CASE STUDY

With Lacework, Snowplow secures their multicloud environments and protects against Log4j

SNOWPLOW

Challenges

- Achieve greater visibility into cloud environments
- Automate writing rules and checking logs
- Improve security posture

Solutions

- Deployed Lacework across 16 AWS sub-accounts in 30 minutes
- Applied Lacework on data pipelines to ensure deployed software is compliant
- Used Lacework to perform safety checks before updates reach customers

Results

- Gained visibility into environments to determine exposure to vulnerabilities, including Log4j
- Used reports from Lacework to easily demonstrate compliance during audits
- Secured AWS and Google Cloud environments and plan to use Lacework to help with future expansion into Azure

> "Had the vulnerability hit earlier, it would have been much more challenging. But we established pretty early on that our exposure to Log4j was low, which we could only do because we had Lacework as part of our security posture."

STEVE COPPIN-SMITH, VICE PRESIDENT OF ENGINEERING, SNOWPLOW

About Snowplow

Snowplow provides a platform to enable any company to collect first-party granular behavioral data for themselves, in their own cloud account, so that data practitioners can free themselves from the constraints imposed by web analytics vendors. It allows customers to track all behavioral event data, assure the quality of that data, and use any tool they want to answer important questions. This high-quality behavioral data is the driving force behind many fantastic digital experiences and the successful companies that provide them.

According to Steve Coppin-Smith, Vice President of Engineering, Snowplow's unique offering means that customers have a lot of control over how their environment is secured. "If they want to layer in a product, they can do that," says Coppin-Smith. "And they have a high level of auditability that they wouldn't get from public Software-as-a-Service (SaaS)." Snowplow uses the phrase "private SaaS" to describe their product, because, as Coppin-Smith says, "it's a SaaS-like experience with all the convenience of SaaS, but run within your own cloud, giving unrivaled levels of auditability."

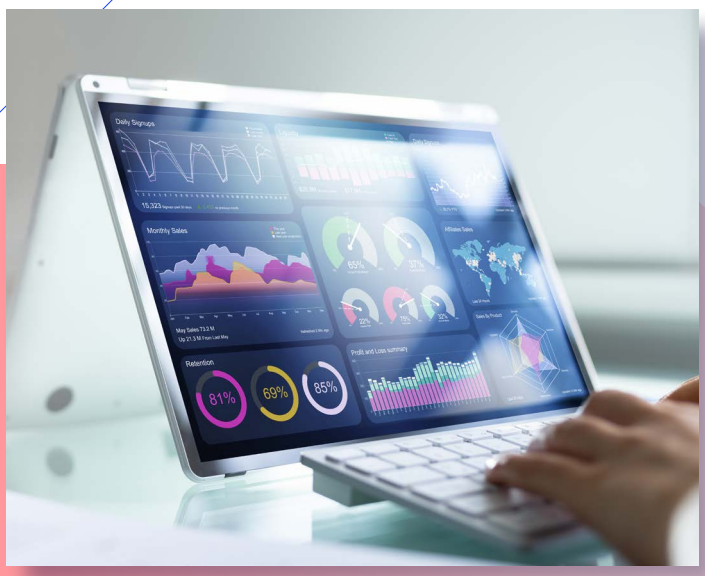
Currently, all of Snowplow's internal systems run on Amazon Web Services (AWS) and they deploy data pipelines for their customers across AWS and Google Cloud. They use a mixture of Kubernetes, Amazon Elastic Container Service (ECS), and Amazon Elastic Compute Cloud (EC2) instances. As Josh Beemster, Snowplow's Head of Technical Operations, says, "it's a mixture of deployment strategies."

Challenges

Prior to finding Lacework, Snowplow had used a number of different security solutions, but there was still a gap when it came to ensuring visibility while maintaining efficiency. "It's hard to know what good looks like if you don't have the visibility into what's happening in your environment," Beemster says. And with the small size of his team, it wasn't possible to manually achieve that level of visibility. "I want the team focused on supporting our clients and developing advancements to our product," says Beemster. "Sifting through logs and network traffic to find issues is important, but I'd much rather have a machine do that than a person."

Tuning rules by hand could easily turn into a scaling problem as well. "We were investing ourselves in manually checking these logs," says Coppin-Smith, "but we expected to grow as a company, which meant we would be growing that problem." With this growth in mind, they realized the value of a solution that could automate rule-writing and improve their information security position.

> "We have Lacework on our pipelines to make sure that how we deploy software, both for ourselves and for our customers, is compliant."
>
> STEVE COPPIN-SMITH, VICE PRESIDENT OF ENGINEERING, SNOWPLOW



> "There's minimal configuration required to start getting value from Lacework, to start seeing if there are issues in the environment, and to start getting actionable and tangible alerts."
>
> JOSH BEEMSTER,
> HEAD OF TECHNICAL OPERATIONS, SNOWPLOW

Solution

When Snowplow discovered Lacework, they decided to test it out with a trial deployment. "Deploying Lacework was incredibly easy, one of the easier integrations I've rolled out," says Beemster. "Snowplow uses a lot of Terraform and the wider HashiStack suite, and Lacework has done a lot of work around their application programming interfaces (APIs) to deliver modules that can plug easily into our estate." In all, he says, "getting Lacework set up across our 16 different AWS sub-accounts took about 30 minutes, and then it was integrated." Their CloudTrail and configuration scanning was done, and he could observe that their container and registry scanning, which they do through Terraform, were configured correctly. "Everything was done in code, exactly how I wanted it to be," says Beemster.

The ease of the installation process also suited Beemster's small team. "We've got a growing team, so we want to avoid doing arduous set ups by hand in the user interface (UI)," he says. But with Lacework, it only took deployment to start saving time and labor. "There's minimal configuration required to start getting value from Lacework, to start seeing if there are issues in the environment, and to start getting actionable and tangible alerts," Beemster says. "It was very, very easy to integrate and get Lacework working."

Snowplow has Lacework applied on their internal infrastructure: their orchestration and tooling. Says Beemster, "We use Lacework in our own internal staging development and production environments before it goes to customers so we can ensure that we're not going to introduce a massive issue into the several hundred environments we've been managing and propagating changes out to. It's a good check and balance." Lacework is also on Snowplow's data pipeline. "We have Lacework on our pipelines to make sure that how we deploy software, both for ourselves and for our customers, is compliant," says Coppin-Smith. "Our customers are free to decide whether to apply an intrusion detection system (IDS) to their pipeline, but whatever solution they decide upon, Lacework provides us all peace of mind that our software deployments are in compliance with industry standards."

Results

Securing multicloud environments

Given Snowplow's range of cloud providers, Lacework has proven to be incredibly valuable. "We're currently running agents in AWS, but we're looking to extend the same thing to Google Cloud," says Beemster. "We're also looking into Azure, so we will want to leverage Lacework there as well." When Snowplow transitioned from AWS to Google Cloud, they spent a fair amount of time invested in understanding how to secure Google Cloud. "It will be interesting when we adopt Azure to see how much time we shortcut," Coppin-Smith says. "Lacework will help guide us and provide evidence that we're doing the right things to secure the Azure cloud. It illustrates to us where we can make improvements to our security posture."

For their expansion into Azure, Snowplow intends to approach from multiple angles. "We need to make sure that we're scanning our replica dev environments and the different clouds that we're deploying in client pipelines," says Beemster. "In these dev and staging environments, we also need to look through ISO compliance standards and other prospective compliance checklists to make sure that we can tick all the boxes for client deployments. We'll be able to demonstrate compliance across multiple clouds, which is really powerful." Even as compliance standards evolve, Snowplow knows Lacework will help them stay current. "We'll have the information given to us so we can address it, which is quite nice and actionable," says Beemster. As Snowplow continues to grow, they look forward to expanding their partnership with Lacework.

Preparing for audits

Coppin-Smith recalls taking security questionnaires prior to deploying Lacework and being asked if Snowplow had an IDS. "We had faith in our people and in our design, but that only goes so far without validation," he says. "With Lacework, we have that intrusion detection capability. It feels like we have our estate independently audited." Now, Snowplow can back up their confidence with a solution that holds them up to best practices.

Snowplow also values how Lacework helps them prove compliance. They're ISO certified and intend to work toward further certifications. "Going forward, we can show that we have not only certain policies, but also a report from Lacework that demonstrates to what extent we're implementing those policies," says Coppin-Smith. He also likes that his team can save time by showing auditors screenshots that offer direct evidence of compliance. "For our first-year audit, we were being interviewed," says Coppin-Smith. "By year two, we could proactively share Lacework screenshots and illustrate that we were compliant to relevant areas of the standard. There's a big difference between our first and second year audits, and Lacework played a part in that."

> "Lacework will help guide us and provide evidence that we're doing the right things to secure the Azure cloud. It illustrates to us where we can make improvements to our security posture."
>
> STEVE COPPIN-SMITH, VICE PRESIDENT OF ENGINEERING, SNOWPLOW

Addressing the Log4j vulnerability

When the Log4j vulnerability sent the security world spinning at the end of 2021, Snowplow was grateful that they had spent the past several years investing in their security posture. The Lacework intrusion prevention capabilities gave them the flexibility to address Log4j in the way that was best for them and their customers. "We have Log4j in our estate, but it took time for us to realize that we weren't using it in the way that it could be leveraged," says Coppin-Smith. "If the rule was to shut down everything with Log4j, we would have caused a lot of disruption for our customers." They were especially concerned with maintaining high availability to their customers during that time. "We had to make a very nuanced set of decisions during those couple of weeks to determine the right cadence and timing to make changes. We didn't want our customers to have huge gaps in their data," Coppin-Smith says. "The way that Lacework is thinking about upcoming intrusion prevention features is very in line with our concerns about balancing the commitments we've made to our customers to keep their pipelines secure and collecting data."

Throughout the challenges of Log4j, Snowplow was grateful that Lacework was there to help. "Had the vulnerability hit earlier, it would have been much more challenging," says Coppin-Smith. "But we established pretty early on that our exposure to Log4j was low, which we could only do because we had Lacework as part of our security posture." Beemster agrees, saying, "If we hadn't had a solution like Lacework before Log4j, I would have been a lot more worried, because I wouldn't have had the full visibility into my environment." Due to Snowplow's use of Lacework, Beemster explains, "I wasn't worried about remote code execution exploits happening in my live environments, because I could see that none of them were happening. I could see exploit attempts, but there was no outcome." Determining that the environment was safe was important for their internal team as well as their customer-facing work. "Lacework gave us assurance that everything was okay, which is huge for peace of mind when we're also running on the same kind of infrastructure we deploy to clients and components we provide to the open source community," says Beemster.

Find out more at lacework.com

SNOWPLOW

Snowplow provides a platform to enable any company to collect first-party granular behavioral data for themselves, in their own cloud account, so that data practitioners can free themselves from the constraints imposed by web analytics vendors. It allows customers to track all behavioral event data, assure the quality of that data, and use any tool they want to answer important questions.