CASE STUDY

Kayrros uses Polygraph to protect precious geo-analytics data

KAYRROS

Challenges

- Convey critical ecological information in the face of malicious attacks
- Defend against intruders with visibility through cloud security posture management (CSPM)
- Understand network communication between components across multicloud infrastructure

Solutions

- Set baseline for alerting on anomalous behavior with Lacework Polygraph® Data Platform
- Increased visibility by using Lacework to process and digest large volume of AWS CloudTrail data
- Gained quick understanding of infrastructure with monitoring and vulnerability management

Results

- Received less than 5 critical/high alerts per day, cutting investigation time and improving remediation
- Raised baseline security level by integrating inline scanner on CI pipelines
- Protected multicloud environment with visibility into infrastructure and vulnerabilities

"I have never seen a solution with the capabilities and comprehensiveness of Lacework."

THOMAS LINCK, HEAD OF INFRASTRUCTURE, KAYRROS

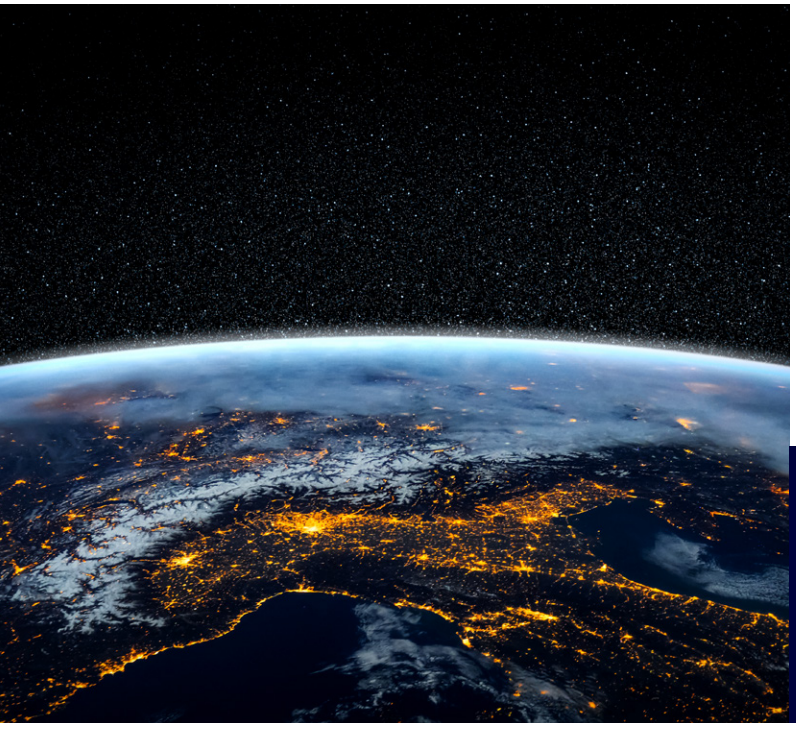
About Kayrros

Kayrros is a leading advanced energy and environmental geo-analytics firm. Founded in 2016, Kayrros uses technology to process satellite imagery, geolocation data, textual information, and multiple sources of alternative data to monitor and measure energy, natural resources, and industrial activity worldwide. Traders, investors, operators, and governments then use this data to make better decisions on energy and the environment.

"We rely on many compute technologies, including containers, to provide the solution and project teams with what they need," says Thomas Linck, Head of Infrastructure at Kayrros. "My team's main job is to ensure that our infrastructure and security are best-in-class — meeting industry standards and providing best-practice configuration."

As part of this effort, one member of Linck's small-but-mighty six-person team is dedicated to incident response, tackling everything from monitoring and availability to security issues. This involves overseeing a complex multicloud environment, which includes Amazon Web Services (AWS) and Kubernetes.

"We're also responsible for adding new infrastructure as business needs arise," Linck adds. For example, when the company wants to produce a new product, Linck's team will create a new AWS account with a new Kubernetes cluster. Then, they'll confirm that they can operate it successfully. "We need to ensure that, at any time, we can deploy anything on our infrastructure, monitor it, and collect logs from it. If anything goes wrong, my team will respond quickly," says Linck.



Challenges

Thomas Linck is fully aware of the risk associated with the industry his company operates within. As a critical player in the energy and ecology sectors, Kayrros is a handler and provider of lots of important — and extremely sensitive — data. "We have a big impact on the ecology world, which makes us vulnerable to attacks," Linck notes.

Keeping data secure at a company like Kayrros isn't simply a tertiary matter for the IT department; it's a matter of existence for the entire organization. "Cloud security is key at Kayrros," says Linck. "It's a concern for the legal team, the compliance team, the financial team. It's a concern for customers who need to know we're securing their data correctly."

For Kayrros, keeping data secure in part meant setting up a sufficient intrusion detection system (IDS) and an intrusion prevention system (IPS). "We want to make sure that the information we provide is authenticated, so we don't have people manipulating our data," says Linck.

By adding IDS and IPS capabilities, Linck's team hoped to achieve greater visibility into their cloud environment. "We wanted to go further than just protecting the perimeter," Linck explains. "If you think of our infrastructure as a castle, we are now adding an extra level of security to watch for intruders inside the walls."

The other key objective for Kayrros was to increase their visibility and compliance with cloud security posture management (CSPM). With risk remediation and continuous monitoring, CSPM can more effectively protect cloud environments from threats. "We had to make sure that our security posture and wellness were at their best level," Linck notes.

The entire company and their customers leaned on Linck's team to find a platform solution that could meet all of their needs. "We needed a one-stop shop for IDS and IPS, vulnerability management, CSPM, and compliance," Linck explains. "At any given time, we need to be able to see and understand the network communication between components of our infrastructure."

Luckily, they found a platform that fit the bill.

> **"The deployment was very easy. It was about a day's work to integrate everything."**
>
> THOMAS LINCK, HEAD OF INFRASTRUCTURE, KAYRROS

Solution

With a clear sense of their security needs, the Kayrros infrastructure and security team set out to find their solution — and came across Lacework. "I have never seen a solution with the capabilities and comprehensiveness of Lacework. Its unique approach automatically learns what's normal across our infrastructure and detects behavior that deviates from the norm," says Linck.

From a CSPM standpoint, Linck's team discovered that the Lacework Polygraph Data Platform could help them achieve their compliance goals with out-of-the-box reports and simple integrations. The Lacework cloud log ingestion capability stood out to Linck's team for its ability to help process both EKS and CloudTrail logs.

This was welcome news to Linck, who saw potential in leveraging his company's AWS CloudTrail data, but was overwhelmed by the sheer volume of data produced by the logs. "CloudTrail is a mine of information, but there's so much data that it can be difficult to use," he says. "At this step in our cloud journey, we needed to make sure we could digest all of this information."

Since Kayrros wanted to go a step further by adding security alerting capabilities, the Lacework team came in to set a baseline. From there, the deployment process immediately kicked off. "The deployment was very easy. It was about a day's work to integrate everything," recalls Linck. "The cloud accounts integration was very simple, with just a Terraform template to run. Integrating with our alerting tool (PagerDuty) was just as seamless."

Linck's team was also impressed with the Lacework IDS capabilities. They quickly witnessed how the Platform, with its patented machine learning technology, allowed them to monitor across their entire environment. Its unique anomaly-based detection capabilities reduce the need for custom rules and policy tuning — and it combs through vast amounts of data to surface just the right number of context-rich alerts, helping users speed remediation processes.

With its ability to surface alerts on anomalous behavior, the Platform gave Kayrros the ability to truly understand their infrastructure. And thanks to its alert prioritization, Lacework empowers Linck's team to respond and remediate with efficiency.

> "We get just a handful of alerts from Lacework — less than five per day."
>
> THOMAS LINCK, HEAD OF INFRASTRUCTURE, KAYRROS

Results

Intrusion detection on autopilot

For Linck's lean team, the Platform's anomaly detection features have been instrumental. "We get just a handful of alerts from Lacework — less than five per day," says Linck. "Our incident response engineer receives them in real time, so he can look into what's happening and determine how to respond."

Linck's team appreciates the Lacework user interface, which features graphs that show how many events have been ingested, and which are critical or high. "By doing this work automatically for us, Lacework saves us a lot of time on security management," Linck explains. "We just see the events when they show up in the Polygraph Data Platform and make sure to resolve them. This allows us to focus on security, which is our top priority."

With a comprehensive view into Kayrros' environment, the Platform has also detected and resolved a number of longstanding issues. "Lacework has enabled us to discover unusual behavior in our legacy tools," says Linck. "Had we not found this behavior, it could have led to security flaws."

Secure and compliant from build time to runtime

Lacework has been a gamer changer in helping Kayrros shift their security practice left by integrating security capabilities into their software supply chain workflows. "When we first used Lacework, we had registry scanning enabled to make sure that our containers were free of vulnerabilities," Linck recalls. "Then, we realized we could check our containers for security flaws before pushing them to the container registry. To do that, we integrated the Lacework inline scanner into our pipelines." The inline scanner makes it easy to scan and assess container images for vulnerabilities.

Kayrros plans to further bolster their security by ensuring that everyone can run an inline scanner on their containers during development. "Lacework is really providing everything we need to shift left and to make sure that the deployment workflow is secure at every stage," says Linck.

Kayrros also plans to leverage compliance tools from Lacework in their continued effort to reduce risk across their clouds. For clients dealing with sensitive energy-related information, compliance is critical. Linck notes, "We know Lacework has built-in SOC 2 and ISO 27001 reports, so we'll definitely use those when the time comes."

> By doing this work automatically for us, Lacework saves us a lot of time on security management... This allows us to focus on security, which is our top priority."
>
> THOMAS LINCK, HEAD OF INFRASTRUCTURE, KAYRROS

More visibility, better understanding

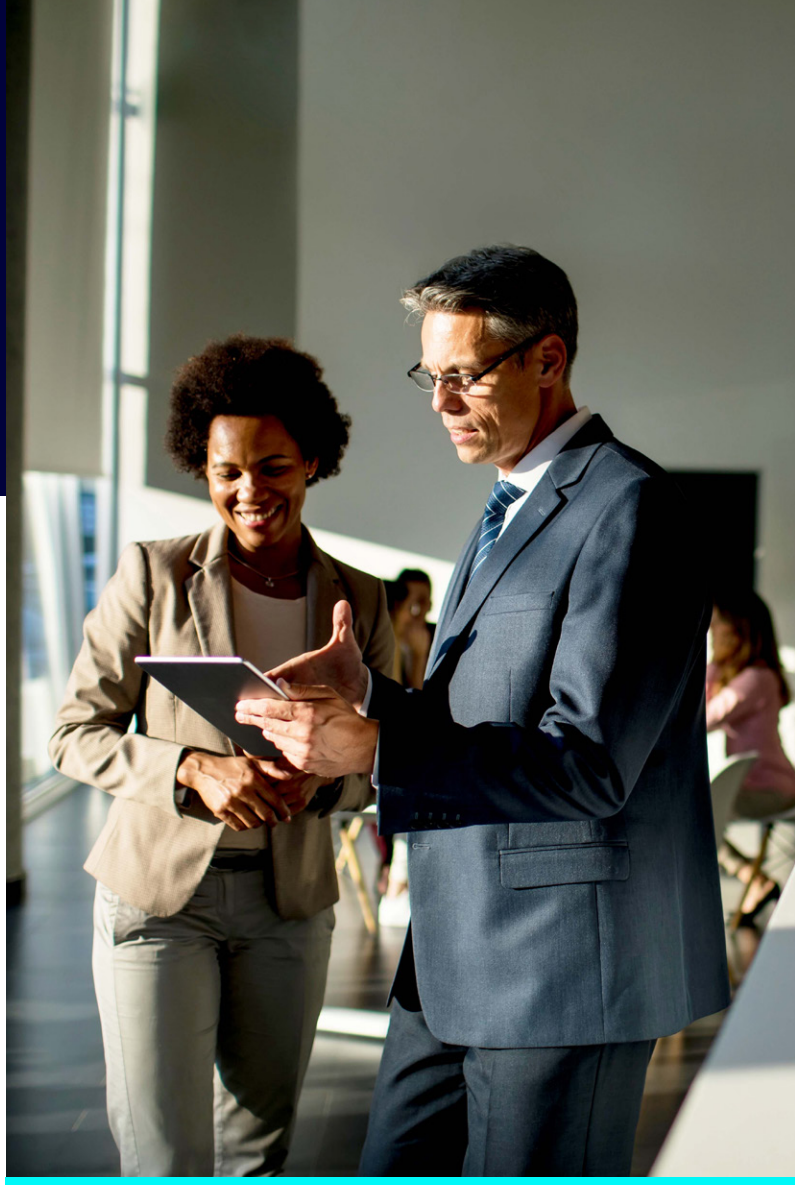
"Lacework helped us achieve deep visibility into our infrastructure," explains Linck. "Now, we have a solid understanding of it."

According to Linck, whenever they need, Kayrros can use the Platform to get crucial details about their cloud environment — even beyond security. "We are able to really comprehend what's going on not only from a security perspective, but also from a network perspective and a system perspective," he says. "With Lacework, we can understand the network communication between the components of our infrastructure at any time and can see security vulnerabilities."

Kayrros is even using the Platform to plot their own security priorities. "Since integrating Lacework, we have all kinds of information to act on," Linck states. "We are now building our security roadmap based on the output from Lacework."

Overall, Linck and his small team accomplished their task: to represent their company and customers in finding an effective, multi-faceted cloud security solution. And this increased sense of security has had a huge impact on the Kayrros team. "Lacework is really bringing us the visibility we need, which is the most important thing for me. I can sleep better at night thanks to Lacework watching out over our cloud environment," Linck concludes.

Schedule a demo today



> "Lacework is really providing everything we need to shift left and to make sure that the deployment workflow is secure at every stage."
>
> THOMAS LINCK, HEAD OF INFRASTRUCTURE, KAYRROS

KAYRROS

Founded in 2016, Kayrros is the leading advanced energy and environmental geo-analytics company. Kayrros harnesses satellite imagery, geolocation data, textual information, and multiple sources of alternative data with machine learning, natural language processing, and advanced mathematics. With these technologies, Kayrros monitors and measures energy, natural resources, and industrial activity worldwide. Their data enables traders, investors, operators, and governments to make better decisions on energy and the environment.