TOP TAKEAWAYS:

Secure Collaboration for Defense

Every builder needs a toolbox,

equipped with the assets that can tighten loose screws or assemble parts to fortify a larger foundation. The beauty of a toolbox is also its agility and portability, for faster effectiveness in various environments. Moreover, it collects all resources in a single place. Cloud technology has become the agency toolbox with vast potential, in particular when it comes to unifying disparate communications technologies, as the pace and nature of warfighting continues to change and the need for more immediate and impactful communications grows ever larger.

Federal agencies and the Defense Department recognize this urgency around cloud technology adoption. Key aspects of a strategy released by DOD in February 2019 emphasize speed in adopting cloud and taking a "warfighter first" approach in a modern age of warfighting where the battlefield transcends physical environments into digital. In tandem with changes to warfighting, the federal cloud-first policy shifts the landscape for communications for defense agencies and those they serve. The Cloud Smart Strategy, released in October 2018 as an update to the cloud first mandate, provided updated and specified guidelines aimed at fostering cloud adoption and implementation in government. With this step, the federal government formally recognized a greater need for secure collaboration, which is an integral part to military success.

Cloud-enabled collaboration tools that unite disparate communication platforms are a central component to the mindset of DOD leaders as they look to modernize the defense infrastructure and support their employees in the field. In a world with more and more tools available, agencies need streamlined communication tools that offer simplicity and flexibility and mission enablement with security baked into a solid, yet agile, foundation.

Currently, defense agencies are about four to five years behind the curve when it comes to IT collaboration. A large majority of military personnel rely on basic analog and digital technologies, restricting the use of collaboration tools like video conferencing and instant messaging. At the core, DOD needs to step back and create a holistic view of how the cloud can help with mission enablement without risking the safety and security of the warfighter.

Here are the ways Cisco's Hosted Collaboration Solution for Defense, or HCS-D, with Impact Level 5 security authorization, answers that call for smart technology and provides the communication in any way, shape or form to collaborate across a team.

Four Crucial Tools in Your Communications Toolbox

Simplicity

It can be difficult to close the gaps when consolidating information and getting the most critical communications across the battlefield, especially in the midst of time-sensitive warfighting environments. The unique high-pressure environment for everyday military stakeholders adds complexities to achieving efficient communication. Tools need to be created with warfighters in mind — it's not as easy as translating commercial communication solutions into the defense space. As opposed to commercial transitions to the cloud, where enterprises can quickly migrate tens of thousands of users, DOD needs to take a toe-in-the-water approach with the simplest, yet most effective, tools that can bring its systems together.

For example, commercial retail communication within an enterprise looks fairly simple. Users schedule a meeting, then can join the meeting on one virtual platform with a URL incorporating both video and audio. More informal methods such as instant messaging create rapid ways to contact the endpoint. However, the sensitivity of military missions and elevated need for security creates a unique scenario for DOD. Communications often become siloed and isolates information, making it difficult for leadership to collaborate across the organization. DOD has challenges in reducing communication silos to provide a seamless platform for the warfighter and garrison is a key piece to greater connection. Tailored technologies can help connect warfighters leveraging a new perspective that reshapes the way DOD thinks about collaboration, without disrupting current processes in place.

Enlisting partners who embrace the communications-as-a-service model creates opportunity for DOD and agencies to embrace the Cloud Smart policy with ease. Solutions such as HCS-D offer a joint capable system that pulls together solutions under one manageable umbrella, leaving the infrastructure management to the provider and granting military leaders control through a simple interface. This not only saves money, but frees up personnel to focus on mission enablement key environments knowing that their information is secure with a company such as Cisco, one of only two IL 5 authorized solutions.

Cisco's approach to secure unified communications embraces investment protection for customers as they move to the cloud. The ability to integrate on-premise and cloud-hosted communications is unique to Cisco: customers are able to continue using end-point devices with enhanced capabilities in a DOD-only cloud. While addressing the government's requirements to achieve enhanced return on investment and potential cost savings, DOD leaders want to be assured any new system provide greater security than the status quo.

Cisco HCS-D delivers a secure unified communications platform but also meets the IL5 security requirement. Because this is a cloud-based solution and the solution is pay as you go, budgeting is straightforward and flexible. The pay-as-you-go pricing provides customers greater simplicity, ability to liberate IT resources, no infrastructure capital expenditure, no need to manage upgrades and faster deployment of new, always current services and technology.

2 Flexibility

The safety net for mission critical environment communication needs to be vast and flexible, making sure messages get to the accurate stakeholders rapidly and 100 percent secure. “Today’s warfighters need to move quickly and fast,” says Larry Frazier, former DISA services executive adviser. “An email is not going to cut it if they have to communicate across multiple groups and divisions.”

To evaluate the current safety net, Congress created the Section 809 Panel to address issues with the way DOD buys what it needs to equip its warfighters. Proposing 98 recommendations in a February 2019 report, the panel members expressed concerns around DOD’s ability to have appropriate and on-going communication, stalling movement of equipment and information to warfighters in need. “Advanced communication technologies provide medical care at a distance and coordinate remote deliveries of food and shelter,” wrote David A. Drabkin and Michelle V.J. Johnson, two members of the panel.

“America’s warfighters deserve the same ease of access to the global marketplace of products, services and ideas.”

It is possible to offer this ease of access through teamwork and secure collaboration with a company that knows the ins and outs of DOD challenges. Cisco offers pay-as-you-go service, with no vendor lock-in, and communication methods from single voice to instant messaging to video and video-enabled web conferencing. Interoperability and flexibility are key in the battlefield, required tools to be agile and highly survivable. Small picture, Cisco provides an on-premise option in case access to the cloud is lost, thus enhancing survivability. Big picture, this generates the flexibility for a transition more accommodating to the speed of DOD technology adoption, allowing agencies to move from existing systems fully into the cloud without roadblocking mission success.

3 Mission Enablement

In addition to broader White House and other federal initiatives aimed at securing communications in defense, individual agencies will occasionally have to blaze their own trails around experimenting with cloud-based tools in advance of broader government initiatives. There are still analog cases used in a world of digital, or cases where communication is restricted to purely audio, but these methods aren't going to make the cut as battlefields become more complex. DOD agencies are prioritizing alternative solutions.

Military critical missions move fast. "Communication tends to be disparate and typically the DoD Command and Control systems are not linked together," says Mike Brazawski, a defense solutions specialist at Cisco, who has been working in the industry for 26 years. DOD has to meet the Cloud Smart mandate while considering communications investments already in place so those communication avenues don't get blocked in time of transition. Military personnel shouldn't have to worry about messaging vulnerable to attacks. Understanding the original communication structure and concerns of military leaders, Cisco created built-in automatic messaging encryption into HCS-D.

Cloud-hosted unified communication can improve mission enablement in multiple areas across the organization, not just within leadership, Frazier says."You'd be amazed to look at the environment in a tactical deployment," he says. "They have tents and racks and racks of equipment all connected via satellite communication or multiple satellite links."

But it's difficult to connect to other stations or from the Army to the Air Force, for example. HCS-D is a game changer for large-scale communication. With HCS-D, the CMS platform gives over 200 users the ability to conference together. It's critical to have a provider that can supplement these tactical set-ups with linked tool sets and provide the warfighter with a collaborative platform.

4

Security

Cisco's government-level security means having a dedicated infrastructure for U.S. government customers and U.S. persons only. Each customer has separate deployments for additional separation of agency data. All data, at rest and in traffic, is protected by FIPS 140-2 compliant encryption.

Cisco continuously scans against databases of current global vulnerabilities to monitor against new, emerging threats. Its government-defined architecture is based on IL5 security requirements, and the company follows government-defined service level agreements to address and resolve security incidents. An independent IL5 third party assessment organization conducts regular audits, and the sponsoring agency also does monthly reviews of security statures.

Cisco's app-based policy enforcement and management means configurations and user roles are set at a per-app level. These policies follow users as they move around in the network. Useage features can be customized, managed and enforced.

In the government and defense

environments, there are more security parameters to embracing collaborative technology than there are in the commercial space. Each decision and technological implementation requires a lot more justification. Why use one technology over another? Comprehensiveness and level of security is a key differentiator.

Cisco collaborative communications solutions has achieved Provisional Authorization
Cisco collaborative communications solutions has achieved Provisional Authorization
by the Defense Information Systems Agency at Impact Level 5 making Cisco one of just two companies with solutions under this scope of authorization and a trusted partner of DOD. HCS-D found a need for 24/7 security coverage that ensures the security remains consistent for DOD agencies from the office to the battlefield and filled that gap. "From a DOD perspective, that survivability and safety net for mission critical environments of cloud-hosted collaborative tools is unmatched," Brazawski says. "We're the only one in the industry that can actually offer that."

For more information on HCS-D or to see it in action, please visit cisco.com/go/hcsd or reach out to cloud_ucdod@cisco.com.