Unlocking the potential of data is a critical endeavor at the Defense Department, and officials are investing in cloud, automated capabilities and zero-trust cybersecurity to store, optimize and protect data in a modernized fashion.

“Data provides us a competitive advantage over our adversaries,” Army Undersecretary James McPherson said at Tuesday’s AFCEA Army Signal Conference. “As with any strategic asset, we must manage and protect our data, and we do this through a hybrid of multiple-cloud ecosystems.”
“Combined with a reliable secure and resilient network infrastructure and aided by artificial intelligence and machine learning, timely access to trusted data will shorten the commander’s decision cycle, enabling better decision-making,” Army Cyber Commander LTG. Stephen Fogarty added. “To be effective, data must be delivered on demand, quickly and automatically. Effective data management requires a reliable and secure data infrastructure and data storage supported by hybrid systems to optimize the benefits of the cloud while allowing greater control and security.”

While DOD continues to work toward hybrid multi-cloud IT infrastructures, a zero-trust cybersecurity approach will also be critical to securing that environment, Fogarty added. Defense Information Systems Agency Cloud Portfolio Manager John Hale advocated a similar approach during Wednesday’s FCW DOD Cloud Workshop.

Securing data with zero-trust cybersecurity is essential with the push to cloud-based services and applications, Hale said. DISA and DOD are looking to increase software-as-a-service (SaaS) in particular, which has compelled Hale's team to evolve from defense-in-depth security to zero trust and zero trust architectures (ZTA).

“Zero trust and ZTA models are going to push us to where we put more and more requirements on SaaS providers in order to meet our security requirements,” Hale said.

The “as-a-service” model that cloud capabilities offer will also aid defense officials in consolidating their networks and data. Fogarty said that Army Cyber Command’s (ARCYBER) data is largely stored in disparate, siloed infrastructure, making it difficult to query data across systems and easier to waste resources and deployment time for making decisions. As ARCYBER looks to integrate and consolidate its data assets, Fogarty wants to move toward enterprise-IT-as-a-service.

“Command-centric network operations will also be part of establishing a global enterprise command and control structure, which will depend on critical initiatives, including enterprise-IT-as-a-service,” Fogarty said. “Enterprise-IT-as-a-service, or ITaaS, is foundational to command-centric network operations.”
Army Futures Command is largely leading the Army in this network modernization effort, creating an integrated tactical network for improved battlefield communications and integrated enterprise networking driven by cloud business and infrastructure services and applications. Army Futures Command AI Task Force Director Brig. Gen. Matt Easley highlighted during a Tuesday ATARC conference the role of the cloud in getting a handle on data to improve AI capabilities and push modernization forward.

“We’re bringing in a whole series of cloud technicians, so we understand how to move our data from our signature systems from the battlefield from a distributor environment, up to a cloud environment to do analytics, and then, again, eventually do AI and machine-learning models, and then move those models and the inference part back down to the edge,” Easley explained.

The Navy has also seen benefits from the cloud in scaling up and expanding data-sharing capabilities in its modernization efforts. Although the Navy was already eyeing the cloud, the mass move to telework with COVID-19 created massive networking demands across the enterprise, and a cloud infrastructure supported the needed network and data-sharing environment for successful remote work, Navy Program Manager Capt. Ben McNeil said.

“We not only need to support Navy, [but also] military folks, civilian folks, also our defense industrial base — our partners around the Navy all have a need to be able to carry with us to be able to share data,” McNeil said. “Our modernization and transformation effort is geared toward building a network the Navy needs to supply the cloud, to be able to support.”

Underlying all of these modernization efforts, regardless of the pressure that COVID-19 has created across the military, is the need to safeguard and optimize data.

“Data must be systemically collected from many platforms and sources, consolidated and stored securely,” Fogarty said. “Transporting data to decision-makers and other users will depend on having an integrated backbone network that is secure, reliable, resilient and adaptable form the enterprise to the tactical edge and back when they can operate in a contested information environment. An integrated network will also help break down data silos, enable interoperability and deliver data at the speed of need."
View printer friendly version
DOD
IT modernization
cloud
data
Zero Trust
AI
Army
Navy
DISA
Standard