CASE STUDY

Cazena secures massive cloud data lakes with Lacework

CAZENA

Challenges

- Visibility in multicloud environments for customers
- Detecting anomalies across large volumes of data
- Limited security resources
- Manual AWS CloudTrail and Azure log reporting

Solutions

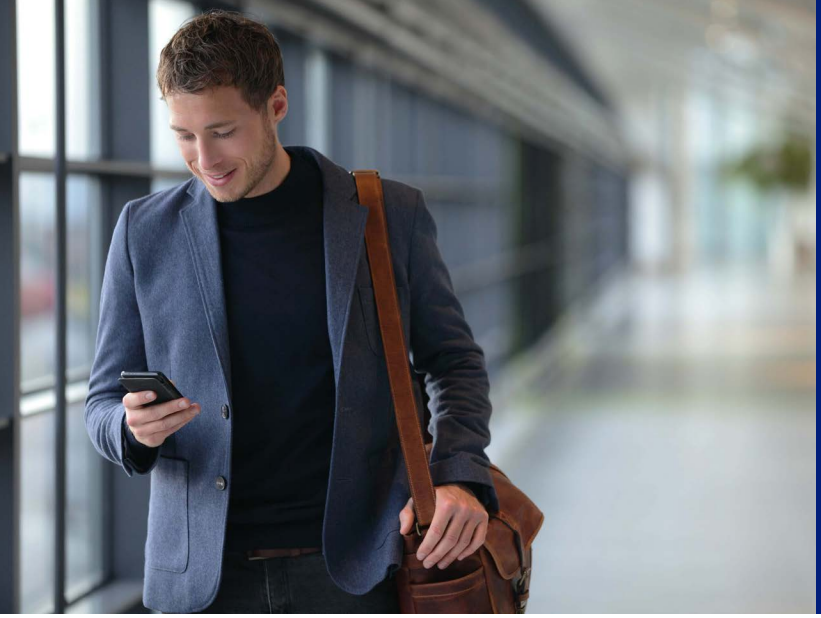
- Lacework shows activity that is out of the norm
- Lacework provides every detail about unusual events
- Lacework automates all log reporting

Results

- Reduced noise generated by the security stack
- Identifies anomalies in customer environments better than customers can themselves
- Cazena achieves the most secure SaaS Data Lake
- Increased operational efficiency

> "I find that Lacework is so granular in detecting anomalies within either Cloud, that it allows me to make all of my other operations better because it's so fine tuned."

BRIAN LACHANCE, CHIEF INFORMATION SECURITY OFFICER AT CAZENA



> "A real value of Lacework is that when it detects something, it doesn't just tell you something happened. It gives you every detail you could imagine about that event."
>
> BRIAN LACHANCE, CHIEF INFORMATION SECURITY OFFICER AT CAZENA

The company and its business

Cazena is a SaaS company that provides cloud-based data lakes as a software service. Cazena's Hadoop data lake environments are production-ready, fully managed, and continuously optimized. "The environments are set up as clusters with various application layers used for analytics," explains Brian Lachance, Chief Information Security Officer at Cazena. "Users have access to all their preferred Hadoop tools. We host the environment in a DevOps SecOps framework. We provide security and constant updates to the environment." Given that their customers are evenly split between Azure and AWS, Cazena provides cloud agnostic tools. Most customers access the data lakes through VPN connections.

The security challenge

For Cazena, the big security challenge is having adequate visibility in an environment in which customers typically use automated tools to access the data they own and control. Lachance says, "We monitor all access to and from our environments. We have folks on our systems that have shell access, running analytical commands. That makes it difficult to determine if something improper is happening on our system." He notes that there are often cases where somebody with authorized access does something that's unauthorized. To monitor all this activity, Cazena decrypts and examines all traffic in their environment, but that represents an enormous amount of activity data.

Choosing Lacework

The challenge of analyzing large amounts of activity data was a major reason why Cazena began seriously considering Lacework. "I thought Lacework had a really unique solution with anomaly detection," says Lachance. "I've used traditional definition based vulnerability detection. Lacework filled a gap for us, which was just to determine what was being done out of the norm." This was really important in an environment where so much activity is driven by autonomous processes. There are so many attack vectors to monitor. Doing it effectively required tools that can consolidate that data into usable form. Lachance notes, "A real value of Lacework is that when it detects something, it doesn't just tell you something happened. It gives you every detail you could imagine about that event."

Implementation

When Cazena tested Lacework, they were immediately sold on what it could do for them. In their particular case, implementation involved integrating it into their automation tools so that it would become part of their customer environments. That required integrating Lacework into their development process.

Greater visibility strengthens the entire security stack

The added visibility and a machine learning approach to alert filtering has helped reduce the amount of noise generated by the security stack. "The reduced noise is key for us," Lachance explains. "We receive alerts non-stop from our enterprise firewalls. We have internal audit monitoring tools. We use Splunk, and that's consistently going off. Using Lacework to reduce that noise has been really great." It has also helped identify potential vulnerabilities they had not considered before. For example, Lacework identified a type of DNS attack on their service that was coming through customer access to their system even when customer traffic was not crossing their network. "We've put a lot more emphasis on DNS security as a result of that finding," says Lachance.

Lachance notes that Lacework is so granular in detecting anomalies within their cloud environment that it has improved the effectiveness of all the other tools in their security stack. This is a capability customers value. "Our anomaly based detection can identify anomalies in their environment better than they can themselves," says Lachance. "Lacework ends up being a sales tool for us."

Find out more at lacework.com