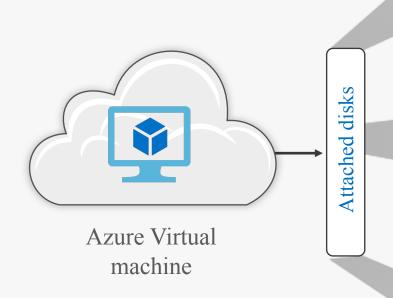
## Virtual machine storage encryption overview

## **VM Storage overview**







**Operating system disk -** Every virtual machine will have an operating system disk.



Backup

**Temporary disk -** Each VM contains a temporary disk.



**Data disk** - A data disk is a VHD that's attached to a VM



A Snapshot is a read-only full copy of a disk.



**Image -** You can create an image from your custom VHD in a storage account or directly from a generalized (sysprepped) VM

## **Azure Storage encryption**



Azure Storage automatically encrypts your data when persisting it to the cloud. Encryption protects your data and to help you to meet your organizational security and compliance commitments. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant

**Key management** - You can rely on Microsoft-managed keys for the encryption of your storage account, or you can manage encryption with your own keys, together with Azure Key Vault.

## **Disk encryption**



- Azure Disk Encryption allows you to encrypt the OS and Data disks used by an laaS Virtual Machine
- For Windows, the drives are encrypted using industry-standard BitLocker encryption technology
- For Linux, the disks are encrypted using the DM-Crypt technology

