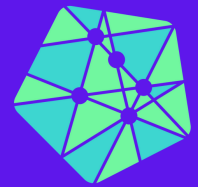# 7 CLOUD MYTHS

## Myth #1: Cost and value.

**The main value of cloud business cases is IT cost reductions.** The common industry introduction to cloud refers to the replacement of key IT activities, access to on-demand infrastructure, provisioned compute, storage, database services, and more. While all these descriptors are accurate, organization leaders often hear them and lose sight of the broader impact cloud can have on transforming the full IT operating model and, most importantly, on the business. Consequently, when they set out to write a business case, they spend months analyzing on-premises costs compared with cloud costs and focus much less time on the main value driver of cloud: the business benefits.

The reality is that the aggregation of business benefits can swamp IT cost efficiencies in cloud. **Cloud can improve almost every aspect of an organization's products, services, or processes.** Superior computing power can lead to a greater understanding of customer needs, for example, while extra processing capacity can be used to run more complex analytics or to create differentiated business insights. Innovation is quicker and less risky because experimentation and testing of new ideas cost less and take less time.
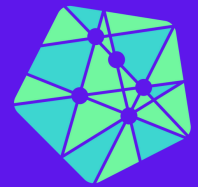
## Myth #2: Cloud computing costs more than in-house computing.

Cloud economics is one of the most contentious current questions in enterprise IT. The reality is complicated, as cost is highly dependent on a company's starting point — and its ability to govern and optimize cloud consumption once there.

Some starting-point differences we see are companies' maturity in on-premises life cycle, license commitments, and types of workloads. **Companies facing large data-center upgrades, for example, will find cloud adoption attractive** as a way of avoiding large capital expenditures on assets they may not fully utilize for years and that risk being deprecated faster than in the past. Where the shared-resource model does not translate into total-cost-of-ownership (TCO) savings, it is often because companies lack correct resource governance, or they migrate applications designed to run internally without adjusting their resource consumption models. Such applications will not fully leverage the benefits of auto scaling and are more costly to administer and maintain than cloud-native applications. Therefore, to keep running costs low and maximize benefits, companies should assess their applications' architectures, remediate their portfolio where needed, and establish new transparency and governance processes. **The core question for cloud economics is whether the reduced run-rate cost on cloud justifies the up-front cost of remediation, assuming all configuration and governance are done correctly.**

# 7 CLOUD MYTHS
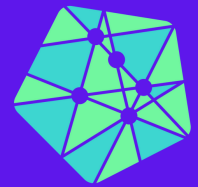
**DIHVB**

**Myth #3: : The security I can set up and control in my own data centers is superior to the security on cloud.**

Historically, executives have cited security of public cloud infrastructure as one of their top concerns and a barrier to cloud adoption. In recent years, however, all major CSPs have made significant investments in their underlying security capabilities. A CSP's business model depends on best-in-class security, and they have each invested billions in cloud security and in hiring thousands of the top cyber experts. Gartner, predicts that, through 2025, **99 percent of cloud security failures will be the customer's fault, not the security provider's**. Developers, therefore, must be retrained to follow carefully defined governance and policies on how to configure the right security controls. For these new policies to be successful, cloud requires companies to adopt a DevSecOps operating model, where security is a key element of every software project. IT organizations should automate security services across the full development cycle and make them available using APIs or risk vulnerable configurations.

More than one large financial institution has had to put its public cloud program on hold due to poor operating-model and configuration decisions. These institutions are now backtracking to invest in automated security controls for future applications, having discovered, like many other organizations, that they can no longer rely on manual security controls and traditional operating models if they want to transition successfully to cloud. **The key question for companies, therefore, is not whether cloud is more secure to begin with, but what measures they need to take themselves to enhance their cloud security.**

**Companies that define the correct policies, adopt a secure DevSecOps operating model, and train or hire the right talent can actually achieve safer operations in their cloud environments than on-premises.**

# 7 CLOUD MYTHS
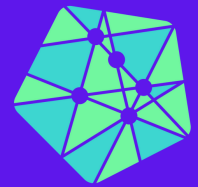
**Myth #4: There is greater latency among applications running on cloud providers' networks than there is on in-house networks.**

Some organizational leaders fear that when they transition to cloud, they will experience higher latency on a CSP's network than on their own. Latency, however, is often the result of the IT department attempting to backhaul its data through in-house data centers. Backhauling, or routing traffic through internal networks, creates higher latency, extra complexity, and poor user experience. IT departments that choose to backhaul usually either lack experience or trust with cloud security (believing they will have greater control by backhauling) or need to access critical data or apps that are in on-premises data centers.

It is important for IT departments that are backhauling for increased security to realize that CSPs now offer strong perimeter options and that there is no need to tolerate latency for security. **In fact, companies may even experience lower latency in cloud, due to CSPs' advantages in content delivery**. With their diverse, global footprint of data centers and their heavy investment in content-delivery-network services, CSPs can provide content at optimal speed, depending on location, content request, and server availability, on a scale that companies would be hard-pressed to achieve in-house.

**Given both the advantage CSPs have in content delivery and the shift away from backhauling, companies should not fear high latency during their move to cloud.**

# 7 CLOUD MYTHS
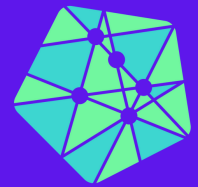
**DIHUB**

## Myth #5: Moving to cloud eliminates the need for an infrastructure organization

The idea of infrastructure as a service (IaaS)—that an external provider will manage your underlying network, hardware, and resources—**is an exciting proposition for many organizational leaders**.

The misconception arises, however, when leaders interpret IaaS as a full replacement for their infrastructure organization. While cloud radically changes the activities, talent, and operating model required in an internal infrastructure group, and beyond it, it does not altogether replace the need for infrastructure management. **When companies transition to cloud, they will encounter hundreds of services that can be combined and configured to affect performance, security, resiliency, and more**. They need an infrastructure team that can build and manage standard templates, architectures, and services for use by their development teams. Shifts in infrastructure are not only helpful in managing cloud but also necessary in order to see the full range of cloud benefits. A large entertainment company saw that when it shifted to a cloud-compatible operating model, its infrastructure team could deploy to production on demand, support a larger infrastructure footprint with leaner teams, and improve time to market, going live in six new locations in record time. In general, traditional infrastructure teams running cloud would be too large and too costly and would miss the benefits of having app teams own shared responsibility for the run costs they incur. On the other hand, having no infrastructure team at all would wreak havoc on an organization's ability to manage and benefit from cloud. Instead, a leaner, more specialized infrastructure organization is required to achieve the full range of agility, innovation, and performance benefits of cloud.

# 7 CLOUD MYTHS
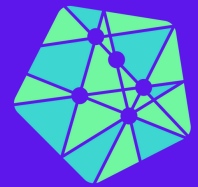
**DIHVB**

## Myth #6: The most effective way to transition to cloud is to focus either on applications or on entire data centers

**It is a common misconception that an organization must opt for one of these two extremes to transition successfully to cloud.** In the application-by-application approach, organizations face unattractive scale dynamics. They will continue to pay for on-premises data centers and IT support, while simultaneously paying CSPs for hosting a subset of applications. Moving a subset of applications also does not lead to business benefits if those applications constitute only part of a business domain's portfolio.

For example, if a business moves a set of applications within the customer-onboarding domain to cloud, but leaves behind the application that generates and stores user profiles, the time-to-market benefits of cloud cannot be fully realized. On the other hand, organizations that move an entire data center to cloud may face substantial up-front investment and risk. Many of the hundreds of applications in a data center probably were not designed to run in cloud. Companies will need to invest in various forms of remediation, which can become expensive and risky when executed all at once. Instead, organizations should look to move business domains to cloud (such as customer onboarding, early-stage drug discovery, consumer payments). **By transitioning the business domains, companies will experience the full range of potential cloud benefits:** faster time to market, greater agility, stronger reliability, and more. In addition to the business benefits, moving a business domain is a much smaller lift than moving an entire data center, meaning that cost and risk will be more manageable. Once one business domain begins to experience these improvements in time to market, agility, and reliability, it will be easier to make the business cases for the remaining domains.

# 7 CLOUD MYTHS
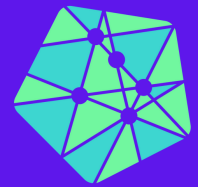
## Myth #7: To move to cloud, you must either lift and shift applications as they are today or refactor them entirely

**When companies make the commitment to move to cloud**, they often face pressure to move fast, minimize costs, and maximize business benefits. As a result, leaders feel they must choose between a quicker and cheaper "lift and shift" transition strategy (to move fast and minimize costs) and a time-intensive and costly refactoring strategy (to capture business benefits). While lift and shift—virtualizing the application and dropping it into cloud as is—can be a faster and more cost-effective way to move many applications into cloud at once, it fails to harness the majority of cloud's benefits. That's because there is no change to the application's architecture, which is often not optimized for cloud and so won't benefit from features like autoscaling, automated performance management, and more.

Furthermore, the non-native application will likely face higher latency or other performance issues, and its preexisting problems will now simply sit in a CSP's data center rather than the company's. On the other hand, a complete refactoring of the application and its architecture to optimize for cloud takes a lot of time, skill, and money. It achieves the benefits that lift and shift ignores, but so slowly and at such great cost that breakeven is often impossible. It also puts the transition at greater risk of error during complex recoding, configuration, and integration. Many companies find they are better off using a "best of both worlds" strategy that takes advantage of specific techniques such as automation, abstraction, and containerization.

**These techniques are less costly and time consuming than full refactorization but still allow companies to achieve the business benefits of greater agility, faster time to market, and enhanced resiliency.**