Solving the Cloud Conundrum:

Security, Procurement, Workforce

govloop

Table of Contents

Executive Summary

Cloud is undeniably powering major advancements, such as enabling digital documentation for faster workflows, in governments everywhere. But the fact remains that many agencies aren't adopting cloud efficiently or effectively.

The reason? Agencies at every level are struggling with three key areas around cloud: procurement, security and workforces. To help them address these potential hurdles, the Office of Management and Budget (OMB) released the Cloud Smart strategy in October 2018.

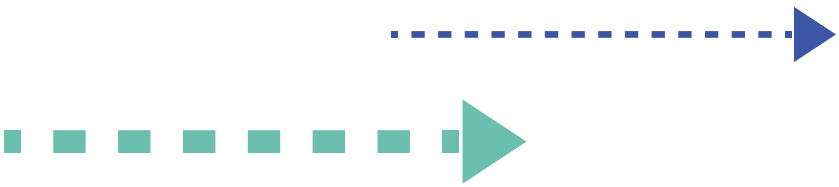
Cloud Smart helps organizations prepare for implementing cloud. It differs from earlier federal cloud strategies by urging agencies to carefully consider procurement, security and workforces before investing in the technology.

And although Cloud Smart focuses on federal agencies, many of the same challenges exist for state and local organizations.

Still, state and local organizations are also making significant progress. The government of Oakland County, Michigan, for instance, is reaping major returns from its G2G Cloud Solutions program. More than 100 agencies use the service, which provides free, cloud-based processing for online and over-the-counter payments. Launched in 2011, the initiative now brings in about $2 million annually in county government revenue.

Agencies that effectively deploy cloud save energy, time and money. Smoothly launching cloud also allows agencies to deliver public services to citizens more easily.

If your agency is experiencing friction during its cloud journey, GovLoop is here to help. This guide explains the role that procurement, security and workforces play in cloud adoption. We also debunk some of the myths about cloud. Additionally, we'll provide you with the facts your agency needs for actively starting cloud services. The less effort your agency expends on cloud, the more it can invest in achieving your mission.



How to Use This Guide

Cloud Smart addresses federal agencies, but it's a strategy with useful wisdom for state and local governments too. To understand why Cloud Smart inspired this guide, think about the following ideas:

1

Consider some common cloud myths

Is cloud always the answer? Is cloud always secure? Does cloud require new skills? Do you always own all your cloud? The answers to these questions will help you understand how cloud can best help your agency.

2

Put cloud procurement front and center

Cloud Smart's focus on procurement isn't just about buying cloud; the strategy is also about understanding the buying process. Cloud Smart explains what cloud models are available, what contracts can help your agency purchase them and how to create the cloud contract that best meets your organizational needs.

3

Don't skip cloud security

Cloud Smart takes cybersecurity seriously, and so should you. It's a policy that makes security integral to cloud-based IT modernization. More practically, Cloud Smart recounts the federal government's cybersecurity initiatives to provide agencies at every level with advice on the topic.

4

Work for your workforce on cloud

Cloud Smart discusses identifying skill gaps for current and future work roles impacted by cloud. The policy also addresses reskilling and retaining current federal employees and recruiting and retaining talent to address those gaps. Cloud Smart finally talks about communicating, engaging and transitioning with employees to cloud.

Industry Spotlight

Hybrid Cloud's True Business Value to Agencies

An interview with Chris Sexsmith, Cloud Practice Lead for Emerging Technologies, Red Hat

The clock's always ticking against agencies that deliver public services. Citizens want private-sector speed from their governments and are impatient with those that can't deliver.

Fortunately, modern hybrid clouds leveraging Software-as-a-Service (SaaS) can help agencies keep pace with these demands in ways that aging IT infrastructures can't. Hybrid clouds deliver services both virtually and with physical, on-premise technology. SaaS, meanwhile, delivers easily accessible products and services using cloud.

Regrettably, agencies nationwide are struggling with legacy tools that once met their needs but can no longer accomplish their missions. These organizations are also spending energy, money and time on systems that are only growing older.

For example, agencies have long relied on virtual machines (VMs) for reducing costs and saving space. VMs imitate physical computer systems virtually using hardware, software or both. Although useful, VMs are increasingly too slow for agencies because they are naturally heavy, imitating a complete operating system (OS) at every turn.

To understand how agencies can ultimately realize their true business value with SaaS hosted in hybrid clouds, GovLoop spoke with Chris Sexsmith, Cloud Practice Lead for Emerging Technologies at Red Hat. Red Hat is an open source software solutions provider.

Traditionally, Sexsmith said, agencies have invested large amounts of manpower and time setting up VM architectures. "Everyone's experienced the pain of requesting a VM and waiting days, weeks or months to get it," he said.

In contrast, Sexsmith noted, modern cloud frameworks present a lighter effort for workers to create and test ideas and features. Cloud also works with more agility, flexibility and scalability than VM and other legacy technologies.

Because cloud comes in many varieties, choosing the right one is hard for agencies. Due to the model's agility and speed, Sexsmith recommends leveraging SaaS whenever possible for agencies.

Not every agency can use all SaaS services, however, and the federal variety is especially limited. This is because of the Federal Risk and Authorization Management Program (FedRAMP), which standardizes federal security assessments, authorization and continuous monitoring for cloud products and services.

"The beauty of SaaS cloud services is that agencies are able to offload the service's development and maintenance to the cloud provider directly," he said.

According to Sexsmith, container frameworks are used to quickly set up development environments and run infinitely scalable applications, both on-prem and in the cloud. These frameworks help agencies rapidly deliver services and innovate new ones.

Ultimately, hybrid clouds can help agencies balance their legacy and modernized technology more easily.

"Red Hat's goal is to partner with you in building secure, agile, modern hybrid clouds with no workloads left behind on the journey," he said. "We can help you not only expose but exponentially increase your business's true value."

"The beauty of SaaS cloud services is that agencies are able to offload the service's development and maintenance to the cloud provider directly."

– Chris Sexsmith, Cloud Practice Lead for Emerging Technologies, Red Hat.

Main Takeaway

It's not too late to start realizing your agency's true business potential with hybrid cloud and SaaS.

State Government Cloud Policies

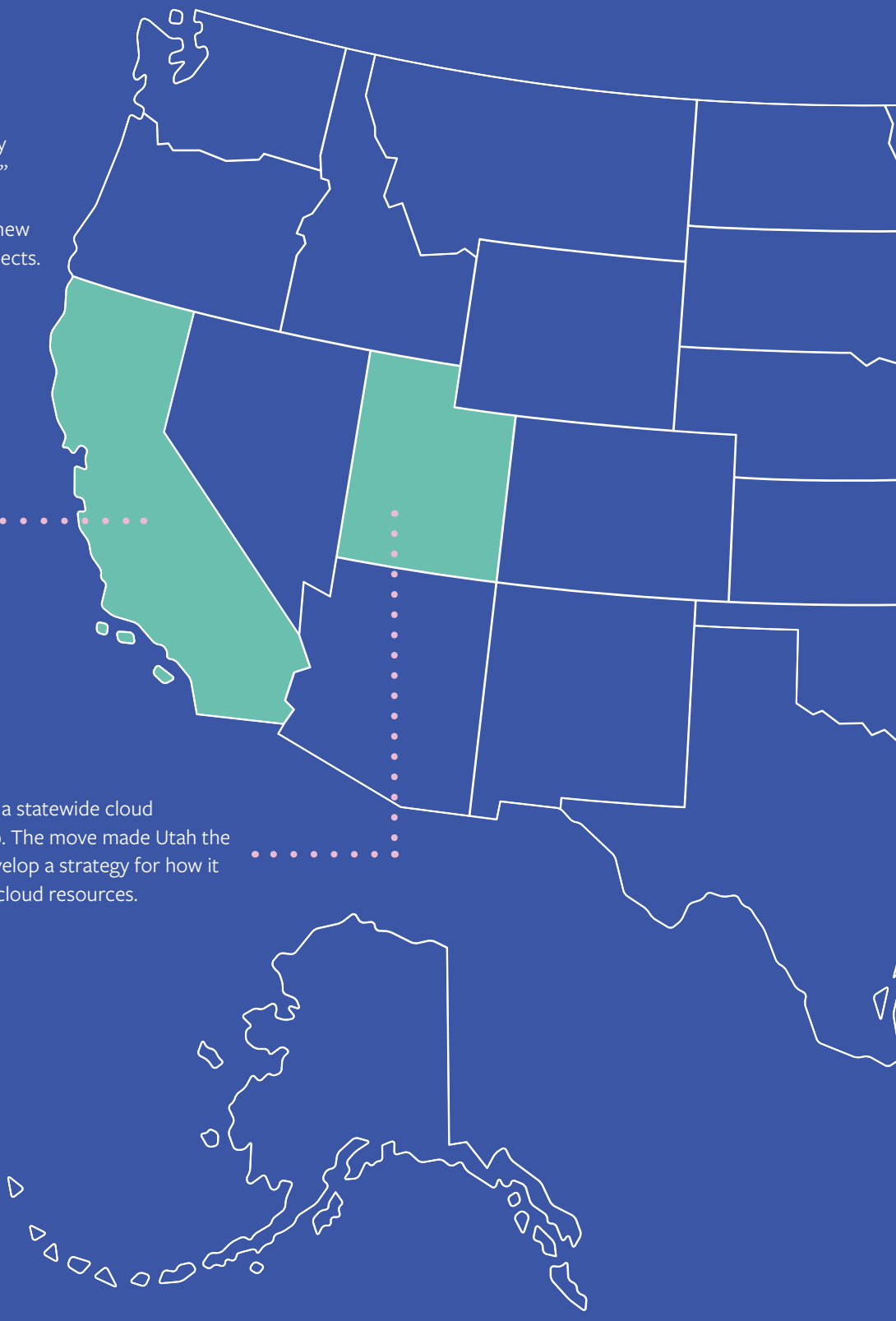
Cloud has spread across the nation in recent years as more state governments adopt the technology. This map displays some of the state governments with clear cloud policies for their agencies.

California

California's Department of Technology (CDT) created the state's "Cloud First" policy in 2014. The policy directs state agencies to shift toward cloud for all new reportable and non-reportable IT projects.

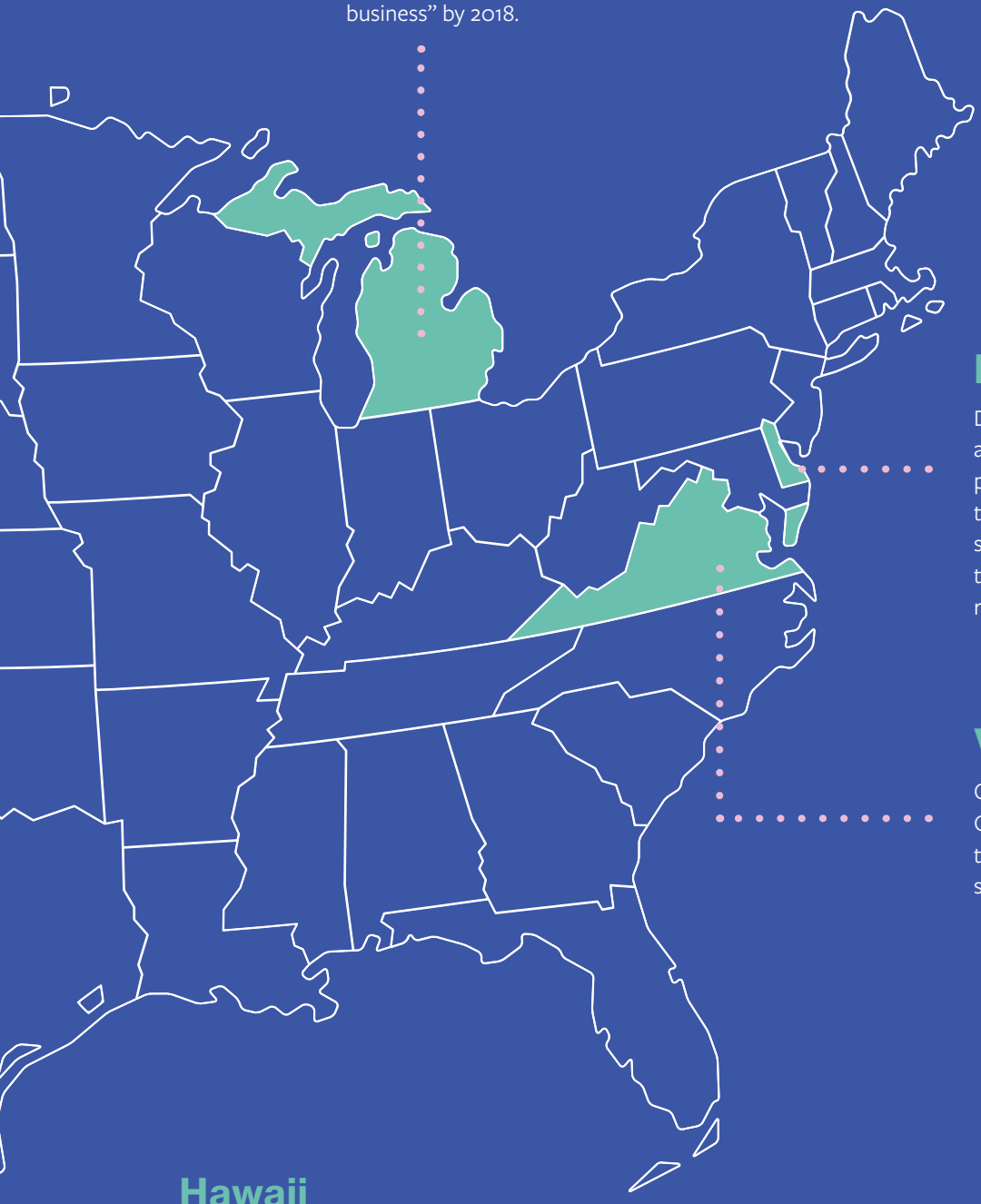
Utah

Utah developed a statewide cloud strategy in 2009. The move made Utah the first state to develop a strategy for how it would leverage cloud resources.



Michigan

Michigan's Department of Technology, Management and Budget (DTMB) included "Cloud First" language in its 2014 "Digital Strategy." The strategy said that "Cloud First" would be the state's "way we do business" by 2018.



Delaware

Delaware's Department of Information and Technology (DTI) created the state's private cloud system in 2009. Since then, DTI has virtualized 80% of the state government's physical servers into this cloud and continues work on the remaining 20 percent.

Virginia

Gov. Ralph Northam (D) signed Executive Order Nineteen into law in 2018, ensuring that Virginia's agencies use cloud for the state's IT services.

Hawaii

Hawaii's "Cloud First" policy launched in 2014, stipulating that state agencies begin using the Hawaii Government Private Cloud (GPC) for all new IT projects. The policy also mandated that Hawaii's agencies migrate their existing applications to GPC, whenever possible.

FIREEYE™

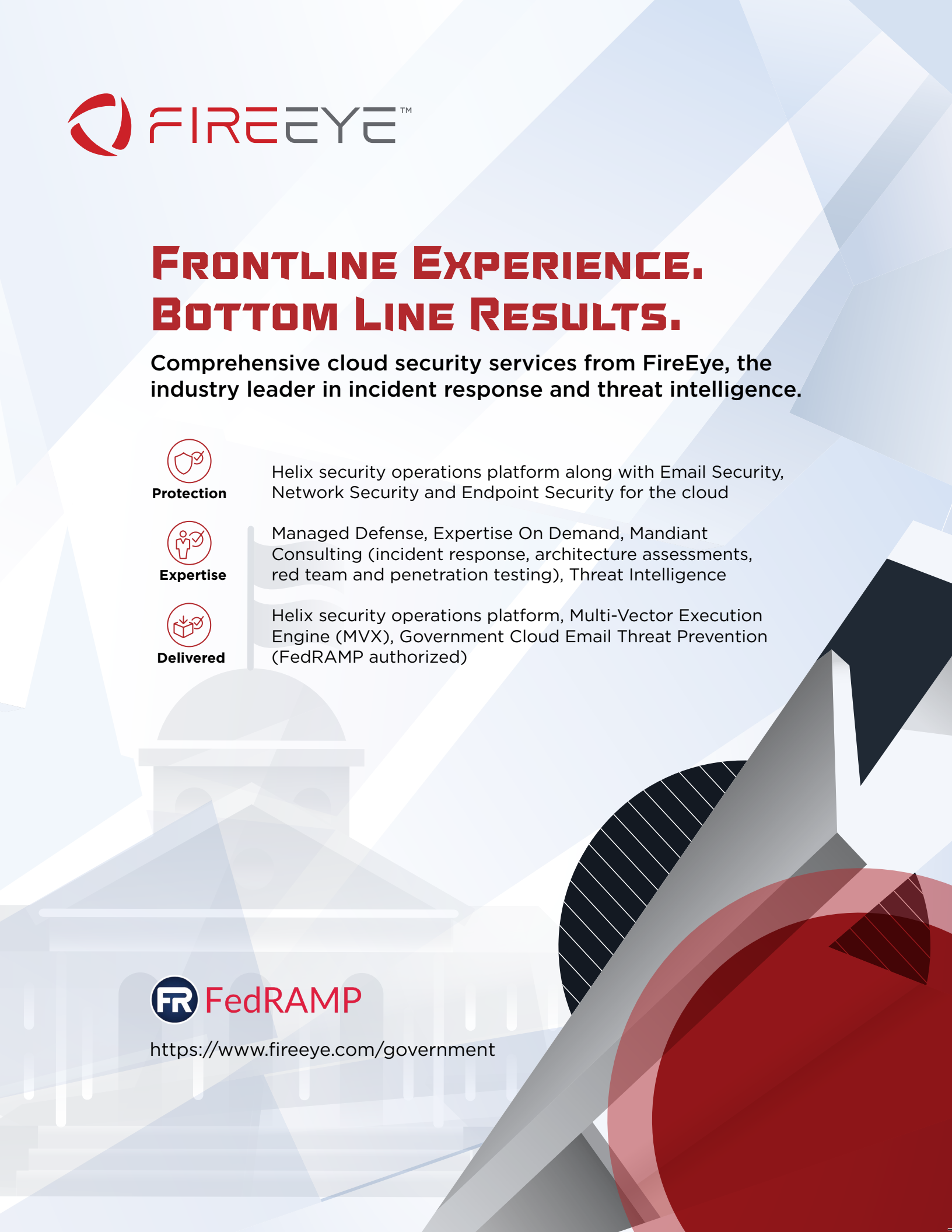
Frontline Experience. Bottom Line Results.

Comprehensive cloud security services from FireEye, the industry leader in incident response and threat intelligence.

Protection
Helix security operations platform along with Email Security, Network Security and Endpoint Security for the cloud

Expertise
Managed Defense, Expertise On Demand, Mandiant Consulting (incident response, architecture assessments, red team and penetration testing), Threat Intelligence

Delivered
Helix security operations platform, Multi-Vector Execution Engine (MVX), Government Cloud Email Threat Prevention (FedRAMP authorized)



FedRAMP

https://www.fireeye.com/government

Industry Spotlight

Managing Your Risk in the Cloud With Key Controls

An interview with Tim Appleby, Director of Federal Programs, FireEye

Cloud computing can provide significant returns on investment and potential cost savings, but it may also represent a significant risk without proper oversight. Although cloud services are relatively secure, agencies are hesitant to adopt the technology as it can potentially place their critical assets and data in harm's way. At issue is who owns what in the cloud, how much control agencies have over their critical assets, and what duties cloud providers are responsible for.

The reality is that cloud vendors can't shield government assets from every risk. Although cloud service providers acknowledge many responsibilities regarding their customer's data and asset protection, the customer is still accountable for their infrastructure and retains many oversight and operational responsibilities.

Ultimately, public and private sector partners must better prepare for these risks by incorporating the same key controls used for managing risks for their traditional on-premise infrastructure in the cloud. Key controls represent methods for managing vulnerabilities and reducing and mitigating risk.

To understand how agencies and their cloud providers can partner on security, GovLoop spoke with Tim Appleby, Director of Federal Programs at FireEye. FireEye is a cybersecurity solutions provider that helps agencies establish the appropriate key controls and oversight customers need to properly mitigate their risk when migrating to cloud providers. "Ultimately, FireEye's approach is to assess a customer's readiness to move to the cloud, assess their risk in doing so, and determine the best solution for the customer based on the resulting return on their investment" he said.

Appleby said that agencies must first assess the key controls protecting their infrastructure, develop oversight for maintaining those measures, and understand their responsibilities in the relationship before moving to a cloud provider. Although a cloud option may seemingly offer significant cost benefits, compensating for the loss of critical controls may offset those savings.

So how should agencies ensure they're on the same page as their cloud vendors? Appleby recommends service level agreements (SLAs). SLAs are included in contracts between agencies and cloud providers. These agreements ensure that agencies get the level of quality they expect from their cloud providers and can audit their cloud's performance accordingly. "Many customers feel that because of their service provider's size, that provider won't change their terms," Appleby said. "But that doesn't always hold true. They're going to bend over backward to get your business."

Overall, agencies must recognize cloud's shared responsibility paradigm. The shared responsibility paradigm concerns the duties that agencies and their service providers share when protecting resources in the cloud. By considering both accountability and responsibility, applying effective and measurable key controls, and ensuring success through periodic oversight, cloud risk can be mitigated to an acceptable level.

"Many customers feel that because of their service provider's size, the provider won't change their terms. But that doesn't always hold true. They're going to bend over backward to get your business."

– Tim Appleby, Director of Federal Programs at FireEye

Main Takeaway

The key to cloud risk mitigation depends on the customer's understanding of their responsibilities, integration and oversight of their key controls, and adoption of available compensating controls to reduce risk to an acceptable level.

1

MYTH #1

Cloud Is Always the Answer

Cloud's versatility makes the technology capable of tackling such diverse problems as citizen engagement, data storage and supporting emerging technologies. Despite this, the notion that cloud always solves agencies' problems is a myth. **The reality is that organizations should only use cloud when it's the best choice for their needs.**

In truth, cloud adoption either helps or hinders agencies based on the choices that organizational leaders make. Subsequently, cloud is the best answer for agencies that carefully prepare for the technology before making it their own.

Michael Valivullah said that he's seen cloud's unpredictability working as CTO of the Agriculture Department's (USDA) National Agriculture Statistics Service (NASS).

"USDA isn't totally in the cloud as we wanted to take a good, risk-based journey to get there," he said during a December 2018 GovLoop roundtable. "It's hard to coordinate all the components within USDA. We're one of the biggest agencies in the federal government."

Valivullah said that USDA's cloud journey immediately included security, a concern that other agencies should share.

"We're trying to classify the data based on the sensitivity," he said of USDA's solution. "For example, we have put email into the cloud because the data is not that sensitive."

Valivullah said that USDA's leaders ultimately recognized that the agency couldn't safeguard its data without private sector help.

"There's a shared responsibility for security," he said of USDA and the agency's cloud provider. "Quite often it's the customer or client who's not identifying the security gap. Agencies need to understand where the gaps are."

Despite this, Valivullah noted that agencies must realize their role in cybersecurity before trusting cloud service providers with that role.

"You need to classify the level of sensitivity of your data as a client," he said. "You also need to determine access. If there are holes in the application, you can't blame the cloud service provider."

Valivullah also said that regardless of the provider involved, agencies must decide who can access their data before putting the information into cloud. For example, he said, agencies shouldn't allow unlimited data access to employees who lack the training for handling such information.

Security isn't the only barrier to cloud adoption, however. According to Valivullah, agencies might not be ready for cloud if their workforces aren't either.

"There are people afraid of the change," he said. "They're afraid that they're going to lose their jobs. This is change management. Cloud has to come very clearly from the management, and it has to come very clearly at every level."

Cloud might not be the answer for agencies who have not prepared their budgets, workforces or security measures for the technology. Valivullah said that agencies must take charge of these or other potential sticking points before adopting cloud.

"Governance is very important," he said. "If you're not governing what's happening around you, it's a free-for-all. Some agencies want to do everything by themselves. You want people you know and trust to be allowed in."

Valivullah acknowledged, however, that cloud's agility, efficiency and security has greatly aided his organization's mission. Cloud's value, he argued, will ultimately win over agencies when they're ready for the technology.

"What are the challenges and what are the opportunities with cloud?" he asked. "Adapt, adjust and learn. Cloud's here, it's going to be here and it's the future."

Case Study

Los Angeles' long road to the cloud demonstrates why the technology might not fit agencies until they're ready for it.

For example, Los Angeles announced in March 2019 that it would adopt cloud after preparing for five years. At the time, Los Angeles agreed to transition from the city's mainframe to CDT's state data center in Sacramento.

Los Angeles' announcement said that the move became possible after city and state IT officials finished prepping key public safety workloads for the switch. The city also cited increasing difficulty recruiting people to work on its aging mainframe. Los Angeles additionally listed cost savings and the state's purchasing power as factors in the decision.

Motivations such as these are among the many reasons that governments avoid cloud. For agencies considering cloud, caution is key. The organizations that successfully embrace cloud do so only after considering their budgets, personnel and security first.

Best Practices

1. Understand your agency's financial and human capital costs before migrating from legacy IT to the cloud.

2. Determine whether cloud is the answer for all, some or none of your agency's IT needs by gauging how well your legacy systems are already handling those responsibilities.

3. Take time adopting cloud to ensure that public services are rarely disrupted during the transition.

Key Stats

$500k In fiscal 2018, smaller agencies were saving $500,000 annually if they had adopted cloud-based collaboration solutions.
Source: The White House

$10m In fiscal 2018, larger agencies such as the Justice Department (DOJ) were saving $10 million annually if they had adopted cloud-based collaboration solutions.
Source: The White House

22% National governments spent 22 percent of their IT budgets on cloud in 2018.
Source: Gartner

600 State and local governments issued 600 cloud purchase orders (POs) monthly in 2017.
Source: DiscoverOrg


Data Integrator
Reporting
Data Mart
Amazon Redshift
AMAZON QUICKSIGHT
Business Users
CAPACITY
DATA
FREEDOM TO
INNOVATE
Data Integrator
+
Big Data
Dev DW
Amazon Redshift
SQL
ETL
Amazon Athena
Data Lake
Amazon S3
Data Analysts
+
Data Scientists
AMAZON REDSHIFT
C-SAT
The federal government trusts the cloud with the
most functionality, innovation, and experience.
aws is how
www.BuildOn.aws

Industry Spotlight

Changing the Game in a New Way with Cloud

An interview with Brett McMillen, General Manager, U.S. Federal Civilian and Ground Station, Amazon Web Services (AWS)

Cloud has been changing the game in government services for over a decade now. Whether it's helping agencies innovate more quickly, be more efficient, save money, or provide better services, the public sector has embraced cloud computing as a way to modernize both their technology and the ability to connect with citizens.

To learn how government is using cloud to innovate in increasingly new ways, GovLoop sat down with Brett McMillen, General Manager, U.S. Federal Civilian and Ground Station, Amazon Web Services (AWS), a leading provider of government cloud services.

When cloud first entered the public sphere, many viewed it as an inexpensive and more efficient way to compute and store data. It still does that, McMillen explained, but he's seen agencies begin to use cloud-native solutions to do more than was previously possible.

"This is a really exciting time to be in government IT, because the number of solutions that are out there, or the number of tools that an IT organization can utilize, has increased dramatically over the last several years," he said. "And a lot of that has been driven because cloud computing makes it easier for these innovators to come up with a software solution and make it available to the customers."

The Veterans Affairs Department (VA), for example, used cloud computing to increase uptime and improve user experience. Over at the Centers for Medicare & Medicaid Service (CMS), staff used cloud for robust data migration and deriving measurable benefits. And the team at healthcare.gov used cloud to deliver a stable and highly scalable set of features capable of handling hundreds of thousands of simultaneous users during peak insurance signup periods.

Now, AWS is taking these cloud services to space, with their new AWS Ground Station service.

Using AWS and AWS Ground Station, agencies can streamline their current satellite data workflows, rapidly experiment with new applications, and deliver products to market faster without the constraints of long-term contracts for infrastructure. Using AWS Ground Station, customers can save up to 80 percent of their ground station costs by paying for antenna access time on demand, and they can rely on AWS Ground Station's global footprint of ground stations to downlink data when and where they need it.

Government uses satellites for a wide variety of use cases, McMillen said, including weather forecasting, surface imaging, communications, and video broadcasts. Ground stations are at the core of global satellite networks, which are facilities that provide communications between the ground and the satellites by using antennas to receive data and control systems to send radio signals to command and control the satellite.

"Today with cloud computing, you're able to quickly and easily get access to best-of-breed technologies and deploy them in near real time," McMillen said. "Cloud computing could solve federal IT's challenges in ways they never could before, and it's really only limited by their imagination."

"Satellite data and imagery today is being used increasingly in a wide variety of applications, from environmental research to scientific studies, security operations, media, and it's being used widely throughout the federal government."

– Brett McMillen, Director, U.S. Federal Amazon Web Services

Main Takeaway

Using the AWS Cloud and AWS Ground Station, agencies can streamline their current satellite data workflows and rapidly experiment with new applications without the constraints of long-term contracts for infrastructure.

2

MYTH #2

Cloud Is Always Secure

One of the most hotly contested myths about cloud involves the technology's security. Is cloud always secure? **Although cloud is undeniably more secure than legacy IT, the reality is that it's a tool that's still vulnerable under certain circumstances.**

Security matters as governments have good reason to worry about their data. The public trusts agencies to protect their sensitive information, and citizens distrust them when they fail.

Cloud isn't safe from this anxiety, however, and security concerns have long dogged the technology. Although cloud typically protects data well, the tool isn't immune to human error.

"We should be in cloud only to enable the mission," said Dave Otto, engineering support for the Homeland Security Department's (DHS) Continuous Diagnostics and Mitigation (CDM) program, during a December 2018 GovLoop roundtable. The CDM program provides ongoing cybersecurity and risk assessments for government networks and systems. "The cloud is as secure as we need it to be or we make it."

For example, Otto said, an insecure data container could leave even the most secure cloud vulnerable to cyberthreats. Otto also warned that many agencies are often set in their ways, focusing on reactive security measures rather than a proactive, risk-based approach involving cloud. Many agencies aren't aware of their assets, he added, which leaves them unprepared for calculating the risk facing those assets.

Whether or not cloud is involved, Otto urged governments to expect the unexpected from security. For example, he said that many agencies were surprised by Edward Snowden's actions in 2013. Snowden, then a National Security Agency (NSA) contractor, leaked highly classified intelligence about one of the agency's controversial surveillance programs.

"What's the likelihood of a Snowden?" Otto asked. "There are those black swan events that we need to prepare for."

According to Dictionary.com, a "black swan" event is "an occurrence or phenomenon that comes as a surprise because it was not predicted or was hard to predict."

Agencies that don't practice unending vigilance are more likely to miss such incidents regardless of whether they use cloud.

DHS's CDM program is one of the many initiatives that help agencies practice stronger cybersecurity using cloud and other technologies. Although Otto acknowledged that CDM improves cybersecurity, he noted that just complying with the program isn't enough.

"We fear the auditor more than we fear the adversary," he said. "We need to get out of the compliance mentality and start thinking about how we involve leadership. We need good communication with the stakeholders."

Otto additionally recommended that agencies select cloud vendors that are renowned for robust cybersecurity. One caveat to this suggestion, he continued, is that vendors are not solely responsible for safeguarding agencies' information.

"It's not their data," he said. "It's not their users. Why is it their risk? We'd like to see better communication across tiers to understand appetite and risk in government."

Speaking at the same GovLoop roundtable in December 2018, Keith Trippie suggested that agencies wary of cloud's security measure the technology's protections against their own. Trippie is DHS's former Executive Director for Enterprise System Development. According to Trippie, agencies should test whether cloud or legacy IT is more secure and then place their data in the better option.

Case Study

The cybersecurity standards that FedRAMP offers suggest that cloud can shelter government data for years to come.

FedRAMP began in 2012 with the goal of standardizing the federal government's security assessment, authorization and continuous monitoring of cloud products and services. The program reached a major milestone in May 2018, when FedRAMP authorized the 100th cloud service provider (CSP) for federal agencies.

Authorized CSPs meet FedRAMP's baseline requirements for securely protecting federal information. FedRAMP authorizations are vital for securing the vast amounts of sensitive data the federal government handles. For context, federal agencies cover a third of the world's internet connections, making the security of those connections paramount. Subsequently, the number of FedRAMP-authorized CSPs means there are now 5 million assets available for federal organizations to use for cloud services.

FedRAMP's fortifications are shielding state and local agencies' clouds, too. For example, CDT began offering FedRAMP Moderate cloud in October 2018. FedRAMP's different levels specify security requirements for cloud vendors based on the sensitivity of data and systems that will be hosted in the cloud. Each level – low, moderate or high – is based on the impact to agencies should their data access points, services or systems get interrupted.

CalCloud's FedRAMP Moderate offering follows the FedRAMP High option the program previously offered.

What's more, making federal clouds securer helps protect the technology for commercial businesses and citizens that rely on services from the same CSPs.

Choices such as these help agencies by providing the level of security necessary for the sensitivity of their data. Data that is moderately sensitive, for instance, does not need high security protections, which would be more expensive and difficult to implement.

Security isn't FedRAMP's only benefit, however. The program also saves money. As of May 2018, FedRAMP has saved agencies $243 million by reusing the program's authority to operate (ATO) certifications. ATOs certify that a system meets federal standards for securely operating IT. FedRAMP's reuse of these benchmarks also saves public servants time securing their agency's ATOs. In turn, this lets government employees focus on serving citizens instead.

Ultimately, FedRAMP gives agencies peace of mind. FedRAMP-authorized vendors are cloud providers capable of helping agencies secure citizen data while those agencies focus on their missions.

Best Practices

1. Practice dedicated cyberhygiene to help keep your agency's cloud secure and free from data handling accidents.
2. Comply with all applicable cybersecurity standards and make sure your cloud partners are following suit.
3. Pick vendors who are renowned for providing secure clouds that can still meet your agency's needs.

Key Stats

Fifty-eight percent of federal senior leaders said in November 2017 that security concerns are their top challenge to consolidating and optimizing their agency's data centers.
Source: Deloitte

Twenty percent of federal senior leaders said in November 2017 that recent advancements in cloud security are driving their agency's efforts to close their data centers.
Source: Deloitte

Twenty-nine percent of state CIOs said that they have shared their cloud security services and monitoring with other government agencies.
Source: NASCIO "2018 State CIO Survey"

Nineteen percent of state CIOs said that they have not shared their cloud security services and monitoring.
Source: NASCIO "2018 State CIO Survey"

Agencies of the US Government:

We salute you. We depend on you, so now let us return the favor. We can help you speed delivery of key services—all with better efficiency and lower costs.

We're all in this together. Don't just take our word for it. See how agencies like yours are succeeding with ServiceNow.

www.servicenow.com/federal

servicenow

Industry Spotlight

Transforming Your Agency's Workflows With Cloud

An interview with Bob Osborn, Chief Technology Officer, Federal, ServiceNow

No government workflow is the same because all agencies have unique missions. Despite this, cloud can improve every agency's workflows by enabling automation and reducing the manual processes for employees.

Agencies are struggling, however, to integrate emerging technologies such as automation into their specific workflows. Automation will enable agencies to perform traditionally manual tasks with minimal human assistance. This tool saves workforces energy and time.

To understand how agencies can make automation fit their workflows using cloud, GovLoop spoke with Bob Osborn, Chief Technology Officer (CTO), Federal at ServiceNow. ServiceNow is a cloud provider specializing in Software-as-a-Service (SaaS) solutions. SaaS delivers centrally hosted software on a subscription basis. For instance, SaaS solutions such as those ServiceNow provides can provide agencies with automated workflows as part of their cloud subscriptions.

Agencies have long struggled with adopting new technologies such as automation because of how long procuring and securing these tools takes. These slow processes have left agencies lagging the private sector in technology upgrades. "IT is always chasing the constant refresh of technology in the workplace," Osborn said. "In the government workspace, this has traditionally been difficult because of the adoption requirements."

SaaS clouds overcome this obstacle by providing a single platform for automating all an agency's data. Ultimately, agencies can tailor their automated workflows by adding the data needed for each. The agency's cloud handles all the organizational data the same, saving time on automating it for workflows. "Everything is interoperable from the beginning," Osborn said.

To see how SaaS clouds help agencies, consider automation's advantages. Organizations automating their workflows reduce the simple, manual work for humans. The result is happier employees who are more capable of satisfying public demands. "You can actually track where you are in the process," Osborn said. "This eliminates a lot of duplicative work and frustration. It changes the entire experience in the workplace."

Osborn said that ServiceNow's SaaS solutions also quickly modernize agencies' operations with cloud applications for workflows such as expenses, payroll and human resources (HR). These clouds can additionally host custom apps that are designed for fulfilling an agency's unique mission requirements.

"In the past, you had to develop legacy systems to accomplish this task," he said. "Integrating data and having interoperability is challenging with siloed applications. It's a huge benefit for agencies to take advantage of this platform approach to transform workflows and improve services."

"Every application in the ServiceNow platform can take advantage of your data because it's been normalized. Everything is interoperable from the beginning."

– Bob Osborn, CTO, Federal at ServiceNow.

Main Takeaway

Agencies can improve their workflows by using SaaS clouds that enable automation and other emerging technologies.

3

MYTH #3

Cloud Doesn't Require New Skills

Cloud's accessibility has generated the myth that using the technology doesn't require learning new skills. **The reality is that cloud presents most government employees with an opportunity to acquire fresh abilities and upgrade their workflows.**

For example, cloud enables digital document storage and electronic signatures to create paperless workflows. Offices that go paperless save energy, resources and time that were spent on paper. Nonetheless, reaching digital documentation's true value requires workers to change their ways.

This reality makes cloud a potentially disruptive technology that can upend established routines. Agencies that ignore cloud's transformational power risk having their employees struggle with the tool. The reality is that agencies that don't know how cloud improves their routines won't use the technology to improve their work.

"Cloud adoption takes a village," Dave Larrimore, DHS's Chief Technology Officer (CTO) for Immigration and Customs Enforcement (ICE), said during a September 2018 GovLoop online training. "Don't bite off more than you can chew."

For instance, end-user employees may find cloud disrupts their routines and tools. Easing them into the technology piece by piece – for example, starting with only cloud-based email accounts – helps them adjust to the technology easier.

Take an agency's communications. The agency's entire component could enter cloud, or workers could move the component in steps. Employees could transfer email, telephones and video to cloud as needed, or all at once. The final choice is the one that best serves the agency's needs.

Larrimore said that for many agencies, cloud adoption requires knowing the best method for readying different parts of their workforces to use the technology.

"A lot of the people who have been there for 40 years, you have to get them to go to training," he said as an example. "A lot of the younger generation, they just need a fun challenge to attack."

DHS's Otto, meanwhile, noted during a GovLoop roundtable in December 2018 that age would likely become a major factor in how agencies prepare their workforces for cloud. "When I entered the workforce, there weren't computers out in the world," he said, noting that cloud didn't factor into his government work until 2010. "It's not like IT has been around for 150 years. Cloud's the world we live in now, and we'll adapt again to the new reality."

Larrimore added that agencies that understand their workforces' unique desires are best suited for launching cloud.

"Do what the people need, not what you want," he said. "Going to the cloud is hard work and requires smart people."

Dan Kempton, Director of Engineering and Cloud Services at North Carolina's Department of Information Technology (DIT), said that agencies must prepare their entire workforces for cloud.

"The internal challenges, cultural challenges, technical challenges, old processes – they all have to change," he said during a GovLoop online training in December 2018. "With internal challenges, agencies and people in those agencies want the cloud now, whether or not they know what they need to do or want to do."

Case Study

The Transportation Department's (DOT) recent efforts preparing its workforce for cloud illustrate how agencies can ready their employees for drastic changes.

DOT created a workforce development program in June 2018 focused on creating a cloud-capable IT workforce at the agency. Run by DOT's Enterprise Cloud Services (ECS) team, the initiative increased the agency's cloud-relevant knowledge and skills.

"When people say, 'Well, what is the end of your plan?' or 'What are you after?' I'm after a culture," then-CIO Vicki Hildebrand told GovLoop in January 2019. "And so, what I'm calling it is our modern IT destination."

DOT's cloud workforce development program began as part of the agency's DestinationsDIGITAL IT transformation initiative. The agency's cloud team began by assessing DOT's cloud skills at the time and then deciding which abilities employees would need in the future. The resulting trainings focused on cloud application migration, engineering, operations and security.

ESC then conducted a Cloud Pre-Assessment Survey aimed at examining DOT's cloud culture. The survey gauged how comfortable DOT employees were with cloud and what else they wanted to learn about the technology.

DOT's research ultimately led to at least two training sessions with a leading cloud vendor, with the first centering on cloud security and instrumentation. The second class, meanwhile, educated participants on the fundamentals of the vendor's cloud.

After that, the program's Phase II started in July 2018 with online trainings for using multiple cloud vendors. The program also provided cloud role-specific training and multiple demonstrations to make DOT employees more comfortable with the technology.

Best Practices

1. Actively communicate all cloud concerns, desires and questions to agency leadership before migrating to the technology.

2. Participate in all available cloud re-skilling and training sessions so cloud's understandable.

3. Take advantage of cloud provided expertise, including Q&As, help desks, tutorials and technical support.

Key Stats

$214 billion

Cloud technologies added roughly $214 billion in value-added to U.S. gross domestic product (GDP) in 2017.
Source: The Internet Association (IA)

2.15 million

Cloud technologies added about 2.15 million jobs to the U.S. economy in 2017.
Source: IA

X3

The economic impact of cloud technologies nearly tripled in the approximately 15 years between 2002 and 2017.
Source: IA

Twenty-two percent of state CIOs said that their agencies have no cloud migration strategy.
Source: NASCIO "2018 State CIO Survey"

THUNDERCAT TECHNOLOGY

vmware®

Complexity Minimized. Performance Optimized.

HELPING OUR FEDERAL GOVERNMENT EASE INTO MODERNIZATION WITH VMWARE'S HYBRID CLOUD SOLUTION

THUNDERCATTECH.COM/PARTNERS/VMWARE/

Industry Spotlight

Hybrid Cloud and the First Step to IT Modernization

An interview with Mike Wilkerson, VMWare Cloud on AWS Specialist for Federal, VMWare; and Nic Perez, Chief Technology Officer (CTO Cloud), ThunderCat Technology

Change can be scary, and many agencies are reluctant to leave their legacy IT behind. Leaders at these agencies often worry that modernizing their IT could drive up their costs or alter their employees' routines.

In recent years, this wariness has become a frequent obstacle to cloud adoption. But the rise of hybrid cloud as a viable option is helping agencies realize that cloud isn't an all-in transformation. Hybrid clouds mix on-premise legacy IT with modernized, cloud-based IT, giving agencies the best traits from each in one package.

To understand how hybrid clouds can help agencies launch IT modernization efforts, GovLoop spoke with Mike Wilkerson, VMWare Cloud on Amazon Web Services (AWS) Specialist for Federal at VMWare, and Nic Perez, Chief Technology Officer (CTO Cloud) at ThunderCat Technology. VMWare is a software virtualization company that provides cloud solutions, while ThunderCat Technology is an IT solutions provider. "Hybrid clouds are attractive as cloud is not a binary, either-or decision," Wilkerson said. "Hybrid clouds allow agencies to put one foot in modernization and it future-proofs agencies, too."

Cloud differs from legacy IT as the former offers services as an on-demand subscription as needed, while the latter provides services continuously. "The challenge with adopting cloud is that agencies don't think about turning things off or how they are able to consume the native services offered by a CSP," Perez said. "They're not used to the elasticity and being able to grow demand."

For proof of cloud computing's scalability, consider Tax Day. Without these capabilities, the IRS must increase the legacy systems footprint each year to meet increased citizen traffic on its websites and via application programming interfaces (APIs). With cloud, the IRS can practically infinitely increase its web services in the days leading up to Tax Day and then immediately reduce them minutes afterward. It's a formula that saves agencies such as the IRS valuable resources, energy, time and ultimately money; it's all automated and much more efficient. "Organizations know where they are today and where they want to go, but they struggle to get there," Wilkerson said. "With cloud, agencies can right-size their environment and pay for only what you consume."

The benefit of hybrid cloud, meanwhile, is that agencies can leverage cloud services without impacting their legacy IT running mission-critical operations. In terms of data, hybrid clouds also let agencies control data they deem too sensitive to host off-premise. VMWare and ThunderCat provide the on-premise hardware and the off-premise cloud services that enable hybrid clouds no matter where agencies' data resides. In turn, hybrid clouds help agencies set the modernization pace that's right for them. "VMware and ThunderCat can help agencies get there," Wilkerson said." We give them a turnkey solution to get from their present state to their future state."

> **"Hybrid clouds allow agencies to put one foot in modernization and it future-proofs agencies, too."**
>
> *– Mike Wilkerson, VMWare on Cloud Amazon Web Services (AWS), Specialist for Federal at VMWare.*

Main Takeaway

Hybrid clouds can ease the growing pains some agencies experience with modernization by combining legacy and modernized IT in one cloud package.

MYTH #4

You Always Own Your Cloud

A persistent myth about cloud is that agencies using the technology own it once their assets become involved. **The reality is that cloud ownership is more complicated, however, due to the technology's largely abstract setup.**

For starters, cloud lacks the same physical presence as earlier IT systems. Cloud's solid boundaries are subsequently hard to define, and many people unfairly compare it to older, more concrete tools.

Cloud's many varieties, meanwhile, further complicate matters. Many of these models involve utilizing cloud on-demand. It's a format that leaves ownership a question of which cloud functions are controlled by agencies, and which are managed by their vendors instead.

These elements mean that ownership ranks among the most confusing aspects of cloud adoption. Managing information, infrastructure and personnel becomes increasingly unclear as more partners share the same cloud services.

Data sovereignty, for instance, is a recurring challenge for agencies partnering with cloud vendors. Both parties handle sensitive citizen data, often leaving the side most responsible for the information's security uncertain.

Trippie, a former DHS official, said that many agencies have found data ownership a sticking point in cloud adoption. According to Trippie, these agencies have resisted adopting cloud as they don't own all the data involved in their version of the technology.

Fortunately, SLAs clarify these and other issues. SLAs are included in contracts between agencies and IT vendors for cloud and other services. In terms of cloud, these agreements determine the performance and service levels expected from the provider. These pacts also decide how the cloud's results are measured and what enforcement mechanisms exist for achieving them.

The Government Accountability Office (GAO) published in April 2016 10 key practices for drafting SLAs for federal agencies' clouds that are valuable for any agency. These measures include:

- Two practices that explain the roles and responsibilities agencies and vendors assume during cloud adoption.
- Five practices that explain how to measure the performance of cloud after adopting the technology from a vendor.
- Two practices that explain how to secure cloud and measure how well-protected the technology is.
- One practice that explains how to enforce consequences for cloud vendors that violate their agreements with agencies and how to penalize these providers.

The cloud model that agencies select while finalizing their SLAs, meanwhile, dictates how much of the technology they own. For many agencies, picking cloud is about deciding what level of control over the technology best suits their missions.

Fortunately, cloud's flexibility means that several models exist for managing the technology's services. SaaS, for example, delivers products and services to agencies using software. In this format, vendors own both the cloud infrastructure and software that agencies use.

Agencies that want more control over their cloud, however, can adopt Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) models. PaaS gives agencies control over a cloud platform, while IaaS provides them with management of the technology's infrastructure. Collaboration-as-a-Service (CaaS), finally, involves agencies using a vendor's cloud-based collaborative services such as communications.

Regardless of the model, cloud's lack of physical infrastructure sometimes puzzles agencies. Agencies that aren't positive about who owns what in their clouds can set the record straight with SLAs.

Case Study

A Louisiana parish's cloud services contract shows how governments nationwide can handle ownership of the technology.

The Lafayette Parish Communications District announced in March 2019 that the parish was moving to a cloud-based dispatch system for first responders. Layette 911 Director Craig Stansbury added that the network was Louisiana's first multi-agency, cloud-based, computer-aided dispatch system.

According to Stansbury, Lafayette Parish adopted cloud as the parish was struggling with its old system, which routed emergency calls through facility servers. The system was required to have a nearly identical backup call center, he noted, nearly doubling the parish's costs.

"When every second counts, the most important thing is to have state of the art technology, and that's what we're trying to bring to Lafayette," said Stansbury, who's also director of the parish's Office of Homeland Security and Emergency Preparedness (OHSEP).

Stansbury confirmed that the parish's contract with Mark43 would solve his agency's problem by making the new system accessible anywhere with internet. For example, he said, dispatchers could receive 911 calls from a mobile command unit. Mark43 is a data services and software provided based in New York.

The parish would additionally contract with two other providers for new fiber cables servicing the Lafayette 911 building, Stansbury added. A related satellite trailer, he continued, would also ensure secure internet access during outages.

Stansbury said computer-aided dispatch helps 911 operators rapidly decide which emergency responders a scene needs. The systems also determine which responders are closest to calls, he continued, and they also coordinate call information between first responder agencies.

By partnering with outside vendors, Lafayette 911 can deliver needed emergency services without managing the underlying technology. Agreements such as these illustrate how agencies can use cloud without getting tangled in who owns the technology.

Best Practices

1. Clearly articulate a vision for cloud in any agreement, including key dates, performance levels, roles and responsibilities for both your agency and vendors.

2. Decide how much control your agency wants over its data, networks and personnel before procuring cloud from vendors.

3. Definitively state security benchmarks, auditing measures and penalties in any cloud vendor agreements.

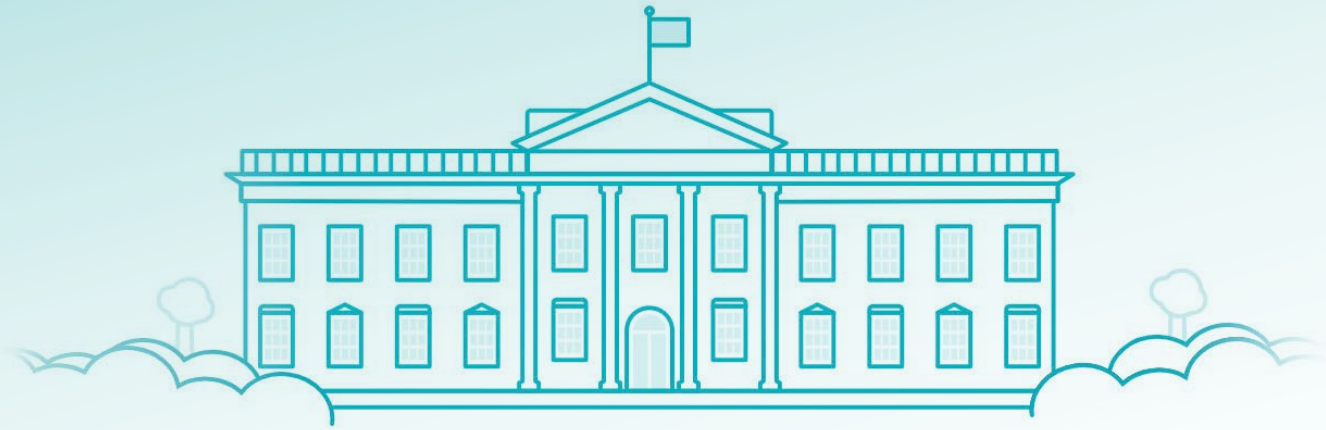
Key Stats

$2 billion of the federal government's IT spending went toward cloud in 2016.
Source: GAO

$4.1 billion The federal government spent $4.1 billion on cloud computing services in fiscal 2018.
Source: Bloomberg Government

Fifty-eight percent of state CIOs said that their agencies had migrated email and collaboration services to cloud.
Source: NASCIO "2018 State CIO Survey"

Forty-one percent of state CIOs said that their agencies were migrating business intelligence services to cloud.
Source: NASCIO "2018 State CIO Survey"



Cloud Data Management for Federal Agencies

Automation, Data Protection, Backup and Recovery

COMMON CRITERIA

FIPS VALIDATED 140-2

For more information
www.rubrik.com/federal

rubrik

Industry Spotlight

Launching Cloud-Based Automation at Your Agency

An interview with Rebecca Fitzhugh, Principal Technologist, Rubrik

Every new technology costs budget money that agencies don't necessarily have. When every dollar counts for agencies, upgrading their legacy systems often depends on what's affordable at the time. Cloud isn't a new technology, but its elasticity makes it ideal for pairing fresh software and tools. For example, cloud's flexibility and scalability make the technology ideal for enabling automation. Working together, automation and cloud can deliver agencies big savings fast.

To understand how cloud enables automation, GovLoop spoke with Rebecca Fitzhugh, Principal Technologist at Rubrik. Rubrik is a cloud data management and enterprise backup software provider. Fitzhugh said that Rubrik's data backup and recovery solutions are an example of the simple victories cloud-based automation enables.

"Rubrik is a modern solution that is purpose-built to help bring your data back online fast," she said. "Leveraging such a solution will also lower your recovery time objective, which ultimately drives business impact."

Many agencies may be struggling with cloud because of their dependence on legacy IT. Hybrid clouds bridge this gap by mixing on-premises and cloud architectures.

"I recommend beginning with the services that can be easily offloaded to cloud," she said. "You get a few small wins while you're identifying the more difficult applications and services and figuring out what the strategy's going to be."

Agencies can ease their cloud migrations by including automation in their journeys. Automation ultimately reduces the amount of manual labor, letting humans focus on more complex, mission-critical work. Take APIs, the building blocks of software. Cloud providers expose API endpoints, allowing agencies to automate provisioning tasks, or to even build applications on top. This results in faster release and upgrade cycles.

"Cloud provides agencies with the opportunity to seek and choose a more optimized business model," Fitzhugh said. "Cloud allows agencies to become more agile and responsive to different, changing conditions."

Why is cloud-based automation valuable? Fitzhugh argued that automating computing, networking, storage and infrastructure makes agencies quicker and more adaptable. "Your IT staff can go through and completely automate workflows that were once done manually, increasing your agency's efficiency even more," she said.

Despite this, cloud's model of sharing responsibilities between buyers and vendors has slowed adoption of the technology. For instance, many agencies are concerned with the data protections their potential cloud providers offer. A declarative, policy-driven framework could additionally help agencies adopt cloud faster. This framework reduces the steps agencies take during cloud migration by focusing on their desired outcome for the technology.

"One of the game-changing aspects of a cloud platform is that it offers the uniform API provisioning of resources. That makes cloud inherently automatable."

– Rebecca Fitzhugh, Principal Technologist at Rubrik

Main Takeaway

Cloud's versatility readily supports automation, which helps software and tools combine for big wins at your agency.

Q&A

With NGA Cloud, Data Center Director Percival Jacobs

The National Geospatial-Intelligence Agency (NGA) has a unique niche due to its role as both an intelligence and a combat support organization. As America's primary source of geospatial intelligence, NGA possesses a role unlike other government offices.

Geospatial intelligence is knowledge of earth's human activity collected using geographic imagery and information. Subsequently, NGA's work is essential to national security. Ultimately, NGA's mission requires cloud services with unusual collaborative capabilities, security restrictions and user access.

Of all the Intelligence Community (IC) agencies, NGA adopted cloud the earliest. NGA deployed the agency's operational capabilities to the IC's Commercial Cloud Services (C2S) in 2014. C2S provides agile, effective cloud computing to IC agencies.

GovLoop spoke with Percival Jacobs, NGA's Cloud and Data Center Director, about the agency's cloud. In the following Q&A, Jacobs explains what other agencies can learn from NGA's cloud experience.

This interview was lightly edited for length and clarity.

GOVLOOP: What makes NGA's cloud unique?

JACOBS: Due to our dual nature, NGA has gained the reputation of being a primary community integrator between IC and [Defense Department] DoD elements. At its most basic level, NGA has worked with a plethora of DoD and combatant command elements to assist their journey into cloud. It's things like sponsoring them to utilize NGA's cloud region, as DoD elements currently don't have direct access to C2S. It's also security accreditation, or even just sharing lessons learned. NGA has become known for its willingness to bring the communities into a common cloud environment.

GOVLOOP: How does NGA's cloud use geospatial intelligence for achieving the agency's mission?

JACOBS: The access to the cloud has made NGA's geospatial intelligence more readily and widely available than ever – it's available to any community partner who wants to access it. Even more, by making our data readily accessible, we can add other intelligence data sources on top of our own, apply artificial intelligence [AI] and machine learning algorithms, and come up with solutions that were previously unavailable to us.

GOVLOOP: How would you describe NGA's cloud procurement?

JACOBS: NGA worked with other intelligence community agencies for cloud environment across the entire IC – C2S cloud. Going at it together is certainly a lot quicker than going it alone. It saves a lot of procurement and acquisition overhead.

GOVLOOP: How secure is NGA's cloud, and how is it protected?

JACOBS: NGA's cloud cybersecurity is incredibly robust. It must be, given that NGA's data and applications are now physically further away and in a vendor's stewardship. However, working with Amazon, DISA and other IC/DoD cybersecurity elements, access to and from the cloud is as secure as on-premise data centers.

GOVLOOP: How has cloud changed NGA's workforce?

JACOBS: Admittedly, it was and still is a culture shift. A lot of the technical expertise NGA had at its disposal was on-premise data center application developers, engineers and so on. Cloud was entirely new, so there were some challenges.

The main lesson we learned here: train, train, train, and don't be afraid to reach out for help. We have engaged with multiple industry partners to help NGA's cloud workforce development, and we're all the better for it.

GOVLOOP: What are some persistent myths about cloud you'd like to dispel?

JACOBS: "My application could never go to cloud." "My application is too costly in the cloud." "My application's performance would suffer greatly in the cloud."

There's always a solution for each of these; the best solution is to win hearts and minds. In some cases, those individuals may be correct, which is why NGA is adopting a hybrid cloud.

GOVLOOP: What are some best practices for implementing and using cloud?

JACOBS: Document the capabilities before and after implementation – their performance, cost and reliability. Assess the capabilities fairly, unbiasedly and go in the order that makes the most sense. Finally, train, train, train the workforce and contract team members alike.


APPDYNAMICS | cisco | DLT
Rapidly Migrate Your Applications into the Cloud with Confidence, Clarity, and Predictability
Assess and plan with accuracy
Validate post move success
Ensure ongoing performance in hybrid environments
Rapidly adopt cloud-native architectures
Drive mission objectives, maximize value
LEARN MORE AT appdynamics.com

Industry Spotlight

How Cloud Boosts Your Agency's Business Intelligence

An interview with Sami Begg, Sales Engineering Manager, U.S. Federal, AppDynamics

The cloud computing agreements between agencies and vendors are increasingly hard to enforce as more applications enter the picture. Although valuable, these apps require agencies to handle more information before operating them intelligently.

This situation occurs as service level agreements (SLAs) grow more complex as more apps are deployed on clouds. SLAs are the agreements between agencies and their cloud vendors about how the technology should operate and be monitored. For agencies, administering these pacts becomes difficult without business intelligence, or analysis of an agency's past, present and future business operations.

To understand how agencies can better enforce SLAs by seeing their entire app landscape, GovLoop spoke with Sami Begg, Sales Engineering Manager, U.S. Federal at AppDynamics. AppDynamics is a performance monitoring solution that has the capability to produce business insights and can help agencies continuously monitor their apps' performance in cloud. "Implementing AppDynamics is extremely easy," Begg said. "We're typically showing users valuable insights about their apps on day one."

For example, improving business intelligence about current and past app performance rates can help agencies understand which of their cloud-based apps are loading slowly and why. These insights enable agencies to determine why specific apps aren't meeting their SLA performance requirements. Agencies can also determine why apps are underperforming before fixing them with their cloud vendors and delivering a better customer experience (CX). "It's important to understand what the end user's perception of your application's performance is," Begg said.

For instance, an app might be consuming more data resources than necessary or have code that is responding to queries slowly. "It's important to identify the different pieces of functionality within an app, and establish performance baselines for each, in order to understand what normal looks like," Begg said. "it is critical to ensure that the end user experience is not degraded when you migrate the application across infrastructure providers."

Ultimately, business intelligence aids agencies by helping them understand how people are using their apps. Agencies can analyze how many citizens they serve from one region, helping them prioritize where they focus their efforts. Insights such as these enable agencies to accomplish their missions quicker and more efficiently. "You have to understand your applications from the perspective of the business functions they serve," Begg said. "Correlating this information provides deep insights into the underlying success of the mission, and is enabled by the Business IQ capability set within AppDynamics."

Although cloud is valuable for hosting apps, some agencies have struggled to create SLAs that explain how the technology should meet their needs. Agencies that better comprehend how their apps work in the cloud can more easily explain to their vendors what they need in their SLAs.

"It's important to understand what the end user's perception of your application's performance is."

– Sami Begg, Sales Engineering Manager, U.S. Federal at AppDynamics.

Main Takeaway

Improved business intelligence helps agencies better enforce their SLAs by understanding how their apps perform in the cloud.

1

COMPONENT #1

Procuring Cloud

Procurement is one of the most important steps agencies take on their journey to adopting cloud. Selecting the wrong cloud program or vendor can leave organizations straining to meet the public's needs. The wrong cloud program or vendor can leave agencies incapable of delivering public services with the reliability, speed and security that citizens expect.

Regrettably, many agencies are overwhelmed by the private sector's large amount of cloud options. This range of choice can leave agencies unsure about which model is best for balancing their modernized and legacy IT. Even worse, organizations with poor clouds suffer service disruptions, security flaws and long-term financial costs.

Fortunately, organizations are realizing that cloud is not one size fits all. Agencies that are considering cloud moves must recognize their unique concerns. Every organization has its individual budget, privacy, operational and security requirements.

"You have to work with your contracting officers," said ICE's Larrimore during a September 2018 GovLoop online training. "It has to be a lot of hard discussions, Googling and sending people to work with our cloud service providers."

Key Stats

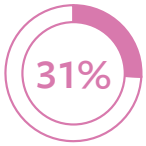
15,731 contracts

The federal government awarded 15,731 contracts related to cloud between October 2007 and April 2019.
Source: USASpending.gov

$8.3 billion

The federal government awarded about $8.3 billion in total prime award amounts related to cloud between October 2007 and April 2019.
Source: USASpending.gov

Thirty-eight percent of state chief information officers (CIOs) said that they had shared their cloud procurement strategy with other agencies.
Source: NASCIO "2018 State CIO Survey"



Thirty-one percent of state CIOS said that they had shared their cloud procurement strategy with other jurisdictions within their state.
Source: NASCIO "2018 State CIO Survey"

Best Practices

1. Include terms and conditions in all contracts with cloud vendors detailing who owns what data, where it's stored, and how it's secured.

2. Research your options so you know how each cloud vendor's reliability, security and other capabilities operate before deciding which one's best for your needs.

3. Think long-term about what you want from a cloud contract in terms of cost, length and vendor ties.

Case Study

DoD's recently released a cloud strategy that offers a clear roadmap to procuring the technology for agencies wrestling with the process.

Released in February 2019, the DoD Cloud Strategy avoids one of cloud procurement's biggest traps: vendor lock-in. Vendor lock-in occurs when an agency procures cloud from one provider who ultimately doesn't meet their needs. The length and cost of cloud contracts can prevent agencies from easily switching vendors if their original provider isn't meeting its needs.

DoD's strategy escapes this hazard by allowing more than one cloud from more than one vendor. For example, the plan demands a "General Purpose" cloud that will meet most of DoD's mission needs using one vendor. Aside from this cloud, however, DoD will also deploy separate "Fit For Purpose" clouds that satisfy the agency's leftover requirements without utilizing any single vendor, including the "General Purpose" cloud provider. This framework lets DoD separate data based on sensitivity without becoming dependent on any cloud vendor.

CITRIX®

Deliver secure mobile apps and desktops to any device anywhere.

Empower the digital government workforce with a complete application and desktop virtualization solution.

www.citrix.com/usgovernment

Industry Spotlight

Unifying Digital Workspaces in Hybrid Multi-Clouds

An interview with Jose Padin, CTO, U.S. Public Sector, Citrix

Digital natives are people who grew up using digital technologies such as social media and smartphones. They're high on government's hiring list because they're tech savvy and frequently understand tools that agencies want to adopt. But part of the challenge that agencies face when recruiting and retaining these individuals is providing work environments that meet their needs.

For example, digital natives are used to working from anywhere on any device, but agencies often can't accommodate this work style because their IT systems often don't support it. To meet employees' growing expectations for workplace flexibility, agencies are turning to Digital Workspaces.

Digital Workspaces combine cloud computing and legacy IT across multiple clouds to keep using traditional technology while adding cloud's flexibility. The unintended consequence, however, is that too many Software-as-a-Service (SaaS) apps applications are spread across multiple clouds. SaaS tools are software centrally hosted on cloud using a subscription basis. Although SaaS applications offer more access options for workers, they can also introduce more complexity and security challenges to agencies. Unified digital workspaces solve this dilemma by managing all apps, data, devices, desktops and users across hybrid multi-clouds in one place. It's a single, secure platform that simplifies work for employees.

To understand how Citrix can help streamline hybrid multi-clouds for agencies, GovLoop spoke with Jose Padin, Chief Technology Officer (CTO), U.S. Public Sector at Citrix. Citrix is a digital networking and cloud solutions provider that can help agencies build unified digital workspaces across as many clouds as needed. "A digital workspace can help aggregate and combine your data into one place," Padin said.

Hybrid multi-clouds are a natural evolution of using cloud infrastructure. Most agencies will leverage hybrid multi-clouds to achieve their mission goals. It's important to understand as clouds develop new and different technology that standardization on one cloud is less likely. Subsequently, it's important to architect and leverage tools that give the agency visibility, security and control across multiple clouds.

Unified digital workspaces overcome the sprawl from growing hybrid multi-clouds by managing the various mobile, web and SaaS apps that agencies have. For example, users may have four separate logins to use four separate apps. Unified digital workspaces provide users with one secure login for all four apps as needed. "Citrix can support any cloud," Padin said. "And with Citrix's workspace, we allow agencies to store your data where you'd like to. Unified digital workspaces increase productivity by making it easy for users to get done what they need to do."

"Citrix can support any cloud. And with Citrix's workspace, we allow you to store your data where you'd like to. Unified digital workspaces increase productivity by making it easy for users to get done what they need to do."

–Jose Padin, CTO, U.S. Public Sector, Citrix

Main Takeaway

Unified digital workspaces increase workplace productivity by simplifying operations in hybrid multi-clouds.

2

COMPONENT #2

Securing Cloud

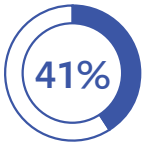
Cloud can store enormous amounts of data, but this capacity also makes protecting such information critical. Since citizens expect their governments to protect their data, agencies that ignore cloud security could lose their trust.

Realistically, cybersecurity demands constant attention from agencies. Threats such as cybercriminals and foreign governments are always evolving, and the weapons they use against agencies are multiplying.

Agencies aren't letting themselves be victimized, however, and many are prioritizing cloud cybersecurity. These organizations are choosing cloud vendors who are reputable for securing their customer's data. Agencies are also encouraging their employees to practice better cyberhygiene when they access, handle or store data in cloud. Finally, federal, state and local governments are creating strict cybersecurity standards for using cloud services, which are keeping agencies safe. For instance, FedRAMP stipulates cybersecurity benchmarks that every cloud vendor must meet before selling the technology to agencies.

"Security is obviously key to any cloud strategy you're doing," said Capt. Craig Hodge, Deputy CTO at DHS's ICE component, during the Advanced Technology Academic Research Center's (ATARC) Federal Cloud and Data Center Summit in June 2018. "We try to get our security team more educated on how to use [cloud's] tools and the development cycle."

Key Stats



Forty-one percent of federal agencies using cloud in September 2018 reported monitoring their services.
Source: GAO

Twenty-nine percent of state CIOs said that they share their cloud security services and monitoring with other agencies.
Source: NASCIO "2018 State CIO Survey"

Nineteen percent of state CIOs said that they keep their cloud security services and monitoring local rather than sharing them with other agencies.
Source: NASCIO "2018 State CIO Survey"

Twenty-three percent of state CIOs said that they share their cloud security services and monitoring with other jurisdictions statewide.
Source: NASCIO "2018 State CIO Survey"

Best Practices

1. Stay aware of where and how data is stored and who can access it when to prevent cybersecurity lapses.

2. Deploy security tools for cloud that foster collaboration and cooperation rather than remaining isolated from each other.

3. Make sure everyone involved with cloud complies with global, federal, state and local cybersecurity standards when required. For example, a cloud must meet FedRAMP's minimum cybersecurity requirements before it can be sold to federal agencies.

Case Study

The Small Business Administration (SBA) recently demonstrated two new ways for fortifying cloud using federal cybersecurity programs.

SBA CIO Maria Roat told GovLoop in February 2019 that her agency first deployed tools from the CDM program cloud in 2017.

SBA then created a pilot for DHS's Trusted Internet Connections (TIC) initiative in 2018 that uses cloud. TIC aims at optimizing, standardizing and reducing the amount of the federal government's external network connections. TIC 3.0 debuted in 2018 with cloud as a potential use case for government network connections following SBA's trial.

"SBA continues to push the envelope on many initiatives," Roat said. "Through the intent and spirit of TIC, we were able to put forward a viable, alternate solution. We are taking the same approach with CDM and evaluating the outcomes that need to be achieved."

TIC began in 2007, and the program has since sparked debate about whether cloud can meet its security requirements. SBA's pilot proved that agencies could meet TIC's cybersecurity benchmarks while utilizing cloud.

CDM, meanwhile, started in 2012 with the goal of delivering actionable, relevant and timely information to protect federal data and network security. The initiative now helps cybersecurity personnel prioritize and mitigate the most serious risks first.

PURESTORAGE®

Build apps here. Run apps there. Protect everywhere.

Pure Storage® cloud data services and cloud data infrastructure helps government unify on-premises and public clouds by providing hybrid cloud solutions that leverage the agility and innovation of multiple clouds at the same time. Now you can develop applications faster and free them from any one cloud. Pure Storage can help you build your cloud, run your applications anywhere, and protect your data everywhere.

Visit **PURESTORAGE.COM/CLOUD** to learn more.

Industry Spotlight

Combining Legacy and Modern IT in Hybrid Clouds to Serve Citizens

An interview with Nick Psaki, Federal CTO, Pure Storage

Agencies want the best of both worlds when it comes to IT. Sometimes cloud is the answer, such as when governments need to accommodate increased web traffic for election night. At other times, legacy IT is too costly or critical to operations for agencies to replace.

Fortunately, hybrid clouds bridge the gap between legacy and modern IT systems by combining data from both. For instance, agencies can use information from their on-premise systems for public-facing apps in the cloud. The services that these apps deliver – such as digital registration forms for driver's licenses – function the same for users regardless of the IT involved.

To understand how agencies can measure their apps' performance with data in hybrid clouds, GovLoop spoke with Nick Psaki, Federal CTO at Pure Storage. Pure Storage is a data storage hardware and software provider that offers cloud solutions. Data ownership is a frequent obstacle to cloud adoption as many agencies are reluctant to give control over their IT systems to vendors. "You don't own the infrastructure anymore," Psaki said of cloud. "The truth of the matter is that it's someone else's data center, but all the other rules of enterprise architecture, such as security, still apply. Our job at Pure Storage is to make sure cloud adoption goes as easily and smoothly as possible."

Data security is one of the reasons that hybrid clouds are increasingly attractive to agencies. For example, intelligence agencies handle classified information and must meet stringent security requirements to protect sensitive data. Although cloud can benefit these organizations, agency leaders may want ownership of on-premise IT systems containing sensitive data. "Security requirements are not optional for government – they're statutory," Psaki said. "The stringent security requirements for their IT systems remains in effect whether they are in the cloud or not."

Scalability is another data concern that hybrid clouds resolve. Traditionally, scaling legacy IT so it meets increased user demands for data is costly and time-consuming. In contrast, hybrid clouds can flex to meet agencies' needs whether data is on-premise or in cloud. "This is all the art of the cloud architecture," Psaki said. "In hybrid clouds, you have constant data movement between the on-premise and cloud architectures."

Pure Storage helps agencies create the hybrid cloud that's best for their unique mix of legacy and modern IT. The data stored in both on-premise and cloud environments operates with the same reliability for agencies and citizens. "What people have discovered is that one architecture does not fit all," Psaki said. "Whether you have data on-premise, in cloud, or both at the same time, Pure Storage's systems are inherently built to provide the type of architecture that agencies' applications need."

> **"In hybrid clouds, you have constant data movement between the on-premise and cloud architectures. The cloud services should be seamless in terms of the integration and the transaction."**
>
> *– Nick Psaki, Principal System Engineer, Pure Storage.*

Main Takeaway

Hybrid clouds help agencies by letting them use data from their on-premise and cloud systems to better serve citizens.

3 COMPONENT #3

Reforming Workforces for Cloud

Cloud can't change agencies if their workforces don't embrace the technology. The organizations that cloud benefits the most are the ones whose employees adapt to implement cloud by learning the right skills to use it effectively.

Preparing workforces for cloud begins with assessing the skills employees need in their new environment. Agencies must determine how cloud can change their communications, services and workflows.

After examining these areas, organizations must then decide what skills their workforces are missing to adopt cloud. These organizations must ultimately reskill their existing workers, hire new ones with the desired knowledge of cloud, or both.

For example, agencies that move all their IT assets to cloud might overwhelm their employees by changing too many established operations at once. One alternative is moving an agency into cloud incrementally. This lets each part of the agency adjust to cloud on their own without disrupting the entire organization.

Delaware CIO James Collins told GovLoop in January 2019 that helping employees understand how fresh tools like cloud will alter their routines is crucial for making IT projects successful.

"I think it's important to say where we want to go from a technology perspective and then evaluate where our staff is related to that and create a path," said Collins, who's also NASCIO's president. "And then we set a vision where the staff can say, 'OK, this is where I fit into that.'"

For evidence of why workforces are crucial for cloud, consider agencies that are beginning their migration to the technology. These organizations may lack people who know how to deploy cloud or maintain it. It's a situation where costs and frustrations can quickly rise as agencies can't properly use an architecture their employees have built.

Collins said Delaware's DTI bypassed this hurdle by identifying what roles the agency needed and then teaching people how to perform them.

"We're developing training paths for our team to take them into being cloud architects, agency relationship engineers and data scientists," he said. "We haven't historically had those roles, and we want to create paths for our team to evolve into them."

For organizations at any level, however, determining what's missing will help fill their gaps cheaper and faster.

For instance, Collins noted that Delaware boasts roughly 600 IT professionals statewide. DTI has about 300 employees, Collins continued, meaning that comparing these totals helps DTI better manage the agency's human capital for cloud. Delaware's tight IT market, Collins added, pressures the state's agencies to make sure that no employee's skills are wasted.

"One of the goals that I have is that I want to eliminate any redundancy that we have so that we can put more people on the tip of the sword where the agencies are establishing their priorities or addressing their problems," he said. "We want to have that IT expertise closer to the front, not all back in the engine room where we have them today."

Key Stats

Forty-one percent of state CIOs said that their organization has a cloud migration strategy in place.
Source: NASCIO "2018 State CIO Survey"

Thirty-seven percent of state CIOs said that their organizations are developing a cloud migration strategy.
Source: NASCIO "2018 State CIO Survey"

The federal CIO Council is working on seven actions for reforming agency workforces for cloud as part of Cloud Smart. One action is considering how cloud migration affects federal positions.
Source: Federal CIO's Office

Cloud Smart vows that the CIO Council will finish these in six months or less.
Source: Federal CIO's Office

Best Practices

Predict what skills your agency needs for adopting cloud and then which talents your organization can leverage once the technology is running.

Communicate cloud-related changes to your coworkers so they are prepared for migration and learn about opportunities to develop new abilities.

Share reskilling, training and recruitment opportunities during your personal engagements, professional events and social media use.

Case Study

The Air Force's largest cloud initiative displays what impact the technology can have on workforces totaling hundreds of thousands of people.

In November 2018, the Air Force Network Integration Center (AFNIC) concluded the first phase of the service's cloud transition. AFNIC's move required migrating 555,000 email accounts based in the continental U.S. to the Air Force's Cloud Hosted Enterprise Services (CHES) program. CHES aims to provide cloud-based communications, email and productivity tools to the Air Force servicewide.

"We're driving the Air Force strategy to capitalize on commercial industry IT services, allowing our Airmen to focus on operating and defending cyberspace," said Col. Doug Dudley, AFNIC commander, in a January 2019 statement.

The Air Force's cloud migration was challenging due to the large number of people involved. The transition risked disrupting email services for all 555,000 users participating in the process, so shifting their accounts required cooperation between multiple, partnered workforces. Ultimately, the project involved two Air Force components, two technology providers, the Defense Information Systems Agency (DISA) and base and major command members.

Dennis Polansky, AFNIC's lead program manager, said that the shift also exposed previously unknown vulnerabilities in Air Force and DISA infrastructures. These weaknesses required Air Force employees to safeguard exposed infrastructure during the move or risk cybersecurity incidents.

"We didn't create these issues, but it was our responsibility to work with experts across the Air Force to correct them before moving ahead," he said.

The migration was part of the Air Force's efforts to improve the service's collaboration capabilities by integrating previously disparate solutions. The Air Force will next migrate other collaboration tools that the service uses to the cloud. Although the first phase focused on email accounts in the continental U.S., future segments may migrate other related components to the cloud. AFNIC listed the Pacific Air Forces, U.S. Air Forces Europe and Air Forces Africa, the Air National Guard and DoD as potential candidates.

CLOUDERA

Realising the Enterprise Data Cloud from the EDGE 2AI

cloudera.com

Industry Spotlight

Seeing Information More Clearly with Enterprise Data Cloud Analytics

An interview with Henry Sowell, CIO; and Marcus Waineo, CTO, Cloudera Government Solutions (GGSI)

All the data in the world won't help agencies if they can't see the insights this information contains. Unfortunately, the more data is generated, the harder it can be for agencies to make sense of public trends and accomplish their missions without the right tools in place.

Cloud computing, however, can help agencies gain insight from their data. Cloud can scale for any amount of information, and it's also a technology that supports robust data analytics. By collecting, storing and analyzing their data with a platform in the cloud, agencies gain data flexibility that supports mission success. For example, data analytics can help agencies better understand populations so that they can target services to the citizens in the most need.

Enterprise data clouds are especially valuable to organizations as they can analyze an agency's data regardless of the IT storing that information. To understand how enterprise data clouds can help agencies quickly comprehend the public's needs, GovLoop spoke with Henry Sowell, CIO; and Marcus Waineo, CTO for Cloudera Government Solutions Inc (CGSI). Cloudera is a data analytics and engineering software provider with cloud-based and on-premise tools.

"Data is an absolute asset and one of the most valuable things for your organization," Sowell said. "We see people struggle to change their operations and thought processes and see data in a new light."
When it comes to data, agencies often employ large workforces in multiple departments. This setup makes fully grasping their agency's data difficult for even the most eagle-eyed employees. "Without access to a holistic set of information, you're making decisions based on a small part of the picture," Sowell said.

Waineo said that enterprise data clouds overcome this obstacle by enabling data analytics anywhere in an organization regardless of the IT involved. With many agencies storing data in the cloud, on-premise or in hybrid clouds combining both, enterprise data clouds are flexible enough for any organization's IT needs. "Enterprise data clouds are built with the community in mind," Waineo said.

Cloud vendor lock-in can limit agencies as their needs expand or result in long-term cost escalation. Enterprise data clouds avoid this pitfall by using open source technology to allow a multi-vendor approach to cloud.

Sowell added that Cloudera's enterprise data cloud enables agencies to do analytics in the cloud, on-premise or both. The outcome for agencies is a better understanding of how they can use data to better assist citizens. "You need to perform analytics where they make sense and when they make sense," he said. "Running analytics helps you better understand the effect that taking action has on achieving your mission."

> **"Without access to a holistic set of information, you're making decisions on a small part of the picture."**
>
> *– Henry Sowell, CIO, CGSI.*

Main Takeaway

Enterprise data clouds enable analytics for all an agency's information whether it's cloud-based, on-premise or both.

Q&A

With Oakland County, Michigan CIO Phil Bertolini

Phil Bertolini knows how cloud helps governments cooperate by erasing the barriers separating them. As CIO of Oakland County, Michigan, Bertolini sees cloud unite federal, state and local partners daily.

Bertolini also serves as the deputy county executive, and he has worked closely on some of his government's key IT projects. For example, Oakland County, Michigan houses two programs that harness cloud's power to help agencies in the county and elsewhere.

The first initiative is called G2G Cloud Solutions, and it launched in 2011. G2G Cloud Solutions is a free service that lets any agency in the U.S. collect payments online, over the counter or both.

G2G Marketplace, meanwhile, started in 2014 and now boasts nearly 1,000 agencies worldwide as registered members. The portal lets approved government vendors sell their technology solutions – including cloud, cybersecurity and e-commerce options – to other agencies.

GovLoop spoke with Bertolini in April 2019 about how cloud enables programs such as these for stronger collaboration and inclusion. In the following Q&A, Bertolini also discusses cloud adoption strategies and debunks common myths about the technology.

This interview was lightly edited for length and clarity.

GOVLOOP: How do agencies procure cloud efficiently?

BERTOLINI: The worst thing you can do is get a bad contract. Then you don't have exit strategies, the ability to keep things secure, or the power to audit. All those pieces need to be in your contract.

The other piece is to go find a partner that's done it. That means engaging your peer community. Find the right vendor, find the right partner and build the peer network so that you can bounce things off people you trust.

Then you must persevere. Those first two to three years are not going to return the money everybody says it does. You're going to have to fight with the financial side of cloud migration and make sure you're looking long term rather than short term.

GOVLOOP: What workforce tactics work best during cloud adoption?

BERTOLINI: In terms of educating procurement, IT and finance employees, you must get to why: Why are we doing this?

Everybody in government loves to save money, but that can't be the only reason for cloud adoption. You must talk about security. You must also discuss the ability to manage environment and ramp cloud services up or down when needed. The education will sometimes come from peers, and sometimes it will be organized education where you can find it. You're doing all these things to make sure that you've got the buy-in necessary to keep moving forward.

GOVLOOP: How does cybersecurity factor into cloud adoption?

BERTOLINI: One of the biggest struggles in government IT is compliance. Meeting all these cybersecurity requirements is difficult. You may end up with multiple security infrastructures. You need to make sure you understand the nuances of that. It's important to have a strong cybersecurity person that understands the differences between virtual on-premise, physical on-premise and cloud environments. You'll potentially have different strategies and architectures for all of them.

GOVLOOP: What are some myths that people believe about cloud?

BERTOLINI: People always say that cloud's less secure. That's not true. In many cases, cloud environments are more secure than what we have now.

Another misnomer is that cloud's cheap. Cloud's not cheap at first. When you do the return on investment or ROI, some people will say it's low cost to get into cloud. It may be low cost longer term, and we've proven that cloud's better than doing things on-prem through the ROI in later years that returns the investment. But during those initial years, you have your on-prem environment and you're also paying for your cloud environment. You're paying for all that initial implementation, and then you're paying by the drink, so your ongoing operational costs go up. Ultimately, your ROI looks terrible for the first two to three years. With so many people out there saying cloud's cheap, you must educate your finance people about how it might take a few years.

A third myth is that cloud's going to solve all your problems. That's not going to happen. Bad technology that you put in the cloud is bad technology in the cloud. If you haven't figured out ways to reengineer your business processes to accept the technologies that are enabling you to provide services, then all you're doing is wrapping technology around bad processes. It doesn't matter whether it's on-prem or in cloud, it's going to be the same.

GOVLOOP: Why are G2G Cloud Solutions and G2G Marketplace beneficial to agencies?

BERTOLINI: What we've done by creating these initiatives is that we're allowing smaller governments to use bigger technologies. We're allowing them to use the technology they need to serve the citizens. It doesn't matter if they're a small, little township; they can serve their citizens the same way as a big city does. The beauty of both G2G Cloud Solutions and G2G Marketplace is that each service is based on sharing.

When I ask another CIO for advice, they're more than willing to give it because they know we're both in a peer group that works together. I'm more likely to trust a fellow CIO or IT director than I am to trust the private sector outright with no relationship.

The advice that I would give people going to the cloud is don't go alone. Go find your peers that are doing it, whether it's in your region, state or nationally. Find those people and talk to them.

After that, don't get vendors that say they can do it without having them prove they can do it. There are many ways to work with the private sector. They're our partners, and we couldn't do it without them.

Industry Spotlight

Shifting Your Cloud Focus From Security to CX

An interview with Ian Greene, Enterprise Architect and Gnan Gowda, Senior Director, Product Management - Global Security, Genesys

Cybersecurity and CX present a balancing act for agencies. Although both concerns are important, these organizations are often short on budget dollars and time.

Fortunately, cloud vendors can help agencies shoulder the burden of cybersecurity and CX, as discussed in GovLoop's research brief with Genesys: How the Cloud Enables a Secure and Safe Customer Experience Made for the 21st Century. For instance, vendors can help agencies by training their employees about cybersecurity threats. This reduces the manpower and time agencies spend on compliance, letting them focus on CX such as improving public-facing websites.

To understand how agencies can deliver more satisfying CX by partnering with cloud vendors on cybersecurity, GovLoop spoke with Ian Greene, Enterprise Architect and Gnan Gowda, Senior Director, Product Management - Global Security at Genesys. Genesys is a cloud and CX solutions provider. "Government agencies are being asked to do more with less, and IT resources are expensive," Greene said. "The reality is they can use this as an opportunity to improve the citizen experience."

For example, cloud can ease the pressure that cybersecurity places on agencies' budgets and workforces. In this scenario, Genesys focuses on protecting the cloud application's cybersecurity while agencies manage the security of their IT environments. Although both parties have cybersecurity responsibilities, agencies ultimately have fewer security controls to manage, such as continuously monitoring their data. "Protecting the data is going to be the No. 1 cybersecurity challenge," Gowda said of clouds. "Although agencies are still responsible for the security of their data, they now have cloud partners who are well equipped to manage cybersecurity on agencies' behalf."

Cloud can also assist agencies by delivering tools that meet the latest standards for cloud security. For instance, these solutions can save agencies time by immediately complying with FedRAMP. "Agencies previously didn't have the resources to provide FedRAMP-level cybersecurity," Greene said. "Now you're free to focus on CX rather than constantly monitoring the system."

FedRAMP requires continuous, agencywide cybersecurity monitoring, so clouds that meet the program's standards have these features built-in. Ultimately, this frees up agencies' cybersecurity and IT employees to focus on improving CX. "Genesys takes the security, staffing and infrastructure requirements for cloud off of your plate," Greene said.

Overall, every agency has unique missions that they accomplish for citizens. By helping with cloud security, Genesys can aid agencies by letting them focus on their specific public services. "Cloud is our business, and creating a secure environment is our goal," Greene said. "You know your citizens better than anyone else. Let us take care of what we do best, so you can do what you know best."

"Although agencies are still responsible for the security of their data, they now have cloud partners who are well equipped to manage cybersecurity on agencies' behalf."

– Ian Greene, Enterprise Architect, Genesys.

Main Takeaway

Cloud can enable agencies to focus more on CX as the vendors who provide the technology can assist governments with their cybersecurity.

Conclusion

Cloud is pivotal for IT modernization, and the technology presents agencies with enormous opportunities. Cloud's agility, flexibility and scalability also makes the tool foundational for other promising technologies like machine learning and AI.

But cloud's benefits shrink if the technology isn't built efficiently. Agencies adopting cloud squander energy, funding and time if they don't carefully consider at least three major factors. Governments that include procurement, security and workforces in their cloud strategies will adjust to any changes with the most benefits.

The struggles many agencies have had with cloud, meanwhile, have created several widespread myths about the technology. Not every agency needs cloud, but the technology is typically more secure than older systems. Cloud use sometimes requires new skills, and owning the tool occasionally requires fresh thinking. Despite public debate over these topics, cloud's value to governments can't be overstated.

Ultimately, implementing cloud is like running a marathon, as it requires smart preparation beforehand. Whether your agency's federal, state or local, readying for your race will get you across the finish line to cloud's value.

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

Thank You

Thank you to AppDynamics, Amazon Web Services, Cisco Systems, Citrix Systems, Cloudera, DLT Solutions, FireEye, Genesys, Pure Storage, Red Hat, Rubrik, ServiceNow and ThunderCat Technology and VMware for their support of this valuable resource for public-sector professionals.

Author

Mark Hensch, Staff Writer

Designer

Megan Manfredi, Graphic Designer

1152 15th St. NW Suite 800
Washington, DC 20005
P: (202) 407-7421 | F: (202) 407-7501
www.govloop.com
@GovLoop