Bill Rials:

Why Automation is the Key to Better Cloud Security

William (Bill) Rials, Ph.D., is a professor and associate director of the Tulane University School of Professional Advancement Applied Computing and Technology Program. Before transitioning to academia, Rials served in CIO, CTO and CISO roles for local governments in Mississippi. He also served as deputy CIO for the state of Mississippi, where he crafted the blueprints for the state's first hybrid cloud strategy and served as chair of the statewide Chief Information Officers Council.

We recently spoke with Rials about how cloud is driving the need for new capabilities around managing and securing complex hybrid and multi-cloud environments and how automation can help address these challenges.

COVID-19 accelerated cloud adoption in government — everything from hosted collaboration platforms to cloud-based call center technology. These solutions were adopted rapidly, and often by organizations with little cloud experience. What do these governments need to be thinking about now?

As cloud services become a staple in any organization's portfolio, greater agility and faster infrastructure changes are the norm. This creates compliance and security governance challenges for government organizations that use traditional, slower-moving IT methods. The primary issue is traditional IT methods can't respond to the speed and agility of the cloud — and IT professionals and end users alike have more power than ever before in their hands with the cloud. Additionally, cloud infrastructure is growing in complexity, requiring specific skillsets.

Because of the ease of availability, many IT professionals are experimenting with public cloud services without fully understanding the complete details from a security perspective. This vastly increases the overall risk profile. Virtually every security breach involving data hosted in public clouds involved incorrect configuration by humans that ended up exposing information or other critical assets.

What are some of the common security mistakes government organizations make when it comes to cloud?

Most organizations still use traditional IT tools and techniques to manage cloud security and compliance. Cybersecurity traditionally has been based on physical security concepts. Think about a medieval castle. The purpose of the castle was to keep the people and contents on the inside safe. The defenders would build high strong walls, towers, a moat and other layered perimeter defenses. Cybersecurity professionals call this concept defense-in-depth. Then the castle defenders would build a drawbridge to control and limit the access into the interior of the castle from a single point. This is like cybersecurity professionals installing a firewall and intrusion detection and prevention tools at the network border to control ingress/egress to the protected assets inside the network. This type of security architecture is fundamentally at odds with today's cloud architecture. Using traditional cyber defense methods will not be successful in a cloud environment.

How can government organizations address cloud security more effectively?

As jurisdictions move to the cloud, it's important to consider automating cybersecurity to remove the human component from the equation. Using proper cloud automation procedures reduces the chances incorrect configurations will be made when utilizing cloud resources.

Cloud assets also should be thought of as an interconnected group instead of individual devices. Depending on the vendor, these may be called managed instances, network security groups or other terms — but they are essentially a group of cloud resources bound together with common security rulesets. Each group could consist of multiple devices such as firewalls, routers, servers, databases, etc. In automated cloud security, the policies and rulesets are placed around the entire group and are agnostic of any public cloud provider. This is especially evident in hybrid cloud computing where a resource group may migrate from an on-premises private cloud to a public cloud infrastructure and retain all its security governance rulesets.

What are some things government organizations should keep in mind when it comes to cloud security automation?

A major aspect of automated cloud security involves configuration governance. Benchmarks should be used to create blueprints of the security configurations in the cloud environment. Any new workloads created in the cloud should leverage these blueprints using automation and orchestration procedures as opposed to manual configuration.

Additionally, the configuration governance should check for ongoing changes and updates and compare against the blueprints automatically. Due to the speed and agility of cloud, configuration governance in the cloud should be automated as close to real time as possible.