

CASE STUDY

Lacework enables Sliide to manage vulnerabilities and demonstrate compliance



Challenges

- Gain 24/7 proof of compliance with the AWS Well-Architected Framework
- Maintain a strong security practice as company scales up
- Maximize tool testing efficiency while minimizing labor

Solutions

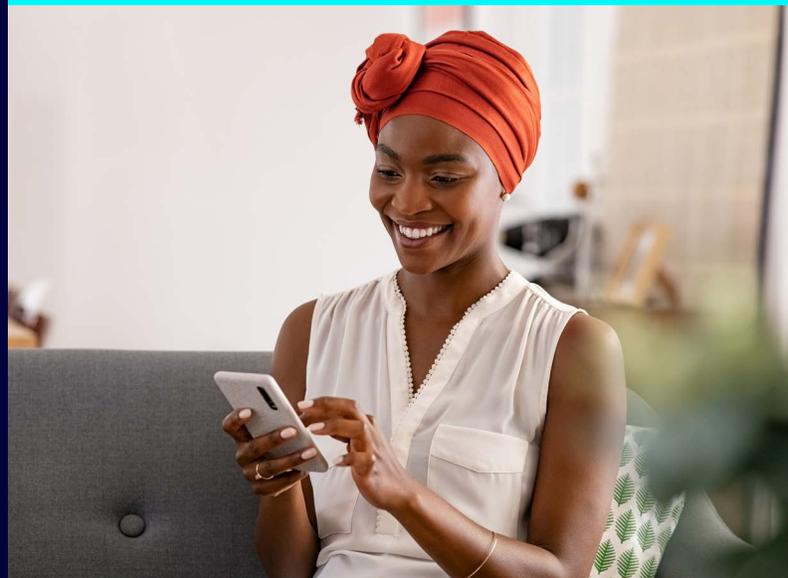
- Set up Lacework in a few hours and left machine learning to baseline over the weekend
- Deployed efficiently by using pre-existing modules from Lacework on the TerraForm documentation website

Results

- Demonstrated compliance daily with automated reports
- Received high-quality alerts to protect against malicious behavior
- Used dashboards to prioritize workflow and visualize vulnerabilities

“With the reports generated by Lacework’s dashboard, we can easily see what resources are compliant, what resources are not compliant, and what we need to do to achieve compliance.”

JAY RAWAL, DEVOPS ENGINEER





About Sliide

Headquartered in London, Sliide develops app, software development toolkit (SDK), and web-based products alongside distribution partners in the mobile network operator, virtual network operator, and service provider spaces. Each partner sources a large number of devices, and Sliide's products monetize parts of those devices by offering a business model that involves sponsored content, advertising, and other activities that impact the device users, most of whom are based in the United States. "We share our revenue with our distribution partners, who benefit because Sliide helps subsidize the devices they're paying for," says Stephen Carl, Sliide's Chief Information Officer. "The end users benefit because they're getting devices that are increasingly sophisticated."

Sliide's products are intended to engage users, reduce churn, and drive revenue. "We offer a complete ecosystem," says Carl. "Not only do we provide the apps, websites, and products, but we also procure all the ad networks and content network partners who supply the detail that makes those apps work. Effectively, we're providing a complete managed service to our partners with revenue share models as the business case." Along with Carl, some of the faces behind Sliide's offerings include lead DevOps engineer Jay Rawal and Chief Technology Officer Vas Fasoulas. Rawal sees to it that Sliide's infrastructure is fault tolerant, resilient, and scalable, while Fasoulas ensures that all of Sliide's apps and products have a coherent, robust architecture.

In terms of their cloud environment, Sliide uses a single Amazon Web Services (AWS) account with a connected Amazon Elastic Container Registry (ECR). Currently, they are in the midst of a large migration project to move services to Kubernetes. All alerts get sent to Slack and Jira, while reports are sent over email.

Challenges

In the past few years, Sliide has significantly scaled their business. Throughout their growth, they have emphasized their security practice. "We've always tried to make sure that our platforms are as secure as they possibly can be," says Carl. "We use AWS's Well-Architected Framework wherever possible, and we make sure we have whatever security tooling in place that we possibly can." Previously, they tried a number of methods to test their tools, including pen testing and bringing in external third parties to try to identify vulnerabilities. However, says Carl, "This was very labor intensive for us. We would have to spin up new environments, and it was detracting from our development work." Sliide knew it was time to seek out a solution.

To bolster their security practice as they grew, Sliide sought a platform to provide them confidence and proof that they were well-architected and on top of vulnerabilities. "But at the same time," Carl says, "we wanted a solution where we didn't constantly have to build something to prove that." They also hoped to find tooling that would demonstrate proof on a 24/7 basis, as opposed to once or twice a year. And finally, they wanted a product they could try before buying, so as not to waste time or money. "We wanted to see what we would be getting with a minimum amount of effort," says Carl.

"We could see the value generated, and we had hard evidence. Choosing Lacework was a no-brainer."

VAS FASOULAS, CHIEF TECHNOLOGY OFFICER

Solution

When the Sliide team described what they were looking for, AWS introduced them to Lacework. Lacework's offerings ticked all of Sliide's boxes, so they set out to deploy the product. They began deployment on a Friday morning, wrapped the setup process in a few hours, and left the machine learning to baseline over the weekend. "The whole process was extremely easy and the barrier to entry was minimal," says Carl. "It suited us greatly."

Rawal agrees that deploying Lacework went smoothly. "It was really easy having all the documentation," he says. "There's so much flexibility in terms of implementation, whether we use scripts or TerraForm or manual deployments into our AWS environment. Anything we could think of, there was a solution." Sliide's security teams use TerraForm for 90% of their AWS infrastructure, so they were excited to see Lacework's pre-existing modules on the TerraForm documentation website. "We just had to copy and paste code, change a few values, and run TerraForm," says Rawal. "It was very efficient. We didn't have any issues."

After deploying, the choice to go with Lacework was a simple one. "Lacework had a clear value proposition and an easy path to test this. We put them in practice as a proof of concept in a matter of days," Fasoulas says. When the team returned to the office after letting Lacework baseline over the weekend, they had effective findings. "We could see the value generated, and we had hard evidence," says Fasoulas. "Choosing Lacework was a no-brainer. It wasn't, 'Why choose Lacework?' but, 'Why wouldn't we choose Lacework?'"

Results

Measuring compliance and managing workflow

Lacework's automatic compliance reports have provided great value to the Sliide team. One of Rawal's quarterly objectives is to ensure that the compliance metric is improving. "With the reports generated by Lacework's dashboard," he says, "we can easily see what resources are compliant, what resources are not compliant, and what we need to do to achieve compliance." Rawal especially likes how user-friendly the reports are. "Everything that's compliant is in green, and I can just sort the list to show only non-compliant resources," he says. "I treat that as a checklist and encode all of those into Jira. Those items turn into tickets and then we pick which to work on, from the most critical to the least critical."

Moreover, Lacework helps show Sliide's compliance posture on a daily basis. "Every morning when Lacework runs the compliance reports, we can verify that the work we did the previous day was completed," says Rawal. "In some cases, when we make particularly frequent changes, we can run the report on an audit basis from the dashboard. So if I make some changes and want to check if that's resolved the non-compliant resources, I can just run a report, which generates a graph showing that the compliance score has increased, and those resources disappear from the non-compliant resources." Thanks to Lacework, Rawal has easily been able to show the whole office how he has achieved his quarterly targets of demonstrating progressively stronger compliance.

"There's so much flexibility in terms of implementation, whether we use scripts or TerraForm or manual deployments into our AWS environment. Anything we could think of, there was a solution."

JAY RAWAL,
DEVOPS ENGINEER



High-quality alerting

Sliide also appreciates how Lacework learns what malicious behavior looks like, and then alerts on it. Before Lacework, they didn't have an alerting system in place and had to manually check for abnormal behavior. Now, things are much easier. "Imagine that your infrastructure on AWS changes because you're scaling up or deploying new products," says Fasoulas. "The Lacework platform is smart enough to identify this as normal behavior. But, for example, if someone hacks into an AWS account and starts launching instances, or if someone is using the wrong environment, Lacework will identify, detect, and let you know so you can address."

Lacework helps Sliide stay safe by keeping track of changes in normal behavior. Rawal recalls a time when he was on vacation and received an alert because he had logged in to AWS from a new location. "I do work on AWS every day, but because I usually log in to AWS from London, when I was in a different place, Lacework flagged it as abnormal," Rawal says. "Even though it was completely safe, it was nice to see that these things are being tracked. If someone managed to get hold of my credentials and log in from somewhere else, we would have noticed right away, and we could have disabled my account to prevent anything bad happening."

Proof through visualization

One of the Sliide team's favorite aspects of the Lacework platform is how it enables them to see exactly what's happening in their environments. "We have video screens in the office, and there's one that permanently shows Lacework dashboards, particularly any incidents that have occurred or any alerts that pop up," says Carl. In fact, this visualization helped Carl justify his team's need for Lacework to other members of the company. "The finance team liked everything about having more stability and having ongoing proof, particularly around vulnerability protection," Carl says. "The graphical representation of how we're being protected is extremely useful to the finance team when dealing with our investor and board community."

Currently, the Lacework dashboards on display in Sliide's office are the global ones, but Fasoulas hopes to incorporate even more. "We plan to have more targeted dashboards, customized ones for different areas, specific filters, and more," he says. As Sliide continues to grow, they are enthusiastic about scaling their ongoing partnership with Lacework.

Find out more at lacework.com



Headquartered in London, Sliide develops app, software development toolkit (SDK), and web-based products alongside distribution partners in the mobile network operator, virtual network operator, and service provider spaces. Each partner sources a large number of devices, and Sliide's products monetize parts of those devices by offering a business model that involves sponsored content, advertising, and other activities that impact the device users, most of whom are based in the United States.