LINK11

CASE STUDY

Labguru

www.link11.com

Labguru Case Study

Global SaaS Provider Achieves Compliant, Customized Cloud Web Security on AWS

Labguru (labguru.com) is the flagship product from BioData. It is a secure web-based ELN [Electronic Lab Notebook] platform for designing, performing, and managing projects in the life sciences. Labguru's customers include a wide variety of biochemical research laboratories, both in academia and industry. As such, it has a number of unusual requirements for web security.

"Initially we had a basic service from CloudFlare, plus we had implemented a lot of security within our platform's code. But as we began to acquire some large customers from industry, we discovered that we needed a better solution to secure the endpoints that we make publicly accessible. There was a growing amount of bot scans, crawlers, and other suspicious traffic that we wanted to eliminate," said Johai Kadosh, BioData's DevOps and Production Manager.

BioData evaluated a number of security solutions, including AWS WAF. Although it has a number of good features, it isn't meant to be a comprehensive solution, and BioData needed much more. The company also evaluated Imperva Incapsula and Link11.

BioData knew that its security solution had to fulfill a list of strict requirements, including compliance, customer privacy, customization, high reliability, minimal latency, and minimal cost.

Industry

SaaS

Challenges

- Scrubbing incoming traffic in the cloud while adhering to strict compliance requirements for customer data privacy.
- Customizing web and API traffic processing according to very complex requirements, carying on a per-customer and a perendpoint basis.
- Blocking hostile traffic with minimal latency.

Solution

Link11 runs in a Virtual Private Cloud under BioData's AWS account, with customized rulesets to meet Labguru's requirements.

Results

- Hostile traffic is blocked, and compliance is maintained; all processing occurs within BioData's AWS resources.
- Compute resource requirements are minimal. Added latency is less than three milliseconds.

"We eliminated Incapsula early, because their prices were way over our budget. Then we looked closely at Link11."

Johai Kadosh
BioData's DevOps and Production Manager

Compliance and Customer Privacy

Mr. Kadosh explained, "We need to comply with GDPR, FDA CFR 21, and other standards. Compliance requires us to have all the data under our account, and all the traffic needs to be handled within our own compute resources."

"Its compute requirements are awesome. I'm putting all my traffic through Link11, from multiple environments. "The machines I'm using are the lowest that Amazon provides. Link11's cost efficiency is one of its greatest features." Johai Kadosh, DevOps and Production Manager, BioData The information that the dashboards and the logs provide is priceless. BioData executives appreciated that Link11 is a compliant solution, and that unlike most other cloud security solutions (which decrypt and often store customer data on their own infrastructure), Link11 performs all its traffic processing exclusively on the customer's resources. After its due diligence was completed, BioData selected Link11 as its web security solution. Because Link11 is fully integrated with AWS, the deployment and launch of Link11 were straightforward.

"The information that the dashboards and the logs provide is priceless."

Johai Kadosh
BioData's DevOps and Production Manager

Power and Customization

Mr. Kadosh said, "Our web platform is very complex; I can't just place a WAF filter in front of it. I needed a high level of customization, and Link11 is very customizable.
"The first thing I noticed with Link11 is that it works. Whatever you configure it to block, will be blocked. Then we began to dive into customization, and realized that we needed some assistance. I reached out to the support team, and they were a tremendous help. The issues that we had were solved very quickly."

"The Best Support"

Mr. Kadosh appreciates the support that he has received. "It's the best we've had so far [from a vendor]. The issues that we've had were responded to right away. Everything was done over SMS or WhatsApp within an hour."

Link11 is a fully managed platform, updated automatically to protect against the latest threats. "Every so often we receive a new AMI [AWS machine image] and it's deployed to the WAF. It's easy, and I like knowing that the IP blacklists and other security rulesets are always being updated."

Reliability

Mr. Kadosh said, "I was concerned about placing the WAF endpoints before all my production environments. It creates a potential bottleneck, and I needed a very reliable solution." Link11's SLA includes 99.999% uptime, and Mr. Kadosh said Link11 has proven to be reliable. "Link11 works."

Link11 Web Application and API Protection (WAAP)

Core technologies include:

Next-Gen WAF/IPS, Multilayer DDoS Protection, Precise ACL, API Security, ATO Prevention, Scraping Prevention, Advanced Human Detection and Bot Management, Unified Management Console, and Real-Time Traffic Analysis.

Added value services include:

Mobile/Native Client SDK, Layer 7 Load Balancing, Global Secured CDN, and a complete DNS solution.

Link11 GmbH | Lindleystr. 12 | 60314 Frankfurt | info@link11.com | +49 69 26492977