Navigating Complexity and Uncertainty in Cloud Computing

Highlights from a recent roundtable, hosted by the Advanced Technology Academic Research Center (ATARC), in partnership with Palo Alto Networks, August 2023

In a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Palo Alto Networks, experts from federal agencies shared their experiences navigating the complexities of cloud computing. In this ever-evolving field, uncertainty abounds as agencies adopt and integrate into hybrid work environments, cloud-native applications and multi-cloud platforms.

Adding to the uncertainty are the complexities of cloud security and the lack of technical resources available to many agencies. Procurement practices, hiring skilled talent, continuous training and the future of artificial intelligence(AI) are other challenges agencies are facing in the evolving cloud computing landscape.

The Current State of Cloud Computing

Agencies kicked off the discussion by sharing how they've successfully transitioned to the cloud. Panelists noted that having a talented team consisting of both contractors and government employees with strong technical capabilities is critical. Similarly, fostering a culture of continuous learning and agile adoption is also important to successful cloud migration and implementation. Agencies that have been successful with cloud provide training in various cloud technologies and then follow through with implementation. The combination has helped to create momentum and improve retention.

> **"People don't want to get trained and not implement the technology."**

Throughout the roundtable discussion, panelists repeatedly emphasized the need for continuous training. Cloud applications are in a state of perpetual change, which means the training received a year ago is likely outdated and may even be obsolete. This can create friction between staff and leadership, since training can often become costly and time-consuming. One panelist noted the importance of in-house opportunities to train and engage employees in cloud technology, including the Cloud and Infrastructure Community of Practice supported by the General Services Administration (GSA).

Small agencies on the panel shared insights on the challenges of implementing cloud computing with limited resources. Although they might be just starting their cloud migration journey, small agencies are able to model their approach from larger, more advanced agencies. Small agencies can also rely on larger agencies for resources when significant security events occur, but are often overlooked when requesting resources of their own. In some cases, small agencies wait for systems to fail in order to receive attention.

Other agencies on the panel operate in a hybrid environment where most applications are in the cloud, and some remain on-prem. This coincides with a strategy to shift from cloud migration to optimization, which involves running workloads as micro services within containers. Agencies are also exploring the potential for virtual call centers.

Panelists noted that each major cloud provider (Amazon, Azure and Google), may offer features or capabilities useful to agencies in different situations and environments. However, managing and securing multiple cloud environments remains challenging.

Trends in Cloud Security

Panelists are already seeing shifts in cloud security trends as the industry moves from individual products to single operating platforms. Operating from a single platform would increase visibility and security and likely grant customers significant savings from an operational perspective.

Currently, the majority of agencies use a proliferation of tools, plug-ins and solutions. Each comes with their own set of vulnerabilities. Managing and securing dozens of tools can quickly become untenable. The solution to operating and securing complex, multi-cloud environments may be a convergence to a single platform combined with AI and machine learning (ML).

However, streamlining is easier said than done. Panelists recommend analyzing current environments, to determine how the tools are being utilized and how they connect with other systems and applications. Conducting an inventory helps with procurement, and the governance process.

Cloud Computing in Hybrid Work Environments

Recent events such as the COVID-19 pandemic and the SolarWinds cybersecurity breach have significantly impacted security in hybrid work environments. However, the biggest challenge agencies are facing with cloud computing is the constant change in cloud service.

Cloud service providers are constantly changing features, offering new options and implementing new features, all of which government agencies must be aware of. Agencies can no longer “set it and forget it”. Staff must constantly learn new features and ensure systems are properly and securely configured.

Smaller agencies are especially challenged by the intricacies of securing hybrid work environments. From ensuring workers remain compliant on home networks to preventing attacks on data centers, under-resourced agencies must consider all aspects of a hybrid work environment. Simply migrating operations to the cloud will not solve these problems. The intricacies of migration are complex and each aspect must be thoroughly considered.

Other challenges include data migration from hybrid environments to the cloud and sharing data outside the organization. Agencies also have lower visibility into hybrid environments, which limits their ability to determine access and identify vulnerabilities.

Cloud Services and Procurement

Procurement is considerably more challenging with the proliferation of cloud services in government. Licensing is extremely complex, particularly when SaaS products require multiple user licenses. Transparent pricing and fees are uncommon among vendors, and agencies struggle to estimate the true cost of procuring new solutions. Often, agencies will meet with vendors and go to conferences in order to not only learn the solution, but also learn how to license the product correctly and cost efficiently.

Internally, agencies may work with dozens of contracting officers, each with their own process and timeline, resulting in disjointed and uncoordinated procurement and added complexity. Depending on their tenure and skill, contracting officers may not know how to put together complex technology contracts. However, there are procurement strategies available to streamline the process in particular situations. The way contracts are written can significantly streamline operations, security and available support in this changing landscape.

> **“Building in roles and responsibilities to contracts, especially when it comes to cloud, is super important.”**

As agencies consider multi-cloud, they should also consider procuring holistic cloud security solutions rather than relying on piecemeal security tools. However, this approach may differ depending on the size of an agency. Smaller agencies will likely continue operating in a single cloud environment with one cloud provider who offers security.

For larger agencies operating in multi-cloud environments, they may choose to have a third-party manage the security of all cloud environments or have a security advisor from one cloud provider oversee cloud security. Panelists noted that it is rare for a federal employee to be skilled in all three cloud environments.

In an ideal world, large agencies would follow a top-down strategy for cloud security. This would create uniformity in how to approach cloud security contracts, upgrades and changes. However, reality is much different. Currently, one agency component or division develops its own unique security strategy based on a specific business need, which moves them ahead in terms of technological advancement.

Meanwhile, other agency divisions remain stagnant waiting for resources or policy guidance. While the divisions may operate within one agency, they are progressing at a very different rate. Because governance was not set up at the beginning of these modernization efforts, there are significant mismatches in system capabilities within one agency.

> **“If your parent organization can't move as fast as you, you're going to end up with this problem.”**

However, business needs and capabilities must be taken into consideration. One system may not work for agencies with different missions and operating locations. Agencies with disparate missions may report to the same parent organization, so a top-down strategy for cloud computing may not be effective or strategic. Even if a parent organization mandates an enterprise solution, smaller agencies may not have the technological maturity to implement the solution.

In addition, smaller agencies often spend significant time and energy keeping old systems running, and do not have the resources to determine what technology they should be implementing. Similarly, procurement vehicles are slow to change. What was optimal pricing in year one will not be optimal in year three. However, agencies may not be able to change contracts because of these price discrepancies.

Managing Security Across Multi-Cloud Platforms

Managing security in a multi-cloud environment starts with a strategy. Agencies should understand the business need for multi-cloud, and then consider governance policies. Governance policies should be consistent across each cloud environment. Then, agencies can consider the personnel and expertise needed to support the multi-cloud environment.

Hiring the right number of teams to manage multi-cloud environments is critically important. Having one team to manage multiple environments may result in significant overtime and lead to an increased risk for technical debt. Panelists recommended hiring one team for each cloud environment, but relying on cloud providers for support is likely still necessary.

> **“Your business requirements are going to be coming at you at a faster rate than you can ever retrain anyone to meet them.”**

Agencies should also pay attention to the support provision in contracts. Not every cloud provider manages support agreements the same way. Some are more responsive and experienced compared to others, so support levels should be factored into multi-cloud governance strategies.

AI and Cloud Security

While most agencies on the panel are awaiting official guidance on artificial intelligence from the Office of Management and Budget(OMB), they agree there are likely merits to using artificial intelligence to enhance cloud security. From automation to identification and remediation, AI will likely play a large role in cloud security in government. However, the process to approve new services is lengthy and may take several months to complete.

Key Takeaways

- Invest in continuous training to stay up-to-date with cloud computing. Staff should attend yearly conferences and routine training offered by vendors to ensure systems are operating correctly and securely.

- Adopt an agile culture. Agencies must adopt new technology and concepts quickly in order to be successful within the ever-changing cloud environment.

- Take advantage of cloud services. Often, lifting and shifting an application into the cloud is more expensive than building a cloud-native system. Take advantage of the cloud’s cost saving opportunities and get the most benefit out of the cloud by scheduling when servers are offline, utilizing smaller systems and auto-scaling.

- Consider holistic security of cloud computing. As cloud computing continues to mature and as agencies begin to consider multi-cloud, visibility into cloud security will become more important.