**Encryption at Rest (How-To for AWS and Azure services)**

**AWS:**
1. EC2 EBS volumes (Windows and Linux):
   You can enable encryption by default or enable encryption when you create a volume.

**Option 1: Enable encryption by default**
   1) On EC2 Dashboard. Click **EBS Encryption** under **Account attributes** in the upper-right corner.
   2) Click the **Manage** button.
   3) Select **Enable** and specify the key that you would like to use for encryption. Then Click **Update EBS encryption**.
Note: Only the new EBS volumes and snapshots that you create after the default encryption is enabled will be encrypted by default.

Option 2: Enable encryption when creating a volume
During the EC2 instance creation, on Step 4 Add Storage, click the dropdown arrow under Encryption to select the KMS key that you would like to encrypt the volume.

2. Container/serverless on AWS
ECR:
When creating a new repository, under the Encryption settings, check “Enable”. You can optionally click the “Customize encryption settings (advanced)” to select a key different from the default AWS managed key.
Fargate:
Make sure it is using version 1.4 and above when creating a Fargate cluster.
EFS volumes (persistent storage) are encrypted by default using AWS managed key (aws/elasticfilesystem).
The ephemeral storage is enabled by default in version 1.4 and above.

Lambda:
Use environment variables to store secrets for use with Lambda functions. Lambda always encrypts environment variables at rest.

Azure:
1. VM (Windows & Linux)
Disk is encrypted by default.
2. Azure Container Registry/Instances
Encryption is enabled by default.

3. Azure Function
Use Azure Storage Account for storage and SA is encrypted by default.

VMware:
1. Encrypt existing VM or Virtual Disk
Option 1:
   1) Connect to vCenter with vSphere Client.
   2) Power off the virtual machine.
   3) Right-click the VM and select **VM Policies > Edit VM Storage Policies**.
   4) Select an encryption storage policy and click **OK**. You can use the default “VM Encryption Policy” or use a custom storage encryption policy.
Option 2:
1) Connect to vCenter with vSphere Client.
2) Power off the virtual machine.
3) Select the VM that you want to encrypt on the left panel and navigate to the Configure tab on the right panel.
4) Select Policies and click EDIT VM STORAGE POLICIES.

5) Select an encryption storage policy and click OK. You can use the default “VM Encryption Policy” or use a custom storage encryption policy.
2. Encrypt a VM when it is created
   1) Launch the New Virtual Machine wizard.
   2) When selecting storage, check “Encrypt this virtual machine” and select the encryption policy. Then click Next.
3) Continue the wizard to finish the VM creation.