CIA Focusing On Multi-Cloud Environments

Important to the CIA from a cyber security perspective is understanding how identity, access, application and data access controls in one cloud service provider are accurately reflected in other cloud service providers.

The CIA has a long history with cloud computing primarily focused on infrastructure services. We have made great progress and transitioned to cloud in that space. Commercial Cloud Enterprises (C2E) opens up the aperture much greater with multi-cloud providers offering everything from infrastructure services all the way up to software services.

Michael Mestrovich
Chief Information Security Officer (retired)
CIA

Previously a lot of focus was on your primary infrastructure services — compute, storage those types of capabilities — but we're really now moving up the stack and working with software solution providers for Software-as-a Service (SaaS).

Some of the big challenges that we're working through are hosted desktop services taking advantage of things like Office 365 to provision desktop automation services, email office automation and others. We are utilizing some of the native cloud service offerings such as digital rights management and data loss protection services that are embedded within those cloud offerings. I think there's a lot of great potential with all of those different offerings. I think the challenge for us going forward is understanding the telemetry of a multi-cloud environment and being able to make sense of that so that we have a comprehensive cyber security and operations view into that multi-cloud environment. With the help of great partners, we're anxious to take cloud to the next level.

Top Priorities

Most of the federal government is in the midst of responding to and planning to implement much of the President's Executive Order on enhancing cyber security and we're no different in that regard. There's also a National Security Memorandum that talks about how to enhance cyber security across the board.

A portion of the memorandum talks about migrations to cloud. But there's other compo-

Mestrovich on the Federal Executive Forum

- Vision for the Future
- Top Lesson Learned
- Progress Made
- Top Priorities

nents as well including multi-factor authentication, standardizing auditing and logging capabilities, zero trust and securing software supply chain. The list goes on and on; so the vast majority of our efforts are going to be focused on implementation of the precepts that are identified in that National Security Memorandum.

As we move into this multi-cloud ecosystem, what's important is not only cyber security, but from an operations perspective, getting the telemetry off cloud service providers providing data in their native format; and being able to then normalize that so that we have a standard single view of operational and performance issues as they're occurring in our multi-cloud ecosystem.

> Equally important to us from a cyber security perspective is understanding how identity, access, application and data access controls in one cloud service provider are accurately reflected in the other cloud service providers.

In the same vein we're pulling off that relevant cyber security information amongst those cloud service providers. We want to be able to understand performance characteristics as we have workloads running in one particular cloud service. We also want to know what are the differences if we move that workload to a different cloud service provider; and then how do we track security relevant audits, identity credential management (PKI) certifications across various different cloud service providers.

Equally important to us from a cyber security perspective is understanding how identity, access, application and data access controls in one cloud service provider are accurately reflected in the other cloud service providers. So if you're making a cloud data access decision to access one cloud service provider, when the same individual or the same entity is trying to make other access calls to other cloud service providers, that process should be normal. I think we need to spend more time gaining better insights into a comprehensive cyber security view across all the cloud service providers as they're operating in real time.

Bold Predictions

In two to three years obviously C2S will sunset and C2E will be fully realized. So, what are you thinking about if I'm a software developer in the Intelligence Community (IC) is: What can I expect to have as far as goods and services at my disposal?

I'll make a potentially bold prediction.

Everything is code; no longer do we have network engineers; and no longer do we have system administrators. Everything is code and if you're the traditional network jockey that jumps on a console a command line, you know your days are numbered. If you're a system administrator who's building servers, your days are numbered.

Everything becomes code and that gets us a lot of benefits and consistency in cyber security. We know the way things are deployed, we know automating the cyber security and the assessment process provides the elements that get us to speed of mission. We know there's a consistently deployed application and service throughout our cloud service providers.

Then focusing on decision-making, you have automated machines and automated processes providing huge amounts of data from the applications themselves and the sensors that we have out there.

> Everything is code; no longer do we have network engineers; and no longer do we have system administrators. Everything is code and if you're the traditional network jockey that jumps on a console a command line, you know your days are numbered. If you're a system administrator who's building servers, your days are numbered.

Somewhere on the back end is the AI engine that's pulling all of that together and sifting through the data. I think it's going to begin to tee up decisions for humans, but ultimately we want that engine to make some subset of decisions for humans because it can make those decisions at scale.

Now I think that the question of ethical AI bridges comes in to focus. For example, what what are the decisions we're allowing the machines to go ahead and make versus what are the decisions we want them to tee up for a human.

I will tell you from a cyber security perspective, we want those AI engines to make decisions at the speed at which they're seeing the threats come in. We just don't have enough time and enough people to analyze all those; and so we've got to craft the framework by which we say this is the boundary within which we want the AI engine to go ahead and make the decisions. Beyond that, tee it up for an analyst to come in and take a harder look. ■