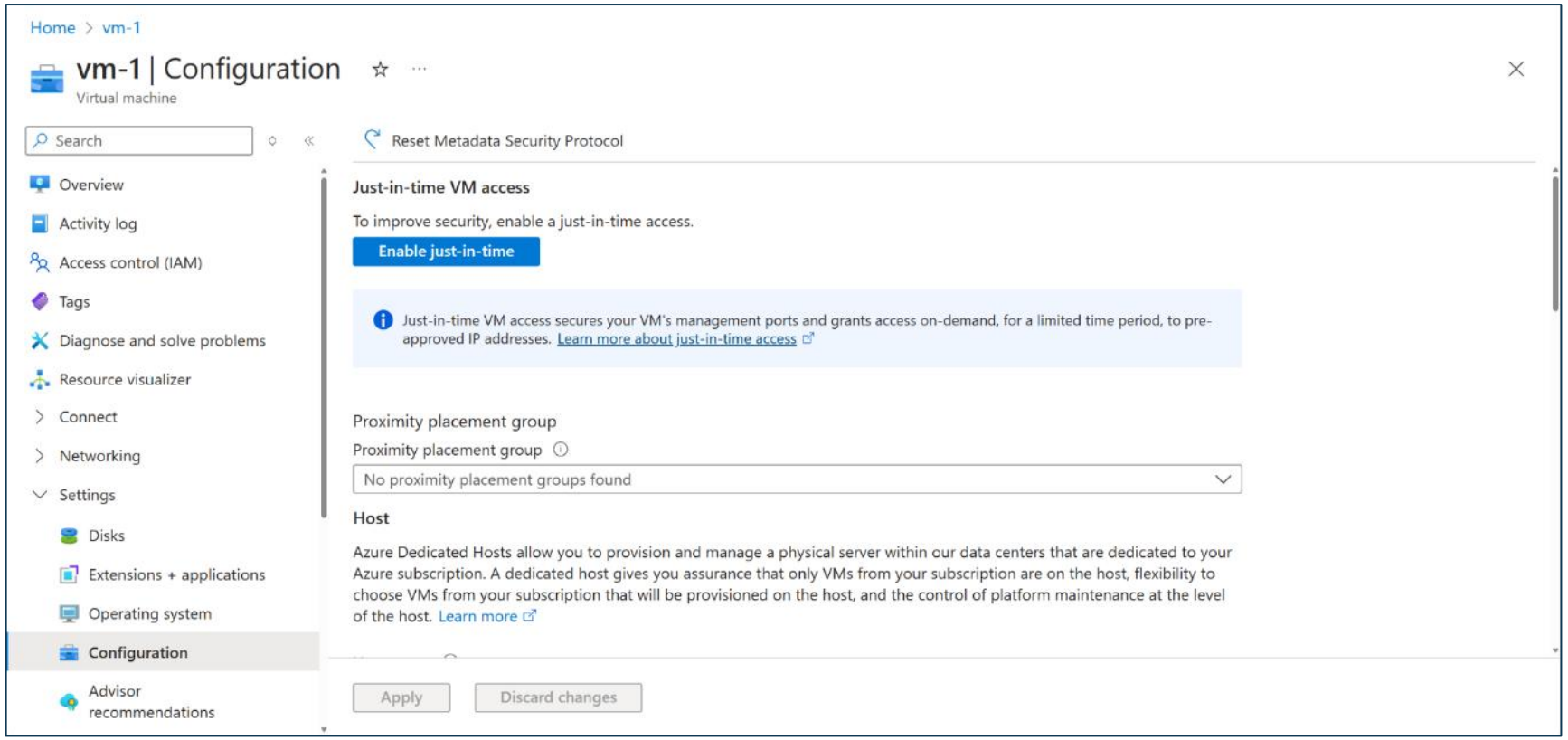
[Launch this Exercise in GitHub]



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.

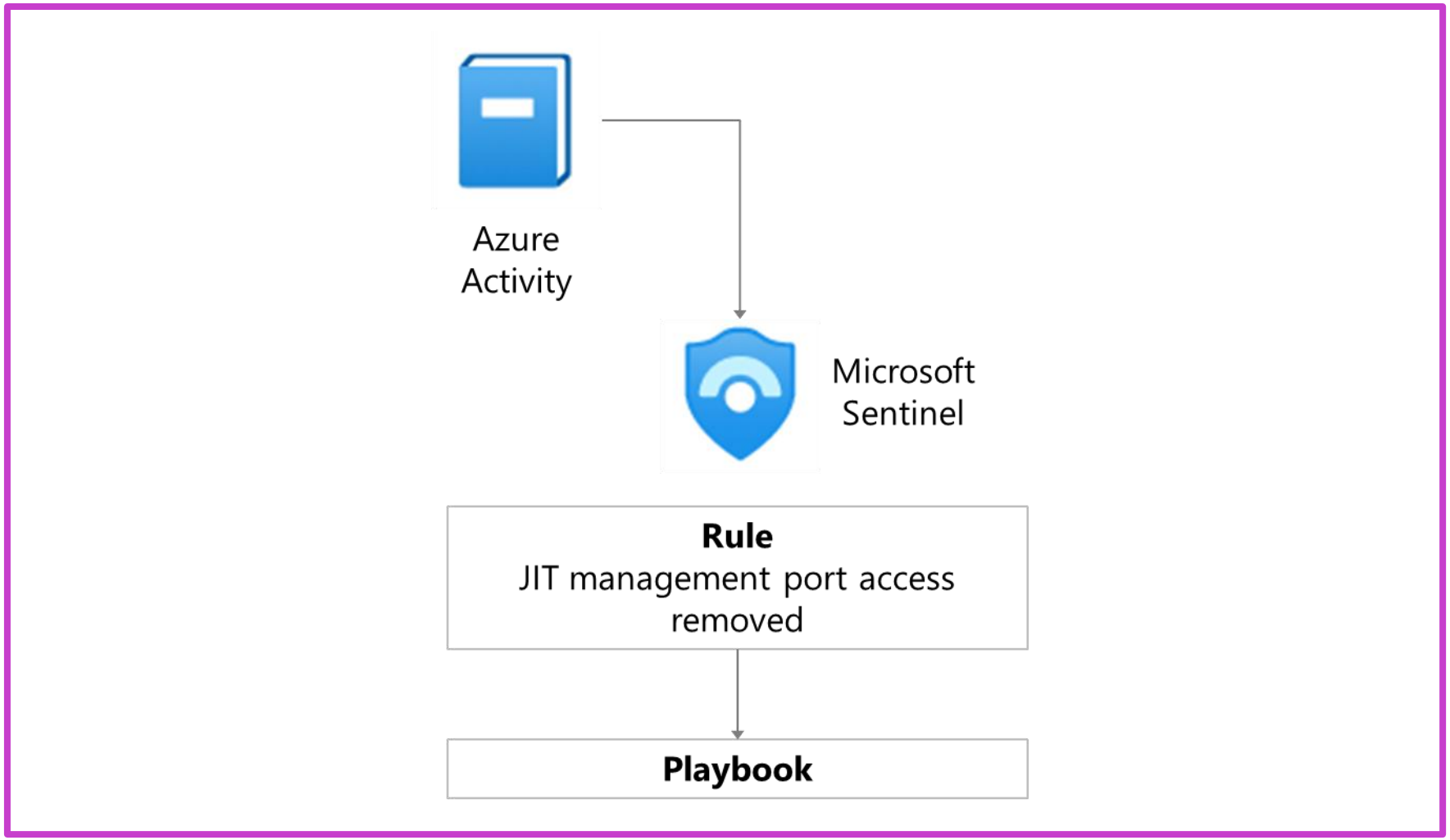
[Launch this Exercise in GitHub]



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