The Essential Role of Cloud Managed Service Providers in Life Sciences Innovation

Successfully navigating life sciences companies needs for scalability, data analytics, security, cost control, and speed.

CONTENTS

Overview

Innovation and speed are the bases for life sciences companies developing new treatments. Time to market, access to data, the ability to scale, the need for data analytics and security, and the ability to control costs along the way are all critical to meeting business objectives. The move from on-premises computing to cloud computing and cloud services has been instrumental in aiding life sciences companies to accelerate their development cycles from startup to manufacturing.

This paper explores the role of cloud managed services providers to serve as a facilitator during the cloud journey, migration through maturity, to help extract the most value from information services in the cloud at the lowest possible cost.

There are four areas, particularly, that this paper addresses:

- New capabilities for life sciences research enablement
- Sensitive data security
- Bottom-line cost
- Desire for single, managed platform for multi-cloud services

New Capabilities For Research Enablement

At the massive Amazon Web Services (AWS) re:Invent conference in Las Vegas last December 2019, the company introduced 70 new products and features that include incredible improvements to machine learning models that help data scientists via Amazon SageMaker. There has been no slow-down in Q1 2020. Keeping up with the new releases, evaluating their impact to the business, incorporating their functionalities, and learning how to manage and secure them, is a continual job that few people have the time, expertise, or desire to do. Yet missing out on the impact of these releases could possibly slow development and progress.

For example, a major release from re:Invent was the introduction of Amazon Outposts, recognizing customers' desire for a single, managed platform with the value of the AWS cloud tools, while still maintaining their data on-premises in their locations. Outposts can be a valuable option for organizations that need to contain data in a company-owned facility or meet restrictions from proprietary lab systems. Outposts provide the unified front-end with cloud and on-premises compute/storage on the back end.

The job of managing your cloud environment and its security expands exponentially with the proliferation of capabilities and services of cloud providers like AWS.

Sensitive Data Security

When life sciences companies build environments in the cloud, it's crucial that they know where the cloud provider's security responsibilities end and where theirs begins. The shared-responsibility model is one of the basic tenets of a successful public cloud deployment, and often the least understood. It requires vigilance by both the cloud provider and customer—but in different ways.

AWS, which developed the shared-responsibility philosophy when it introduced the public cloud, describes it succinctly as, "knowing the difference between security in the cloud versus the security of the cloud." This model, which is radically different from how organizations are used to securing their own data centers, creates a disconnect for newer cloud enterprises. Their first question is often, "Is the cloud secure?"

The real question is, "Is my cloud being managed securely?"

The security of the cloud refers to all the underlying hardware and software: compute, storage, and networking, in both the customer's and the provider's environments. But the cloud provider takes care of theirs; the customer takes care of theirs.

Configuration of the foundational services is in the hands of the customer, including customer data; apps and identity-and-access management; operating system patches; network and firewall configuration; data and network encryption; continual security and compliance monitoring; resource allocation; and the list goes on. Add to that the burden of protecting critical data on laptops and mobile devices, in offices and remote, wherever there is internet access.

Sensitive Data Security, continued

If this seems overwhelming, it's because it can be. Especially for bandwidth-strapped IT folks who may not have the time, resources, or expertise to configure, continually optimize, monitor, secure, and ensure compliance for all the organization's cloud resources and users, 24x7x365. The good news is this can be solved with the correct tools, processes, and expertise in a continual approach with defined objectives.

The Bottom Line: Cost

If you are going to put your applications out there in the cloud, and continue to adopt new cloud services, you must also have a plan for securing them, managing them, and ensuring compliance and cost-optimization. For early-stage biotechnology firms, the cloud offers a capital-free deployment of data center resources, allowing enterprise-like features and functionality at SMB monthly costs. As data grows, however, governance and controls are critical to ensure there is not exponential cost creep.

With traditional data centers, engineers would specify the required performance, bandwidth, and equipment fixed monthly cost, conduct an upfront procurement of servers, storage, routers, firewalls, switches, etc., and then go about the business of setting up the equipment and getting end users connected to applications. In today's cloud-first world, cloud and network engineers have to take into consideration the per-byte cost of data transfer, router instance size, load balancer sizing, firewall licensing models, and even the regions to and from which data is routed. Each one of these components has a direct financial impact on the ROI and TCO of an organization's cloud initiatives. One poor choice can run up thousands of dollars of unexpected costs.

Experience shows that cloud customers need to have the visibility and governance of their cloud environments down to each byte of data transferred. It pays to have the right cloud resource management process and tools in place to effectively operate in the cloud. There are many solutions on the market today that can help technical teams make good design choices, and then monitor the economic implications in real-time, to avoid a cloud networking design mistake that could be the downfall of a cloud project.

You could hire a whole team of new people and build your own 24x7x365 network operations center, or you could save a lot of money by working with a highly credentialed cloud managed services provider with the people and platform already in place. PTP utilizes CloudCheckr in our platform to give cost savings visibility to customers where we deliver on average a 25% reduction in monthly cost.

ptp Infinite Innovation

Desire for a single managed platform to manage multi-cloud services

With so many releases and new products introduced into the mix, it becomes very difficult for an IT team to manage.

That's where a third-party managed service provider comes in: to keep up with the continual updates; to constantly monitor, make recommendations, optimize and secure; to keep eyes on your enterprise at all times, and to keep you informed along the way, all in a single, managed platform to which you have access.

Many life sciences companies that use a primary public cloud provider (like AWS) turn to third-party resources like PTP to help them fill in the gaps in their own skillsets and knowledge, and to augment the tasks required to properly manage and secure their cloud environments. This spreads-out the accountability for the "care and feeding" of the overall IT infrastructure. That's why cloud managed services, like PTP's platform, are gaining immense popularity right now.

When it comes to the continual monitoring and configuration of security services such as user access, authentication, security breach alerts, security threat remediation, and the like, a growing number of life sciences companies prefer not to leave it up to chance. They hire PTP to ensure that their cloud environment is under the watchful eye of certified cloud security experts who can immediately spot, remediate, and report on any performance impacting or malicious activity.

The cloud has proven to accelerate the deployment of business-critical systems to process lab and science data, facilitating movement from phase to phase for life sciences organizations. With the correct partner and expert oversight, you can harness the potential without succumbing to cost-overruns or creating new opportunities for security breaches. PTP's PeakPlus™ services are the answer more life sciences companies are turning to than ever before.

ptp Infinite Innovation