CLOUDVISORY

CASE STUDY 01 | AWS SECURITY

With Cloudvisory we now have granular visibility, management, audit and enforcement of security policies in AWS allowing us to more rapidly expand.

This Service Provider has been experiencing explosive growth over the last few years. A global leader of cloud services for customer engagement, communications and collaboration. Their offerings are designed to help companies worldwide, improve service.

Their growth has been enabled by the cloud – Amazon Web Services (AWS) specifically. AWS has allowed them to scale operations quickly, supporting thousands of customers via their cloud based applications. With over 4000 virtual instances and growing, the company has a lot to manage.

With such rapid change and a need to support customers from all over the world, responsibility for security policies was pushed to developers who began scripting policies as part of their orchestration processes. What seemed like a good idea during early phases of the company, quickly became a concern for the Security Organization as the company grew.

The concerns were:

1. How could they know scripted policies were correct? There were no audit mechanisms in place.
2. When policies needed to change across Virtual Private Clouds (VPCs) or across virtual instances inside a VPC, how could these changes be made accurately, quickly and at reduced cost?
3. How could they make sure that customers only had access to their allowed VPC's and couldn't jump across to other customer VPC's?
4. As virtual instances were spun up or down, how could they ensure the right policies were provisioned or de-provisioned?
5. If malware entered the environment or accidental changes were made by an administrator how could they know?
6. How could they demonstrate to customers that the environments were secure from malware threats and that all data was flowing according to policy?
7. Additionally, the Security Organization now wanted to take control back for policy management. To do so, they would have to find an automated way to manage security within AWS.

As part of their detailed security re-vamp, this company made sure to put forth desired design considerations for security:

- Discovery of the existing infrastructure objects and data-flows so they could be compared against existing policies to ensure the right native Security Groups are in place
- Automated, granular, micro-segmentation of the environments to clearly separate out policies by VPC. This would halt the East/West threat and also keep customer's in their own VPC's
- Real-time, dynamic adjustment of policies to environmental changes, for speed and accuracy
- Real time monitoring and policy enforcement to alert on and block rogue activity
- Visualization of the environment to demonstrate security compliance to senior management and customers

Hence this Provider went to the market in search of a security partner. Their analysis turned up Cloudvisory. Deployed in relatively short order, the Cloudvisory platform proved its worth by discovering all existing infrastructure objects and data flows then identifying missing granular AWS security policies needed to secure the environment. These were quickly and accurately provisioned across hundreds of virtual instances. Visualizations allowed both management and customers to gain confidence in the security of their environments. Now, as the company continues to expand, security policies are automatically provisioned based on a new instance's "Context". Then, these policies are instantly monitored and enforced. Policy changes are handled with relative ease and at lower cost. Security is now automated and under control so expansion can continue at light speed!

Reach out today for a demo and a test drive of Cloudvisory's Cloud Security Platform

WWW.CLOUDVISORY.COM