compare between on premise and cloud computing?

Deployment

On Premises: In an on-premises environment, resources are deployed in-house and within an enterprise's IT infrastructure. An enterprise is responsible for maintaining the solution and all its related processes.

Cloud: While there are different forms of cloud computing (such as public cloud, private cloud, and a hybrid cloud), in a public cloud computing environment, resources are hosted on the premises of the service provider but enterprises are able to access those resources and use as much as they want at any given time.

Cost

On Premises: For enterprises that deploy software on premise, they are responsible for the ongoing costs of the server hardware, power consumption, and space.

Cloud: Enterprises that elect to use a cloud computing model only need to pay for the resources that they use, with none of the maintenance and upkeep costs, and the price adjusts up or down depending on how much is consumed.

Control

On Premises: In an on-premises environment, enterprises retain all their data and are fully in control of what happens to it, for better or worse. Companies in highly regulated industries with extra privacy concerns are more likely to hesitate to leap into the cloud before others because of this reason.

Cloud: In a cloud computing environment, the question of ownership of data is one that many companies – and vendors for that matter, have struggled with. Data and encryption keys reside within your third-party provider, so if the unexpected happens and there is downtime, you maybe be unable to access that data.

Security

On Premises: Companies that have extra sensitive information, such as government and banking industries must have a certain level of security and privacy that an on-premises environment provides. Despite the promise of the cloud, security is the primary concern for many industries, so an on-premises environment, despite some of its drawbacks and price tag, make more sense.

Cloud: Security concerns remain the number one barrier to cloud computing deployment. There have been many publicized cloud breaches, and IT departments around the world are concerned. From personal information of employees such as login credentials to a loss of intellectual property, the security threats are real.

Compliance

On Premises: Many companies these days operate under some form of regulatory control, regardless of the industry. Perhaps the most common one is the Health Insurance Portability and Accountability Act (HIPAA) for private health information, but there are many others, including the Family Educational Rights and Privacy Act (FERPA), which contains detailed student records, and other government and industry regulations. For companies that are subject to such regulations, it is imperative that they remain compliant and know where their data is at all times.

Cloud: Enterprises that do choose a cloud computing model must do their due diligence and ensure that their third-party provider is up to code and in fact compliant with all of the different regulatory mandates within their industry. Sensitive data must be secured, and customers, partners, and employees must have their privacy ensured.

Khalid Mohamed fakhry Albahnasy

200170049