BioSpectrum the business of Bio & Health Sciences ASIA EDITION

Overcoming Cloud Networking Challenges: Building secure foundation for Pharmaceuticals

November 16, 2021 | Opinion | By Warren Aw, Managing Director, APAC, Epsilon

Pharma and biopharma enterprises face a unique set of challenges on top of the overarching challenges of the cloud



In recent years there has been an explosion of cloud connectivity options, including a variety of private cloud, public cloud, multi-cloud and hybrid cloud models. According to Statista, in 2022, the global public cloud services market is expected to grow by approximately 22% to reach $482 billion.

There are a number of challenges related to networking and security created by the adoption of both single and hybrid cloud architectures. For pharmaceuticals and biopharmaceuticals, these challenges are intensified further due to the highly sensitive nature of patient data that is often accessed.

Pharma and biopharma enterprises must choose a cloud partner that will work with them to overcome the challenges and support them to be successful in the cloud with whatever model they choose. It's crucial for these enterprises to find a cloud networking solution that is simple, yet powerful and efficient, with the backing of an expert in the field.

Complications in the Cloud

There are a number of challenges related to networking and security created by the adoption of both single and hybrid cloud architectures. One key challenge is network and security complexity, in terms of single or multi-cloud, connecting to the cloud, and having consistency across clouds. Another key problem facing enterprises is observability and troubleshooting, including total non-existence from cloud providers, multi-cloud visibility and flying blind.

These issues are only amplified by skill gaps, lack of automation, different native constructs and clouds that are application-focused.

Pharma and biopharma enterprises face a unique set of challenges on top of the overarching challenges of the cloud:

- **Transport** – When your data is in motion, it must be protected, whether it's the transfer mechanism, encryption in motion or simply access to the data whilst in transit.
- **Auditable** – All facets of data protection must be auditable, including the network, its access and its transport data.
- **Encryption** – All data must be encrypted whether at rest or in motion.
- **Availability & Processing** – Systems and data should be available at all times, and flexible enough to deal with incidents quickly and efficiently.
- **Security** – The defense of the data, systems, infrastructure and network must be defended with up-to-date security technologies and processes.
- **Access** – Only those permitted to access certain types of data, system and/or infrastructure should be able to, and access should be easily maintainable.

Network and Security

Cloud technologies have improved pharma and biopharma by making data more accessible and on-demand. However, with an increase of these technologies, there is also an increase of cybersecurity risks if not properly managed and protected.

Generally, the following are the key areas of security concerns and challenges organisations must be aware of:

- **Access to the network** – If you have access to a network, you have access to data – so managing who has access is critical. This means effective management of users and other system access.
- **Data-in-motion security** – When data is in transit or moving between systems, sites and even countries, it must be made as secure as possible.
- **Auditability** – Many regulators stipulate that any activity and change must be reviewable, trackable and open to audit. Keeping a consistent and linked path showing all networking changes is critical.

In a 2021 survey, 64% of respondents named data loss or leakage as their biggest cloud security concern, according to Statista. Therefore, how pharma and biopharma enterprises manage and secure their networks is as critical as any other form of security. If patients are to be protected, a reliable cloud network platform must be adopted to centralise the data, simplify operations and comply with security laws and regulations.

Partnering for a Secure Foundation

Cloud Service Providers (CSPs) do not deliver enterprise-class networking and security. Enterprises need more than basic networking and security, whilst a lack of common standards across clouds causes cost, time and resource issues.

IT and network teams are faced with more complexity when managing applications and workloads in the cloud, yet CSPs do not overcome these challenges or meet the needs of their enterprise customers. Enterprises in the pharma and biopharma sector need to find a simple yet powerful cloud model to enhance operations, comply with regulations and keep up in a changing market with new innovation.

The right enterprise-class cloud networking partner will make it simple to set up, automate, and support application environments, data stores, and other business infrastructure requirements across clouds including Microsoft Azure, Amazon Web Services, Google Cloud and more, with access to advanced networking and security tools that enterprises expect.

Enabling Success End-to-End

Organisations should be able to take advantage of IT efficiencies to save costs and respond to business opportunities and emergencies much more quickly and easily, with the confidence that its cloud partner will enable this.

Providers that offer an end-to-end cloud service across single and multi-cloud services with automation, operational visibility and control, can fulfil what pharma and biopharma enterprises need to expand their cloud capabilities. Your cloud networking solution should allow you to directly control native cloud networking constructs to maintain cloud simplicity and automation. It should also enable customers to consume security services to meet their security and compliance requirements.

Ultimately, pharma and biopharma enterprises will only truly be able to unleash their full potential when they choose a partner that understands cloud demands within the industry and can provide the 360° solutions to match.

Warren Aw, Managing Director, APAC, Epsilon- Singapore