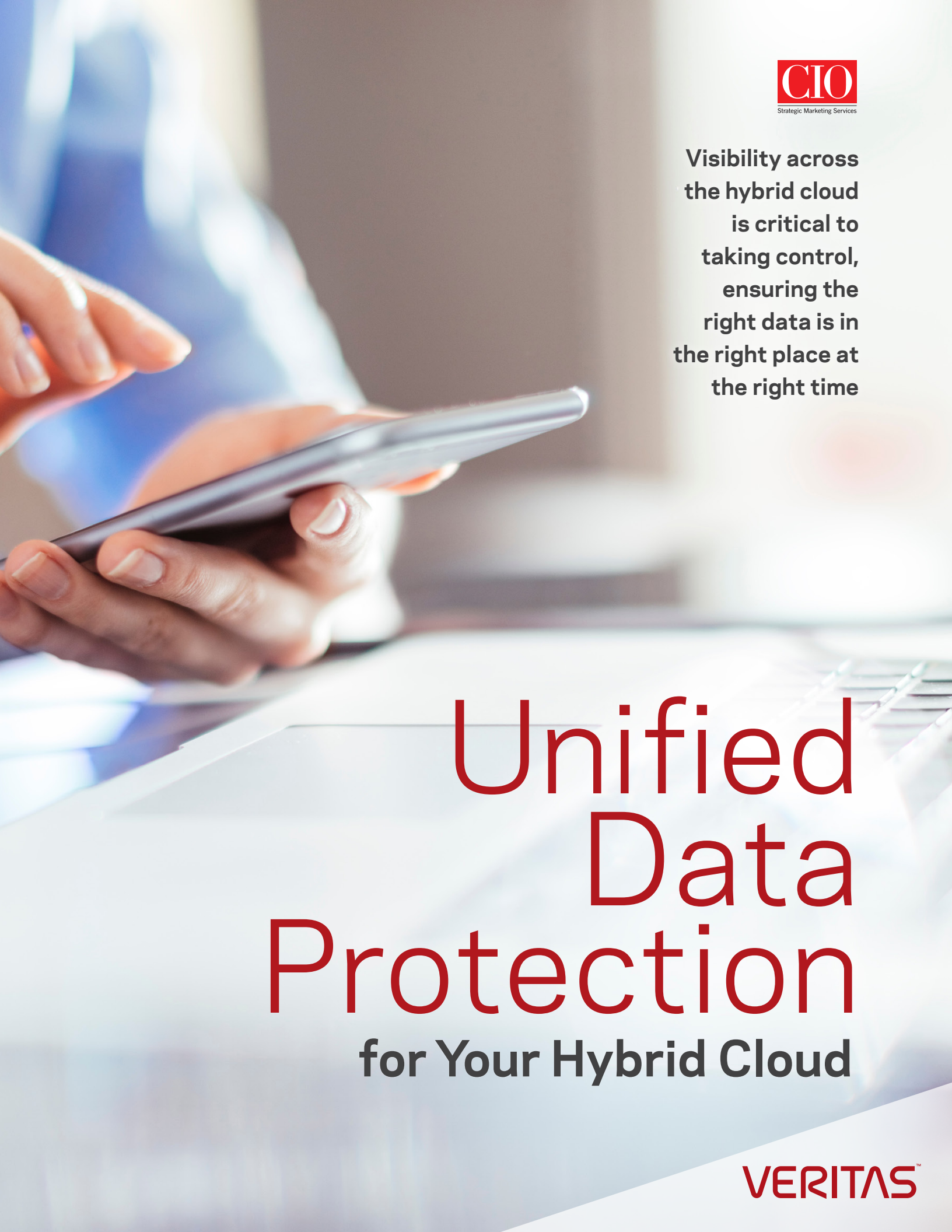


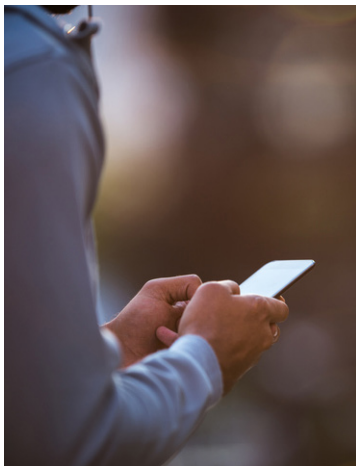
CIO
Strategic Marketing Services

**Visibility across the hybrid cloud is critical to taking control, ensuring the right data is in the right place at the right time**

# Unified Data Protection

## for Your Hybrid Cloud

VERITAS™



**IT leaders must play a critical role in enabling those strategies by supporting new initiatives that utilize new data types, particularly unstructured data from sources such as social media and Internet-of-Things devices.**

DATA-DRIVEN STRATEGIES are critical to the success of today's businesses. IT leaders must play a critical role in enabling those strategies by supporting new initiatives that utilize new data types, particularly unstructured data from sources such as social media and Internet-of-Things devices.

In this pursuit, IT leaders have embraced cloud services of all kinds from a wide variety of providers. The scalability and flexibility of the cloud make it easy to add applications, services, and infrastructure quickly to meet digital business needs as they arise. According to a recent Veritas global survey of IT decision makers, 74% of enterprises use multiple cloud vendors, while 23% use four or more.[1] And the report predicts the number of business-critical workloads in the public cloud to double in the next two years.

Although mission-critical applications like CRM and ERP are increasingly moving to the public cloud, on-premises IT infrastructure in the form of private clouds will continue to play an important role. The resulting hybrid clouds present unique management challenges, particularly with regard to data protection.

"IT environments are fragmenting across public and private clouds, and that is causing issues with data visibility -- the ability of administrators to see what data is located where," says Arjan van Proosdij, Global Solutions Marketing Lead at Veritas Technologies.

The stakes are high: Failure to address data protection effectively across the hybrid cloud will impede the ability of an organization to move quickly to advance data-driven strategies while keeping costs under control.

## Data protection challenges: Multiple locations, ROT, and 'dark data'

To understand the challenges of data protection across the hybrid cloud, it's important to consider what data is stored where. When a cloud service is used, data sent to the cloud may be stored in different cloud data centers in different locations, possibly in different countries.

The proliferation of data of different types creates special challenges. The vast majority of data stored by organizations is not mission-critical. Organizations must winnow data carefully to avoid discarding data of value, but (equally important) to avoid drowning in a sea of useless data. Another recent Veritas survey revealed some telling findings with regard to corporate data:

- Only 15% of data is mission-critical
- 33% of data is redundant, obsolete, or trivial (ROT)
- 52% of data is "dark data," the value of which has not been identified and may include business-critical data as well as ROT data.[2]

Further complicating matters, many organizations have deployed disparate data management and data protection tools in distinct silos across on-premises and public-cloud environments.

1 "State of the Hybrid Cloud Research Report," conducted for Veritas by Cicero Group, January 2016.

2 "The Global Databerg Report," conducted for Veritas by Vanson Bourne, March 2016.

**The proliferation of data across hybrid clouds calls for a new approach to data protection.**

## Sky reaches for higher level of data protection

Sky, a leading entertainment provider headquartered in London, had long relied on tape backup. That changed in 2012, when the company, which serves 22 million customers in several European countries, decided the time had come to move to disk-based backup to improve recovery times and reduce costs.

"Our new primary backup method needed to be expandable and adaptable with effective deduplication," says David Kerr, Storage Backup and Support Manager at Sky.

Already a user of Veritas NetBackup, Sky chose to deploy Veritas NetBackup ™ Appliances with Veritas™ Information Map. The phased implementation of 34 appliances has made significant inroads in reducing ROT.

"We see deduplication rates of up to 90% on the dashboards. Without deduplication rates like this, disk-to-disk backups are not viable," Kerr says.

Sky managers use Information Map to understand the nature of their unstructured data. Utilizing the metadata collected directly from the NetBackup catalogue, Sky administrators can identify valuable data, data that poses risks, and ROT data, and then make decisions that optimize data storage, reduce risks, and cut costs.

"Very quickly, Veritas Information Map gave us a fantastic, graphical view of our file system backups," says Kerr. "What we call our unstructured data could be accessed by age and business relevance. We're able to make informed decisions regarding how we store our data, and have been able to save on storage and backup resources."

Sky has cut backup administration time by 73%, which frees up staff to focus on higher value tasks, according to Kerr. Sky has also seen a drop in support calls, even while delivering 24x7 support.

"At Sky, Veritas Information Map allowed us to quickly identify opportunities to increase efficiencies," Kerr says.

"Acquiring a number of different data protection prodoucts will make management of data protection more complex and less efficient," Van Proosdij says.

Organizations also face a daunting task in managing personally identifiable information (PII) across international boundaries. The upcoming General Data Protection Regulation (GDPR) adopted by the European Union, as well as ISO 27018, which is being adopted by public cloud services, call for strict management practices over PII, especially with regard to where and how long data is stored.

## It starts with global data visibility

Gaining global data visibility — the ability to identify data according to type, importance, and storage location — is the first step toward more efficient storage. Visibility in turn enables data classification. The ability to classify and map all data visually allows administrators to quickly and easily identify essential and inessential data. After ROT data is identified and eliminated, the optimal storage location, whether on-premises or in the cloud, can be determined for the remaining data.

**The first challenge that many IT leaders may encounter as they proceed down this path is the traditional belief that backup is not an urgent priority.**

One widespread problem at many organizations is the proliferation of employees' private data, including personal photos and videos, across the corporate storage infrastructure. Such data, of course, does not qualify for corporate backup. By classifying data and then setting and following strict policies, organizations can remove large quantities of employees' private data from the backup schedule, so that only the data that is essential to the corporate mission is backed up.

Classification also provides a guide to data that can be moved to the cloud. For example, data governance policies might prohibit the storing of personally identifiable information off site. However, data that's not critical but important enough to retain might be ideally stored in a cloud environment. Further, deleting non-essential data from cloud storage and applying deduplication can create significant economies.

"Instead of storing 5 terabytes of data in the cloud, let's say you store only 2 terabytes. That not only can save a significant amount on your monthly cloud bills, it also optimizes your backup process," explains van Proosdij.

## A new approach: unified data protection

The proliferation of data across hybrid clouds and an increased level of regulation call for a new approach to data protection. Traditional backup and recovery must evolve to unified data protection across the physical and virtualized infrastructure of the hybrid cloud. An effective unified data protection solution identifies what data is stored where, and what data needs to be recovered quickly. This kind of solution provides a foundation for fully proactive enterprise data management, which will enable an organization to be agile in its protection, preservation, and delivery of business services.

The first challenge that many IT leaders may encounter as they proceed down this path is the traditional belief that backup is not an urgent priority. With battles being fought over increasingly scarce IT dollars, and the push to launch new data-driven business initiatives, it is too easy for many IT leaders to push backup toward the bottom of the priority list.

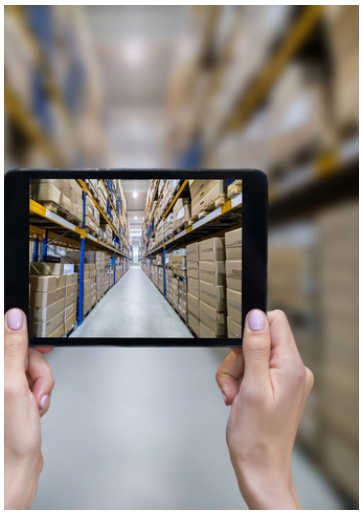
In addition, when new cloud applications are launched, low priority is often placed on backup. Although this practice may not create immediate problems, as applications become mission-critical, backup becomes equally critical. However, it is seldom easy to "bolt on" backup after an application has been up and running for some time. Because of these tendencies, strong leadership is important to give high priority to data protection, and to establish and adhere to policies so the correct protection level is applied to different types of data.

## The goal: predictable resiliency

To gain maximum benefit from the cloud, administrators should be able to enforce policies and move workloads as well as backups between public and private clouds managed from a single console. Using cloud-based services for data protection enables organizations to save the cost of building their own backup infrastructure. The goal should be for cloud-based applications to experience the same enterprise-level data protection as local servers and data, and to be able to recover just as quickly.

## Avoiding copy data sprawl

A significant best practice is to establish copy data management processes that are integrated with the overall unified data protection strategy. In many organizations, data is copied for a variety of purposes, particularly for application test and development. But too many copies can lead to copy data sprawl, unnecessary data storage costs, and security risks.



**Unbridled proliferation of data copies is prevented, along with significant waste of storage resources, especially when such copy data is backed up.**

## Veritas 360 Data Management

Veritas delivers a full spectrum of solutions for managing and protecting data across hybrid clouds, including:

- Backup and recovery
- Business continuity and availability
- Storage management, including software-defined storage
- Information governance
- Integrated copy data management

Veritas NetBackup gives administrators visibility across all applications, data types, and locations from a single pane of glass, whether the data is in a public or private cloud. Integration between Veritas NetBackup and Veritas Information Map enables administrators to:

- Prioritize the data that needs to be on performance-optimized local storage for fast recovery.
- Decide what data can be moved offsite to more cost-effective cloud storage for disaster recovery.
- Identify cold data that is a candidate for archiving to achieve compliance.
- Dispose of ROT data to free up storage space.

Veritas Velocity is a data virtualizaion appliance that performs integrated copy data management.

The rich data insight that Veritas provides enables administrators to enforce backup lifecycle policies that automatically move data through the different tiers of storage as it ages. This prevents data from being overprotected or retained beyond its natural life, which helps cut costs. Veritas serves 86% of the global Fortune 500, helping these organizations collect, protect, analyze, and optimize their data.

Effective copy data management creates a "single copy" of the data as well as metadata, including information relating to backup. Virtual copies are created from this single copy, and accessed on demand using role-based access permission. By enabling administrators to easily set user privileges from a central interface, virtual copies of production data are only accessible by authorized users, which reduces security risks. Unbridled proliferation of data copies is prevented, along with significant waste of storage resources, especially when such copy data is backed up. Additionally, instead of traditional physical copies, which take hours or even days to create, virtual copies can be provisioned in seconds enabling end users to access the data they need in minutes. Now, data requesters can create as many virtual copies as they need, whenever they need them.

"It costs lots of money, not to mention the time and resources needed, to store and manage these copies," says Kate Lewis, Head of Product Marketing for Copy Data Management at Veritas Technologies.

According to IDC, copy data may consume more than 60% of disk capacity. Unnecessary copies and copy backups can also lead to unnecessary facilities costs, including data center floor space, electrical power, and cooling. Similarly, when backups of copy data are sent off to the cloud to be stored, companies can incur large and unnecessary cloud service expenses.

**Businesses must assign a high priority to a comprehensive unified data protection strategy.**

According to IDC, "Most organizations have long been multivendor storage consumers, and now with the added complexity of cloud storage, the back-end repository details may be unknown. Thus IT managers will want to consider products that can manage copy data independently of the storage media, whether on premise or in the cloud or a hybrid of the two."[3] An integrated copy data management appliance is an effective way to address these issues.

## Conclusion

Although business-critical workloads are increasingly migrating to the public cloud, private clouds remain important for many applications. The resulting hybrid cloud architecture is becoming prevalent at companies across all industries. However, the use of multiple cloud providers combined with the rapid growth of multiple types of data, particularly unstructured data, creates data protection challenges.

Businesses must avoid the traditional pitfall of giving short shrift to data protection and must instead assign a high priority to a comprehensive unified data protection strategy. That strategy should encompass visibility and classification, as well as predictable resiliency and integrated copy data management.

The ability to manage data protection from a single pane of glass and to move data between public and private clouds will enable businesses to achieve the agility they need to support the data-driven business initiatives of today -- and tomorrow.

**To learn how Veritas can help your data stay visible, available, and protected, go to www.veritas.com.**

3 "The Copy Data Problem: Analysis Update," by Phil Goodwin and Ashish Nadkami, IDC, 2015.

## RELATED CONTENT

# 7 Simple Truths You Should Know About the Hybrid Cloud

### The journey to the cloud is all about managing multiple environments, which is what 'hybrid' really means

**By Gavin McShera,** Contributor, *InfoWorld* | Nov 25, 2016

I'M ABOUT TO TELL YOU SOMETHING THAT MAY SHATTER WHAT YOU THINK about the cloud: The hybrid cloud does not exist.

The enterprise cloud adoption manual puts hybrid cloud at the top of the list. But you cannot buy one off the shelf. It's not one-size-fits-all.

Rather, the hybrid cloud is made up of models, processes, and multiple providers. The moment you start paying for a public cloud service, no matter how small or simple the service might be, you are in a hybrid cloud model. Ignore the textbook definitions: The "hybrid cloud" simply means you're delivering IT services that use more than one hosting model.

What determines the success of your delivery model? It's the rules and processes you put in place for adopting new services from cloud providers. Here's what you need to know about the hybrid cloud.

**To read the rest, click here**

Despite the challenges, organizations must start addressing data protection, even if it means starting small.

# The Changing Data Protection Paradigm

## It is impossible to keep data secure and free from alteration when you can't keep track of what you have, where it is and what its value is. So where to begin?

**By Robert C. Covington,** Advisor, *Computerworld* | Sep 22, 2016

I SPENT LAST THURSDAY AS I USUALLY DO, ON THE TRACK AT THE YMCA while listening to my favorite podcast, **Down the Security Rabbithole.**

The episode, titled "Data Protection Primer," discussed the importance of protecting data security and privacy. One of the guests, Vlad Klasnja, the data protection and privacy manager for Optiv, made the point that despite the challenges, organizations must start addressing data protection, even if it means starting small. This put my main brain into high gear for the balance of my run, thinking through how we collectively got into this mess, and how we can begin to climb out of it.

Twelve years ago, I was the technology head for a consumer credit bureau. Our data was obviously very sensitive, and, even at the time, heavily regulated. While protecting this data was a challenge, it was fairly easy compared to what organizations face today. I had little else to protect other than my consumer database. I knew exactly where the data was: replicated between two data centers, and on backup media at a secure storage facility. It was minimally accessible to the outside world. Even the data that was indirectly web-accessible resided in my facilities.

**To read the rest, click here**

# Visibility, Security Top Concerns for Cloud Computing Adoption

## Enterprises are concerned about where their data is located and how it's protected

**By Maria Korolov,** Contributing Writer, *CSO* | Nov 10, 2016

Enterprises considering adopting public clouds are concerned about where their data is located and how it's protected, according to a new survey by IDG.

Companies will have about 60 percent of their IT environment in public, private, or hybrid clouds, according to a survey of about 1,000 IT decision makers.

Of those considering public cloud deployments, the top concerns were where data is stored, at 43 percent of respondents, and security, with 41 percent of respondents.

And with all the high-profile hacks of well-known online brand names, it's no surprise.

However, clouds are not necessarily less secure than on-premises deployments, said Rich Campagna, VP of Products at Campbell, Calif.-based Bitglass, Inc.. The company's research team is working on a cloud adoption report that examines cloud usage at more than 120,000 organizations, which will be released next week.

**To read the rest, click here**

# Trends in Enterprise Cloud Adoption

Network World | Dec 2, 2016

At the AWS re:Invent show in Las Vegas, Network World's Brandon Butler chats with WIlliam Fellows, co-founder of The 451 Group, about the latest cloud trends for enterprise companies.

**To watch video, click here**

# How much cloud is too much cloud?

## Not every enterprise application makes sense for the cloud. Here's how you'll know when you've exhausted the right migration candidates

**By David Linthicum ,** InfoWorld | Dec 6, 2016

I'm often asked: Should all application workloads exist in the public cloud? The right answer is one that most people don't want to hear: It depends.

It depends on what industry you're in. It depends on performance expectations. It depends on security requirements. The list goes on. Some enterprises will reach the point where 80 to 90 percent of their workloads exist in the cloud: some will only get to 50 percent.

There is a point at which it does not make sense to migrate any more applications to the cloud. This is due largely to the fact that there is no significant economic benefit in doing so. It doesn't make sense to migrate what doesn't pay for itself.

This is why I insist on making a business case that outlines the business benefits of moving to the public cloud for each and every workload. Most business cases are obvious, some will need deeper study, and some will fail to show any value. When it no longer makes sense to migrate any more applications to the cloud, you've reached your natural saturation point.

Despite the fact that it will take many years to reach that saturation point, you can actually calculate today what that point will likely be. It's just a matter of doing some deep analysis on your existing workloads to figure out which ones can go to the cloud and which ones can't.

On the other hand, who can predict the future, especially the future of technology? In five years, the cloud may have evolved enough that there will be a business case for those applications that initially did not make sense for migration. Still, it's a safe bet that all applications won't move to the cloud, even as cloud technology gets more cost-effective and better at addressing workload needs, such as compliance, security, and performance.

The chances are good that you'll find the saturation point sometime in the next five to ten years. That is not a bad thing. It is an even better thing if you understand where that saturation point is by thinking pragmatically about the use of the public cloud and justifying everything you move. By doing so, you'll save money, time, and disappointment.

**To read the rest, click here**