# TOP **FIVE MYTHS**

## For Pharmaceutical Companies Moving to the Cloud

As a pharmaceutical company, moving enterprise applications such as clinical trial management, CRM, collaboration tools, ERP, pharmacovigilance/clinical safety software, or e-commerce to the cloud makes a lot of sense when you're delivering to a global user base. The cloud is accessible from anywhere in the world, and you can achieve significant savings in infrastructure costs, right? Not so fast. Success in the cloud is not automatic, and not fully understanding what your cloud migration entails can result in a process fraught with budget overruns, backlogs of issues, and unacceptable end-user experiences. Let's debunk five common myths about moving to the cloud and offer the best practices to set you up for success in the cloud.

**MYTH: Moving my application to the cloud means I am automatically distributed everywhere I need, resulting in great performance across the globe.**

**REALITY:** IaaS and PaaS providers typically operate a relatively small handful of data centers globally. Being in the same region, or even the same country, is not the same as being in every single city where a good or a bad user may be located. Even in a scenario where your website or application is replicated across multiple data centers within your cloud provider ecosystem — which is extremely costly and complex — your application is still only deployed in a handful of locations globally, which can be detrimental to the performance experienced by end users.

**CLOUD BEST PRACTICE:** Augment the reach available from your IaaS or PaaS provider with a solution that enables applications and websites to be optimized for performance end to end — from the cloud data center all the way across the Internet to where the end users are located. This minimizes overall spend and removes the technical complexity of trying to serve global traffic using several cloud origins including replicating data, managing traffic flows, maintaining state across geographic regions, and leveraging ancillary services such as reporting, etc.

**MYTH: Being in the cloud will offer protection that can scale to meet the demands of any cyberattack.**

**REALITY:** If your application is designed correctly, most cloud providers will allow for workloads to auto-scale compute and storage resources. However, simply adding more compute and storage resources will not provide the instantaneous scale needed to prevent the input/output of the cloud data center from being consumed by the incoming attack, rendering your application unusable.

**CLOUD BEST PRACTICE:** Make sure your cloud security solution has the real-time scaling capabilities required to ensure compute, storage, and bandwidth resources are not consumed by an attack.

**MYTH: Because I am in the cloud, scaling infrastructure resources will be cheap and easy — especially compared to the old way of using on-premise data centers.**

**REALITY:** When you first start out and have very low usage, using a cloud provider can be very cost effective. But as your usage grows in terms of compute cycles, storage requests, and the use of additional infrastructure resources, many organizations find their monthly cloud spend gets very expensive, very quickly. In addition, scaling at the infrastructure level to support additional capacity requirements is often not linear (i.e., a 2x traffic influx may not equal 2x the amount of infrastructure resources). This results in increased cost and complexity to design and operate in the cloud.

**CLOUD BEST PRACTICE:** Organizations can prepare to scale cloud usage cost effectively in two primary ways. The first is by designing their applications so they can fully utilize the auto-scale capabilities of cloud providers. The second is by leveraging additional cloud-based services, such as a CDN, to offload as much application usage and bandwidth requirements as possible close to end users, which is superior to paying to process and deliver 100% of the workload within the cloud data center.

**MYTH: To improve security in the cloud, you have to sacrifice performance.**

**REALITY:** If designed correctly, your cloud security solution should not negatively impact performance.

**CLOUD BEST PRACTICE:** Select a cloud security solution that is separate from your IaaS or PaaS provider and has the scale, distribution, and proximity required to not only prevent security threats but also improve performance for end users.

**MYTH: Though the cloud presents availability issues, we can overcome them easily by replicating workloads across multiple cloud data centers.**

**REALITY:** Replicating your workloads adds significant cost and complexity. Using multiple cloud data centers causes costs to skyrocket and the list of available features and services typically varies across IaaS and PaaS data centers within a cloud-provider's ecosystem, making application design much more challenging.

**CLOUD BEST PRACTICE:** Leverage a single, primary cloud origin, a secondary failover location either on-premise or in a co-lo facility, and a tertiary failover environment that can serve a basic, lightweight version of your website or application in the event both your primary and secondary environments are offline.

By being mindful of the above myths and the best practices to accompany them, you are positioning your cloud journey for success and will see tremendous benefits in terms of cost savings, greater agility, faster time to market, and better end-user experiences.

Learn more at **www.akamai.com/cloud**

Akamai FASTER FORWARD