It’s Time for the Next Generation of Public-Sector Cloud Management

INDUSTRY PERSPECTIVE

UNISYS | Securing Your Tomorrow®

govloop

Introduction

New cybersecurity mandates. The Modernizing Government Technology Act. External threats from all vectors, and internal hazards from insider threats. Shifting goals, budgets and missions. The Federal IT Modernization Report. The President’s Management Agenda.

Thanks to developments such as these and the need to adjust and respond, the pressure to adopt cloud computing technology is continually increasing in the public sector – and successful large-scale adoption remains elusive. Federal agencies are facing an ever-evolving set of drivers, all while needing to meet cloud-first directives and deliver efficient services to citizens who have rising digital expectations.

Despite this complexity, the public sector is still moving to the cloud at a rapid pace to take advantage of efficiencies, scalability and productivity. There remain, however, a number of barriers that agencies encounter when moving to the cloud. Reworking legacy governance models, addressing training and organizational change and the ability to port existing security accreditations are just a few.

So how can the public sector leap over barriers and successfully – and securely – migrate to the cloud?

The answer lies in selecting the right managed services provider – one that can build a cloud-native governance platform that allows agencies to migrate at scale, ensure cost-effective cloud consumption, govern transparently and effectively and bake security into everything they deliver. That’s where Unisys and Fugue come in. Unisys works with government IT teams to help transform their digital services and move safely and securely to the cloud. Fugue automates cloud operations and compliance for the public sector. With Unisys CloudForte, its new cloud management solution based on Amazon Web Services (AWS), Unisys and Fugue provide the ability for agencies to move to the cloud quickly and safely, with compliance governance processes built in.

“The time is now to offer a next-generation cloud adoption and management practice based on the principles of automation, security by design and continuous compliance,” said Peter O’Donoghue, Vice President of Application Services at Unisys.

To learn more about CloudForte, as well as how agencies can transform cloud operations and compliance, GovLoop sat down with Scott Westenhofer, Cloud Platforms Lead for Unisys; Josh Stella, Co-Founder and CEO of Fugue; and Peter O’Donoghue.

Moving to the Cloud: Still a Challenge for the Federal Sector

Because cloud has become more common, one might think that deployment and adoption of cloud computing is easier than ever in government. But that’s not necessarily so.

“The public sector is still very focused on Infrastructure-as-a-Service in most cloud migration efforts, with small pockets of evolved agencies viewing cloud as more of a platform versus just compute, network and storage,” said Westenhofer. “Additionally, IT teams may not think about how necessary the human factor is in cloud and how they can retrain their workforce to have more of a cloud-native mindset. Finally, federal operations teams need to be thinking more about how their processes can evolve or scale and handle automated change versus traditional ITSM workflow-based change.”

A recent survey by Unisys echoed these thoughts. In its IT Modernization Revolution survey from September 2017, the company polled 200 federal IT decision-makers and found that they are experiencing a number of significant challenges while attempting to drive IT modernization across their agencies – particularly around cloud.

“We found it particularly interesting that the majority of survey participants self-reported ‘unanticipated difficulties’ in adopting cloud services,” explained Unisys’s O’Donoghue in a blog post. “This finding is in line with our own experiences. **Adopting the cloud is a deceptively tricky business.**”

Here are the top 10 challenges Unisys found when it comes to cloud adoption and deployment:

1 There's a lack of understanding of the public cloud "shared responsibility" model – meaning what needs to be managed and by whom for successful IT and cyber ops.

2 Federal IT teams often do not have a practical playbook that helps agencies turn the concept of wanting to move to the cloud into a tangible work plan.

3 There can be a lack of skills and workforce training to effectively plan for and successfully operate workloads running in the public cloud.

4 Concerns around securing government apps and data running in the public cloud and corresponding data ownership still exist.

5 Often teams do not fully understand a FedRAMP package or don't fully trust it and insist on a fresh top-to-bottom security review.

6 Difficulties in making a compelling business case to leadership to justify the cloud migration are common.

7 Challenges in reworking legacy data center-centric, tried-and true-governance models and service management tools to manage the public cloud still exist.

8 Costs associated with paying for two environments simultaneously during a migration are still quite high.

9 Establishing and sustaining contract vehicles that can flex to accommodate innovation of cloud service providers is difficult.

10 Billing and providing a transparent invoice for cloud services that a contracting officer can understand and approve is a perplexing task.

But perhaps the biggest challenge of all is that cloud deployments are often taking place without planning for security from the beginning. This puts agencies at risk for data breaches and compliance violations, and also makes it difficult to attain security accreditations (Authority to Operate). In short, agencies are often leaping into the cloud without a thoughtful plan for how to securely operate their environments once there.

That's where a modern managed service provider comes in. In the following pages, we'll look at how the right managed service provider can help the public sector overcome challenges in thriving in the cloud.

Choosing the Right Managed Service Provider for Your Cloud Journey

Choosing the right technology and cloud is only the first step on your journey to digital transformation. You need to also implement it effectively, and use it strategically to reap the returns.

Making sure your agency selects the right managed service provider (MSP) is another critical step in succeeding in the cloud. An MSP is a vendor that offers managed and professional services that support infrastructure and platform operations and have the ability to deliver cloud-optimized solutions.

So how do you make sure to select the right MSP that will serve your needs?

First, your MSP should have demonstrated mastery of how to operate and deliver the full complement of services on AWS. Such mastery is evident in a combination of the AWS MSP and AWS Government designations. Look also for investments in training a large proportion of the partner's workforce in AWS as evidence of adoption of a cloud-native mindset.

Your MSP should have a proven track record of success in the cloud with other federal customers. Cloud adoption requires a steady and experienced hand. Can your MSP bring large-scale migration and modernization experience to help you minimize your risk and accelerate your success?

It’s important to pick an MSP that is able to provide DevOps and management skills to provision, configure and maintain cloud-based environments so your agency’s cloud can take advantage of automation and efficiency, and minimize disruption to the citizens using your services.

Your MSP should also offer a focus on operational integration. Migration to the cloud is about more than workloads. Your agency’s IT and cyber operational approach needs to be reworked to take advantage of AWS cloud offerings while still enforcing necessary controls to mitigate operational, financial and security risks.

Adopting cloud at scale is a team sport. Your MSP’s approach should be as much about people as it is technology. Look for practical and scalable approaches to transform human capital to embrace a cloud-native mindset, to become practitioners backed by best practices and automation starter kits.

Also, your MSP needs to provide a practical approach for large-scale migration. It should help you to identify and prioritize legacy IT assets to migrate, enabling you to measurably grow your ROI. It should have accelerators to migrate portfolios of applications quickly, reducing risk as it goes.

Finally, and critically, a security-first mindset is key. Your MSP should help you start and accelerate the process of getting and keeping an authority to operate (ATO) in the cloud. It should also be able to make sure that your security compliance processes are automated and that your environment is properly governed and secure.

CloudForte™ Next-Generation Cloud Adoption and Management

Clearly, getting to the cloud can be complicated. Every cloud project and migration effort is unique — even potentially within the same agency or organization. Similarly, the analysis, strategy and planning for cloud implementations will vary. Each aspect of the cloud migration — from business case to security requirements — should inform the selection of the best vendors, tools, timeline and resources to deliver the results your agency and its citizens need.

Unisys is diving into meeting these cloud challenges head-on with the release of CloudForte, its new cloud management solution with AWS.

CloudForte allows for the adoption of a cloud-native governance platform over AWS that enables agencies to move and migrate to the cloud, govern their cloud environment safely and scale it with full confidence that they can meet any security compliance necessary. It provides real-time governance, management and compliance abilities for anybody operating in AWS.

CloudForte supports government IT teams that must meet mission need by offering a highly automated governance framework that assures continuous security compliance without adding undue process weight. The platform also enables cost-effective management of enterprise IT operations, which can help public-sector IT teams work within agile and DevOps environments while still harnessing cloud platform services and enforcing governance and security policies.

"We wanted to be able to give our customers full access to their AWS accounts, so they can use every service available using AWS native interfaces (Management Console, API, CLI, SDK, etc.)," said Westenhofer. "And that's what we're able to do with CloudForte for AWS."

CloudForte for AWS helps public-sector IT teams navigate and excel in the AWS cloud environment in four different arenas: consumption of cloud services; management of services; acceleration of adoption; and transformation to a cloud-native organization.

Consume

Commercial tools don't always meet the unique requirements of federal contracts given government compliance needs. CloudForte's fully automated chargeback system takes all the guesswork out of usage and billing and simplifies federal contracting officers' jobs as they process invoices.

Command

CloudForte plugs the gap in the "shared responsibility" model by providing cost-effective solutions that manage images, backups, logging, monitoring and incident management. The management tooling "speaks" AWS natively, which permits clients to leverage new cloud-native services on the day they are released by AWS. This enables teams to move with speed and agility to solve mission problems without compromising on enforcement of governance and security policy compliance.

Accelerate

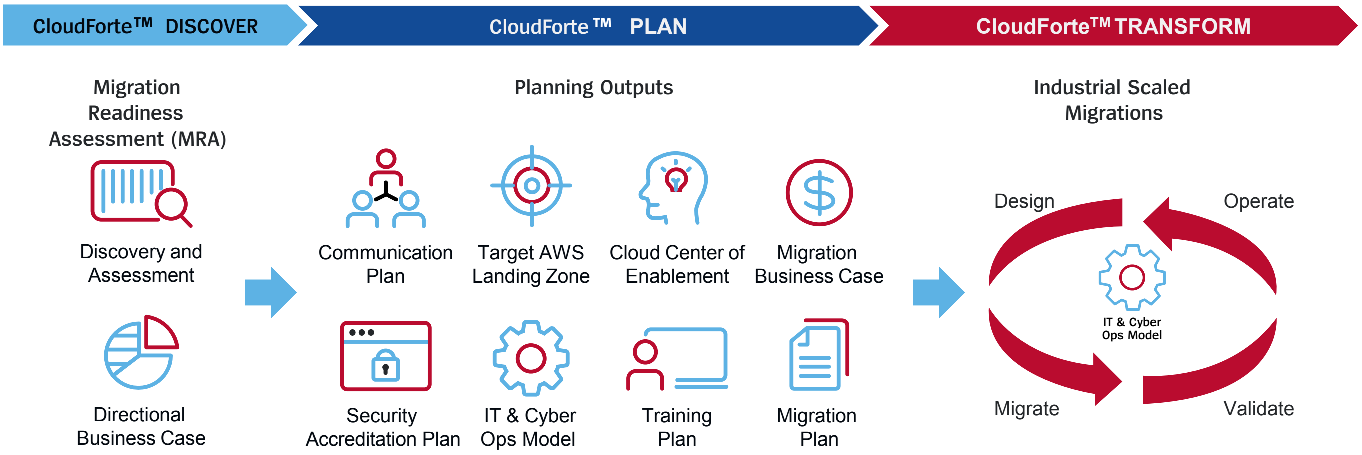
Cloud adoption requires a steady and experienced hand. CloudForte offers an industrial-scale approach to migrate legacy workloads and applications, enabling federal customers to increase return on investment as quickly as possible. This approach to migration ensures agencies can take advantage of the inherent resilience, cost-effectiveness and security offered natively on AWS. CloudForte also addresses the challenge of transforming organizations to adopt a cloud-native mindset and to accelerate the attainment of security accreditations.

Transform

CloudForte provides an industrial-grade modernization of legacy applications, which helps organizations mothball costly, vulnerable applications and divest themselves of predatory enterprise license agreements by tackling the hard migrations with Unisys' advanced migration services.

> “At Unisys, we are committed to helping clients on their cloud journey go fast, securely. Our mission is to provide our clients with the necessary tools for today’s technology and support to deliver better outcomes securely, rapidly and cost-effectively to move to the cloud.”
>
> — Peter O’Donoghue, Vice President of Application Services, Unisys

Accelerating Your Journey to the Cloud



CloudForte™ DISCOVER

CloudForte ™ PLAN

CloudForte™ TRANSFORM

Migration Readiness Assessment (MRA)

Discovery and Assessment

Directional Business Case

Planning Outputs

Communication Plan

Target AWS Landing Zone

Cloud Center of Enablement

Migration Business Case

Security Accreditation Plan

IT & Cyber Ops Model

Training Plan

Migration Plan

Industrial Scaled Migrations

Design

Operate

IT & Cyber Ops Model

Migrate

Validate

The CloudForte™ Approach to Scaled Cloud Migration

- Focused on Rehosting and Replatforming
- Enables Quickest Migration Strategy
- Provides Quickest Time-to-Value
- Minimizes Application Changes
- Upgrades Technical Infrastructure
- Leverages Cloud-Native Features
- Accelerates ATO Adoption

Fugue: Providing CloudForte the Guardrails for Growth

Efficiency, success, a strategic vision and the ability to meet mission need are all critical to cloud migration and deployment. But none of them can or should take precedence over security.

Fugue helps private- and public-sector organizations identify security and compliance violations in cloud infrastructure and ensure they are never repeated. Fugue's patented technology is the only solution that automatically remediates and restores unauthorized infrastructure changes back to a known good state.

With security more important than ever, the public sector must move from manual compliance and security checks to embrace automated, cloud-native solutions for cloud infrastructure. Otherwise, organizations run the risk of deploying an IT infrastructure that is noncompliant and insecure.

Within CloudForte, Fugue enforces the governance processes around provisioning and deployment of Unisys CloudForte service automation to customers' accounts. This in essence means that Fugue, through its automation abilities, supports the "guardrails" that Unisys creates around cloud developments to ensure they occur without risk.

"Fugue won't let you build infrastructure on AWS that doesn't meet compliance and policy standards," said Josh Stella, CEO of Fugue. "If you have NIST 800-53 control concerns, for example, we will tell you where you're getting something wrong, or if you're trying to do something that breaks the rules in your cloud environment."

Additionally, Stella explained, once that environment is deployed to the cloud, every 30 seconds, Fugue examines the environment, and if anything has shifted, changed or if any vulnerabilities have been opened in that cloud infrastructure, Fugue automatically corrects them.

When combined with CloudForte, Fugue's strength is in helping federal agencies run efficient, agile and secure operations in the cloud. When using CloudForte enhanced with Fugue security compliance, agencies can accelerate the Authority to Operate process by providing centralized visibility and control across DevSecOps teams, thereby avoiding policy violations and misconfigurations in the cloud.

By integrating Fugue for security and compliance policy automation and enforcement, CloudForte delivers DevSecOps enablement. Whereas DevOps accelerates operations with infrastructure-as-code and automation, DevSecOps accelerates security with policy-as-code and automation. Now, security and compliance can be integrated alongside infrastructure and feature code for policy validation and enforcement, without slowing down innovation. With DevSecOps with CloudForte, security and compliance become innovation enablers.

"Human error is far less likely with Fugue's infrastructure governance automation technology," Stella said.

"One of the reasons we're so excited to partner with Unisys and AWS is that we really believe this is the right way to do this," Stella concluded. "And the right way to do this is to put controls and automation in place, so that federal customers are safe going to the cloud, but don't cut themselves off from all this new innovation that is coming out of AWS."

With security more important than ever, the public sector must move from manual compliance and security checks to embrace automated, cloud-native solutions for cloud infrastructure.

Conclusion

Building cost-effective, flexible and secure cloud platforms is difficult enough as it is. Doing cloud right is even more challenging given the ever-increasing demand from government agencies facing challenges related to legacy IT, complexity, cost and an evolving set of regulations that complicate governance.

But where some may see cloud adoption as a challenge, with the right partner, cloud adoption also represents a major opportunity to deliver government services more flexibly, securely and cost-effectively. Cloud technology is still the best way forward for efficiency, security and innovation and is the go-to platform of choice for agency CIOs driving digital transformation. Agencies just need to make sure they have the right cloud managed service provider – one that removes the risk from large-scale adoption and ongoing IT and cyber operations.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 270,000 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

About Unisys

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most demanding businesses and governments on Earth. Unisys offerings include security software and services; digital transformation and workplace services; industry applications and services; and innovative software operating environments for high-intensity enterprise computing.

For more information on how Unisys builds better outcomes securely for its clients across the Government, Financial Services and Commercial markets, visit www.unisys.com.

About AWS

With over 2,000 government agencies using AWS, we understand the requirements US government agencies have to balance economy and agility with security, compliance and reliability. In every instance, we have been among the first to solve government compliance challenges facing cloud computing and have consistently helped our customers navigate procurement and policy issues related to adoption of cloud computing. Cloud computing offers a pay-as-you-go model, delivering access to up-to-date technology resources that are managed by experts. Simply access AWS services over the internet, with no upfront costs (no capital investment), and pay only for the computing resources that you use, as your needs scale.

To learn more about AWS, visit https://aws.amazon.com/government-education/government/

About Fugue

Fugue finds security and compliance violations in your cloud infrastructure and ensures they are never repeated. Fugue knows what is supposed to be running in your cloud environments, and if anything changes, Fugue returns things to their original state. The company has eight patents granted and 16 pending. Privately held and headquartered in Maryland, Fugue's investors include New Enterprise Associates, Future Fund, Maryland Venture Fund, and Core Capital Partners. Gartner named Fugue a Cool Vendor in Cloud Computing 2017.

To learn more about Fugue, visit www.fugue.co.

govloop

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

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

www.govloop.com
@GovLoop