eBOOK

6 Challenges Driving Cloud Adoption

OneNeck®
IT SOLUTIONS
a TDS® Company

OneNeck®
IT SOLUTIONS
a TDS® Company

Contents

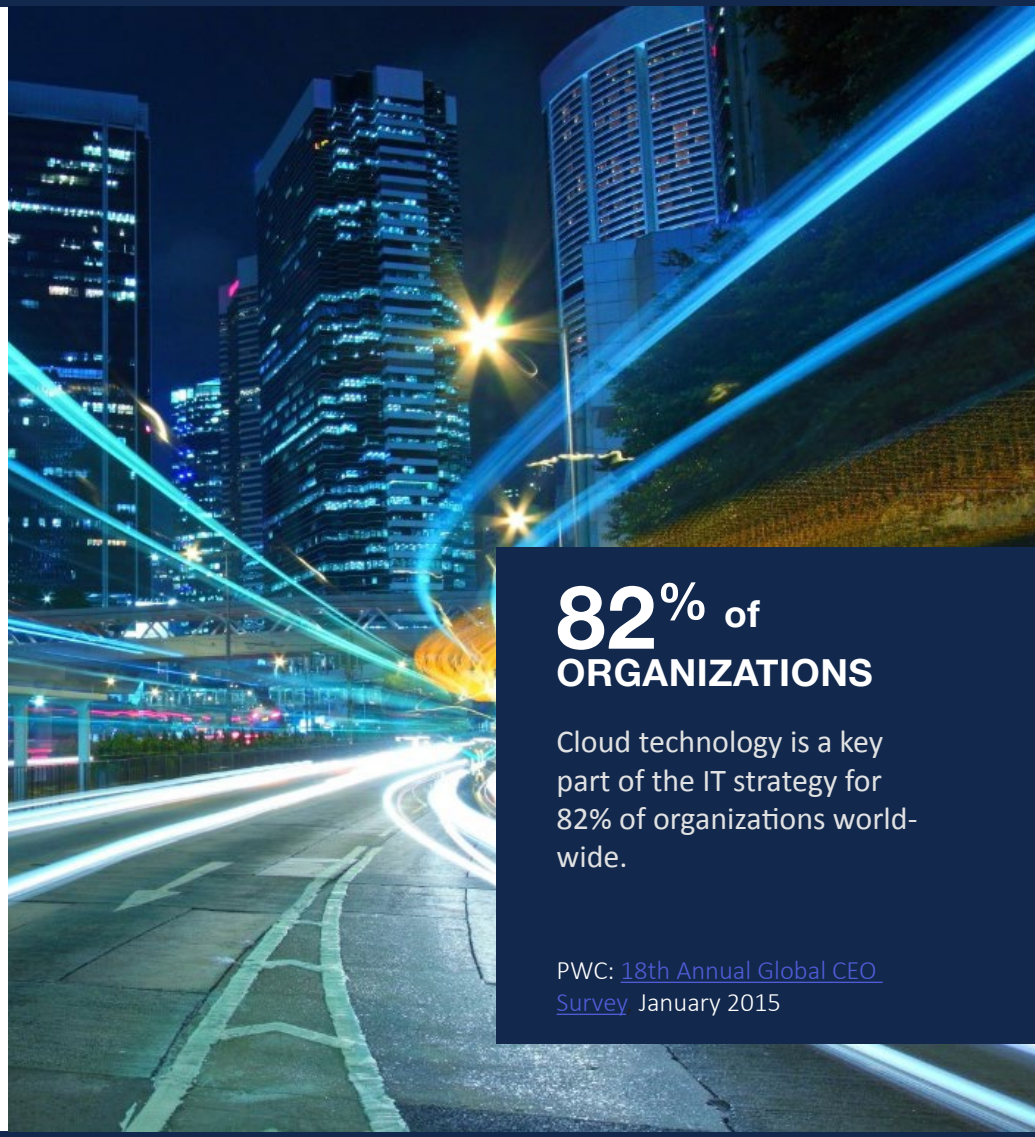
Painting the Picture...

The IT services industry has undergone massive, and disruptive changes over the past decade. Virtualization, cloud computing, the growth of mobile and Big Data have reshaped user expectations and the reality of how computing is delivered.

As a result, today's CIOs are no longer solely responsible for the management of IT, but now for supporting business growth by reducing costs, increasing efficiencies and driving innovation – all in effort to build a strategic advantage. The solution – cloud.

But before tackling the journey to the cloud, IT leaders must understand what is driving the move to the cloud. There's actually a strategic reason behind every cloud adoption effort, and identifying and prioritizing these cloud drivers is the key to success in developing and executing your cloud strategy.

In this eBook, we examine these challenges that the cloud solves, while also considering some of the reasons the cloud can help your organization keep pace and compete in a digital world.



82% of ORGANIZATIONS

Cloud technology is a key part of the IT strategy for 82% of organizations world-wide.

PWC: 18th Annual Global CEO Survey January 2015

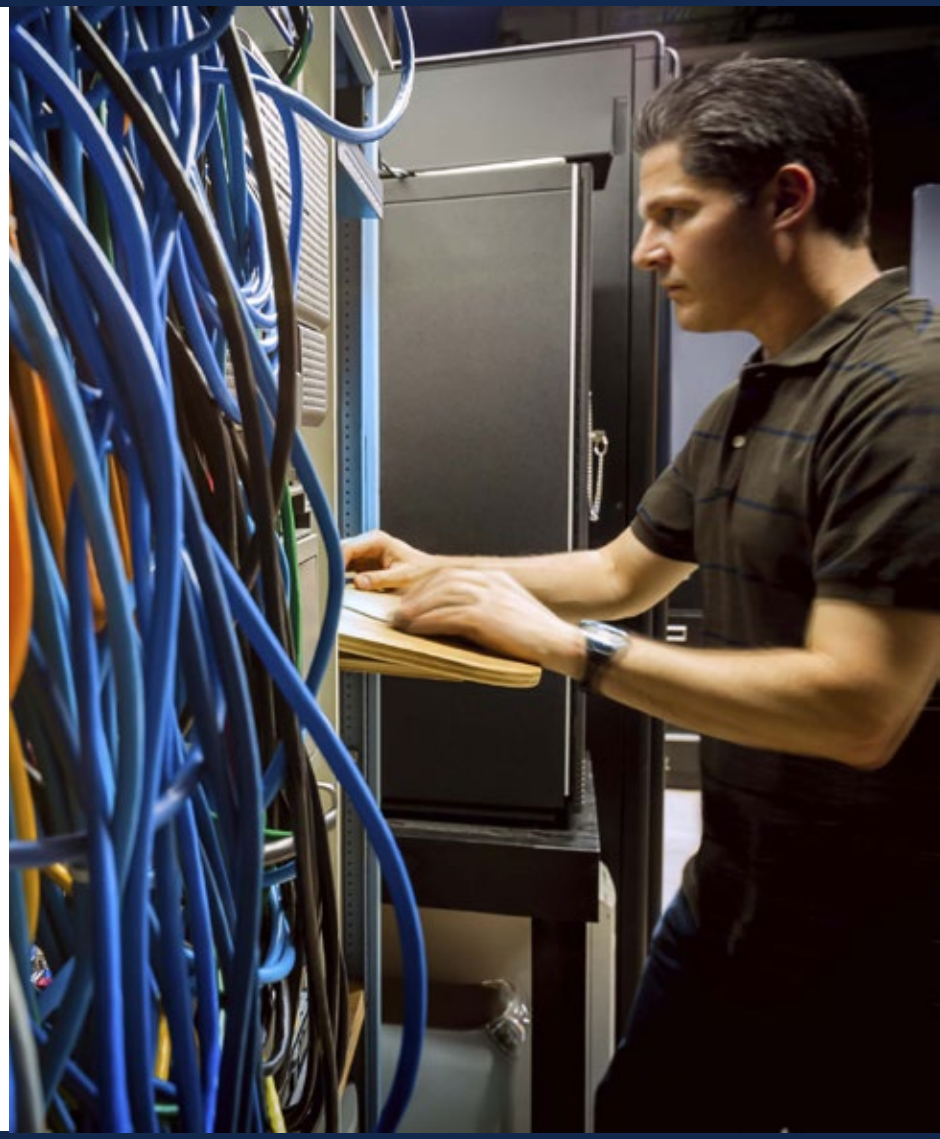
Challenge 1: Lack of Resources & Expertise

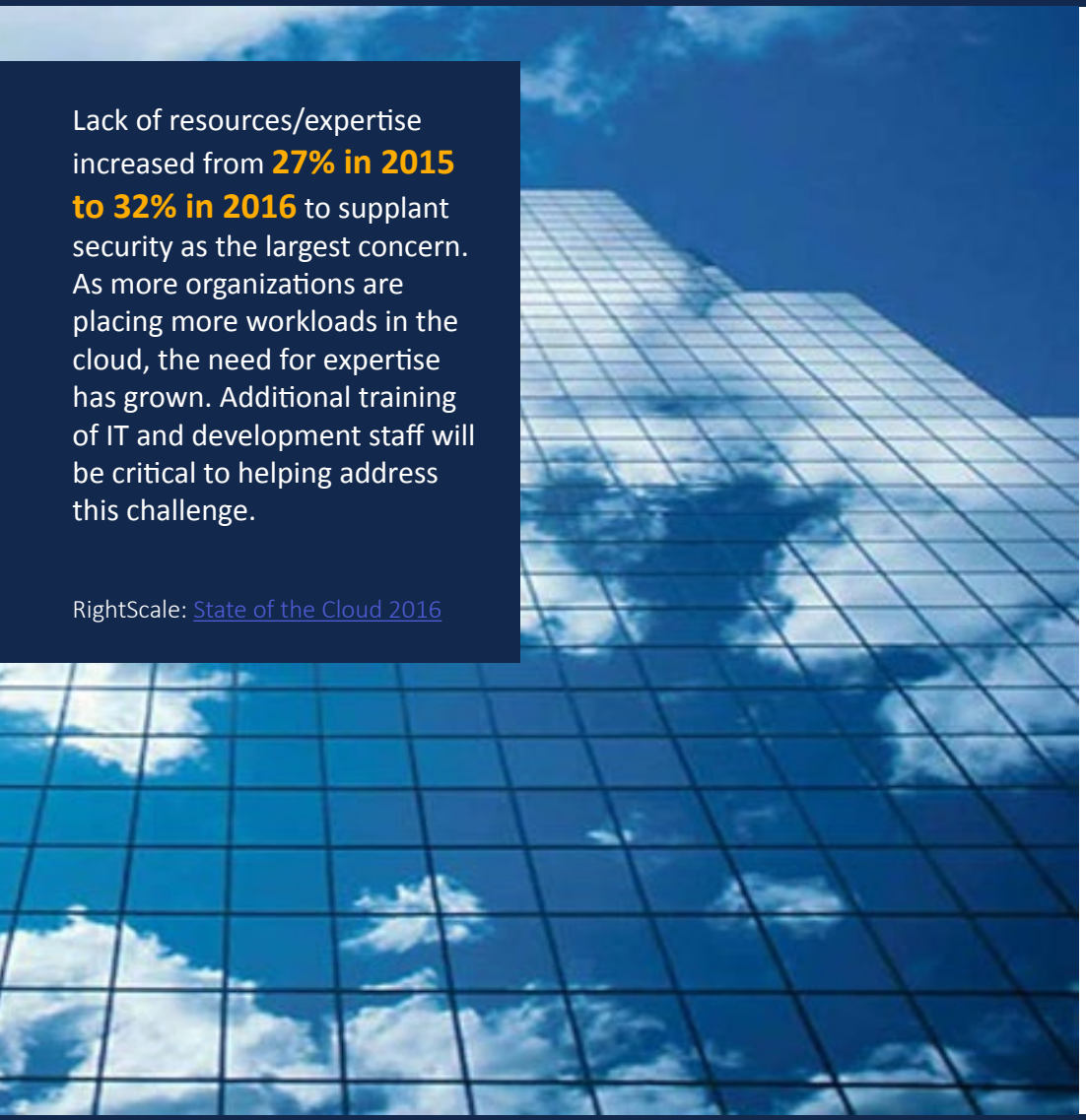
These days, the cloud seems to move at the speed of light. As such, successful cloud deployments require the help of certified experts with skills in multiple categories, including cloud architecture, deployment and security and performance optimization. As a result, cloud experts are in short supply and high demand. This lack of expertise or resources presents a significant barrier to cloud entry as most IT organizations do not have the resources they need internally to embrace and consume cloud services effectively and at scale.

Training of IT and development staff is critical to helping address this challenge. With already stretched IT budgets, sometimes it simply isn't cost effective to have to train, hire and retain the expertise required. One way to fill in the expertise gaps in any organization is to leverage third-party managed cloud providers. External help enables an organization to accomplish everything from assessing an application's cloud readiness to selecting the right cloud for a specific workload, and then dealing with the hassles of migration.

Leveraging third-party cloud providers can provide the following benefits:

- **Access to Experts:** Cloud Providers have the expertise on staff provides you with access to the professionals who can deploy, run and optimize your applications, reducing your need to hire this expertise in-house.





Lack of resources/expertise increased from **27% in 2015 to 32% in 2016** to supplant security as the largest concern. As more organizations are placing more workloads in the cloud, the need for expertise has grown. Additional training of IT and development staff will be critical to helping address this challenge.

RightScale: State of the Cloud 2016

- **Streamline Operations:** Cloud providers can ensure a smooth flow of data between necessary for operations to run efficiently, and will allow your management team access to the data they need in order to make intelligent business decisions.
- **Optimize Performance and Scalability:** Deploying your data and applications in a managed cloud environment ensures that the infrastructure supports the application's interoperability, scalability, database, bandwidth and security requirements.
- **Easily Monitor and Support Applications:** Managed cloud providers can monitor and support applications meaning your operations will run smoothly and end users will be happier – easing the burden for your IT department.
- **Adapt to Change and Reduce Complexity:** Through the use of best practices, standardization and automation you gain the ability to adapt to changes quickly and reduce the overall complexity of your IT environment.

To choose a provider for your organization, look for one with related expertise, who offers cloud, managed services and professional services to assist you through your cloud transition and beyond.

Challenge 2: Security & Compliance

The risks of cloud migration are largely captured in one word – *security*, and many of the organizations that are not adopting cloud cite security as the reason. Make no mistake – there will be more attacks on the cloud in 2016. The cause for this is not because of the cloud itself, but because there are simply more deployments in the cloud than ever before. Maintaining compliance and ensuring visibility into controls is key for cloud users, no matter what cloud architecture your organization adopts public, private or hybrid.

However, the security challenges faced by organizations wishing to use cloud services are not radically different from those dependent on their own in-house environments. The same internal and external threats are present and require risk mitigation or risk acceptance. Here are a few measures you can take to mitigate your risk in the cloud.

- **Start With a Plan:** Organizations should strategically approach their migration to the cloud. Start with a thorough evaluation of your data to identify the most sensitive and valuable data to determine the data most at risk. Once the data risks are understood, organizations need to set policies to protect that data by defining best practices and approved cloud use cases, and implementing appropriate governance and compliance controls.
- **Assess Security Protocols:** Assessing a cloud providers security protocols are a mandatory part of the evaluation process. Security begins with the physical security of the cloud provider's premises. The provider should have access controls that restrict physical access to its premises as well as robust online access controls that limit which employees can access your servers. They should provide encryption of logs and data and keep your sensitive data isolated from other cloud customers, even as part of backups. The cloud provider should provide network-level security features including next generation firewalls, intrusion detection and intrusion prevention software.

In order for organizations to move computing resources and applications to the cloud, the value must exceed the risk.

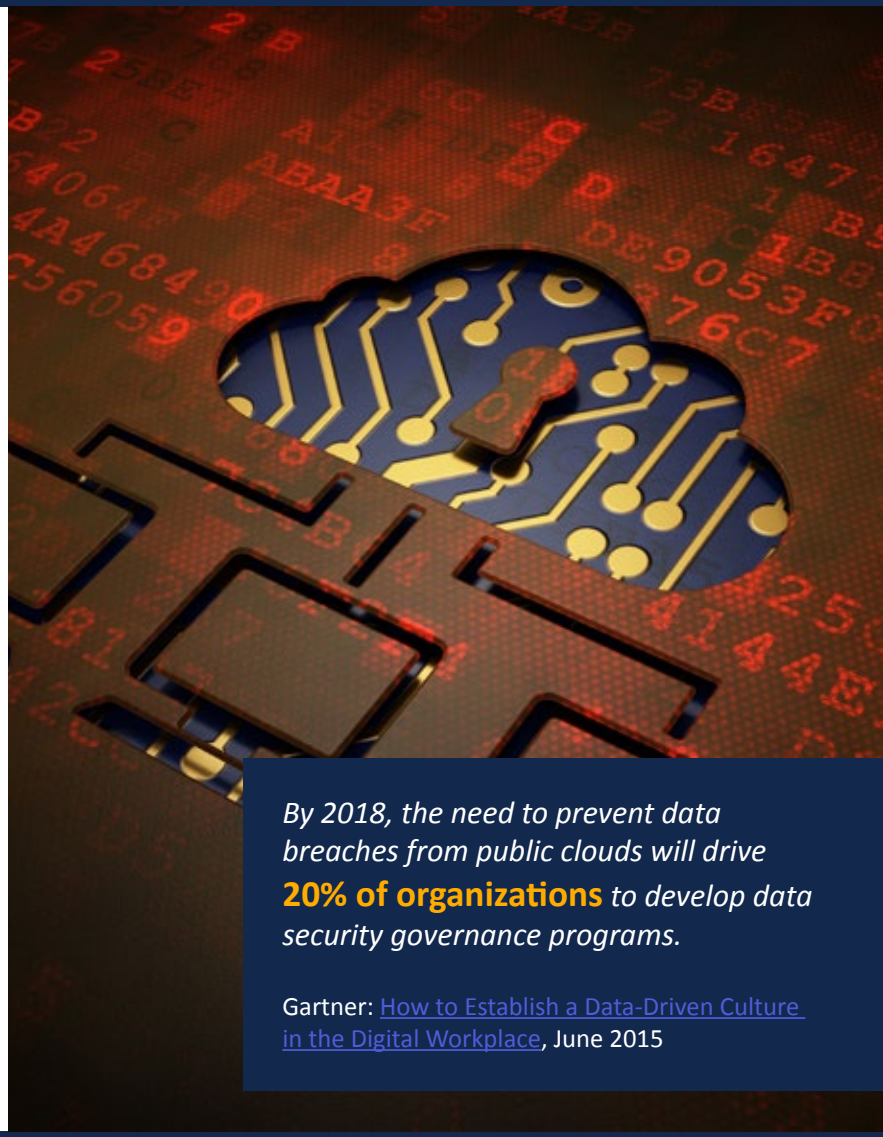
As cloud adoption moves to the mainstream and expands from tactical uses to strategic platforms, enterprises will need to address cloud security and compliance issues more holistically.

This will be especially true as organizations look to use cloud in cases where highly sensitive data is involved, where rigorous compliance requirements apply, or for business-critical applications.

Forrester Research, Inc: Security and the Cloud

- **Review Certifications:** Review the provider's security-related certifications, including ISO 27001. Depending on your industry and the data you plan to hold in the cloud, you should look how they meet appropriate compliance mandates, such as HIPAA. Don't just take the cloud provider's word for it; review any independent audit reports. Once you contract with a vendor, you should plan your own periodic reassessment in case changes at the provider or in the services you require impact the security controls.
- **Understand Your Risks and Ask More Questions:** Don't rely on network-level security but build strong security functionality into the application layer. Encrypt sensitive data both in motion and at rest. While cloud providers offer encryption you need to understand how the data is encrypted and how key management is handled. Conduct tests and vulnerability assessments that verify the security of your cloud-based data. A majority of attacks are initiated through web applications so find out how your cloud provider protects against vulnerabilities like SQL Injections, CSRF, XXS and Session Management. Create a list of questions for your provider to make sure you have covered all your bases.
- **Stay in Control:** Understand that even though you have vetted your cloud provider it is ultimately your responsibility to understand the inherent risks of your data, apply controls and manage SLAs. Extend your current security fundamentals to the cloud and understand your back-end processes. In addition, you need to train your employees in safe computing practices and define and enforce BYOD policies and controls.

The cloud offers amazing benefits for those who properly implement and secure their infrastructure. Ensure that you have dotted all your i's and crossed all your t's when it comes to keeping your organization safe in the cloud.



By 2018, the need to prevent data breaches from public clouds will drive **20% of organizations** *to develop data security governance programs.*

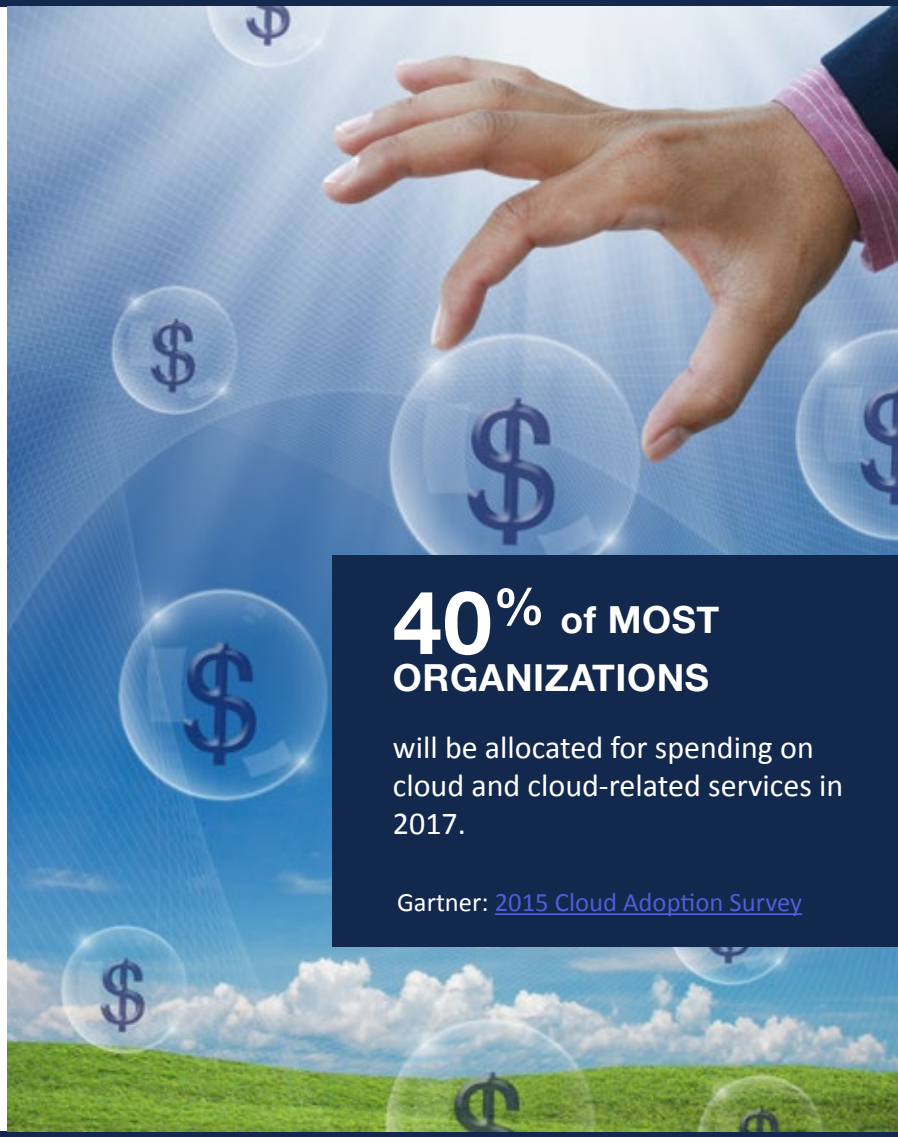
Gartner: How to Establish a Data-Driven Culture in the Digital Workplace, June 2015

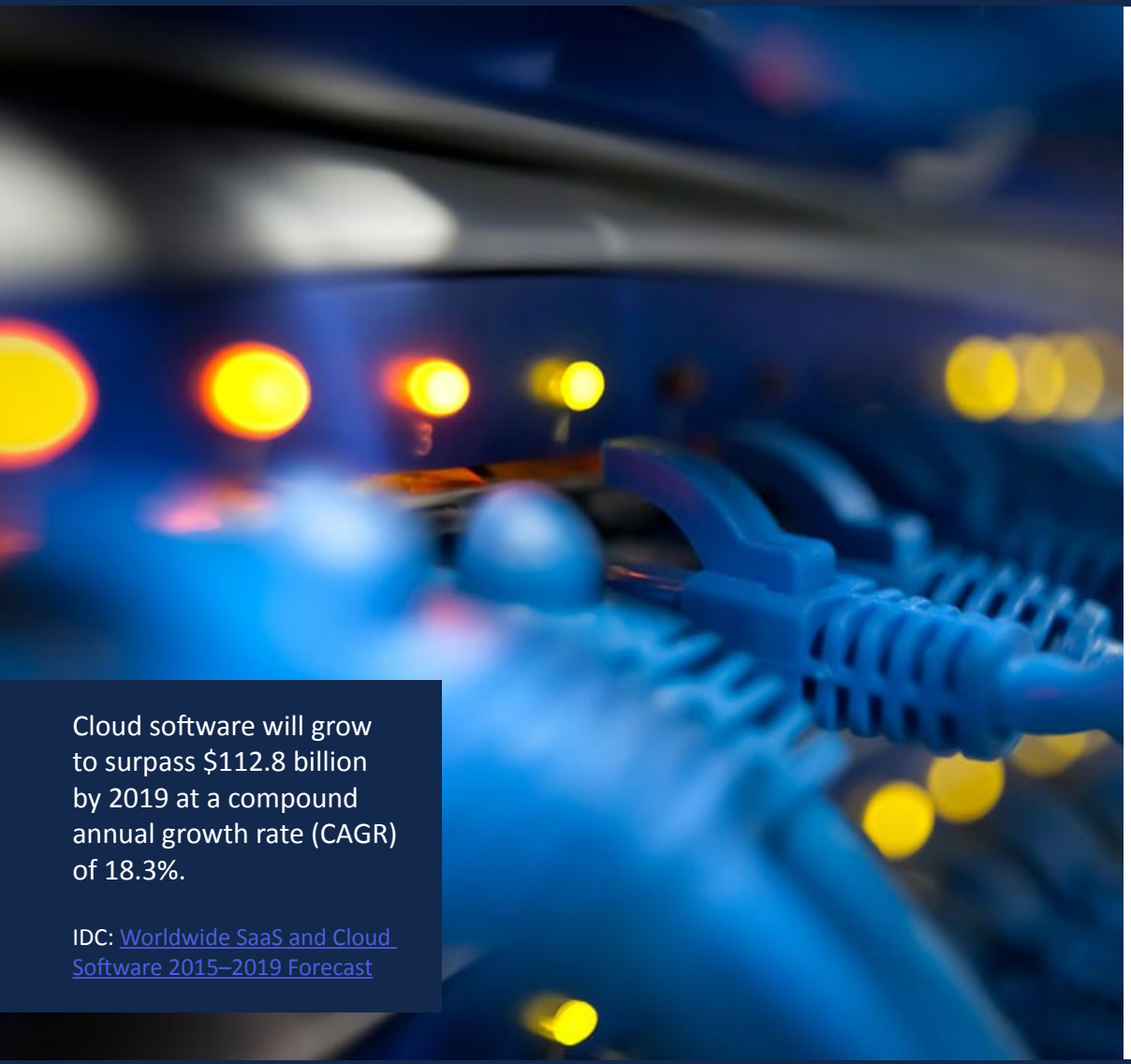
Challenge 3: Managing Costs & Aging Infrastructure

There are numerous drivers pushing organizations to the cloud; however, the mass acceptance of the cloud is in part clearly financial, as it allows organizations to let go of some of their costly IT infrastructure and shift computing costs to more manageable operational expenses. These drivers can be:

- **Reduced Licensing Costs:** Many organizations have experienced a considerable reduction in license and services spend by adopting cloud services, as often it has been the case that the cost of moving to the cloud is actually much lower than the license renewal of their legacy apps.
- **Less Hardware:** Migrating to the cloud enables organizations to reduce cost and maintenance by minimizing the hardware footprint.
- **Pay for Resources as Needed:** As a business grows, resources must rapidly expand with it, though not before they're really needed, leading to unused capacity and costing the business money. The ability to quickly provision resources as needed, while only paying for only what is used, is key.
- **CapEx to OpEx:** Moving to the cloud most often helps lower capital expenditures, as a simple subscription-based model is an easier option and requires little to no on-premises equipment and physical maintenance costs. What's more, operating expenses are also reduced as businesses don't have to have an in-house team monitoring availability 24/7.

It's important though to not assume you will save money by moving to the cloud unless you have done the crucial work to analyze your organization's unique situation. In their 2015 Cloud Adoption Survey, Gartner recommends:





Cloud software will grow to surpass $112.8 billion by 2019 at a compound annual growth rate (CAGR) of 18.3%.

IDC: Worldwide SaaS and Cloud Software 2015–2019 Forecast

- Utilize total cost of ownership and other models on a case-by-case basis.
- Segment cloud into use cases.
- Look beyond cost issues.
- Be certain to check with financial specialists about the implications that a switch from capital expenditure (CapEx) to operating expenditure (OpEx) may have. Don't assume that OpEx is always better than CapEx.
- Keep revisiting previous cloud analysis as the market and prices fluctuate.

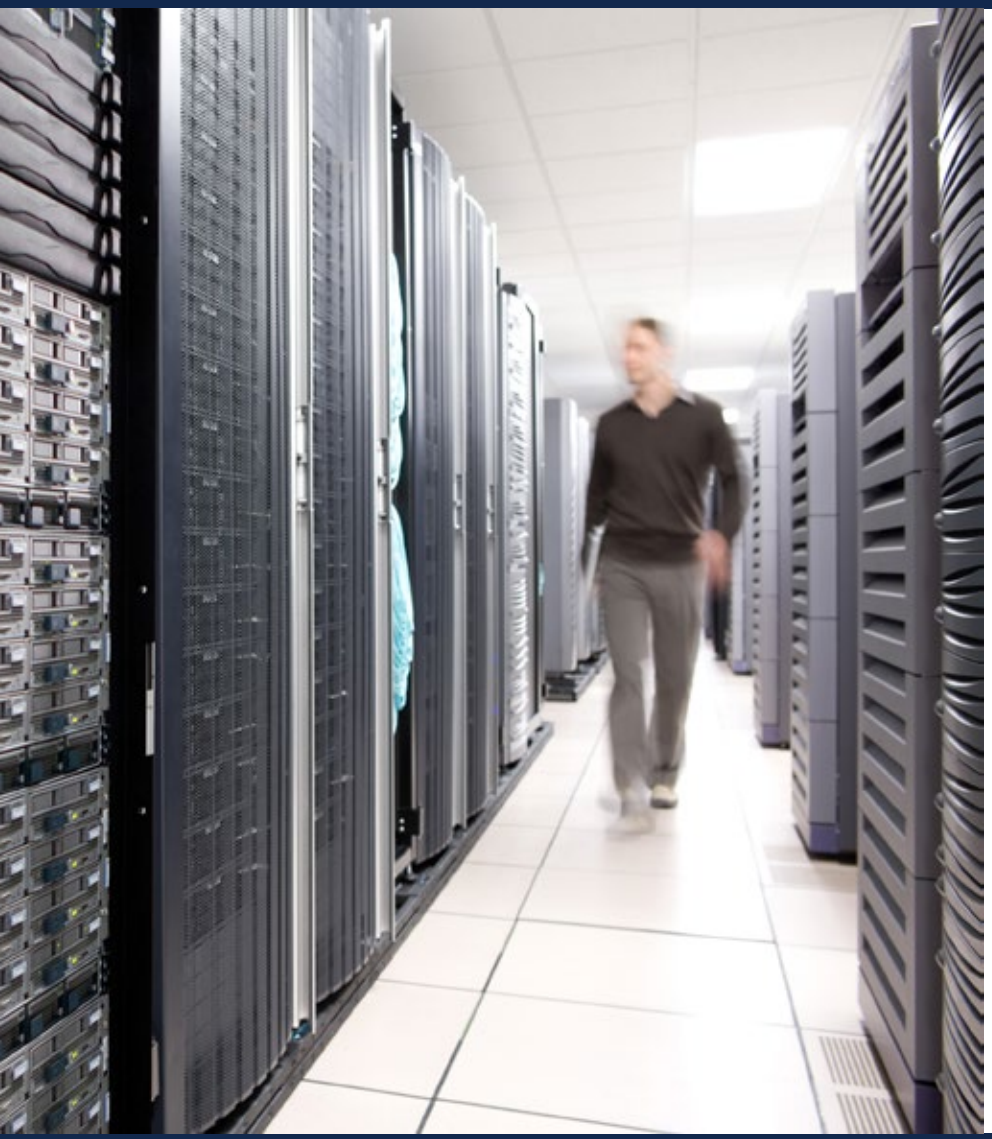
If one carefully looks at each of these financial considerations, then a move to a cloud solution could potentially be a smart decision that impacts the bottom line and helps an organization remain competitive in a real-time world.

Challenge 4: Private Cloud Complexities

At its most basic definition, private cloud computing represents the collection of assets that are fully controlled, operated and managed by the owning entity. Out of that pool, IT can create VMs in any configuration that your supply of resources will support. Many IT professionals are intrigued by the idea of a private cloud to reduce performance bottlenecks, simplify management and maintain a higher level of security and compliance.

While private cloud can be enticing, there are still roadblocks that drive IT to public third-party, cloud resources. These include:

- **Up-front Cost:** Convincing one's organization to drop a quarter of a million dollars for a private cloud solution, even if it will cut IT spending, is a huge up-front investment at a time when IT spending remains low.
- **Potential Unused Resources:** Unlike public cloud, private cloud is not delivered through a utility model or pay-as-you-go basis because the hardware is dedicated. So, there is the potential for unused and unnecessary resources taking up footprint in an on-premises solution.
- **Hybrid Complexities:** Merging cloud and in-house processes is rarely simple, and some work is necessary to enable the kind of automation and orchestration features that make private cloud appealing. IT will probably end up needing to turn to third-party tools and possibly a third-party consultant.



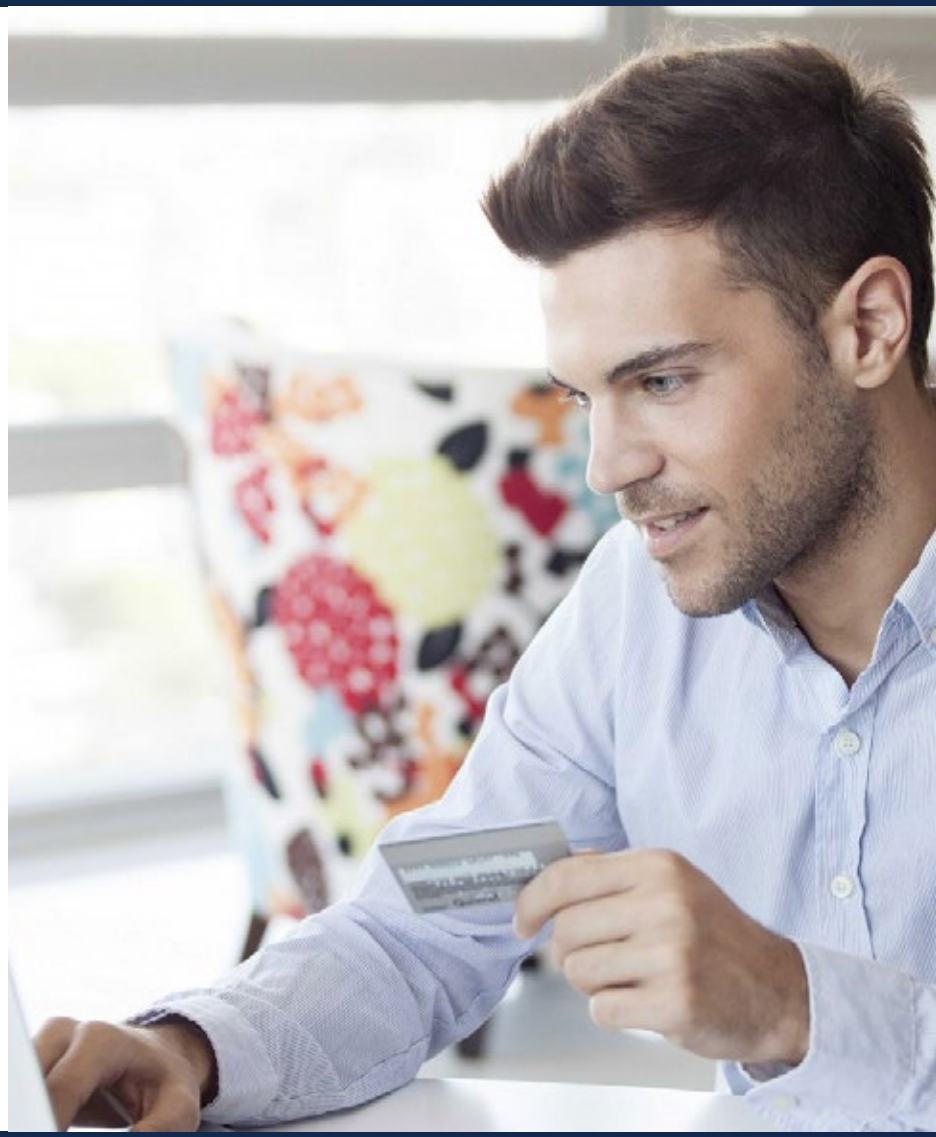
- **Performance Management:** Many IT professionals don't actively manage system performance, even after virtualizing. But to really get the benefits of cloud, performance monitoring should be a critical part of any private cloud strategy. It's important to embrace performance and capacity management at a data-center level when adopting private cloud computing, but this requires more tools than what a virtualization platform alone can provide.
- **Not Changing Processes:** Instituting a private cloud isn't just about installing new technology; it's about having a workforce that uses the features of the cloud to their fullest extent in their work process, and when organizations fail to recognize the need for adapting processes, their private cloud will meet challenges and potentially fail. In fact, according to Tom Bittman in a blog on the Gartner Blog Network, failure to change operational models was the number one reason for private cloud failure.

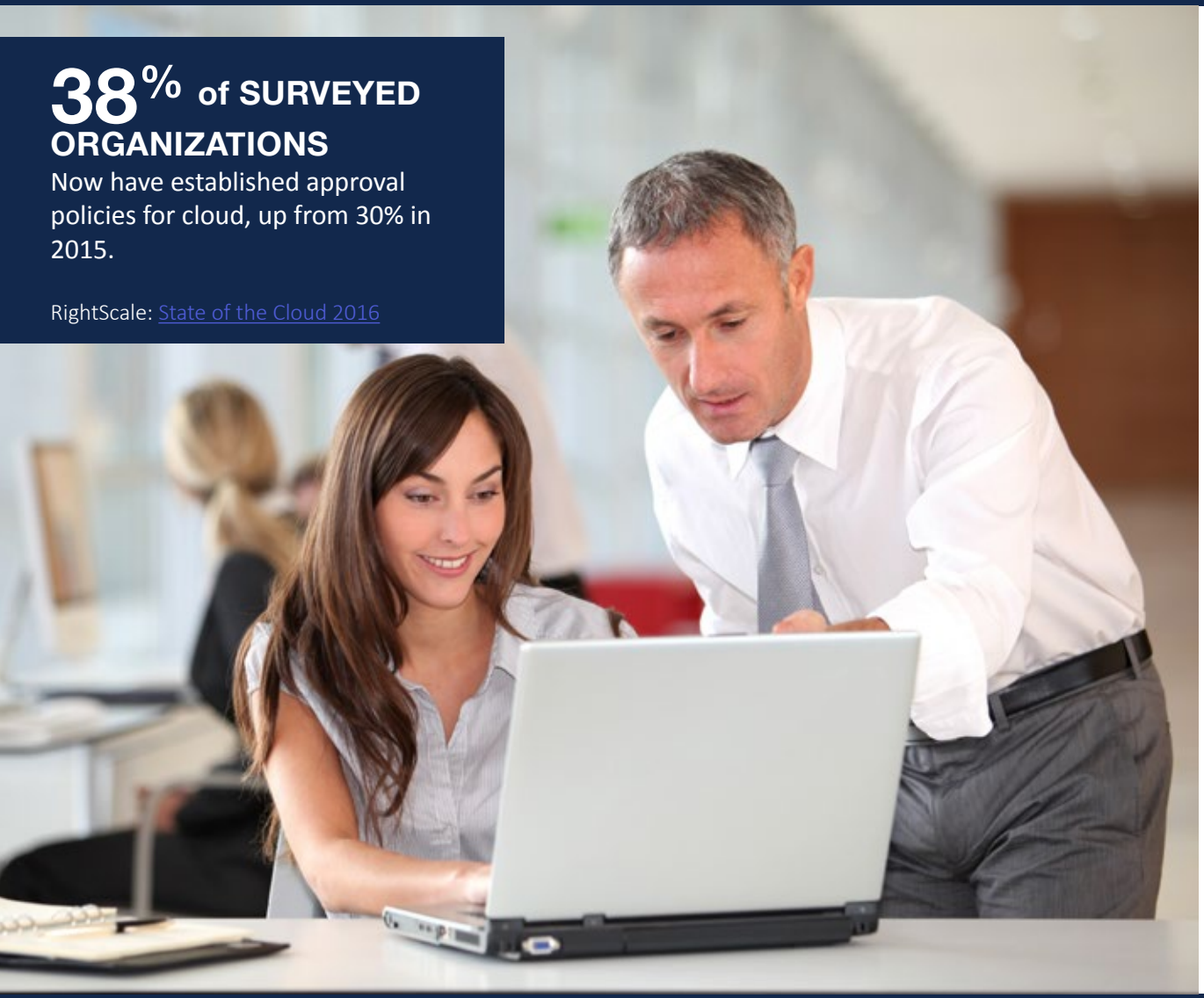
So, which way is right? Public or private? A recent IDC report forecasts strong spending for both public and private clouds, and says each segment continues to grow fast, with a 13% compound annual growth rate through 2017 to greater than $20 billion annually. So essentially, no matter whether you choose public, private or a hybrid approach for your organization, either can be the right choice today. The key part is that when it's time to implement your cloud strategy, work with a vendor that has deep understanding of the technical aspects of providing both private and public clouds who will help you make the right choices.

Challenge 5: Governance & Control

While the cloud has opened the door to endless possibilities in today's rapid-fire pace of business, it has also opened the door to security and compliance risks, keeping many IT professionals up at night. This is why governance control is key in moving to the cloud, as it is the mechanism through which organizations can ensure effective management of information security in the cloud. Without it, organizations are opening the door to:

- **Increased Spend:** While the cloud brings greater agility, it can also bring increased costs due to Shadow IT, where users outside of IT (and without IT's consent) turn up cloud platforms on which to run their department workloads. In fact, Cisco research finds that, on average, CIOs estimate their organization is using only 51 cloud services, while the actual number is closer to 730.
- **Data Loss:** Shadow IT means there could be corporate data residing outside typical controls designed to ensure security and compliance. Lack of understanding the impacts of security risks, compliance complications, and potential legal issues within different deployments of the cloud can open an organization up to risk.
- **Missing Deadlines:** Since IT has no control over the development of the cloud provider's capability/functionality, there may be long development lifecycles. The lack of ability to quickly roll out competitive functionality can quickly lead to lost customers and profits.





38% of SURVEYED ORGANIZATIONS
Now have established approval policies for cloud, up from 30% in 2015.

RightScale: State of the Cloud 2016

At the end of the day, cloud governance is tightly woven with business goals and policies to ensure that services are optimized for user expectations. Because IT and business goals are tightly woven in a joint strategy, it is important to look at cloud governance from a holistic business perspective. Start looking at the relationship between IT and the business units and start working with them early to understand what their needs are for IT and to find out why these individuals are going outside IT and the corporate standards.

It really comes down to enabling the business. IT and security executives need to enforce data policies and procedures, all while ensuring mobile worker productivity and meeting employees needs for maximum productivity. This cloud governance can be accommodated through risk analysis and management, led by a qualified security professional. They will ensure risk is properly managed and balanced against the needs of the business and individuals who require cloud services. Only then will companies have a sound cloud governance strategy.

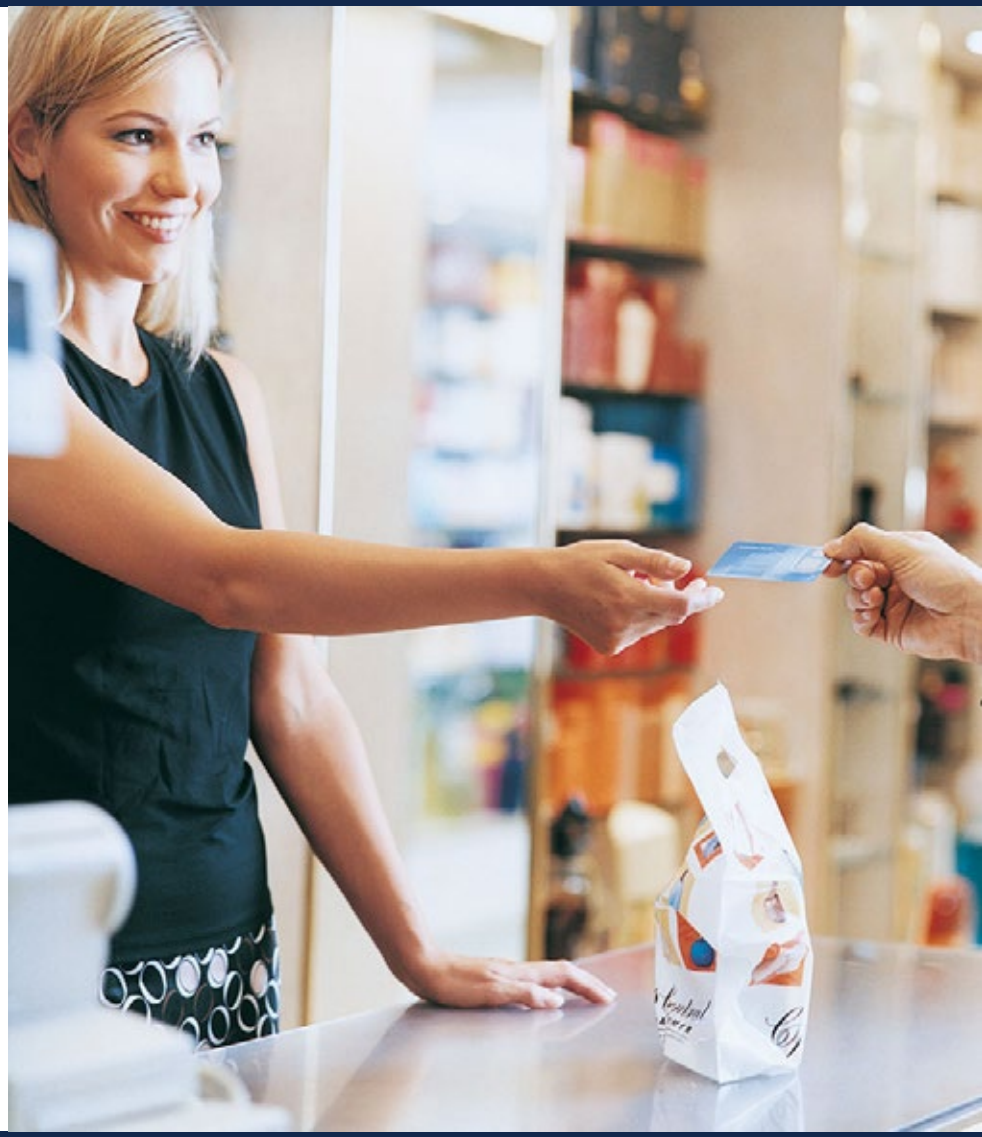
Challenge 6: Performance & Availability

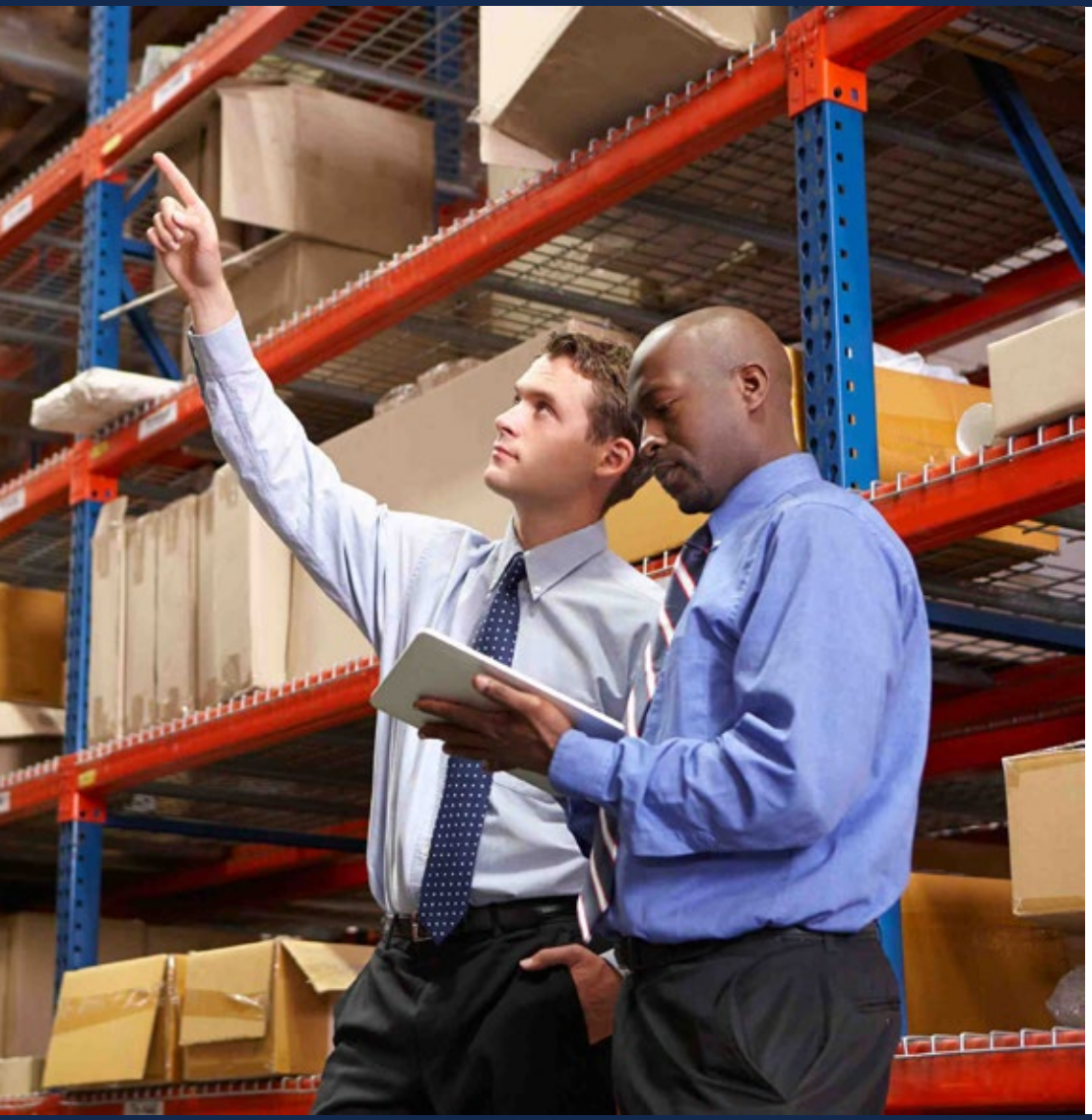
Businesses depend on their IT system. Reliability and availability are significant concerns and one of the primary reasons many are hesitant to buy cloud services, especially for mission-critical business applications and data.

Availability in the cloud will be critical for its long-term success with an enterprise. It's not limited to availability of just the applications and data being utilized that matters, but also the need for it to be accessible to the consumer anytime, anyplace without delay.

To address these challenges, cloud providers offer SLAs (service level agreements) for "uptime" and "availability". Delivering on a stringent SLA requires a provider's commitment to best practices and processes, a thoroughly redundant architecture, 24/7/365 staffing by trained and experience technicians, and best of breed hardware, software and network products.

While availability SLAs often meet the needs of many cloud-compatible applications, high-end applications in the cloud tend to require more than just an availability guarantee. Businesses need to define a set of application-specific performance metrics that govern performance and enforce them. This can often be achieved through the use of application performance monitoring tools that take into account everything from end user experience to runtime application architecture, business transactions and component monitoring to generate analytics and reporting to give you the data you





need to ensure your application systems are operating at peak efficiency.

In addition, evaluate your workload. The research firm IDC reports that understanding the characteristics of workloads is crucial when deploying applications to an organization's cloud environment. To optimize your cloud deployment you need to understand an application's requirements in six key areas in order to place it correctly:

- Performance
- Security
- Compliance
- Data protection
- Storage
- Automation

Through evaluation against those criteria, applications can be ranked as Tier 1, Tier 2, or Tier 3. The Tier 1 are critical applications with the strongest requirements for reliable performance or application security while Tier 2 and Tier 3 have less stringent demands. With these sets of criteria in mind, businesses can then match their applications and data to the appropriate cloud to ensure performance and high-availability.

In Summary... Not All Clouds Are Created Equal

Migrating to the cloud can provide your organization access to new services, increased speed and agility, collaborative capabilities, and managed services such as security, data backup, data restoration, and disaster recovery capabilities. Before businesses get caught up in a full-blown cloud transition, it's important to understand what issues the cloud solves, how adoption challenges can be addressed and how difficult the transformation can be without a clearly defined strategy to get there.

OneNeck IT Solutions is committed to helping our customers gain clarity from cloud complexity. We help customers navigate the cloud to get the Right Application, Right Cloud, and Right Time! Whether your workload is best suited for a major public cloud or within a private cloud we have an option for you.

Are you ready to extend your IT capabilities with the cloud, or do you need help building out your cloud strategy roadmap? Our approach is to fully understand your business needs and requirements and then help you identify the right cloud infrastructure for your workloads. We conduct a thorough Hybrid Cloud Infrastructure Assessment that covers all the bases to complete successful migration to the cloud: workload analysis, bandwidth analysis and end-user experience analysis.

Want to learn more? Contact us today to schedule a meeting, and we'll answer all of your questions. We look forward to helping you with...

The Right App. On the Right Cloud. At the Right Time.

The OneNeck Cloud Advantage:

- Enterprise-class performance and reliability
- End-to-end security
- Independently-validated scalability
- Financially-backed, reliable SLAs
- 24/7 support
- Ongoing innovation
- A support team that cares

(855) ONE-NECK

www.OneNeck.com

OneNeck®
IT SOLUTIONS
a TDS® Company