Thanks to Cloud and Encryption, USCIS Data Stays Secure

A cloud environment is just another data center with minimal controls; it’s the security stacks that matter.

Amanda Ziadeh

Fri, 06/01/2018 - 11:26

Illustration: makyzz/iStock

The cloud and the U.S. Citizenship and Immigration Services have been friends for years, and the agency trusts that having its data in a cloud environment is safer than traditional data storage methods — as long as security is baked in from the start.

Aside from stronger security, having data readily accessible enables data-driven decision-making and improves business and organization processes. But we know this: Government agencies have been told time and time again by cloud service

providers and federal advocates the benefits of migrating to the cloud.

But for USCIS, it also makes users of the data more aware of vulnerabilities and risks, improving security from a personnel standpoint, too.

“Being able to provide that data and build models on it and use machine learning helps them to do their jobs better, and when they see that, it becomes a much higher priority, and security is a piece of that,” said Sarah Fahden, the Identity, Records and National Security division chief for USCIS. She spoke at the May 31 Data Security Summit in Washington, D.C.

And for Fahden, the security aspect of modernizing IT and shifting to development operations was unquestionable. She started her career in IT security before transitioning to big data and software development.

“It was inherent that everything has to be sure from the start, and if it’s not secure, it has to be secured immediately,” she said.

So, contracts at USCIS went from DevOps to Development Security and Operations, or DevSecOps. Essentially, it’s the iterative development methodology with security at the start.

“That’s why I put that word in there,” Fahden said, so everyone on the contract thinks about security from the very beginning, and so there aren't individual security practitioners trying to keep up with numerous teams to make sure what they’re doing is secure. There’s no way one person or two people could do that anyway, Fahden said.

“It’s the job and problem of the entire team, at every single team, and all of the individuals in the team,” she added. “They’re all stewards of what they’re building and the data they’re protecting.”

And about four or five years ago when Fahden was still in her IT security role at USCIS, she was tasked with doing a risk assessment of enterprise Amazon cloud offerings compared to its GovCloud.

After the assessment, she found there wasn't a significant number of additional security measures included as part of the GovCloud offering. In fact, the biggest was that not all of the people managing the physical servers were U.S. citizens, but rather identified as "U.S. persons."

"My answer was that that risk does not outweigh the loss of benefits being in the other environments," Fahden said. "Because in the other environments, you have access to all the latest technologies that Amazon's providing, really quickly."

In the GovCloud, it could take months to years to get those tools.

"And the way we should be thinking about cloud, any cloud . . . is that it's just another data center that provides some minimal amount of controls that we have here," Fahden said, so the rest of the controls are up to the systems and data transferred to the cloud.

So, Fahden's solution was back-end encryption.

"Encryption needs to be inherent in everything that we do, it should be at rest, it should be in motion . . . everything should be encrypted," she said. Encryption was the answer, and that's how USCIS built its cloud environment (along with other necessary and compliant security requirements).

And contrary to the outdated belief that security won't be able to keep up with the speed of DevOps and iterative development, Fahden said it's the opposite. DevSecOps allows USCIS to secure data and applications and to respond to incidents "so much faster," while providing the tools to build in security from the start.

"So the answer to me, to securing our data, is cloud, that is the answer, and encryption," Fahden said.

The Amazon Web Services cloud applications allow USCIS to implement tools like audit logging, configuration logging, continuous monitoring, containers and flexible servers as needed, and quickly. It also uses Chaos Monkey to introduce server failures to make sure certain applications can withstand disruption and remain resilient.

So, as opposed to the "if I can't physically see my data, it's not secure" mentality,

Fahden’s sticking to cloud.

“I would say we are way more secure than a data center,” she said.

View printer friendly version
U.S. Customs and Border Protection
cloud
data
data centers
Amazon
DevOps
DevSecOps
Sarah Fahden