5

CLOUD TRENDS TO WATCH IN GOVERNMENT

govloop

Table of Contents

Executive Summary

Much time and funding have been devoted to getting cloud underway at all levels of government, and 47 percent of agencies actively use cloud services now, according to Gartner. That likely will grow in concert with federal cloud investments, which research firm IDC expects to reach about $3.3 billion in 2021.

Cloud adoption isn't just a trend at the federal level. Investments in cloud continue to stay high on the National Association of State Chief Information Officers' annual Top Ten Policy and Technology Priorities list.

And as cloud technology has evolved, so too have the possibilities it enables. Clearer uses are coming into view. Benefits are no longer just big-picture, such as greater flexibility, cost savings and increased efficiencies – but more honed. For example, cloud is enabling mission-specific efforts, such as making research more collaborative by facilitating medical data-sharing, protecting children from abuse through data analytics and giving U.S. warfighters an advantage over adversaries with AI.

To learn how agencies are realizing these benefits, we looked at what's happening in the public sector to encourage cloud innovation. We found that agencies, supported by government initiatives to embrace the technology, are tapping into five key trends:

Trend 1 Cloud supports emerging technology applications, such as artificial intelligence and the Internet of Things

Trend 2 Cloud enables better government services

Trend 3 New acquisition approaches ease cloud adoption

Trend 4 Cloud tackles security challenges

Trend 5 Private cloud models are picking up steam – again

This guide explores how some agencies are paving new cloud-supported paths and making the most of the technology. First, let's see how mandates and other efforts have given cloud a boost.

Government Embraces Cloud

The Cloud First policy, released by the White House in 2011, was only the first step toward federal agencies' study and implementation of cloud. Since then, several laws and initiatives have emerged to provide more guidance. In this section, we briefly highlight key advances and explain how they are shaping the future of cloud in government.

The Modernizing Government Technology Act of 2017 authorizes a central pot of money from which agencies can borrow to fund modernization efforts, which are often based on cloud. A March 2018 omnibus spending bill set the fund at $100 million through Sept. 30. Agencies submit a plan proposal to the Office of Management and Budget, and if OMB approves it, they can get a loan. Agencies have five years to repay the loan, likely using savings from their modernization initiatives.

The Report to the President on Federal IT Modernization, delivered Dec. 13, 2017, puts a heavy emphasis on the use of commercial cloud to drive efficiency and reduce costs in its goal of building a "more modern and secure architecture for Federal IT systems." Specifically, the report calls on the government to accelerate adoption of cloud email and collaboration tools. "Existing policies and programs will be rapidly and iteratively updated to eliminate barriers to cloud adoption, and agencies will rapidly migrate applicable capabilities to commercial cloud services," the report states.

The Federal Cloud Center of Excellence at the General Services Administration is an interagency working group that aims to foster cloud understanding and use. The center is working on a Cloud Adoption Survival, Tips, Lessons Learned and Experiences, or CASTLE, guide. The draft version takes a scenario-based approach that divides agency cloud needs into four categories: inventory assessment, application preparation, migration support and cloud service provider (CSP). Users of the guide find the scenario that most closely matches their concerns and may follow its advice.

The Federal Risk and Authorization Management Program (FedRAMP), launched in June 2012, is a governmentwide program that provides a standardized approach to the security assessment of cloud products. Agencies that use FedRAMP-certified cloud products and services know they have already been cleared for low, moderate or high levels of security. Since the first authorization was granted to Autonomic Resources, FedRAMP has undergone several updates. In September 2017, FedRAMP Tailored became available as a way to streamline the FedRAMP process for low-risk systems, such as collaboration tools and tools that develop open source code. Two months later, FedRAMP released the Agency Authorization Playbook to give agencies best practices and step-by-step guidance on implementing the process to grant an Agency Authority to Operate, or ATO. An ATO is granted to cloud service providers when they meet the program's security criteria.

Federal Q&A:
Research Collaboration in the Cloud at NIH

Vivien Bonazzi, Project Leader of the NIH Data Commons Pilot Phase

At the end of 2017, the National Institutes of Health launched the NIH Data Commons Pilot Phase. It involves a consortium of data scientists, computer scientists, IT engineers, cloud service providers and biomedical researchers that is looking at ways to store and share biomedical data in the cloud. The goal is to accelerate biomedical discoveries, while also adhering to data privacy and security requirements. We spoke with Vivien Bonazzi, Project Leader of the NIH Data Commons Pilot Phase effort, to find out more. Bonazzi's comments were lightly edited for length and clarity.

GOVLOOP: How did the pilot come to be?

BONAZZI: Biomedical data – there's huge amounts of it. We're talking terabytes and petabytes of data, and it's pretty hard to use that data in the current storage that we have either at local researchers' sites or even at NIH, so people have started using the cloud. The cloud does two things: You bring the tools to the data, so that you have all the data there and multiple people can come in and use that data. The second thing is shareability. You can have anybody potentially around the world in different geographical locations working together. If the data is all in one place, then you can actually work on it.

GOVLOOP: What does the pilot entail?

BONAZZI: One part is: How do we store data on the cloud and also pay for the compute? Another one is: What are a collection of services that we can operate over the data in the cloud so that we can make maximal utility for the folks who don't necessarily have strong computational backgrounds? Over the next six months, we're going to be testing those ideas and saying, "OK, if we have this data in the cloud, how do we make sure that we do have the right authentication [and] authorization system that does all the things that NIH needs to make sure that the data's protected?" That's one of the elements. Another one is this term FAIR, which is findable, accessible, interoperable and reusable or reproducible. The idea behind that is if you just put data in the cloud or anywhere and you can't find it, you can't use it and it's not reproducible, then essentially, you've just got junk.

GOVLOOP: Would any of this be possible without cloud technology?

BONAZZI: We've been doing it without cloud technology for a while, but the killer for us has been the volume of data. You could argue that you could do this on local servers, but the problem is you'll be looking at very large network servers. If you have five groups working on this and they all have their own five individual servers with replication of the data on each one of those, I would argue that's not very cost-effective. It stops collaboration between researchers because they can't work on each other's systems. The cloud allows the unification point, where you can have potentially one copy of data and multiple researchers with approved authority to use that data. And they don't have to maintain the IT systems associated with it in the local services.

5 CLOUD TRENDS

Trend 1:
Cloud Supports Emerging Technology Applications

What's happening

It used to be that AI was the stuff of sci-fi films and that sensors let you pass through automated doors. Cloud is changing that. It enables practical use cases of emerging technologies by providing the storage and computing capacity, flexibility and price points that other platforms have lacked. Tech such as machine learning, language processing and the Internet of Things are going from virtual reality – which cloud also supports, by the way – to actual reality.

Benefits from cloud-supported technologies, such as IoT and AI, are getting attention. For example, the United States could see labor productivity increase by 35 percent by 2035 because of AI, an Accenture report found. For government agencies looking to harness the momentum of emerging tech, there's help. For example, the General Services Administration's Emerging Citizen Technology Office launched its Artificial Intelligence for Citizen Services program in 2016, and last year, the National Institute of Standards and Technology released a draft revision of its Special Publication 800-53 to account for the Internet of Things.

See it in action at the federal level:

The Defense Department spent $7.4 billion in fiscal 2017 on cloud computing and AI, up 32 percent from 2012, according to a Govini report. The reason for the increased investment? To make AI and autonomous systems the cornerstone of DoD's Third Offset Strategy, a plan to use technology to outmaneuver adversaries in future warfighting missions.

"Rapid advances in Artificial Intelligence (AI) — and the vastly improved autonomous systems and operations they will enable — are pointing towards new and more novel warfighting applications involving human-machine collaboration and combat teaming," Robert Work, former Deputy Secretary of Defense, wrote in the report. "These new applications will be the primary drivers of an emerging military-technical revolution. The U.S. military can either lead the coming revolution, or fall victim to it."

The report breaks AI into three segments: learning and intelligence, advanced computing and AI systems. Within the first, natural language processing grew the most, at 16.8 percent, and quantum computing jumped by the same amount in the second segment.

About a third – 33 percent – of the total 2017 spending went to AI, but "before AI can be applied at scale, DoD must transition to the Cloud," the report states.

"That's the key thing with cloud services: It increases our flexibility, where we're not focused so much on infrastructure and platform development, but more focused on achieving results and making use of the data."

See it in action at the state level:

Cloud fuels many services that the Utah Department of Transportation provides. Most recently, UDOT helped develop the Connected Transportation Cloud, which lets officials see how data about the department's health and performance stacks up against business goals. The solution connects data silos into one dashboard that teams can access and share. It lets users, such as Utah, map strategic goals to indicators that they can measure continuously. They can also visualize budgets, including payroll and capital projects in addition to revenue sources.

The department's three main business objectives are eliminating fatalities, preserving transportation infrastructure and optimizing mobility through "Keep Utah Moving." The state uses private cloud services to pull together vehicle accident data for crash mapping in order to monitor problems and tweak the transportation system, said Dave Fletcher, the state's Chief Technology Officer.

"That's the key thing with cloud services: It increases our flexibility, where we're not focused so much on infrastructure and platform development, but more focused on achieving results and making use of the data," Fletcher said.

UDOT has been using a cloud-based data portal called UPlan to track all assets, maintenance planning, projects, traffic and safety since about 2009.

But the separate Connected Transportation Cloud will "provide clear metrics on basically everything that the Utah Department of Transportation does," he said. "I would say that UPlan is a little more operational and that Transportation Cloud is more strategic. UPlan includes data on all of the transportation assets that UDOT possesses, while Transportation Cloud tracks performance of those assets and relates that performance to strategic objectives, while also providing predictive capabilities."

Looking ahead, data is the future, UDOT Executive Director Carlos Braceras said in a 2016 presentation. To connect the data that will come from cars, traffic lights and stripes on the road, with the department, UDOT will rely on cloud.

"Cloud is not a goal in and of itself for us," Fletcher said. "It's just a facilitator that enables us to do things quicker and integrate new or more useful technologies quicker."

Next Steps:

Start small with something that will draw attention and wins. For instance, automate menial tasks so that employees can focus on more creative, mission-critical ones. Automation could save almost 100 million hours a year for federal workers, so a small difference can go a long way, especially toward getting support from managers who can help push bigger projects later.

Assess where cloud can ease pain points for government workers and the public alike. For example, Los Angeles uses smart parking meters with IoT that tells people where spots are open and when their meter is going to expire. For the city, revenues from parking have increased 2.5 percent.

Don't let funding deter you. Look for partnerships with industry and nonprofit organizations, apply for grants and build on existing infrastructure where possible.


Elastic
Map
Reduce
Amazon
Machine Learning
AMAZON
WEB SERVICES
BUILD
ON
aws
www.BuildOn.aws
REAL TIME
DATA
Amazon EC2
Model Repository
Developers

The New Age of Cloud in Government

An interview with Brett McMillen, Senior Manager, Federal Civilian, Amazon Web Services

Over the course of the last 10 years, government IT processes have undergone massive changes. At the beginning of this decade, cloud computing was, for the most part, in early adoption stages. These days, its value is widely accepted.

In fact, almost half of all government organizations are actively using cloud services, according to research published by Gartner in October 2017. The study found that local governments spend 20.6 percent of their IT budgets on cloud, and national governments spend 22 percent.

Statistics like these show that the public sector has entered a new phase of maturity in its cloud adoption — one in which agencies are now migrating mission-critical systems to the cloud. To examine this theme, GovLoop recently sat down with Brett McMillen, Senior Manager of Federal Civilian at Amazon Web Services (AWS).

"It's a pretty exciting road that we've been on. When I was first [working with federal civilian customers] about seven years ago, most of what the federal government was doing was finding specific workloads they could move into the cloud," McMillen said. "And what's happened in the last several years is that agencies have been moving enterprise workloads and mission critical apps into AWS. They're realizing the many things they can be doing in the cloud."

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.

As an example, he cited recent work with U.S. Customs and Border Protection (CBP), which has been tapped by Congress to develop biometric verification as people leave the country. The agency has sought to tackle the requirement with a customer-centric solution.

CBP already has a passport photo for passengers, McMillen said, so they know what people look like. In the future, airlines could be able to use facial recognition and artificial intelligence to verify that the person approaching the gate is indeed the person who is supposed to get on the plane. Airlines have told AWS they might not require boarding passes in the future, according to McMillen.

Other agencies, such as the Federal Election Commission (FEC), are now using cloud to boost citizens' confidence in government systems. AWS worked with the FEC to collect millions of campaign finance records, thousands of legal documents and more than 40,000 pages of other content and assemble it onto a new customer-centric website. The agency went further, building open APIs to allow other applications to retrieve near real-time information from FEC records.

Prior to the implementation of the FedRAMP, cloud adoption often proved time-consuming and expensive. That's largely because individual agencies were repeatedly seeking authorization for the same products and services, slowing the speed at which government could securely provide helpful solutions, McMillen said. That's now changing with shared services including those provided by the General Services Administration (GSA).

With cloud.gov, GSA provided a FedRAMP-approved platform that's supported by AWS and is available for others to quickly and easily launch web applications. When agencies build a system on cloud.gov, they are aided by the platform's FedRAMP compliance and reduce the amount of work they need to do.

Across government, agencies are looking for similar ways to streamline and standardize cloud acquisitions.

"Most of the departments we're dealing with are coming up with agency-wide acquisition vehicles," McMillen said. "They're coming up with authorization that anybody can utilize and easily deploy with all the governance and government regulations and securities that they need and they are creating standard operating procedures."

These new realities have made McMillen optimistic for the future. If the last seven years have been this eventful for cloud progression, he reasoned, the next seven must have even more in store.

"What we're finding is that when you start taking all of these cloud services together, the problems that you can solve are only limited by your imagination," McMillen said. "In general, what we're seeing is the government being able to better utilize its data as assets, and more and more that, IT is becoming an enabler of citizen services."

Trend 2:
Cloud Enables Better Government Services

What's happening

Government agencies at all levels are finding new ways to serve constituents using cloud-based technologies. Whether it's better approaches to sharing data, as NIH is doing; making people safer through social services; improving transportation; or protecting the environment, cloud is facilitating government services. As mentioned in the previous section, these cloud-enabled services are often tied to emerging technologies that can automate previously manual tasks. For instance, the Centers for Disease Control and Prevention uses AI for real-time tracking and reporting of poliovirus.

It's important to note that citizens aren't always the end user – sometimes employees are. After all, "hundreds of burdensome rules and requirements have built up over decades, forcing Federal agencies to devote valuable resources to compliance that is no longer meaningful. Time, energy, and dollars spent complying with outdated, redundant, and unnecessary requirements can be better spent on accomplishing mission outcomes," according to the President's Management Agenda.

See it in action at the federal level:

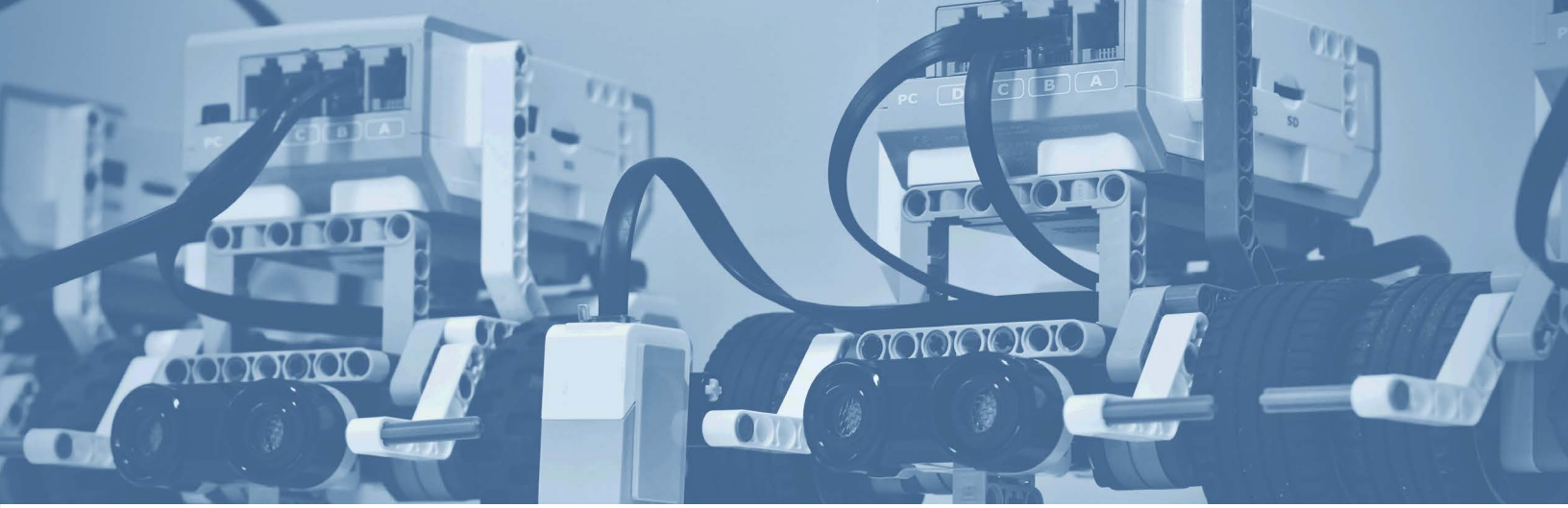
U.S. Citizenship and Immigration Services has a computer-generated virtual assistant named Emma that can answer questions and direct people to information on USCIS's website. Named after Emma Lazarus, who wrote the poem at the base of the Statue of Liberty, the tool answers questions in English and Spanish.

Emma is hosted in a secure cloud platform. The majority of Emma's AI and machine learning reside in a conversation intelligence platform that acts as a data scientist and scales to analyze millions of unstructured data elements and conversations to identify trends, recognize and label new intents, enhance understanding and make recommendations for the USCIS employees who "train" her, wrote Marilu Cabrera, Public Affairs Officer at USCIS, in an email.

The tool also uses natural language understanding for comprehension and natural language generation to enable Emma to respond based on the context and what she understood.

"Immigration policy information can be complex. Emma helps USCIS applicants and stakeholders find the information they need quickly and easily," Cabrera wrote. "Emma interacts with applicants and stakeholders in a similar way to how a human would — through conversation. Emma asks clarifying questions to help applicants and stakeholders drill down to the specific form or information they need."

Launched at the end of 2015, Emma answers more than 450,000 questions a month.



See it in action at the state level:

The Missouri Department of Natural Resources teamed with the Arizona Division of Environmental Quality to create the Gateway for Community Assistance (GCA), a template of a scalable state agency portal that has shared web-based services and tools. Packaged as a one-stop shop for local communities on a state agency website, GCA addresses the states' need to provide their communities with online access to tools and resources that address their environmental and infrastructure planning needs.

To use GCA, users create profiles tied to their interest areas, such as air quality or stormwater. Then, they can view relevant state, federal and nongovernmental environmental resources; see announcements about grant opportunities and upcoming events; and use the Assistance Wizard to get customized recommendations.

With the help of an Environmental Protection Agency Exchange Network E-Enterprise grant, the states built GCA using cloud.

"By using the cloud infrastructure, the team reduced computing cost by providing a single view of their Virtual Machines," according to a document submitted to the National Association of State CIOs by Missouri CIO Richard Kliethermes. The Missouri Office of Administration's Information Technology Services Division "created an application that can run reliably and one that can scale from 10 users to 10 million users, without any additional coding. This scalable infrastructure allows the application to use any number of processers."

Through GCA, Missouri expects to save 100 to 350 hours per year of staff time that had been devoted to researching localities' requests. That amounts to a savings of about $4,700 per year. Other states can access the GCA technology through EPA's Information Exchange Network, a web-based system through which state, tribal and territorial partners can share environmental and health data.

Next Steps:

Chances are you have the data already. Cloud and automation enable you to use it more wisely – and free up employees to put their time to more effective use.

Put together a business plan to illustrate return on investment, keeping in mind that ROI is not always about a dollar figure. Sometimes it's about how much a service helps.

To determine the success of your service, establish metrics to analyze performance goals and channels for customer feedback. Ask "what metrics will best indicate how well the service is working for its users," the Digital Services Playbook recommends.

THUNDERCAT TECHNOLOGY

Symantec™

A Service-Disabled, Veteran-Owned Small Business

Complexity Minimized. Performance Optimized.

Cyber Security Solutions for Public Sector Government

Your Federal, State and Local Government Cyber Security IT Experts that bring together a knowledgeable, focused, and nimble team. From discovery and assessment to proof of concept and implementation, ThunderCat takes a "Special Forces" approach to quickly deliver state of the art technology.

Elevate your security strategy to identify, protect and respond to advanced security threats

Ensure critical organization data can only be accessed by the right people, at the right time, and for the right reasons

Optimize limited budgets and staffing

Deploy critical security controls

Are you *#CyberReady*?
ThunderCat, where it all comes together.

WWW.THUNDERCATTECH.COM

Moving to the Cloud With Operational Security

An interview with Justin Robinson, Solutions Architect, ThunderCat Technology

Today in the public sector, the use of cloud, as well as the security surrounding it, has evolved significantly. Five years ago, the government introduced FedRAMP. And today, agencies and vendors are working together to protect government assets in the cloud.

Despite this progress, there are still concerns about data security, and how agencies should manage risk and oversight for the mission critical data that is stored in the cloud.

Agencies must be concerned with the security of the data traversing on-premise, hybrid and cloud environments. GovLoop sat down with Justin Robinson, Solutions Architect at ThunderCat Technology, to learn how an integrated, end-to-end cloud security environment can be applied and how ThunderCat and Symantec are helping agencies operationalize their cloud security.

"Today most agencies are challenged with mandates to move data from legacy systems into the cloud," Robinson explained. "But there is no uniform policy approach to doing this. This means that agencies must be both innovative and informed in their approach."

Federal IT leaders planning their cloud security strategy need to think about an operational and integrated cyberdefense approach, one that reflects the complexity of their IT operations and infrastructures, with their mix of cloud and on-premise solutions.

By investigating how data moves from one platform to the next, along with the paths in between, agencies can gain a holistic view of how their data in the cloud is being used. This includes operational cloud security solutions to govern access, protect information, defend against advanced threats and protect workloads as they move to – and from – the cloud. Agencies must understand where your data is and whom/what is accessing it in order to manage risk.

Cloud workload protection is critical to think about, Robinson said. Cloud security requires agencies to protect their workloads by deploying trusted security controls, monitoring across public and private clouds, across on-premises data centers, as well as automating compliance assessments. Doing this is made easier when working with the right vendor who has the precise tools and understanding of government needs.

"Symantec's suite of cloud workload protection tools is one solution," Robinson said. The suite offers a single cloud-based console that protects workloads across public and private clouds, and physical on-premises data centers.

Data loss prevention is another critical puzzle piece of cloud security, Robinson said. Information in motion is information at risk, meaning that agencies need to look at protecting data, including eliminating blind spots through data loss prevention policies. As the public sector stores more and more of their sensitive data in the cloud, it can be increasingly difficult to manage citizen information and protect it against loss and theft. What's required is a strong approach to data layer security that can protect assets wherever they may exist. DLP functionality coupled with CASB capability can ease the burden of implementing data layer security for the cloud.

"Symantec's Data Loss Prevention (DLP) tool answers these questions with a comprehensive approach to information protection that embraces today's cloud- and mobile-centered realities," said Robinson.

Risk management of data in the cloud is the final piece of the puzzle when it comes to operational cloud security. IT teams need to be able to embark on the process of identifying, assessing and controlling threats to their cloud networks. Symantec offers advanced tools that can help agencies effectively manage IT risks associated with key business processes, groups, or functions as well as communicate the impact of IT risk to mission stakeholders in a manner that drives change.

Symantec's product portfolio combined with ThunderCat's services deliver a powerful experience for government. ThunderCat provides an understanding of the federal landscape and an expertise in cybersecurity. They understand, support and work with public sector customers on how to properly respond to complex government mandates, how to store and secure their data to reduce operational risk.

"ThunderCat helps agencies address these issues by identifying areas to quickly improve their cybersecurity maturity," Robinson said. "With data layer security, we can help agencies protect their data, whether it's on premise or in the cloud, and we can protect it in a way that meets government mandates and adheres to risk management for their federal agency."

While the future of cloud is assured in government, agencies may be less sure about how to navigate cloud security. But by focusing on data loss prevention, data layer security and risk management, government agencies can double down on cloud security with confidence.

Trend 3:
New Acquisition Approaches Ease Cloud Adoption

What's happening

A better way to acquire IT that more closely matches the speed of innovation has long been a priority for agency CIOs. The government has responded with ways to accelerate procurement. For example, it added cloud to GSA's Schedule 70 and implemented FedRAMP, which lets agencies evaluate cloud vendor capabilities and security features more efficiently. Because such reviews are part of the acquisition process, FedRAMP helps the procurement move along. The program now covers 5 million assets of the world's largest cloud providers and offers four security baselines, ranging from low-impact Software-as-a-Service to high-impact systems that agencies heavily depend on to get work done. State and local governments are also innovating, using techniques such as brokered services and chargeback models. Brokered services means either an IT agency acts as a middleman for cloud vendors and other users, or a third party serves that role, handling cloud choices. Either way, the go-between gets a cut of the revenues. Chargeback models apply the cost of cloud to the business unit that uses it, rather than a central IT shop handling all costs as overhead.

See it in action at the federal level:

DoD's Defense Innovation Unit-Experimental (DIUx) took the lead on a contract to Virginia-based REAN Cloud for streamlined cloud migration services by using an "other transaction agreement" contract. These legally binding agreements are not standard procurement contracts, grants or cooperative agreements, and so they are not subject to the federal laws and regulations, such as the Federal Acquisition Regulation, that apply to typical procurement contracts, according to a military document.

The benefits of using such an agreement include "greater speed, flexibility, and accessibility in performing research and prototyping activities. It can also be used to design and implement innovative business models within the government that would otherwise not be feasible," the document states.

DIUx originally issued the agreement in February with a value of $950 million, but a month later, the unit capped it at $65 million after the Pentagon said the agreement exceeded its original scope of providing a prototype by moving it to production for use departmentwide. Still, the contract serves as a model for how agencies can speed cloud acquisitions by working with industry to implement innovative technology and processes.

Separately, DoD released in February draft requirements for another cloud contract worth up to $10 billion that will provide the department with commercial cloud infrastructure and platform services. Controversy has surrounded the contract because many feel only Amazon Web Services can meet its requirements.

FedRAMP now covers 5 million assets of the world's largest cloud providers and offers four security baselines, ranging from low-impact Software-as-a-Service to high-impact systems that agencies heavily depend on to get work done.

See it in action at the state level:

Before the Indiana Office of Technology (IOT) took ownership of IN.gov in 2006, a contractor ran the state's website on a business model that was heavily transaction-based. During the past 10 years, however, IOT has moved to a brokered services model. Now, the office collects fees from other state agencies for services that IOT provides.

"We're the only state that has this particular model," Robert Paglia, Chief Administrative Officer at IOT, said at an IOT funding and budget overview in September 2017. "When we took it over, there was a negative $250,000 net loss of the program and there were 15 resources. Today we have over 50 resources and we generate a net income of over $3 million on IN.gov."

IOT itself has a $132 million annual budget and operates on a chargeback model in which it aims to recover exactly what it spends. Costs include personnel, hardware, software licensing and support. To set costs, the office evaluates consumption from previous years and what is currently trending, and divides that figure by the number of people who will use the technology, said Indiana CIO Dewand Neely at the meeting. He works with the budget office to offset any net losses, and when there's excess of revenue, it goes back as a rebate to the agency or to the general fund.

Neely relies on feedback to know when IOT is good at providing a particular service and when it's not. That way, the office can either improve it or broker a deal with another vendor.

Next Steps:

The Cloud Center of Excellence has put together a draft Cloud Acquisition Professionals Cloud Adoption Survival Tips, Lessons and Experiences guide that lays out common challenging acquisition scenarios and ways to address them.

Attend a virtual or in-person workshop of GSA's Cloud Access for Federal Enterprise, an initiative to simplify cloud acquisition in government. In May, CAFE will host a virtual event on how to buy cloud Infrastructure-as-a-Service, for example.

Cloud has brought the IT department and business office together to evaluate the best acquisition opportunities. This new relationship can be tricky, though. To smooth it, check out the framework offered in "A Service Brokering and Recommendation Mechanism for Better Selecting Cloud Services."

Automation as the Cornerstone of Secure Government Cloud Success

An interview with Adam Clater, Chief Architect for North America Public Sector, Red Hat

Government IT teams are at a crossroads when it comes to balancing citizen and user demands, technology, and security priorities. For example, there is also an enormous push to consolidate data centers and move processes to the cloud and shared services — and to do it quickly. But agencies must adopt these changes in a secure manner, without exposing government systems to hackers and potential data breaches.

For agencies at all levels of government, reconciling the need for security and protected data with storing information in the cloud can be a difficult process. This is especially true given the many IT compliance mandates and the fact that securing infrastructure and workloads are often manual processes.

How can government agencies move workloads to the cloud quickly, while staying secure, and not requiring an increase in manual processes?

The answer is automation. To better understand how automation is enabling secure cloud adoption in government, GovLoop sat down with Adam Clater, Chief Architect for North America Public Sector at Red Hat, a leader in open source technology, is automation.

At its core, automation is the use of technology to perform tasks without human assistance. And IT automation is the use of a system of instructions to carry out a repeated set of processes, which replaces manual work done to IT systems.

IT automation in the cloud helps with efficiency, delivering value faster, and solving IT and business workflow challenges.

"Automation is the cornerstone of cloud, datacenter consolidation and IT modernization," Clater said. "No matter what aspect of IT you are engaging with, automating manual processes is proven to increase reliability by reducing manual errors, decreasing time to deliver IT assets and is key to building self-service capabilities for your enterprise."

Clater recommended that agencies look to implement a strategy that automates application management, security and deployment in order to facilitate workload migration to the cloud.

"Automating your cloud workloads gives agencies more flexibility to deliver services faster and scale workloads and services in a way that reduces bottlenecks," Clater noted.

The next phase that agencies are beginning to move into is automating the application of security controls. More recently, Clater explained, agencies are being exposed to automation technologies that address issues of security scanning, remediation and documentation.

"It would be next to impossible for any agency to scan their infrastructure from a security perspective without pretty extensive automation," Clater said. "When you conceptualize the idea that you might run a hundred or more automated tests against a single host, and there could be hundreds or thousands of hosts throughout an agency's infrastructure, automation is really key to that."

Agencies are also integrating security automation technologies with their existing tools. This integration helps them to better track any changes on their networks or in the cloud and to ensure those changes are fully documented. As part of this documentation process, agencies must also ensure they are using pre-approved technology building blocks.

One of these instances is the OpenControl project. The project is the undertaking of an open source community working to develop the tools necessary to align security assessments and authorizations with modern, continuous software development and delivery. Agencies such as 18F, the National Institute of Standards and Technology, and others contribute code to the project, as well as vendors like Red Hat.

"Red Hat is one of the largest contributors to the OpenControl project," Clater said. "We've been making a lot of code commits to automate documentation around our products."

One other manner in which Red Hat that helps government automate processes and security compliance in the cloud is through their automation engine, Red Hat Ansible Automation. It automates cloud provisioning, configuration management, application deployment, intra-service orchestration, and more. Using Red Hat Ansible Automation, agencies can standardize common tasks, freeing up resources and ensuring consistency and compliance around security.

To truly unleash government innovation and take full advantage of moving services to the cloud, the public sector must turn to automation. When repetitive labor and processes are solved by deploying automation technologies, then and only then will IT managers truly have the needed freedom to spend more time exploring and adopting new technologies, rather than spending their time keeping the lights on. Integrating automation practices will help balance the scales and provide agencies with a more solid platform for future cloud growth.

Trend 4:
Cloud Tackles Security Challenges

What's happening

Some agencies are preparing to move more sensitive data to the cloud, and they are using FedRAMP to set the parameters for security. But about 70 percent of CIOs told the Professional Services Council that FedRAMP changes have not helped their agency adopt cloud services, according to the council's 2017 Federal CIO Survey.

FedRAMP isn't the only resource for the latest in cloud protection, however. The National Institute of Standards and Technology released in February Special Publication 800-145, a report that clarifies how to qualify a computing capability as a cloud service and how to determine whether a service fits in the IaaS, Platform-as-a-Service or SaaS models. Additionally, the "Report to the President on Federal IT Modernization" calls out the transition of perimeter-centric security efforts to data-centric ones, which "emphasizes placing protections closer to the services and information systems in which sensitive data is stored and accessed."

See it in action at the federal level:

The Small Business Administration is pilot-testing a workaround to the Trusted Internet Connection, an 11-year-old initiative to optimize and standardize the security of individual external network connections that federal agencies use. The agency's deputy CIO says TIC, which was designed to secure on-premises systems, doesn't mesh well with cloud, and he plans to prove there are other options.

"We think the cloud is more secure," SBA's Guy Cavallo said at a recent GovLoop event. "So [whatever is] not nailed down, we're moving it to the cloud."

SBA is working with another unnamed agency on the pilot, with each testing separate solutions. The security features are comparable, if not better than what TIC provides, Cavallo said. For example, his team picked up on 13 attempted connections from Vietnam, a country where SBA doesn't maintain offices. As a result, the agency blocked those IP addresses from making future access attempts.

TIC isn't ready to be made obsolete, however. TIC 3.0 is in the works with an eye toward cloud.

See it in action at the state level:

When Pennsylvania's Office of Administration, Office for Information Technology (OA/OIT) moved from an on-premise service model to a cloud-based one, officials worried about putting data outside its protected network. To ease fears, the commonwealth instituted a Risk-Based Multi-Factor Authentication (RBMFA) enterprise service.

It uses two-factor authentication. The first factor is a worker's username and password, and the second is a software token on the employee's device of choice. Once installed on a trusted device, the token is unlocked for each use by entering a preset personal identification number. On an untrusted device, it could be unlocked by answering registered challenge/response questions or providing a one-time code sent by text message to a registered smartphone.

"The service encompasses a risk profile which considers various factors including the data or application being sought, the geographical location of the request, the nature of the device being used, and number of access attempts in a given time period," according to a document submitted to NASCIO.

In choosing a service, OA/OIT piggybacked on an MFA solution that the Pennsylvania Department of Human Services was successfully using, state Chief Information Security Officer Erik Avakian wrote in an email. "This enables us to avoid having multiple, siloed MFA solutions being used by different agencies," Avakian wrote. "Working collaboratively also helped drive quicker adoption and economies of scale and reduction of duplicative effort."

RBMFA went live in June 2016 and serves all agencies on the state network. This single system has cut multifactor authentication costs from $15 per year to about $1 per year, contributing to an annual savings of more than $1 million.

"Overall, the RBMFA service has performed well and met our expectations," Avakian wrote.

Next Steps:

Use a layered approach that can protect data on-premise, in the cloud and even at the edge. Data is king, as they say, but it doesn't exist in one place – nor should it. If all your eggs are in one basket, that would be a mighty valuable basket to breach.

Develop an enterprise security strategy with the help of agency leaders, who "need to agree that cloud computing has become indispensable and that it should be governed through planning and policy," according to Gartner.

Study Gartner's Hype Cycle for Cloud Security, which indicates technologies that are ready for mainstream use or future implementation.


Microsoft
Azure Government
Advance your mission
with the cloud you can trust
Breakthrough innovation
Unparalleled flexibility
Mission-critical security
Learn more about Azure Government
Request a free Azure Goverment Trial

How Government Can Adapt to a New Secure Hybrid Cloud Paradigm

An interview with Susie Adams, Chief Technology Officer, Microsoft Federal and Karina Homme, Senior Director, Microsoft Azure Government

Today, citizens using government services expect secure and mobile digital experiences, delivered any time, at any place, on any device. And the same is true about the government workforce, who needs access to an increasingly complex hybrid IT environment in which connections and services are no longer fully managed by the agency.

To do this, more and more of the public sector are moving their operations and applications to the cloud. But while agencies have adapted to shifting to the cloud, achieving security can still be a concern in hybrid cloud environments. The answer is to shift to a new model of cloud security where identity is the new firewall, and devices are the new perimeter, and flexibility is built in to the approach.

To understand how agencies can adapt to this new hybrid cloud paradigm, GovLoop sat down with Susie Adams, Chief Technology Officer, Microsoft Federal and Karina Homme, Senior Director, Microsoft Azure Government. Microsoft Azure Government provides cloud services to more than 7,000 federal, state, and local customers and offers the compliance, security, and flexibility that the public sector needs.

Similar to many other industries, government needs the agility to respond to almost any situation at any given time. But while the private sector can easily find such flexibility in the cloud, for governments, it's not quite as simple. In addition to obtaining the computing and development power of the cloud, agencies must adhere to the highest levels of security while meeting complex U.S. government compliance regulations. That is complicated by the fact that today, data lives everywhere, not just in data centers or on desktops. But, how do you put a firewall everywhere?

The key is to approach security differently. As your data expands, identity should become your new firewall. That means that rather than tracking the billions of pieces of information swirling in and out of IT systems, agencies should monitor the users who access that data. While an agency's data might be nearly infinite, they can define who should have access to what information and systems, when, and from where.

Additionally, policies and tools developed for an IT environment managed solely behind a secure physical perimeter are no longer adequate. Data must be protected on any device and in transit over any type of connection within a virtual perimeter that spans both the agency data center and cloud providers in what could now be called an agency "digital virtual estate," according to Microsoft Federal CTO Susie Adams.

As data moves outside the agencies physical network and data center boundaries, identity becomes the key to unlock access for end users and system access to data regardless of where it lives. "The digital estate with the ID layer provides a stable hybrid-cloud solution so that agencies can combat cyberthreats, be more efficient, and reduce costs," said Adams. That layer also needs to work fluidly with hybrid clouds, multiple partners and multiple devices, she further explained.

Finally, flexibility is key for government agencies looking to move to a secure hybrid cloud environment. "Using Azure Government, our public sector customers are able to move their data between devices, their data center, and the Azure Government cloud in a hybrid or multi-cloud infrastructure," said Karina Homme, Senior Director, Microsoft Azure Government.

It's more critical now than ever for agencies to take a holistic end-to-end approach to security that focuses not just on protect and respond, but on detection capabilities. Incorporating tools that leverage hyperscale cloud capabilities, such as Microsoft Azure Government, that focus on threat detection using big data analytics and machine learning is crucial.

Microsoft Azure Government offers the flexibility and built-in security features that enable leaders to test out their theories, lower costs quickly and achieve modernization.

In today's public sector environment, the new security paradigm for government means understanding that identity is the new firewall; devices are the new perimeter; and that breaches will eventually take place.

Addressing these shifts with flexibility, portability, and the right vendor solutions with built-in security approaches is the way forward for government agencies moving their most critical data and applications to the cloud.

Trend 5:

Private Cloud Models Are Picking Up Steam – Again

What's happening

As agencies seek to move more sensitive data to the cloud, it's little wonder that private cloud models are gaining popularity. Private clouds are used by a single entity and isolated from others, giving agencies more control and security. Perhaps some of the most compelling cases for private cloud come from the intelligence community's Commercial Cloud Services contract, which has cut the time it takes to provision a server from 180 days to minutes.

Recent statistics about private clouds are telling. Governments will implement private cloud at twice the rate of public cloud through 2021, Gartner predicts, "despite private cloud not delivering the same benefits in scale, functionality, cost savings or agility as public cloud can." A 2016 MeriTalk survey found that 64 percent of federal IT managers said they were most likely to place a majority of their cloud-based applications in a private cloud, while 54 percent of state and local IT managers said the same.

A 2016 Deltek report found that agencies spent $1 billion on private cloud computing in the preceding three years, and a 2017 IDC report put total federal cloud spending closer to $3.3 billion by 2021. Still, it's worth nothing that some studies have shown that private clouds hosted by larger CSPs are more secure than on-premises solutions. The bottom line: Do your homework; cloud isn't a one-size-fits-all, silver bullet or insert-other-cliché-here solution.

See it in action at the federal level:

The Defense Information Systems Agency's milCloud is a cloud services portfolio "that features an integrated suite of capabilities designed to drive agility into the development, deployment and maintenance of secure Department of Defense applications." With milCloud 2.0, DISA is expanding not only service offerings, it's also redefining milCloud's structure.

MilCloud 2.0, which launched Feb. 1, connects commercial Infrastructure-as-a-Service offerings to DoD networks in a private deployment model. DISA awarded CSRA a $498 million contract in June 2017 to run the on-premises, private cloud solution. This is a departure from milCloud 1.0, which was government-run.

DISA gave milCloud 2.0 provisional authority for impact level 5 data in March, clearing the way for it to access and host controlled unclassified information, mission-critical information and national security systems.

"It's more secure than a commercial cloud, but it's a capability that's provided on-premise," former DISA Director Lt. Gen. Alan Lynn said of milCloud 2.0 at the 2017 AFCEA Defensive Cyber Operations Symposium.

64% of federal IT managers said they were most likely to place a majority of their cloud-based applications in a private cloud while 54 percent of state and local IT managers said the same.

See it in action at the county level:

In 2011, Oakland County, Michigan, launched G2G Cloud Solutions to "improve government services by sharing technology with other government agencies at little or no cost," according to the G2G Cloud website. It began by providing services internally and with some local municipalities. Today, almost 100 government entities statewide use it, and in 2017, the county transacted $58 million through it.

"They're able to use our G2G Cloud Solutions as a Software-as-a-Service," said Phil Bertolini, county CIO. "Part of our technology is housed in a cloud. We use different versions of the cloud. ... What's good for those local communities is they don't have to have any of the infrastructure to go ahead and use the technology."

The county opted to use a private cloud for this e-commerce initiative because of the sensitive data, such as credit card numbers and personally identifiable information, involved in the two payment services agencies can get through G2G. One is over-the-counter payments, which let people pay by swiping their credit cards. The other is online payments.

"You don't want that out there where it can be hacked," Bertolini said. "When you talk about public or private cloud, it's really where you're housing your technologies and housing your data, how you're using it. It's going to be the difference in the type of information you're using and how critical it is that it be secure and confidential."

Next Steps:

GSA's 2017 Hybrid Cloud Almanac outlines steps to take when considering cloud options. The first is to conduct a thorough inventory of all current IT assets, including infrastructure, applications and governance structure. This will help you determine the type of data you want to move to the cloud. Then you can review the almanac's definitions of cloud options to help you choose the right one.

The DISA Cloud Playbook defines the cloud adoption cycle as learn, choose, buy, configure, transition and utilize. But note that this is a cycle, and it will repeat as technology and your needs evolve. Have a strategy in place that allows you to continuously review your needs and be flexible about adapting them.

Need to refresh your cloud-savviness? Check out the Defense Acquisition University's primer on cloud computing and GovLoop's Cloud Crash Course or any of our interactive courses on cloud.

State and Local Q&A:
Preventing Child Abuse With Cloud

Leslie Chaney, Chief Information Officer, New Hanover County

Wanda Marino, DSS Assistant Director, New Hanover County

New Hanover County, North Carolina, is working to keep children safer through its use of the cloud-based Visual Investigator tool, which uses predictive analytics to determine changes in risk factors for abuse and neglect. The county's Department of Social Services (DSS) processes 300 reports of child abuse or neglect every month, and by integrating case data with data from the jail and 911 calls, the system alerts DSS workers to changes that could affect a child in their charge. We talked with Leslie Chaney, the county's Chief Information Officer, and Wanda Marino, DSS Assistant Director, to learn more.

GOVLOOP: What gaps were you looking to fill with this tool?

CHANEY: We had 20 years' worth-plus of case management data, but it was not easily accessible. It's in a legacy system, and if a case worker wanted to research the history of a client or of a perpetrator or of anyone on a case, it took a lot of time. They had to go through several screens of data. There was no linkage for them that was easily accessible. SAS [and the Duke Endowment] approached us about partnering with them on this pilot to take that data and put it in a format that's much more usable and quickly accessible to workers as they're trying to determine risk on a case.

GOVLOOP: What role does cloud play?

CHANEY: We were able as our IT department and as DSS not to worry about the technical details of how many servers we were going to need [and] what kind of technical architecture. We had people who work on the database side work on the data aspects, and then at DSS, they just use a browser to access the system. We've taken the cloud-first approach in the IT shop because we are medium-sized, and we would rather put our resources toward systems and using them to their full potential rather than managing infrastructure.

GOVLOOP: I would imagine that this allowed you to get this going much quicker than if you were doing it yourself.

CHANEY: For sure. There was no procurement of systems, no installation, integration – any of that.

GOVLOOP: How would a government worker use this?

CHANEY: The data has a lot of search tools in it and it builds those linkages that were missing in our old system, so if a worker gets an abuse or neglect report, for example, and they have created their cases, they can look in the Visual Investigator tool at any of the people related to the case and see their past involvement, see other cases that they've been part of, and it's on a timeline so they can see all of the history that we have around the people on that case. The system also uses predictive analytics to assign a risk score to the people that are involved in that case, and that's based on past involvements and substantiated claims of abuse and neglect.

GOVLOOP: What benefits have you seen?

MARINO: We are still in a testing/using phase. We have been doing training, and in some of the training we have actually run up on alerts that gave us information about someone that had been released from jail. This individual had been a perpetrator and we had not gotten an alert [through traditional means] that this person had gotten out of jail, and that would be a high risk to the family.

Conclusion

Within less than a decade of being told to put cloud first, IT departments have made great strides. About half of agencies use cloud services already, and they are starting to see cloud's greater capacities as they move out of the foundational phase.

Cloud's potential shows no signs of slowing. In late 2017, Gartner predicted double-digit growth in government use of public cloud services, with spending forecast to rise on average 17.1 percent per year through 2021. Globally, local governments spend 20.6 percent of their IT budgets on cloud, and national governments spend 22 percent.

Today in the United States, support for the cloud exists at the highest levels of government. Efforts such as FedRAMP, NIST guidelines, the MGT Act and the Cloud Center of Excellence have grown out of a need to encourage cloud adoption – and quickly.

Public officials are taking note. At all levels of government, organizations are using cloud to transform how government operates.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 270,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

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

Thank You

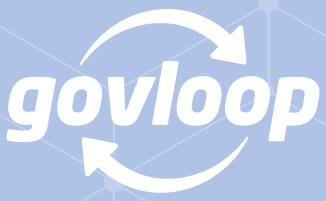
Thank you to Amazon Web Services, Microsoft, Red Hat, Symantec and ThunderCat Technology for their support of this valuable resource for public-sector employees.

Author

Stephanie Kanowitz, Writer

Designer

Megan Manfredi, Junior Graphic Designer



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

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

www.govloop.com
@GovLoop