


# In a Regulated Financial Services Industry, Orca Security Helps Cake Become Proactive on PSD2 Compliance




**cake**

INDUSTRY  
Financial Services

CHAMPION  
Pieter Schelfhout:  
Head of Engineering

CLOUD ENVIRONMENT  
AWS

"We couldn't wait on periodic security checks. Orca helped us move to a method that's automated, that's checking every day, and that we can follow up on more easily."



**Pieter Schelfhout**  
Head of Engineering  
Cake

## Cloud Security Challenges

- ✗ Needed to move from a periodic, manual process to an automated one to gain actionable insights into its cloud security posture
- ✗ Must comply with Europe's Revised Payment Services Directive (PSD2) to operate as a financial services app
- ✗ Take a proactive stance on quickly finding and fixing misconfigurations

## Cloud Security Results

- ✓ Gain an "inside-out" view of a complex AWS environment: 3 accounts, 240 containers, 100 databases, 50 buckets, 20 VMs, 360 policies
- ✓ Full workload level visibility without agents
- ✓ Avoid two FTEs and tedious manual work
- ✓ Can prove to auditors it complies with PSD2

## Cake is a Unique New Banking App for European Consumers

Cake's mobile banking app analyzes a person's financial transactional data to help them better understand, control, and improve their finances. It's supported by a unique business model that shares revenue with users. It brings together all of a person's bank accounts, provides insights into their financial data, and helps them optimize their daily income and spending.

Cake also has a commercial offering for partners and retailers that provides reports and insights based on aggregated, anonymized data. Partners can use the data to send specific offers to Cake's users, who can earn cash-back Rewards if they accept an offer.

Europe is the ideal location for the startup company to launch its business, according to Head of Engineering Pieter Schelfhout. "We're taking advantage of PSD2. It's EU legislation that's opening up the financial markets and data market inside of Europe," he says. PSD2 makes the company's business model possible, but strictly regulates the security and privacy of data passing through Cake's app.

"Licensed by the National Bank of Belgium, we're a regulated company with a passport for Europe. That means we get audited. Everything around our business model—our IT infrastructure, security, privacy—is part of our license. It's all very controlled here in Europe; we have to comply with certain standards and expectations."

Cake was introduced to Orca Security by their trusted advisor Shift Left Security. Shift Left Security helps companies build, develop and

operate secure applications running in Amazon Web Services, Microsoft Azure, Google Cloud Platform or private clouds.

## Orca Security Fits with Cake's Continuous Monitoring Approach

Schelfhout says, "We built our infrastructure and security policies, and have audited it from the beginning. We use third parties to do a first level check; they check our architecture, penetration testing, and so on. Now we want to evolve to a more permanent monitoring and evaluation of our platform. Orca Security is a tool that lets us continuously scan our environment."

Schelfhout truly appreciates that Orca is a tool that can be used every day, not every three months. He's making it part of Cake's permanent production process. "It gives us an overview of all vulnerabilities

"Orca is fully cloud-native, so integrates well with AWS. Its compliance feature checks all kinds of policies that should be enabled in a cloud environment—especially in Amazon environments, which is what we really care about."

**Pieter Schelfhout**  
Head of Engineering,  
Cake

we have, and matters we can immediately act upon. It's all real time and fits well with the level of monitoring we want to achieve."

## A Cloud Environment Most Enterprises Would Envy

With versions for both iOS and Android, the Cake app is mobile-only. But its built-from-scratch infrastructure is entirely in the cloud. Except for a few scattered APIs, the company is all-in on AWS, where it has several accounts: one each for staging, QA, and production. A set of microservices run Kotlin Java with a stack that surfaces everything pertaining to financial data.

Cake runs Spark in a Kubernetes cluster. That's where all data aggregation and analysis is done, and where its data science environment plugs in. It then explores and builds new models, which are also deployed as microservices.

A Cake-for-Business online portal runs separately from its other services. Cake's three domains are fully separated, yet are connected by an event messaging bus that exchanges information among components. Modern app approaches fully leveraging AWS cloud capabilities, Cake uses S3 buckets for storage, AWS Athena riding on top to query the buckets, and AWS KMS to encrypt all the databases at once.

## Orca Catches Otherwise Unseen Errors in a Complex Environment

Cake's AWS environment is made all the more complex by all the options AWS provides. It needed a

tool such as Orca to surface potential configuration problems. "Even for our experienced team, it's a full-time job to really stay on top of whatever Amazon is doing," Schelfhout remarks. "We wanted an external point of view that readily exposes any misconfigurations and other issues. Cake already automates and tests many of these checks, but even then configuration errors can propagate throughout the system."

Although Cake has only three AWS accounts, it has nearly 360 active policies due to there being numerous containers. Being all too easy to overlook a mistake, Schelfhout cites an example: "It's straightforward that the default security group of every VPC should restrict all traffic. All is good for most of our policies, except 49 had an issue we needed to fix. It being an automated scanning tool that checks everything, it was Orca that informed us of that, thankfully."

There being so many moving parts, he explains how configuration errors can easily spread. "With the three accounts we're currently scanning, we have about 80 containers in each. There are about 100 databases, 50 buckets, and roughly 20 VMs. The QA configuration may be correct, but then something goes wrong. The production environment doesn't have the same configuration, so then we need to assess those differences. Even though Cake has a strictly automated release process, we appreciate having Orca check our work and make sure that everything remains in sync."

## Automation – Essential to a Secure Environment

Initially Cake used a manual issue-checking process, relying on its own expertise during periodic testing. It then adopted environment checks from an

external point of view, though these ran only every few months. “Yet we release new features almost daily and things move quickly,” says Schelfhout.

Manual checks of Cake’s environment would require at least two full-time people doing very intensive work, Schelfhout asserts. “It’s a lot of work without a tool such as Orca. Now we can readily see issues on its dashboard and add them to our regular fix release process. We’re able to operate more smoothly, and increase our productivity.”

Both the security and DevOps teams benefit from using Orca, as they get an inside-out view of Cake’s infrastructure. “Orca is really focused on all that DevOps touches—policies, configurations, and assets that need to be kept up-to-date. It’s a really insightful tool; our teams can spot problems really fast that would otherwise be hard to detect.”

## Orca Has Earned Its Place in Cake’s Toolbox

Schelfhout really likes how easy Orca is to use. “The compliance report is great because, in my role, it provides a thorough overview regarding how well everything is doing. From a DevOps point of view, they mainly look at the dashboard’s Assets and Alerts tabs. They then check out how their clusters are doing and whether everything is correctly configured—it’s all practical insight that our teams can take immediate action on if necessary. Orca helps keep the Cake environment clean and functioning as expected, all the while being compliant with all-important regulations.”



## 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.



Connect your first cloud account in minutes  
and see for yourself: [Visit orca.security](https://www.orca.security)

