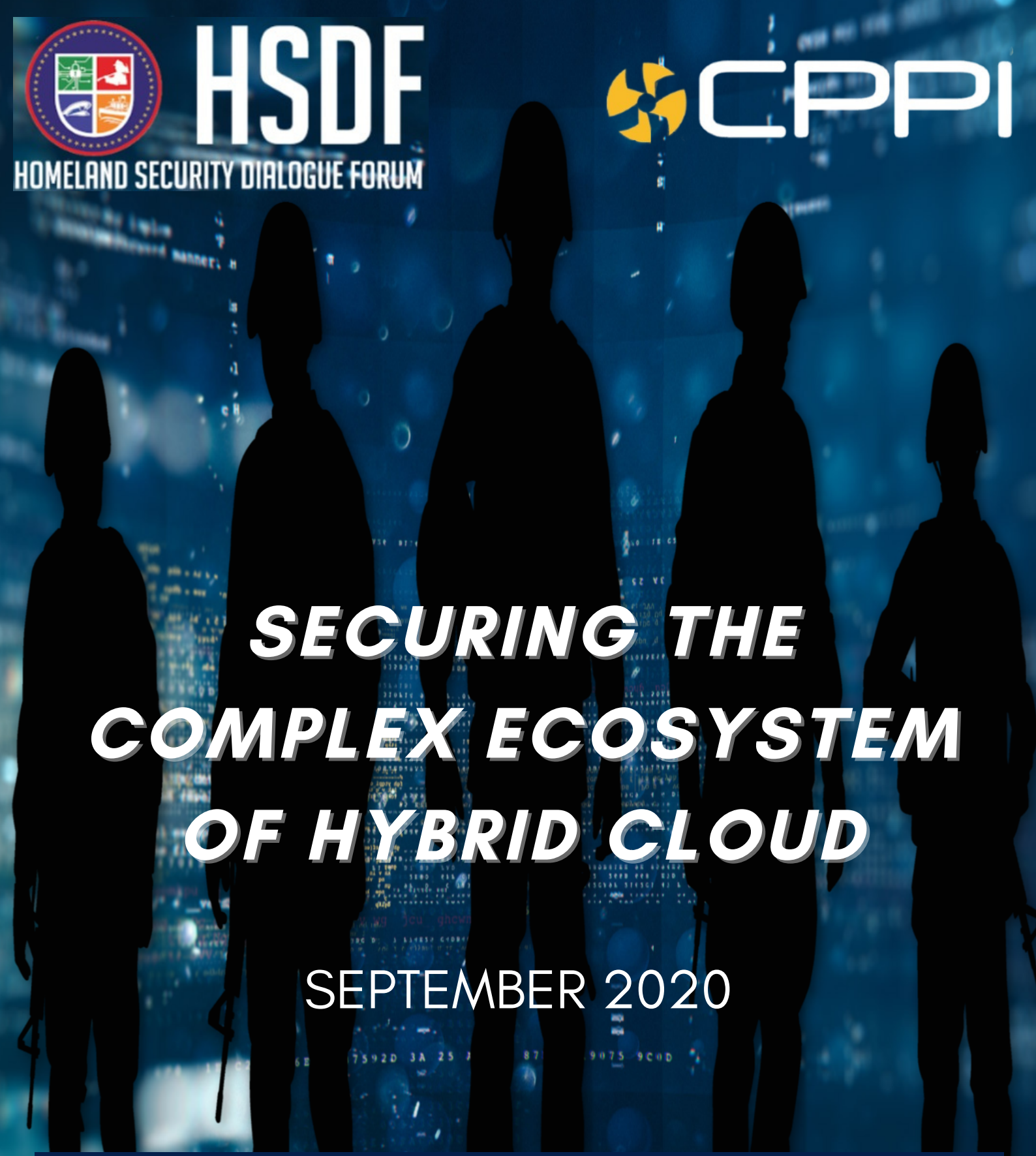


HSDF
HOMELAND SECURITY DIALOGUE FORUM

CPPI

SECURING THE COMPLEX ECOSYSTEM OF HYBRID CLOUD

SEPTEMBER 2020

ORIGINAL REPORT

PREPARED BY THE CENTER FOR PUBLIC POLICY INNOVATION (CPPI)
AND HOMELAND SECURITY DIALOGUE FORUM (HSDF)

INTRODUCTION

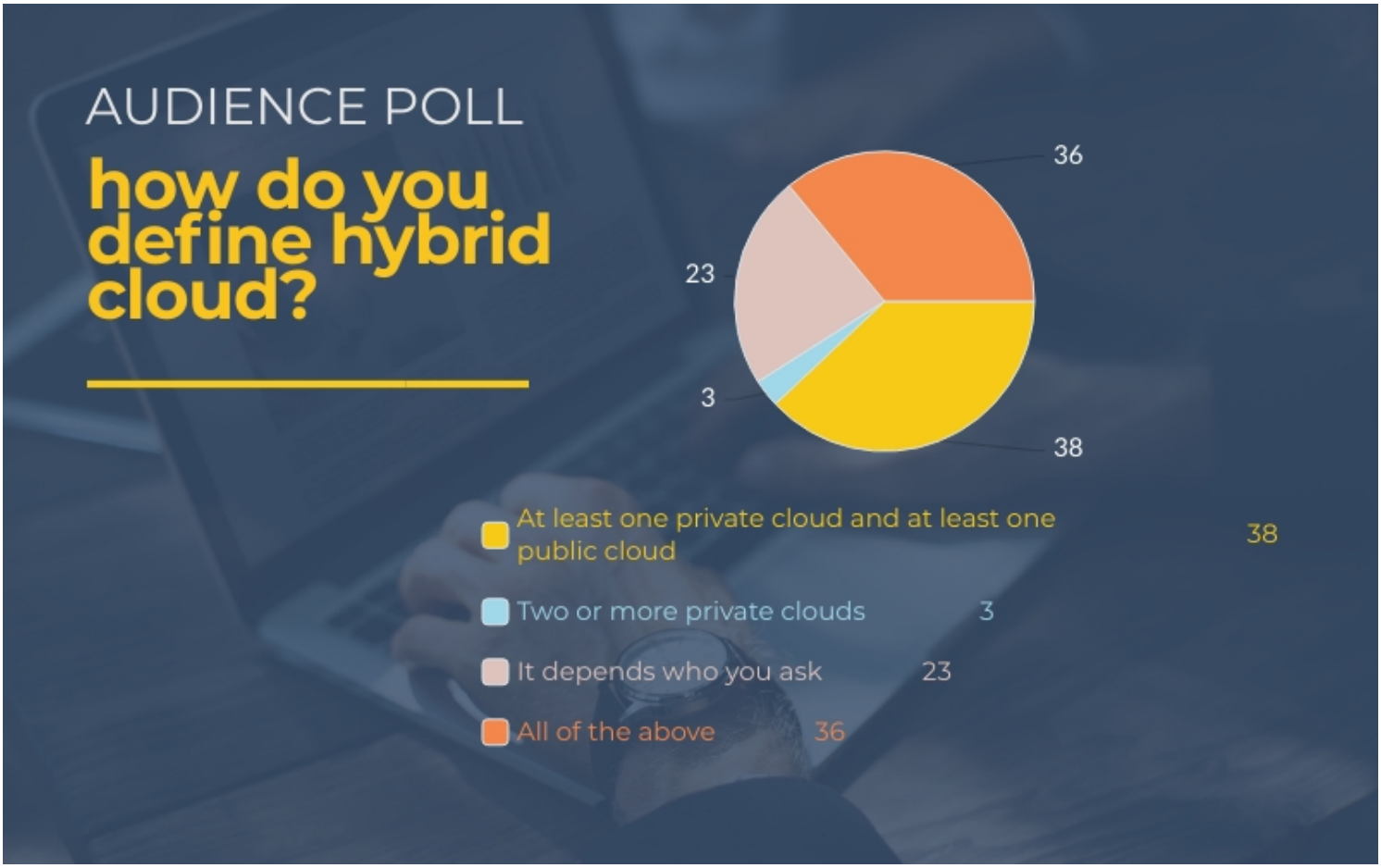
Hybrid cloud environments are more prevalent than ever across federal agencies. It has become apparent that hybrid cloud delivers additional capability across the enterprise to support a vast array of government missions—from enabling data access in remote locations to layering on Artificial Intelligence applications. The flip side to this enhanced capability are new attack vectors and vulnerabilities that emerge as a result of hybrid architecture. Understanding why hybrid cloud has become a necessity for the federal government, along with how to ensure its security, was the major theme of the virtual symposium: *Securing the Complex Ecosystem of Hybrid Cloud*. Hosted by the Center for Public Policy Innovation (CPPI) and Homeland Security Dialogue Forum (HSDF) on June 17, 2020 these topics were explored through a series of keynotes and panel discussions with experts from across government and industry. The following report includes a close examination of a number of topics covered throughout the symposium in relation to hybrid cloud and security across the federal space.

DEFINING HYBRID CLOUD

How does the federal government define hybrid cloud? This question came up throughout the symposium, as different organizations have differing perspectives. Mr. Grant Schneider, Federal Chief Information Security Officer (CISO), commented that "we all live in hybrid environments" and this adds to the security challenges.

A poll of the audience members—which included a mixture of industry and government stakeholders—revealed that a majority think hybrid cloud consists of at least one public cloud and one private cloud. The answer that came in close second was "it depends who you ask" in terms of defining hybrid cloud, which speaks to the remaining ambiguity on this topic across the public and private sectors.

Mr. Neal Ziring with the National Security Agency (NSA) said they define hybrid cloud as a "heterogeneous environment where there is an integration of services and mission systems spread across on-premise systems and one or more multi-tenant cloud platforms." This was the most robust definition offered during the symposium and helps to highlight where some of the security challenges exist.



THE ROLE OF OMB ON CLOUD POLICY & SECURITY GUIDANCE

Situational awareness is fundamental to securing the hybrid cloud environment, according to Federal CISO Grant Schneider. During his keynote remarks he explained that as federal agencies change the shape of their enterprise and architecture, they also increase the threat surface. In addition, the massive shift towards telework during the pandemic creates additional opportunities for our adversaries. Schneider went on to share that the Office of Management and Budget (OMB) is responsible for three main elements to improve security posture across federal agencies to include:

- *Policy guidance*-developing and overseeing policies for agencies to secure their environments, setting those policies, and working closely with agencies on adoption and implementation.
- *Risk management*-working with agencies on a risk management approach that will reduce the likelihood of compromise.
- *Compliance*-ensuring that federal agencies are complying with government-wide security policies, whether that is legislation, OMB or NIST guidance, or directives from the Department of Homeland Security.

"Compliance gets a bad rap in cybersecurity, but remains very important," observed Schneider. "We take what is in FISMA legislation and couple this with the President's directives and make sure OMB's policies are specific, but also broad enough." OMB recognizes the need to strike a balance so federal agencies have flexibility given their different IT environments, but also the ability to successfully adopt these policies.

Schneider also emphasized the importance of the shift from a "cloud first" to a "cloud smart" approach. Moving to a secure environment that encompasses not just perimeter security, but also includes mobile and cloud environments, is key to cloud smart efforts. Federal agencies need to ensure they are providing security for their data wherever it resides. Going back to his initial point on the importance of situational awareness, agencies need to understand "who and what" is operating on their systems.

Finally, OMB has been coordinating closely with agencies on cyber workforce development efforts and implementation of the President's Executive Order on America's Cybersecurity Workforce.

Schneider commented that the ability to reskill the existing federal workforce is critical, along with recruiting more talent to the government. He also commented that individuals that leave the government for positions within industry are still part of the larger cyber ecosystem, and there are opportunities for the public and private sectors to work more collaboratively to leverage cyber talent.

Executive Order on America's Cybersecurity Workforce

The Executive Order will implement the following programs to strengthen the nation's cybersecurity workforce to meet the challenges of the 21st century including:

- promote the work of cybersecurity professionals within the Government, including by creating a President's Cup Cybersecurity Competition.
- launch a rotational program where employees can expand their cybersecurity expertise through temporary reassignments.
- encourage widespread adoption of the NICE Cybersecurity Workforce Framework.
- aim to close skills gaps for defense and critical infrastructure cybersecurity.
- instruct federal agencies to identify cybersecurity aptitude assessments that they can use to reskill employees with potential in the cybersecurity field.
- establish the Presidential Cybersecurity Education Awards to recognize and reward excellent educators teaching cybersecurity-related subjects.

Source: NIST

HOW HYBRID CLOUD ENABLES MISSION SUCCESS

Making the case for strong executive leadership at federal agencies

"It is no secret that cloud adoption has seen double digit growth year after year across federal agencies, "commented Mr. Dan Jacobs with the IT Modernization Centers of Excellence within the General Services Administration (GSA). This figure is expected to reach $10 billion annually in the coming years. According to Jacobs, cloud adoption is happening at a rapid pace because of two major factors:

- *It has become cheaper to adopt cloud*. GSA and other acquisition centers have been constantly adapting to make sure agencies are getting the best value for their dollar. Market research as-a-service and cloud migration templates free for download, for example, make it easier, cheaper, and faster to adopt cloud.

- *Standardization has made it easier for agencies to make risk-based decisions when moving to the cloud*. Obtaining Authority to Operate declarations, or ATOs, have always been one of the biggest hurdles for cloud adoption, but now there is strong federal governance in place to make ATOs work faster. Also, FedRAMP allows for rapid adoption of solutions that are low risk.

In working with over a dozen federal agencies through the GSA IT Centers of Excellence, Jacobs observed that what works at one agency doesn't necessarily work at another. Agencies that have been most successful at executing a cloud smart strategy have strong executive leadership in place. "Strong leaders empower agencies to make informed decisions to drive business outcomes. CIOs like Maria Roat and Dave Shive are known for a reason. They have a dogged commitment to modernization. This is hard work and it takes a lot of resolve. They prepare the battle space, then execute with excellence."

Panel moderator Ms. Margie Graves, the former Deputy Federal CIO was in agreement, "There's such a huge opportunity to reimagine the [IT] services, and that takes special leadership."

One agency that has experienced success with cloud adoption is the State Department. Mr. Brian Merrick who leads the Cloud Program Management Office discussed some of their unique operational needs including having 275 posts around the world, geographic separation, a multitude of functions and needs, and different data classification levels. Cloud adoption has been critical to help meet their mission. Ms. Mahtab Emdadi with Dell Technologies discussed their experience in supporting federal customers and commented, "We are seeing the savvy CIOs realize that cloud isn't a place, but an operating model. It is important to leverage the innovation and not the technology."

BEST PRACTICES FOR SECURING DATA IN THE CLOUD

For security, data is at the core, and choosing a cloud that has encryption all the way across is important for federal customers, according to Mr. Mark Johnson with Oracle Corporation. Once there is an encrypted cloud in place, agencies then need to make sure the infrastructure and applications are secure. Security built-in at all layers reduces risk, especially since agencies need to assume they are operating in a zero trust environment.

Johnson also offered that agencies can mask their data and experiment with different cloud environments safely. "This can help harness innovation and see what is best for your agency," he commented.

Data security doesn't have to be complex according to Johnson, one impactful way to reduce complexity is using a software-as-a-service (SaaS) model so that agencies can hand-off the complexities to the provider. Merrick with the State Department agreed, "Security operates on a very granular level in the cloud environment and cloud providers have done the really important work on security that government agencies don't necessarily have the resources to do on their own," he commented.

Graves echoed these sentiments saying that working at the data layer is the key to security and agencies need to monitor what is going on with the data. "These environments are no longer castle and moat; it is more Internet as transport." Jacobs with GSA brought up the issue of data ownership in relation to security. "Is the security data lake owned by the Chief Data Officer or the CISO? It seems like a simple question until you start to really consider it," he offered.

THE NEED FOR ZERO TRUST ARCHITECTURE AND THE CHANGING CLOUD THREAT ENVIRONMENT

What defines zero trust? Zero trust has been around for quite some time. The Department of Defense coined this approach a little more than a decade ago and it continues to evolve, commented Mr. Ned Miller with McAfee. NIST has also taken steps to define zero trust for the federal government with an architecture approach. "The good part is that it requires an organization to evaluate their architecture and look at it through a zero trust lens to include all parts of access control to device management. It is a capability set that has to be applied at all parts of a business," commented Miller.

Dan Prieto with Google Cloud described zero trust as not a product, not a technology, but a different way of thinking about the technology. It boils down to the need to authenticate every interaction on a network because trust is not assumed. Network access is based on the user and attempts to use applications and data. "The way to get to the future of security is to focus on outcomes," he commented.

Federal agencies are at differing stages when it comes to understanding zero trust and there is no one-size-fits all approach to their security needs, observed Miller. Different organizations have adopted capabilities to fill unique gaps and it is going to take some time before the whole of government is on the same page.

Mr. Neal Ziring with NSA offered some observations, "The tricky part in a cloud environment is putting zero trust principles into effect that apply consistently across on-prem capabilities and workloads among the different cloud providers." As the federal government moves in the direction of zero trust, agencies need to recognize that the infrastructure and workloads set-up in the cloud are not static.

"We need tooling, instrumentation, and analytics that are similarly dynamic," commented Ziring.

"Zero trust will continue to evolve in terms of the definition. We have guidance from NIST now on zero trust. GSA is starting to talk about the pillars of zero trust. The conversation continues to change and it will likely be three to five years until federal agencies have done the planning in order to begin to implement zero trust," said McAfee's Ned Miller.

One critically important element to the federal government's cyber posture is the Cybersecurity & Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS). "Maintaining visibility into the .gov domain is at the heart of what CISA does," commented Mr. Brian Gattoni, CTO at CISA. "[My fellow panelists] are right, it will be a number of years until zero trust is fully realized, and it is rare that we can all get together and have these kinds of conversations. If we do it right, the visibility is inherent in the tool sets we use for zero trust."

The threat is going to evolve as well, according to Gattoni. "Every time someone wants to move to a different layer in the stack, there needs to be some kind of check in place. Now you're creating new paths, and we can't be so naïve to think the adversary won't try to keep migrating into that world." Baking in the visibility and data planning and logistics functions will be important to achieving zero trust.

THE NEED FOR ADDITIONAL ZERO TRUST POLICY AND IMPORTANCE OF SEMANTICS AROUND CLOUD

Some symposium speakers felt there is more policy that is needed around cloud adoption and security. Prieto with Google Cloud discussed the lag between policy and leading-edge technologies. This lag is often embedded in the efforts of practitioners, and getting to a true zero trust architecture will require additional policy. The NIST draft architecture is a good way to start to inform conversation, according to Prieto and zero trust policies should be less prescriptive and more outcome oriented with a data-centric approach. "The proof isn't in how many tools you adopt, but are you actually migrating towards more user and data centric controls," he commented.

Panel moderator Luke McCormack, former CIO at DHS, recognized that innovation around security is rapidly changing in the federal space. It will be critical to lay down some additional instrumentation that will allow for adoption of these policies as seamlessly as possible.

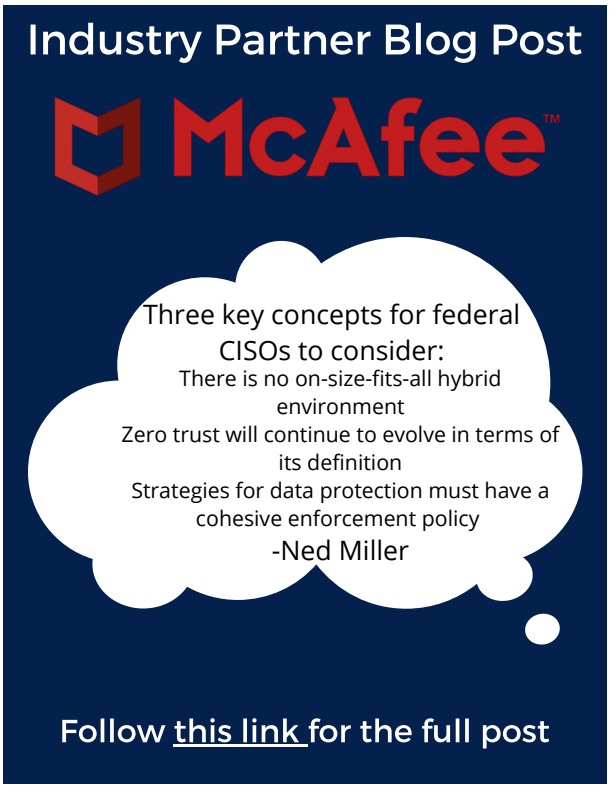
"As agencies continue to think about securing their hybrid cloud structure, they need to have consistent semantic policies around marking and controlling data," said Ziring with NSA. Ned Miller with McAfee agreed, observing that one of the biggest challenges is that there is no single vocabulary across cloud providers to describe securing these environments. This lack of concise semantics can lead to technology sprawl issues within federal agencies.

FILLING THE GAPS IN THE FEDERAL WORKFORCE WHEN IT COMES TO CLOUD AND SECURITY

"For the cloud conversation on talent, we need help in understanding where to go next," commented CISA's Gattoni. The cloud was not first utilized by the government, but rather the private sector, and it is not something federal civilian agencies necessarily develop or own independently, he observed. It takes a different type of skill set, given the nature of the cloud. Gattoni also thinks it is important to develop a "cloud native mindset," so it is not just lift and shift to the cloud, but how agencies can create new capabilities within the cloud.

Gattoni acknowledged the need to start to develop those capabilities within our federal engineers so agencies are not overly reliant on the private sector.

The federal government also needs more talented data logisticians—a group of people that can pre-position the data to support the analysts on the mission-side, according to Gattoni. This would go a long way to support cyber risk operations by better recognizing the logistics layer underneath all the analytics.



THE AIR FORCE HAS EXCELLED AT LEVERAGING CLOUD TECHNOLOGY AND SCALING SECURITY SOLUTIONS ACROSS THEIR ENTERPRISE

Mr. Nicolas Chaillan, appointed the first Chief Software Officer at the U.S. Air Force, commented that this is the first time this role has been adopted within any military or civilian agency, but he suspects we will see more of these roles created in the future. His focus has been on enabling the adoption of innovative software best practices, leveraging Artificial Intelligence and Machine Learning capabilities, while removing impediments to IT innovation.

When it comes to utilizing cloud effectively, "It is all about timeliness and the ability to adapt to challenges," said Chaillan. There are a couple major aspects to the Air Force's success with cloud including the creation of Platform One, along with incorporating the DoD Enterprise DevSecOps Initiative (DSOP) enterprise-wide.

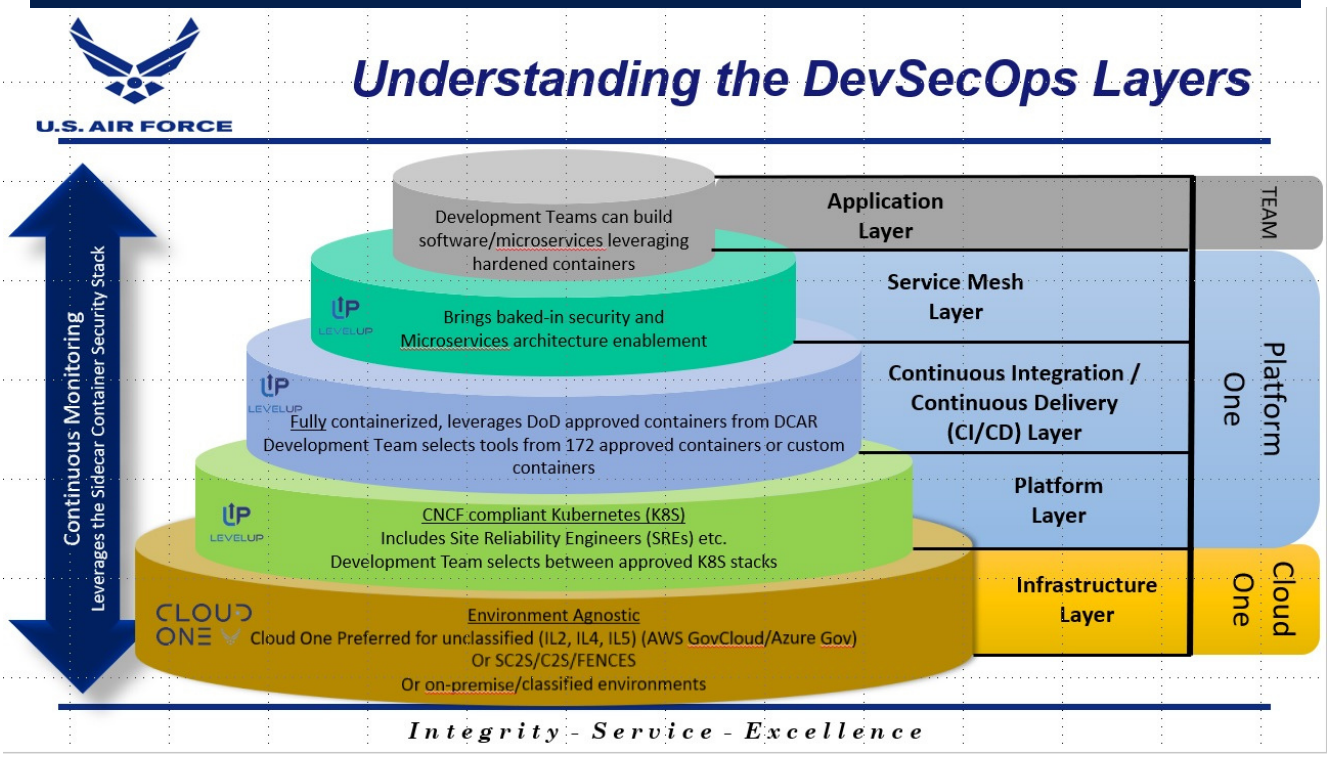
Platform One is a centralized team that provides DevSecOps and Software Factory Managed Services across DoD programs with security baked-in. Interestingly, Platform One is the first DoD-wide continuous ATO. "A critical piece to Platform One and why we have been so successful with adoption and scaling across DoD is that we saved one hundred years of program plan time in just one year by moving to DevSecOps," commented Chaillan.

DoD Enterprise DevSecOps Initiative (DSOP) is focused on using automated software tools and standards so warfighters can deploy and operate software applications securely and flexibly while maintaining interoperability. DSOP ensures that the Air Force won't be locked-in to any one cloud provider and this is really important if you want to move quickly, commented Chaillan. The "Infrastructure as Code" concept is a critical DevSecOps ingredient to ensure that production environments do not drift from development/testing environments. No human should make changes in production environments, said Chaillan, changes should only be made in source code.

The Air Force needs to work as a team, and that makes everything easier, but at the same time it means they are using a lot of complex technologies across a diverse mission space, commented Chaillan. "The key is to make sure you find the right team. When I first started, there were over twenty teams at the Air Force building different platforms and technology stacks. I visited the various teams and selected just a few to help build Cloud One and Platform One. Now we have the best talent in place to tackle our problems," said the Chief Software Officer.

What is really critical to their cloud journey is that the Air Force has many customers and programs across classification levels. Automation, reducing the attack surface, and quickly changing code are key to enhancing security of the cloud, said Chaillan.

To view Mr. Chaillan's presentation in its entirety, follow this link.



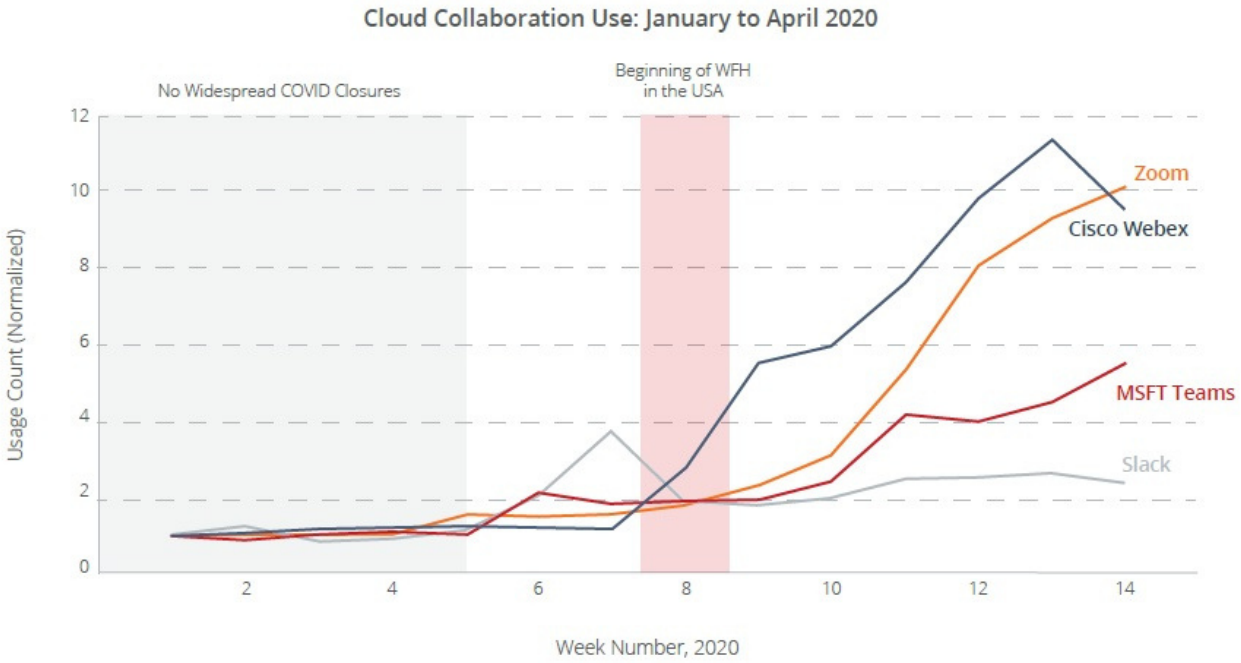
IMPACT OF COVID-19 ON TELEWORK AND NEED FOR FEDERAL IT MODERNIZATION

Emdadi with Dell Technologies commented that the current pandemic has demonstrated that federal customers are getting very smart about when to use public or private clouds. "Our customers needed something to work fast, but now that remote work will stick around for a while, we find ourselves in a place of making this work right. It is exciting to see customers get better at workload placement in the cloud." Johnson with Oracle said that COVID-19 has forced federal agencies to experiment with new things and this could help accelerate innovation.

"Enterprise use of collaboration cloud services has more than doubled since the beginning of the year."
See corresponding graph below
Source: McAfee Cloud Adoption and Risk Report

Congressman Gerry Connolly (VA-11), who chairs the Subcommittee on Government Operations said, "COVID-19 has really exposed a lot of vulnerabilities and shortcomings when it comes to our supply chains, IT systems, and telework policies." For example, the Small Business Administration has been front and center during the pandemic and Congress pumped billions into the SBA within just a few weeks. Their IT systems failed because they were not equipped to handle the volume of traffic, according to Connolly.

Rep. Connolly also commented that this pandemic has helped to demonstrate the benefits of telework for the federal workforce. "I've been an evangelist for telework even before I got to Congress. The key about telework is that it provides us with a core capability to do continuity of operations," he said.



ADDITIONAL ADVICE FOR FEDERAL AGENCIES AS THEY MOVE FORWARD WITH THEIR RESPECTIVE CLOUD JOURNEYS

There is no one-size-fits-all approach to cloud, do not reinvent the wheel

A centralized approach is great for small and medium sized organizations, but large agencies may struggle a bit to get all the business units on board, commented Dan Jacobs with GSA. One misconfigured process can have a large, negative impact and any management software needs to be combined with good governance. If agencies remove the barriers to adoption itself, accelerate risk determinations, and lower the total cost of cloud ownership, they will be on the path to successful cloud adoption.

Nicolas Chaillan with the Air Force recommends agencies have a strong enterprise capability in place, but it doesn't need to be one-size-fits-all, it is important to have options. He also said that there is no need to reinvent the wheel or build things from scratch, take advantage of all the open code and open source offerings. Mark Johnson with Oracle agreed adding that is it important for federal agencies to leverage the work that has been done before, this is something not done enough in government.

Have a holistic view of your cloud environment

"Federal agencies are going to have many different entities using the cloud from on-prem, off-prem, machines, and micro-containers, how do you bind the identity of all these different entities to the actions they perform and the data they create?" asked Ziring with NSA. If this can be accomplished, agencies can have a holistic view of their cloud environment and also the ability to analyze it.

Think about application rationalization

Several speakers on the program encouraged agencies to think about what really needs to be moved to the cloud. "In order to be cloud smart, you need to rationalize applications," commented Emdadi with Dell Technologies. Two critical questions to ask include: Where do I want to work? Where do I have data?

Approach cloud as an operating model, not a place

Emdadi said that when federal agencies embrace this approach, it will reveal the many different cost models available. She went on to add that you know an agency is being smart when they stop issuing a sole-source contract for cloud services, and rather, begin to issue IDIQs for infrastructure-as-a-service. This approach will ultimately help agencies in creating a cloud environment that will enable them to meet modernization goals.

CONCLUSION

As the federal government moves ahead with a cloud smart approach, there are a few items that make success more likely. The first is the need for strong executive leadership on cloud and IT modernization, including CIOs that can take more innovative approaches and recognize that cloud is not just a part of the IT architecture, but an operating model to deliver mission critical capabilities. Taking advantage of tools such as ATOs, open source offerings, and government-wide procurement programs, such as FedRAMP, can help accelerate adoption and reduce costs for agencies. For agencies like OMB and DHS, striking a balance on policy is critical—policy needs to provide necessary guidance and oversight, but also have some flexibility to ensure it meets the needs of individual agencies and is responsive to their unique IT and security environments. Finally, leveraging the innovation and investment already made by the private sector around cloud technologies and security can be incredibly beneficial.

It will take true public-private partnership to continue to build-out and improve cloud environments, as well as move towards a zero trust architecture to secure government assets and data. Building a strong cloud foundation will be necessary for adopting technologies such as Artificial Intelligence and Machine Learning to advance mission outcomes. Hybrid cloud has truly become a catalyst for innovation across federal civilian and military agencies.

To view the full video recordings from this event, click on the tile below.

ABOUT THE EVENT ORGANIZERS

The Center for Public Policy Innovation (CPPI) is a 501(c)(3) not for profit educational think tank whose mission is to assist government officials in addressing the many challenging issues brought on by the rapid advancement of Information Technology. CPPI provides policymakers with groundbreaking thought leadership on transformational technology, informed policy analysis, and innovative strategies to help ensure American competitiveness in the global economy and comprehensive security on the homefront. CPPI convenes educational symposiums, site visits, and other forums that bring together stakeholders from government, industry, academia, and the civic sector to discuss policy issues in a collaborative environment. For more information visit: cppionline.org.

The Homeland Security Dialogue Forum (HSDF) was established in 2003 to boost the level of informed dialogue between the public and private sectors on homeland and national security issues and explore the important role of technology in hardening our nation's vulnerabilities. HSDF has organized more than 450 meetings and other special events with top officials from the Department of Homeland Security; other relevant federal, state, and local agencies; and foreign governments. HSDF is supported by a number of leading technology companies and security solutions providers. For more information visit: hsdf.org.

THANKS TO OUR EVENT PARTNERS:

McAfee Together is power. Google Cloud ORACLE DELL Technologies carahsoft