FEDInsider

WHITEPAPER

The Truth in Cloud:
Exposing the Risks to Government

DLT | VERITAS

The Truth in Cloud: Exposing the Risks to Government

Introduction: *Federal agencies are using multiple public clouds in addition to on-premises private and non-cloud infrastructures. This mutli-cloud adoption is creating increasingly complex environments and making it difficult to manage and protect data. Without proper data management, hybrid and multi-cloud environments can quickly become just another series of expensive and risky silos. All cloud migration strategies should encompass data management best practices to maximize cloud adoption benefits while minimizing risk.*

Eight years into cloud adoption, federal government leaders possess a better understanding of cloud benefits and challenges. Now, the government wants to build on the Obama administration's Cloud First policy to ensure the technology fits the mission that agencies are trying to serve.

"Cloud smart" calls for agency managers to assess the maturity levels of their cybersecurity, procurement practices, and workforce training before moving their IT operations to cloud infrastructures.

"One thing that's guaranteed with moving to the cloud is exploding complexity," said Kshemendra Paul, cloud action officer and deputy director of the Strategy and Mission Information Sharing and Services Office within The Department of Homeland Security's (DHS) Office of the CIO. "There's the opportunity to improve cybersecurity, but that requires smart management and optimization."

DHS is one of the largest federal agencies comprised of twenty-two component agencies with diverse missions. The organization has a multi-cloud, hybrid IT environment with a mix of several cloud computing models including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

DHS Strives for Enterprise Cloud Approach

DHS IT is on the move in transitioning to the cloud, Paul said. In 2017, only 9 percent of DHS' Federal Information Security Act (FISMA)-compliant systems moved to the cloud, but that grew to twenty-one percent by early 2018. The number is even larger now. There are some challenges with DHS' push toward the cloud, though. The bottom up aspect had led to an uneven approach and uneven benefits. While some programs are seeing some advantages, DHS has not discovered an enterprise-wide business case yet.

The keyword is "yet."

"It's not surprising that there's been some challenges as folks go to the cloud. They have to work around barriers like traditional security models," Paul said. However, as agencies successfully work around those challenges, they're paying for the new and old technology at the same time.

Moreover, like most government organizations, DHS' procurement models are not designed around the cloud. This and a variety of issues are driving DHS to bring an enterprise approach to cloud adoption. As a response to this set of uneven bottom up progress, DHS senior management wants to bring an overlay of a top down, more managed approach to help optimize the movement. Not to centralize, but to help optimize, Paul said.

"We think we can better leverage our data in the cloud, looking at the lifecycle of the data, moving upstream to better engineered instrumentation [and] moving downstream to linking the data both for near real-time and real-time operational use and analytics to support improved optimized IT service delivery," Paul explained.

More Data. More Complexity.

Organizations are dealing with more data today than ever before. New technologies like Internet of Things (IoT) devices and sensors are gathering data at a rapid rate, most of it unstructured. Government managers are learning how to devise actionable information from the vast amounts of data while finding an infrastructure to support it.

As a result, organizations need a comprehensive view of data management for greater data visibility. "If you don't know where and what your data is, you can't protect it, you can't manage it well. The complexity of our environments today makes visibility really critical, especially as we think about how we transform to be digital," said Jonathan Alboum, former Department of Agriculture CIO and now U.S. public sector CTO for Veritas Technologies.

The integration and deployment of multiple clouds makes the management and protection of data more challenging. Without proper data management, hybrid, multi-cloud environments can quickly become just another series of silos, compounding costs and risks, Alboum noted.

Adding to the complexity are misconceptions many IT managers in enterprises and government still harbor about the cloud. Recent research conducted by Veritas, based on interviews with customers, indicates many IT managers are unclear about their responsibilities. Clearing up these misconceptions will help organizations better understand their data management and data protection responsibilities versus their cloud service provider's (CSP) role and responsibility for data protection.

MISCONCEPTION #1:

My CSP is responsible for protecting our data in the cloud

47% backup all data in the cloud

39% backup only business-critical data

68% use a backup option from CSP

There is a common misconception among IT managers that the CSP is going to complete backups on their behalf. Although some of a manager's responsibilities fall to the provider, the manager still owns the responsibility for their data.

"Despite what some people think, the cloud service provider is not backing up data for you in the way that you need it," Alboum said. "You really need to understand what your requirements are around data protection in order to have the right data protection solution in a cloud environment.

Technologies that CSPs provide are part of a much larger data protection scheme, but they're not the end all. "Understand what the cloud service provider offers, understand what your requirements are, and look to see if there are alternatives," Alboum advised.

MISCONCEPTION #2

My CSP is responsible for application uptime in the cloud.

83% feel CSP protects against outages

55% feel Work Load uptime is CSP's responsibility

36% have experienced an outage

73% report having experienced downtime

The reality is that most CSP Service Level Agreements are focused on keeping the infrastructures up, not on a customer's application. If an event such as outage occurs, it is really the customer's responsibility to assess how their applications are working.

The cloud is akin to a data center environment, run by a set of off-site professionals that provide a service with great capabilities. It's also a technology stack that can fail. Managers must prepare for that possibility and devise a plan to ensure business continuity.

MISCONCEPTION #3

My organization's cloud provider takes care of all data privacy and compliance regulations.

76% agree my CSP is responsible for all data privacy and compliance regulations.

38% say the responsibility of compliance auditing lies primarily with the CSP.

These stats above show that managers thought the responsibility for compliance auditing lied primarily with the CSP. This is not necessarily true.

The concepts around privacy and compliance are critical in the federal government. Anyone who has handled Freedom of Information Act (FOIA) requests, electronic discovery, or records management requirements knows how difficult it is to manage these disciplines if you don't know what and where your data is.

Managers need data protection that gives them the ability to store their data in an optimized way, the ability to move data and applications around from one cloud to another, and from the cloud back to on-premise or between clouds.

“That gives you flexibility and business continuity. When you’re doing all those things and you’re classifying your data well, now you’re ready for compliance activities, be it FOIA or e-discovery,” Alboum said.

5 Data Management Tips to Build a Successful Multi-Cloud Strategy for Government:

1. ESTABLISH DATA VISIBILITY

Many agencies see their on-premises secondary data stores as perfect candidates for cloud migration. However, Veritas’ 2016 Global Databerg Report finds that more than fifty-percent of this data is “dark”, meaning no one knows what it is. The study also finds thirty-three percent is redundant, obsolete, or trivial (ROT), and just fifteen percent is used for operations.

Agency managers need to be aware of how much data they have, where it is stored, who has ownership and what the data’s purpose is. Migrating data that is virtually useless can result in high storage costs. With greater data visibility, data with limited value can be moved to second or third tier resulting in low cost storage and avoiding first-tier cloud storage and egress costs.

2. ELIMINATE DATA PROTECTION SILOS

Shifting workloads to the cloud raises concerns about how it will be protected and whether data protection should be unified under a single platform and cloud agnostic solution. Leveraging a unified data protection platform – rather than costly and disparate point products – allows agencies to effectively protect workloads across on-premises and cloud environments.

3. PRIORITIZE DATA REGULATORY AND COMPLIANCE ISSUES

Routine requests for information, such as an audit, FOIA request, or eDiscovery often result in time-sensitive searches and retrieval efforts. Fragmented data environments, across multiple cloud infrastructures, further complicate this process.

The rapid growth of unstructured data exposes organizations to potentially harmful personally identifiable information leaks. Automated data classification, along with proactive, policy enforcement against common retention requirements, supports an enterprise approach to data governance and drastically increases the speed, accuracy and efficiency of information requests.

4. LEVERAGE SOFTWARE-DEFINED STORAGE

New technologies, like the Internet of Things (IoT), multiply organizational data granting agencies the opportunity to use this data to improve program performance and constituent experiences. But, addressing data storage needs across multi-cloud environments for both transactional and analytic workloads can be challenging, since connection protocols, performance requirements and capacity needs can vary so greatly.

Software-defined storage can pool existing storage resources for specific processing requirements and extend storage tiers to the cloud to optimize for cost and performance. It breaks the dependency on the underlying storage platform, enabling agencies to choose whatever appropriate, cost-effective hardware meets their needs.

5. ENABLE WORKLOAD MIGRATION/PORTABILITY

Most organizations do not give enough thought to how they would fall back from the cloud or change providers. The motivation for a multi-cloud strategy is to take advantage of best-of-breed cloud services, avoid cloud lock-in, and have an insurance policy against cloud failure.

Conclusion

As agencies migrate to multi-cloud and hybrid IT environments, data is everywhere. It's in a traditional data center, and both private and public cloud environments. Consequently, application and data portability between cloud environments is critical. These capabilities must be architected into cloud solutions from the beginning. Agency managers should be in discussion with their vendors and CSPs to understand what it takes to move between clouds – for business continuity, for data transfers, or to avoid vendor lock-in.

Additionally, agencies should consider a comprehensive data management approach for data protection, application uptime, and business continuity. Agencies must understand what data they have and where it is located so if managers receive oversight, FOIAs, eDiscovery or reference management requests, they can find the data irrespective of what environment it is in.

"All these things are better when you think about data management in a holistic way, a comprehensive approach" that gives you greater data visibility, data discovery, data protection, data backup and data recovery, Alboum noted.

CASE STUDY DHS

DHS's Approach to Cloud Migration — Challenges and Tactics

The Department of Homeland Security is taking a holistic approach in its cloud journey.

There are many different aspects to consider — standardization, acquisition, organizational readiness, governance, and the reality that the departments' two main enterprise data centers — DC1 and DC2 — have contracts that are expiring in 2020.

"That's a real driver for us in terms of transforming our infrastructure. At the center of this is security, and that's by design," said Kshemendra Paul, cloud action officer and deputy director of the Strategy and Mission Information Sharing and Services Office within The Department of Homeland Security's Office of the CIO.

DHS's move to the cloud will help component agencies operate more efficiently as they fulfill mission objectives. However, it is also in response to government-wide mandates that are well understood, such as Presidential Executive Orders, The White House IT Modernization Report, The President's Management Agenda, and developing cloud Continuous Diagnostic Mitigation guidance.

"All of these [mandates] are underlying a more managed approach as we move to the cloud. We think that with that more managed approach, we can quantify benefits in advancing the mission by increasing agility and speed, by improving cybersecurity. And there's the potential to do that," Paul said.

As DHS moves to the cloud, the department is also modernizing its network, One Net. That's in line with the government wide effort to move to Enterprise Infrastructure Solutions (EIS), the next-generation telecommunications contract vehicle.

"It is also giving us an opportunity to better update the network, update the posture to be more cloud ready and integrate more modern concepts into our network. There's also a push on Security Operation Centers (SOCs) consolidation," he said. "It's starting with a push towards sharing and having more compatible and eventually standardized operating procedures in the different SOCs, which would support efforts advancing towards more integrated instrumentation, including cloud CDM" [Continuous Diagnostics and Mitigation].

Security is the number one area where the various DHS agencies and programs across the board see opportunity to improve. Consequently, security is a critical focus going forward. DHS senior management is being more intentional and upstream about how the department handles security.

"So how is DHS going to make this happen? The bottom up move of the components to the cloud is broad based, driven by the marketplace, driven by opportunities that individual programs need to improve their service delivery and cost structure," Paul explained. To that end, DHS is standing up a cloud steering group chaired by the undersecretary for management. The different chief experience officers, chief financial officers, and senior management from the component agencies sit on the cloud steering group. "The chief information officer is the executive secretary and I'm the cloud action officer supporting the CIO to operate this governance structure," Paul said.

DHS headquarters were able to get a better sense of the challenges the components face in this cloud journey by polling and talking with IT managers and the workforce.

Enterprise Guidance: There is a desire to have a consistent strategy that helps bridge what components are doing. This requires developing a common cloud maturity model to help the workforce, teams, and organizations evolve towards a service model.

There is the coming expiration of DHS contracts with DC1 and DC2. "DC1 is a government contractor-operated facility that is going to continue with some evolution," Paul said. DC2 is a contractor-owned, contractor-operated facility. DHS is looking to vacate that facility by June 2020. About 133 FISMA applications are in that data center. Most of the components want to move their applications to the cloud, while others want to move to another data center.

Instrumentation of common security controls, analytics and metrics are critical functions for DHS to maintain an enterprise-wide view on its assets and data to operate as an enterprise and better manage what is being spent on IT.

"That's going to generate a tremendous amount of data. We want to use that data both in real-time and near real-time security and IT operations activities and some level of statistical aggregates," Paul said. In addition, DHS will develop a warehouse to support analytics and data driven improvement of IT service delivery, cost, and performance metrics. Security by design is critical, too. It is important to have security technical controls built in early in the application and system development process, known now as DevSecOps (Development, Security, Operations).

Funding and Acquisition: DHS is looking to implement an enterprise approach to prioritizing limited funding of resources, identifying opportunities for shared infrastructure and shared capabilities. At the same time, DHS wants to approach industry in a more organized fashion to both gather ideas to refine its cloud strategy and to solicit solutions to add to enterprise procurement vehicles. "We think it's important to reinvest savings as we're going along here. There is some expectation of savings. Again, those savings wouldn't be recaptured at corporate. They'd be reinvested at the component and program level to support further optimization," Paul explained.

Workforce: Knowledge about cloud-based development operations and security is a scarce commodity. Developing the DHS workforce from traditional legacy models for IT service development and delivery and cybersecurity towards the more "as a service," higher degrees of automation, is a real challenge. The key for DHS is to build from what it has learned from its early adopters.

Components agencies such as U.S. Citizens and Immigration Services, and U.S, Immigration and Customs Enforcement "are universally recognized within our department as on the leading edge and have successfully implemented component-level shared capabilities and infrastructure," Paul said. Customs and Border Protection, Transportation Security Administration (TSA) and some programs in the Federal Emergency Management Agency (FEMA) are also pathfinders.

"The key to developing the workforce is investing in collaboration to capture those lessons learned and best practices to share horizontally across the department," Paul said. Additionally, DHS management must highlight, at the cloud steering group, the best ideas and learning that have already been paid for and integrate that into plans going forward. "You really use that to color and drive the work to reduce barriers," he said.

Security: The big issue here is the lengthy authority to operate timeline. "That's really a label or a bumper sticker, Paul said, "for a whole series of issues as folks are moving to the cloud, recognizing that policy exceptions or currently in place workarounds need to evolve into some future-state cloud security model.

DHS Tactics: How to Move Forward

DHS is using the cloud steering group to drive better collaboration horizontally at all different levels across the department. The department is setting goals and linking it to accountability with other management processes around policy, resource allocation, budgeting, performance metrics, workforce development, and procurement. DHS senior management is continuing to highlight component leadership in this regard and reinforcing the already existing desire to move to the cloud. Emphasis is being placed on the idea of the Cloud Center of Excellence, packaging the lessons learned and best practices from component agencies and accelerating the movement of that information across the department.

At headquarters, the group that Paul is a part of, also has a good-sized portfolio of applications, in addition to enterprise infrastructure that runs the applications. The infrastructure includes applications based in other lines of business outside of the CIO shop. DHS is aggressively moving that application infrastructure to the cloud.

Finally, DHS is committed to partnering with industry and other federal agencies to source the best knowledge about how to go forward. An example of this is within the department, with aspects of DHS government-wide cybersecurity mission, the Cyber and Infrastructure Security Agency (formerly known as the National Protection and Programs Directorate). CISA's goal is to advance the department's national security mission by reducing and eliminating threats to U.S. critical physical and cyber infrastructure.

"They're running a lot of the protection for the dot gov domain. We're committed to working closely with our partners and DHS' Science and Technology Directorate to align our activities in the nexus of cloud and cybersecurity," Paul said.

"In many ways, my boss feels that we here in the management directorate and CIO, should be a best first customer, as well as we can, for [CISA] and the work they're doing -- bringing our operational expertise and the reality of understanding operations into the policy process around these sorts of issues," Paul said.

Reaching out to the components to find out their biggest barriers before developing strategy is a simple idea, yielding some interesting insights, Paul noted. Security is linked with technical architecture and how it should be secured. They are looking for guidance in forming enterprise and migration strategies. Then there are the workforce, funding and acquisition issues. You would think that funding and acquisition would be an agency's biggest concern. But it was evenly balanced between the four areas – enterprise guidance, funding and acquisition, workforce, and security, Paul said.

"That reflects the fact that the components are already moving – moving to the cloud is seen now as a natural evolution and there's a balance here between enterprise strategy and guidance, engineering around IT architecture and security, and workforce development. All four areas are key to what we must do to go forward," Paul concluded.

www.DLT.com
For further information, contact Dana Suarez
dana.suarez@dlt.com

DLT | VERITAS

www.VERITAS.com/publicsector