Lacework™

MARQETA

AWS SECURITY CASE STUDY

Faster Application Engineering and Stronger Security

The Company and Its Business

Marqeta, a leader in modern card issuing and payment solutions for businesses, provides tools and a platform for building highly configurable solutions that support both physical and virtual payment cards. With its open API, the Marqeta platform gives businesses a simple way to tailor and manage their own payment card programs to create world-class experiences and new modes of commerce. Marqeta is growing and uses a cloud-based infrastructure to support its expanding operations and customer base.

The Security Challenge

To support its growth and customers who need fast time to market, Marqeta decided to move away from their hybrid architecture of a data center and monolithic AWS EC2 instances to more flexible containerized microservices with Amazon Elastic Kubernetes Service (Amazon EKS) "Our monolithic approach was slow. Spinning up an EC2 required permissions and configurations before developers could even begin work. It took weeks," says Gary Tsai, Application Security Engineer for Marqeta. They decided to take a more agile approach. Every team would own their own functionality and infrastructure that they would build with secure microservices.

CHALLENGES

- Create a faster more agile DevOps process
- Improve process visibility while moving to containerized microservices architecture with Amazon EKS
- Modernize existing AWS systems while meeting compliance regulations and achieving a high degree of visibility

SOLUTION

- Improve process visibility while moving to a Amazon EKS containerized microservices architecture
- Total visibility and validation of all containerized instances and activity

RESULTS

- Faster application development and improved security monitoring with no additional AWS expertise
- Security team freed to focus on other issues like endpoint detection and threat hunting

Choosing Lacework

Marqeta knew they needed a security solution before they started rebuilding their AWS infrastructure with EKS containerized microservices, so they began searching for a solution that would work with their new architecture. They tested products from different vendors, and although some offered agents they could build into a VM instance, there was no flexible way to monitor container activity. Then they found Lacework, which was designed for the cloud. It provided total visibility into EKS containers, it would easily scale to accommodate their growth, and they could install it without special expertise.

Implementation

Installing the Lacework agents turned out to be incredibly easy. That was ideal for a production environment where developers are not security experts. Tsai describes it in this way: "I told them they could figure it out for themselves, or I could explain it to them. I went through it with them. It took maybe four clicks, and you wait five minutes, and boom, the accounts are recognized and Lacework is now ingesting all cloud trail data. It was mind-blowing for them." You deploy, and then go about your business knowing you now have visibility into everything that is happening.

Accelerated Development and Better Visibility

Lacework solved the visibility problem and accelerated the development of secure microservices. "We use terraform scripts to deploy our cluster," Tsai explains. "Every team uses that same template, and that template includes the Lacework agent. They just run through the confirmation, a couple of clicks, and that's it."Now the teams are quickly spinning up their own microservices, and security has immediate visibility into everything running in the environment. Lacework consumes all the cloud trail logs and alerts to anything that is not right. All of this is being done with no special AWS expertise.

> "It took maybe four clicks, and you wait five minutes, and boom, the accounts are recognized and Lacework is now ingesting all cloud trail data. It was mind-blowing."
>
> — **Gary Tsai**, Application Security Engineer at Marqeta

Lacework has given the security team more visibility than they ever had and relieved them of burdensome tasks. "I no longer spend time triaging," says Tsai, "and I do not review any logs." This has freed up security to focus on other issues, such as implementing endpoint detection and threat hunting. It also provides a new layer of assurance in compliance reporting. In addition to reporting on their DevSecOp practices, they can produce actual data showing the effectiveness of what they are doing.

Lacework

About Lacework

Lacework security platform has been specifically designed to simplify how organizations implement a security-first model in their cloud infrastructure by addressing the challenges of both build-time and run-time operations. It provides the leverage of a unified security solution to integrate security across your entire development lifecycle. By integrating the multiple layers of cloud security in one platform, Lacework provides account protection, automates intrusion detection, secures containers, and ensures configuration compliance across AWS, Azure, GCP, and private clouds. Lacework's comprehensive view across cloud workloads and containers delivers one-click investigation and simplifies cloud compliance. Having these capabilities will not only strengthen your organization's overall security posture, it will also empower your DevSecOps teams with deep visibility and agility to successfully meet the requirements of the cloud era.