Find Your Cloud 9
Strategies to help you find your silver lining in the cloud

You’re tasked to drive innovation—from building a virtual environment to increasing operational efficiencies to designing a comprehensive security posture. Yet financial pressures persist; budgets go down, rarely up, and you are told to do more with less.

Even more critical, IT not only needs to align with the business but must become the business—delivering its customers solutions to get their jobs done quickly, easily, and cost-effectively.

It’s no wonder why many CIOs are searching for that silver lining in the cloud. Cloud computing aims to increase business agility, accelerate innovation, and improve effectiveness of the workforce, all while reducing cost.

Despite the advantages, concerns over reliability, security, availability, and performance still cloud their thinking on whether to leverage this dynamic environment.

To gain a better understanding of what factors are driving many organizations to implement cloud solutions and to provide recommendations on how organizations can prepare for the cloud, CIO Digest spoke with a leading industry analyst and key IT decision makers.
IT as a service

The first thing organizations need to consider as they look to the cloud is which approach they want to take and the considerations for each. And it’s not only about the science of how to adopt cloud technologies. It’s the art of thinking differently. “Delivering cloud services is essentially a cultural change, including people and processes—to deliver IT as a service-centric approach that enables the business,” says David Bradshaw, research manager at International Data Corporation (IDC) EMEA. “The ability to offer cloud services—sourced externally or internally—is something IT must have as a weapon in their toolkit for getting things done in a cost-effective and flexible manner to meet customer needs.”

In general, there are three cloud adoption models that are proving successful for businesses today. Computing power provided by well-known vendors such as Amazon.com, Salesforce.com, Symantec, and others in the form of a public cloud. The different types of pay-per-use service offerings include—software (SaaS), platform (PaaS), and infrastructure (IaaS)—delivered over the Internet.

An alternative is to build a private cloud infrastructure that offers the benefits of a public cloud while allowing the business to maintain ownership of its data and equipment. IT is the service provider; internal infrastructure is shared across departments with the objective of standardizing IT services.

Lastly, IT environments are becoming more complex with their mix of legacy physical systems, next-generation virtual assets, and cloud-based services. Under this scenario, organizations work in a hybrid cloud environment—multiple cloud systems that are connected in a way that allows processes and data to be moved easily from one deployment system to another. An example would be online backup where data is local and in the cloud.

These cloud deployment models all share common attributes such as shared infrastructure, multitenancy, Web services, elastic scale-up/scale-down capabilities, metering, pay for only what you need, and self-service.

What to host in the cloud

The ability to respond to business demands on the fly while containing cost are key drivers for the cloud. But how do businesses determine what applications or services to manage on premise or in the cloud?

“Organizations considering cloud services must first ask key questions around business strategy,” Bradshaw explains. For example: “What is their core competency? Do they need to own the technologies or run the services in house to benefit from those core differentiators? Can the business requirements be met with the cloud service?”

From the IT strategy point of view, IT should look at what IT assets are coming up for renewal. Could non-core services such as messaging security or payroll services be more efficient, secure, and cost-effective if hosted in the cloud versus on premise? Is IT better off having someone else run those processes so they can concentrate on what really makes a difference?

In short, before heading into the cloud, organizations should address what services should be placed where and why and does it match with the business strategy, is it safe and secure, and does it deliver value for the money?

Meeting business needs is the real driver behind implementing a private cloud.”

– Ismael Moreno, IT Manager, SESCAM

“Meeting business needs is the real driver behind implementing a private cloud.”

– Ismael Moreno, IT Manager, SESCAM
Cloud performance
As IT departments extend into cloud services, they need to address the complexity of monitoring, alerting, and reporting on information and infrastructure assets across physical, virtual, and cloud platforms.

Key indicators for measuring the return on cloud computing include lower and controlled cost, the ability to rapidly scale up and down, elastic provisioning, enhanced asset utilization, risk and compliance improvements, speed in the delivery of new applications, and enhanced service levels. “The ability to design a platform that best meets the needs of the business is the overall benefit of cloud computing,” Bradshaw says.

Who are you going to call?
A public cloud is a way to increase capacity to meet business needs, without investing in new infrastructure.

Today, more and more businesses are receptive to consuming cloud-based solutions. This is good news for cloud veterans Aprimo, Inc. and LivePerson that have each been in the cloud services space for over 15 years.

Aprimo delivers Integrated Marketing Management services to both BtoB and BtoC marketers. “Marketing is open to services in the cloud, but quality and security of information remains a key concern for IT,” says Darren Del Duco, vice president of Cloud Services Infrastructure Engineering at Aprimo. To ensure service quality, Aprimo maintains stringent service level agreements (SLAs) both with its customers and internally. “We are able to provide a measurable ROI and a track record of availability to mitigate concerns, which enables marketing to focus on their business and deliver greater efficiencies,” Del Duco explains.

The largest provider of real-time customer engagement, LivePerson, hosts over 13 million chats per month. “We work with both the business and IT to help customers identify their requirements and any potential risks to ensure the right controls are put in place,” states Guy Bejerano, chief security officer at LivePerson. “Then, we make sure we deploy a secure solution for them.”

“In effect, IT is delegating responsibilities to an outside vendor that can provide resources on demand,” Bradshaw notes.

These are some key considerations when evaluating public cloud service providers:

1. **Reputation.** Research how long a vendor has been in business and ask for references on how the vendor is performing.

2. **Security standards and checkpoints.** Understand how secure your data needs to be and ask the vendor how they address security issues and potential breaches.

3. **Backing up and moving data.** Investigate how the cloud provider makes backup copies of your data and how easily you can move data to another vendor or your environment, or move data between on-premise and cloud-based environments.

4. **SLAs.** Work hard to get a good SLA with clear financial penalties to ensure good service. Both the business and IT should be involved in negotiating and then enforcing these.

5. **Try before you buy.** The benefit of cloud computing is that it’s easy to switch on and off. Start with a proof of concept; begin with a small deployment and then expand.

Secure cloud cover
“Implementing cloud services does not necessarily bring about new challenges,” Bradshaw states. “What it does is recontextualize many existing ones.” Security
continues to be an issue in any IT landscape.
To ensure you have the right security controls in place, you need to categorize your processes and data—some of which will be business and security critical. Using the security policies established as a guide, you could then determine the most appropriate way to source them, according to Bradshaw.

Malware and spam blocked from the cloud
“Security is an area where organizations should leverage the cloud and the experts in the field,” Bradshaw notes. “Why not filter out attacks in the cloud before they hit your network and servers?”

Like many healthcare providers, security is a top priority for Lake Health, Inc., which must protect its two hospitals and 14 medical facilities and physician offices that span across three counties in Ohio.

“IT should not be an obstacle to innovation or workflow,” states Keith Duemling, information security officer at Lake Health. “So we leverage advanced technologies that will help drive increased efficiency and deliver high quality service to the organization.”

To ensure patient information is protected and compliant with industry regulations, Lake Health re-evaluated its messaging security solution. The previous solution required four to eight hours of IT staff time per week on average to maintain against incoming spam and malware. As a result, Lake Health went from an on-premise email gateway to a cloud-based messaging security environment based on Symantec Email Security.cloud.

“With Email Security.cloud, we’ve had no disruptions from email-borne threats, and it captures in excess of 99 percent of incoming spam messages,” Duemling notes. “And since the solution is hosted, we didn’t need to build out—and then main-

Reduction in pipe consumption and an almost 75 percent decrease in help desk volumes both due to email, saving help desk staff around eight hours per week on average,” Duemling observes. “And with less spam getting through

“We work with both the business and IT to help customers identify their requirements.”

– Guy Bejerano, Chief Security Officer, LivePerson

Vital stats speak for themselves
A key differentiator for Lake Health was the aggressive SLAs Symantec.cloud provides, including 100 percent protection against viruses. In addition to providing 100 percent uptime and improved network bandwidth, Symantec Email Security.cloud reduced IT staff time spent weeding through unsolicited mail and help desk tickets.

“Since moving to Email Security.cloud, we’ve seen a 50 percent reduction in pipe consumption and an almost 75 percent decrease in help desk volumes both due to email, saving help desk staff around eight hours per week on average,” Duemling observes. “And with less spam getting through
our organization,” Duemling says. “This will save IT staff a projected 16 hours per month.”

Backup you can count on
Another concern for customers is how their corporate data will be backed up and protected in the cloud. To monitor data protection and quickly recover critical information—including both physical and virtual servers—Lake Health also uses Symantec Backup Exec and Symantec System Recovery. The healthcare provider uses VMware and Citrix XenServer for server virtualization.

Aprimo also needed to protect an increasing amount of customer data while scaling in a cost-effective manner. Aprimo migrated from a local storage platform using Symantec Backup Exec to a storage area network VMware-based environment that relies on Symantec NetBackup for data protection. As part of this process, Aprimo consolidated over 300 physical servers onto six hosts that now accommodate 800 virtual machines.

“We needed a solution that could confidently back up, recover, archive, and discover information, whether it’s on premise or in the cloud,” Del Duco says. “NetBackup capabilities enable us to provide more value to our customers by offering comprehensive data protection instead of charging a single fee for storage, disk space, disaster recovery, backup, and data transfer.”

Build the cloud and they will come
The goal of deploying a private cloud is to make the IT environment more effective and efficient while increasing utilization of the assets such as servers and storage systems. “One of the requirements for a private cloud is a large-scale environment that’s shared,” Bradshaw says. “This allows IT to get the economies of scale for significant cost savings.”

In addition to the fundamentals of having a standardized, scalable, and secure physical infrastructure, a core component to building a private cloud involves virtualization—including virtual compute and storage resources. Thus, private cloud deployments are a balancing act between supporting existing infrastructure and moving to extend to a virtual environment in a way that automates the provisioning of IT services.

Achieving balance
Servicio de Salud de Castilla-La Mancha (SESCAM), a healthcare provider in Spain, understands what a delicate balance it is to do more with less, while providing 24×7 quality patient care for its two million patients. SESCAM determined a private cloud infrastructure was the best approach to achieve this balance.

“More than ever, IT strategies must align with business requirements,” says Ismael Moreno Fernandez, IT manager, at SESCAM. “Meeting business needs is the real driver behind the implementation of our private cloud.”

A key obstacle was the support for multiple platforms and systems without changing the underlying infrastructure. The next focus was on data center consolidation and virtualization.

To facilitate a seamless migration across its physical and virtual platforms, SESCAM standardized on a series of Symantec storage and availability management technologies, in addition to Symantec Endpoint Protection. The intent was to not only enhance virtualization but also support the organization’s cloud strategy.

As part of the move to a private cloud, SESCAM began migrating from a UNIX to a Red Hat Enterprise Linux platform, running on Cisco servers using VMware vSphere for...
virtualization management. The migration from the physical environment is expected to be rapid. Moreno anticipates 70 percent virtualization on the organization’s 800 servers to be achieved by next year-end.

A private cloud deployment also includes virtualized storage resources to support storage-related workloads such as backup and storage on demand. For SESCAM, a vital component was the ability to leverage technologies that would support its disparate infrastructure and minimize the complexity of managing data throughout the IT environment.

According to Moreno, features like deduplication, compression, and storage tiering in Veritas Storage Foundation 6 from Symantec will help SESCAM maximize its storage efficiency without impacting the application availability. And the ability to further leverage Veritas Cluster Server and Veritas Dynamic Multi-Pathing helped increase performance and high availability of systems, thereby resulting in lower cost. “We also needed a backup solution to help facilitate the move to the cloud,” Moreno states. “Symantec NetBackup improved the migration of all our systems by minimizing risk, and it provides a consolidated view across our physical, virtual, and cloud environments.”

“Symantec technologies support our private cloud strategy, giving us the ability to deploy IT services faster—from months to days and at a lower cost and maintain aggressive SLAs for our internal clients,” Moreno adds.

Scale big or go home
Hosting more than 1.3 billion consumer website visits each month, LivePerson understands how to scale big. “Being able to withstand the high seasons such as Cyber Monday is critical to our business and our customers,” states Gonen Wilf, head of production at LivePerson. “We need to be able to deploy rapidly when a customer needs more capacity and have the flexibility to scale down, which provides our customers with a scalable pricing model.”

LivePerson has a heterogeneous IT environment with over 1,000 servers spread over four data centers in different regions. As 24×7 availability is a business requirement, LivePerson leverages Veritas Cluster Server as part of a larger set of availability toolsets. “Veritas Cluster Server gives us a proven solution that meets our business-critical requirements around availability,” Wilf notes. “It provides us with the confidence that we can deliver on our SLAs for customers.”

Data protection in a hybrid world
Lake Health’s IT landscape operates in a hybrid cloud environment. With over 3,000 medical and clinical staff who share patient information between themselves, Lake Health built multiple layers of protection using Symantec products.

To increase visibility into their security posture and secure endpoints across its physical, virtual, and cloud environments, Lake Health uses Symantec Endpoint Protection and Symantec Endpoint Encryption. Altiris Client Management Suite is replacing Symantec Ghost Solution Suite to be used for imaging new systems and re-imaging damaged systems.

“We’re able to leverage Symantec products on both the physical and virtual side, and in the cloud,” Duemling states. “Symantec solutions have helped us achieve our goal in enabling Lake Health to deliver quality patient care.”

SESCAM not only built a private cloud, but also operates in a hybrid cloud landscape. To gain more visibility in securing endpoints and reduce risk of data breaches, SESCAM uses Symantec Endpoint Protection and PGP Universal Email Gateway. “Symantec Endpoint Protection helps us protect both physical and virtual servers, while PGP helps us maintain high level patient privacy,” Moreno explains.

The silver lining
Regardless of where you are on your cloud journey, it’s important to understand cloud computing risks and benefits, whether it’s consuming cloud-based services, building a private cloud, or working in a hybrid cloud environment. SESCAM’s Moreno offers this advice: “Like any new IT strategy, there will be risks and benefits; review these with everyone in your organization. Look at the cloud as a transformational model, with IT as the facilitator in defining better business requirements and services for the organization. And if you rely on companies who deliver proven virtualization and cloud-based technologies, you can reduce risk and complexity in addressing data protection and information security in the cloud.”

Courtenay Troxel is the manager of online content and customer newsletters at Symantec and a managing editor for CIO Digest.

Lake Health Security Stats
> 100% of email-borne malware blocked
> 100% availability of messaging security system
> Up to 75% fewer helpdesk calls related to messaging security
> 40 hours/month saved on imaging new and re-imaging existing systems
> 50% less network bandwidth consumed by messaging system
> 99% of incoming spam messages captured