Hands-On Lab

Azure Security Center and AWS Integration

Contents

Before You Begin

In this lab you will stand up an EC2 instance and have that Windows VM report into Azure Security Center. This includes upgrading Azure Security Center to the Standard tier. Your first 60 days will be free, and you can return to the Free tier any time.

We recommend that you open the Azure Portal in one tab within your browser and then the AWS Console in another tab.

If you have an account on AWS you can use that environment as long as it will not impact any production or customer environments. We recommend that you create a fresh, clean AWS environment for this lab.

We are provisioning a low-powered instance within AWS, so please be mindful that it will not be a fast computer.

Create an Account on the AWS Free Tier

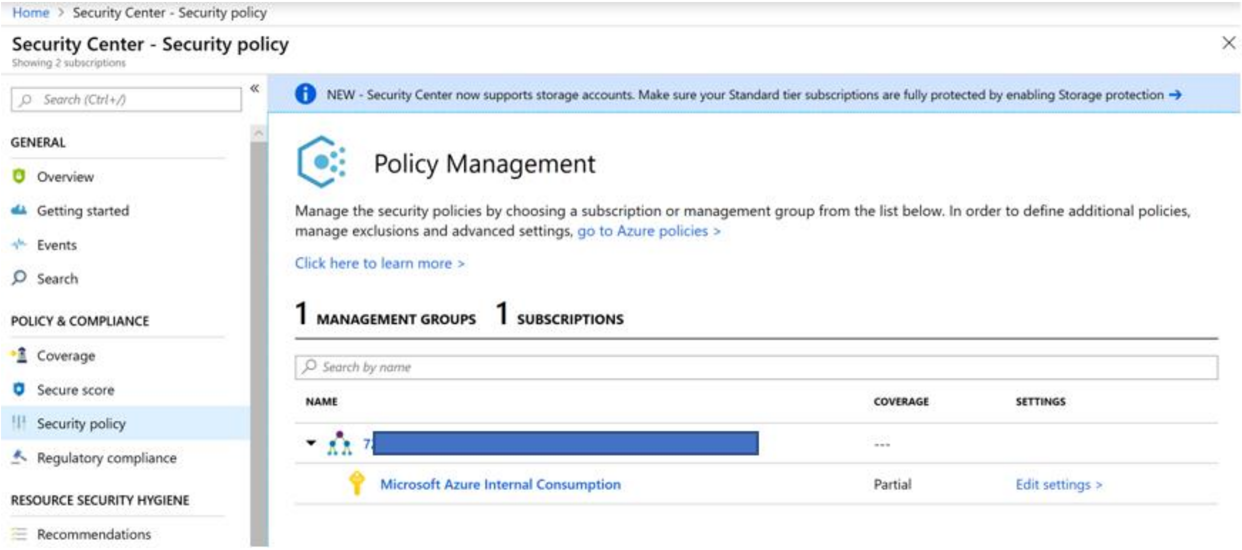
1. Surf to the following link and click on **Create a Free Account** https://aws.amazon.com/free/
2. On the **Create an AWS account,** enter the following and click **Continue:**
    a. Email Address
    b. Password
    c. Password Confirmation
    d. AWS account name
3. On the Contact Information screen choose **Personal** and complete all fields. Click **Create Account and Continue**.
4. On the **Payment Information** screen complete all field and click **Secure Submit.**
5. On the Phone Verification screen complete all information and click **Call Me Now.** Enter your pin when prompted and click **Continue.**
6. On the Select a Support Plan screen click **Free.**
7. Personalize you experience and click **Submit**.
8. Click **Sign In to the Console** in the upper-right hand corner of the screen. https://console.aws.amazon.com/
9. Sign in to AWS.

Build a Windows Virtual Machine

1. In the AWS console, click on **Launch a virtual machine**.
2. On the Choose AMI screen, find the **Microsoft Windows Server 2016 Base** AMI (Amazon Machine Image) and click **Select**.
3. On the Select an instance type choose **t2.micro** and click **Next: Configure Instance Details**.
4. Click **Next: Add Storage**
5. Size the storage to **30** (GiB) and **General Purpose SSD (gp2)**, which are included in free tier
6. Click **Review and Launch** and then **Launch**
7. On the Create a key pair screen, select **Create a new key pair** and use Key Pair Name **AWSRDPKEY**, then click **Download Key Pair.** Save the .PEM file to your Downloads folder and then click **Launch Instances**.
8. From the EC2 dashboard, click the edit (pencil) next to the instance Name and rename your new instance to **AWSHYBRID,** then click the checkmark to apply the name.

Upgrade to the Azure Security Center Standard tier

1. Logon to the Azure Portal, click **All Services** then **Security Center**, and then under the Security Center main menu, select **Onboarding to advanced security**.
2. Under **POLICY & COMPLIANCE → Security Policy**, Security Center lists subscriptions and workspaces eligible for onboarding. Select your subscription from the list and click **Edit settings**.



Home > Security Center - Security policy

Security Center - Security policy

Showing 2 subscriptions

NEW - Security Center now supports storage accounts. Make sure your Standard tier subscriptions are fully protected by enabling Storage protection →

Policy Management

Manage the security policies by choosing a subscription or management group from the list below. In order to define additional policies, manage exclusions and advanced settings, go to Azure policies >

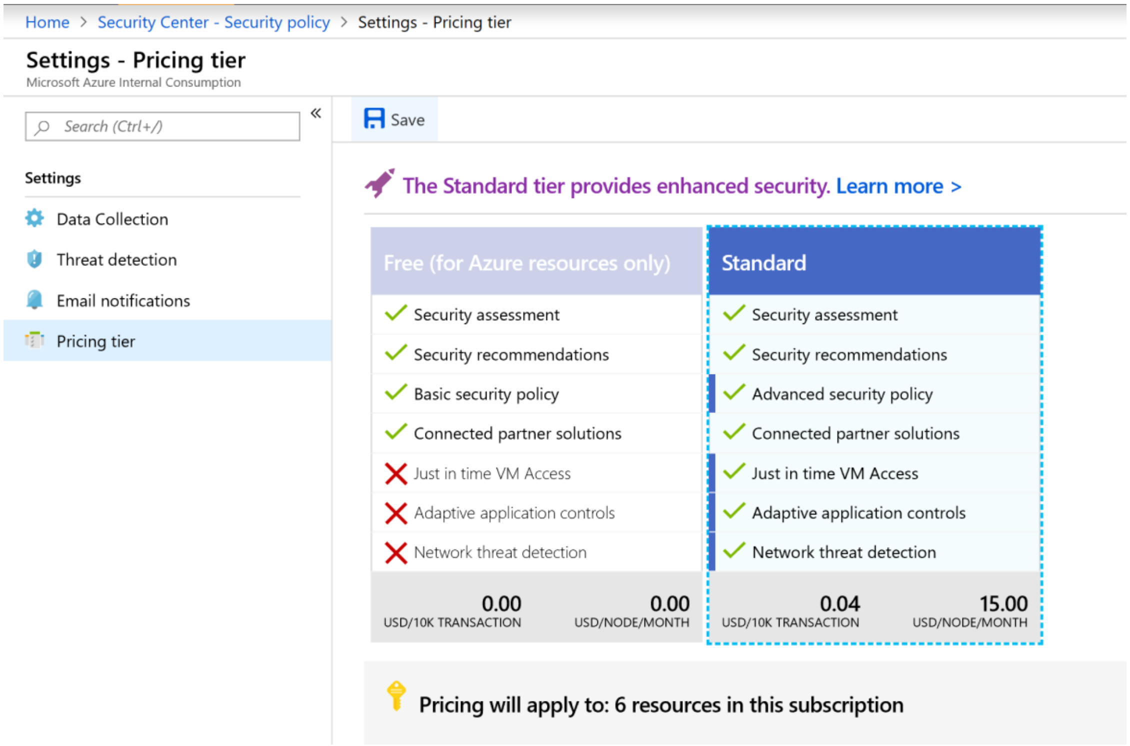
Click here to learn more >

1 MANAGEMENT GROUPS 1 SUBSCRIPTIONS

Search by name

NAME	COVERAGE	SETTINGS
7[redacted]	---	
Microsoft Azure Internal Consumption	Partial	Edit settings >

3. Under **Pricing Tier**, select **Standard** to upgrade from Free to Standard and click **Save**.



Home > Security Center - Security policy > Settings - Pricing tier

Settings - Pricing tier

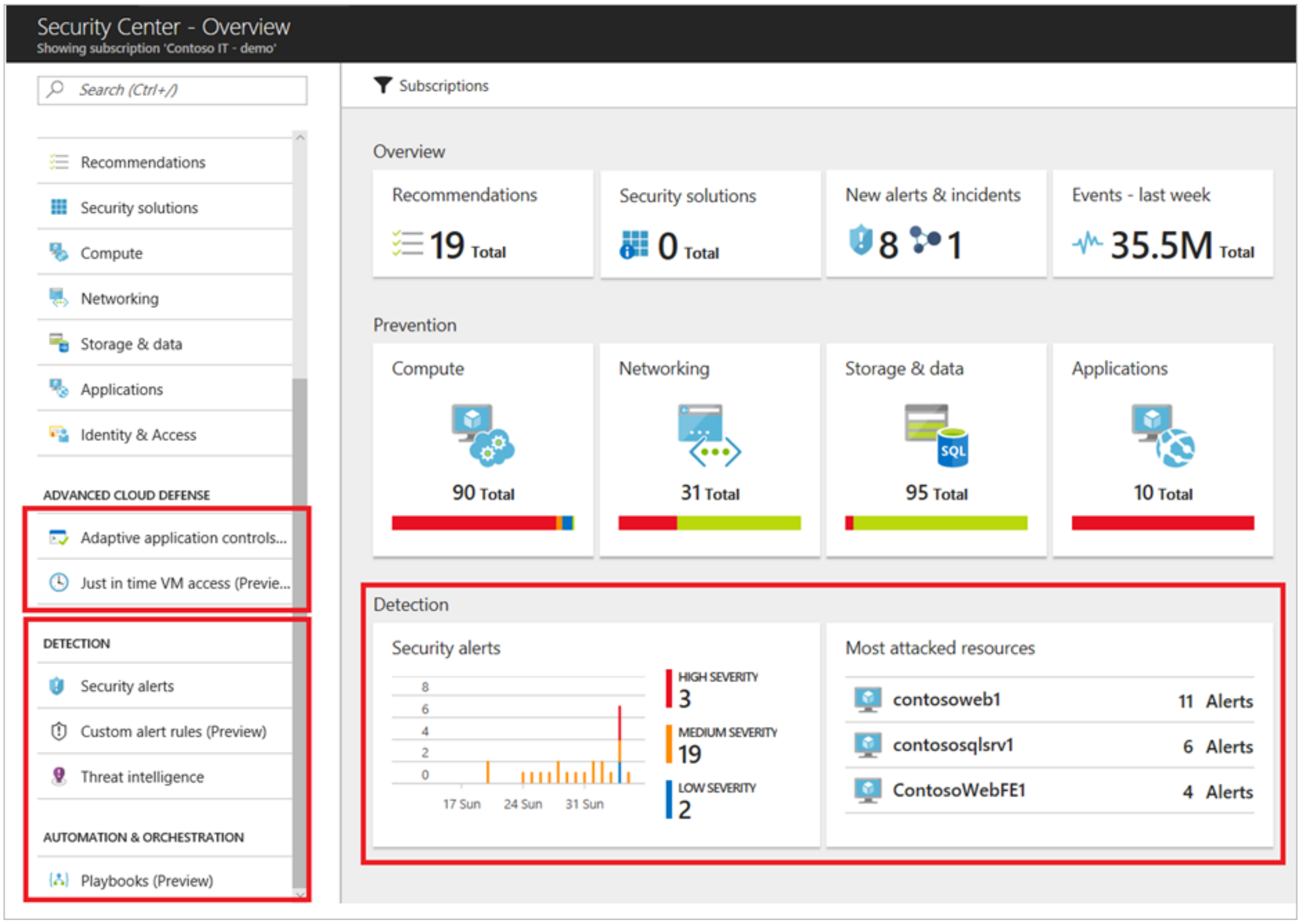
Microsoft Azure Internal Consumption

The Standard tier provides enhanced security. Learn more >

Free (for Azure resources only)	Standard
✓ Security assessment	✓ Security assessment
✓ Security recommendations	✓ Security recommendations
✓ Basic security policy	✓ Advanced security policy
✓ Connected partner solutions	✓ Connected partner solutions
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls	✓ Adaptive application controls
✗ Network threat detection	✓ Network threat detection
0.00 USD/10K TRANSACTION 0.00 USD/NODE/MONTH	0.04 USD/10K TRANSACTION 15.00 USD/NODE/MONTH

Pricing will apply to: 6 resources in this subscription

Now that you've upgraded to the Standard tier, you have access to additional Security Center features, including **adaptive application controls**, **just in time VM access**, **security alerts**, **threat intelligence**, **automation playbooks**, and more. Note that security alerts will only appear when Security Center detects malicious activity.



Security Center - Overview

Showing subscription 'Contoso IT - demo'

Search (Ctrl+/)

Recommendations

Security solutions

Compute

Networking

Storage & data

Applications

Identity & Access

ADVANCED CLOUD DEFENSE

Adaptive application controls...

Just in time VM access (Previe...

DETECTION

Security alerts

Custom alert rules (Preview)

Threat intelligence

AUTOMATION & ORCHESTRATION

Playbooks (Preview)

Subscriptions

Overview

Recommendations	Security solutions	New alerts & incidents	Events - last week
19 Total	0 Total	8 1	35.5M Total

Prevention

Compute	Networking	Storage & data	Applications
90 Total	31 Total	95 Total	10 Total

Detection

Security alerts

HIGH SEVERITY 3

MEDIUM SEVERITY 19

LOW SEVERITY 2

Most attacked resources

contosoweb1	11 Alerts
contososqlsrv1	6 Alerts
ContosoWebFE1	4 Alerts

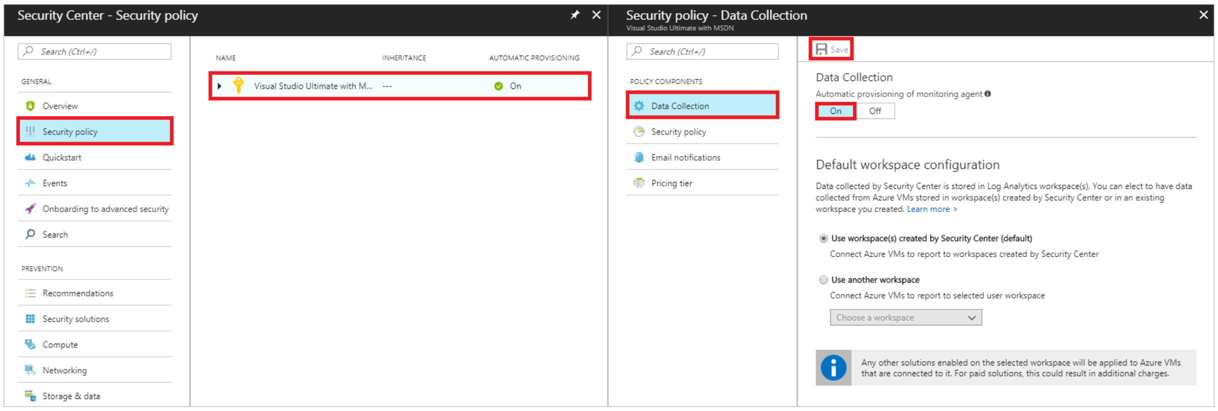
Automate data collection

Security Center collects data from your Azure VMs and non-Azure computers to monitor for security vulnerabilities and threats. Data is collected using the Microsoft Monitoring Agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. By default, Security Center will create a new workspace for you.

When automatic provisioning is enabled, Security Center installs the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created. Automatic provisioning is strongly recommended.

To enable automatic provisioning of the Microsoft Monitoring Agent:

1. Under the Security Center main menu, select **Security Policy**.
2. Select the subscription (Azure Pass) and click **Edit Settings** again.
3. Under **Security policy**, select **Data Collection**.
4. Under **Data Collection**, confirm the Data Collection is set to **On** to enable automatic provisioning.
5. Select **Save**.



Security Center - Security policy

NAME	INHERITANCE	AUTOMATIC PROVISIONING
Visual Studio Ultimate with M...	---	✓ On

Security policy - Data Collection

Visual Studio Ultimate with MSDN

Data Collection

Automatic provisioning of monitoring agent

[✓ On] Off

Default workspace configuration

Data collected by Security Center is stored in Log Analytics workspace(s). You can elect to have data collected from Azure VMs stored in workspace(s) created by Security Center or in an existing workspace you created. Learn more >

● Use workspace(s) created by Security Center (default)

Connect Azure VMs to report to workspaces created by Security Center

○ Use another workspace

Connect Azure VMs to report to selected user workspace

Choose a workspace

Any other solutions enabled on the selected workspace will be applied to Azure VMs that are connected to it. For paid solutions, this could result in additional charges.

With this new insight into your Azure VMs, Security Center can provide additional Recommendations related to system update status, OS security configurations, endpoint protection, as well as generate additional Security alerts.

Create a new Log Analytics Workspace

1) Under the Security Center main menu, select **Compute & apps** under the RESOURCE SECURITY HYGIENE section.
2) Click the **+ Add Computers** option.
3) If you haven't already added a Log Analytics workspace, click **add a new workspace**
4) and then on the Security and Audit blade click **Create New Workspace** and enter the following information:
    a. Log Analytics Workspace: **LA-<initials><4digits> (e.g. *LA-JRL5945)***
    b. Subscription: Azure Pass
    c. Resource Group: Create new > **RG-DEMO-ASCAWS**
    d. Location: **East US**
    e. Pricing Tier: **OMS** (per node)
    f. Click **OK**

It will take several minutes for your OMS workspace to be provisioned. When the task is complete, click **OK** on the Security and Audit blade. Your portal should return to the Add new non-Azure computers blade.

Connect to your EC2 Instance

By now your EC2 instance should be provisioned and launched.

1) Return to the AWS console and click **Proceed to EC2 console**.
2) In the console, ensure the AWSHYBRID instance is highlighted and click **Connect.**
3) On the Connect To Your Instance screen, complete the following:
    a. Click on **Get Password**
    b. Click **Choose File** and select the .PEM file from your Downloads folder.
    c. Click **Decrypt Password**.
4) Select and copy your password and then click on **Download Remote Desktop File.**
5) Click **Connect** on the Remote Desktop Connection Window.
6) Click on More Choices, the Use a different account.
7) Enter awshybrid\administrator as the username and then paste your password into the Password field. Click **Ok** and then **Yes**.

NOTE: If your RDP Connection fails you may need to modify the Security Configuration by:

1) *With the AWS Console click Security Groups.*
2) *Select Security Group associated with your VM and then select the Inbound tab at the bottum.*
3) *Click Edit and enter the following:*
    a. *Type: RDP*
    b. *Protocol: TCP*
    c. *Port Range: 3389*
    d. *Source: Custom*
    e. *0.0.0.0/0*
    f. *Description: Allow Remote Access from Internet*

4) *Click Save*

Install the Agent

1) When AWSHYBRID boots to the desktop, click **No** on the Networks blade.
2) Within the EC2 instance and open Internet Explorer. Use the recommended settings and click **Ok**.
3) Go to Settings → Internet Options → Security (tab) → Internet → click the Custom Level button and then scroll down to the Download section
4) Select **Enable** under File Download and then click **Ok** twice
5) Paste this URL (http://go.microsoft.com/fwlink/?LinkId=828603) into the EC2 instance's Internet Explorer address field and hit **Enter**.
6) Download and run MMASetup when prompted and complete the following:
    a. Click **Next** on the Welcome Screen.
    b. Click **I Agree** on the License Terms.
    c. Click **Next** on the Destination Folder.
    d. On the Agent Setup Options screen check **Connect the agent to Azure Log Analytics (OMS)** and click **Next**.
    e. Switch back to your desktop and in the Azure Portal click on **Security Center**
        i. Select **Compute & apps** under RESOURCE SECURITY HYGIENE and then select **VMs and Computers.** *Note that the EC2 instance (AWSHYBRID) is not currently in the list of VMs being monitored.*
        ii. Click **+ Add Computers**
        iii. Click on the Log Analytics workspace Security Center is using and then copy the **workspace ID** and **primary key** values and paste them into the MMA setup wizard **Workspace ID** and **Workspace Key** fields (running on the AWS instance), respectively, then click **Next** to continue installing the MMA agent.
    f. Select **I don't want to use Microsoft Update** and click Next.
    g. Click **Install** on the Ready to Install screen.
7) When setup is complete click **Finish**.

When complete, the Microsoft Monitoring Agent appears in Control Panel. You can review your configuration there and verify that the agent is connected.

View Results

1) Close all blades within the Azure Portal and return to the Microsoft Azure dashboard.
2) Open Security Center and under **Compute & apps** under RESOURCE SECURITY HYGIENE, click on **VMs and Computers, +Add Computers**, click on the Log Analytics workspace Security Center is using and note the number of VM & Computers. Since we provisioned a low-powered instance it can take 60 minutes for the t2.micro EC2 instance to report into the Azure Security Center and up to a day before you receive security recommendations.