

MICROSOFT SENTINEL

Click-to-Run™ Solution Deployment Guide



Azure Sentinel Deployment Guide

This guide was designed to provide channel partners with the post deployment steps required to successfully deploy Azure Sentinel.

Below is a list of action items as part of the deployment process and post deployment recommendations to customize the cloud environment.

Technical Requirements – Customer Inputs

- What Region will the solution be deployed to?
- What will you name the Resource Group?
- Will you be using an existing Log Analytics Workspace or creating a new one?
- If a new Log Analytics Workspace, what will you name it?
- How many days of retention do you need?

Table of Contents

- How do I access Sentinel after deployment?
- How do I modify Sentinel settings (price tier, log retention days, etc)?
- How do I remove Sentinel?
- How can I add additional data sources?

Example Deployment User Interface

 **Configure your Sentinel v1 Solution**

Location

Select data center location

East US

Resource Group Name

C2R-Sentinel

Basic Information

Select Log Analytics Workspace

Create New

Workspace Name

sentinelws

Advanced Settings

Select Pricing Tier

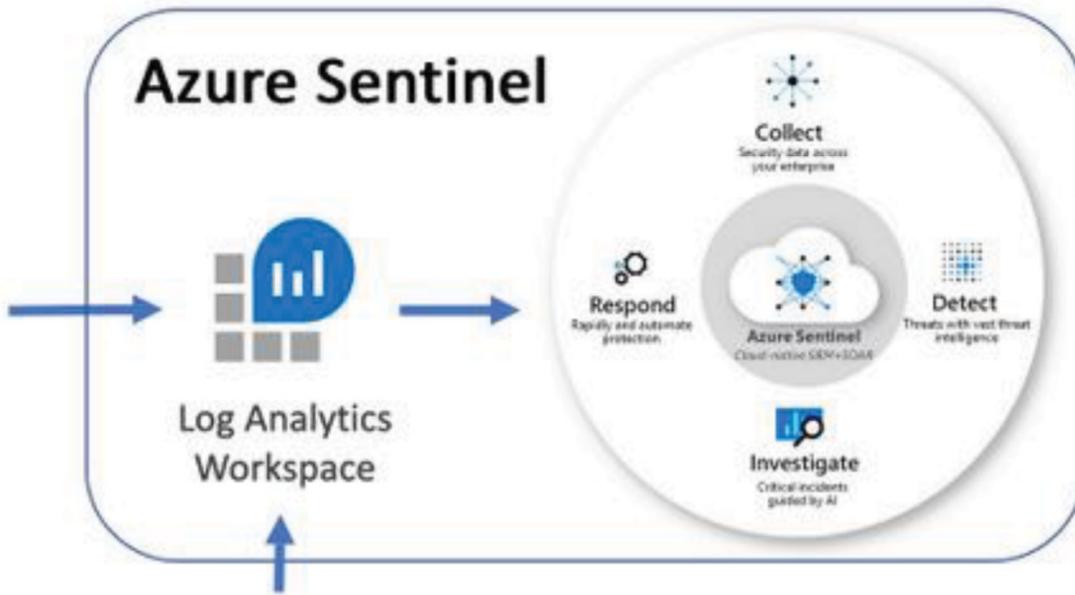
PerGB2018

Retention (In Days)

30

[Deploy Now](#)

Architecture Diagram



Resources Deployed

The following resources are deployed to build and configure this bundle.

- Log Analytics Workspace
- Azure Sentinel

Cost Breakdown

Azure Sentinel pricing

Azure Sentinel is billed based on the volume of data ingested for analysis in Azure Sentinel. Azure Sentinel offers a flexible and predictable pricing model.

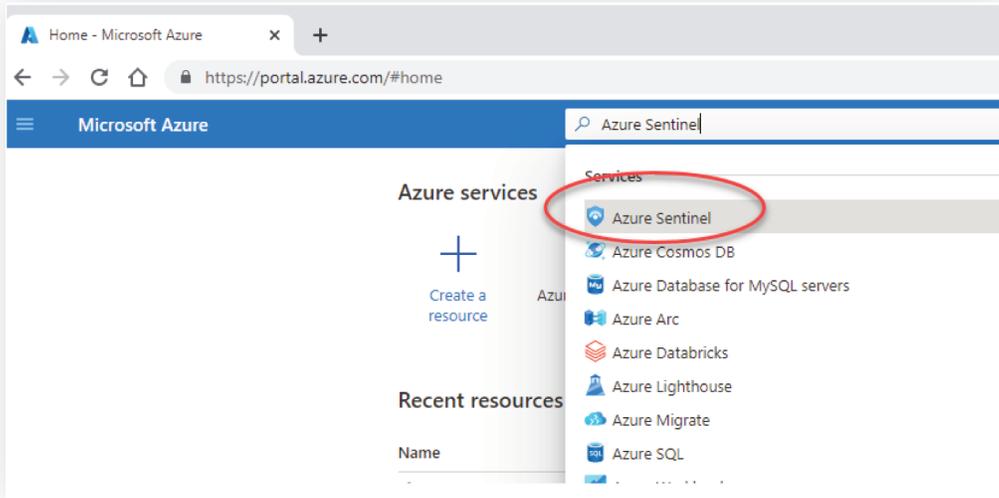
There are two ways to pay for the Azure Sentinel service: Commitment Tiers and Pay-As-You-Go. The cost for Azure Sentinel depends on the pricing tier selected. Learn more about [Azure Sentinel pricing](#).

i This does not include the Azure Log Analytics price for ingesting data. Learn more about [Log Analytics pricing](#).

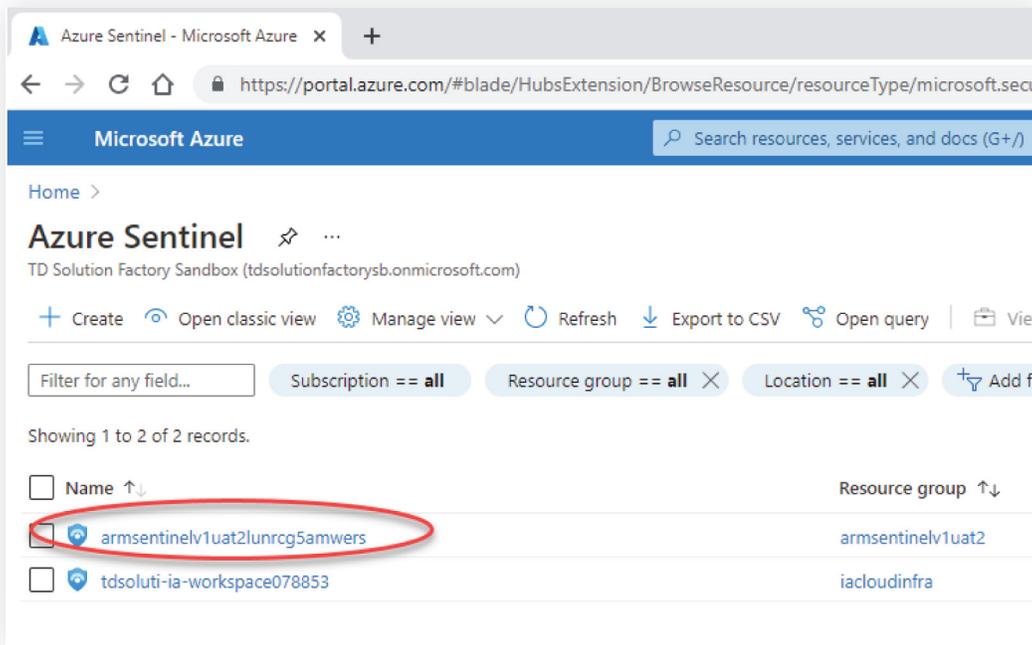
- ∨ **100 GB/day**
50% discount over Pay-as-you-go
- ∨ **200 GB/day**
55% discount over Pay-as-you-go
- ∨ **300 GB/day**
57% discount over Pay-as-you-go
- ∨ **400 GB/day**
58% discount over Pay-as-you-go
- ∨ **500 GB/day**
60% discount over Pay-as-you-go
- ∨ **1 TB/day**
61% discount over Pay-as-you-go
- ∨ **2 TB/day**
63% discount over Pay-as-you-go
- ∨ **5 TB/day**
65% discount over Pay-as-you-go
- ∨ **Pay-as-you-go**
Per GB

How to Access Sentinel After Deployment

After deployment of the Click-to-Run™ Solution you can log into the Azure portal and search for “Azure Sentinel” to locate the Azure Sentinel section of the portal.

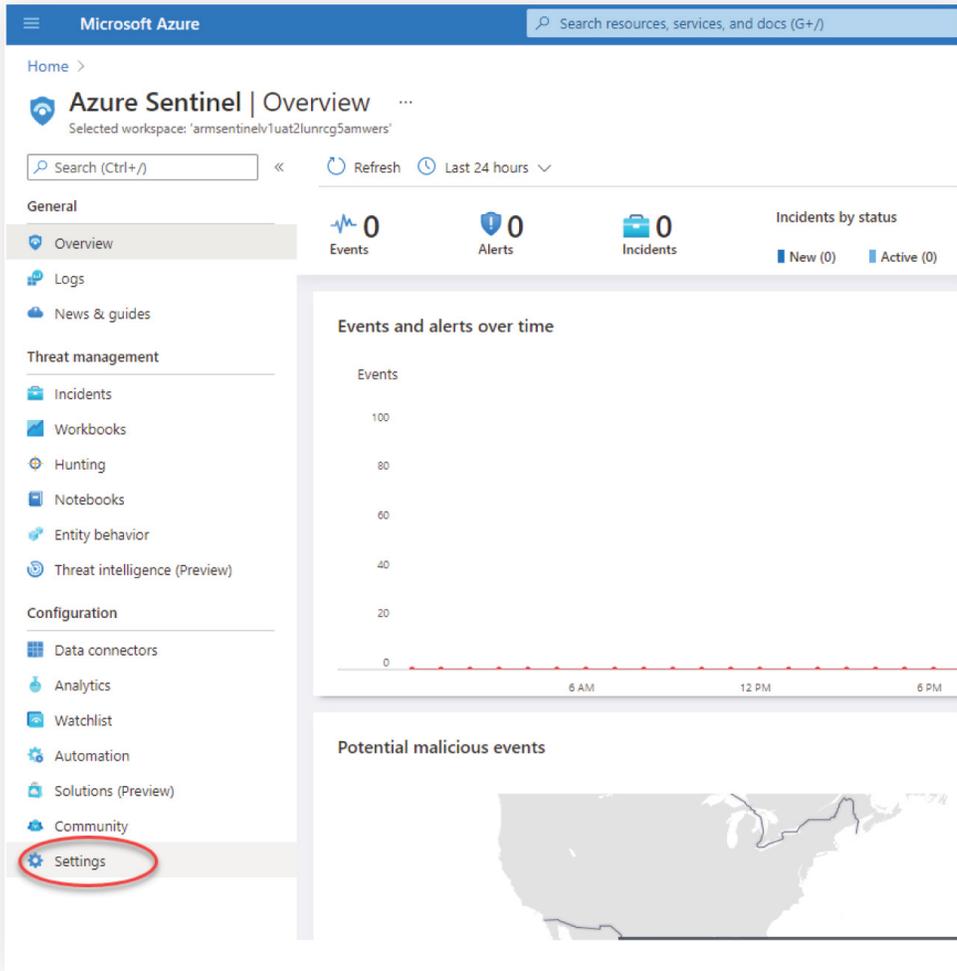


Then simply click on the log analytics workspace that you created during the deployment.



How to Modify Sentinel Settings After Deployment

After deployment of the Click-to-Run™ Solution you can log into the Azure portal and search for “Azure Sentinel” to locate the Azure Sentinel section of the portal.



From the Pricing tab you are able to adjust the pricing tier and also adjust the retention days.

Microsoft Azure

Home > Azure Sentinel

Azure Sentinel | Settings

Selected workspace: 'armsentinelv1uat2lunrcc5amwrs'

Search (Ctrl+/) << **Pricing** Settings Workspace settings >

Azure Sentinel pricing

Azure Sentinel is billed based on the volume of data ingested for analysis in Azure Sentinel. Azure Sentinel offers a flexible and predictable pricing model. There are two ways to pay for the Azure Sentinel service: Commitment Tiers and Pay-As-You-Go. The cost for Azure Sentinel depends on the pricing tier selected. Learn more about [Azure Sentinel pricing](#).

i This does not include the Azure Log Analytics price for ingesting data. Learn more about [Log Analytics pricing](#).

- 100 GB/day
50% discount over Pay-as-you-go
- 200 GB/day
55% discount over Pay-as-you-go
- 300 GB/day
57% discount over Pay-as-you-go
- 400 GB/day
58% discount over Pay-as-you-go
- 500 GB/day
60% discount over Pay-as-you-go
- 1 TB/day
61% discount over Pay-as-you-go
- 2 TB/day
63% discount over Pay-as-you-go
- 5 TB/day
65% discount over Pay-as-you-go

The 5 TB/day Commitment Tier offers a fixed, predictable fee with a 65% discount over Per GB pricing. Data ingested above the Commitment Tier level is charged at the same discounted price. There are additional charges if you increase data retention beyond the 90-day included retention. You have the flexibility to change your pricing tier any time after the first 31 days of commitment. Learn more about [Azure Sentinel pricing](#).

i This does not include the Azure Log Analytics price for ingesting data. Learn more about [Log Analytics pricing](#).

Apply

Pay-as-you-go
Per GB

Current tier

i You can increase your workspace data retention to **90 days for free** because you are an Azure Sentinel customer. [Configure retention](#)

Update Pricing Tier

Adjust Retention Days

From the Settings tab you can remove the Azure Sentinel solution from the log analytics workspace.

The screenshot shows the Microsoft Azure portal interface for Azure Sentinel. The top navigation bar includes 'Home > Azure Sentinel' and 'Azure Sentinel | Settings'. Below the search bar, there are tabs for 'Pricing', 'Settings', and 'Workspace settings', with 'Settings' being the active tab and circled in red. The left sidebar contains a navigation menu with categories: 'General' (Overview, Logs, News & guides), 'Threat management' (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence (Preview)), and 'Configuration' (Data connectors, Analytics, Watchlist, Automation, Solutions (Preview), Community, Settings). The main content area is titled 'Entity behavior analytics' and includes sections for 'What is it?', 'How to enable it', and 'Anomalies'. A 'Configure UEBA' button is visible. At the bottom of the page, a dropdown menu is open, showing options: 'Playbook permissions', 'How do we use your data?', and 'Remove Azure Sentinel', with the last option circled in red.

From the Workspace Settings tab, you will be presented to a settings screen where you can click to connect additional data sources.

The screenshot displays the Microsoft Azure portal interface for Azure Sentinel. At the top, the navigation bar shows 'Microsoft Azure' and 'Home > Azure Sentinel'. The main heading is 'Azure Sentinel | Settings' with a sub-heading 'Selected workspace: 'armsentinelv1uat2lunrcg5amwers''. Below this is a search bar and a breadcrumb trail: 'Pricing > Settings > Workspace settings >'. The 'Workspace settings >' link is circled in red.

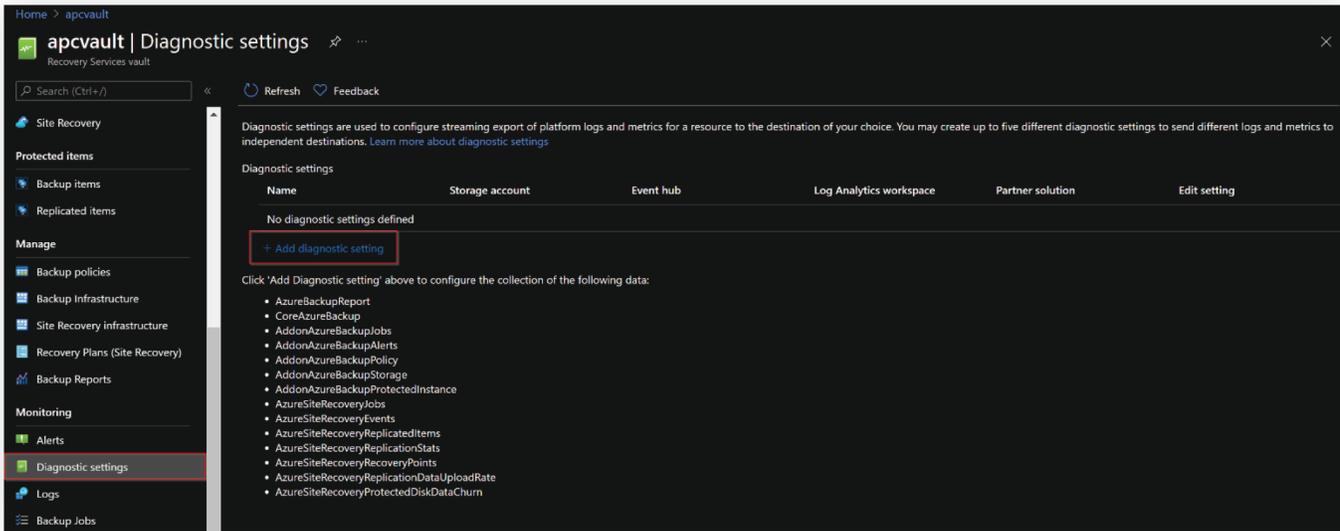
The main content area shows the workspace details for 'armsentinelv1uat2lunrcg5amwers'. It includes a search bar, a 'Delete' button, and a list of settings. The 'Essentials' section lists: Resource group (change) : armsentinelv1uat2, Status : Active, Location : East US, Subscription (change) : Microsoft Azure, Subscription ID : 80115be8-23dd-4136-918f-965b0b078853, and Tags (change) : Click here to add tags.

The 'Get started with Log Analytics' section provides an overview and three numbered steps:

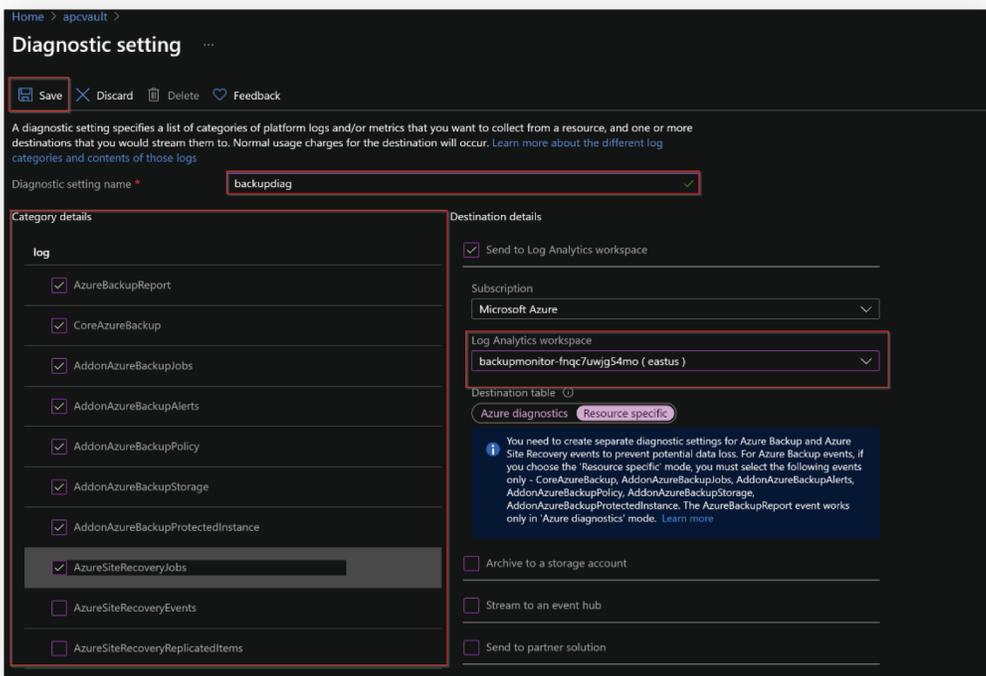
- 1. Connect a data source**: Select one or more data sources to connect to the workspace. This step is circled in red. The listed data sources are: Azure virtual machines (VMs), Windows and Linux Agents management, Azure Activity logs, Storage account log, and System Center Operations Manager.
- 2. Configure monitoring solutions**: Add monitoring solutions that provide insights for applications and services in your environment. View solutions.
- 3. Monitor workspace health**: Create alerts to proactively detect any issue that arise in your workspace. Learn more.

Additional sections include 'Useful links' (Documentation site, Community) and 'Maximize your Log Analytics experience' with steps for 'Search and analyze logs', 'Manage alert rules', 'Manage usage and costs', and 'Create and Share Workbooks'.

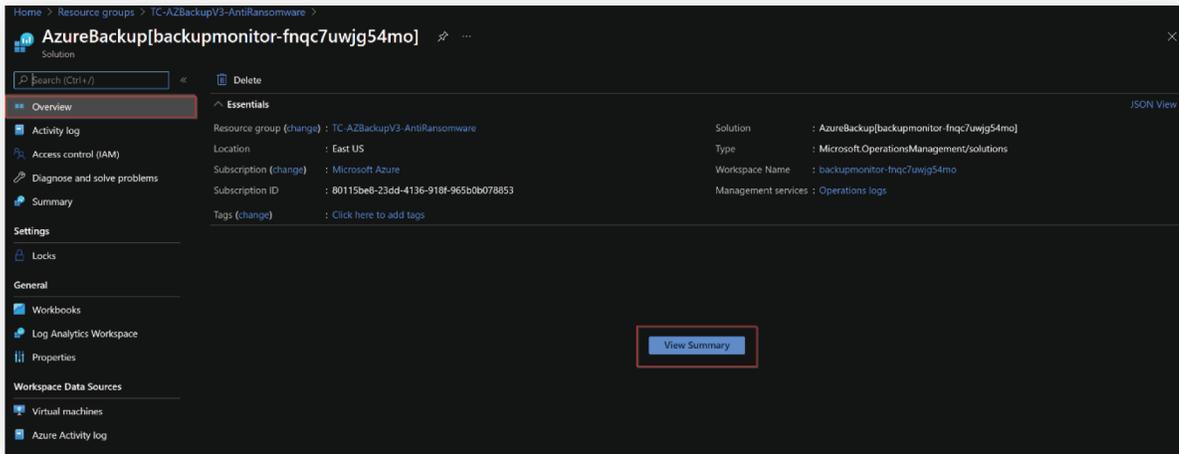
1. Navigate to your Recovery Services Vault and Select 'Diagnostic Settings' under the Alerts section.
Select 'Add diagnostic setting.'



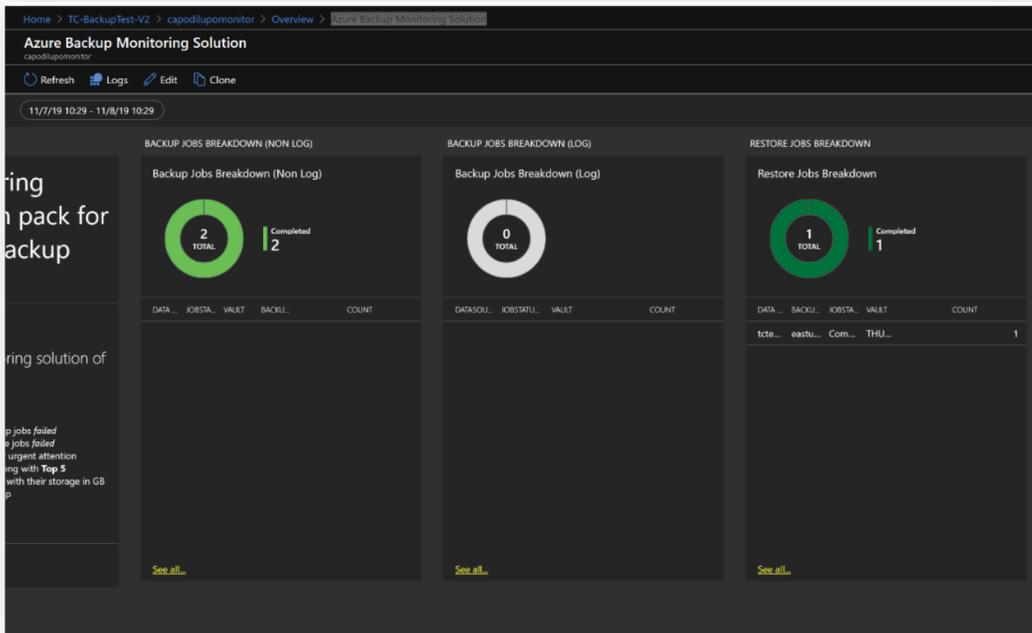
2. Give your custom Diagnostic settings a name. Select the backup and site recovery events that you would like to monitor from the Azure Backup solution. Specify the Log Analytics workspace that was created during this pre-configured deployment. Confirm your configuration and click 'Save'.



- Once your scheduled backup jobs have run, you can view the monitoring dashboard provided by the OMS solution. Navigate to the OMS solution and select 'View Summary' from the overview section to see more detailed information.



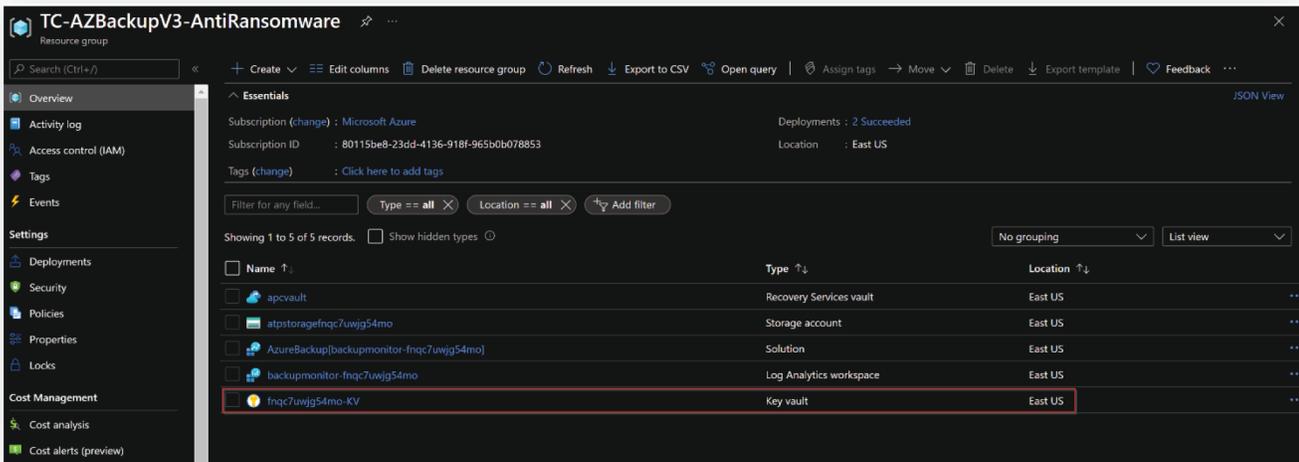
- You may now view detailed dashboards and monitoring reports for your scheduled VM backups.



Azure Key Vault

You may optionally deploy an Azure Key Vault as part of the AZ Backup V3 Enhancements. Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. The Key Vault must be configured post deployment to fit your use case and scenario.

More information on how to configure can be found [here](#).



ATP Storage Account

This pre-configured solution also gives the option to deploy a storage account with ATP. Advanced Threat Protection (ATP) for Azure Storage provides an additional layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit storage accounts. This layer of protection allows you to protect and address concerns about potential threats to your storage accounts as they occur. These features work in conjunction with Azure Defender and Security Center. **To learn more, [click here](#).**