

A New Approach to Managing Data Complexity

VERITAS™

RESEARCH BRIEF



Executive Summary

Data is at the heart of everything we do, and that's especially true in government. Daily, agencies must defend against malicious threats aiming to exploit their data, while also complying with regulations that govern how data must be stored, managed and protected.

But what ultimately makes data a valuable and strategic asset for government employees is its ability to drive timely and informed decision-making.

The 2019 release of the Federal Data Strategy, coupled with technological advancements such as artificial intelligence (AI) and the rise of more sophisticated cyberattacks, has moved the urgency of data management beyond the IT shop to a core pillar of how the federal government operates.

To better understand how agencies are responding to this new normal of managing data complexities, GovLoop partnered with Veritas Technologies LLC and TVAR Solutions to survey over 100 government employees about their data challenges, priorities and future state goals. One common theme was clear: **As the amount and variety of data that agencies must manage increases, so has the need to secure that data and make it readily available to decision-makers.**

In this report, you will hear from Veritas experts on how and why agencies should prioritize availability, protection and insights of their data to make informed decisions that benefit the public, employees and the overall mission. Veritas is a data management company that works closely with TVAR Solutions to deliver complete, turnkey solutions to the public sector.

To set the stage, let's first explore how government employees describe the current state of their data and top-of-mind challenges.

"The use of data is transforming the economy, government, and society," according to the Federal Data Strategy. "If the Federal Government does not maintain its role as a preeminent supplier and sophisticated and ethical user of data, it will no longer be able to fulfill its civic duty to the public."

Current State of Government Data

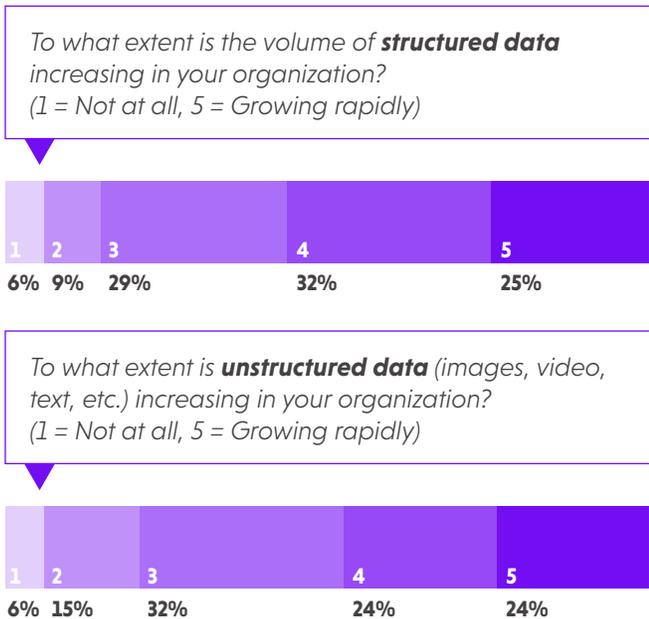
The amount of structured and unstructured data that agencies manage is growing – and at similar rates (See Figure 1).

That's a shift for agencies when you consider that the growth rate of unstructured data, such as voice, video and text, had been outpacing structured data, said Mike Malaret, Director of Sales Engineering for the U.S. Department of Defense and Intelligence Communities at Veritas.

Examples of structured data include census and employment data, product safety data and airline on-time records. Some structured data collection is required by law and other regulatory requirements, which contribute to the overall growth rate that respondents expressed.

Among the challenges that agencies face in this environment is selecting the best option for data storage. This isn't the type of government decision-making that creates news headlines but it's a foundational matter that affects costs, security, the availability of data and agencies' readiness to use tools such as analytics and AI.

FIGURE 1

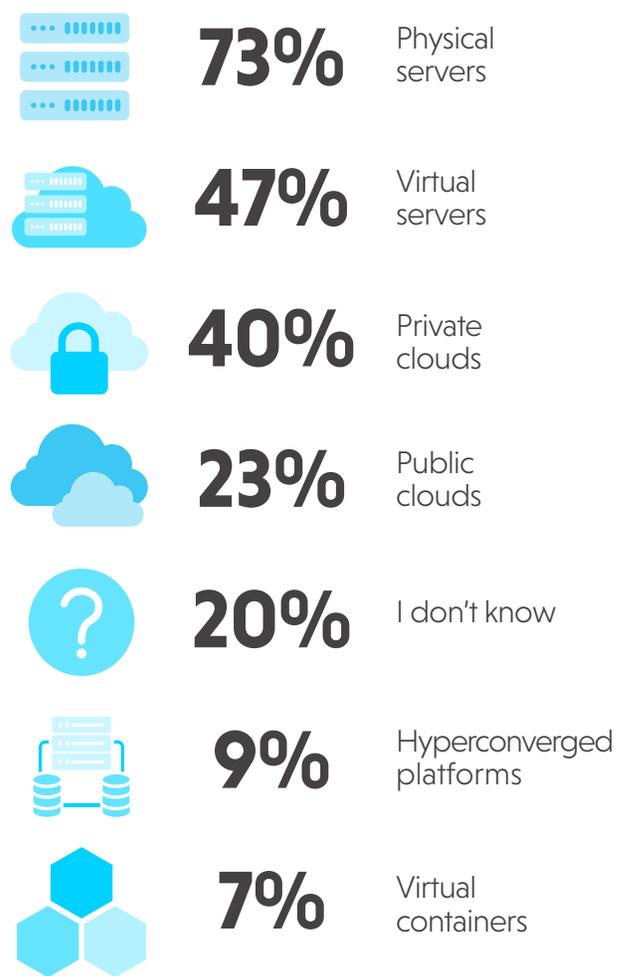


"Most solutions that are available in the market space today will focus on one or the other: structured or unstructured data," Malaret said. "It's rare, but not impossible, to find solutions that have the ability to provide insights from both structured and unstructured data."

In terms of how agencies store and access data, the vast majority of respondents (73%) are using physical servers, followed by virtual servers (47%) and private clouds (40%) (See Figure 2).

FIGURE 2

*Which of the following platforms does your organization use to **store/access data**? (check all that apply)*



What the survey data reveals, in part, is that agencies have not yet fully embraced cloud computing. Although the government has shifted from adopting cloud by any means necessary to doing so more thoughtfully and strategically under the Cloud Smart strategy, adoption has not been as rapid as the administration would have hoped.

And, in some cases, there's good reason for a slow-but-steady approach to cloud adoption. There are often software applications that need refactoring, or source code alterations so the app can function optimally in a cloud environment. It also takes time to fully understand what data agencies have before they make any decisions about moving to the cloud.

It's with this in mind that we asked respondents about their future data storage plans and where they are heading over

the next two years (See Figure 3). As agencies firm up and mature their cloud strategies, they should expect virtual servers and private clouds to be growth areas for them.

Ultimately, as data grows and storage needs evolve, agencies must grapple with how best to secure data and make it readily available to those who need it to drive decision-making. We asked respondents about their top challenges, specifically around security, data availability and how well they can glean insights (See Figure 4).

In the following sections, we will dissect these challenges, what they entail and practical ways that agencies can address each area.

FIGURE 3

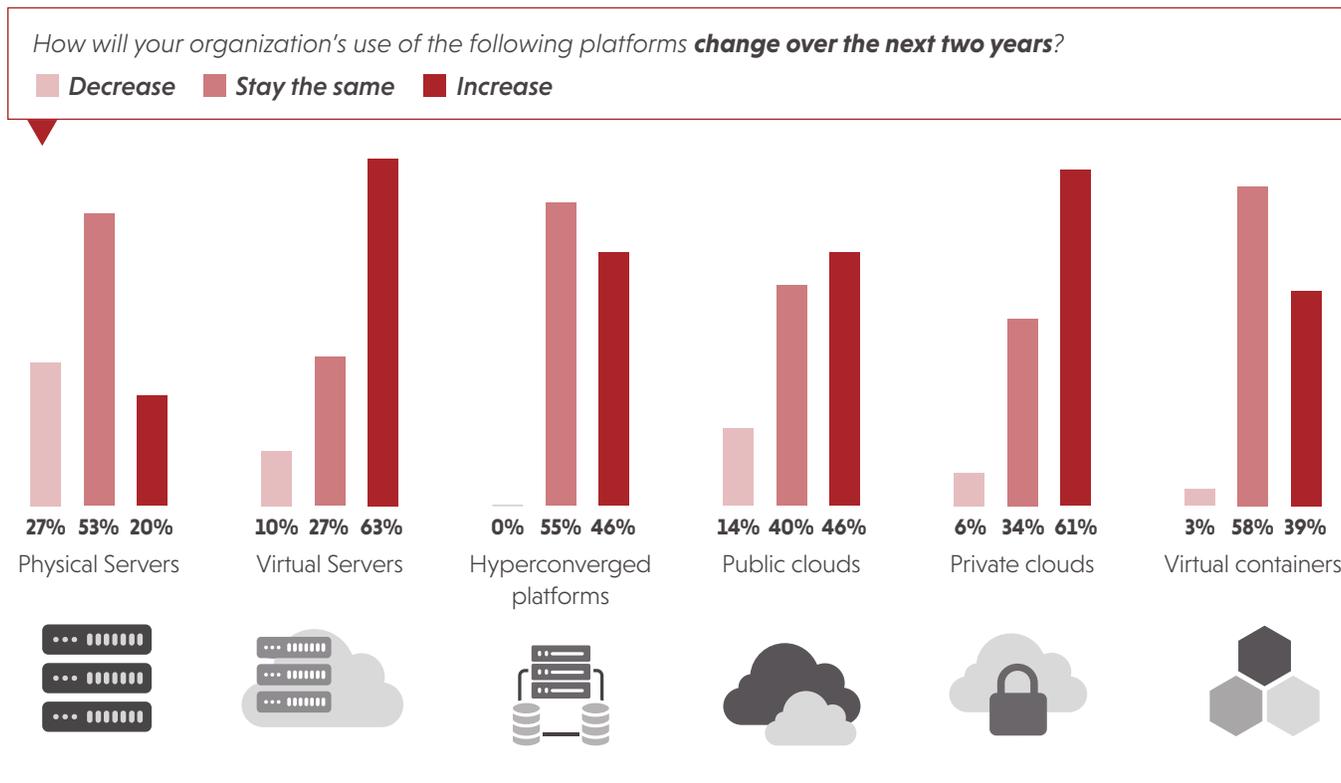
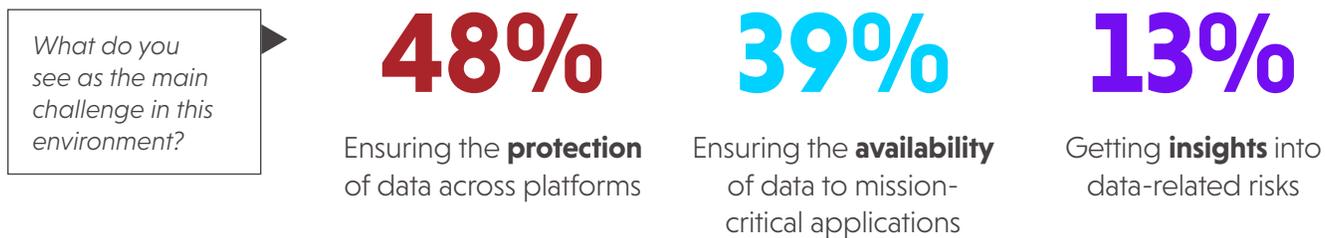


FIGURE 4



Challenge 1: Data Availability

Think about the critical applications that support the work you do every day. What data from those systems do you rely on to make timely decisions? When you think about data availability in these terms, it becomes a top-of-mind issue for all employees.

The bottom line: Data availability is vital for us all, whether we realize it or not. Ensuring applications are always available and deliver on the service level agreements that your 24/7 operations demand, whether virtual, on-premises or in the cloud, is critical.

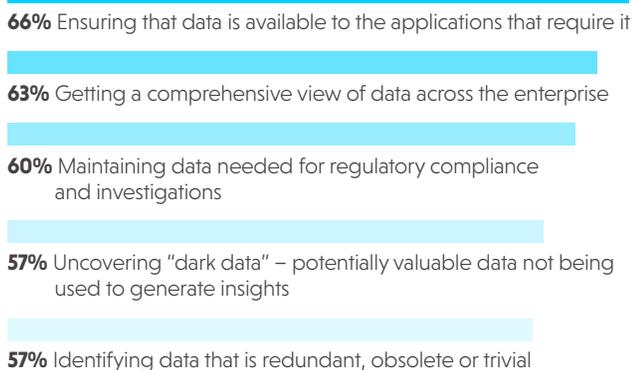
Our survey data confirms data visibility is a challenge on all fronts, making it equally tough to maintain compliance, identify redundant and dark data and ensure data is available across applications (See Figure 5).

Respondents also shared in their own words what visibility challenges they face:

- "Sharing databases between departments across state government."
- "Collaborating on access, custody, distribution, archival, and reporting on data within various user groups."
- "Getting management to enforce staff [to] stop storing [data] in thousands of Microsoft Excel spreadsheets on their own without communication. Makes compiling for any global requests almost impossible."

FIGURE 5

What challenges does your organization face around **data visibility**? (check all that apply)



A 2018 Defense Department Inspector General report illustrates how closely aligned these data visibility challenges really are. The report, citing a July 2018 memorandum from the department's chief information officer to DoD officials, stated that at the time DoD had not reported over 30% of its software inventory.

By law, all agencies are supposed to track their software inventories. Because DoD and its components had not completed that inventory, they lacked visibility over their assets, according to the IG report. This meant they were also unable to determine the extent of existing vulnerabilities that could impact operations if information processed, stored or transmitted by software applications was compromised.

Data visibility is further complicated when agencies continue to amass redundant, obsolete and trivial (ROT) data. This ROT data is stored in government systems and continues costing money and obscuring more relevant data.

"We see redundancy in datasets in pretty much every environment that you come across, especially with unstructured content," Malaret said. "It's important to be able to have insights into the utilization of that data. There is great benefit in seeing where data exists, where the duplicate data is located and what orphan data is in your environment."

Orphan data is data that doesn't have ownership, which can apply to large amounts of data that have grown exponentially over time. But if agencies can't account for this data, they can't begin to assess if it is necessary and what value it actually serves. Having tools that can identify that data is critically important, Malaret said.

Armed with this information, agencies can prioritize what data is most critical to their mission requirements and begin to shed their systems of ROT data – freeing up resources and reducing the time it takes to analyze data.

In the next section, we'll look more closely at the challenges and opportunities that agencies face around data protection.



Challenge 2: Data Protection

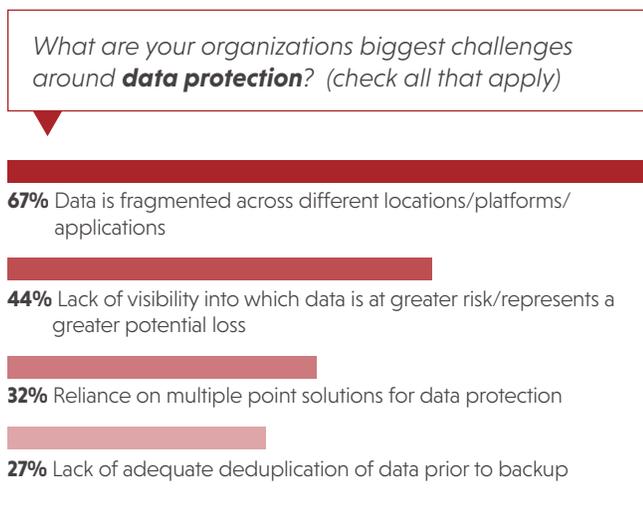
Few cross-cutting responsibilities span all teams, offices and departments in government – regardless of employees' titles. Take cybersecurity, for example. Agencies continue to evangelize the criticality of securing government networks and have made clear that it's a shared responsibility, not just the job of a select few in the IT department.

But just as important as cybersecurity – yet often overlooked – is the need for secure data management across organizations. Although employees create, analyze, share and store data in various ways and across different platforms and applications, most don't see themselves as data stewards with a key role in maintaining and ultimately protecting that data.

Based on our findings, securing data continues to be a top challenge for agencies, specifically when it comes to protecting data stored in silos, as it often is in government (See Figure 6). This is especially true when personnel may need to share data across different systems or programs.

Another challenge for 44% of respondents is prioritizing which data is at greater risk and represents a greater potential loss if compromised. This has been an ongoing challenge for agencies as they've worked over the past five years to properly identify and secure the federal government's most critical data, or high value assets (HVA).

FIGURE 6



The federal government took a pivotal step in December 2018 to update its approach for defining HVA – moving from a single definition to multiple categories – to give agencies greater flexibility when identifying and designating information or IT systems as critical assets. Those categories include:

Informational Value – The information or information system that processes, stores or transmits the data is of high value to the government or its adversaries.

Mission Essential – The agency that owns the information or information system cannot accomplish its primary mission essential functions (PMEF), as approved under Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.

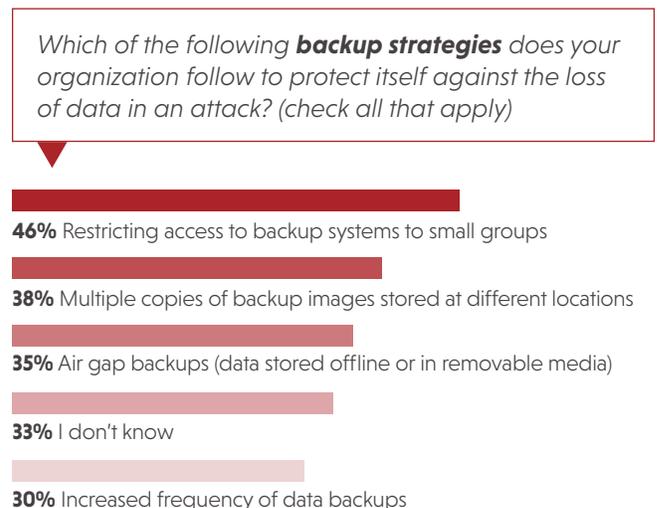
Federal Civilian Enterprise Essential (FCEE) – The information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

Clearly defining what data is most critical to your organization helps to also determine how best to secure that data, using the appropriate security controls. Think of it this way: You wouldn't use the same money, energy and effort to secure your new car as you would an inexpensive bike.

Another piece of the data protection puzzle that agencies must account for is the lack of adequate duplication of data prior to backup. This doesn't mean creating more data silos, but rather accounting for strategic duplication of data in the event of security attacks such as ransomware (See Figure 7). This consideration should be a part of an agency's overall data protection plan, Malaret said, which includes having high-availability solutions across data centers and a strong data backup strategy to protect against the loss of data.

Ultimately, agencies need secure and timely access to data to support decision-making.

FIGURE 7



Challenge 3: Data-Driven Decision-Making as a Priority

The rise of data has opened new doors for government agencies. Increasingly, they are collecting, analyzing and using historical facts and trends to improve policies, citizen services and respond to pressing social challenges.

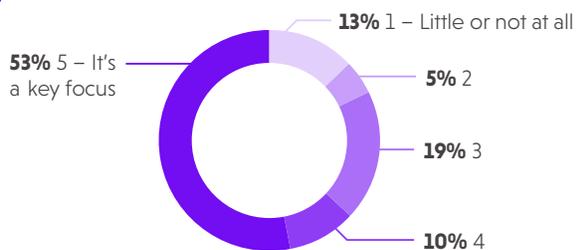
This data-driven method of decision-making offers serious benefits to agencies, which explains why more than half of respondents (53%) said it is a key focus for their agency (See Figure 8).

But what about the other 37% that seems to be either middle-of-the-road or uninterested in making data-driven decisions? For some agencies, it isn't so much that the desire to make data-driven decisions is lacking, the issue is they don't have the necessary capabilities to fully support those efforts.

The other major challenge, which we noted in the previous section, is that government organizations are not taking full advantage of data that is available to them. In some cases, they aren't quite sure what data they have, which makes prioritizing data-driven decision-making a challenge.

FIGURE 8

*To what extent is your organization focused on **data-driven decision-making** – leveraging data to gain insights into operations and services and to inform strategic decisions? (1 = Little or not at all, 5 = It's a key focus)*



We pulled some helpful best practices from a [Health and Human Services Department resource](#) that outlines practical steps for data-driven decision-making. Regardless of what your mission focus is, these four iterative stages outlined below can help you use data more strategically.

1. Formulate key questions.

The process begins with identifying and clarifying the key questions to be answered for your organization. These questions may address the need to solve a specific problem, learn more about a target population or improve a program or organizational process.

2. Collect and analyze data.

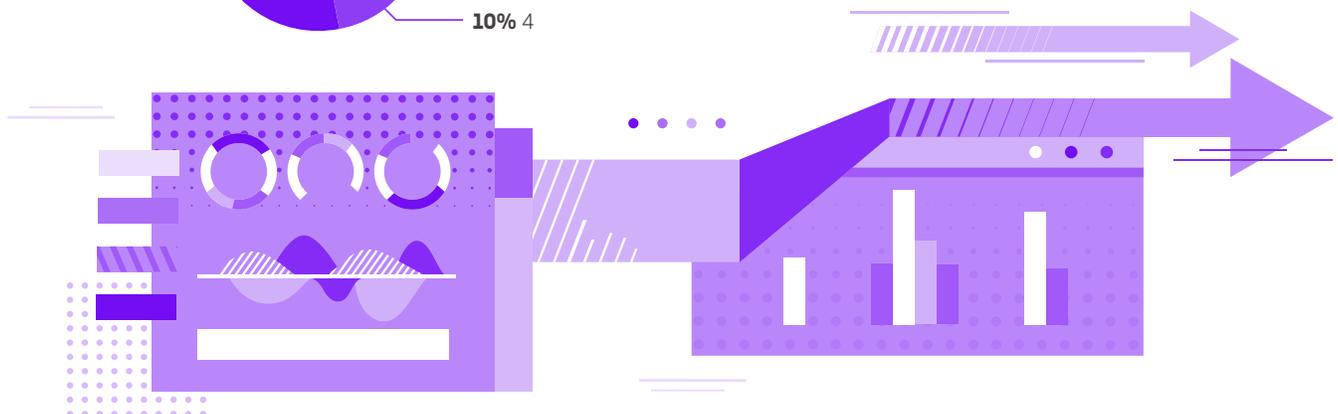
Guided by the key questions, identify available data and collect new data as needed. Access to high-quality data is critical.

3. Communicate results to decision-makers.

Share results with key decision-makers within and between levels of the organization or broader service system. Dissemination may take place through various communication channels and formats, depending on the information needs of stakeholders.

4. Refine processes, organizations or systems.

Decision-makers use information gathered during the previous stages to assess gaps in services; strengthen the performance of programs, organizations or systems; and assess the impact of services on outcomes of interest. As more information is collected, the process remains ongoing with additional evidence producing new insights and subsequent questions for further data collection and analysis.



Future State of Government Data

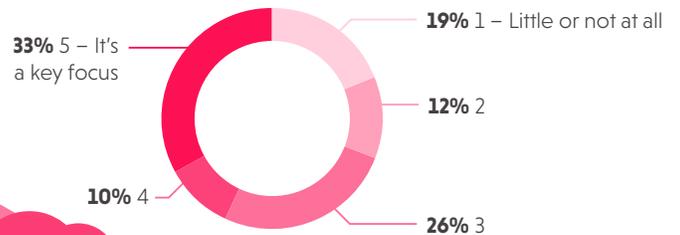
Ultimately, agencies want to reduce the complexity that comes with securing, managing and storing data. That's a top focus area for about 43% of respondents (See Figure 9).

When these three areas are addressed in unison, agencies will begin to experience the fullness and usefulness of their data.

Malaret explained that reducing data complexity isn't about an individual product or tool but more about taking a look at what problems your agency or organization is trying to solve. Although technology does play a critical role, the key is identifying the need before making investments.

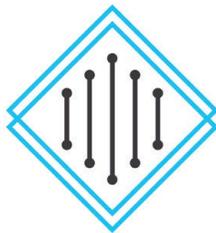
FIGURE 9

To what extent is your organization looking to **reduce the complexity** of the data management environment over the next two years? (1 = Little or not at all, 5 = It's a key focus)

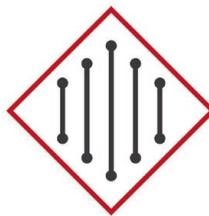


How Veritas & TVAR Solutions Help

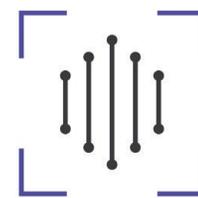
Agencies can defy data complexity with the Veritas Enterprise Data Services Platform. An Enterprise Data Services Platform offers a standardized way for agencies to manage their data complexity using a single solution. For example, the Veritas platform, in partnership with TVAR Solutions' unique data management services, provides:



Availability by ensuring applications are always available and deliver on the service level agreements that your 24/7 enterprise demands, whether virtual, on-premise or in the cloud.



Protection by keeping data secure at scale and no matter where it lives, with simplified yet robust data protection solutions.



Insights into data that allow you to take action to increase operational efficiency, optimize costs and enable regulatory readiness.

Conclusion

In the digital age, government agencies are producing and consuming unfathomable amounts and types of data. But without proper visibility, most of the information remains unorganized, and therefore inaccessible.

If agencies can't see what they have, they can't properly secure that data or use it for decision-making. To buck this trend, agencies need a smart data management strategy that provides data availability, protection and insights.

This approach is no longer optional for federal agencies. Agencies need to gain control of their sprawling data estates in a streamlined, comprehensive and highly secure manner.



About Veritas Technologies

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 99 of the Fortune 100—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas supports more than 500 data sources and over 150 storage targets, including 60 clouds.

Learn more at:

www.veritas.com/government



About TVAR Solutions

TVAR Solutions was founded in 2006 and is headquartered in McLean, VA. TVAR Solutions is a small business information technology value added reseller that markets exclusively to the Federal Government and its system integrator partners. TVAR Solutions aims to provide innovative solutions that address complex computing infrastructure challenges.

For more information, please visit www.tvarsolutions.com



About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | [@govloop](https://twitter.com/govloop)



1152 15th St. NW Suite 800
Washington, DC 20005

P (202) 407-7421
F (202) 407-7501

www.govloop.com
@GovLoop