No Longer Pie in the Sky

The Cloud, Once Considered Exotic or Impractical, Is Emerging as a Pillar of Modern Defense

When lives are on the line, timing is everything. Forces on the ground must be able to access information in real time to make critical decisions. The same is true for cyberoperations; without lightning-fast performance and access to real-time information, it's virtually impossible to prioritize tasks, allocate optimal resources and make the best decisions.

Defense Department agencies today often run into roadblocks in both of these mission-critical areas, hamstrung by slow networks, storage and computer constraints, and legacy infrastructure that makes it difficult to maintain smooth operations.

By way of providing solutions to those challenges, cloud computing allows Defense agencies to build, deploy and rapidly innovate operations. Moreover, cloud services improve the availability, accuracy and timeliness of the intel that advances missions while keeping troops safe. These benefits have resulted in a groundswell of support for cloud computing within the Defense Department.

Network performance is critical to forces on the ground. Moving workloads to the cloud creates important military benefits, such as the ability to quickly send and access data and infrastructure. To meet the demand for high-speed operations, cloud

Joseph Eddins, Airman Magazine

providers are investing in high-bandwidth networks that make it possible for agencies to quickly scale, from basic virtual machine to high performance compute workloads. Combined with powerful compute and storage resources developed by major cloud providers – a robust capacity that exceeds the Defense Department's current needs – these features will help the Defense Department to modernize military forces.

Innovation is driving operations into the cloud. Access to advanced cloud-based infrastructure and applications make it possible to leverage advanced analytics and other advanced information resources. Those capabilities, delivered in the most usable formats, provide insights to data analysts and resources when and where they need it.

Moving to the cloud is a major step in modernizing Defense infrastructure, capabilities and applications, without having to replace resources already in place or dedicate scarce IT staff to the task.

Pentagon leaders are voicing support for moving operations to the cloud. "Accelerating DoD's adoption of cloud computing technologies is critical to maintaining our military's technological advantage," Deputy Defense Secretary Patrick M. Shanahan said in a January memo.

The Defense Department is putting its money where its mouth is, awarding huge contracts such as the Joint Enterprise Defense Infrastructure (JEDI) cloud acquisition that is underway. The Army, Navy and Air Force are making awards, as well. Undersecretary of Defense Acquisition and Sustainment Ellen M. Lord recently urged Defense agencies to embrace the cloud as an agent of change.

"If we keep doing business the same old way, our software will be outdated, it will cost far more than it needs to, we won't be able to attract the best software talent, and we'll lose our technological edge," she said. "Change is uncomfortable, but as I tell our team all the time, we need to get comfortable with being uncomfortable."

A NEW OUTLOOK

For Defense agencies, the cloud's benefits are surpassing perceptions of risk.

While there has been progress in cloud adoption throughout the Defense Department over the past few years, many agencies have spent months or even years researching their options without taking action. Now, for the first time, cloud computing is at an inflection point, largely because decision makers view the benefits of adoption as being greater than lingering perceptions of risks.

Staff Sgt. George Davis

"The time has come, and the best way for agencies to approach cloud adoption today is simply to get started," said Derek Strausbaugh, chief digital officer for Microsoft's DoD team.

When moving into the cloud, it's important to assemble a capable team early in the process. Getting the right people involved in a cloud project – and getting input from all stakeholders – is crucial to avoiding unexpected roadblocks. The team should include everyone expected to work with or benefit from cloud technology, including developers, security specialists, IT operators and mission experts.

It's also important that the core tea m understands how cloud technology works and its expected impact on mission. "Investing in the workforce is more important than you might think, because expecting them to just pick it up doesn't work well," Strausbaugh said.

Resistance to change is by far the biggest non-technology impediment that agencies face when adopting any new technology or work process. Even if you try to do everything right, "cultural blockers" could get in the way.

"There is still a perception that the cloud is a threat to the way things are, but that's a good thing," Strausbaugh said. "Doing things the way they have always been done requires a lot of human capital for things like maintenance and monitoring. With the cloud, these tasks can be automated, done more reliably and cost effectively. It's not about replacing people but elevating their responsibilities so they can focus on things like how to optimize mission outcomes."

Existing policies also can impede the progress of cloud adoption. For example, policies for gaining access to data often vary among programs. Standardizing these requirements makes it easier to build appropriate controls for everything from data labeling and granular data access to just-in-time access – precisely the types of controls that work well in cloud computing environments.

Another "cultural blocker" is the time it takes to procure and deploy technology. The process of getting an application approved or platforms deployed to run on a Defense network can take months. It's simpler and faster to stand up applications in the cloud's more streamlined and agile environment. Efficiency is particularly important in a large department like the Defense Department, which manages thousands of applications throughout the world.

Then there are the technical blockers. One of the most problematic is the proliferation of legacy technology, among them mainframes, applications written in long-dead languages and virtual machines. Much of that legacy tech doesn't work in the cloud. Agencies that rely on legacy technology often are reluctant to let it go.

Virtual machines, for example, were the pinnacle of modern computing at one time. The key is finding a way to bridge the transition, and vendors have many viable options. Microsoft worked with VMware to develop a bare metal service that runs VMware on Azure Compute in the cloud making it possible to migrate applications optimized for VMware. While this method doesn't provide the same level of cost savings and agility as native cloud-built apps, it does allow Defense agencies to reuse their VMware-optimized applications

Security is another potential tech blocker, although it shouldn't be as much of an issue today because cloud vendors working with the Defense Department must comply with DISA's Cloud Computing Security Requirements Guide (CC SRG), FedRAMP, and security requirements specified in the Defense Federal Acquisition Regulations (DFARS). Some vendors also must comply with requirements of the International Traffic in Arms Regulations (ITAR).

When workloads move to the cloud, cloud providers become responsible for the physical security. A secure software-defined network handles the ingestion and departure of data between DoD and the cloud. Depending on the type of cloud services used, cloud providers can also become responsible for the security of the presentation and application layers. This makes it

DOD'S SECURE NETWORK IS COMPLICATED, WITH POINTS OF PRESENCE ALL OVER THE WORLD

much easier to implement secure solutions all the way up to the application level.

The cloud makes agencies more secure in other ways. Incidents of human error or misconfigured systems that can result in security breaches are less likely to happen in the cloud. And because agencies are no longer responsible for overseeing security standards, the risk of security inconsistencies declines.

Legacy networking can also be an impediment to effective cloud adoption. That's especially true for Defense agencies; the DoD's secure network is complicated, with points of presence all over the world, and unique needs for inspecting and blocking traffic. While agencies typically have local networks, they often rely on DISA or other Defense entities for "last mile" connectivity" to the cloud.

Because of these complexities, it is critical that cloud service providers work closely with the agency to understand requirements. With the right information and expertise, cloud service providers can recommend the optimal solution in a software-defined networking approach while adhering to security requirements.

THE PAYOFF

Agencies migrating to the cloud forecast greater efficiency, nimbleness and security.

Despite the challenges of modernizing IT through cloud computing, the effort can pay off in a big way.

"When you go to the cloud, you've modernized your applications, [so] you can get data out of the application," said DISA director Army Lt. Gen. Alan R. Lynn in a December symposium. "If you can take a lot of different applications and pull the data out of them, that's powerful."

One Defense agency has spent the past few years working on ways to use cloud services to modernize its mission, especially in the area of logistics. At the start of the project, the agency had more than 20 data centers, thousands of applications and a mix of legacy technology. It adopted a cloud-first approach that included modernizing applications, adopting Azure SQL for database services and shifting resources from Defense data centers to third-party data centers. Today, the agency can develop and disseminate new applications to users much more quickly. These apps can more easily migrate data across applications, allowing disparate groups to share information in new ways. As a result of this process, the agency has closed data centers more quickly than anticipated.

Elsewhere, another Defense agency is porting all applications to the cloud — everything from mainframes to simple web apps and portals. This platform-as-a-service (PaaS)-first approach requires some unique and creative capabilities that include everything from .Net and Linux to open-source database services and data warehousing workloads. When finished, the agency expects significant cost savings and greater operational agility.

For the Defense Department, the process of moving functions and services to the cloud is clearly gaining momentum. Results will be apparent by next year, industry observers predict.

"The future is bright," Strausbaugh said. "There is a better partnership between government and industry than in the past, and the fact that there is a willingness to look at the tactical edge illustrates that there is a level of trust developing between the Department and the cloud service provider community to not only operate at or above the level of security DoD expects, but to be able to deliver these critical services in a timely fashion to satisfy what is the most demanding customer anyone could ask for."

Staff Sgt. George Davis