Keys to the cloud: Unlocking digital transformation to enhance national security

According to recent research, federal spending on cloud computing is anticipated to grow from $6.8 billion in 2020 to nearly $7.8 billion in 2022.

As this adoption accelerates, the information environment remains highly distributed and riddled with duplicative information, hindering decision makers with limited access to authoritative data, poor data integration across disparate systems, and low-quality data. This, paired with the "anything you can do, I can do better" mantra adopted by today's nation-state threat actors, has left mission-critical information vulnerable to attack as it undergoes the great cloud migration.

These agile threat actors – without any red tape to stand in their way – have already adopted a cloud-centric mindset, oftentimes at the expense of our national security. Meanwhile, emerging technologies like artificial intelligence and machine learning that lend themselves to assisting defensive efforts are rendered useless unless the defense community focuses more time, energy and resources on becoming cloud-centric.

Ultimately, the issue of national security hangs in the balance, and the best way to ensure we stay ahead of the curve is by using the cloud to "digitally overmatch" our opponents and unlock the full potential of digital transformation.

Overwhelming opponents

Originally coined by the Army, the concept of "digital overmatch" stems from the idea that the respective branches of the military can easily overwhelm their opponents on the

ground due to their superior resources. Now, in the era of cyber-enabled conflict, this concept can also be applied to the non-Defense space. Given that data is such a strategic asset, defenders must ensure they can outpace and outmaneuver adversaries by using data-driven technologies such as the cloud, and deliver on-demand resources across all domains whenever and wherever they're needed.

Without commercial and government innovation in cloud-native technology, federal agencies and the military are unable to maximize the full potential of their modernization strategy.

"Digital overmatch" in action

By leveraging the concept of digital overmatch, a warfighter on the battlefield can become one with the sensor grid, capturing and receiving information – from instant language translation to situational awareness – in real-time. Simultaneously, commanders can see the big picture or drill down to a specific element on demand, accelerating decisions with accurate, timely information to deny adversaries any advantage. Additionally, the cloud offers the ability to hyperscale in real time.

For example, if a high-ranking official wants to see if they can move a specific group of soldiers who are currently overseas, there's a great deal of information they must capture and digest as quickly as possible. Are they trained on artificial intelligence? Are their shots up to date? Are they adequately equipped for the desert terrain? This data currently may sit in 15 to 20 different systems, necessitating weeks or even months of analysis to determine if they're ready to be deployed.

With a cloud-centric philosophy, commanding officers could have all this information at their fingertips and make well-informed decisions regarding their combat readiness in a matter of hours or even minutes. By having this information at

the ready, better-trained troops with specialized equipment can be deployed faster, ultimately saving lives. Instead of hardware like aircraft carriers, guns or bullets being the deciding factors in modern conflict, data has quickly become the most valuable battlefield currency.

Digital transformation and national security: Implementation hurdles

Despite the clear benefits of a cloud-centric approach, there are still hurdles to overcome to move toward widespread adoption. First and foremost, all internal stakeholders must be trained to maintain a digital cloud mindset to use the latest technologies for their intended purposes, which can take valuable time. There's also a common misconception that if data is in the cloud, it's more susceptible to fraud, theft, or attacks by cyber actors, when the opposite is true.

With a properly designed cloud environment, data is more resistant to ransomware, while also being more accessible. In fact, without the cloud, a zero-trust architecture that ensures information is categorized and protected would be impossible to control. Regardless of these hurdles, a cloud-enabled future offers countless benefits and enables workflows to easily keep up with innovation, user demand and regulations.

A step in the right direction

So, where can federal agencies start on this digital transformation journey and what can they do to put together an operating model for multi-cloud capability? For some, the process might seem overwhelming or too expensive, but the reality is there's no need to start from scratch.

Instead, agencies should look to their peers to guide and inform their cloud journey, as many organizations – public and private sector alike – already have the knowledge and

solutions readily available to help expedite this migration at both speed and scale. For example, the Air Force has been recently leading the way via their Cloud One offering, which is able to migrate all their systems to the cloud while also developing them natively. Federal agencies don’t need to reinvent the wheel to successfully adopt a cloud mindset.