eGUIDE

OneNeck IT SOLUTIONS a TDS® Company

presents

Embracing the Cloud with Confidence

We all know the cloud is continuing to pick up steam. This is highlighted in new research by Gartner that finds the shift to cloud computing will impact more than $1 trillion in compounded IT spending over the next five years, making cloud computing one of the most disruptive forces in IT spending since the first days of the digital age.

The report, “Market Insight: Cloud Shift — The Transition of IT Spending from Traditional Systems to Cloud,” finds that while all IT spending is forecast to grow from $3.5 trillion in 2016 to $3.9 trillion in 2020 (a CAGR of 2%), growth in spending on cloud computing will far outpace that, hitting a CAGR of 17.5% through the same period. The result is a cloud shift totaling $114 billion in IT spending in 2016, growing to $216 billion in 2020.

Read more...

Gartner says the shift is driven by organizations adopting the cloud to:

- Replace existing IT systems (hardware, software and/or services): As traditional IT systems reach end of life, more companies are opting to forgo capital-intensive replacements and instead purchase alternatives in the cloud, where upfront costs are less, overall costs are distributed across monthly subscriptions and upgrades are faster and easier.
- Complement or extend existing IT systems: Instead of purchasing extra hardware and software to accommodate peak seasonal loads or handle temporary projects, many companies use the cloud to scale capacity up and down as needs require.
- Create new applications and/or services: Spinning up new services in the cloud creates significant cost and time-to-market advantages when deploying new applications and services.

The research firm finds this shift to the cloud currently impacts spending on all IT hardware, software and services businesses, although some are affected more than others. Of the five IT spending categories Gartner tracks, the shift to the cloud indirectly affects devices and communications services, but it directly affects the other three:

- Data center systems, including server hardware, external controller-based storage, enterprise networking equipment and unified communications.
- Enterprise software, including enterprise application software and infrastructure software.
- IT services, including business IT services and IT product support.

And this impact won't lessen any time soon, since 88% of organizations using cloud services or planning to use them in the future say they embrace a cloud-first strategy, where they choose the cloud first over all other options when it comes to IT expenditures.

Shift Brings Both Risk and Opportunity

While cloud adoption varies by country, region, vertical and organization size, companies with deep investments in traditional non-cloud systems will likely see significant cloud shift as they look to augment or replace those systems, while those with lighter technology investments will see a more incremental shift.

The cloud is here to stay. To capitalize on the future, OneNeck IT Solutions has the experience to reduce your reliance on traditional IT while maximizing your value in the cloud, ensuring a cohesive blend of traditional and cloud environments. OneNeck builds best-in-breed cloud solutions and roadmaps to leverage your current investment and create long-term strategic business enablement.

6 Challenges Driving Cloud Adoption

While the rewards are great, the journey to the cloud is not always a clear path. Whether your organization has already adopted the cloud, you are in the process of moving towards the cloud or you are still just thinking about dipping your toes into the cloud, as an IT leader you need to spend the time to understand the business motivation and strategic drivers that underlie your organization's migration to the cloud.

Over the years, IT has moved out of the backroom to support business growth. CIOs are now tasked with the directives to reduce costs, increase efficiencies and drive innovation, and the cloud is the catalyst for realizing these strategic advantages. However, successfully identifying and prioritizing the forces driving change are key to successfully executing a cloud strategy.

In PWC's 18th Annual Global CEO Survey, 82% of organizations worldwide name cloud technology as a key part of the IT strategy. To realize the cloud's full potential, IT leaders need to understand the common challenges driving cloud adoption. Now while there are many reasons an organization my move to the cloud, here are 6 common ones we've seen…

1. Lack of in-house IT expertise and resources

   There is a scarcity of expertise in cloud architecture, security, deployment and performance optimization. Most organizations lack the skills needed in-house to confidently move forward with their cloud initiatives.

   In a survey by Softchoice, a lack of the right skills led 34 percent of IT leaders to experience a cloud failure caused by their staff's action.

   Successful cloud deployments require the help of certified experts with advanced skills. To acquire these skills, the choices come down to training, hiring or outsourcing. External resources who can streamline operations, optimize performance and scalability, monitor and support applications, easily adapt to change and reduce the complexity of your cloud infrastructure, are often the most economical choice for not only the speed but also the success of your cloud migration.

2. Security and compliance concerns

   Every day we see a news of another organization who has been compromised, and this risk is the number one reason organizations delay their move to the cloud. The reality is that security in the cloud is not all that different than on-premises. To mitigate risk, organizations need to have a strategic plan that identifies where the risks lie and address how to protect sensitive data.

   Security policies and protocols should be set in place that addresses physical security, as well as cloud security, and includes encryption, backups and disaster recovery. It's important to find out how your cloud provider meets appropriate compliance mandates,

such as PCI-DSS and HIPAA, and check for certifications such as the ISO 27001. To understand the inherent risks, conduct tests to determine vulnerability points, apply controls and manage SLAs. And, most of all, remain vigilant.

3. Cost of aging infrastructure

An aging, on-premises infrastructure is expensive to upgrade and maintain, and a big reason behind the push to the cloud. However, before moving critical applications, it's important to understand how the move to the cloud will affect your operations. Gartner recommends analyzing total cost of ownership unique to your business, to segment the cloud use cases and look beyond cost issues alone. They also state that you should check with financial specialists to understand the implications of switching from a capital expenditure (CapEx) to operating expenditure (OpEx).

4. Private cloud challenges

Although there are numerous advantages to private cloud in reducing performance bottlenecks, simplifying management and maintaining a higher level of security and compliance, the upfront and implementation costs, can be much higher than expected. Considerations for resources that go unused and the complexities of managing the hybrid infrastructure make private cloud a candidate for third-party management with a vendor who has a deep understanding of the technical aspects of providing both private and public clouds.

5. Cloud Governance

Effective management of information security in the cloud is a key concern. As employees increasingly access cloud applications on non-approved devices, IT departments lose control over the cloud environment. To address shadow IT and prevent data loss, CIOs need to develop comprehensive procedures for approving cloud applications. Risk needs to be properly managed and balanced against the needs of the business and individuals who require cloud services.

6. Reliability and availability of services

Some businesses remain skeptical about whether the cloud will be able to run mission-critical applications with the reliability that is required. Organizations can proactively address this concern with strong SLAs and by defining application-specific performance needs ahead of time to optimize cloud deployments.

Cloud adoption is a critical business initiative. OneNeck IT Solutions is committed to helping our customers gain clarity from cloud complexity. We help our customers navigate the cloud to get the Right Application, on the Right Cloud, at Right Time! Whether your workload is best suited for a major public cloud, within a private cloud or even in a hybrid cloud solution, we can help you decide what option is best for your unique business.

City of Minneapolis

Keeping the City Running with Cloud and Managed Services from OneNeck

The Customer

Minneapolis is the largest municipality in Minnesota with more than 400,000 residents, forming half of the Twin Cities with the neighboring state capital, St. Paul. Minneapolis serves as a center of commerce for the region, including support for a large agricultural region with food processing, as well as manufacturing, computing and health services. Running the City's infrastructure requires a complex enterprise network with customized software for each government department and agency.

The Challenge

The City of Minneapolis had been working with their previous IT outsourcing partner for 13 years and desired to find a new managed services and outsourced IT partner to manage the City's IT infrastructure. In addition, the existing network infrastructure was aging, and the City needed an experienced IT services partner to provide cloud and managed services that encompassed server, storage, network, security, database, OS and data protection services. After issuing a comprehensive RFP for outsourced IT services, the City of Minneapolis selected OneNeck out of a field of 18 prospective partners to handle this comprehensive list of services.

The OneNeck® IT Solutions Answer

Because of OneNeck's comprehensive hybrid IT service offerings, OneNeck had all of the resources needed to manage the City of Minneapolis' computing infrastructure. As part of the contract, OneNeck would provide colocation services leveraging OneNeck's national footprint of highly-secure data centers it owns and operates. One data center was to host the City's production application environment, while disaster recovery for mission-critical and business-critical applications would be supported from another OneNeck data center.

OneNeck also was able to bring all the expertise required to maintain enterprise operations, including managed services for networking equipment such as routers, switches and firewalls across 70 locations. Data hosting using OneNeck's' ReliaCloud® infrastructure-as-a-service (IaaS) platform was able to support more than 250 servers with 180 terabytes of data, including dedicated servers for non-virtualized assets.

The OneNeck team also brought the expertise to transition and upgrade critical components the City's PeopleSoft environment to support human resources and finance. Migration included transitioning and supporting hundreds of applications for specific city services, such as waste management, land management, parks and recreation and more.

WATCH

Video Case Study

Des Moines Orthopaedic Surgeons (DMOS) Realizes Cost Savings with ReliaCloud

When DMOS made the decision to move their critical data to the cloud, they partnered with OneNeck to make it happen.

Watch Now

Like any IT transformation, there were bumps along the way that the City and OneNeck worked through together. Since the existing contract was still in place when the new contract was signed, the OneNeck team was unable to gain access to the computing environment prior to the hand-off. There was no way to perform an initial assessment. However, when the contract did expire, OneNeck was able to work with the installed systems and initiate the migration without any real problems.

Part of the reason for the success was the ongoing communications between the OneNeck team and the City's IT team. From the first day the contract was signed, the City demonstrated their eagerness to forge a partnership and committed their time and resources to the project. To ensure success, the OneNeck project team and the City's IT group met twice each day to plan and assess progress.

As the OneNeck team moved through each phase of the project, they encountered a few surprises. For example, they discovered that most of the installed enterprise systems were at the end of their lifespan. There was no alternative but to take the outdated systems and make sure they continued to work; letting the system go down was not an option.

The biggest surprise came with the implementation of the Criminal Justice Information System (CJIS). Before work could begin on the CJIS project, the entire OneNeck Operational Support team, more than 100 professionals, had to be screened for security clearance, including fingerprinting and background checks. However, OneNeck worked closely with the City to satisfy all of the City's security and compliance requirements, even though it impacted progress on the overall transition project with the City.

The Benefits

Despite these challenges, the OneNeck team was able to complete Phase 1 of the project on time and within budget. Some of the IT environments were even ahead of schedule.

OneNeck was able to scale the capacity of the ReliaCloud environment quickly to accommodate 70 separate locations and 3,500 users with more than 250 servers and 180 terabytes. Much of the first six months of the project included migrating data and workloads from the existing service provider's data center to ReliaCloud.

As the relationship evolves, the City of Minneapolis will continue to look to OneNeck as a strategic service provider. OneNeck continues to supplement the City's team with diverse expertise, across many technologies, bringing solutions and resources as needed, even outside the originally contracted services.

The City is already seeing on-going benefits as they are more flexible and more responsive to stakeholders needs. City administrators expect to save more than $3 million annually with OneNeck, and as new upgrades and applications are needed as part of organic growth, the City will continue to benefit from OneNeck's versatility and ability to plan and manage a dynamic IT infrastructure.

Reigning in the Cloud with Governance

Today, more than 40 percent of all enterprise workloads run in the cloud. According to 451 Research, this will likely jump to 60 percent by mid-2018. As the use of multi-cloud environments continues growing, the task of ensuring all the varied workloads remain secure and compliant is no easy feat. This is especially true when business units move workloads to the cloud without the knowledge or approval of IT.

Enter: Cloud Governance.

Like government, the word governance originates from the Greek verb κυβερνάω, which means to steer. It relates to decisions that define expectations, grant power or verify performance. In cloud governance, enterprises apply specific policies or principles to the use of cloud computing services with the goal of securing all remote applications and data. Tech Target writes that governance of cloud services can be viewed as an extension of service-oriented architecture governance, although the unique properties of a public cloud architecture, such as multi-tenancy, present slightly different concerns.

What makes cloud governance so extremely challenging? It's because cloud workloads:

- Lack accountability. Enterprises are often uncertain just who is responsible for safeguarding the sensitive data stored in the cloud, making it difficult to determine

if proper security and data privacy policies are in place and enforced.

- Need security. You can't govern what you don't see. When IT is not involved in reviewing a cloud provider's security — or are unaware of all the cloud applications, platforms or infrastructure services in use across the enterprise — they are unable to confidently manage risk.
- Sidestep compliance. Cloud governance is not only a security issue, but a compliance issue as well. Cloud applications are often used without IT having conducted proper training on cloud security, policies and procedures. If IT doesn't have control over how employees or third parties access and handle sensitive workloads in the cloud, meeting privacy standards and compliance regulations is very difficult.

Strong cloud governance is essential for ensuring the right cloud security policies are in place, and most importantly, are followed across the enterprise. Even if you feel you have a sound security strategy, without cloud governance, your organization is at risk for data theft, loss or exposure.

Cloud governance should be implemented at three layers:

1. Service level governance (also known as API-level governance): Employees attempting to gain access to cloud services must first pass through a centralized access point to confirm user authorization. This ensures that only users with permission to access a particular cloud service are allowed.
2. Data level governance: Enforce controls at the data level to meet data privacy requirements and ensure the availability, integrity and overall security of your data in different cloud models, including public and private. Only those employees with the right access, authorization and permissions should have access to sensitive data stored in the cloud.
3. Platform level governance: To avoid overpaying for subscription-based services while ensuring a single point of control for complex, distributed clouds, set policies that specify cloud providers use automation and proper controls to optimize provisioning and de-provisioning of cloud resources.

One final consideration that cannot be overlooked is the exit strategy. Despite the fact that the cloud is a great fit for many of today's workloads — it's not a fit for every workload. When you determine the problem isn't just a provider who's not a good fit, you'll have to plan a retreat. Therefore, an exit strategy is imperative.

With the right governance strategy in place, cloud-based workloads can be as secure and compliant (in some cases, more so) than on-premises. With a strong cloud partner who has the expertise and technical acumen, you'll be ready to take on the complexity and positioned to successfully govern your cloud environment.

Hybrid Cloud Risks that Businesses Must Manage

In theory, hybrid cloud encompasses the best of both worlds - the flexibility of public cloud fused with the privacy and security of private cloud. That sounds like an amazing concept, but in practice there are still many cloud-resistant applications and services.

Should your enterprise be investing in a hybrid cloud infrastructure?

According to Gartner analyst, Lydia Leong, private cloud innovation is falling behind the pubic cloud making it difficult for private clouds to match the efficiency and capabilities of the public cloud. For most organizations who are not at a large scale and don't have a custom-tailored use case, Leong believes private cloud just doesn't make sense.

That being said, hybrid cloud initiatives are not dead. According to the RightScale 2016 State of the Cloud Report, private cloud adoption increased from 63 percent to 77 percent, driving hybrid cloud adoption up from 58 percent to 71 percent year-over-year.

Key areas that businesses must take particular care to address when making the transition to a hybrid cloud system include:

- IT Architecture. A hybrid cloud is highly sophisticated and consists of a woven architecture of public and private cloud. IT staff need to have an expert-level understanding of how this complex platform operates. More often than not, such a high level of expertise needs to be acquired through third-party services.
- Bandwidth and Latency. Cloud access via private network provides enhanced security, but this often also means increased latency, especially when it comes to bulk data transfers and real-time data streams.
- Disaster Recovery. Disaster Recovery (DR) is a critical

issue, and not all cloud providers are created equal. The number of data centers a cloud provider uses can determine the level of DR they are capable of, and a complete failover plan is a must. In addition, if your cloud provider does not own the physical space of the data center, there could be business continuity and legal ramifications to consider.

- Security. In an on-premises data center, mobile security, network security and privacy are all under the control of the corporate IT department. When data is stored in the cloud, IT does not have the same level of control. Encryption is a requirement for transfer of data in a hybrid cloud infrastructure. Your cloud providers choice of encryption can raise security and compatibility issues that you will need to address.

Hybrid IT vs. Hybrid Cloud

The answer could lie not in a hybrid cloud model, but rather in hybrid IT. Hybrid IT is essentially a non-cloud IT infrastructure that operates in tandem with a public cloud. The thought is that gradually, the IT infrastructure would migrate to the public cloud as innovation makes the public cloud a more viable and safe platform for more workloads.

It may be true that some applications will never make sense to move to the cloud, and not all virtualized infrastructure is classified as cloud. A hybrid IT model allows organizations to continue to run their legacy systems built on existing architecture. This model can be less expensive than pushing towards a private cloud and rearchitecting applications to operate on a new infrastructure.

The practice of colocating enterprise data centers alongside high-speed connections to major public cloud platforms is one way in which the hybrid IT model can play out. Laurent Lachal, Ovum's senior analyst for infrastructure solutions stated, "There's a whole infrastructure being created and an increasing connection between the colocation providers of the world and cloud providers."

Before deciding which way to go, Gartner's Leong recommends that organizations first decide on what type of IT will best meet the needs of the business. For smaller companies, a hybrid IT solution may be the more budget-friendly option. Organizations can always migrate to a public, private or hybrid cloud later, based on ongoing needs.

Hybrid Cloud vs. Multi-Cloud: What's the Difference?

In today's digital world, terms like "hybrid cloud" and "multi-cloud" are thrown around interchangeably. But there is a difference, and understanding it is key to getting the most out of your cloud strategy.

Gartner has predicted that by 2020, a corporate "no cloud" policy will be as rare as a "no Internet" policy is today. Similarly, IDC predicts that, by 2020, 67% of enterprise IT infrastructure and software will be cloud-based offerings.

Both hybrid and multi-cloud solutions have their use cases, but a new breed of applications and services is driving the need for highly flexible service delivery, pushing multi-cloud to the forefront of today's cloud conversations. But which approach is most appropriate for your unique needs?

So, What's the Difference?

TechTarget defines hybrid cloud as a cloud computing environment that uses a mix of an on-premises, private cloud and a third-party, public cloud, with orchestration between the two. The intent is to enable the flexible deployment of workloads, applications and data across private and public clouds.

On the other hand, multi-cloud refers to a combination of multiple public cloud services and providers. These aren't necessarily managed through orchestration software and could very well be separate deployments where never the twain shall meet.

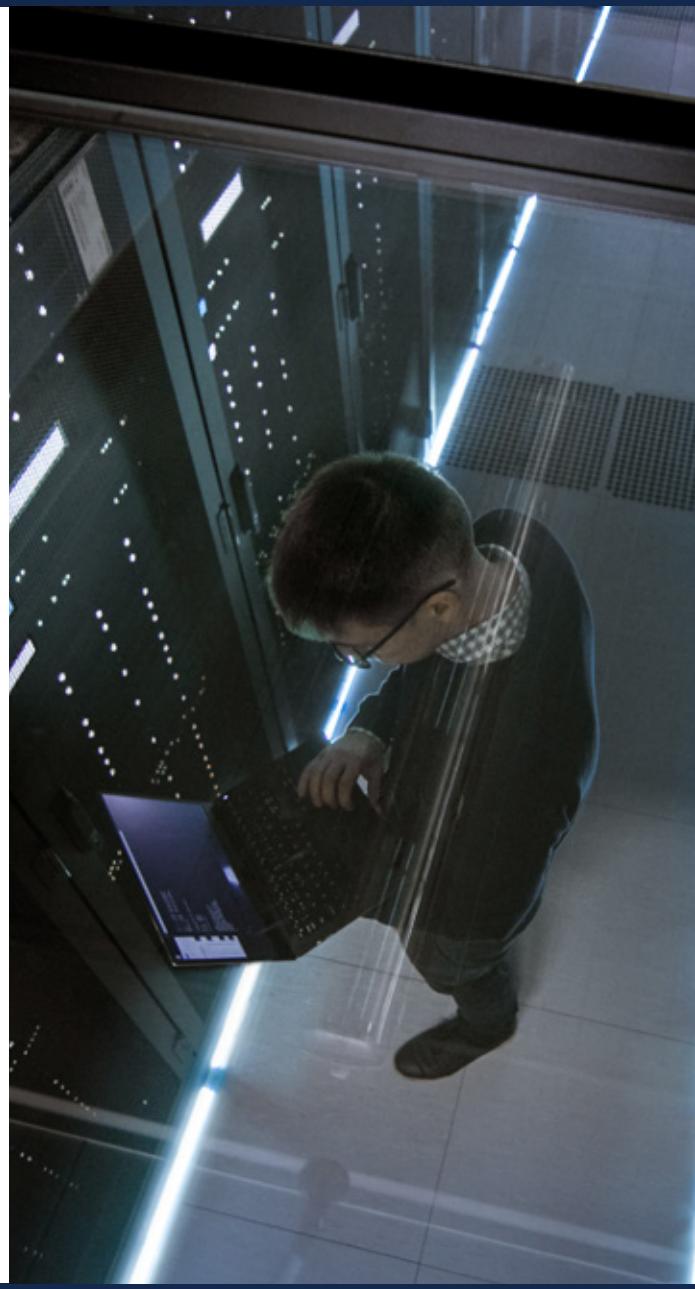
When Does a Hybrid Approach Make Sense?

While there are still many misconceptions around hybrid cloud, hybrid cloud deployments are frequently found in large enterprises with significant investments in IT infrastructure and large, skilled IT teams. This approach provides the flexibility to leverage the existing IT infrastructure to test a cloud deployment without the risk of making a full switch.

The approach is ideal for organizations that already have a virtualized environment. It allows for a slow migration to the cloud by retiring old equipment as it reaches end-of-life and using an orchestration solution to switch virtualized workloads.

But... Multi-Cloud Sounds Good Too.

It's hard to argue with one of the big benefits of multi-cloud – CHOICE. The ability to operate from anywhere and move and deploy workloads to any cloud brings a plethora of options to a cloud strategy. You don't have to change your business



requirements to fit a specific provider's processes, but multi-cloud allows you to shop around and find a provider that matches each part of your business.

One of the big benefits of a multi-cloud approach is the risk of being locked into a single cloud provider can be avoided. If you're not housing all your data, apps and workloads with a single cloud vendor, you're not at the mercy of that provider's pricing and exit fees, or should you outgrow them, you're not locked into just their cloud.

Additionally, we all acknowledge the reduced capital expenses that cloud offers, but downtime can be extremely costly to the bottom line. This is where finding the right cloud provider for specific areas of your business can help alleviate costly downtime – cloud provider services can vary, so the right combination of providers can be the ideal mix for your business needs, not to mention that in the case a provider fails, you're not locked into just one cloud.

Businesses that are less locked down in terms of technology have more freedom to rapidly grow (and shrink) technology services in alignment with business need. Those businesses will have a lot more options and flexibility. This is perhaps the most compelling business case for a multi-cloud environment which incorporates multiple cloud vendors.

Is Hybrid Cloud or Multi-Cloud Right for You?

To create innovative solutions that grab and keep the attention of their customers, businesses must innovate quickly and cost-effectively. This new economy rewards those who can move quickly. So, it's no surprise IDC projects that, by 2018, 85% of enterprises will be pursuing a MultiCloud strategy. Yet, according to a 2016 Business Cloud News Report, 57% of all organizations do not have a multi-cloud strategy whatsoever.

Success in a multi-cloud approach requires strategic planning to manage risk and match applications and workloads to the cloud service that fits best in terms of service, pricing, infrastructure and connectivity.

But ultimately, for some organizations it's a combination of hybrid and multi-cloud that offers true flexibility in terms of cost, resilience and elasticity – especially for enterprises with existing on-premise data centers or private-cloud deployments. There is no "one size fits all" in a multi-cloud world, so no need to force-fit your workloads into one cloud. After all, your cloud starts with YOU.

(855) ONE-NECK

www.OneNeck.com

OneNeck®
IT SOLUTIONS
a TDS® Company