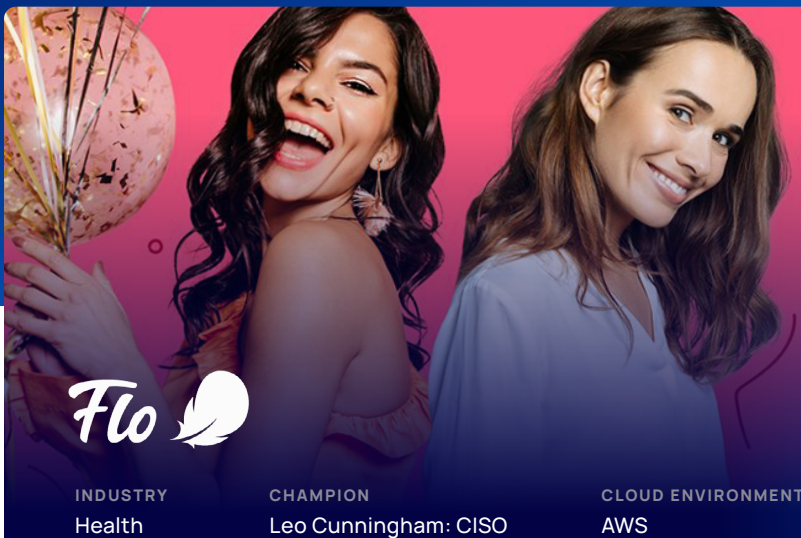# Flo Health Builds an Automated Defense Strategy, ROI Time Savings Equivalent to Five Full-Time Employees, and Eases ISO Compliance Efforts with Orca Security

"With Orca Security, we saw a return on investment straight away, which is unheard of with most security tools."

Leo Cunningham
Chief Information Security Officer
Flo Health

INDUSTRY
Health

CHAMPION
Leo Cunningham: CISO

CLOUD ENVIRONMENT
AWS

Cloud Security Challenges

- Rapid pace of a startup can result in security lapses

- Adopt a data-driven, automated approach to security

- Increase visibility into the cybersecurity posture across the entire technology stack

- Ease ISO compliance efforts

Cloud Security Results

- Orca consolidates alerting into one place and gives a detailed view of the security posture for the entire cloud estate

- Integration with Jira and automation reduces friction with software engineers and accelerates time-to-remediation

- Orca eases compliance efforts for CIS, PCI DSS, ISO, and more

- Return on investment has been strong and almost immediate; the closed-loop process saves the time of five full-time employees

200 million women rely on Flo Health's app for critical health insights

Flo Health provides a health product that encompasses solutions for females at every stage of their life (start of menstruation, cycle tracking, preparation for conception, pregnancy, early motherhood, menopause). Flo provides curated cycle and ovulation tracking, personalized health insights, expert recommendations, and a private community for women to share their questions and concerns. The app records thousands of data points to help them make informed decisions about their health.

Prioritizing safety, Flo keeps a sharp focus on being the most trusted digital source for women's health information. The app uses intensive data science and AI to deliver the most personalized content and services available. Flo's period tracker is currently available in 22 languages on iOS and Android. 60% of the app's 200 million users are located in the US and Europe.

Leo Cunningham joined Flo Health in early 2021 as its Chief Information Security Officer. He is tasked with building a world-class security function. He also helps Flo employees make the right decisions pertaining to handling data and the technology that supports it.

"Flo is an engineer-led, data-driven company, which helps us make informed decisions around the security of any new product features or development," says Cunningham. "I wouldn't say it's a traditional security function. As a cloud-native startup, we want to use the latest and greatest security technology. We think of traditional security solutions as a drawback to our rapid pace of development."

Orca is a standout in a crowded field of security products

Flo Health evaluated at least ten security tools. "We have all that security information on AWS, but it's across many components," says Cunningham. "The challenge is, how do we take a snapshot of time and place around what we have from a security point of view and have it all in one location? What does that look like against compliance benchmarks like CIS? How do we automate a lot of those tasks and remediation?"

Among the tools considered were Rapid7, Palo Alto Networks, Splunk, as well as traditional SIEM services. "We need a vendor that can understand our requirements and our technology stack, and who can partner with us for the long term. Traditional security products typically require a lot of configuration," says Cunningham. "What stood out about Orca, among many things, is that it is a younger company with a lot of vibrant activity in the background. Gartner says it's one of the coolest up-and-coming vendors, and that's what we want—a new wave solution that isn't tied to past approaches or technologies."

> "We compared about ten security tools, and Orca Security was a standout. We were completely blown away after a 10-minute demo. Other products were just stuck in the mud."
>
> **Leo Cunningham**
> Chief Information Security Officer
> Flo Health

"Orca spins up so quickly, and its ease of navigation is so important. I showed it to our C-level executives and they understood it quite well. Orca is well structured."

Following a brief evaluation, Flo Health committed to the Orca Security platform. "With Orca being agentless, our cloud security lead got it up and running and we took our first snapshot within a few hours. After that, it was very easy to get a login and start adding integrations. It plugs in seamlessly with what we have," explains Cunningham.

Orca Security's closed-loop integration and automation with Jira saves the cost of about five full-time employees

The Orca Security platform is part of a long-term strategy. Flo Health has set up integrations and automation into Jira, which Cunningham calls "a complete game-changer. Orca takes a snapshot and sends items into specific engineering queues in Jira, where the software engineers can work on them right away."

Automation is Cunningham's team goal. "We want to completely automate as much as we can," he says. "The information that Orca provides is very clear. 'Here's the vulnerability's precise location, the attack path, and the links to address it.' Then we can fix it, update Jira, and it's recalibrated back into Orca in the next snapshot. The process is such an improvement over having to dig about, looking for things manually, then figure out the remediation."

This closed-loop process has proven to be a real time-saver for Flo Health. Cunningham estimates it saves the time of about five full-time employees. "Orca has been essential in automating tasks without having to get six people on a call and telling them what to do. We created an easy workflow process that they can read. Orca completes its daily scan and sends very specific information about how to remediate or advise. When people wake up the next day they're ready to go. The teams sign in, see a Jira ticket, then do their thing. Then they post to us that it's been done, which we validate the following day when Orca takes another fresh snapshot."

"The integration between Orca and Jira is a game-changer for us. Orca is key to automating the work tasks for our global teams. This lets us release code continuously ten times a day into the cloud, making us much more efficient."

Leo Cunningham
Chief Information Security Officer
Flo Health

Orca Security complements AWS native tools and accelerates time-to-remediation

Prior to implementing Orca, Cunningham said Flo Health's visibility was limited. "We were scrambling, looking at multiple AWS dashboards while we needed to know something ASAP. When you can't get an answer right away, it undermines our team methodology and overall security approach."

The company uses several native AWS security tools, including GuardDuty, Inspector, CloudShell, and Tower. "Orca consolidates everything we have, and it looks deep down into our technology stack—including within containers," says Cunningham. "It's important to have something that can instantly tell us what we have, if there are any impacts, what needs to be done, and what's the practicality—that is, what's the size of that impact across our estate?

Orca provides that and gives us additional mileage as to what we're looking at across our infrastructure and cloud. No other technology was able to provide us with that on the cloud infrastructure side."

Complete coverage for cloud misconfigurations, exposed S3 buckets, and language libraries

Cunningham notes that the rate of change in a startup company is exponential at times. It's very easy for someone to miss something like a misconfiguration or an S3 bucket that's exposed. And Flo Health's technology stack is massive. Orca is able to consolidate everything across a wide domain, as well as other items that people might not necessarily perceive as security issues—but are. For instance, Orca looks at specific third-party language libraries such as Scala and Python as well as plugins like Adobe.
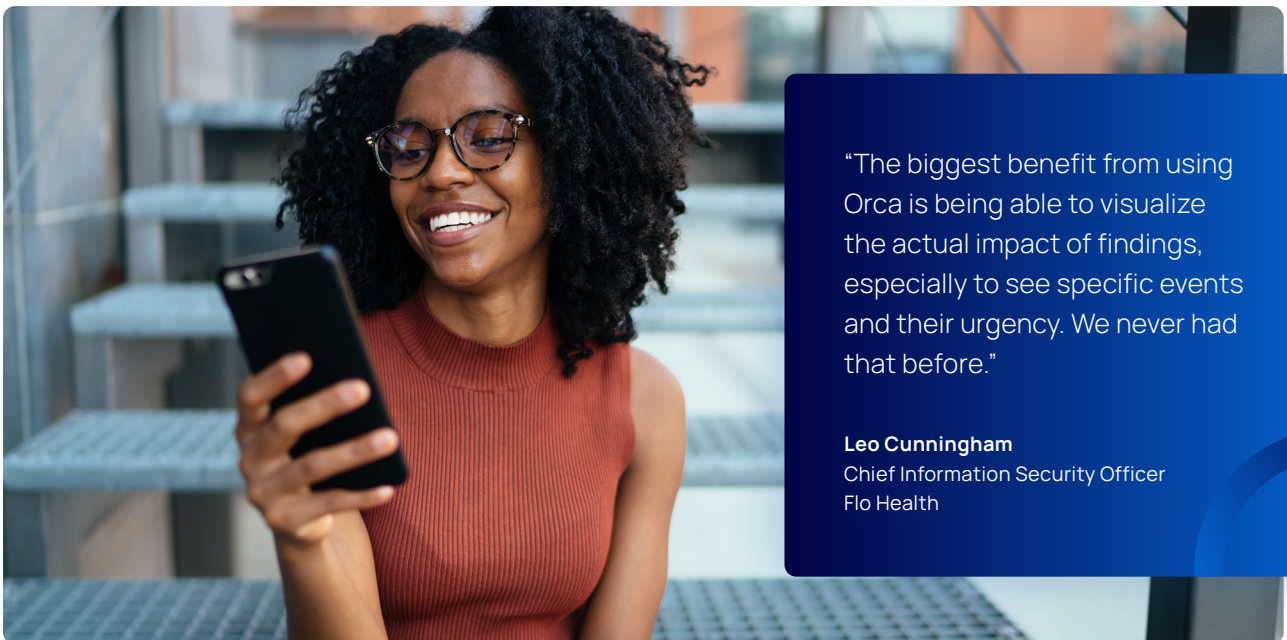
"The biggest benefit from using Orca is being able to visualize the actual impact of findings, especially to see specific events and their urgency. We never had that before."

Leo Cunningham
Chief Information Security Officer
Flo Health

orca security

Orca Security reduces alert fatigue

"Once we fine-tune a bit on the backend, Orca then creates a filter of what is classified as urgent, or less so. Then we create our Jira work queues to get the response process going. There's no fatigue from over-alerting—it's all under control. This has empowered us to build a security intelligence capability within Flo," says Cunningham.

Orca helps Flo Health meet compliance mandates such as ISO 27001

"Orca has an extensive list of compliance benchmarks for CIS, PCI DSS, ISO, and more so you know where you are in meeting them. It's very helpful to cloud engineers who aren't necessarily security people. They become educated as to how something relates to security, especially in dealing with PII or other sensitive data. Orca really helps us with external audits as well.

"As we build out our world-class security function, Orca has exceeded our expectations. We're building a long-term security strategy around this platform," says Cunningham.

About Orca Security

Utilizing its unique patent-pending SideScanning™ technology, Orca Security provides cloud-wide, workload-deep security and compliance for AWS, Azure, and GCP. After an instantaneous, read-only and impact-free integration to the cloud provider, it detects vulnerabilities, malware, misconfigurations, lateral movement risk, authentication risk, and insecure high-risk data—then prioritizes risk based on the underlying issue, its accessibility, and blast radius - without deploying agents.

orca security

Connect your first cloud account in minutes and see for yourself: **Visit orca.security**