Barriers to the CLOUD Remain

Common language, phased approach and a strong value proposition can help cloud implementations.

EVENT OVERVIEW

Shutterstock

As government agencies make their move to the cloud, the biggest hurdles they face have little to do with the actual technology. There's overcoming the lingering perception that the cloud is less secure. Then there's also changing the organizational culture.

These barriers aren't deal breakers, as some agencies have already demonstrated with successful cloud implementations. Clearly communicating the goals and benefits, using a phased approach and demonstrating the value of cloud have all helped. If done properly from the start, cloud computing has the potential to be even better than an on-premises solution, particularly from a security standpoint, according to government and industry experts speaking at a recent event.

About six years ago, the White House launched its Cloud First initiative. This was intended to encourage agencies to consider cloud computing as a platform for their IT operations because of the flexibility and the opportunity for cost savings. Since then, some agencies have forged ahead with cloud, but at an uneven pace.

One of their top concerns remains lingering security concerns about cloud computing platforms, according to speakers at a March 30th event: Overcoming Barriers to the Cloud. This perception is changing thanks in part to the government agencies and numerous vendors who have provided products, services and other resources to help make the path to the cloud easier.

"I am a strong believer that you can get a better solution in the cloud if you do it right than something that you can do in-house," says Dr. Michaela Iorga, Senior Security Technical Lead, Cloud Computing, for NIST. Iorga spoke at the event.

To help agencies get it right, NIST is drafting several cloud security-related publications. For instance, its Cloud Computing Security Reference Architecture will help agencies select cloud-based services based on their requirements. NIST is also working on a publication that will apply the risk management framework to the cloud. It's not really a question of "if" agencies embrace cloud computing within their enterprise, but "when," says Iorga. Cloud has potential, and agencies must prepare to make the move.

Data Protection Done Right

There may be lingering perceptions the cloud is not secure, but that just isn't true, says Loren Hudziak, Solutions Architect, at Google. It doesn't matter where an agency's data is stored. How it is protected determines whether or not it is safe, he says.

"Asking questions like, 'Where is your data located' does nothing to prevent you from getting attacked," says Hudziak. "The question you need to be asking is how is our data protected and secured."

Google uses a distributed architecture that sends multiple copies of pieces of data to at least two geographically distributed data centers, says Hudziak. It also has more than 500 dedicated security professionals, supports defense in depth and multiple layers of security.

Cloud-based platforms have an advantage when it comes to mounting an effective defense against large-scale attacks, says John MacKinnon, Senior Manager, Public Sector Channels and Programs, at Akamai Technologies. More sophisticated and frequent attacks are on the rise, including distributed denial of service attacks, he says, but Akamai

is able to thwart these before they hit the data center.

"Absorbing those attacks on the edge it will make it easier than to fight the fight at the data center level," says MacKinnon. "Wouldn't you rather have visibility to the end where the access end point for the person coming in (is located)?"

Akamai and Google are both FedRAMP-compliant cloud service providers. The General Services Administration's Federal Risk and Authorization Management Program (FedRAMP) offers a standardized approach to ensuring cloud services and products are secure. GSA recently announced some changes to the program in the hopes of expediting the cloud service provider review and approval process.

"We're never going to compromise security, but the way we tackle authorizations and go about it can change," says Ashley Mahan, FedRAMP Agency Evangelist, at GSA. FedRAMP wants to increase the speed to authorization to six months, she says.

FedRAMP also plans to increase transparency into what's available for agencies and who is providing it, pilot a baseline set of high security controls, and help match cloud service providers with agency needs. "We're here to make sure the cloud the federal government uses is secure," says Mahan.

Prepare Your Culture

For some agencies, security isn't the top concern when it comes to the cloud. Establishing the right culture to support this non-traditional approach to computing is the stumbling block.

Cloud security and cloud technology have been proven. Agencies just have to be ready for it, says Michael Fairless, Branch Chief, US Securities and Exchange Commission. "We don't have a lot of time left to wait for the cloud," says Fairless. "We've got to go out and find it ourselves. In order to do that, we need to think about culture."

People's mindset needs to change. So too does the manner in which agencies communicate the message. "Are we thinking about them in a traditional approach or thinking about them through innovation and an agile approach," says Fairless. They must have a common frame of reference that explains "the why" and a common language for everybody to use within the organization.

For the SEC, the cloud proved to be a faster and cheaper solution than the on-premises approach. The agency awarded a contract last November, and already has its first data center workstation up and running. The aim is to build systems that will help the SEC catch securities fraud perpetrators in in less than a year or in real time.

Ultimately, agencies must find a way to build capabilities that "empower the skeptics, engage the innovators, and embrace the customers," says Fairless.

At the Defense Department, communicating the why and how of cloud computing, including where it fits into the mission, was essential for adoption of the technology. "Know why you are going to the cloud," says Robert Vietmeyer, Associate Director for Cloud Computing and Agile Development, Enterprise Services and Integration Directorate, at the Office of DoD CIO. "What is the value proposition?"

Cloud can help organizations save money, reengineer platforms, re-host existing systems, and improve agility, says Vietmeyer. However, not everything can move to the cloud. DoD didn't turn to the cloud initially because it didn't trust commercial or off-premises solutions.

Building a solution itself in its own data centers proved culturally difficult, says Vietmeyer. The people, processes, technologies and vendors, were all "wrong" for the cloud. Since then, the agency has outsourced low-impact, public-facing applications to the commercial cloud and is currently moving its moderate impact, unclassified systems to the commercial cloud.

The gradual approach also made sense for NASA. It takes a lot of upfront work and patience to move to the cloud, says Roopangi Kadakia, Web Services Executive, at NASA. Know your stakeholders, culture, champions and detractors, she says. Make sure you develop specific goals, outcomes and objectives. "Take a phased approach. Do not try to boil the ocean."

NASA was an early cloud adopter. Since then, it has migrated more than 160 applications to the public cloud. After some consolidation, that number is now down to about 100. "When I started at NASA, cloud was just a five-letter word," says Kadakia. Since then, she says the cloud has been the biggest game changer in government.

Ultimately, cloud has to deliver better service or better prices in order for organizations to adopt it, says Dr. Paul Tibbits, Deputy CIO for Architecture, Strategy and Design, at the Department of Veterans Affairs. "The more we can do with cloud where it makes sense and there is an obvious value proposition, we want to do that," he says. The major impediment to moving to the cloud is not being able to articulate the value proposition.

At the VA, cloud computing, as with other investments, must fit into the department's overall strategic plan, says Tibbits. "We're trying as we move forward to make the VA strategic plan more impactful on the rest of the decision making throughout the department." One of the department's initiatives is improving its strategic sourcing—buying the right thing at the right price and right time. This includes cloud services.

It makes more sense to buy something that already runs, instead of developing it in-house, says Tibbits. This buy-first approach helps off-load complexity and takes advantage of the knowledge and expert talent pool in industry "that will be harder and harder for us to get," he says.

Discover a more modern way of working

Everyone works better together, anywhere, at any time - securely. Harness the true power of your people. Make the shift to modern government enterprise with **Google Apps for Work.**

Secure

Unrivaled architecture for security you can trust

Smart

Work better, faster, from anywhere

Proven

Trusted by millions of businesses

Communicate | Store | Collaborate | Manage

Government Solutions from Google. Make the shift today.

Google for Work

www.googleforwork.com

Session Highlights

Here are some take-aways from the individual sessions

SESSION 1

Office of Information and Technology: Building Veteran IT—Together

Speaker

Dr. Paul Tibbits, Deputy CIO for Architecture, Strategy and Design, Department of Veterans Affairs

Dr. Paul Tibbits

"It's **impossible** to have **satisfied customers** if you don't have **satisfied employees**."

- The value proposition for cloud computing has to be clear for it to be attractive to organizations.
- The VA needs to focus on systems thinking and end-to-end process reengineering to improve service and reduce its costs.
- Seventy-nine percent of veterans who receive care from the VA also see private health care providers, so the VA should share data with these providers to improve patient care and outcomes.
- The MyVA vision includes plans to: create seamless, integrated, and responsive VA services; identify common services such as HR and IT; establish a culture of performance to raise issues at the local level; create more strategic partnerships; and empower employees.
- The Center for Veteran Experience is developing Vets.Gov, which is a single electronic face to the veterans.
- The VA wants its strategic plan to drive its resourcing activities.
- The VA is looking at what cyber security standards are needed to protect medical devices.
- The VA wants to use strategic sourcing: Buy the right thing at the right price at the right time including cloud.

SESSION 2

Making the Commercial Cloud Government-Ready

Speaker

Robert Vietmeyer, Associate Director for Cloud Computing and Agile Development, Enterprise Services and Integration Directorate, Office of DoD CIO

Robert Vietmeyer

"**Cloud implementations** at the enterprise level look **more like programs**, and if you don't resource it and approach it that way, I think you're going to **get yourself in trouble** if you think this is like a software buy."

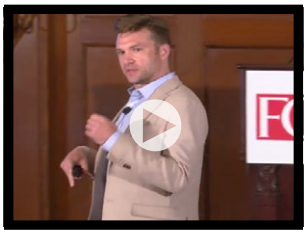
- Know why you are moving to the cloud, know where it fits into the mission and know the value proposition.
- The maintenance cost of legacy systems impacts DOD's ability to invest in new things.
- Lessons learned: avoid cloud washing where old products are repackaged as cloud products; write cloud policies applicable to all IT services in general; know that the cloud doesn't solve all your needs; some cloud solutions are thin in what they can do, so know your responsibilities; it is culturally difficult to build your own cloud.
- DoD has moved public facing applications to the commercial cloud. It's more challenging to move moderate impact systems and core DoD workload to the cloud.
- It is challenging to extend network defense operations into the cloud.
- DoD wants to open some facilities to let vendors operate clouds from within that environment.
- Cloud is hard especially at the enterprise level; it takes a lot of integration with directories and the networks.
- Don't approach the cloud like software buy.
- Have to reengineer to take advantage of how cloud operates.

SESSION 3

Can Your Data be Safer in the Cloud?

Speaker

Loren Hudziak, Solutions Architect, Google



Loren Hudziak

"You cannot fight the **battle of the future** using the technology of the past."

- On-premises systems are not necessarily more secure than systems in the cloud.
- It's not where your data is located that is important, but how it is secured and protected.
- Attackers are becoming more sophisticated and are finding ways to circumvent traditional, outdated approaches of data protection such as perimeter defenses, which are expensive to maintain, easy to target, and can be breached.
- Google designs its own data centers, chip sets, motherboards, servers, planetary scale file system.
- Google uses a distributed architecture to shred data, and distribute multiple copies to at least two geographically distributed data centers.
- Google has more than 500 dedicated security professionals, believes in

Session Highlights, *continued*

defense in depth and multiple layers of security.

- Compliance and accreditation are important, but they offer a false sense of security.

SESSION 4

Overcoming the Cultural Barrier

Speaker
Michael Fairless, Branch Chief, US Securities and Exchange Commission

Michael Fairless

"We don't have a **lot of time left** to wait for the cloud ... We've got to **go out and find it ourselves**. In order to do that, we need to **think about culture**."

- The cloud isn't a technology challenge or a security challenge, but rather a culture challenge.
- SEC designs systems to monitor, track, identify, control and prosecute people suspected of security fraud.
- It's harder to identify securities fraud today, but the stakes are higher. The difference between a 14 millisecond and 13-millisecond trade equates to $10b to $20b in profit to someone.
- To build systems and data science capabilities to help SEC catch perpetrators in in less than a year or in real time, the agency needs a massive amount of processing capability.
- An on-premises approach proved too slow and expensive to get up and running, so the SEC turned to the cloud.
- It awarded a contract in November, and already has its first data center workstation up and running.
- With cloud, don't take a traditional approach, develop a common frame of reference (the why) and a common language, and avoid ambiguity.
- Build capabilities that find a way to empower the skeptics, engage the innovators, and embrace the customers.

SESSION 5

Building Cloud from the Ground Up

Speaker
Dr. Michaela Iorga, Senior Security Technical Lead, Cloud Computing, NIST

Dr. Michaela Iorga

"I am a strong believer that you can **get a better solution in the cloud** if you do it right than something that you can do **in-house**."

- By 2022, there will be between 75 billion to 300 billion networked devices in use.
- The backbone of the Internet of Things is the cloud. The cloud has potential, but agencies need to be ready for it.
- Every minute on the Internet, there are more than 204 million e-mails sent globally, 4 million Google search queries, and 2.4 million pieces of Facebook content shared.
- Identity thefts, ransom ware and government breaches are on the rise.
- NIST supports agencies move to the cloud through special publications including:
- SP 500-299 Cloud Computing Security Reference Architecture, a draft of which has been reviewed by the public.
- SP 800-174 Security and Privacy Controls for Cloud-based Federal Information Systems, which is a work in progress.
- SP 800-173 Cloud Computing Security Reference Architecture 800-173, which is in draft form and applies the risk management framework to the cloud.
- Agencies should leverage FedRAMP to make the process to the cloud cheaper and better.
- Agencies are responsible for the entire cloud ecosystem.
- NIST is working on an Open Security Controls Automation Language, which would help customers compare cloud services from different providers, speed up FedRAMP's assessment process, support security SLAs and metrics, and make automated continuous monitoring possible.

SESSION 6

Partner Insights

Speaker

John MacKinnon, Senior Manager Public Sector Channels and Programs, Akamai Technologies

John MacKinnon

"**Absorbing those attacks** on the edge it will make it easier **than to fight the fight** at the data center level."

- Akamai Technologies, the world's largest cloud platform, has more than 210,000 servers at more than 2,300 locations around the world.
- On a typical day, the company responds to more than two trillion requests, delivering almost 30 percent of daily web traffic.
- In addition to delivering content and applications to users faster, Akamai also defends applications and sites against those trying to attack them and bring them down.

Session Highlights, *continued*

- Akamai has more than 100 federal customers and many state and local customers.
- The company went through the Joint Authorization Board level FedRAMP process and has a provisional authority to operate.
- Denial of service attacks are still the most prevalent, however threats targeting the application layer are on the rise.
- The government experienced about 1.3 percent of DDOS attacks and web application attacks.
- Combining the company's FedRAMP Content Delivery Network with a certified cloud solution provider may help agencies capture more value from their cloud strategy in less time.

SESSION 7

The Evolution of FedRAMP

Speaker

Ashley Mahan, FedRAMP Agency Evangelist, GSA

Ashley Mahan

"Everyone can agree with me... **we want authorizations faster**. We're never going to **compromise security**, but the way we tackle authorizations and go about it **can change**."

- FedRAMP is focused on four key improvements: increasing speed to authorization to six months, increasing transparency including what's available and who is providing it, piloting a high security baseline set of controls, and help matching cloud service providers with agency needs.
- The FedRAMP agency evangelist outreach efforts include: increase awareness of the FedRAMP process, improve the FedRAMP agency authorization process, develop acquisition contract language, advise internal agency process, and encourage interagency collaboration.
- A FedRAMP agency authorization is required at the point when federal data is transitioned to the cloud service.
- Between June and December last year, agency authorizations increased 53 percent, JAB authorizations increased 25 percent, and training enrollees increased 340 percent.
- GSA is starting a FedRAMP agency working group.

SESSION 8

Pitfalls to Avoid on the Road to the Cloud

Speaker

Roopangi Kadakia, Web Services Executive, NASA

Roopangi Kadakia

"Used a **phased approach**. Do not try to boil the ocean. You have to **have a strategy** of where you want to go."

- In the beginning of your cloud effort, know your stakeholders, culture, and champions and detractors. Then make sure you develop goals, outcomes and objectives.
- From a cloud perspective, make sure the strategic plan aligns with the results your agency wants.
- Cloud lessons learned: Use a phased approach (clean it up, standardize it and optimize it); in procurement focus on the problem not the solution; when migrating applications realize it won't be perfect and unforeseen situations will occur; align strategic goals of the agency; realize competition for experienced cloud personnel is high; build security in and automate as much as possible; know your architecture and build it correctly in the cloud; and be able to measure outcomes, objectives and goals.
- Challenges in the cloud include: the hybrid model, which is the way of the future; commercial software as a service and the security model; and mobile applications.

SECURE YOUR
CLOUD with
Akamai
amazon
web services
TOP CONTRACTS
GSA
CIOCS
SEWP V
DLT

CLOUD ADOPTION

Government Cloud Adoption Efforts Lag as Security Concerns Persist

When the Obama administration's CIO declared that the government would move to a cloud-first policy for its technology procurements, it was sending a clear message that agencies would be expected to modernize their IT shops.

But five years later, that transition still seems like it's in its early stages, according to Mark Kneidinger, director of the Federal Network Resilience Division at the Department of Homeland Security. "In 2015 many agencies are still using cloud computing similar to 2010," Kneidinger observed during a recent field hearing members of the House Oversight and Government Reform Committee held in San Antonio.

Many of the applications that agencies have shifted to the cloud might be considered commodity IT, such as email or collaboration tools that CIOs sometime describe as the low-hanging fruit—functions that can be moved to the cloud with relative ease and minimal disruption. But agencies have been far slower to migrate more elaborate, mission-oriented systems, and legacy IT remains in widespread use throughout the government.

Shutterstock

SECURITY MISCONCEPTIONS

Hurd: Feds' cloud security concerns are overblown

Is security the biggest issue facing federal agencies that are considering a move to the cloud? "It shouldn't be," said Rep. Will Hurd, (R-Texas) at the Bloomberg cloud computing conference in Washington on Nov. 17. Hurd said some of the most forward-looking and sophisticated cloud applications in the federal government are being used by the CIA.

As one of the key Capitol Hill watchdogs on federal IT, Hurd thinks the federal "Cloud First" policy and the Federal IT Acquisition Reform Act are levers to push the federal government out of its current IT inertia. He remains solidly behind both, and promised to come down hard on laggards in his position as chairman of the IT Subcommittee of the House Committee on Government Oversight and Reform.

"Server-huggers will have an uncomfortable time" if they appear before the committee to talk about why they're lagging behind on IT reform efforts, Hurd said. According to Hurd, agency concerns about cloud security are a "huge misconception." None of the recent high-profile government computer breaches have been made through a cloud provider, he noted.

PUBLIC CLOUD SUCCESS

NASA presents a 'flagship' example of public cloud

As agencies look at migrating services to the cloud, NASA's move to a public cloud infrastructure has become a use case for speed, cost savings and increased security.

The space agency is currently using three different kinds of cloud environments: the private AWS GovCloud for protected data and information that falls under International Traffic in Arms Regulations (ITAR); internal networks, which run in GovCloud or on hybrid virtual private clouds; and the AWS public cloud, which hosts the majority of the agency's apps and web services.

Approximately 15 percent of NASA's applications and websites are hosted in private clouds, with the rest in public or hybrid environments, according to

Roopangi Kadakia, web services executive in NASA's CIO Office.

CONTINUED SECURITY CONCERNS

Security Concerns Continue Amid Cloud Adoption

While most top IT executives at companies of all sizes continue to express concern about the security of data in the cloud, that hasn't slowed their move to embrace this new infrastructure as a home for corporate data. A new survey and report reveal their top security nightmares and provides some recommendations about how to protect data in the cloud.

The Internet of Things (IoT) generates a lot of data, which organizations can store in the cloud. But how are they keeping it all safe?

Many companies are realizing they face this challenge and are ramping up efforts to improve data security as they embrace new platforms, including IoT and cloud-based applications, according to a recent survey conducted by 451 Research.

TOP SECURITY THREATS

The dirty dozen: 12 cloud security threats

Enterprises are no longer sitting on their hands, wondering if they should risk migrating applications and data to the cloud. They're doing it—but security remains a serious concern. The first step in minimizing risk in the cloud is to identify the top security threats.

As the RSA Conference last week, the CSA (Cloud Security Alliance) listed the "Treacherous 12," the top 12 cloud computing threats organizations face in 2016. The CSA released the report to help both cloud customers and providers focus their defensive efforts.

The shared, on-demand nature of cloud computing introduces the possibility of new security breaches that can erase any gains made by the switch to cloud technology, the CSA warned. As noted in previous CSA reports, cloud services by nature enable users to bypass organization-wide security policies and set up their own accounts in the service of shadow IT projects. New controls must be put in place.

Shutterstock

TOP SECURITY ISSUE

27 Data Security Experts Reveal The #1 Information Security Issue Most Companies Face With Cloud Computing & Storage

Cloud computing is quickly becoming a mainstay for many technology companies today because of its superior flexibility, accessibility, and capacity compared to traditional online computing and storage methods. But just like traditional storage and data sharing methods, cloud computing comes with its own set of data security issues.

At Digital Guardian, our mission is to provide data security solutions and services to help businesses protect their most valuable digital assets. In doing so, we follow the top data security issues facing companies in today's digital world and work with security experts from all around the industry. As cloud security risks grow, we wanted to compile some tips from data security experts on the most common (and avoidable) issues companies face when it comes to the cloud and securing their data to ensure they avoid security issues and common problems like data loss prevention. To do this, we asked 27 cloud computing and data security experts to answer this question: "What is the number one issue most companies face with cloud computing and data security, and what can they do to address the issue?"