



AZ-500

Microsoft Azure Security Technologies



Agenda

- 1 Manage identity and access
- 2 Secure networking
- 3 Secure compute, storage, and databases
- 4 Manage security operations KV

Defender Cloud
Sentinel

Learning Path: Manage security operations

Plan, implement, and manage governance for security

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

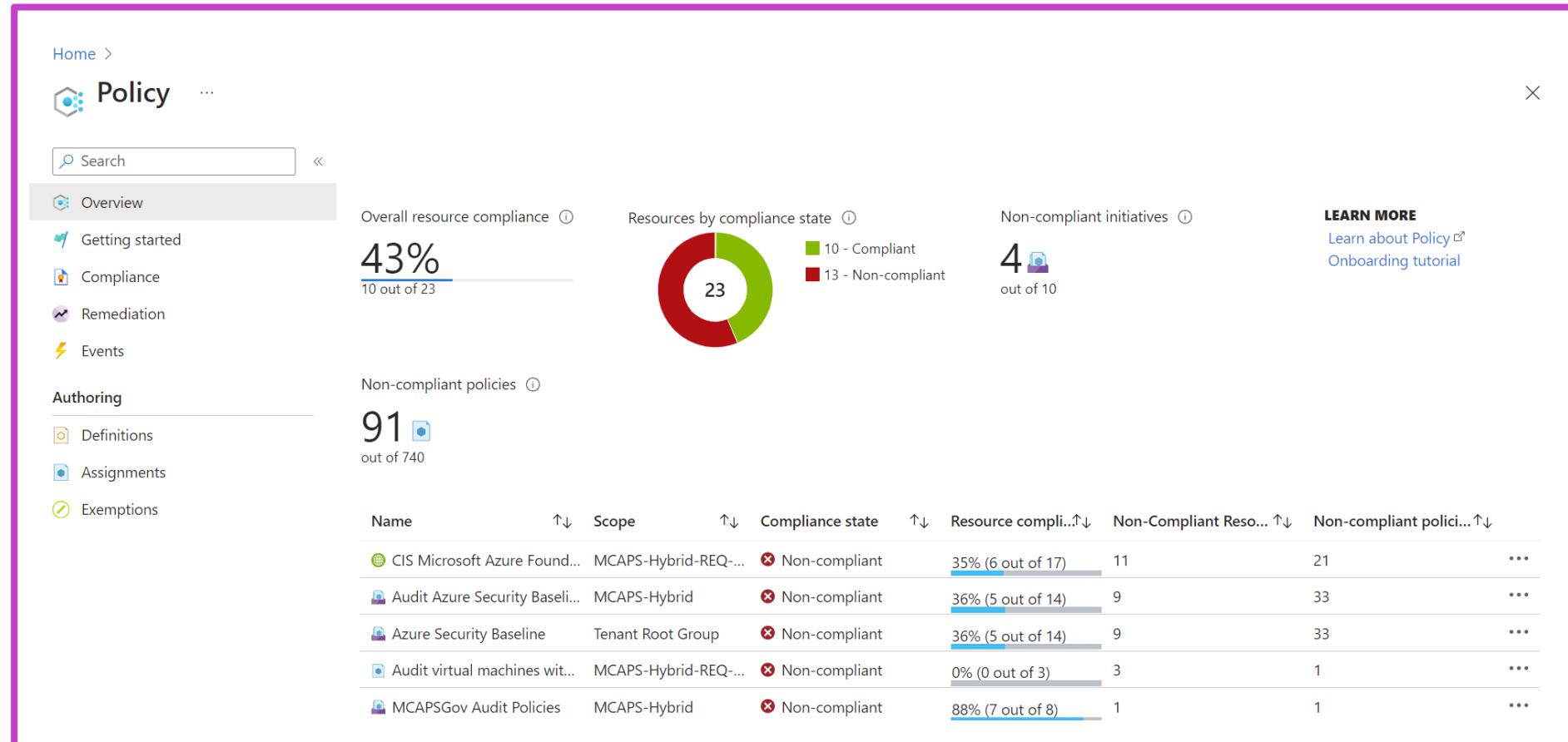
After completing this learning path, you will be able to:

- 1** Implement security operations, establish governance, 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.

Plan, implement, and manage governance for security

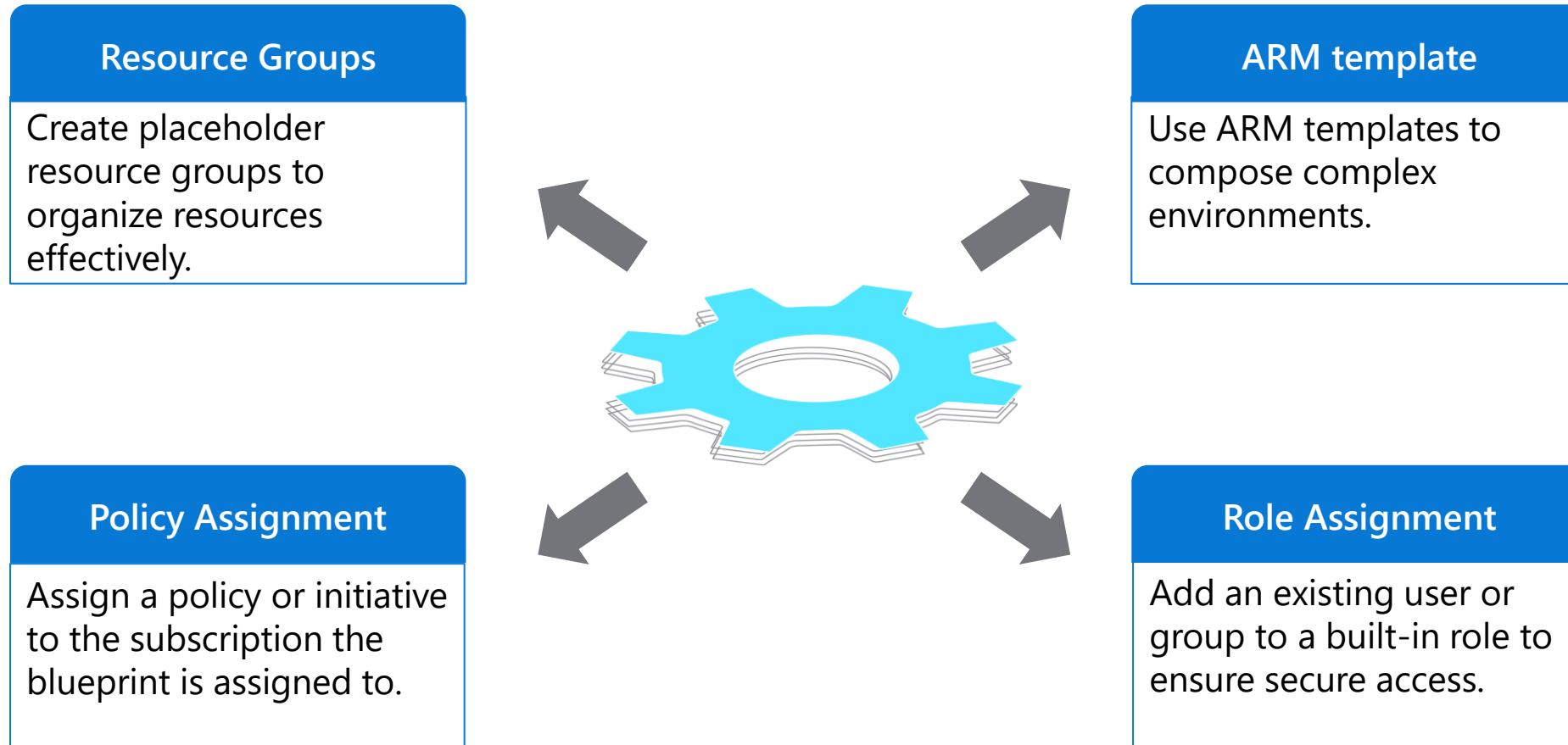
Create, assign, and interpret security policies and initiatives in Azure Policy

- Use Azure Policy for compliance with standards and SLAs.
- Assign policies and initiatives for future resources and compliance tracking.
- Resolve non-compliance and implement new policies organization-wide.

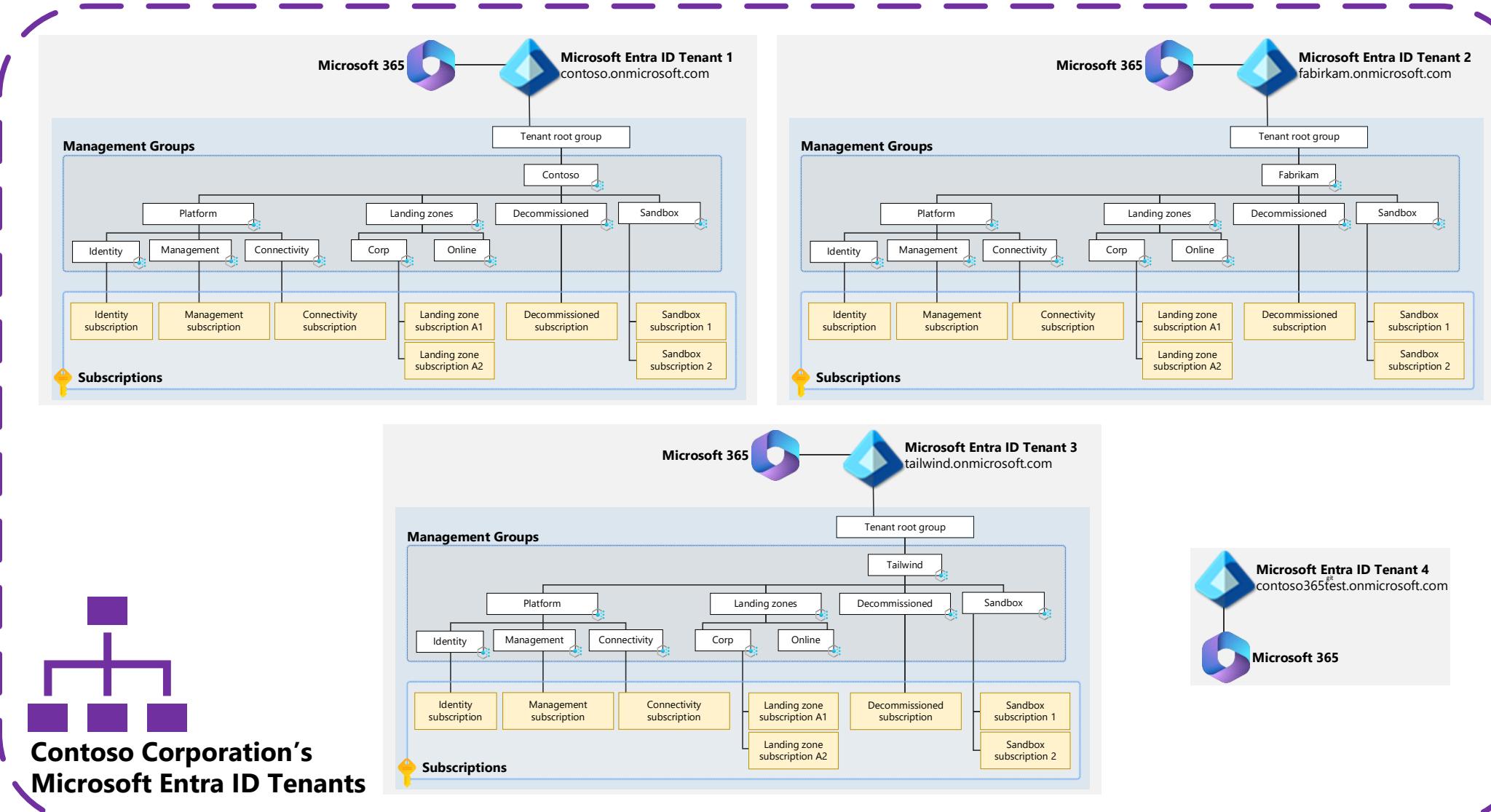


Configure security settings by using Azure Blueprints

Azure Blueprints supports the following resources as artifacts:

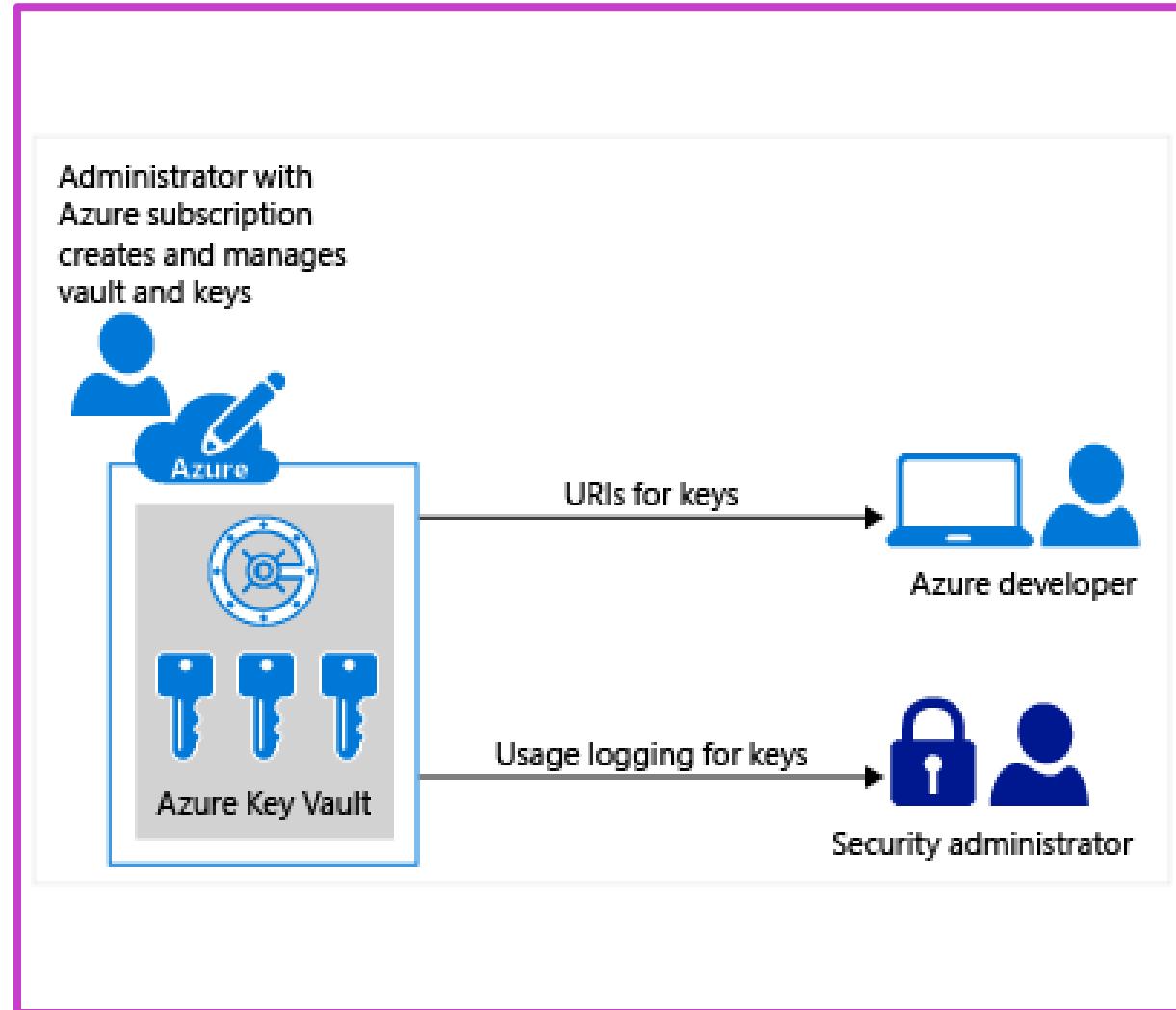


Deploy secure infrastructures by using a landing zone



Azure Key Vault

- Azure Key Vault securely stores API keys, passwords, certificates, and cryptographic keys.
- Supports vaults for software/HSM-backed keys and managed HSM pools for HSM-backed keys only.
- Offers managed identities for secure authentication and enforces TLS for data-in-transit protection.



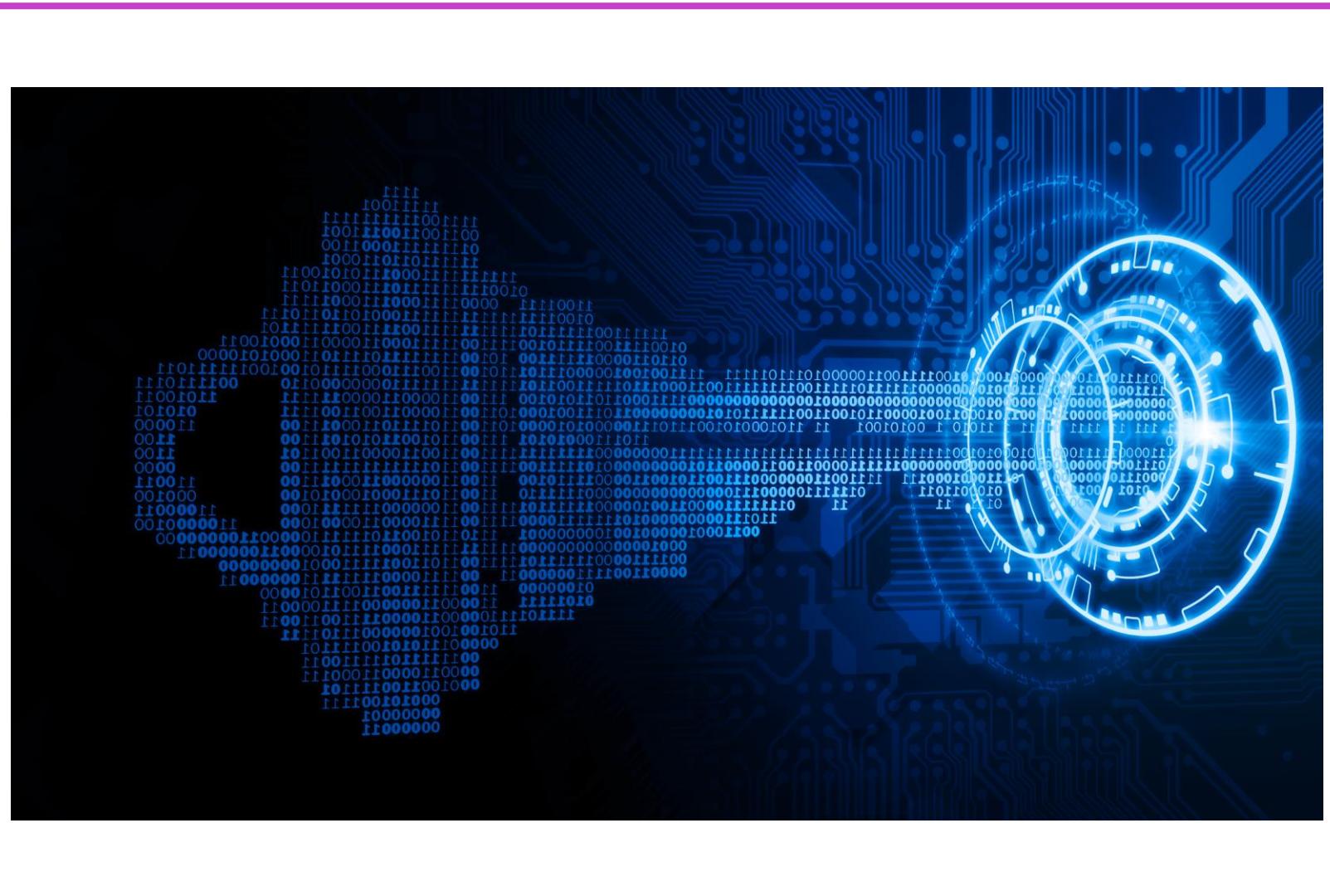
Azure Key Vault security

- Azure Key Vault securely stores API keys, passwords, certificates, and cryptographic keys.
- Supports vaults for software/HSM-backed keys and managed HSM pools for HSM-backed keys only.
- Offers managed identities for secure authentication and enforces TLS for data-in-transit protection.



Azure Key Vault authentication

- Authentication with Key Vault is integrated with Microsoft Entra ID to authenticate security principals.
- Security principals can be users, groups, or service principals with unique IDs for Azure resource access.
- Key Vault authentication flow involves token retrieval, firewall checks, and permission validation for operations.



Create and configure an Azure Key Vault

1. On the Azure portal, select **Create a resource**.
2. Search for “**Key Vault**”, select the relevant result and select **Create**.
3. Specify a name, subscription, and location, and complete the process

The screenshot shows the Azure Key Vault Overview page for a vault named "AKV-Contoso". The left sidebar lists navigation options: Home, Overview (selected), Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events, Settings, Keys, and Secrets. The main content area displays the "Essentials" section with the following details:

Resource group (change)	msbRG	Vault URI	https://akv-contoso.vault.azure.net/
Location	East US	Sku (Pricing tier)	Standard
Subscription (change)	mbaldwin - content development for Azure security	Directory ID	72f988bf-86f1-41af-91ab-2d7cd011db47
Subscription ID	60d1af23-8f73-401c-b411-b4c581ea61c2	Directory Name	Microsoft
		Soft-delete	Enabled
		Purge protection	Disabled

Recommend when to use a Dedicated HSM



Use Azure Dedicated HSM
when you need:

- FIPS 140-2 Level-3 compliance
- Single tenancy of the cryptographic storage device
- Full administrative control and sole access to the device for administrative purposes
- High application performance
- Unique cloud-based offerings



Best fit for “**lift-and-shift**” scenarios that require direct and sole access to HSM devices.



Unfit for scenarios such as: Microsoft cloud services that support encryption with customer-managed keys that are not integrated with Azure Dedicated HSM.

Configure access to Key Vault

Configure vault access policies



Old style

Configure Azure RBAC



New

You can use these options:

- Azure Portal: Under the **Principal** selection pane, configure the options.
- Azure CLI: Assign the access policy using the `az keyvault set-policy` command
- Azure PowerShell: Assign the access policy using the `Set-AzKeyVaultAccessPolicy` cmdlet

With Azure RBAC, you can have

- One place to manage all permissions across all key vaults
- The ability to set permissions on different scope levels: management group, subscription, resource group, or individual resources
- Separate permissions on individual keys, secrets, and certificates with Azure RBAC for key vault

Manage certificates, secrets, and keys



Manage certificates

- Azure Key Vault assists in handling X.509 certificates.
- Ensures secure storage, management, and policy formulation.
- Users can input contact details for alerts.



Manage secrets

- Granularly isolate secrets for enhanced application security.
- Store credentials in secret values; rotate bi-monthly.
- Oversee access using Key Vault logging.



Manage keys

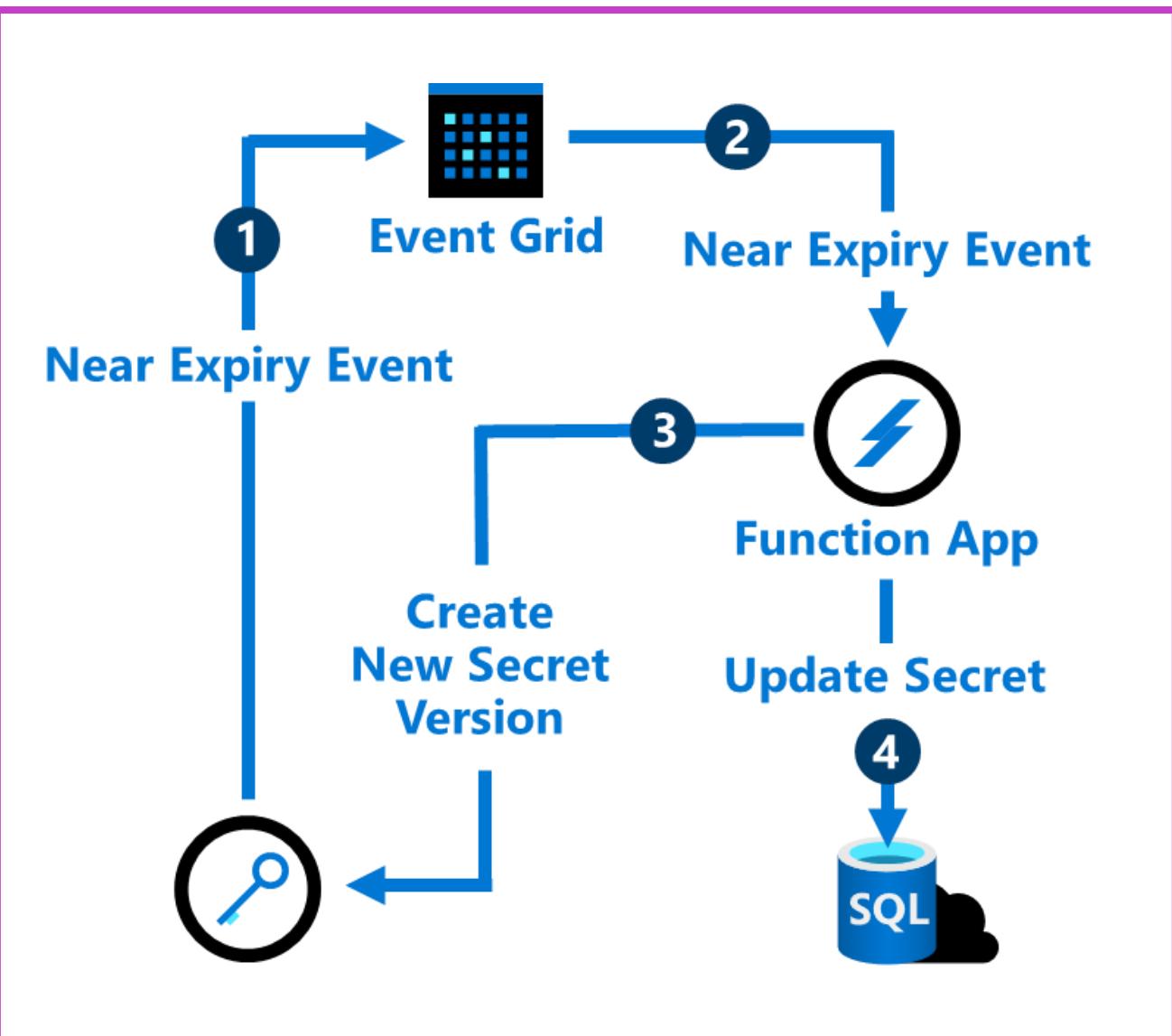
- Encryption keys: platform-managed or customer-managed.
- Storage options include Azure Key Vault and Dedicated HSM.
- Options vary by FIPS compliance, management overhead, and application suitability.

Configure key rotation

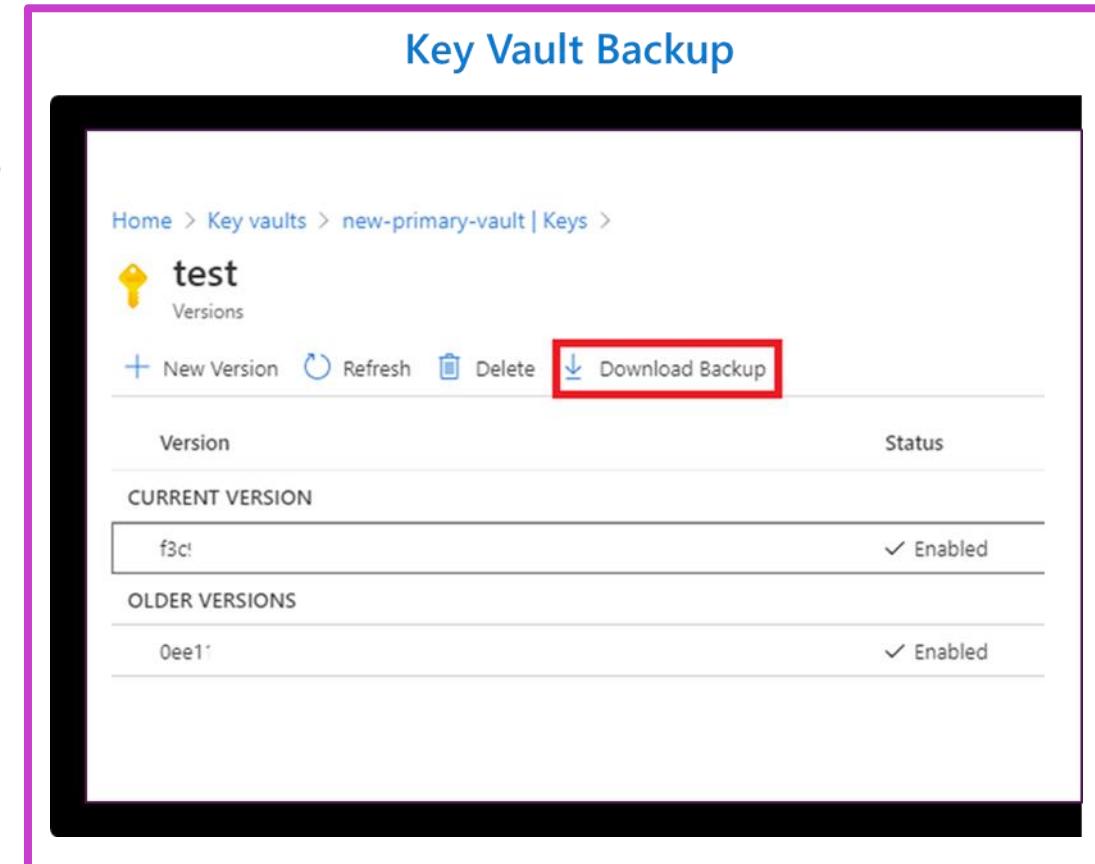
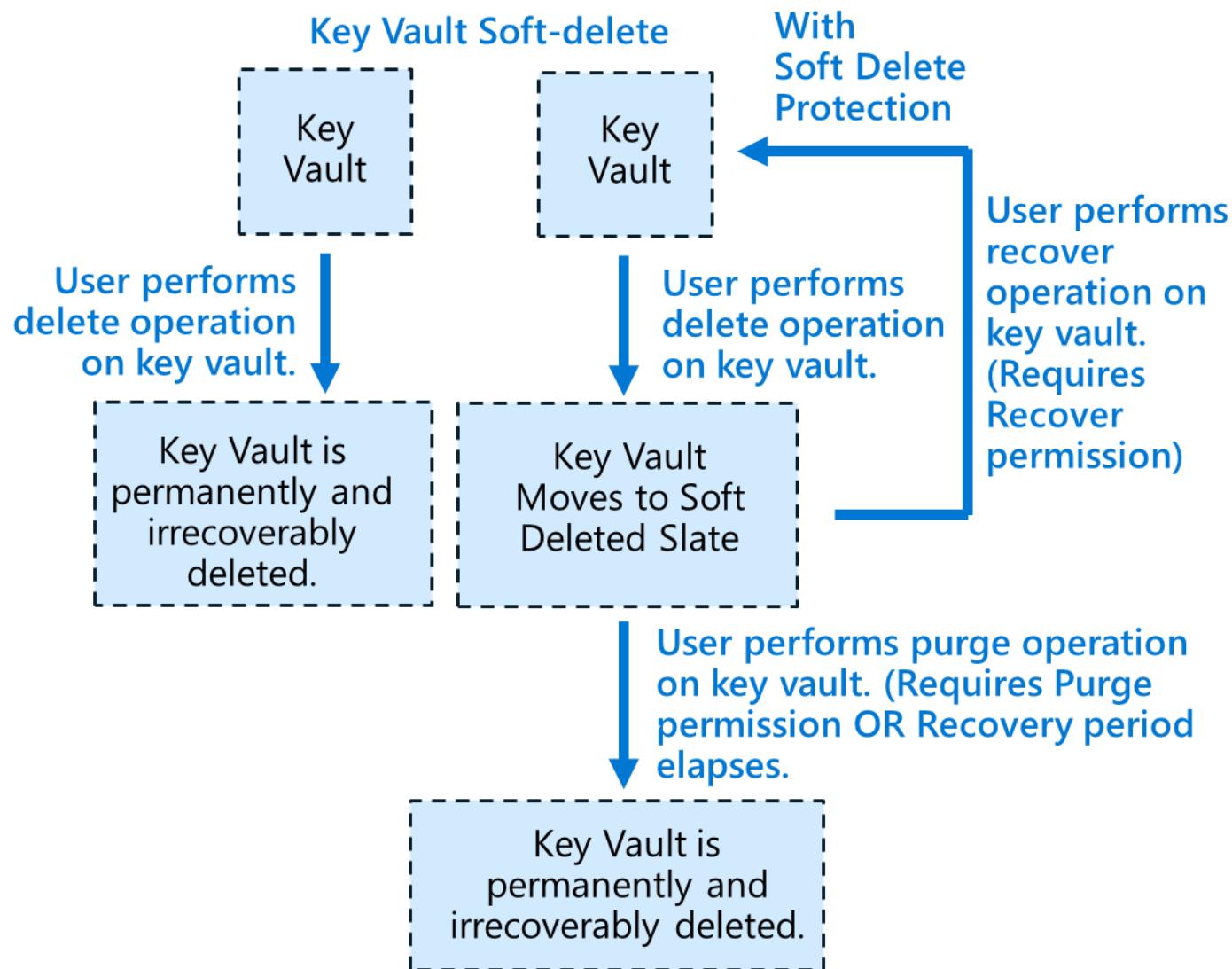
Update keys and secrets without affecting your application

Rotate keys and secrets in several ways:

- As part of a manual process
- Programmatically with the REST API
- With an Azure Automation script



Configure backup and recovery of secrets, certificates, and keys



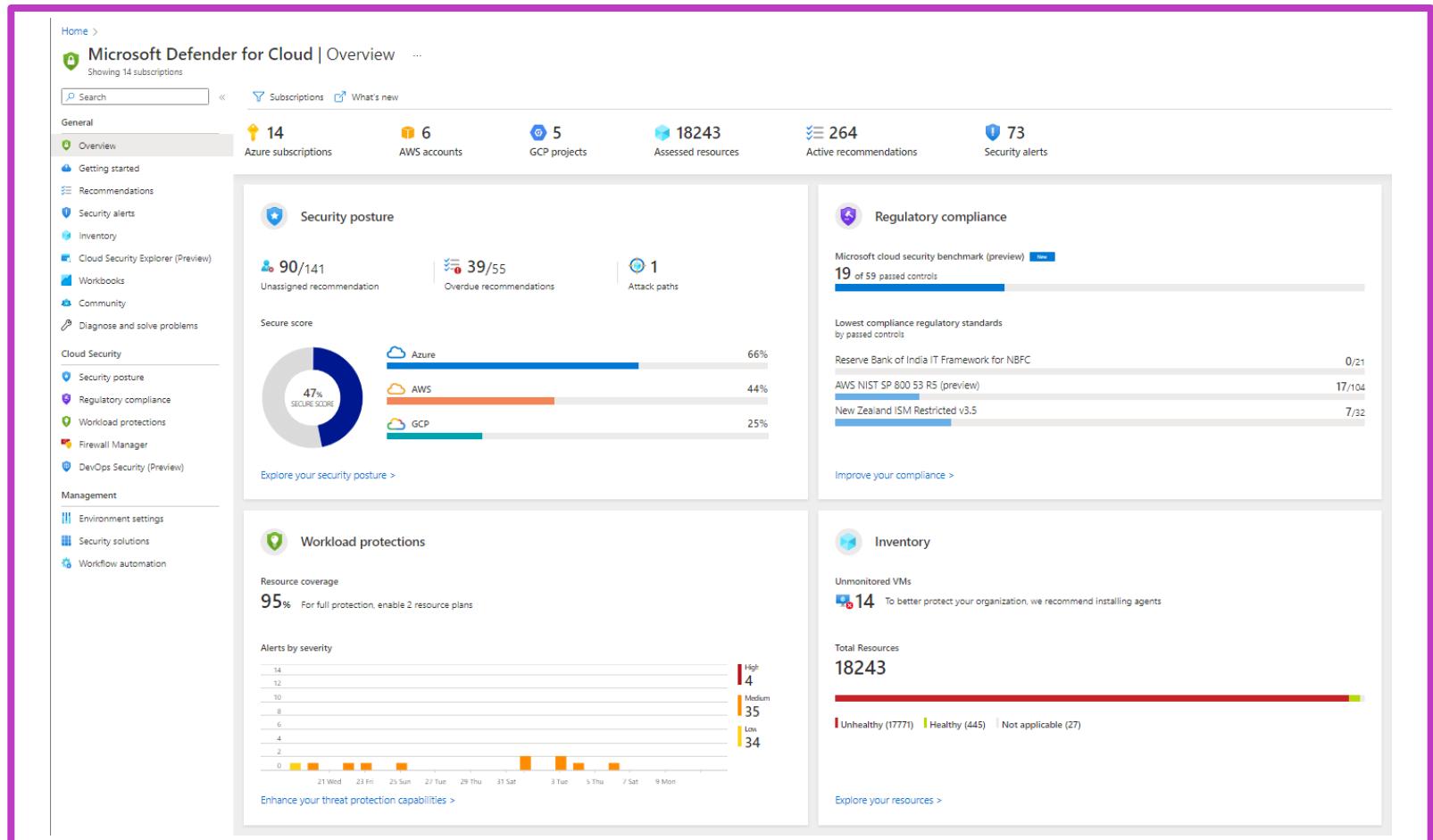
Manage security posture by using Microsoft Defender for Cloud

Implement Microsoft Defender for Cloud

Microsoft Defender for Cloud is a Security Posture Management and Workload Protection Platform for Azure, on-premises, and multicloud (Amazon AWS and Google GCP) resources.

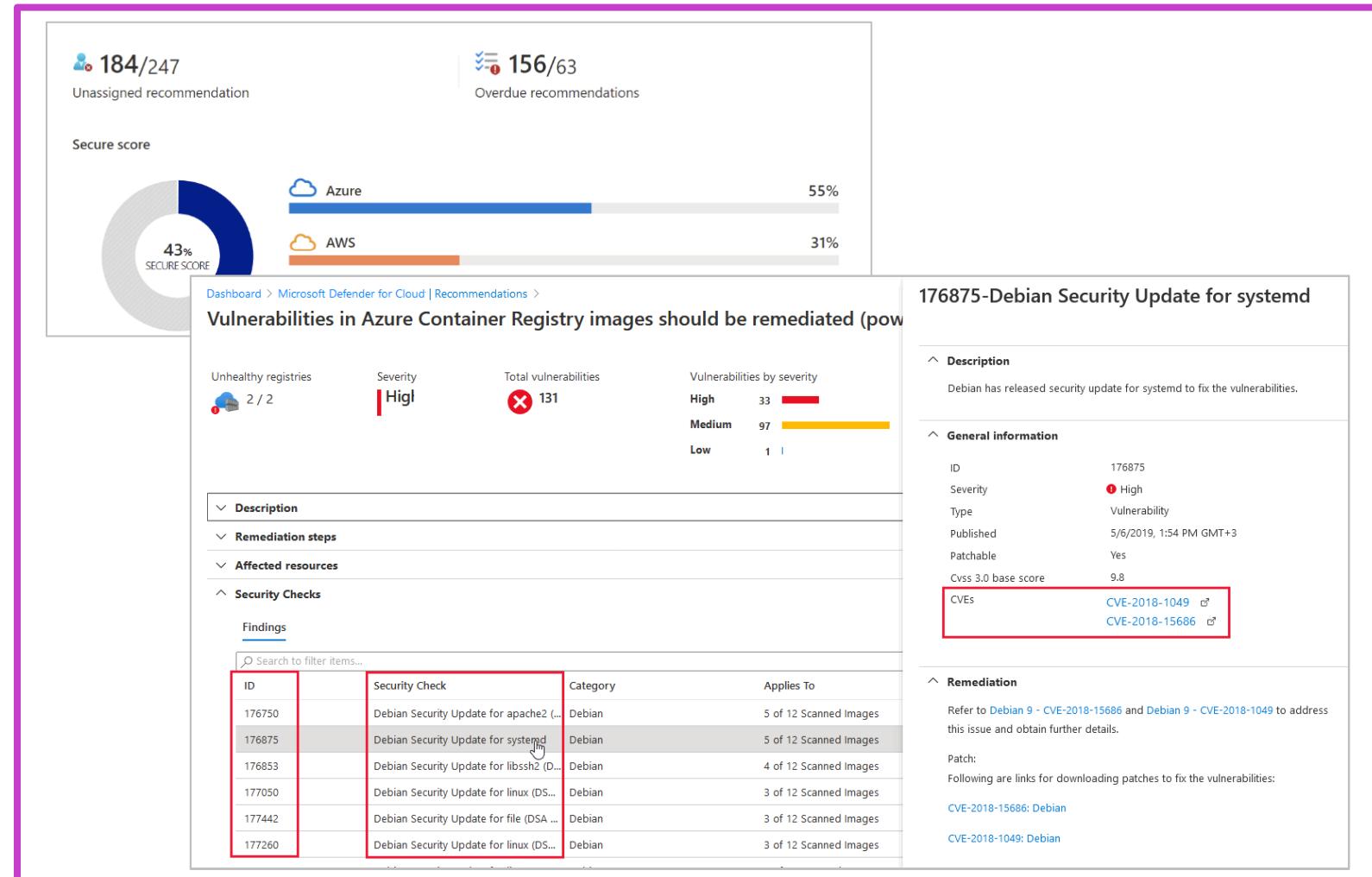
Microsoft Defender for Cloud's features covers the two broad pillars of cloud security:

1. Security Posture Management
2. Workload Protection



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 displays the Microsoft Defender for Cloud Regulatory compliance dashboard. On the left, a sidebar menu includes General, Cloud Security, and Management sections. The main area shows a summary of 2 subscriptions, with the 'NIST SP 800-53 R4' tab selected (marked with a circled '1'). Below this, a section titled 'AC. Access Control' is expanded, showing various control details (marked with a circled '2'). To the right, a separate window titled 'AC.2.7 Role-based Schemes' shows a table of actions (marked with a circled '3').

1. NIST SP 800-53 R4

2. AC. Access Control

3. AC.2.7 Role-based Schemes

Add industry and regulatory standards to 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

Settings | Security policy ...

CyberSecSOC

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 initiatives 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 interface. On the left, a blue sidebar features a clipboard icon with a pencil and a plus sign, indicating the process of adding a new initiative. The main area displays two windows:

- Add custom initiatives:** A modal window with a red border. It contains a "Create new" button (highlighted with a red box) and a "Refresh" button. Below these are instructions: "To create a new [custom policy initiative](#), click **Create new**. Or, to add an existing initiative from the list below, click **Add** in the relevant row." A note states: "After adding the policy initiative, it will be listed as a recommendation in the **Recommendations** blade, and to have it added in the **Regulatory compliance** dashboard." A table lists one initiative:

NAME	DESCRIPTION	STATUS	Actions
Organizational policy	custom policy	Not assigned	Add

The "Add" button in the table is also highlighted with a red box.
- Organizational policy:** A configuration page with a red border. It has tabs for Basics, Parameters, Remediation, Non-compliance messages, and Review + create. The Basics tab is selected. It includes fields for Scope (with a link to "Learn more about setting the scope"), Exclusions (with a link to "Optional 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



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

Identify and monitor external-facing assets

With Microsoft Defender External Attack Surface Management, you can monitor internet-exposed assets with a global network that graphs online relationships.

It provides:



Continuous visibility beyond the firewall by:

Discovering unmanaged resources

Providing multicloud visibility

Identifying exposed weaknesses



Capabilities such as:

Real-time inventory

Attack surface visibility

Exposure detection and prioritization

Integrated threat protection

Configure and manage threat protection by using Microsoft Defender for Cloud

Enable workload protection services in Microsoft Defender for Cloud

- To enhance security on multiple subscriptions in Defender for Cloud, select "**Getting started.**"
- Choose subscriptions and workspaces on the "**Upgrade**" tab. Click "**Upgrade.**"

- Activate enhanced security in Defender for Cloud via Environment settings.
- Choose the desired subscription or workspace.
- Select "**Enable all**" for comprehensive Defender for Cloud plans.

The screenshot shows the Microsoft Defender for Cloud Getting started page. On the left, there's a sidebar with navigation links like Home, General, Overview, Getting started (which is highlighted with a red box), Recommendations, and Security alerts. The main content area has a heading "Enable Microsoft Defender for Cloud's enhanced security features on your subscriptions. Get started with a 30-day free trial". It includes a "Upgrade" button (also highlighted with a red box) and a "Learn more" link. Below this, there's a section titled "Enable Defender for Cloud on 1 subscriptions" with a table showing resource counts and status. At the bottom is a large blue "Upgrade" button.

The screenshot shows the Microsoft Defender for Cloud Environment settings page under the "Settings | Defender plans" section. It has a "Select Defender plan" dropdown with an "Enable all" button highlighted by a red box. The page lists various service categories: Defender CSPM (Free), Servers (Plan 2), App Service, Databases, Storage, Containers, and Key Vault. Each category has its own "Details >" link and some usage statistics.

Configure Microsoft Defender for Servers

Remember the following while configuring Microsoft Defender for Servers:

- This product includes automatic, native integration with Microsoft Defender for Endpoint.
- You can enable Defender for Servers and then enable Defender for Endpoint unified integration to provision the Defender for Endpoint agent on all supported machines in the subscription.
- To configure Defender for Servers, you can choose from:
 - Plan 1: Includes Microsoft Defender for Endpoint (MDE) integration, automatic provisioning, and lower licensing cost.
 - Plan 2: Includes everything in Defender for Servers Plan 1 + All other enhanced security features.



Configure Microsoft Defender for Azure SQL Database

Enable Microsoft Defender for Azure SQL Database at subscription or resource level.

Access Defender for Cloud in the server's Security area.

If enabled, choose "**Configure**" to modify **Defender for SQL** settings.

The screenshot shows the Azure Security Center portal with a focus on the 'Azure Defender for SQL' settings for a specific database. The interface is divided into two main sections: a left panel with quick access metrics and a right panel with detailed configuration options.

Left Panel Metrics:

- 1:** Shows 0 Recommendations, 0 Security alerts, and 0 Findings. The status 'Azure Defender for SQL: Disabled' is highlighted with a red box.
- 2:** Shows 2 Recommendations, 0 Security alerts, and 3 Findings. The status 'Azure Defender for SQL: Enabled at the subscription-level (Configure)' is highlighted with a red box and a cursor is hovering over it.

Right Panel Configuration:

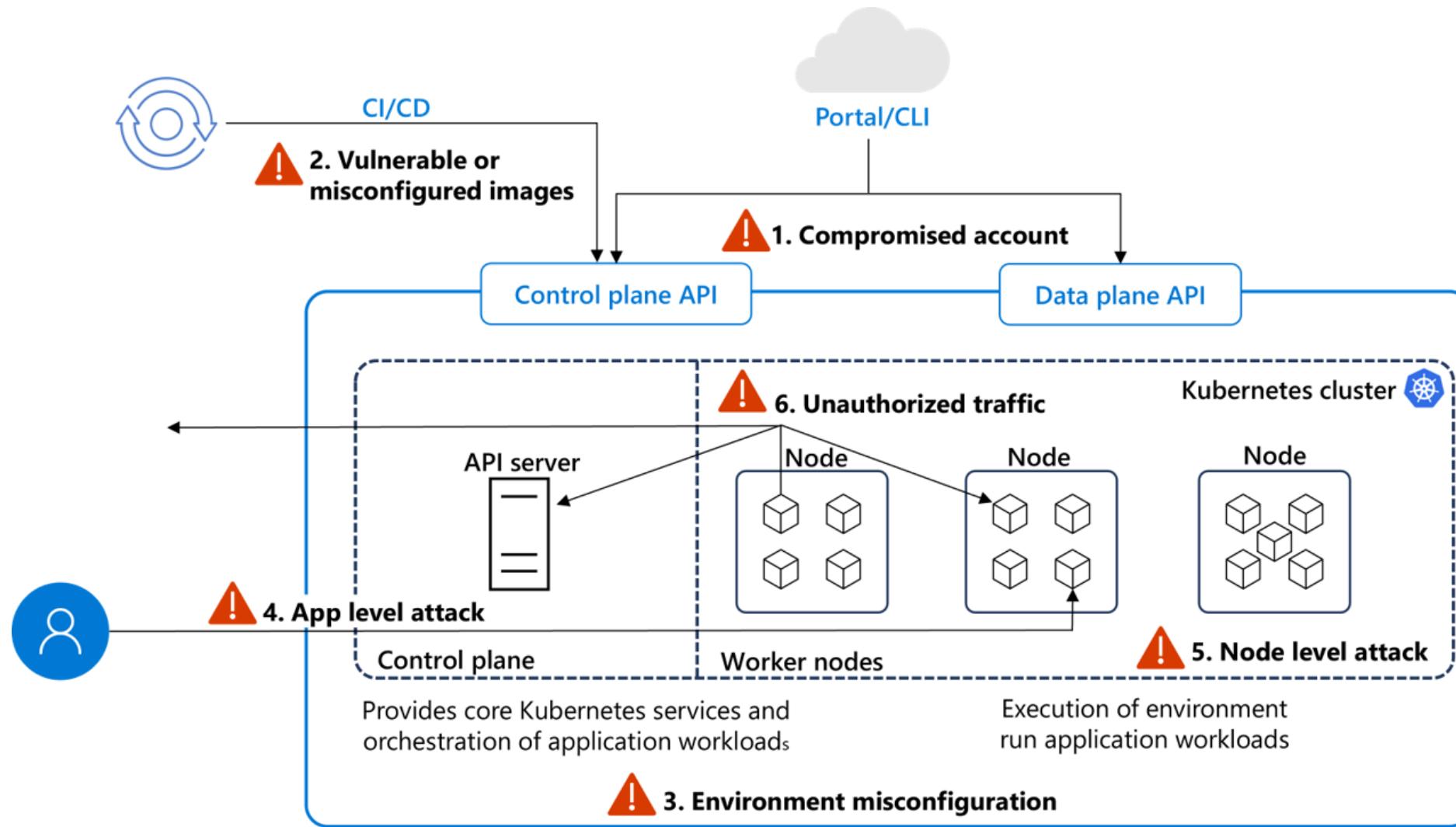
- Server settings:** Shows the server name 'ads-server' and buttons for 'Save', 'Discard', and 'Feedback'.
- AZURE DEFENDER FOR SQL:** A toggle switch is set to 'ON'. A note states: 'Azure Defender for SQL costs 15 USD/server/month. It includes Vulnerability Assessment and Advanced Threat Protection. We invite you to a trial period for the first 30 days, without charge.'
- VULNERABILITY ASSESSMENT SETTINGS:** Includes fields for 'Subscription' (set to 'ASC DEMO') and 'Storage account' (set to 'sqlvaujrhslwghh7a2').
 - Periodic recurring scans: A toggle switch is set to 'ON'. A note says: 'Scans will be triggered automatically once a week. In most cases, it will be on the day Vulnerability Assessment has been enabled and saved. A scan result summary will be sent to the email addresses you provide.'
 - Send scan reports to: A dropdown menu is set to 'Email addresses'.
 - Also send email notification to admins and subscription owners: A checkbox is checked.
- ADVANCED THREAT PROTECTION SETTINGS:** Includes fields for 'Send alerts to' (set to 'Email addresses') and 'Advanced Threat Protection types' (set to 'All').
 - Send alerts to: A dropdown menu is set to 'Email addresses'.
 - Also send email notification to admins and subscription owners: A checkbox is checked.
 - Advanced Threat Protection types: A dropdown menu is set to 'All'.
- Other Options:** Includes a note about enabling auditing for better threat investigation experience.

Container security in Microsoft Defender for Containers

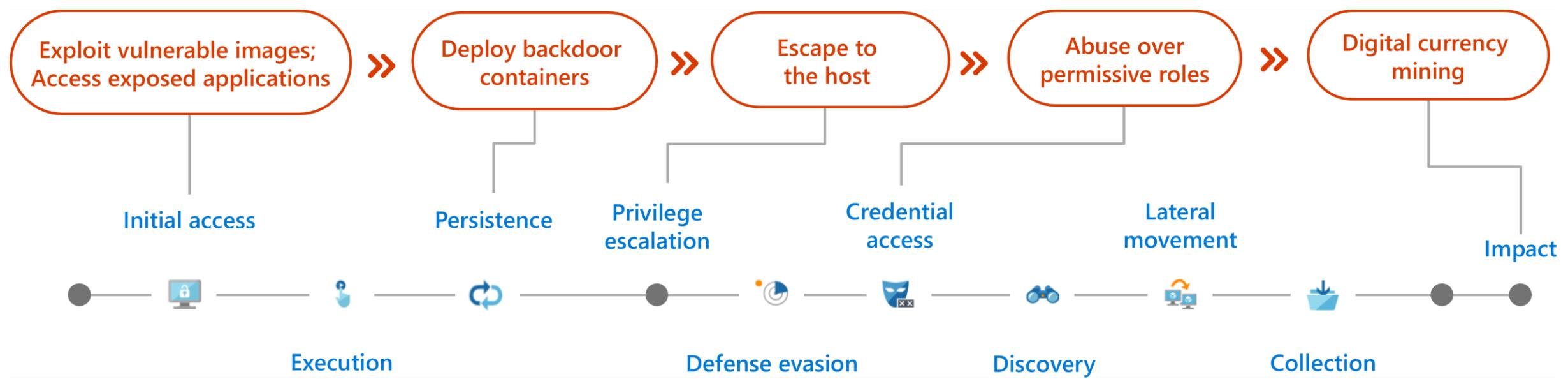
The screenshot shows the Microsoft Defender for Cloud Recommendations interface. On the left, a sidebar lists navigation options: General, Overview, Getting started, Recommendations (which is selected), Security alerts, Inventory, Workbooks, Community, Diagnose and solve problems, Cloud Security, Security 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 at the top allows filtering by recommendation status, severity, and resource type. The resource type filter is highlighted with a red box.

- 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

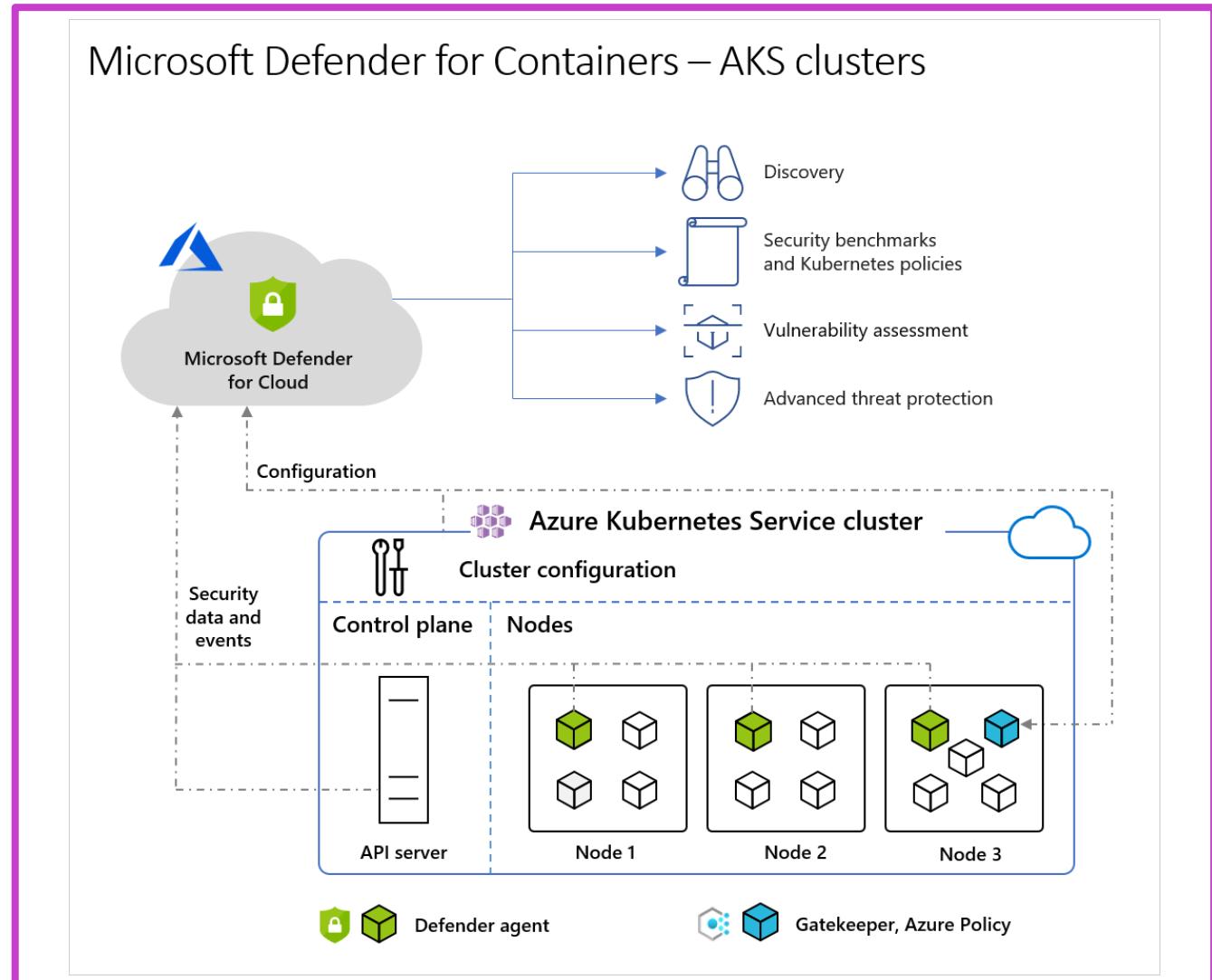


Common attack techniques



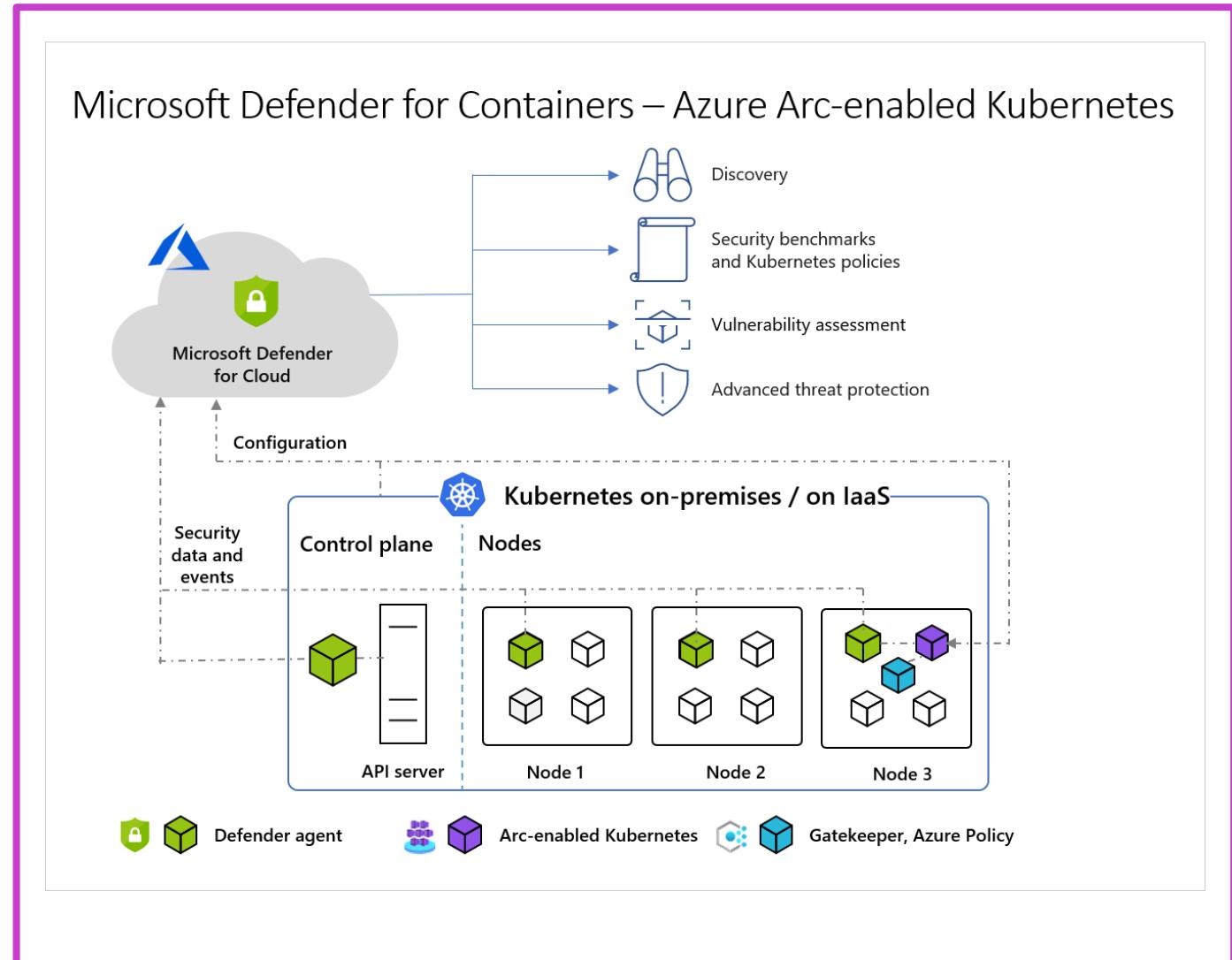
Architecture diagram of Defender for Cloud and AKS clusters

- 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.



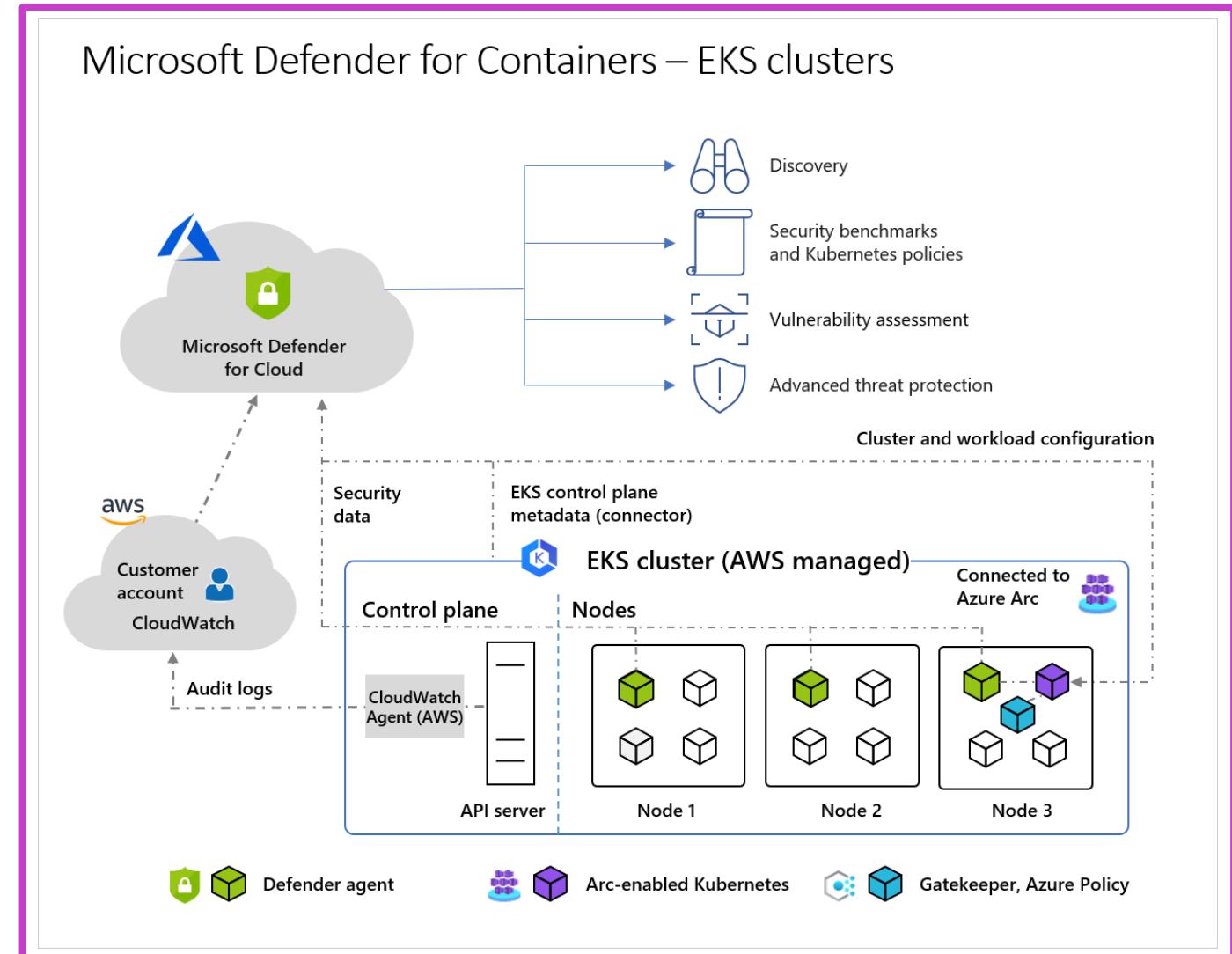
Architecture diagram of Defender for Cloud and Arc-enabled Kubernetes clusters

- 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.



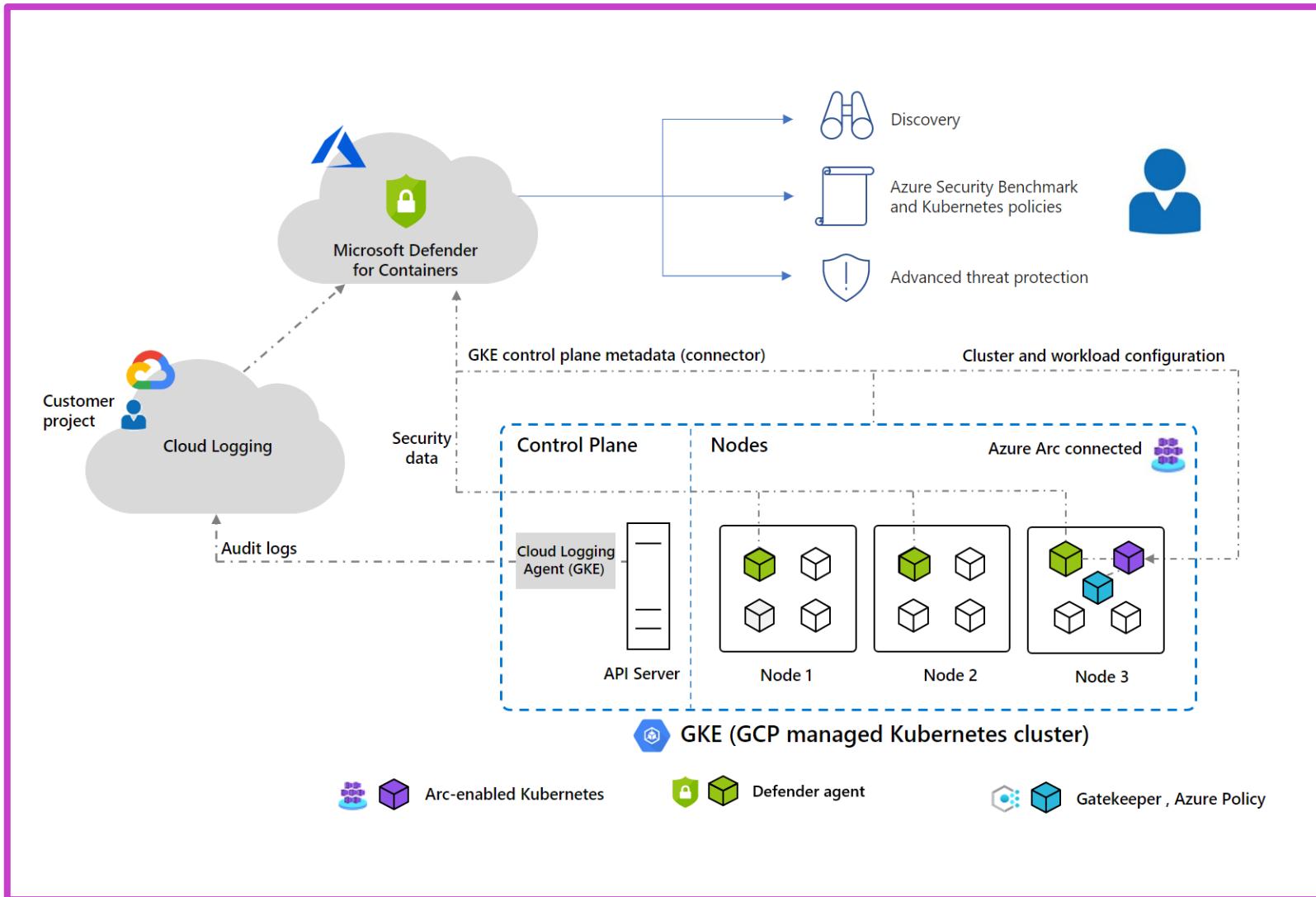
Architecture diagram of Defender for Cloud and EKS clusters

- 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.



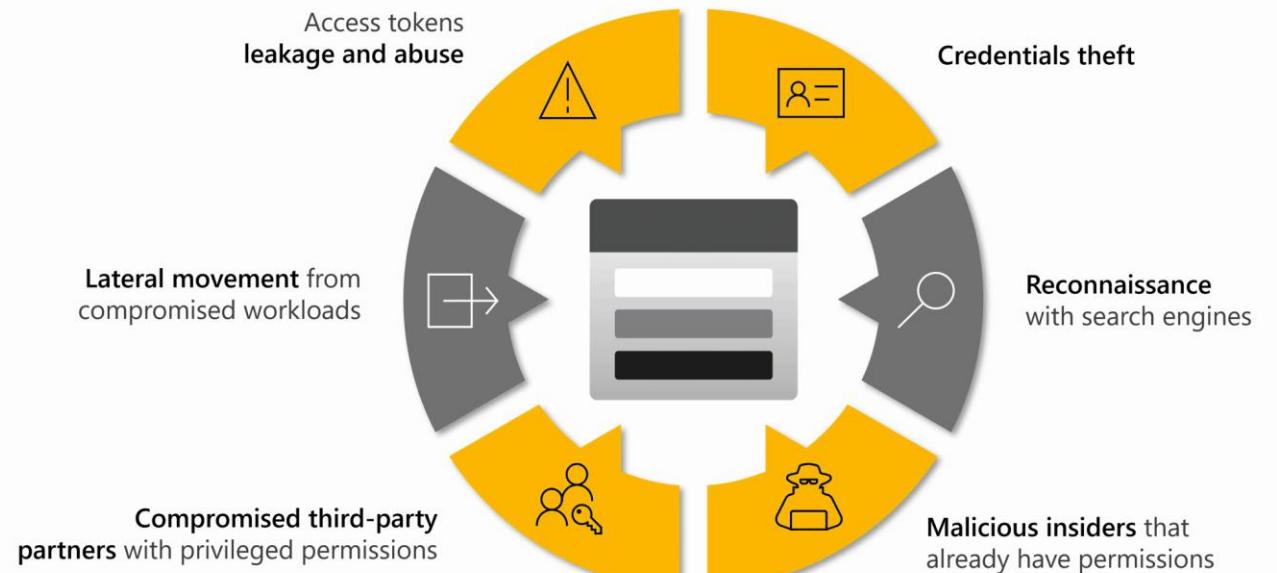
Vulnerability assessments for Azure

The screenshot shows the Microsoft Defender for Cloud Recommendations page. The top navigation bar includes 'Home > Microsoft Defender for Cloud' and 'Showing subscription 'CyberSecSOC''. Below the navigation is a search bar and various filter options like 'Refresh', 'Download CSV report', 'Open query', 'Governance report', and 'Guides & Feedback'. On the left, a sidebar under 'General' has sections for 'Overview', 'Getting started', 'Recommendations' (which is selected), 'Attack path analysis', 'Security alerts', 'Inventory', 'Cloud Security Explorer', 'Workbooks', 'Community', 'Diagnose and solve problems', 'Cloud Security' (with sub-options like 'Security posture', 'Regulatory compliance', 'Workload protections', 'Firewall Manager', 'DevOps security (preview)'), 'Management', and 'Environment settings'. The main content area displays a summary: 'Secure score 35%', '176/249 Active recommendations', and '184 Attack path'. It also includes a 'Search recommendations' bar and filters for 'Recommendation status == None', 'Severity == None', 'Resource type == None', and 'Add filter'. A table lists recommendations with columns for 'Name', 'Max score', 'Current score', 'Potential sc...', 'Status', and 'Unhealthy resources'. One specific recommendation, 'Container registry images should have vulnerability findings resolved (powered by Microsoft Defender Vulnerability Management)', is highlighted with a red border.

- Azure Vulnerability Assessment: Easy discovery and remediation for container vulnerabilities across Azure Container Registry.
- Continuous scanning triggers for newly pushed images and those running in AKS clusters.
- Detailed scan process includes inventory creation, vulnerability reports, and continuous rescans.

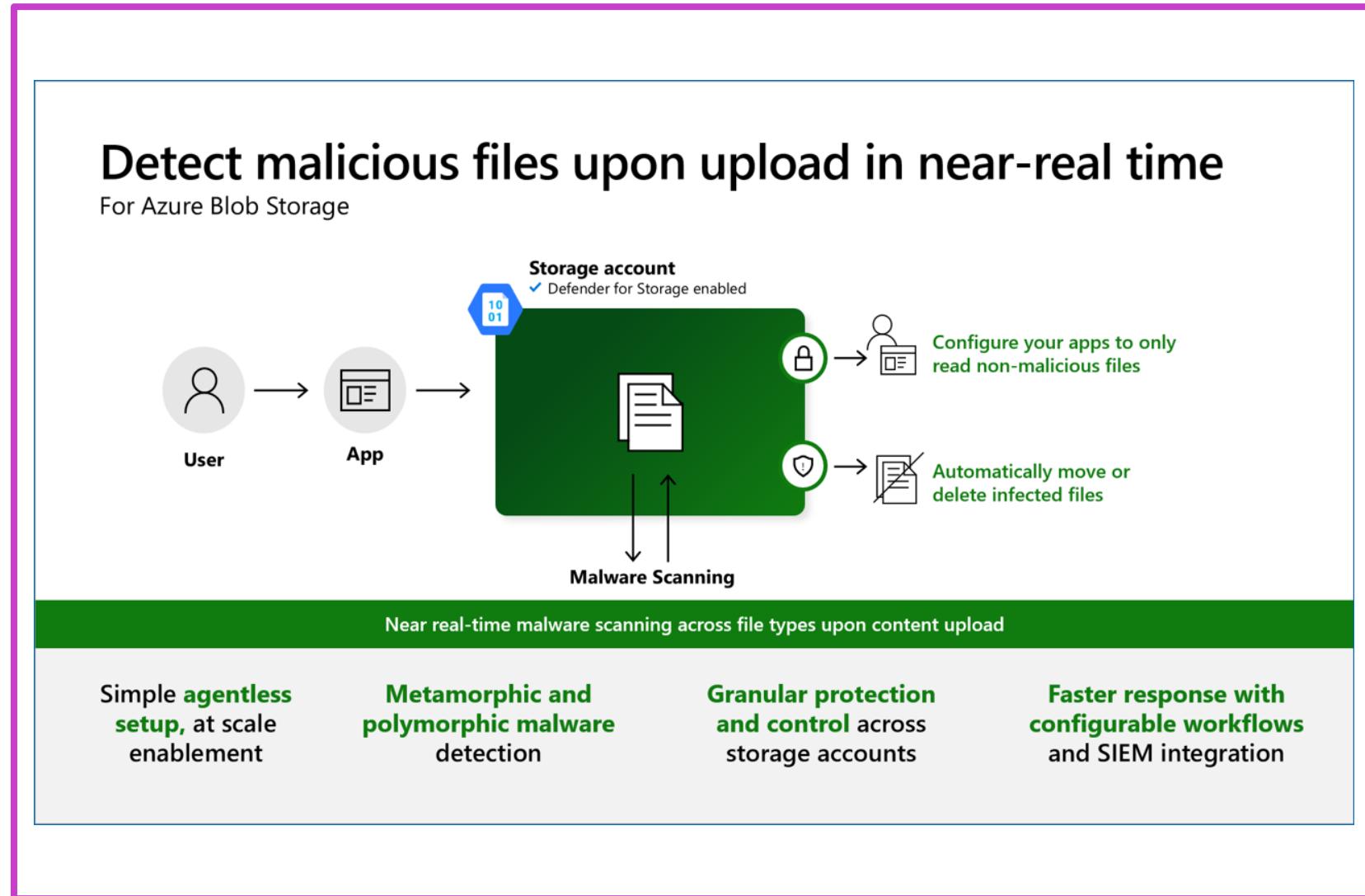
Microsoft Defender for Storage

- 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.



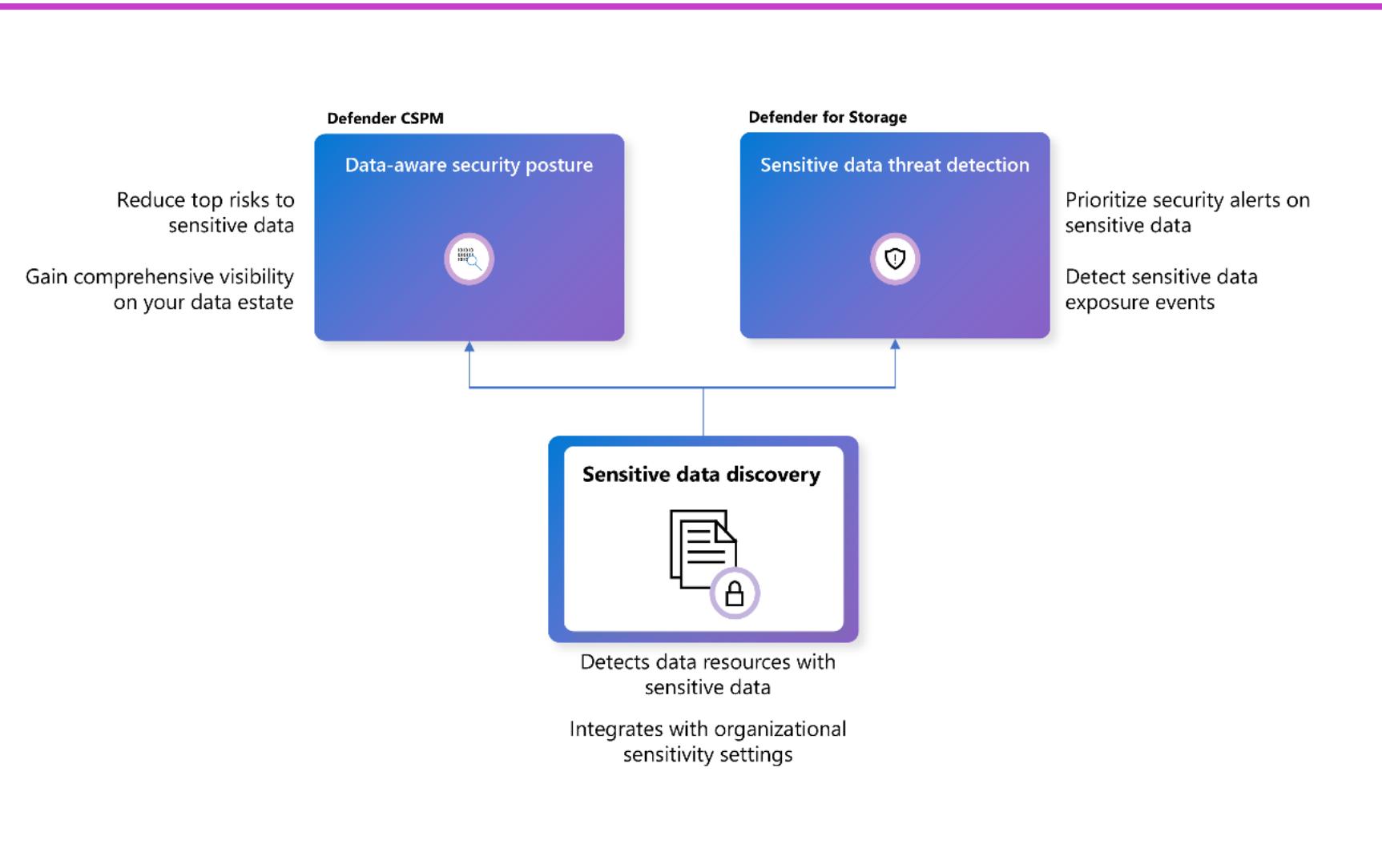
Malware scanning in Defender for Storage

- 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.

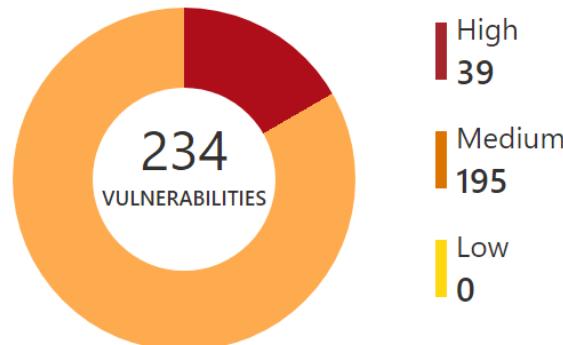
The screenshot shows the Azure Policy Definitions interface. The top navigation bar includes 'Policy | Definitions', a search bar, and buttons for 'Policy definition', 'Initiative definition', and 'Refresh'. The left sidebar has links for 'Overview', 'Getting started', 'Compliance', 'Remediation', and 'Events'. The main area displays a table of policy definitions with columns for 'Name', 'Definition location', 'Policies', 'Type', 'Definition type', and 'Category'. Two entries are visible: 'Configure Microsoft Defender for Storage to be enabled' (BuiltIn, Policy, Security Center) and 'Configure basic Microsoft Defender for Storage to be enabled (Activity Monitoring only)' (BuiltIn, Policy, Security Center). A note at the top states: 'The export to GitHub experience has been deprecated due to scalability issues. We are looking to introduce a similar experience using SDK in our documentation.' Below this, a detailed view of the first policy definition is shown. The title is 'Configure Microsoft Defender for Storage to be enabled'. The 'Assign' button is highlighted with a mouse cursor. The 'Essentials' section shows the policy's name, description, available effects, category, definition location, ID, type, and mode. The 'Definition' tab is selected, displaying the JSON code for the policy:

```
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 }
```

Defender for Cloud DevOps Security

Security Overview

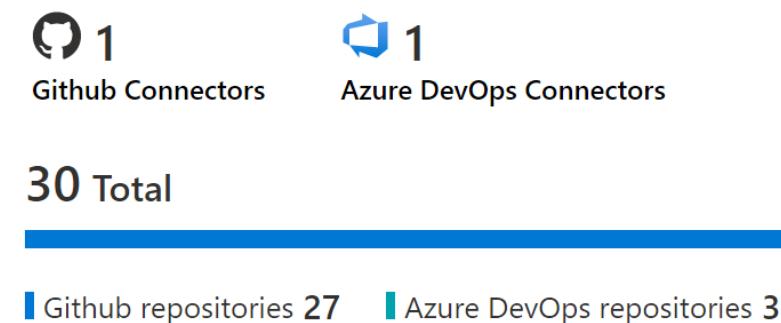
DevOps security vulnerabilities ⓘ



DevOps security results



DevOps coverage



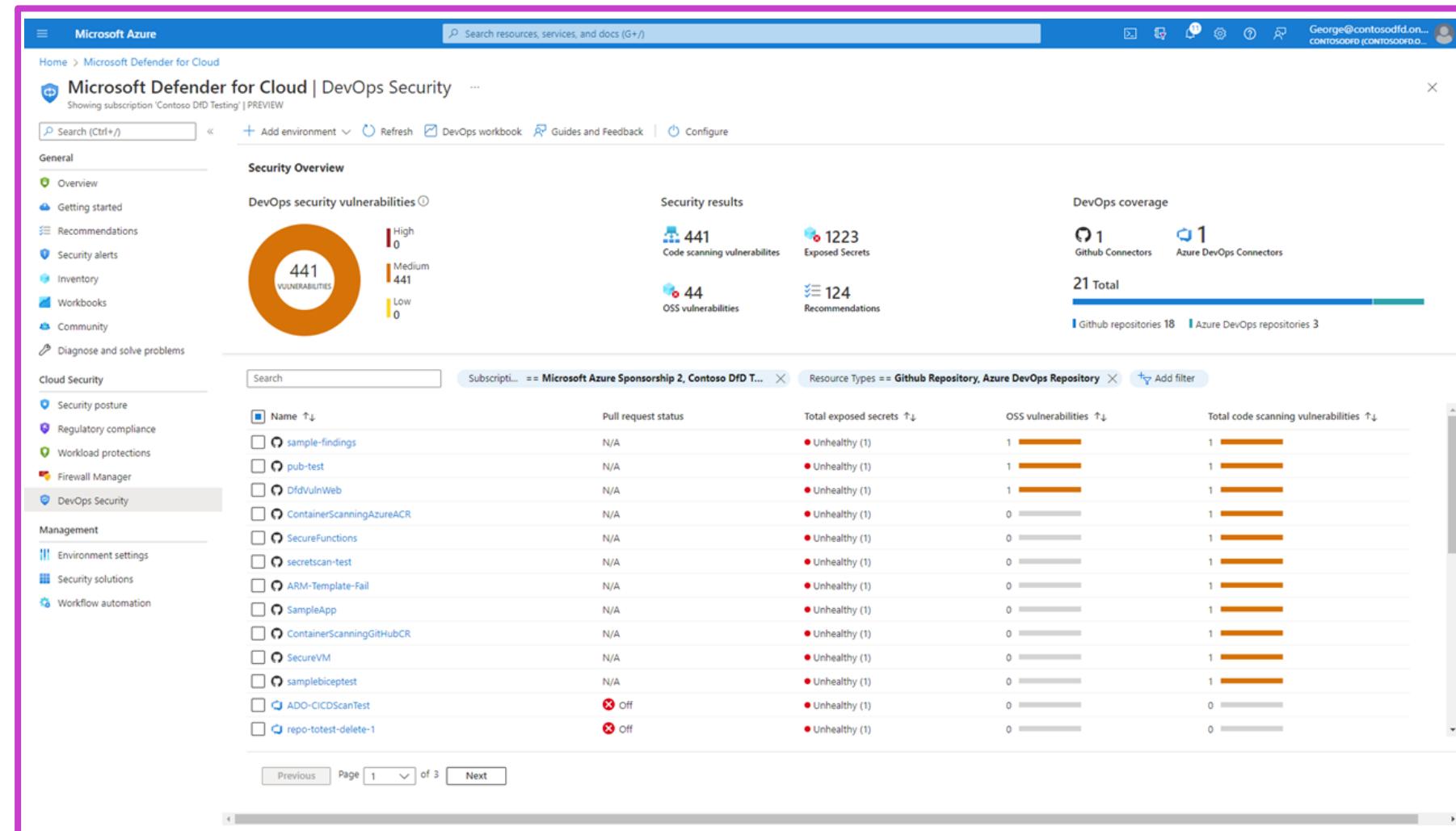
- Provides visibility, posture management, threat protection across Azure, AWS, GCP, on-premises.
- Centralizes DevOps security, integrates with Azure DevOps, GitHub, GitLab for application protection.
- Prioritizes code remediation with contextual insights, secures IaC templates, container images.

Defender for Cloud DevOps Security required permissions

Feature	Permissions
Connect DevOps environments to Defender for Cloud	<ul style="list-style-type: none">• 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.



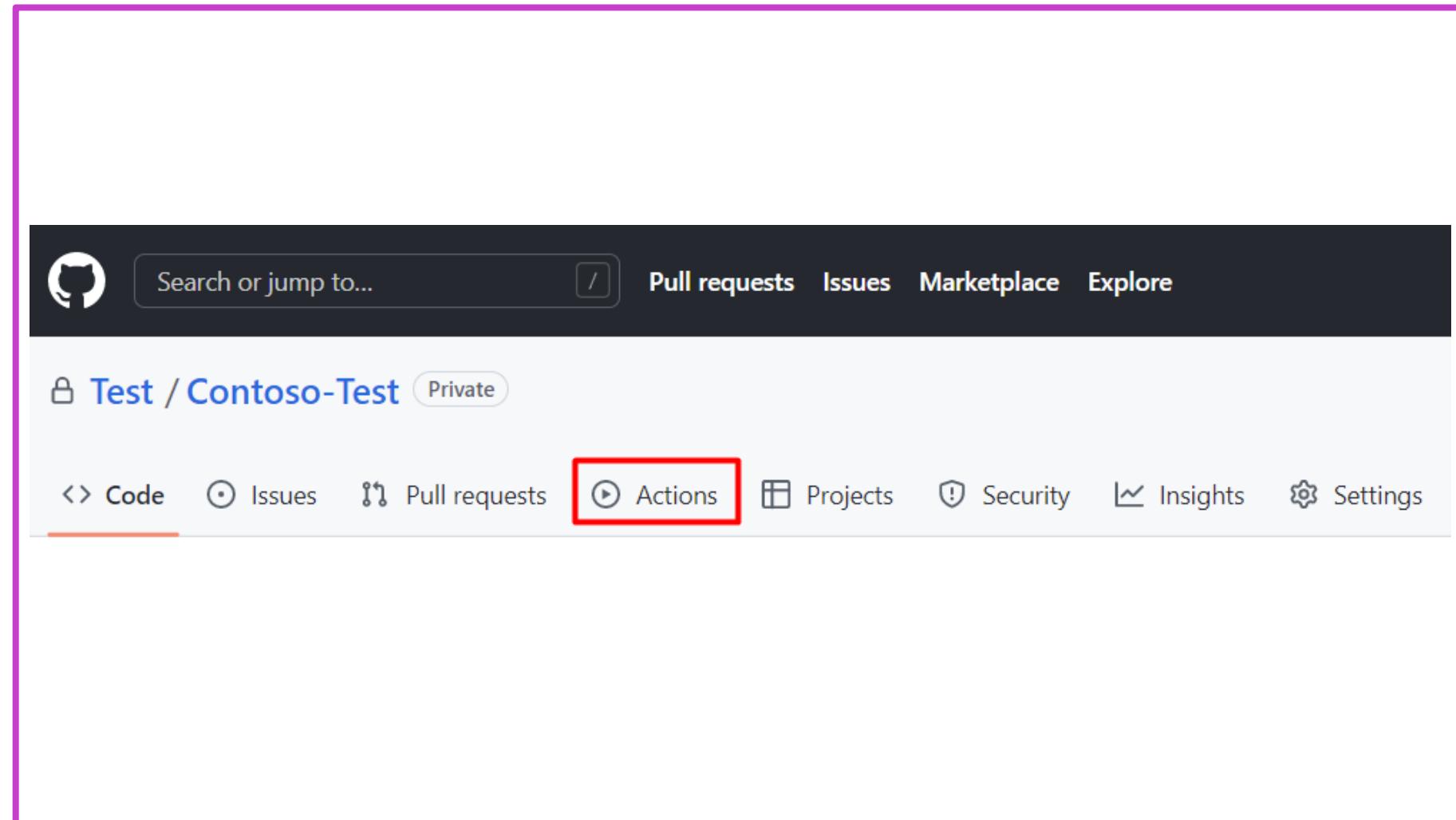
Connect your GitHub Environment to Defender for Cloud

- 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.

The screenshot shows the Microsoft Defender for Cloud Environment settings page. At the top, it displays connectivity status for various cloud providers: 1 Azure subscription, 0 AWS accounts, 0 GCP projects, 1 GitHub account, and 7 Azure DevOps accounts. A welcome message for the multi-cloud account management page (preview) is present. The main area lists environments, with 'GitHubConnector' highlighted by a red box under the 'GitHub (preview)' section. The left sidebar includes sections for General (Overview, Getting started, Recommendations, Security alerts, Inventory, Workbooks, Community, Diagnose and solve problems), Cloud Security (Security posture, Regulatory compliance, Workload protections, Firewall Manager), and Management (Environment settings, Security solutions, Workflow automation). The environment settings section is currently selected.

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.



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): Shows a list of security alerts with columns for Resource, Activity start time (UTC+2), and MITRE ATT&CK® tactics. A modal window titled "Add filter" is open, allowing users to refine results by Alert name, Affected resource, Resource type, Tags, Creator, Owner, and environment. Filter criteria "Severity == High" and "Time == Last month" are applied.

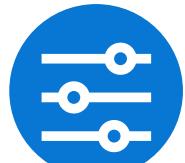
Right Panel (Respond to security alerts): Displays a detailed view of a "Potential SQL Injection" alert. Key information includes:

- Alert details:** High Severity, Active Status, 06/11/20, 1... Activity time.
- Alert description:** Potential SQL injection was detected on your database Demo on server R-DEV\SQLEXPRESS.
- Affected resource:** R-DEV (Azure Arc machine) Env: Development, DS-ThreatDetection_Demo Subscription.
- Intent:** Pre-attack.
- Related entities:** Account (1), Azure resource (1), IP (1), Network connection (1).
- Vulnerable Statement:** SELECT * FROM sqli_users WHERE ...
- Detected by:** Microsoft.

The "Alert details" tab is selected, and a "Next: Take Action >>" button is visible at the bottom.

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.

Evaluate vulnerability scans from Microsoft Defender for Server

The following vulnerability assessment options are available in Defender for Servers:



Microsoft Defender Vulnerability Management

- Offered in both Defender for Servers Plan 1 and 2.
- Auto-enabled for machines with Defender for Endpoint's Vulnerability Management.
- Shares prerequisites with Defender for Endpoint across Windows, Linux, and networks.
- Requires no extra software installation.



Qualys vulnerability scanner

- Exclusive to Defender for Servers Plan 2.
- Ideal for **third-party EDR** or **Fanotify-based setups** without Defender for Endpoint.
- Defender for Cloud's integrated Qualys doesn't support proxy or connect to existing Qualys.
- Vulnerability findings limited to Defender for Cloud.

Configure and manage security monitoring and automation solutions

Monitor security events by using Azure Monitor

You can enable Azure Monitor in Azure and non-Azure virtual machines by installing an agent.



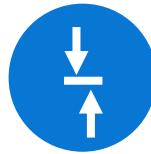
To monitor security events with
Azure Monitor:

Use Log Analytics Workspace to review logs and perform queries on log data

Collect platform logs and metrics

Collect Azure Virtual Machine internal host logs

Perform custom queries



Azure security baseline for Azure Monitor covers areas such as:

Network Security

Asset Management

Identity Management

Logging and Threat Detection

Privileged Access

Posture and Vulnerability Management

Data Protection

Backup and Recovery

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.

Create and customize 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 Microsoft Sentinel Analytics rule wizard interface. The title bar reads "Analytics rule wizard - Create new rule". Below it, a navigation bar has tabs: General (which is selected and highlighted with a red border), Set rule logic, Incident settings (Preview), Automated response, and Review and create. The main content area is titled "Analytics rule details". It includes fields for "Name" (with a red asterisk indicating it's required) and "Description". Under "Tactics and techniques", there is a dropdown menu showing "0 selected". Under "Severity", there is a dropdown menu showing "Medium". Under "Status", there are two buttons: "Enabled" (which is highlighted in blue) and "Disabled". At the bottom of the form is a blue button labeled "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



Module Labs

Lab 07 – Key Vault

Create a Key Vault and configure permissions

Add a key and a secret to the vault

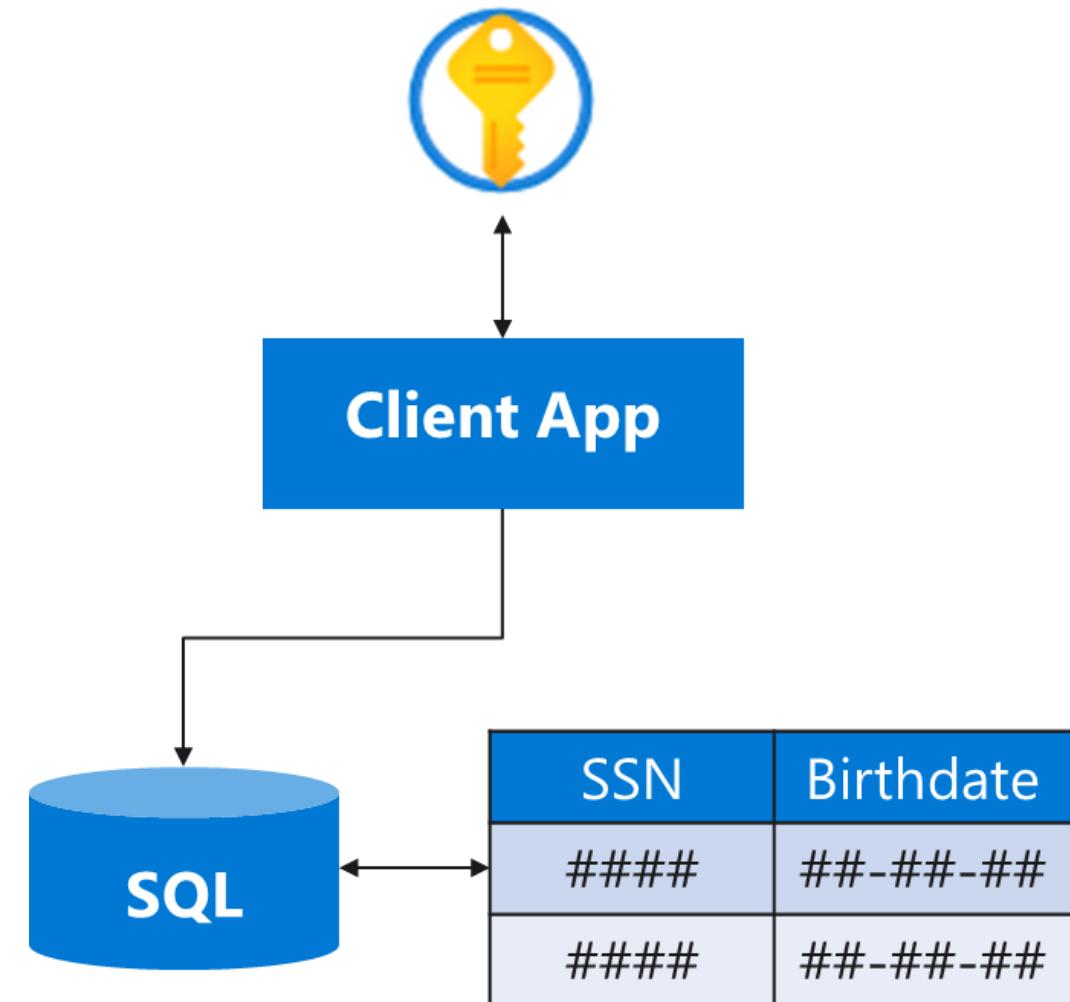
Register a client app that uses the key

Create a SQL database

Encrypt columns in a table

Build a console app to test the encryption

Key Vault



Lab 07 - Key Vault

Exercise1, Task1

AZ500LAB10

az500-10-vnet1 10.110.0.0/16

Subnet0 10.110.0.0/24



az500-10-vm1
10.110.0.4



SQL Server
Management Studio



Visual Studio

Exercise2, Task5



OpsEncrypt

Exercise1, Task2, Task3, Task4



az500kvxxxx



MyLabKey



SQLPassword

Exercise2, Task2

Key Vault
Access policy



Default Microsoft Entra ID tenant

Exercise2, Task1



sqlApp

Exercise2, Task3, Task4



medical



SQL Server

Lab 08 – Azure Monitor

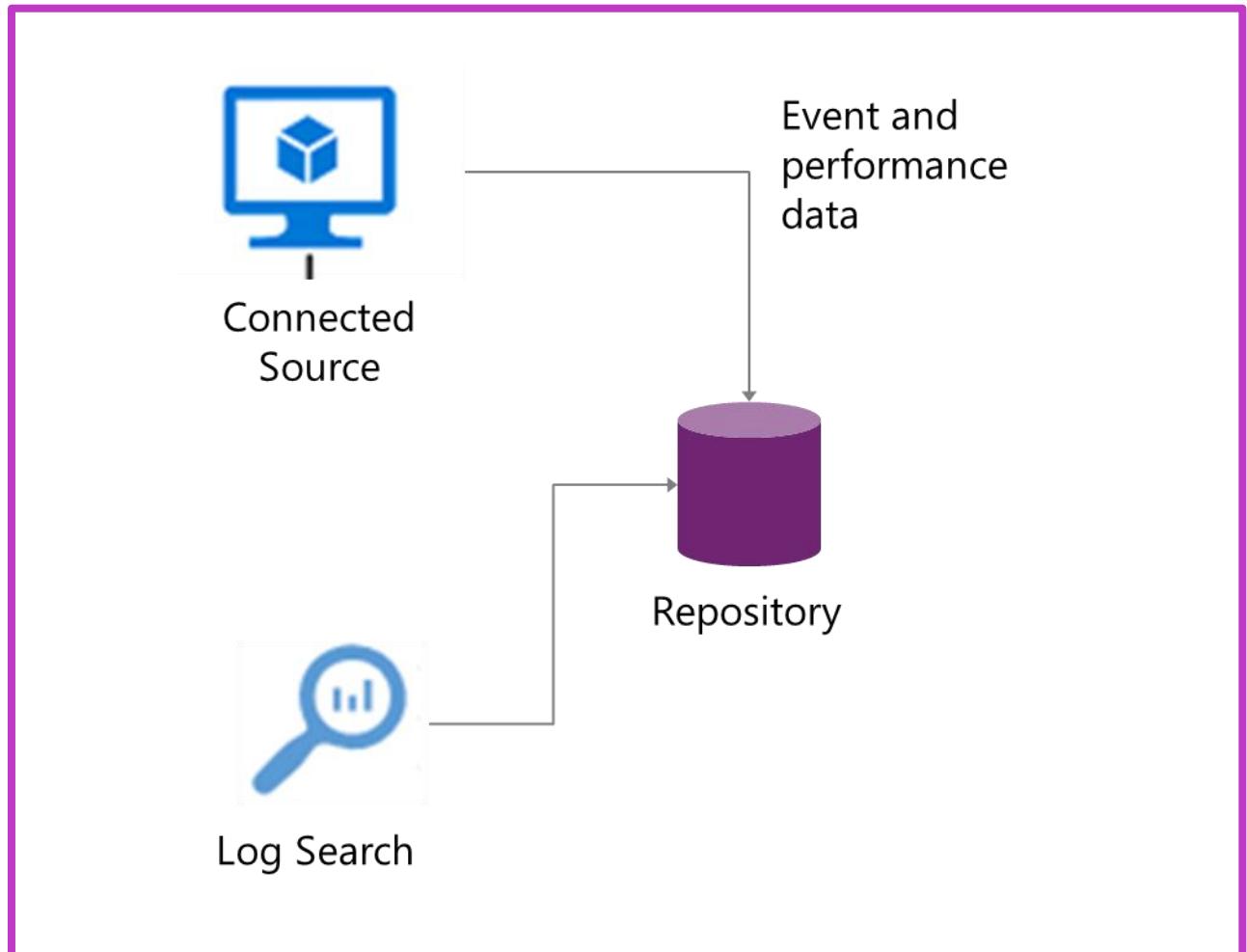
Deploy an Azure virtual machine

Create a Log Analytics workspace

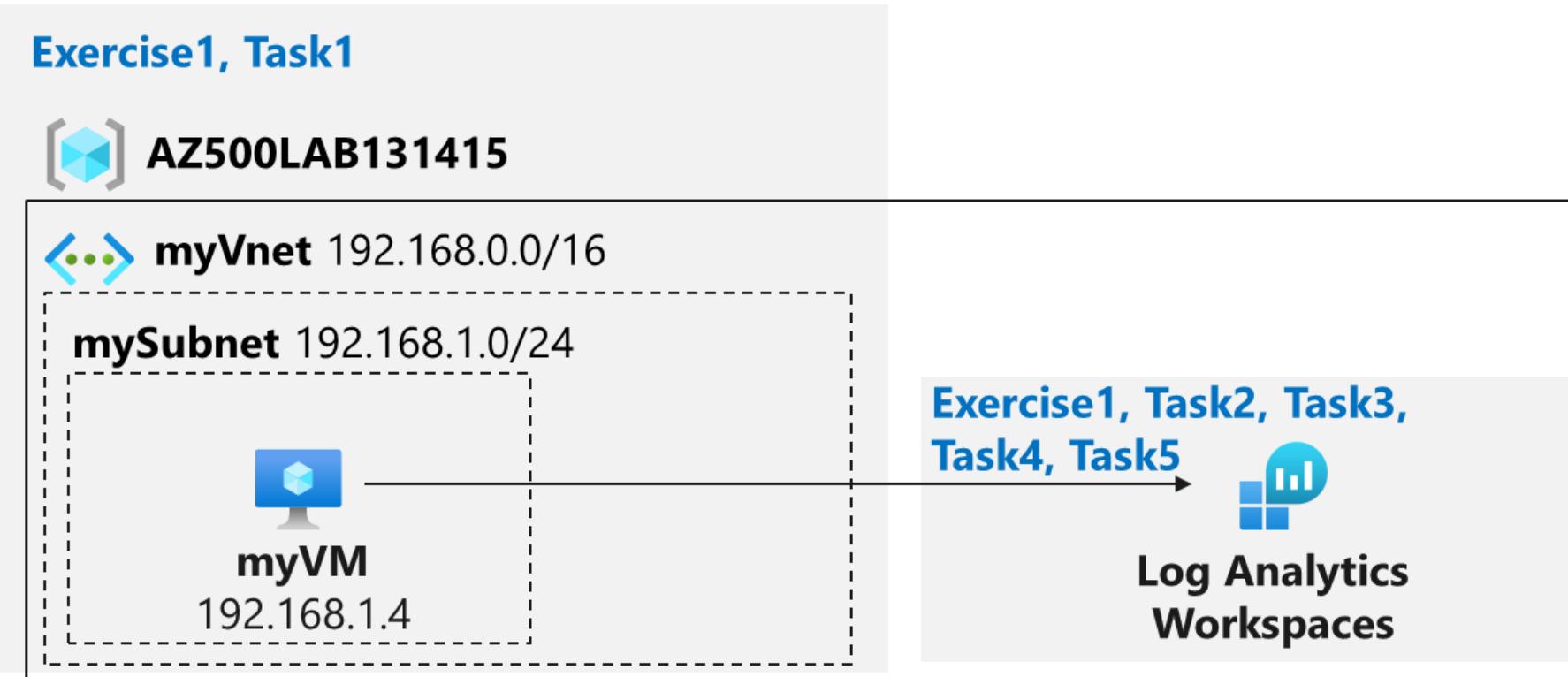
Enable the Log Analytics virtual machine extension

Collect virtual machine event and performance data

View and query collected data



Lab 08 – Azure Monitor



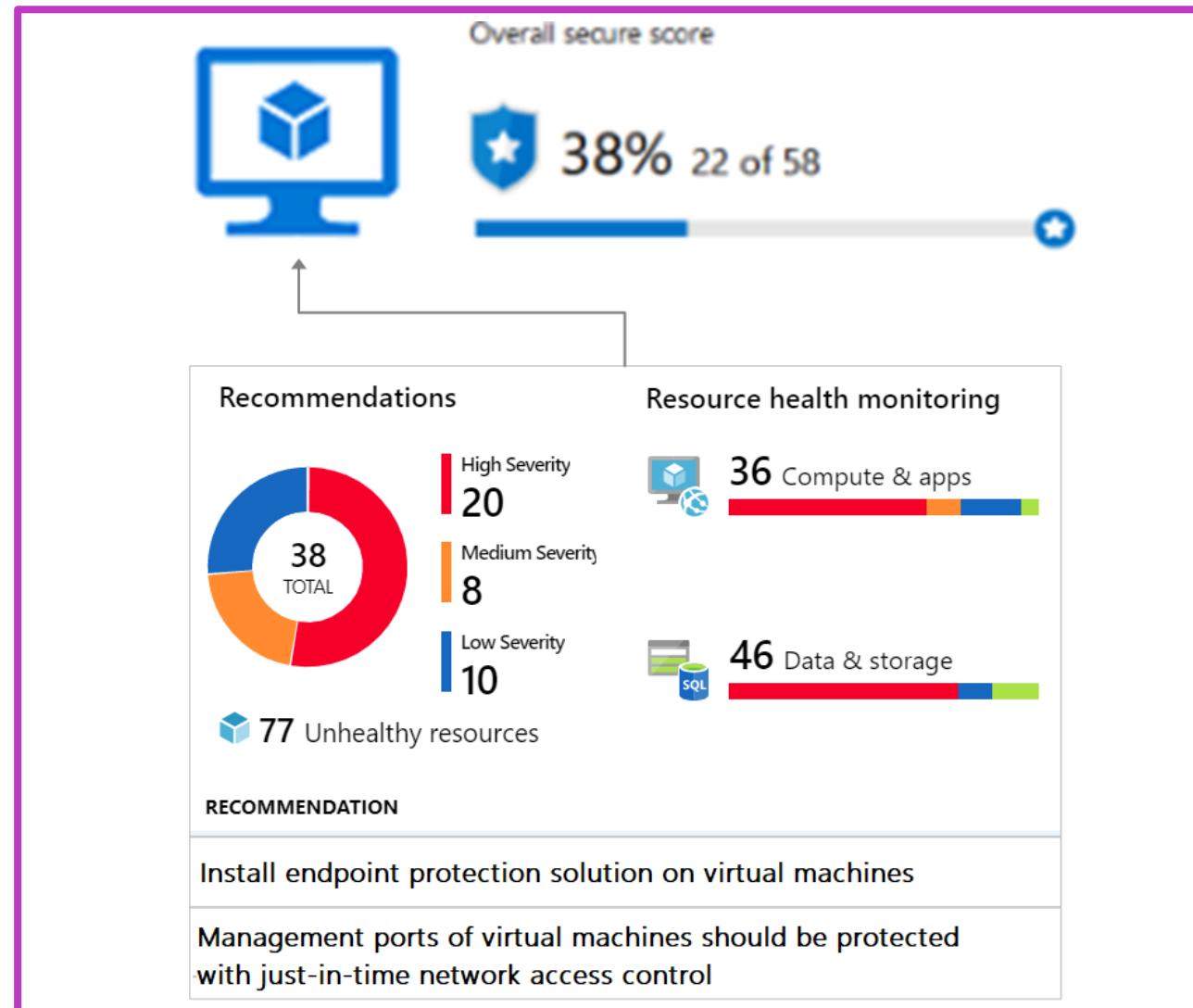
Lab 09 – Microsoft Defender for Cloud

Configure Microsoft Defender for Cloud to monitor a virtual machine

Review Microsoft Defender for Cloud recommendations for the virtual machine

Implement recommendations for endpoint protection and Just in time VM access

Review the Secure Score



Lab 09 – Microsoft Defender for Cloud

Lab13, Exercise1, Task1

[!] AZ500LAB131415

<--> myVnet 192.168.0.0/16

mySubnet 192.168.1.0/24



myVM

192.168.1.4

Lab13, Exercise1, Task2, Task3,
Task4, Task5



Log Analytics Workspaces

Lab14, Exercise1, Task1, Task2,
Task3



Microsoft Defender for Cloud

Lab 10 – Microsoft Sentinel

On-board Microsoft Sentinel

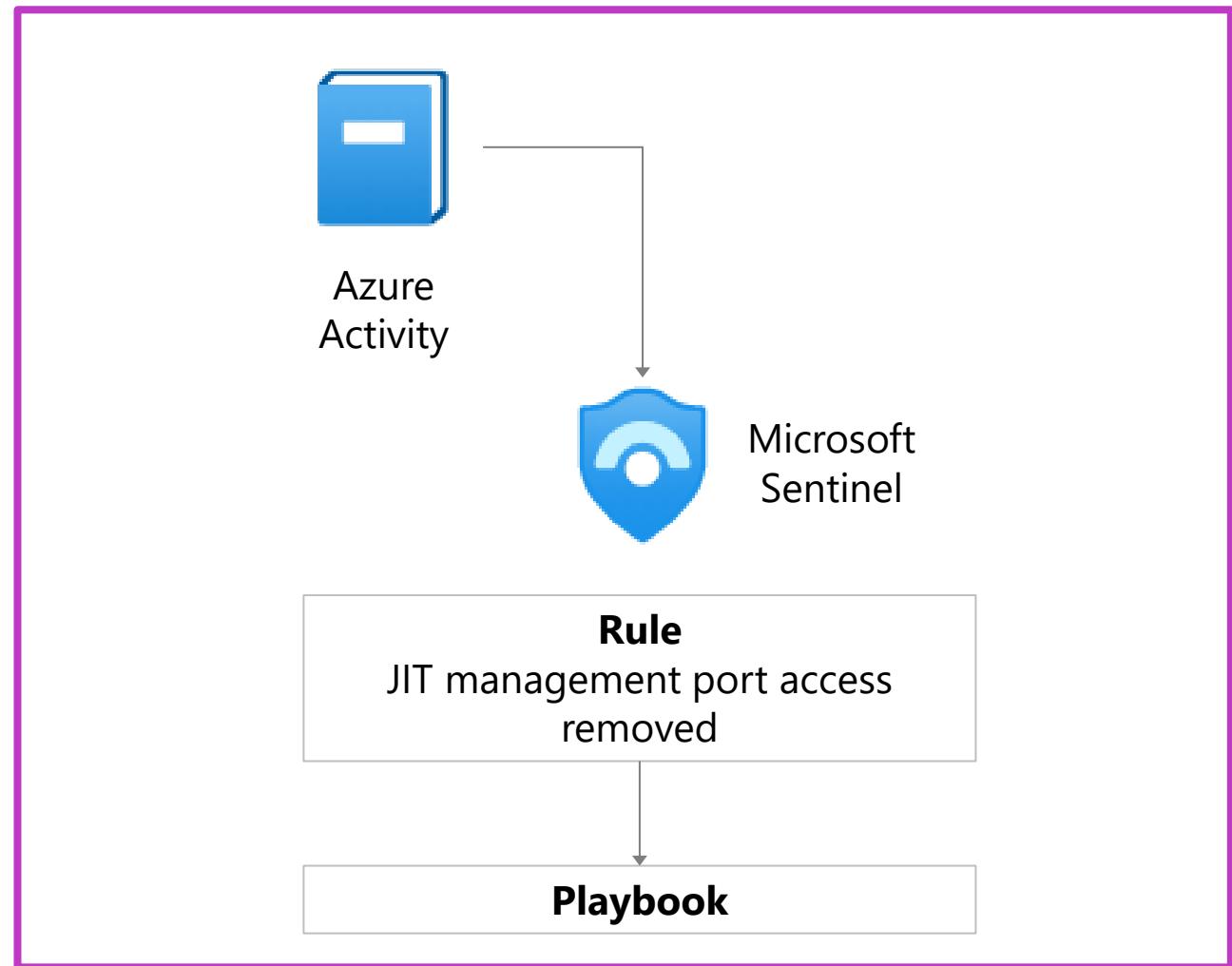
Connect Azure Activity to Sentinel

Review and create a rule that uses the Azure Activity data connector

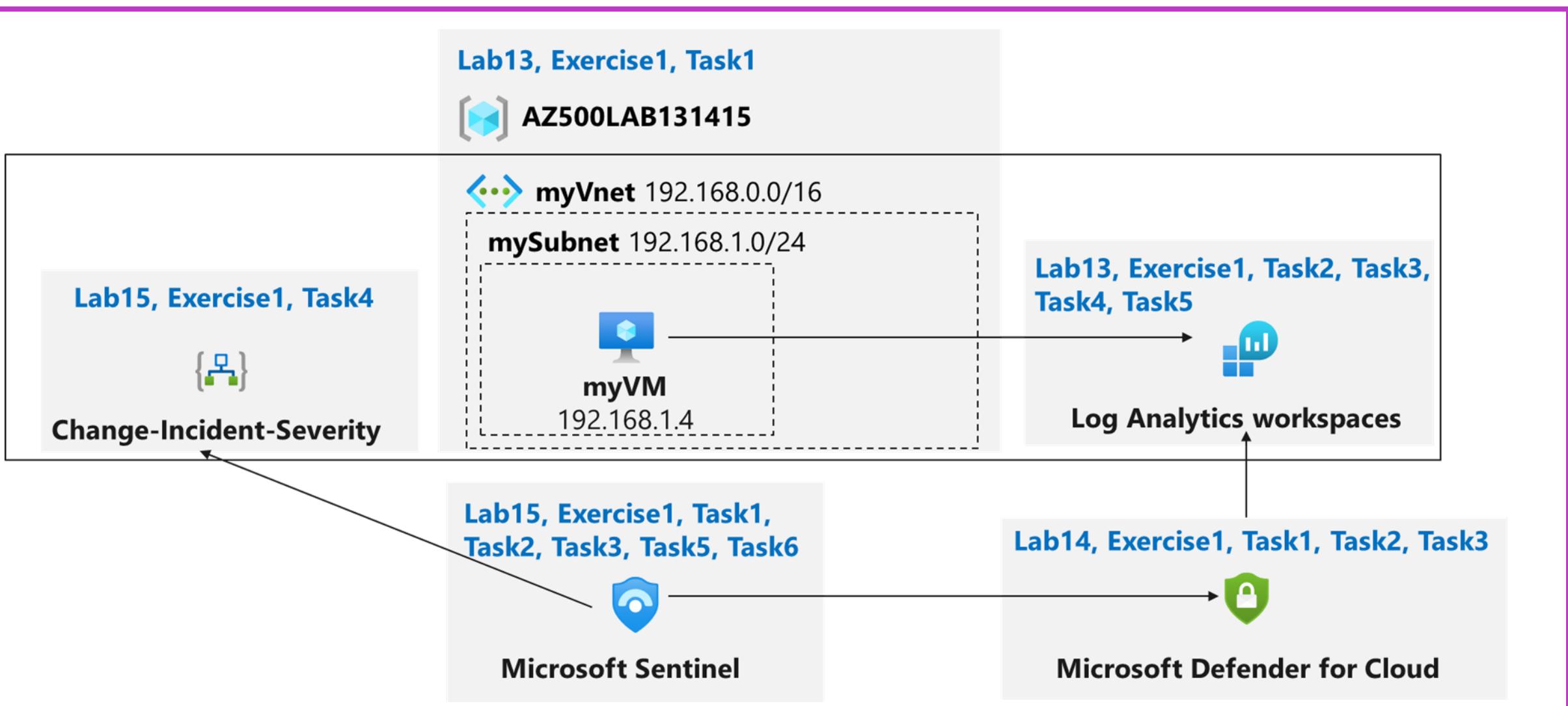
Create a playbook

Create a custom alert and configure the playbook as an automated response

Invoke an incident and review the associated actions



Lab 10 – Microsoft Sentinel



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