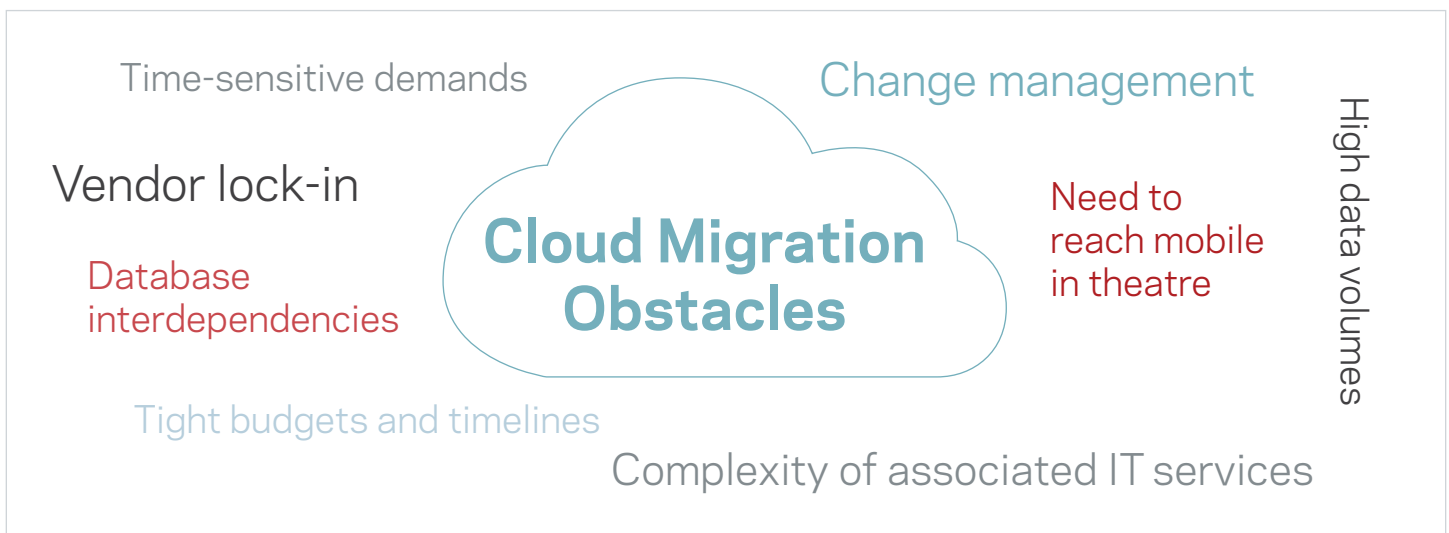


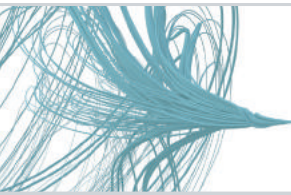
Take Control: Harnessing Data to Simplify  
and Accelerate Cloud Migrations.

The truth in cloud.



*The Department of Defense (DoD) has a new mission - to accelerate cloud services adoption enterprise-wide, with a particular focus on commercial cloud services. This direction is in close alignment with the White House, which identifies cloud and shared services as the primary catalysts for widespread IT modernization - and associated cost savings, efficiency gains, and stronger cyber security - in the Federal government.*

Cloud holds enormous potential to transform government IT, migrations can be easier said than done, causing several concerns. Often, even after selecting a service provider, migration becomes a daunting challenge due to complexities of change management - resulting in low cloud adoption. The difficulty of migrating workloads to the cloud depends on several factors: the time-sensitive nature of the demand, the huge volume of data to be classified and migrated, database interdependencies, and the complexities of the associated IT services that must also be moved. Because of the volume of networks that exist and the importance in reaching mobile in theatre, it is critical that common governance policies exist for all migration plans. Most organizations have a set budget and timeline to accomplish each cloud migration, and failure to align with the strategic plan can have costly consequences.



In addition, due to the mission-critical nature of their work, DoD agencies cannot afford downtime, so developing an effective migration plan can be even more challenging. Ensuring uptime can get tricky as applications and systems are spread across on-premises, private clouds, and public cloud environments, which can lead to fragmentation as organizations often use point tools to manage different parts of their IT infrastructure. In turn, this fragmentation can drive increased operational costs, reduced visibility, and an increased risk of IT downtime. Finally, agencies must consider the portability of their platform, ensuring they can move in an agile fashion across data centers and multiple clouds. While all these issues exist, it is necessary and important for DoD agencies to make the leap.

### The Way Forward

Holistic data management and a strong information governance strategy can provide the framework needed to 1) properly assess the environment by visualizing your data, 2) design a path forward, 3) test migrations with real data and low risk, 4) execute and 5) innovate.

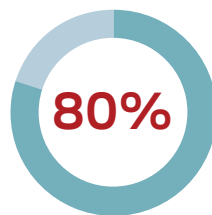
### 1. PREPARE

#### Leverage visualization tools to identify and classify data to clean up in preparation for migration.

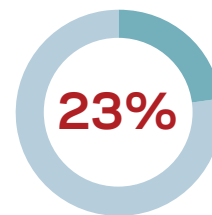
Today, most agencies are not managing their data as a strategic asset. They often treat it as an administrative burden, with little to no knowledge of what it contains, who owns it, how much risk it presents, or even where it is. This is especially true of unstructured data (various emails, videos, documents, files), which make up the vast majority of data and is the most difficult to identify and manage.

**48.7%**

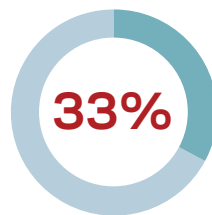
Average annual data growth per year



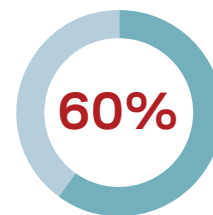
80% of data is unstructured



23% Average file size growth in last year



33% of organizational data has not been modified in at least three years



60% of files are copies that add no value



---

## Why is it so hard?

Several factors are contributing to the challenge:

- **Fragmentation:** In today's diverse IT landscape data can be located almost anywhere – from a variety of traditional storage drives to public cloud services such as Amazon and Azure, private clouds containing virtualized and containerized apps, mobile devices and personal cloud services such as Box.
- **Volume:** More data was created in the last two years than in all of human history<sup>1</sup>. By 2020 the digital universe will contain 44 zettabytes<sup>2</sup> (that's 21 zeroes, in case you were wondering) – over 80% of it unstructured and the responsibility of organizations to store somewhere<sup>3</sup>, including the estimated 60% of files that are copies of originals that add no value<sup>4</sup>. Organizations experienced an average data growth of 48.7% in the last year, with the average file size increasing by 23%, while one third of organizational data has not been modified in at least three years<sup>5</sup>.
- **Complexity:** The typical IT organization has accumulated hundreds of separate data management tools and component solutions over time in a piecemeal fashion, for individual functions such as backup, archiving, disaster recovery, copy management, etc. The lack of integration between these tools perpetuates complexity and cost, and inhibits IT's ability to respond to changing demands.

The inability for IT to see, control or regulate their data in the face of these challenges has profound implications:

- **Lack of data visibility and control:** You can't manage what you can't see. Without the ability to obtain a clear line of sight into your data environment and understand what you have, you can't make proactive decisions about what to keep, what to delete, or which availability or protection services to provide.
- **Increased risk:** Organizations must comply with strict requirements for data handling, privacy, and sovereignty. Data breaches are also becoming more widespread, potentially resulting in catastrophic damage to an agency's reputation or worse – national security crisis.
- **Unnecessary cost:** Many IT organizations do not have effective policies for their data, leading to employees and departments keeping everything forever. Not only is this inefficient and risky, it adds considerable unnecessary cost in acquiring ever more storage. Agencies could realize immediate savings by deleting unneeded files or moving them to cheaper environments such as cloud or 'white box' commodity drives.

With Veritas, agencies can make informed decisions about all of the information they currently manage – helping to get their data sprawl under control. Agencies can find their data, determine who has access to it, and classify it by value and risk to the organization. Then, they can assign policies to the data for user authorization, access time requirements, and retention.

---

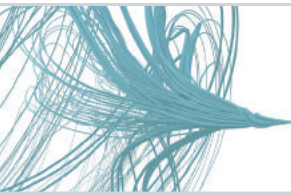
1 Big Data: 20 Mind-Boggling Facts Everyone Must Read, September 2015

2 IDC Digital Universe Study, 2014

3 12 Very Shareable Stats on Big Data, Bridg, September 2015

4 IDC Report "The Copy Data Problem" 2015

5 Veritas Data Genomics Index Report, 2017



Getting a handle on your information before moving to the cloud is a vital first step in ensuring a smooth migration and continued effective policy enforcement, no matter where information resides or where it travels. With Veritas, agencies can synthesize intelligence across unstructured data sources and take action to ensure they are best positioned to counter information risk by:

- Tracking and reporting on file usage and security.
- Automating retention management, classification, and supervision, while simplifying search and discovery over both structured and unstructured data.
- Providing visibility across on-premises and cloud-based systems to help agencies better understand and control their fragmented data assets.

## 2. PLAN

### Review use and affiliation, organize, dedupe, and archive data not necessary to the migration.

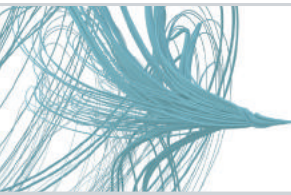
Visibility is a pre-requisite to identifying and classifying the huge volumes of files being stored, informing decisions regarding retention and compliance, reducing risk, and managing storage more efficiently.

Many organizations lack real-time visibility into IT health. They rely on point solution interfaces for different areas of their environment – a fragmented approach that can easily lead to an incomplete picture. Alternatively, they may rely on virtual machine mobility solutions that don't offer insight into what's most important – the applications and their dependencies.

Veritas' 360 approach to data management brings together the key capabilities of insight, availability, and protection, enabling organizations to take control of their information and infrastructure as they plan for cloud migrations. With this approach, agencies can:

- **Improve visibility and control:** Quickly obtain data visibility and take action from a single aggregate viewpoint to inform agency decisions, align protection policies, delete unwanted data or copies, and predict future resource needs.
- **Ensure end-to-end resiliency:** Go further than backup and disaster recovery as separate procedures by proactively moving applications and their associated data intelligently via orchestration and automation as needed to meet uptime or capacity demands.
- **Resource optimization:** Allocate infrastructure resources correctly the first time, without under- or over-provisioning, and streamline the provisioning process by providing self-service data access and the ability to proactively handle peaks in demand.
- **Risk management:** Quickly identify areas of data risk and make informed decisions about remediation, assess compliance readiness, monitor data access patterns, and enforce policies independently of underlying infrastructure.

With this framework in place, DoD agencies can develop and follow standard data operations guidelines to ensure their data is classified and protected appropriately – before a cloud migration, during cutover, and beyond – no matter where their data resides. Comprehensive data management establishes and improves sets of standard processes over time, providing a predictable measure of consistency.



### 3. RECOVERY AND MIGRATION REVIEW

#### Test migrations with real data and low risk.

Once you have established a data governance model, and identified and classified its information, you can move to the next step in your agency's cloud migration. But, before spending time, effort, and dollars migrating workloads, it's essential to ensure a positive outcome. Without a way to test that your migration will work and that your workloads will work optimally in the cloud after the move, you may be leaving things to chance, which is never a good strategy. It's like having a power generator but never testing it to ensure it works before the power goes out. Likewise with migration testing, you must be able to test your strategy before you put it into action in order to mitigate risk.

A successful migration starts with a successful test. There are multiple aspects to this strategy:

- First, you need to replicate your agency's data to the cloud.
- Then, you must ensure that the testing solution you are using is fully automated, and creates a real-time copy of the replicated data. This copy then gets attached to your test workload on the compute instance before it is brought online. This is important because you don't want to connect directly to the replicated data stream which could possibly cause production issues.
- Finally, you want to be able to repeat tests easily without manual efforts, reliance on multiple teams, or disrupting production environments. This is crucial as IT environments are constantly changing and can be impacted by configuration drift. Being able to perform repeatable and automated migration testing before the actual migration is the only way to be assured that your plan will work.

### 4. MIGRATION/EXECUTION

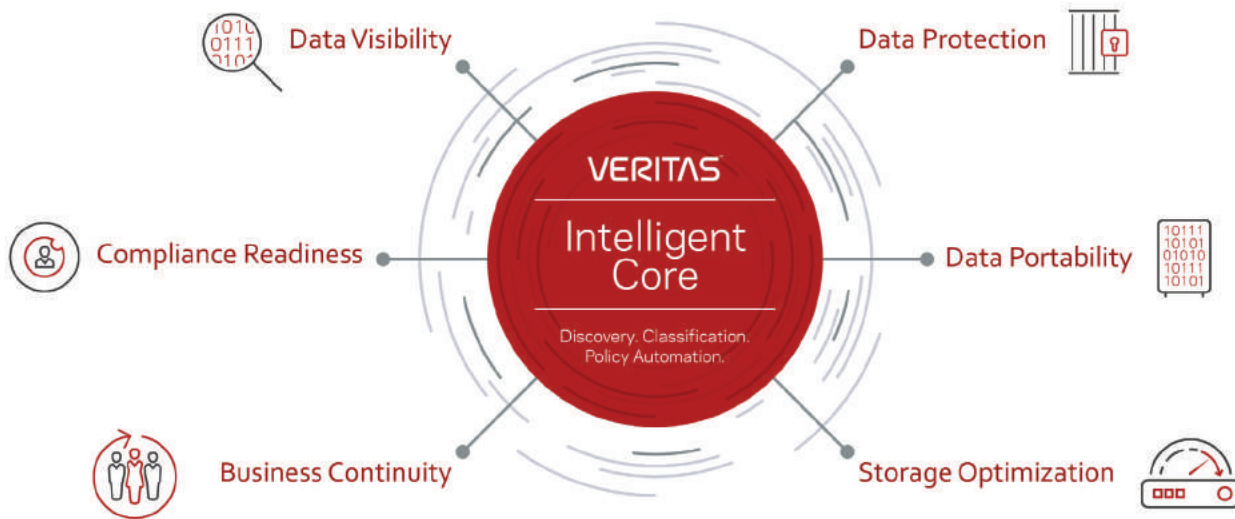
#### Provide uptime and availability to applications and associated data in a migration.

DoD workloads are complex entities made up of multiple tiers with a huge number of dependencies. Migrating these types of complex workloads can be complicated since you must maintain start/stop consistency and ensure that the dependencies are honored.

The IT environment must be reliably preserved to ensure it is always safe, intact, and accessible with no service disruption; this demands scalable, fast, and efficient backup and recovery of any environment (virtual, physical, open source, or cloud) without disrupting operations.

Finally, adopting public clouds into an already multi-vendor, multi-platform environment can cause fragmentation issues, which in turn reduces visibility into government IT health. Maintaining real-time visibility is important so you can make well-informed mission decisions and easily ensure that your agency is meeting service continuity objectives, including recovery time and recovery point objectives.

With an effective data governance framework (and all associated policies) in place, once a migration is complete, managing the cloud environment is just like managing another data center. With a common operating environment and one set of tools to manage your data across cloud and on-premises environments, you can reduce training costs and improve resource performance, because all IT administrators are using the same interface and tools to ensure data is protected and available. With this common platform, data can truly become a competitive advantage.



## 5. RESILIENCY AND INNOVATION

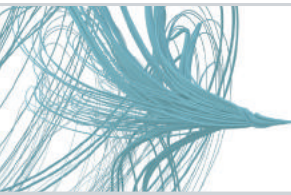
### Ensure visibility into and availability of data across multiple data centers and clouds.

With a successful migration, an agency can have unprecedented agility and a platform for innovative data analysis and intelligence that can more effectively support mission objectives. But uptime is critical. As workloads and data increasingly run on diverse platforms and across multiple data centers and hybrid clouds, agencies must maintain constant availability of key applications and data, while keeping pace with the transformation and ensuring service level objectives are met.

The bottom line is that no cloud is failsafe. Some organizations incorrectly think they are protected because they are replicating or backing up data across sites, but forget that without recovery orchestration for the application itself, they are exposed to downtime. Even the most robust perceived public clouds can go down due to something as simple as human error. If this occurs, your agency's mission will be negatively impacted by lost budget, productivity, and time.

Veritas can help you:

- **Implement a resiliency solution for your public cloud workloads that is different from the basic resiliency add-ons available through your cloud provider.** A robust solution will be able to alert your organization instantaneously when an outage occurs, and easily failover your workloads to another zone or region in the cloud or even back to your on-premises environments.
- **Unify resiliency management across all environments - including physical and cloud.** Using different recovery tools across different environments can cause fragmentation, which leads to unpredictability and risks. A more efficient and optimal way of managing resiliency is to use a single solution that caters to all environments, one that reduces fragmentation and increases visibility.
- **Provide real visibility into IT health and compliance.** Relying on multiple virtualization admins, backup admins, and server admins for information can lead to delays and inefficiency. You may also run the risk of missing critical information during times such as when



a natural disaster strikes and your employees may not be available. A single pane of glass visibility into your IT health lets you know how well your agency is tracking to defined recovery objectives, at the virtual machine level as well as the mission level.

▪ **Deliver predictable service level objectives.**

Predictably meeting service level objectives is the most critical aspect of a resiliency strategy, as many organizations don't know how much data they will lose and how long it will take to recover in the event of an outage or disaster.

▪ **Automate orchestration across complex multi-tier IT applications.** Many applications today have a huge number of dependencies that will only get more complex with the rise of cloud-based architectures and containerization. Maintaining uptime for multi-tier applications that have complex dependencies is possible with the right solution.

Finally, agency priorities can fluctuate over time and may require an organization to move workloads back to on-premises, or even to another cloud. Organizations must stay flexible and agile so they can adapt easily to changing goals. With guaranteed resiliency, agencies are able to maximize the visibility into their data and develop insights that can drive innovation in support of the DoD's mission.

### **Flexibility Equals Freedom**

In order to achieve the breakthroughs promised by cloud, insight, availability, and protection capabilities need to be applied across the entire IT landscape in a scalable, consistent, and manageable manner rather than in silos with isolated effect.

This means adopting a software-based approach, with the ability to span across many different environments regardless of the underlying infrastructure, and to apply policies centrally rather than at multiple separate points.

But it is no longer enough to provide these capabilities independently – even if they are state-of-the-art solutions. It is necessary to integrate these capabilities to further reduce complexity, streamline operations, and find synergies that otherwise are not achievable.

The ability to reliably move and orchestrate workloads across a heterogeneous IT landscape – including multiple clouds – is necessary to maintaining resiliency and cost effective on-demand access to apps and data under changing conditions. You need to stay flexible and agile so you can adapt easily as your directives change. To do this you need to ensure you aren't putting all your eggs in one basket – or in this case, one cloud.

Veritas provides enterprise data management to tens of thousands of global customers with an award-winning portfolio of solutions. These solutions can confidently be adopted as needed to meet your data management needs, and are backed by world-class support and services.

Cloud migration can be daunting, but with Veritas, it doesn't have to be. We can work with your agency to understand and manage your data assets to improve performance, reduce infrastructure footprint, cut costs, ensure uptime, and increase user adoption.

Visit [www.veritas.com](http://www.veritas.com) to learn more about how to achieve data governance, migrate to the cloud, and harness the power of your information.