Applying Security To The Cloud Isn't Simple, But It Is Possible, And The Result Is Well Worth the Effort

By Christopher Porter, CISO of Fannie Mae

In 1977, one of the first movies about a data breach was released. Star Wars isn't often thought of as a story about cybersecurity, but it really is an early cautionary tale of the importance of taking data security seriously. Just imagine how different the movie would have been if the plans for the Death Star had better access control, if the Empire's SecOps team were scanning for vulnerabilities, and if the data had been encrypted. The plans would never have leaked, and the Death Star and likely the Empire would have survived.

Fast forward to today, and not much has changed as evidenced by the constant stream of news covering data breaches Ever since the "cloud" became an IT industry buzzword, the topic of security has been a key concern. When cloud technology was in its infancy, many enterprises were reluctant to move applications or information into the cloud because they thought it was too risky. As the cloud industry has evolved, security has improved to the point where it is often more secure to have applications in the cloud than on premises. However, security breaches in the cloud can still happen with regularity. Below are some lessons learned from my experiences in applying security to the cloud.

People, Processes, and Systems. As enterprises begin to migrate to the cloud, there are best practices that can ensure governance and control even in a shared risk and responsibility environment like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform. However, you have to have the right people, processes, and systems in place to identify and consistently implement them. For example, IAM best practices recommend that you ask your team if they know to do the following:

(1) Audit if root keys exist
(2) Identify that users and groups exist, and that users are not getting direct permissions
(3) Check that users comply with company password policy
(4) Identify users who do not have MFA enabled
(5) Validate IAM user utilization, and disable/remove inactive accounts

Beyond just knowing to do these things, your team must also have the skills and expertise to implement these best practices in one or more cloud environments and prioritize their time to consistently execute them.

In part, your move to the cloud is for automation, so you don't want anything that creates manual friction in the security operations process. The reason you pick the cloud is to go faster. One way to address the issue of implementing best practices is through configuration management. With a shared risk model, the public cloud has myriad configuration options. For example, you need to configure access control, network access control lists, etc.

You need to make sure you are configuring your cloud infrastructure in the way that you intended and confirming this through testing and validation. Certain threats and vulnerabilities can be the result of an error of omission, like forgetting to check a box that says, "Don't make this public." These systems need to operate with at least some level of automation to ensure that security measures aren't killing the very speed and agility that makes operating in the cloud attractive.

People: Build Your Talent. As alluded to above, one risk of moving to the cloud is the lack of available talent in the cloud security space. Cloud security specialists are in high demand, and there simply isn't a large enough supply. (On that note, if you have a relative in college, tell them to study cloud security architecture.) The takeaway is that the people who know how to apply security to the cloud, who understand threat protection and response in the software-defined infrastructure world of the public cloud, are hard to find. You must build these people from the inside and then put in place appropriate retention mechanisms to ensure that you don't lose them quickly to someone else.

"When it comes to the cloud, security can never be an afterthought."

Processes: Collaboration. As the security team navigated our way through the cloud migration process, we recognized that the key to success was in our ability to collaborate with the architecture organization, the development organization, and the infrastructure organization throughout the build. Our security processes could not be created in silos. Security can't simply walk in and apply policies to the cloud environments in a vacuum. This will result in friction, which will decrease the value of the cloud. This is ultimately where the discipline of DevSecOps comes into play. You have to change the culture of the security organization to work collaboratively across the entire organization from the very inception of your organization's cloud strategy.

Systems: Understanding Build vs. Buy. You have to know who you are as a company and think about the approach you are going to adopt in the fast-evolving world of cloud security. For example, Fannie Mae is a very COTS oriented company. We very quickly realized that you couldn't just take your legacy COTS products and apply them to cloud infrastructure and have them work effectively. You have to understand the controls you need to apply to the cloud to make it as secure as you need it to be from the beginning. You then need to determine whether to build or buy. If you choose to buy, you have to find the right systems that will support this option. Given the rate of change in the cloud, I think it will be difficult for most organizations to effectively build and maintain the tooling. However, the key is that you should not try to simply take your legacy tools and try to make these work in the cloud environment. For example, you can't simply take your traditional database monitoring tool, and apply it to the native database services in the cloud. This was one of the biggest challenges for us – getting over the hump of not being able to just move things over. If you are using cloud the right way, you need to use cloud-native services to reap the benefits.

4th Party Risk Management. One area of security concern relative to the cloud is 4th party risk management. This seems to fly under the radar, and it should be a core component of your cloud risk management framework. Many companies think that by simply using the cloud, they gain resilience, but this isn't entirely true. We see an increasing number of vendors who are all exclusively using IAAS. If you aren't aware of what clouds, and wherein those clouds, your vendors are placing the services that are delivered to you, then you are overlooking a key risk area. Even if the vendor runs their application across multiple availability zones in a single cloud, they are susceptible to a single vendor dependency risk. Having a systematic approach to managing 4th party risk will become increasingly important as more companies move to the same cloud, and often even the same "part" of the cloud.

Get Right, Get Small, See Big. So how do you put all of this together? My strategy at Fannie Mae is called, "Get Right, Get Small, See Big." In order to get it right, you need to fix known security gaps and then get small by shrinking the attack surface. Seeing big is made possible by having the right visibility that allows you to react to incidents in more efficient manner.

Build it Right from the Beginning

When it comes to the cloud, security can never be an afterthought. If you build it right from the beginning, you can greatly improve security and reduce risk. In fact, you can achieve a higher level of security than legacy infrastructure. With legacy infrastructure, you can be constrained to insecure footprints where the fixed infrastructure and legacy interrelationships between systems make it difficult to make changes. However, with the cloud, you can set things up right from the start and fully segment your environment, including clean segmentation between development, testing, and production. Because a cloud environment is brand new, you can make sure you have the right access control and separation of duties and build your cloud infrastructure in a more automated way. You have the opportunity to do it right in the public cloud, if you are patient, build the right team, and collaboratively implement the right processes and systems from the beginning.

Christopher Porter

Christopher Porter is Fannie Mae's Vice President and Chief Information Security Officer, reporting to the Senior Vice President and Head of Operations and Technology. In this role, Porter helps to communicate the importance of information security across the enterprise and to develop Fannie Mae's defense and response capabilities. He is responsible for all aspects of cyber security at Fannie Mae – including emerging threats/ risk mitigation, policy development, and protection of the firm's data and systems assets.