LACEWORK

CASE STUDY

Hypergiant uses Lacework to meet multiple compliance frameworks, consolidate tools, and cut down alerts to operationalize cloud security

HYPER GIANT

Challenges

- Eliminate need for constant rule-writing
- Manage dozens of AWS accounts safely and efficiently
- Meet rigorous compliance requirements

Solutions

- Brought environment up to NIST 800-171 standard during Lacework trial
- Immediately got actionable alerts and started auditing their environments
- Low-effort, high-reward deployment with minimal maintenance down the line

Results

- Consolidated three different tools
- Cut alerts down 70% to about three per day
- Reduced engineer workload by 20 hours per week
- Achieved necessary compliance to win more than $10 million in new business
- Democratized access to security event data and incorporated security directly into development process

> "The effort-to-pay-off ratio was fantastic. I've never had an easier-to-install product. In under two hours, I was done deploying it, had a multi-account CloudTrail, and had completely aggregated all of the CloudTrail for 30+ AWS accounts. How much easier can it be?"

BREN BRIGGS, VICE PRESIDENT OF DEVOPS AND CYBERSECURITY, HYPERGIANT

> "We're getting more high quality events and the log trash and alert noise has gone away. We get about three alerts a day, and they're always actionable."
>
> BREN BRIGGS, VICE PRESIDENT OF DEVOPS AND CYBERSECURITY, HYPERGIANT

Hypergiant overview

Founded in 2018, Hypergiant is an artificial intelligence enterprise software company that solves difficult problems in aerospace, defense, enterprise, and critical infrastructure industries. Their work in these spaces has led them to develop a strong DevSecOps discipline, not to mention a terrific design team. Bringing together all of their strengths, they create holistic solutions for their customers.

DevSecOps is at the core of Hypergiant's success. Bren Briggs, the Vice President of DevOps and Cybersecurity at Hypergiant, says, "DevSecOps is in our DNA. We've been doing this since day one, and from the ground up, it's integrated into our entire engineering process. Our approach is to make DevSecOps its own vertical."

Hypergiant has dozens of Amazon Web Services (AWS) accounts, and the number continues to grow. Briggs notes the importance of applying things like service control policies (SCPs) to their cloud accounts, as well as having a hierarchy where they're able to manage the rules applied to these accounts. "We're basically 100% infrastructure as code," says Briggs. "We have a lot of continuous integration/continuous delivery (CI/CD) that goes into this process, and we need to get ground truth of what's actually happening once the code is deployed and how users and entities are behaving in our environment."

Challenges

Managing this large number of AWS accounts posed several issues to Hypergiant. "We were facing a problem with account sprawl, where we had lots of different AWS accounts and we had to aggregate the logs from all of them," remembers Briggs. Even with the use of a multi-account CloudTrail, the process was difficult. "We realized that having agents to configure for every cluster and every AWS account was going to be burdensome," Briggs says. "We could aggregate and send logs into our aggregation solution fairly easily, but once they arrived into our SIEM, the problem was writing rules. And we had to write a lot of rules."

So they decided to baseline their environment, which required a lot of time spent sitting still as they observed it. "The needs of the business pulled against that," says Briggs. "We needed to move forward and keep developing new features and land new customers." Additional challenges arose during this process, as Briggs notes: "your baseline assumes that you are observing correctly, that you understand a lot of these elements of your application and how it behaves." But with its success depending on the expertise of those observing, accurate results weren't guaranteed, and the team at Hypergiant was wary. Instead, says Briggs, "We wanted to have something that was going to learn our environment and tell us things about it as we were writing rules." And the rules themselves became another issue that they were eager to address. "Writing rules for a constantly shifting or growing environment is very, very difficult," says Briggs. "That's another problem that we wanted to avoid."

Solution

Hypergiant needed a solution that could provide automation to help them manage all their AWS environments with speed and safety. When Lacework offered a two-week trial, Briggs leapt at the opportunity. "I dove right in and started remediating problems," he recalls.

He was especially excited by the ease of deploying Lacework. "The effort-to-pay-off ratio was fantastic," Briggs says. "I've never had an easier-to-install product. In under two hours, I was done deploying it, had a multi-account CloudTrail, and had completely aggregated all of the CloudTrail for 30+ AWS accounts. How much easier can it be?"

During the trial period, says Briggs, "we took an environment from effectively nothing in GovCloud and brought it all the way up to NIST 800-171 standard using infrastructure as code. That was instrumental in demonstrating that we had that capability and how quickly we could achieve it." In fact, seeing that capability in action paid off incredibly well for Hypergiant. "That was able to land us some very important business," Briggs says. "We continue to see the results of that."

Lacework has saved Hypergiant an incredible amount of time and effort so far. By using the Lacework agentless approach, which gathers insight into the AWS accounts, they no longer have to configure agents for each cluster and account. And during the trial, Briggs discovered the ability to automate deployment with Terraform. "We wrote a Terraform model that pushes out the config portion of the Lacework deployment," he says. "Now that's part of our standard baseline for all of our AWS accounts. Terraform gives each new account a baseline security config, and Lacework is part of that. Every new account automatically inherits those configurations and updates them as we go." With the ease of installing and automating, Briggs concludes, "Installing and deploying Lacework was a fantastically smooth experience."

In addition to the effortless deployment, Briggs loved that Lacework automatically provided solid data, right away. "We were able to immediately start getting actionable alerts and start auditing our environments," he says. "We can audit all of our accounts with the click of a button to see what their configuration state is, and if they're in compliance with certain frameworks or not. Again, super low effort, super high reward."

Results

Reducing rules

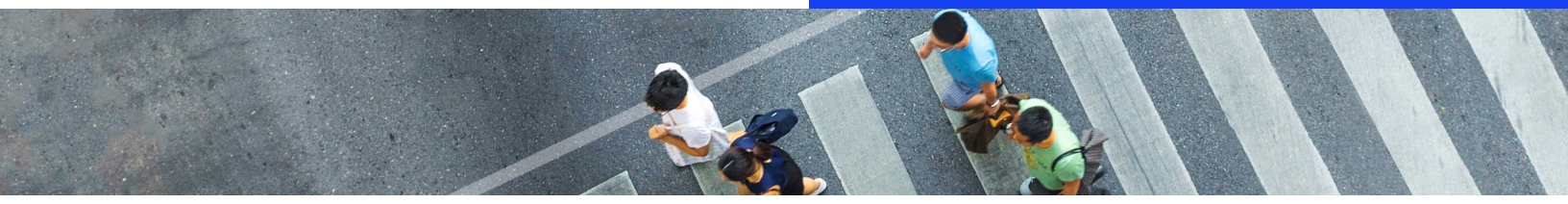
It only took a few days of running Lacework to convince Briggs that this was the right solution for Hypergiant. He particularly appreciates how the Lacework AI and ML works to surface events. "It's not noisy, and we can easily look at the raw data to see what's going on," says Briggs. "We're getting more high quality events and the log trash and alert noise has gone away. We get about three alerts a day, and they're always actionable."

But Briggs also appreciates that the Lacework platform complements his own team's occasional need to write their own rules. "We can augment what Lacework is doing, but with far fewer rules," says Briggs. "We're writing a fraction of the rules that we would have if we had chosen another solution." By minimizing the rules that Hypergiant's engineers have to write, "It allows us to move forward, to use infrastructure as code, but far less of it in order to get that observability and that ground truth of what's going on in our environment," Briggs says.

Meeting compliance standards

Given Hypergiant's extensive work with federal organizations, it's imperative that they meet a rigorous set of compliance standards. Lacework has the ability to help with compliance was a key selling point. "Lacework was able to show us where we were deficient in our baseline configuration when we were comparing ourselves against the NIST 800-171 and NIST 800-53 standards," says Briggs. "I was over the moon about it."

> "Lacework was able to show us where we were deficient in our baseline configuration when we were comparing ourselves against the NIST 800-171 and NIST 800-53 standards. I was over the moon about it."
>
> BREN BRIGGS, VICE PRESIDENT OF DEVOPS AND CYBERSECURITY, HYPERGIANT



Before Lacework, Briggs says he spent three or four days mapping NIST 800-171 controls directly from the regulation into AWS features and controls. "It was a lot of work. It took several days to get my head around these controls that we need to implement," says Briggs. "And then we came in after deploying Lacework, and not only did the platform have a much more nuanced idea of how these controls need to apply, but it had also set up some automatic and continuously scanning methods for detecting those configuration deficiencies." Lacework allowed Hypergiant to quickly solve the gap between understanding the 800-171 standard and applying it in the AWS environment. "The Lacework judicious application of AI and ML to generate and surface these events is what sets the platform apart," says Briggs. "It's very clever." Thankfully, Hypergiant can continue to rely on Lacework to ensure success when it comes to evolving compliance needs.

Consolidating tools

Hypergiant was also able to consolidate, integrate, and replace multiple tools when they switched to Lacework. "We ended up consolidating three tools together into Lacework," says Briggs. "Then we were able to integrate our existing ChatOps and alerting tooling as well." Now, it's a breeze to find and correct issues. "Say there's a module we're using to deploy all of our S3 buckets and it's missing an option required for doing federal deployments," Briggs says. "Lacework flags it immediately. We can go in and update that feature and we can solve that problem across all of our workspaces simultaneously."

Enabling developers

Since Hypergiant started deploying Lacework, they've used the platform to help developers make security part of their process. "Ultimately, security is everybody's responsibility," says Briggs. "It's our job to make sure that developers are able to push code quickly and that they're able to see and remediate vulnerabilities early on. This is a minimally invasive tool that doesn't change the developer workflow, but it gives us far more visibility into what's happening."

For example, Briggs recalls a recent experience where one of the developers was using a known unsafe Docker pattern in a deployment process and image. "Lacework filtered that up," Briggs says. "It told us that a new application launched with this image." When they went in to investigate, they realized that Lacework was there to educate its developer users. "Lacework automatically identified this anti-pattern because it requires super high privileges to run," says Briggs. "And then we were able to use Lacework to show the developer how to achieve the same result without the unsafe and highly privileged anti-pattern."

Using Lacework has proved indispensable across the board. "It's really so much more than catching a hacker coming in from the outside," Briggs says. "Lacework alerts us to supply chain problems, it lets us know when new applications are launched, and it tells us when we have developers who need to use alternative patterns."

All told, Briggs has been thrilled with the impact Lacework hast on assisting developers. "One of the major outcomes that I didn't anticipate, but am definitely thrilled to see, is how we're able to democratize access to the security event data," he says. And with Lacework to help educate developers, Hypergiant can easily integrate security into the development process, which is right in line with their company values. "We're trying to make security an integral part of our culture," says Briggs. "Not only should security be everybody's job, but everybody should feel comfortable doing it." Thanks to Lacework, all developers at Hypergiant can safely and effortlessly create secure environments as they continue to learn.

Schedule a demo today.

HYPER GIANT

Founded in 2018, Hypergiant is an artificial intelligence enterprise software company that solves difficult problems in aerospace, defense, enterprise, and critical infrastructure industries. Their work in these spaces has led them to develop a strong DevSecOps discipline, not to mention a terrific design team. Bringing together all of their strengths, they create holistic solutions for their customers.