Keeping Data Private: How do we do it

There is no disagreeing that cloud computing is changing the way IT infrastructure can be delivered, managed, and consumed. Correspondingly, cloud computing – whether delivered as infrastructure as a service, software as a service applications or email as a service – requires organizations to put a thought into their security model the further they advance up the cloud adoption curve.

Tech Agile in its efforts to maintain Data Security and Privacy at the infrastructure level implements reasonable and appropriate measures designed to help secure Your content against accidental or unlawful access or disclosure and thereby maintain data privacy of the information. Encryption of data (data-at-rest) has long been recognized as a best practice to enforce the security and privacy of data, regardless of where it resides.

Tech Agile ensures that all of Your individual Virtual Machine (VM) data is encrypted at rest. The system generates an encryption key and maintains for each VM. The system itself generates a 64-character hash when a VM namespace is created and stored in the separate memory space of each Compute node, which means for each of Your VMs there are unique hash keys generated using parameters such as the date and time of creation of VMs.

As the data is written to the block device on the Compute node, it is appended onto a Storage object on the Write cache. Further when this object is synced to the Storage backend, it is transported over a secure channel to the Storage Controller node selected to handle the object Put operation. Before it is encoded, to be spread over multiple Storage nodes (forming the Storage Cluster), that data block is encrypted with 256-bit AES algorithm before the object is written out. Therefore, only a Compute node with the correct access rights and key will be able to decode the data.

So in a nutshell, the encryption key is generated by the system, attached to the plain data block and processed further using 256-bit AES algorithm by the Storage Controller Nodes, and the resultant encrypted data is stored in a secure, fully encrypted fashion at rest on the Storage Cluster. Be rest assured, Your data is stored in a very safe and secure manner.

Your Responsibilities

No matter what measures and controls are put in place by the infrastructure provider to secure Your data, that does not absolve You from maintaining Your own due diligence and responsibilities. It is of paramount importance to note that You are solely responsible, but not limited to, for the following:

- The security of the virtual server/desktop at the Operating System level and all installed applications
- Safeguarding any data stored on the virtual server/desktop from unauthorized access
- Generating strong password(s) at the Operating System level and all installed applications preventing any unauthorized/unwarranted access
- Maintaining confidentiality of the password(s) generated above
- The configuration, maintenance and troubleshooting of the installed Operating System and any application in all circumstances, including application upgrades
- In the event that automatic Operating System patching is disabled, you are responsible for installing all OS security updates