LACEWORK

CASE STUDY

Clariness restructures IT security compliance processes and establishes DevSecOps discipline

CLARINESS

Challenges

- Distribute security responsibilities across multiple teams
- Achieve an external ISO 27001 certification
- Receive more actionable insights from alerts

Solutions

- Worked with Lacework Professional Services to implement security across the organization
- Established future goals after conducting cloud security assessment
- Created compliance solutions to help with audits

Results

- Adopted best practices for compliance audits, including CIS Benchmarks and ISO 27001
- Consolidated several tools and rewrote standard operating procedures
- Embedded security into their process to establish a strong DevSecOps discipline

"I started looking into solutions that could scale, that could be intelligent, and that could provide insight into patterns so we could use machine power to augment human power."

GOPI KRISHNAMURTHY, VICE PRESIDENT OF PRODUCT AND ENGINEERING, CLARINESS

> Lacework is a one-stop shop for security and compliance.
>
> GOPI KRISHNAMURTHY, VICE PRESIDENT OF PRODUCT AND ENGINEERING, CLARINESS

About Clariness

Clariness was founded in 2005 with the mission of improving patients' lives. They accelerate patient recruitment for clinical trials, bringing new medicines and treatments to patients faster. With data-driven, indication-based marketing and a double pre-screener, Clariness reduces the workload and frustration for sponsors, sites, and patients alike.

The backbone of Clariness is a platform they built to run their software end-to-end, so their engineering and product teams work closely together. At the helm of this cross-functional effort is Gopi Krishnamurthy, the Vice President of Product and Engineering. Krishnamurthy and his team of around 20 people run all aspects of technology at Clariness, including cloud engineering, platform building, IT administration, and the helpdesk.

Clariness operates almost entirely in the cloud, with their infrastructure on Amazon Web Services (AWS). They run all their platforms on open-source Kubernetes and are in the process of moving into Amazon Elastic Kubernetes Service (EKS). "Our technology is quite varied," says Krishnamurthy. "We have a lot of code that runs on Java Spring, and we have modern stacks that we have implemented recently with React and Angular on our front end." For legal compliance purposes, they also have a third-party data center where they send their backups, "but otherwise, we are fully on AWS," Krishnamurthy says.

Challenges

When Krishnamurthy joined Clariness in mid-2021, he hoped to improve his department's operations by restructuring the teams in a more cross-functional way. "I wanted this type of transformation to be augmented by systems, and particularly systems that are supported by machine learning," Krishnamurthy notes. "I started looking into solutions that could scale, that could be intelligent, and that could provide insight into patterns so we could use machine power to augment human power." In addition, he wanted something that could help implement a shift-left security mindset.

Krishnamurthy also needed a solution that allowed the entire organization to see the importance of security. "I wanted to decentralize and democratize security within the company so that everybody could experience some element of ownership," he explains. "I was looking for a solution where I could bring people together and distribute the accountability by using a tool across the team." Instead of restricting security to the product development team, Krishnamurthy adds, "Our goal was to bring security from platform support to DevOps to security. It's all about the process, and we needed a tool to support this change."

Aside from a process overhaul, Clariness was looking for a tool that could streamline their compliance process. "One of our internal goals was to do an ISO certification," says Krishnamurthy. And his team wanted to grow their ability to act on alerts. "We needed more actionable insights coming out of events or alerts so our teams could know how to proceed, and take security to the next level," he says.

Solution

As Clariness prepared to deploy, they connected with the Professional Services team at Lacework to receive further guidance. "We had multiple sessions with Professional Services about how to implement security and build it into our organizational culture," states Krishnamurthy. "They helped explain how to use the data we received from Lacework to maximize our insights. That was one of the first big benefits we saw." Professional Services also stepped in to make the deployment process more transparent, which helped Krishnamurthy convince Clariness management that Lacework was the right solution for them.

Working with Professional Services, Clariness conducted a cloud security assessment. "We did an assessment that provided us transparency into our cloud security posture, so we could benchmark it and then see how we were meeting our goals," Krishnamurthy says. "For example, since we want to achieve an ISO certification, we were able to work with Professional Services to discuss where we wanted to be by the end of the year and how we could get there."

During the security assessment, Krishnamurthy's team discovered an additional need for pen testing due to other audit requirements. "We went to the Professional Services team to see if Lacework could help with pen testing," remembers Krishnamurthy. "They were able to bring in a partner to make that happen. The Professional Services team was so helpful and flexible, and I'm happy they were able to offer us this partner introduction."

Results

Improving compliance audits

Since deploying Lacework, Krishnamurthy notes a shift in mindset when it comes to audits. "Having a third-party perspective has helped us develop greater transparency and adopt best practices," shares Krishnamurthy. "It has completely changed the mindset of our team, and allows our engineers to think differently. We avoid an organizational bias towards our product, which has been a big advantage."

Clariness is looking to achieve a number of compliance standards, both internal and external, in the near future. At the moment, they are working on external audits for ISO 27001 and Good Clinical Practice (GCP), and internally, they're focusing on CIS Benchmarks. Down the road, says Krishnamurthy, "there's more coming from the business side of things, which will drive technical components like how we run security and how we store and manage data." This exploration may include HIPAA as well. Krishnamurthy adds, "Lacework is a one-stop shop for security and compliance."

Consolidating tools

Prior to Lacework, Clariness had a lot of different tools. "Our tools were installed, running, and using our resources, but they didn't force us to take action. They just spit out a lot of information," Krishnamurthy remembers. "Once we started with Lacework, we moved these tools aside so we could use Lacework for maximum dynamic application testing. Now, when something goes into our infrastructure or into production, it's 100% monitored by Lacework, and there's no other tool taking care of it." In fact, Krishnamurthy's team has rewritten their standard operating procedures to account for how Lacework monitors their infrastructure and informs them of what actions to take.

> "One of our internal goals was to do an ISO certification. We needed more actionable insights coming out of events or alerts so our teams could know how to proceed, and take security to the next level."
>
> GOPI KRISHNAMURTHY, VICE PRESIDENT OF PRODUCT AND ENGINEERING, CLARINESS

Ensuring compliant data storage and fixing legacy gaps

After completing the cloud security assessment, the Clariness team had the information they needed to make a number of key improvements. For one, says Krishnamurthy, "we were able to achieve a lot in terms of our data storage and our ability to process information, which helped ensure that our data stores are compliant."

Additionally, they were able to clean up security gaps that resulted from years of work on their legacy infrastructure. "These weren't necessarily relevant to our current product platform delivery, but there were still security holes that we identified and fixed," Krishnamurthy adds. "Thanks to actionable insights from Lacework, we fixed 20 critical vulnerabilities in the first week after the cloud security assessment." And their remediation has become much more efficient, too. Now, Krishnamurthy explains, "Our time to respond to a security incident is less than four hours, and our mean time to fix the critical issue is two days."

Establishing a DevSecOps discipline

Clariness also gained the ability to embed security into their process. The Customer Success team participated in the initial onboarding process to demonstrate how to set up, monitor, and act on alerts, as well as how to integrate certain channels. "Now we have a process, which didn't exist before, to show us how to take action on security alerts," says Krishnamurthy. "Lacework has helped us shift our security left. Before, we were a DevOps company, and now we are a DevSecOps company." In general, Krishnamurthy appreciates how Lacework has assisted with their process across the board. "We like the process and how Lacework works," he concludes. "Going forward, we want to take a few pages out of their book and make sure that we can do the same in our environment."

Schedule a demo today

> **"Lacework has helped us shift our security left. Before, we were a DevOps company, and now we are a DevSecOps company."**
>
> GOPI KRISHNAMURTHY, VICE PRESIDENT OF PRODUCT AND ENGINEERING, CLARINESS

CLARINESS

Clariness was founded in 2005 with the mission of improving patients' lives. They accelerate patient recruitment for clinical trials, bringing new medicines and treatments to patients faster. With data-driven, indication-based marketing and a double pre-screener, Clariness reduces the workload and frustration for sponsors, sites, and patients alike.