Lacework

Jitterbit

CASE STUDY

Jitterbit Secures Dynamic Cloud Environment, Containers, and Microservices at Scale.

The Company and Its Business

Jitterbit is a cloud-based company that enables customers to quickly build APIs to tie together their different business processes. “We are the glue that integrates different systems,” explains William Au, Senior Director of DevOps, Operations, and Site Reliability at Jitterbit. “We can move data, sync data, and we can run business processes.”

Hosted in an Amazon Web Services, Jitterbit allows users to build their own APIs in the cloud environment, and then they can either deploy the APIs to the cloud or to on-premises environments.

The Security Challenge

Jitterbit’s operational environment is highly dynamic, autoscaling up and down with VMs, containerized microservices, and applications. They have over 400 active instances at any given time for their clouds in the US, Europe and Asia. “These containers and instances can spin up and down at any moment,” Au says. “I was very concerned about keeping track of every instance. It got to the point where I gave up. I just couldn’t do it anymore.” As Jitterbit continued to grow, monitoring platform activity was only getting more difficult, and the company could not hire enough security people to keep up. They began to seriously look for tools to help them fill the gap.

CHALLENGES

- Tracking activity of a large number of container and VM instances in a dynamic environment
- Security team unable to keep up with growth in systems and inaccurate alerts

SOLUTION

- Lacework provides complete visibility into containers, VMs, and apps
- Lacework tracks all activity data and provides accurate alerts about important events

RESULTS

- Confidence that everything in the environment is being tracked and analyzed, without additional staff
- Streamlined compliance reporting across their cloud environment issues and close them almost immediately
- Automated rule writing secures cloud, containers, and microservices without slowing innovation

Choosing Lacework

Jitterbit began searching for a tool they could use in their cloud environment that would consume application logs, compare monitored behavior to a database of vulnerabilities, and analyze logs for unusual behavior patterns. "We did a little bake off between Darktrace and Lacework," Au says. What they found was that Darktrace was really a very different product than Lacework. Darktrace monitored things like open ports on instances, which was important, but Jitterbit already had that covered through other tools in their stack. Lacework, on the other hand, was different. It looked at actual application activity logs for each individual instance. It aggregated and analyzed log data, and provided alerts about unusual behavioral patterns.This was not something any of their other security tools could do.

> "What we really appreciate about Lacework is that it actually works."
>
> —**William Au**, Senior Director of DevOps, Operations, and Site Reliability at Jitterbit

Implementation

Jitterbit found the Lacework implementation to be an easy process. "We were pleased with the short amount of time it took to get Lacework up and running," says Au. He notes that Lacework's support team was exceptional and really helped through the implementation process, with good documentation and support. "It was way easy," says Au. "We were generating reports within the first week of implementation. Just to compare, we also implemented Rapid7, and we're still trying to figure out its reporting features. Rapid7 doesn't even have a report function for containers."

Doing More with a Small Security Team

Lacework provided benefits right away. First of all, the amount of data it collected from active instances was enormous, but Au and his team no longer had to look at all the data. Au notes, "We are putting 110 million lines of log data into the system. It sifts through all that using machine learning to focus on what is important. It saves us lots of time." It also enables them to actually monitor all those instances that are coming and going in their dynamic environment. "I know there's 400 things out there and their activity data is now being pulled into Lacework. If anything critical shows up, Lacework will alert us," says Au. "I no longer worry about rogue systems in production. It allows me to manage so many systems with just two people."

One challenge with security automation tools is the number of false alerts they generate, but that has not been a problem with Lacework. "With some tools we get a lot of alerts that mess up our back end because now folks spend time checking to see if those things are real. What we really appreciate about Lacework is that it actually provides accurate alerts," Au notes. An added benefit is the support Lacework provides for SOC 1 and SOC 2 compliance. Au explains: "Through its reporting, this system provides a really good way of giving evidence that we are in compliance with rules about logs being aggregated, logs being monitored, the kinds of alerts we are getting and how we respond. It supports the whole process life cycle."

As they move forward with Lacework, they plan to incorporate it into their build process. "We want to incorporate a scan into the build process so if a container fails, it doesn't go to production," Au says.

About Lacework

Lacework delivers security and compliance for the cloud. The Lacework Cloud Security Platform is cloud-native and offered as-a-Service; delivering build-time to run-time threat detection, behavioral anomaly detection, and cloud compliance across multicloud environments, workloads, containers, and Kubernetes. Customers significantly drive down costs and risk by freeing themselves from the burden of unnecessary hardware, rule writing, and inaccurate alerts. Lacework is trusted worldwide by enterprise companies at the forefront of embracing the cloud. Find out more at www.lacework.com.