CloudHealth by vmware

Bazaarvoice uses VMware Secure State to scale public cloud security best practices

BAZAARVOICE COLLECTS, STORES, AND MANAGES CONSUMER GENERATED CONTENT, LIKE PRODUCT REVIEWS, ON THEIR CLIENTS' WEBSITES.

Their clients include the world's leading retailers representing a variety of categories, like home improvement, apparel and fashion, and consumer electronics.

THE PROBLEM

When Anji Greene was hired to manage cloud security at Bazaarvoice, she knew she had her work cut out for her. In order to innovate quickly and attract and retain top talent, Bazaarvoice empowers their development teams with extreme levels of autonomy. Each team manages their entire application, including its cloud infrastructure, and are not restricted to any core set of tools.

With so many teams—and cloud accounts—it made it even more difficult than usual to get a full picture of their cloud assets. "A Fundamentals of Security class will tell you that it's critical to maintain an up to date inventory detailing where are your assets and where is your data." Anji said, "It's so hard in a cloud environment to do that, especially when you have all these different teams with different cloud accounts." The second complication was a cultural one; a struggle that may sound familiar to organizations trying to move their applications to the cloud.

In order to integrate seamlessly into this developer-first mindset, Anji needed to convince these teams that she was there as a partner, not an adversary, and find innovative ways to help them build secure solutions, not to restrict them.

> *"From an education perspective, [VMware Secure State's rules] made it very obvious that I needed to be thinking about certain things. Like RDS, I hadn't even started thinking about best practices around permissions, patching, etc. VMware Secure State gave us a set of rules to get started with in RDS."*
>
> ***— ANJI GREENE***
>
> Director of Security, Baraarvoice

© 2019 CLOUDHEALTH BY VMWARE ®

“The role of security is changing,” she described, “and we had to work from the inside out to build trust that we aren’t putting crazy policies in place just to have policies.”

Developers often fear that security will restrict what they can do, and ultimately slow down their time to deployment, but Anji focuses her role on supporting the developers and improving their processes, so they can move just as fast, maybe faster, while deploying secure applications. “Since I’ve come to BV I do my best to find tools & methods to help the developers apply good security, it’s not my job to do it for them.”

HOW VMWARE SECURE STATE HELPED

INSIGHT OVER INTERFERENCE

One of the ways VMware Secure State helped Anji integrate security practices into her development teams, was by providing team owners with insights about risks in the cloud infrastructure they were responsible for. VMware Secure State runs automated scans of all cloud accounts to provide continuous visibility into the state of things, but also provides email alerts that use object tags to send a list of relevant violations to each team owner.

The results? “Most of the time people are like, ‘Oh, I didn’t even know this was configured this way.” Information that teams can easily react to—and quickly correct.

SERVICE BASED ROLL-OUT

Anji was concerned about the best way to roll out a monitoring and alerting tool internally. She wanted to provide relevant information that people could act on, but other solutions create so much noise that it can be difficult to process, let alone choose where to begin fixing thousands of violating cloud objects.

“The challenge was making the solution operational. How do I get people to take action?” Because VMware Secure State offers service-specific micro-audits, Anji chose to roll-out a single service at a time.

She started with S3 to prevent against that foulest of accidental misconfigurations—the dreaded open S3 bucket. Summer 2017 saw headline after headline of breaches caused by open S3 buckets, from the data breach that exposed thousands of job applicants to top secret jobs to the breach of 14 million Verizon customers’ data to the data of almost 200 million voters leaked online by GOP analytics firm.

> *“Protecting your cloud security configuration is important— I think of it as the security perimeter of your data center—it makes sense to protect and audit these controls before you deploy instead of after. Right now the best thing we can do is add more visibility and hooks so the teams know when they are doing the wrong thing. And I love the idea of integrating with DevOps because it makes security proactive instead of reactive. We need to integrate more and more security practices as part of the deployment process.”*
>
> ***— ANJI GREENE***
>
> Director of Security, Baraarvoice

© 2019 CLOUDHEALTH BY VMWARE ®

By focusing on S3 to start, Anji allowed her teams time to adjust to getting this new type of feedback and integrate it into their own workflow. The result? No open S3 buckets that weren't intended to be that way. And once the teams had mitigated any S3 risks, they were ready to move onto the next critical service—IAM.

SCALING SECURITY EXPERTISE

A key feature of VMware Secure State is its out of the box rulesets. These rulesets provide security checks based on AWS's best practice configuration recommendations as well as industry benchmarks such as the Center for Internet Security's AWS Benchmarks. These rulesets quickly make security expertise available across the organization, and also provide a way to keep up with all the new changes in cloud.

"From an education perspective, [VMware Secure State's rules] made it very obvious that I needed to be thinking about certain things. Like RDS, I hadn't even started thinking about best practices around permissions, patching, etc. VMware Secure State gave us a set of rules to get started with in RDS."

THE FUTURE OF CLOUD SECURITY

While Bazaarvoice is already leveraging VMware Secure State to provide distributed security knowledge, they are looking to the future, and how to integrate VMware Secure State's @Deploy scanning to get feedback to the developers even sooner in the process. Their goal is to be able increase the speed and precision of their deployments, eventually being able to block a build with any agreed-on high severity violations.

© 2019 CLOUDHEALTH BY VMWARE ®