CBP: Operating The Cloud In Critical Environments

Besides our cloud migration journey and focus on zero trust, we are laser focused on automation.

Customs and Border Protection's (CBP) largest focus is on zero trust and identity and access management. These are the key pillars of role-based access we're pushing really hard.

We're using tools Okta and Zscaler and we're also looking at a multi-account architecture, which allows us to segment our our accounts so if we have a cyber issue we can actually limit the blast radius.

Ed Mays

Deputy Assistant Commissioner (DAC), Infrastructure and Support Services,

and Chief Enterprise Infrastructure Officer Customs and Border Protection (CBP)

Department of Homeland Security (DHS)

At the same time, one of our largest efforts for the future is having a dedicated procurement contract that will allow us to support our cloud growth, because we plan on being out of data centers hopefully by 2025-2026. That is a top priority for us.

Also we are looking at a cloud services brokerage, to manage all the services for cloud — providing business case analysis, architecture and all kinds of services to our customer base. We're going to go from are minimal services to a full service organization where our app developers can just come in a la carte and choose what they want to work on. We've been doing this a lot so we know there's lots of services that could be provided. That's going to be our big focus.

Understanding & Securing Data

We just pushed out our data strategy for the cloud which makes it imperative that we understand and secure our data. As part of that focus, one of our largest, most important programs is non-person entity security — machine to machine or machine to software communications.

It's critical to make sure those machines actually can authenticate and verify that it's an actual organizational entity that it's communicating with. That's not only pretty important to us; it's a priority not just for CBP, but for DHS and the entire government as well. Doing this is providing a lot of return on investment, because I don't have to

Mays on the Federal Executive Forum

- Progress Made
- Profiles of Success
- Top Priorities
- Top Lesson Learned

guess anymore. I know when you know what those certificates are, who they belong to and when they expire. That makes these certificates pretty important to us.

If you are operating in a mission critical environment, actually having machine learning tell you what's happening in your environment and preventing all unauthorized events from occurring is a game changer for us. When I first came to CBP probably circa 2016-2017, we had outages almost weekly because there was so much information and more than 100,000 endpoints to monitor. This has made our lives a lot better and a lot more controlled and secure.

> While we have made substantial progress, we really want to get to standardized automation by using new tools and having one approach across our enterprise.

Besides our cloud migration journey and focus on zero trust, we are laser focused on automation. While we have made substantial progress, we really want to get to standardized automation by using new tools and having one approach across our enterprise. We have also focused our laser on customer experience, making sure that not only can we deliver code that does what it is supposed to do, but also making sure that it was easy to use and a quick study.

Keep A Close Eye

One of the top lessons we have learned is about monitoring from a cyber perspective — watching what's happening in your environment and looking for potential data loss.

For example, we had something happen in our Office365 tenant; it wasn't a bad thing, but it was one of those things that we were monitoring and you know we actually saw it. We alerted Microsoft and it gave us a lot of confidence that what we were doing was right and was going to protect us.

That's huge because about three years ago we didn't have that. So we're in a much better place in terms of data loss prevention monitoring in terms of security.

As far as the future is concerned, if you look around two to three years from now, I would like to see an environment with an AI powered platform that allows us to create, understand and act on knowledge effectively and quickly. For instance with our cloud services brokerage, we want to be able to architect quickly and dynamically and get the best delivery and fastest delivery for the lowest cost without having a lot of human interaction. I think that's going to drive our value stream and if we can secure that and move it fast, I think that's where we want to go. ■