FEDInsider

WHITEPAPER

LONG-TERM RETENTION IS KEY TO MAKING THE MOST OF FEDERAL DATA

aws VERITAS DLT A TECH DATA COMPANY

FEDInsider

Long-Term Retention is Key to Making the Most of Federal Data

Agency Strategies for Streamlined Data Management

Federal agencies are quickening their pace in adopting cloud computing under new guidance from the White House's Cloud Smart policy and legislative encouragement from Congress. The main reasons most often cited for the move is cloud computing's ability to offer agencies a flexible, expandable and efficient platform for information technology (IT) operations.

The Cloud Smart policy provides agencies with guidance on how to "fully actualize" the potential of the cloud by addressing the three primary concerns raised during early implementations – security, workforce, and procurement issues. Cloud Smart considers the effects of moving to the cloud, so agencies implement transitions that are a "thoughtful execution that incorporates practical realities," rather than just adopting a new infrastructure and way of conducting operations.

"We are essentially a data-driven department, whether that's on the front end of preventing crime, investigating crime and potential crime, or going to court. The information is key to connecting the dots. We probably have one of every analytic product out there."

JOE KLIMAVICZ
Deputy Assistant Attorney General, CIO & CDO, Department of Justice

One of the most important factors is data, the lifeblood of government services and operations. A major benefit of cloud computing improved access data, facilitating advanced analytics that yield insights from mountains of information. This involves taking advantage of more immediate data – from recent business transactions to national security intelligence – and diving into the secondary and tertiary data that can reveal, for instance, historical trends for analysis.

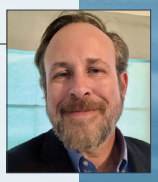
"Data analytics is huge," said Joe Klimavicz, Deputy Assistant Attorney General, CIO and Chief Data Officer for the Justice Department, at a recent FedInsider event in Pentagon City, Virginia. "We are essentially a data-driven department, whether that's on the front end of preventing crime, investigating crime and potential crime, or going to court. The information is key to connecting the dots. We probably have one of every analytic product out there."

Analytics can improve productivity, enhance decision-making, personalize service, and improve customers' experiences, among other things. Collecting, sorting, storing, managing, and using all of that data while keeping it secure can be challenging, as Klimavicz and other speakers at the event detailed.
For security, it comes down to managing risk from procurement through deployment. For performance, a lot hinges on access to data, which relies on a strategy for long-term data retention.

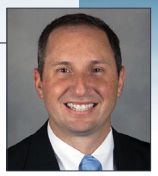
Contributors

- **David Blankenhorn**
  Chief Technology Officer, DLT Solutions, a Tech Data Company

- **Brett Hartmann**
  Distinguished Systems Engineer & Data Protection Engineer, Veritas



- **Doug Jones**
  Digital Modernization Technical Core Competency Lead, Leidos



- **Dan Kasun**
  Sr. Manager, Worldwide Public Sector Partners, Amazon Web Service

- **Joe Klimavicz**
  Deputy Assistant Attorney General, CIO & CDO, Department of Justice

- **Mark Krzysko**
  Principal Deputy Director, Enterprise Information, DoD, OUSD (A&S)

- **Deepak Kundal**
  Chief Data Officer, National Geospatial-Intelligence Agency

- **Gary Stevens**
  Deputy CISO, Executive Director, Information Security Policy & Strategy, Dept. of Veterans Affairs

aws VERITAS DLT A TECH DATA COMPANY

Long-Term Retention (LTR) in the cloud – as opposed to data storage on tape or disc – can meet many enterprise needs, combining highly scalable storage with ready access. " An effective LTR strategy reduces complexity through analytics and pattern recognition, lowers cost by aligning storage strategies in backup, archiving, recovery and retention, and satisfies storage and security requirements." said Brett Hartmann, Distinguished Systems Engineer & Data Protection Engineer, Veritas Technologies.

Starting with Security

Concerns regarding security are at the core of how the federal government handles data. The federal government, which plans to spend $7.1 billion on cloud services (Defense & Civilian combined) in 2020, budged $17.4 billion in 2020 cybersecurity funding, according to the Office of Management and Budget.

A survey of 16,099 federal IT and IT security practitioners by the Ponemon Institute, released in June 2019, found that they still see security as the biggest hurdle to cloud. When asked which areas inhibit Cloud First adoption, 67% of respondents cited security, 60% said workforce issues, 51% said management, and 47% said procurement.

When asked what factors made cloud migration difficult, the "inability to achieve a strong security posture" led the list, cited by 65% of respondents, followed by the migration complexity across on premises and the cloud (61%), visibility into resource utilization, metering, and monitoring (60%), and workforce constraints (59%). The inability to manage risks and enforce government policies also made the list, cited by 56% of respondents.

Despite these concerns, the cloud actually is secure – often more secure than keeping data locally on servers that might not have been updated with the most recent patches or can be accessed by insiders. With a major cloud provider such as Amazon Web Services (AWS), data is stored offsite at locations inaccessible to most people, the files are encrypted, and the servers are regularly updated. They provide built-in firewalls, redundancy to protect against outages or hardware failures, and artificial intelligence tools to identify vulnerabilities. They provide levels of security that an organization may not have the budget or workforce to handle.

However, a customer still has security responsibilities, as spelled out in the Shared Responsibility Model. A provider ensures the security of the infrastructure and services, while the customer has responsibility for its data, platform, and operating systems. Overlooking those responsibilities can create vulnerabilities. Gartner projects that through 2025, 99 percent of cloud security failures will be the customer's fault.*

Long-Term Retention also helps organizations address many of the concerns cited in the survey, by increasing security and visibility, streamlining compliance, and easing the burden on the workforce.

Numbers, Stats:
*Smarter With Gartner, Is the Cloud Secure?
October 10, 2019

What makes migration to the cloud difficult?

- Inability to achieve a strong security posture: 65%
- Migration complexity across on premises and cloud: 61%
- Lack of visibility into resource utilization, metering, and monitoring: 60%
- Workforce constraints: 59%
- Inability to migrate workloads across cloud infrastructures: 57%
- Inability to manage risks and enforce governance policies: 56%
- Lack of provisioning, automation, and orchestration: 44%
- Procurement and budget constraints: 44%

When government officials talk about security, data is at the heart of their concerns because so much of it is sensitive. Combining security with accessibility is another level of complexity to the cloud picture. Moreover, using data while keeping it secure is being done on the fly, noted Gary Stevens, Deputy Chief Information Security Officer and Executive Director for Information Security Policy and Strategy for the Veterans Affairs Department (VA).

"Do we really understand how the data connects?" he said, referring to how one data element is being serviced by other data elements, for example, in an environment like the VA's that must also provide security and privacy protections, while meeting a host of regulatory requirements. "I think that's still evolving," Stevens said, describing the challenge of simultaneously making the best use of data while keeping it secure.

"The plane is flying in the air, and we're adding the wings while simultaneously trying to deliver the capability," he said. But since the security of the data is paramount, "let's put the fortress around it in the meantime."

Securing Data While Making The Most of It

Organizations want to tap into their full troves of data to perform the analytics that can help improve the quality of their services. Finding the balance between using and securing data depends on managing risk, which can vary based on an agency's mission.

For others, the risk involves more immediate needs. The National Geospatial-Intelligence Agency (NGA), which supports the U.S. Department of Defense and the Intelligence Community collects reams of data from satellites, drones, and other sources and analyzes it for actionable information. The NGA's priority is to use the most current information to support warfighters, but it does not have enough human analysts to comb through the data. To achieve its mission, the NGA employs technology to sort and classify the "tremendous" volume and velocity of the data coming in, said Deepak Kundal, Chief Data Officer for the NGA. "That's where artificial intelligence (AI) and machine learning (ML) has been playing a key role."

For agencies, managing that data is a learning process. "We can get tremendous mission value from that data, but how do you balance the risk?" said Doug Jones, Digital Modernization Technical Core Competency Lead for Leidos. There are questions about who owns the decisions based on data and how to manage the data, among other factors. The equation can change with each agency mission. "We find that there's literally not a guidebook on how we do this," Jones said.

"The plane is flying in the air, and we're adding the wings while simultaneously trying to deliver the capability," he said. But since the security of the data is paramount, "let's put the fortress around it in the meantime."

GARY STEVENS
Deputy CISO & Executive Director, Information Security Policy & Strategy, Dept. of Veterans Affair

Another concern is determining the project with which to start. "The risk of failure is a big one. It's probably the biggest one," said Dan Kasun, Senior Manager of Worldwide Public Sector Partners for AWS. The thought of

making a substantial investment and failing can hold some agency leaders back. However, that's one area where a cloud investment can reduce risk by lowering the costs of investing in infrastructure. "Bringing down that risk is a big thing," he said.

The cloud also can eliminate some of the risks by providing automated tools that can sort and classify data as it's being moved into the cloud.

Long-Term Retention Optimizes a Cloud Strategy

"Paradigm shift" is a familiar, often overused, term in IT circles, but the move to the cloud can change the way agencies operate, and it requires leaders to rethink how they go about their business. They need a clear cloud strategy that includes long-term retention.

"Many of us have treated data as a responsibility" because of record-keeping or regulatory requirements, said Kasun. Moving to the cloud was seen mostly in terms of the cost benefits of maintaining data without investing in new data center hardware. "Stepping back and taking a look and seeing that data as an asset for your organization… just hasn't been a luxury that many agencies have had," he said.

To get the best results, agencies need to be able to access all of their data, which means gaining better control of it. Much of the data agencies keep is still stored on tape, which is expensive, cumbersome, and needs to be physically shipped offsite, making it inaccessible in the short term.

The move to cloud computing – coupled with the proliferation of mobile devices and the Internet of Things (IoT) – expands the amount of complex data agencies collect, collate, analyze, and store. Worldwide, more than 2.5 quintillion bytes of information are created every day, according to Domo's most recent Data Never Sleeps report, and by 2020 it's estimated the total will amount to 1.7 megabytes of data per second for every person on the face of the Earth. The amount of data the government collects mirrors that growth, though compared with the data generated on the web, its importance and sensitivity is much greater. In addition, federal record management requirements mandate that agencies keep a wider range of records for longer than before.

The makes it easy to access data and use it effectively. Veritas, for example, offers a Long-Term Data Retention solution with AWS and AWS Partner Network (APN) Technology Partners, which combines Veritas' on-premises appliances with AWS Cloud storage solutions. It employs Veritas' NetBackup for data backup and recovery that is optimized for AWS, CloudCatalyst for end-to-end deduplication, and access to facilitate on-site and tiered backup to AWS. The solution can solve the problem of protecting and managing data. It moves data from tape to an accessible platform, making it possible to glean the insights from it.

As part of their solution, the NetBackup infrastructure can send data to a CloudCatalyst server in formats that are deduplicated, compressed, or optimized for storage on AWS. By maintaining optimization, the CloudCatalyst server maximizes data transfer performance while reducing storage consumption, which can lower the costs associated with storing massive amounts of data. Likewise, Veritas' Long-Term Retention capabilities cut the costs of tape storage and management.

The solution is highly scalable, taking advantage of the capacity and security of AWS. AWS holds the U.S. Department of Defense provisional authorizations for information up to and including the Secret Level under the Defense Information Systems Agency's Security Requirements Guide. It can solve agencies' LTR issues, while delivering high performance, compatibility with storage formats, reliability, and ease of management.

Conclusion

When it comes to data, there are three principles for operating in the cloud: availability, protection, and insights. Agencies are making progress in dealing with managing and using data in a cloud infrastructure, although IT leaders admit they have a long way to go to achieve their goal of maximizing the value of their data while keeping it secure.

Mark Krzysko, who leads Enterprise Information for the DOD's Acquisition, Technology, and Logistics community, said that agencies need to improve on what he calls "data intellectualism."

"We have to be wiser and understand the tech terms, the data terms, and the system terms for us, and that means every one of us," he said. "We've got to improve our intellectual capacity to understand these products," in order to acquire and use them correctly.

David Blankenhorn, Chief Technology Officer for DLT Solutions, a Tech Data Company said another challenge is overcoming the inertia of being stuck in older, outdated ways of doing business. "The first step is probably the hardest," he said, but "you have to get started" on identifying how to get to and gain insights from the data agencies have, while maintaining security.

Employing the right tools and expertise, like Veritas' Long-Term Retention solution on AWS, can simplify the process and deliver the results agencies need.

"We have to be wiser and understand the tech terms, the data terms, and the system terms for us, and that means every one of us,"

MARK KRZYSKO
Principal Deputy Director, Enterprise Information,
Department of Defense, OUSD (A&S)

FEDInsider
Viewpoints on Government Management

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
@FedInsider

DLT
A TECH DATA COMPANY

DLT Solutions
2411 Dulles Corner Park, Suite 800
Herndon, VA 20171

800-262-4358
sales@dlt.com
www.dlt.com

DLT Solutions is the premier government solutions aggregator that specializes in understanding the IT needs of the federal, state, local and education, and helps simplify the process of doing business in the public sector.