CASE STUDY

Reltio uses Lacework to consolidate tools, achieve deep visibility, and address alerts 4x faster

Reltio

Challenges

- Uncover weaknesses, misconfigurations, and vulnerabilities
- Gain efficiencies and eliminate tools (originally using 4+ different products)
- Achieve consistent visibility across AWS, Google Cloud, and a microservices architecture

Solutions

- Ran a bake off to see how Lacework raises critical alerts
- Deployed Lacework across 3,000 systems in a few days

Results

- Investigated and resolved issues 4X faster than before, across all criticality levels
- Gained deep visibility into an ephemeral environment with massive amounts of data
- Enabled better collaboration between security and DevOps teams

> "Lacework provides us with ubiquitous visibility and detection capabilities across all environments."

TERENCE RUNGE, CISO, RELTIO

> “Lacework excelled, scaled, outperformed, gave me the visibility I needed, and gave me the ability to rapidly act on any sort of alerts.”
>
> TERENCE RUNGE, CISO, RELTIO

About Reltio

Reltio is a versatile, cloud-native data management platform that enables organizations to deliver hyper-personalized and connected experiences for their customers. They serve a broad range of customers, including high-end fashion brands, national chain restaurants, the technology and energy sectors, and nine of the world’s ten largest pharmaceutical companies.

As the Chief Information Security Officer (CISO), Terence Runge is responsible for security, compliance, risk, audit, IT, and some aspects of privacy. Reltio’s compliance requirements include SOC2, SOC1, HITRUST, and FedRAMP. Relative to cloud security, Reltio emphasizes securing cloud infrastructure, workloads, and runtime. In addition, Reltio security is invested in identity and access management to make sure that IAM roles and privileges are appropriate and the minimum required.

Reltio primarily leverages AWS and GCP and is in the process of exploring Azure. Reltio has also been making a significant move to a microservices architecture over the last two years. With just over 4,000 subdomains exposed to the internet, it’s critical for Reltio to assess and understand their attack surface on a continual basis. “Essentially, we’re a set of exposed APIs with a very thin UI layer,” says Runge. “It’s all infrastructure as code. Lacework provides us with ubiquitous visibility and detection capabilities across all environments.”

Challenges

Among Reltio’s biggest concerns are finding any sort of weaknesses, misconfigurations, or vulnerabilities. New vulnerabilities or changes to third party libraries could introduce risk to infrastructure and cloud services. Even with checks to make sure new or updated libraries are not introducing weaknesses, it’s not foolproof — there’s always a concern that something was accidentally exposed. For this reason, Reltio relies on defense in depth to identify changes and actively test for weaknesses and misconfigurations.

When Runge first came on board, Reltio had just moved to a microservices architecture. He recalls his second or third week on the job when he was asked to complete a security review of the new architecture. Since he wasn’t yet a Lacework customer, he had to work around the clock to explore different open source options, tooling, and methodologies. “I couldn’t just turn on Lacework and say, ‘Show me your report,’” says Runge. Instead, he had to spend hours conducting his own investigation with several different tools, until he eventually arrived at the realization that there was a real problem: he discovered multiple critical issues that could lead to remote compromise, so the team spent the next several months re-architecting and redeploying so they could reach a more secure state. This whole process validated that Reltio needed a solution like Lacework. “What’s concerning to me is that somebody might not have the ability to continually assess the security and compliance of the cloud environments,” says Runge. “A well-intentioned engineer might think that what they’re deploying is secure, which could result in fairly immediate exploitation.”

In addition to this experience, a few other factors inspired Runge to seek out a security solution. He arrived at Reltio with a clear set of goals: to gain efficiencies, to reduce the number of technologies in place, and to make sure that the technology offered complete visibility and detection capabilities across the entire environment. At that time, however, Reltio was using technology from more than four different suppliers, which was working partially (or not at all) in various environments. Runge wanted a technology that worked in AWS, in GCP, and in a microservices architecture, and that would give him consistent detection and visibility capabilities. But was it possible to meet all of these needs? Runge came to the conclusion that he might have to spend more, and buy two or three technologies, to get what he needed. And then, just in time, one of Reltio's DevOps engineers returned from a conference where he'd seen an exciting product demo. "You have got to check out Lacework," he told Runge.

Solution

Under Runge's direction, Reltio took a deep dive into the Lacework product. "We did not just run a demo or a POC," he says. "We did a full bake off against the incumbent technologies that we had in place." The bake off was especially high-stakes because the current platform was up for renewal at the end of the month — and, with the incumbent's close ties to Reltio, there were investors to consider as well. "We were up against the clock, up against investors, and up against incumbent technology," Runge recalls.

> **"10,000 times easier than anything else I ever deployed."**
>
> DEVOPS ENGINEER, RELTIO

The bake off highlighted the products strengths. Runge appreciated that, instead of seeing an alert in the platform and having to go back to the AWS console to drill in, Lacework allowed him to go right into the information he needed. "Lacework excelled, scaled, outperformed, gave me the visibility I needed, and gave me the ability to rapidly act on any sort of alerts," says Runge. And unlike the competitor, Lacework passed a red team test with flying colors, raising critical alerts that demonstrated the system's effectiveness.

But by the last week of the month, Runge was on the verge of sticking with the incumbent simply because he didn't think there was time to switch over to Lacework. "I didn't have the time to displace anybody," he remembers worrying. "And I couldn't run the risk of having an audit finding because I had a gap." So Lacework jumped in, working closely with Reltio to help with implementation. After a few days, Reltio's DevOps engineer came back to Runge with the news that Lacework was deployed, and not even in a test environment.

They were done, having deployed Lacework across 3,000 systems. "That was 10,000 times easier than anything else I ever deployed," the DevOps engineer wrote to Runge. With that, Reltio's future was set: the competition was out, and Lacework was in.

From a diplomatic angle, Runge didn't make the easy choice. He had to spend weeks justifying the switch to investors, CEOs, and various executives. But it was all worth it. "Lacework ended up displacing about four suppliers' technology, gained efficiencies, saved money, and made the analysts' jobs a lot easier, to the point where we can now, on a daily basis, quickly adjudicate any sort of medium, high, or critical finding that comes into us."

Results

Visibility wins out with Lacework

Once Runge's team spent several months rebuilding their microservices architecture, it was time to redeploy. Runge told them exactly what to expect. First, Lacework would discover automated activity like pings, sweeps, and probes, which shouldn't be points of concern. Then, in about two weeks' time, the real test would arrive: they would see a concentrated attack against them. Sure enough, they came under significant attack, which showed up in Lacework as a critical alert. "We saw it last for about three hours, we weathered it, they didn't get anywhere, and the attack subsided," Runge says.

Alerts like these have been one of the greatest assets to Reltio. Before they adopted Lacework, says Runge, working through an alert was incredibly time-consuming. It could take a whole day to work through one event and would require analysts to chase down information in multiple consoles. Now, for events across all criticality levels, it's 4X faster to investigate and resolve issues. Lacework allows the Reltio team to drill into each alert and examine the Lacework Polygraph visualizations to get all the context they need. With a new level of visibility, they now have a clear story to take to DevOps. "We can just create the Jira ticket, tag someone from DevOps, ask them a question, get an update, and we're done," says Runge. "It's very straightforward." With speed and simplicity, Lacework grants Reltio access to crucial information on a regular basis.

Drilling in with Polygraph™

Runge remembers one particular use case where Polygraph proved invaluable. When the team got an alert that there was a new file, Runge and the analysts immediately began to investigate what was going on. They found a number of red flags: the file was an executable, the hash value didn't match, and it was being run as root. Using Polygraph, they were able to drill in and backtrack until they could trace the file back to someone in DevOps. As it turns out, he was just trying an experiment — nothing malicious was going on. But Polygraph's ability to help the Reltio team identify the source was huge. In the case of a major security breach, Lacework provides everything Runge could want, including a swift notification, the ability to drill into the alert, hash values, and information on what the user was running as and what systems it was connected to. In under an hour, they were able to trace the file back to an actual person and get the issue cleared up. This level of actionable visibility helped secure Lacework's position as core technology in the security stack.

Working at scale

Compared with other options in the market, Lacework stood out to Reltio for its command of the fundamentals. Because Lacework has figured out how to scale successfully and is built on a solid foundation, it was the clear choice to support Reltio's massive amounts of data. The environment at Reltio is highly ephemeral and very dynamic, with about 3,000 systems that go up and down every single day. Runge appreciates being able to deploy Lacework quickly in that environment, which maintains the visibility he needs. His analysts also value Lacework's reports, which allow them to work efficiently. In fact, they usually analyze the report rollup on a daily basis and adjudicate in an hour or two. In the future, once there's more automation in place, they expect this amount of time to shrink even further.

When it comes to automation, the analysts have already seen some of these incredible benefits in integrating Lacework with Tines. By combining Lacework and Tines, Reltio can take action and automatically resolve security alerts in real-time as they occur. "What the analysts have built out with Tines and Lacework is amazing," says Runge. "The analysts are cutting down their work dramatically, probably to the equivalent of half a body, or about $100,000 a year. That's massive." But, concludes Runge, the quality of Lacework is his number one priority. "The cost savings are great," he says. "But I care most about the speed and efficiency of my team — Lacework delivers huge value in that area."

Find out more at lacework.com

Reltio

Reltio is a versatile, cloud-native data management platform that enables organizations to deliver hyper-personalized and connected experiences for their customers. They serve a broad range of customers, including high-end fashion brands, national chain restaurants, the technology and energy sectors, and nine of the world's ten largest pharmaceutical companies.