HOW 5 FINSERV CISOS NAILED CLOUD SECURITY & COMPLIANCE

C6 Bank Strengthens Cybersecurity as a Core Value with Orca Security

INDUSTRY
Financial Services

CHAMPION
Jose Luiz Santana, Partner & CISO

CLOUD ENVIRONMENT
AWS, Google Cloud

> *“Since the beginning, security has always been one of the most important pillars for C6 Bank. Orca helps us strengthen that pillar.”*
>
> **Jose Luiz Santana**
> CISO
> C6 Bank

Cloud Security Challenges

- ✗ Gain full visibility into multi-cloud infrastructure
- ✗ Find a security tool with the versatility to perform numerous functions
- ✗ Surface threats and map them to the MITRE ATT&CK Framework
- ✗ Gather information to meet compliance requirements, including Brazilian frameworks and other global regimes

Cloud Security Results

- ✓ Orca provides complete visibility and easy-to-use security across AWS and GCP
- ✓ More than a CSPM or CWPP tool, Orca offers threat hunting, vulnerability assessment, incident response and more from a single, unified platform
- ✓ Orca’s ability to surface threats mapped to the MITRE ATT&CK Framework is a powerful way to understand threats
- ✓ Orca helps C6 meet compliance requirements for both Brazilian and United States banking regulations

Full-service digital banking serves millions across Brazil

Launched in 2019, Brazil's C6 Bank is growing rapidly as a full-service digital bank. With more than 25 million customers on its digital platform today, C6 Bank is one of the fastest banks in the West to have reached 1 million customers. The company began with 15 employees and has grown to a workforce of around 4,000 people. The impressive start caught the attention of JPMorgan Chase, which took a 40% stake in C6 Bank in 2021.

The bank offers a range of services, including checking and savings accounts, debit and credit cards, toll tags, multi-currency global accounts, investments, and lending products. C6 Bank serves individuals as well as small and mid-sized businesses, and has accounts opened in all of Brazil's 5,570 municipalities.

Jose Luiz Santana is one of the bank's founding members. He is also the Chief Information Security Officer. "We are a digital bank with no branches," says Santana. "Our main goal is to provide financial services to the Brazilian market in an easy, high-tech way that helps our customers to have a good relationship with money. We want to help people achieve their goals and the objectives in their lives."

> *"Security is a business enabler and a competitive differentiator for C6 Bank."*
>
> **Jose Luiz Santana**
> CISO
> C6 Bank

C6 Bank is a recognized leader for its security program

Santana says the bank is totally cloud-first. From the bank's inception, the founders placed a high priority on security. "We view security as one of the most important pillars for our company," says Santana. "It's a business enabler and a competitive advantage for us. From the CEO on down, everyone embraces the principles of security."

Santana brought a background in both technology and financial services as part of the founding team. Over the years, he has built what is widely recognized as one of the most talented and skilled teams of security experts in Brazil. "We have set expectations, not only within the bank but in the broader Brazilian business community, that our security team is a leader in the ideas and projects that we bring forth in cybersecurity."

Everton Souza concurs. Souza is the Global Security Director of C6 Bank's systems integration partner, Oplium. "C6 Bank has the highest level of cybersecurity maturity," says Souza. "Many companies – not just in financial services but all industries – see C6 Bank as the trend-setter in terms of their security program and the tools they use."

Partnering with Orca Security to improve cloud security outcomes

Santana went to the RSA Conference and met with Avi Shua, Chief Innovation Officer and Co-Founder of Orca Security, in the exhibit hall, where they discussed Orca's vision for cloud security. Santana learned what the Orca tool can do now and what is planned for the future. "That sold me," he says.

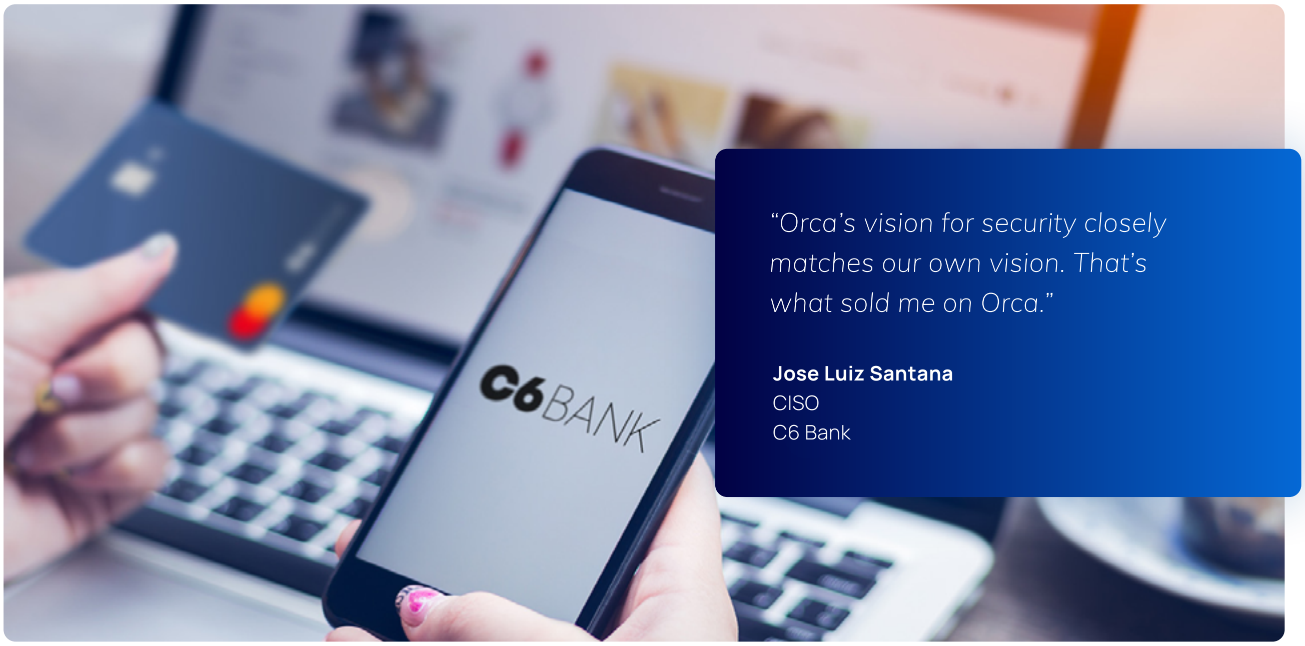
"I bought into the vision of what Orca will do in the future. Of course, what the tool does now is pretty cool, too. It's very similar to what I want and how I think that security controls in the cloud environment should be."

Orca is integral to securing Infrastructure-as-Code (IaC)

What he likes about Orca is what can be done with metadata. "It's the ability to use all the metadata of the cloud provider to build your controls and to give you insights to prevent and detect threats," says Santana. "C6 Bank built the cloud environment using Infrastructure-as-Code, so every security engineer we hire has to know how to code. It's not the development environment; it's all the infrastructure environment, but I want to merge the two things because that's what cloud enables you to do."

His team has not implemented Orca's capabilities as part of their build and deploy or development pipeline yet, but that is the goal. "Today we have Orca working alongside our development pipeline," says Santana. "We're setting up automation to get the approval from the security group, which is built on my code repository. Someone submits a security group rule by a pull request and a security team member approves that pull request because it's just code. That's the mindset here."

Santana says that Orca has the same approach. "I can do everything about security with the information from Orca because it's all about infrastructure as it relates to code. It's a level of abstraction that the cloud provides. And this is cool because I'm planning for Orca to provide my vulnerability assessment too. Orca provides guidance on how to enable remediation, as well as monitoring and threat hunting. The information is all there in a single platform."



"Orca's vision for security closely matches our own vision. That's what sold me on Orca."

Jose Luiz Santana
CISO
C6 Bank

The value of the Orca Platform is in its versatility

The Orca Platform fulfills C6 Bank's need for a variety of security functions. "The versatility of the tool increases the return on our investment," Santana explains. "Something could be a threat, and Orca maps it to the MITRE ATT&CK Framework to ease identifying where the threat is, and at what level and at what stage, so that we can prioritize what to solve first. We view Orca as cloud security posture management, cloud workload protection, vulnerability assessment management, and incident response in a single solution. As a CISO, I'm happy to get so much out of one tool."

C6 Bank also uses Orca to demonstrate compliance with a variety of regulations. As a financial services company, the bank must satisfy both Brazilian and U.S. regulators. "We have to provide information to FINRA and other federal regulators, and Orca eases the collection of information and reporting," says Santana.

Oplium's Souza adds that Orca helps his team see the real situation of the health of cloud security. "We can get to so many different points inside the C6 Bank cloud to see, for example, problems with the paths, or with a suspicious comportment."

About Orca Security

Orca Security is the industry-leading Cloud Security Platform that provides complete coverage and centralized context of your entire cloud estate, enabling security practitioners to spend less time correlating long lists of disconnected alert and focus on remediating the actual risks that have the most impact on the business. Founded in 2019, Orca is trusted by hundreds of customers globally.

orca SECURITY

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

Insurance Innovator Lemonade Goes from 0 to 100% Cloud Visibility with Orca Security

INDUSTRY
Insurance

CHAMPION
Jonathan Jaffe, CISO

CLOUD ENVIRONMENT
AWS

> *"Orca is without a doubt the most important cloud security product we've got. It's hard to overstate the importance of having a digestible source of information that doesn't overwhelm you or inspire loathing."*

Jonathan Jaffe
Chief Information Security Officer
Lemonade

Cloud Security Challenges

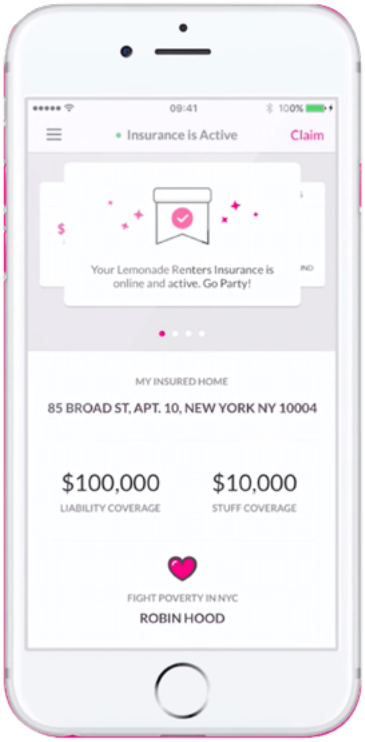
- ✗ Get complete visibility for the entire cloud estate
- ✗ Quickly prioritize important issues into "digestible bites"
- ✗ Minimize the impact on DevOps

Cloud Security Results

- ✓ 100% coverage of cloud accounts with full visibility and prioritized remediation all with zero impact to DevOps and the production environment
- ✓ Able to meet compliance mandates and demonstrate controls to auditors
- ✓ Orca dashboard shows actionable insights of prioritized issues
- ✓ Peace of mind that there are no gaps in coverage

Lemonade is Revolutionizing the Insurance Market

Lemonade provides insurance in the US and Europe. It's part of the "insurtech" market, whereby insurance providers use advanced technology to offer innovative products and services that traditional entities can't match. As a relatively young company, Lemonade has a cloud-native technology stack that lets it operate 100% online. This makes Lemonade an agile competitor in the insurance market. For example, Lemonade delivers policy quotes by an artificial intelligence bot over the web and through its mobile apps. At the same time, Lemonade is A-rated, fully regulated, and reinsured by the most trusted names in insurance.



Your Lemonade Renters Insurance is online and active. Go Party!

MY INSURED HOME

85 BROAD ST, APT. 10, NEW YORK NY 10004

$100,000 LIABILITY COVERAGE

$10,000 STUFF COVERAGE

FIGHT POVERTY IN NYC

ROBIN HOOD

CISO's Prior Orca Experience Leads the Way

Lemonade's infrastructure is entirely in the AWS cloud, where it can be a challenge to get real-time insights about vulnerabilities and security risks. Even Amazon's native tools don't provide all the information that security and DevOps practitioners need.

Jonathan Jaffe joined Lemonade as its CISO in 2020. He immediately sought to get complete visibility for the entire cloud estate to better assess security risks. "When I came on board, there wasn't an adequate solution in place telling me about our vulnerabilities," he says. "I wanted much more visibility into cloud vulnerability issues than what we had."

Orca Beats Agent-Based Competitors Lacework and Palo Alto Prisma Cloud

"We assessed Orca Security, as well as Palo Alto Prisma Cloud, and Lacework," says Jaffe. "At my last company, we used Lacework for over a year. In the last four months of my time there, we also ran Orca in a PoC, so it was easy to do the Orca comparison side-by-side. And, we evaluated Prisma Cloud, extensively."

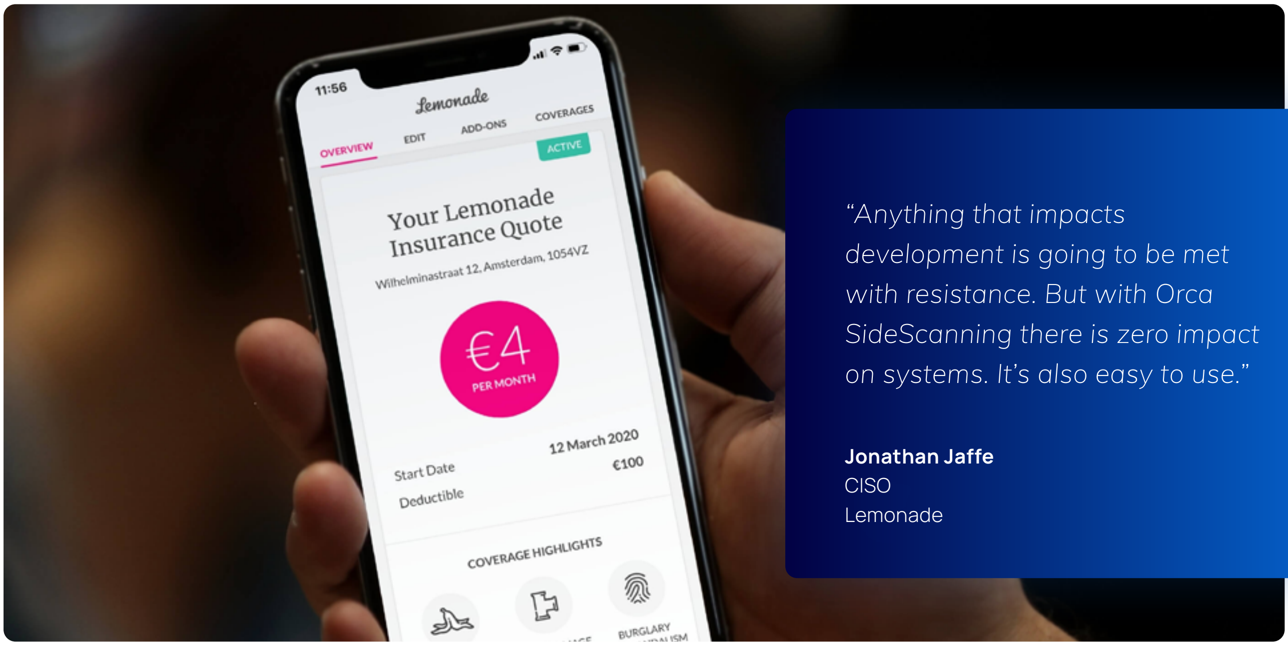
At Lemonade, the evaluation team had to rely on product demos for Prisma Cloud and Lacework, though Jaffe was already intimately familiar with both Orca and Lacework. "Unlike Orca, the others require agents. DevOps wasn't excited about installing and maintaining agents. DevOps also feared the performance hit agents could have on our systems, especially production. And, based on my prior experiences with Lacework, I knew I'd be fighting with missing visibility because of missing agents." Orca took half an hour to set up and fully deploy for the PoC. "It was nothing to get it going," Jaffe says. "We saw results immediately. In under 24 hours, we could see all the resources and the environment in all of our AWS accounts. Moreover, we could quickly and easily see the issues that Orca found, which, fortunately, were small and manageable.

100% Coverage and Prioritization of Security Issues

Jaffe sought several important features in a security solution. "The first is 100% coverage, which is something we'd never get from anything that requires agents to be installed. I have to feel comfortable that we don't have gaps in coverage."

Another must-have feature is the ability to prioritize what needs fixing. "Lacework provides loads of information, but we didn't find it useful; To the contrary, we found it impaired our ability to remediate issues. Having too much diluted the value of the few gems it might have surfaced. Moreover, it doesn't prioritize information in a useful way. When we used Lacework, our security analyst spent most of his time struggling to understand which problems he should spend his time to solve. If he could get past this problem and choose an issue to chase, he'd run into the next problem: was there really an intrusion, or is it yet another false positive?—All of this had to occur before he could get to remediation. Before Orca, we'd give up seeing an issue to resolution because the information was organized so poorly.

"Orca is the opposite. With the information presented in a matrix, we can look at it by threat type, vulnerability, account, affected resource, and so on. We can view the top five items by categories, such as neglected assets or vulnerabilities.



> *"Anything that impacts development is going to be met with resistance. But with Orca SideScanning there is zero impact on systems. It's also easy to use."*
>
> **Jonathan Jaffe**
> CISO
> Lemonade

This puts problems into small bites we can chew through, one at a time. instead of being overwhelmed, which is how many other products make you feel. We can quickly address prioritized issues, putting off or altogether dismissing those of lesser importance.”

For Jaffe and his team, the Orca dashboard provides a calming effect because it doesn’t overwhelm them by providing too much information. He says, “Orca’s real value is in covering a huge amount of my cloud security, notifying us about vulnerabilities and—by a highly reduced degree—actual threats.”

Evidence of Controls for Audits

With its headquarters being in New York, that state’s Department of Financial Services (NYDFS) regulates Lemonade’s business. In addition, the company is subject to various EU regulations and has its own SOC 2 audits. Orca’s reports help Jaffe provide evidence for controls for the various regulations and audits. “Orca has helped reduce my audit effort; for example, I can run reports that show we maintain least privilege controls and that we use multi-factor authentication.”

Orca also alerts Jaffe if there are potential data loss issues or if personal data is exposed in risky areas. The Lemonade team can remediate such issues long before they become a problem that would show up in audit reports. “Orca is great at detecting potential exposure of credit card data, email addresses, and social security numbers or other national IDs,” says Jaffe. “These are priority issues that we can quickly remediate.”

> *“Orca alleviates our number one pain: where are our cloud-related security risks? Before Orca, we simply didn’t have the visibility I needed.”*
>
> **Jonathan Jaffe**
> Chief Information Security Officer
> Lemonade

Lemonade

Renters Policy Declarations

POLICY NUMBER	START DATE	EXP. DATE
1234	Jun 06, 2018	Jun 06, 2019

NAME	ADDRESS
John Doe	123 Main St, Portland, OR 1234

COVERAGE SUMMARY

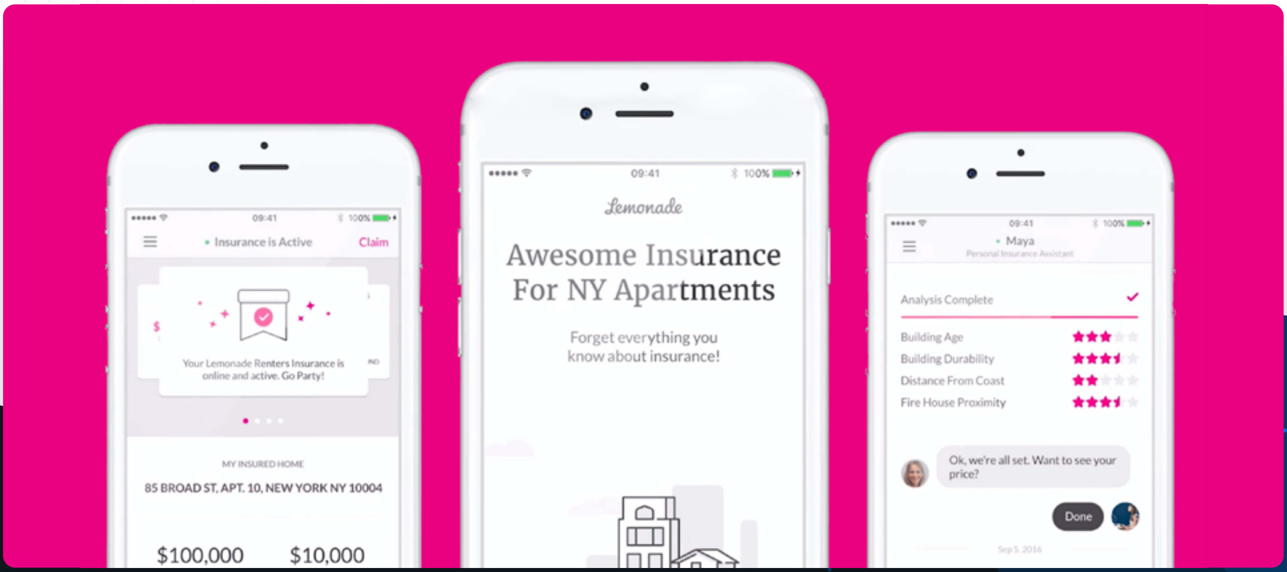
Personal Property	$10,000
Loss Of Use	$3,000

At-Risk Items Have Been Vastly Reduced

Lemonade has significantly reduced its at-risk items. "We cut them down to one-sixth of what they were, and now we can keep that under control by monitoring them," says Jaffe. "Orca lets us shine a light on things so we know what to fix and what we don't have to worry about."

What Jaffe likes most about Orca is the way it lists prioritized issues. "You can see the top five items by categories, such as neglected assets or vulnerabilities. That puts problems into digestible amounts so we can chew through them one at a time, instead of being overwhelmed, like a lot of other products make you feel."

He also loves the interface, stating that the dashboard provides a calming effect because it doesn't overwhelm him by providing too much information. Jaffe says, "Orca's real value is in covering a huge amount of my cloud security—notifying me about vulnerabilities, and to a lesser degree, actual threats."


Insurance is Active
Claim
Your Lemonade Renters Insurance is online and active. Go Party!
MY INSURED HOME
85 BROAD ST, APT. 10, NEW YORK NY 10004
$100,000
$10,000
Lemonade
Awesome Insurance For NY Apartments
Forget everything you know about insurance!
Maya
Personal Insurance Assistant
Analysis Complete
Building Age
Building Durability
Distance From Coast
Fire House Proximity
Ok, we're all set. Want to see your price?
Done
Sep 5, 2016

About Orca Security

Orca Security is the industry-leading Cloud Security Platform that provides complete coverage and centralized context of your entire cloud estate, enabling security practitioners to spend less time correlating long lists of disconnected alert and focus on remediating the actual risks that have the most impact on the business. Founded in 2019, Orca is trusted by hundreds of customers globally.

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

Paidy Turns to Orca Security for Multi-Cloud Visibility, Saves Two FTEs and $500,000/Year in Cloud Security Management Costs

INDUSTRY
Financial Services

CHAMPION
Jeremy Turner, Senior Cloud Security Engineer

CLOUD ENVIRONMENT
AWS, Azure, GCP

> *"We have 12 AWS accounts. We didn't know what's in all of them, so we plugged them into Orca. Within 30 minutes we had a good idea of what was running in all accounts. We couldn't have done that so quickly any other way."*

Jeremy Turner
Senior Cloud Security Engineer
Paidy

Cloud Security Challenges

- ✗ Hundreds of developers pushing microservices into dozens of accounts across multiple clouds make it difficult to track and secure every asset in the company's cloud estate
- ✗ Cost to build a solution on their own would be a minimum of two FTEs for a year, then $500,000 annually to maintain
- ✗ Looking to proactively protect PII, and comply with Japanese regulations such as the Cross-Border Privacy Regulation and Personal Information Protection Law

Cloud Security Results

- ✓ Took thirty minutes to start gaining visibility into its cloud estate; plugged twelve AWS accounts into Orca Security which identified an "imminent compromise"
- ✓ Saving $500,000 a year in tedious cloud security work
- ✓ Can prove to auditors it has the capability to identify and protect PII
- ✓ Faster onboarding of merchants drives revenue increase

Paidy – a Japanese Financial Institution in the Cloud

Paidy is a Fintech leader in delivering cardless payments and other financial services to the Japanese mass market and businesses. Its solutions are at the forefront of revolutionizing online and mobile payments, P2P transfers, personal finance, and merchant settlement. Paidy enables customers to check out using only their email address and a mobile phone number. No credit card or preregistration is needed. To prevent fraud, every transaction is authenticated using a PIN over SMS. Customers can shop now and pay one consolidated bill the following month.

Paidy's entire platform runs in the cloud—primarily across multiple AWS accounts, but also Azure and GCP. It has multiple test and development environments. With the platform processing financial transactions, security is of the highest concern. CISO Felix Beatty is responsible for optimizing Paidy's overall security posture.

"We are essentially a financial institution in the cloud," says Beatty. "Because we've grown so rapidly—having gained more than three million customers in under a year—there are areas of our business where we can improve; one of them is cloud security. Most of our services run in the cloud today, so we need cloud security solutions that immediately surface critical issues so we can resolve them quickly."

> *"An agent may or may not work on this Linux kernel, and the same is true for versions of Windows. There are just so many variables that come into play. After years of dealing with agents, then seeing how easy it is to install and use Orca, I knew that its agentless approach was both a major innovation and a game changer."*
>
> **Jeremy Turner**
> Senior Cloud Security Engineer, Paidy

Paidy's Large-Scale Cloud Environment Makes Total Visibility a Challenge

Gaining visibility into everything on the Paidy platform is one of his top challenges. "We have a large and complex cloud environment; it's difficult to manage all these dynamic assets," Beatty says. "We have hundreds of developers trying to push microservices as fast as possible into the cloud, spinning instances up and down, creating backups, creating S3 buckets, and moving so fast that it's very difficult to know at any given moment what we have. We need to know, 'What is the current security posture of all of our cloud assets?'"

Jeremy Turner, Senior Cloud Security Engineer, is his right-hand man in securing the cloud environment. The two have been a team since before joining Paidy and know how to approach its security challenge.

Security Agents are Great—If and When They Work (Usually They Don't)

"I've been doing this a long time," says Turner. " I've learned that anything dealing with security and vulnerability usually requires installing some type of agent. If you've worked in infosec for a while, you know that agents break, they need to be updated, and they could be vectors for other security vulnerabilities."

Turner admits that agents are great—if and when they work. "Usually they don't. There are so many dependencies and other things to think about. An agent may or may not work on this Linux kernel, and the same is true for versions of Windows. There are just so many variables that come into play. After years of dealing with agents, then seeing how easy it is to install and use Orca, I knew that its agentless approach was both a major innovation and a game changer," says Turner.

Legacy Vulnerability Scanners and AWS Tools Were Unfit

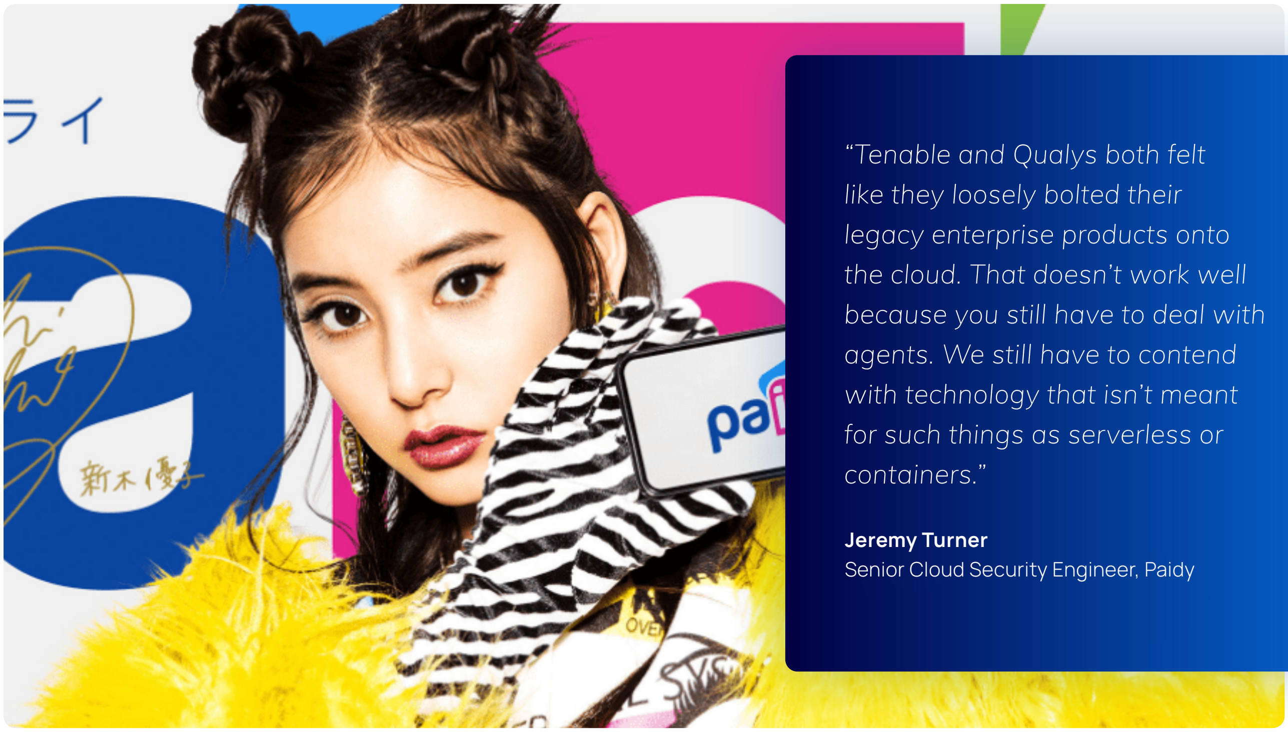
The Paidy security team had experience with a variety of legacy tools adapted for the cloud. Turner says, "I've used Trend Micro, Qualys, and Tenable, either in an enterprise environment or in testing. Tenable and Qualys both felt like they loosely bolted their legacy enterprise products onto the cloud. That doesn't work well because you still have to deal with agents. We still have to contend with technology that isn't meant for such things as serverless or containers."

Paidy also ruled out using network scanners. According to Turner, "Having experience with non-authenticated scanners, I knew they had limited visibility and can create downtime.

"Authenticated scanners might provide you with more vulnerability data, but still require lots of work to configure, as well as elevated privileges. This opens your enterprise up to risk because you essentially have another shared account and password."

Cloud providers such as Amazon do provide security scanning tools. "Amazon's AWS Inspector, a vulnerability scanner, requires an agent. Usually it's baked into the Amazon AMI, but it only works with certain AMIs," he continues. "AWS GuardDuty ticks the box for a vulnerability scan and compliance check. But reporting is its biggest issue; using the data can be a challenge. It just pops out a list of vulnerabilities, then it's up to us to figure out what to do about them."

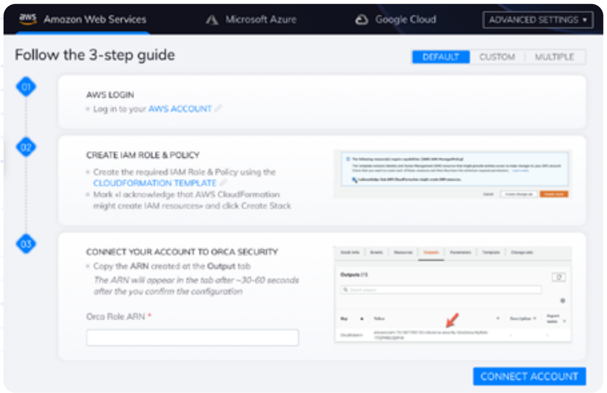
Beatty adds, "Because we have multiple AWS accounts and are multi-cloud, it was difficult to have a single view where we could monitor everything that is happening. Multi-cloud visibility was our



"Tenable and Qualys both felt like they loosely bolted their legacy enterprise products onto the cloud. That doesn't work well because you still have to deal with agents. We still have to contend with technology that isn't meant for such things as serverless or containers."

Jeremy Turner
Senior Cloud Security Engineer, Paidy

number one issue. Secondarily, we don't have the time and resources to orchestrate a tool using, for example, AWS services or something similar. We want to use a service that doesn't require any agent—where we don't need to regularly update it and it simply works." For Paidy, Orca Security meets all of those needs and more.



Follow the 3-step guide

01 AWS LOGIN
- Log in to your AWS ACCOUNT

02 CREATE IAM ROLE & POLICY
- Create the required IAM Role & Policy using the CLOUDFORMATION TEMPLATE
- Mark «I acknowledge that AWS CloudFormation might create IAM resources» and click Create Stack

03 CONNECT YOUR ACCOUNT TO ORCA SECURITY
- Copy the ARN created at the **Output** tab
  The ARN will appear in the tab after ~30-60 seconds after the you confirm the configuration

Orca Role ARN *

Orca SideScanning™ Provides Much-Needed Visibility

The Orca Security platform is vastly different from other security tools. Delivered as SaaS, it reads cloud block storage out-of-band, from the side—hence the term SideScanning™. No code runs within a customer's cloud environment. Instead, Orca builds a read-only model of their cloud environment, which it then scans to assess potential security issues.

Having full visibility is what Turner appreciates most. "Visibility is a problem every organization has. Orca almost immediately gave us both wide and deep visibility into our threat landscape," says Turner. "When we take that data and show it to folks, their eyes open. We had an instance where Orca revealed an 'imminent compromise' of a system that's been floating in a test environment for probably two or three years.

The system was running a totally outdated OS. Once Orca identified it, we created a ticket for an engineer to immediately address. We were fortunate to capture the vulnerability before the system went into UAT and production."

Beatty agrees on the value of visibility: "There's no excuse for overlooking problems when they're presented right there for you. When the Orca dashboard displays 'imminent compromise,' it doesn't get any clearer than that."

Orca also helps Paidy with account sprawl issues. "We run 12 AWS accounts," says Turner. "We didn't know what's in them all, so we plugged them into Orca. Within 30 minutes we had insight as to what was running in all accounts. We couldn't have done that so quickly any other way."

Asset management is another function Orca Security provides to Paidy. Orca provides an inventory of each asset's location, metadata, and a vulnerability list. "It's pretty cool when I can pick an instance and see who's logged into it, how many failed login attempts there are, or what packages are installed on it. I appreciate being able to do that without depending on an agent for every instance," says Turner.

Orca Security Identifies and Protects PII, Easing Paidy's Compliance Efforts

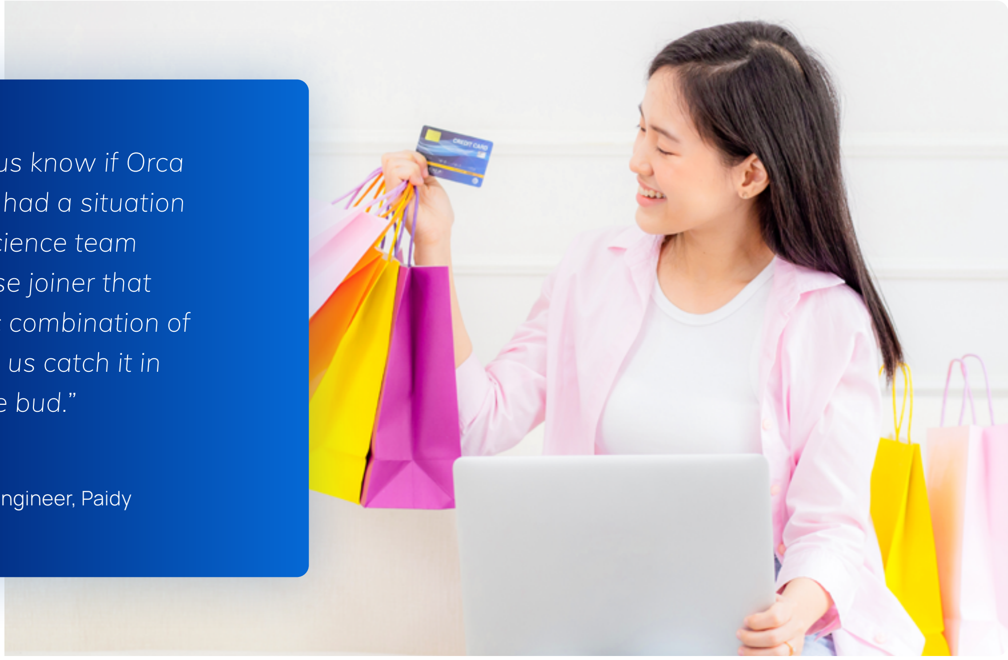
As Paidy gains more experience with the Orca Security platform, its team finds more ways to use the data it generates. "As a Fintech company, we're very mindful of toxic combinations of data—Orca helps us with this," says Turner. "For example, customers must provide their cellphone number to use our service. But if we're dealing with home or email addresses combined with possible bank account information and purchase history, then we get into PII issues and Japanese data privacy regulations."

Turner explains how Orca helps protect PII. "One feature lets us know if Orca suspects PII. It's like a beacon telling us, 'This server contains email addresses that don't belong to paidy.com. What's going on?' We can then investigate. Right now the tool doesn't say, 'Here's a toxic combination of data' but it does show us where to hunt. We had a situation where the data science team created a database joiner that led to such a toxic combination of data. Orca helped us catch it in time to nip it in the bud."

Paidy must comply with a number of data privacy laws. Japan's Cross-Border Privacy Regulation is similar to the EU's GDPR, and the country's Personal Information Protection Law was enacted in 2004. Orca helps prove to auditors that Paidy is fully capable of identifying and encrypting personal information. Paidy rests easy knowing it has the capability to scan for vulnerable PII.

Turner uses Orca Security's integration with Jira to open tickets. In turn these trigger workflows so people and processes can take appropriate actions; for example, to encrypt sensitive data or to remediate other issues that Orca finds.

> *"One feature lets us know if Orca suspects PII... We had a situation where the data science team created a database joiner that led to such a toxic combination of data. Orca helped us catch it in time to nip it in the bud."*
>
> **Jeremy Turner**
> Senior Cloud Security Engineer, Paidy



Orca Increases Paidy Revenue by Accelerating Merchant Onboarding

Orca helps Paidy onboard more merchants, thereby increasing its revenue. “Typically merchants want to do a third-party security review of us,” says Beatty. “Orca makes it easier for us to show that we’re scanning for vulnerabilities and mitigating as appropriate. This puts merchants at ease about our security posture and helps establish trust with them.

Beatty considers what it would cost if his team had to integrate and customize multiple legacy solutions to get visibility into their environment. Paidy estimated it would require two FTEs and half a million dollars per year to spin up and manage such a solution—a cost considerably higher than the Orca service that is fully managed and maintained on its behalf.

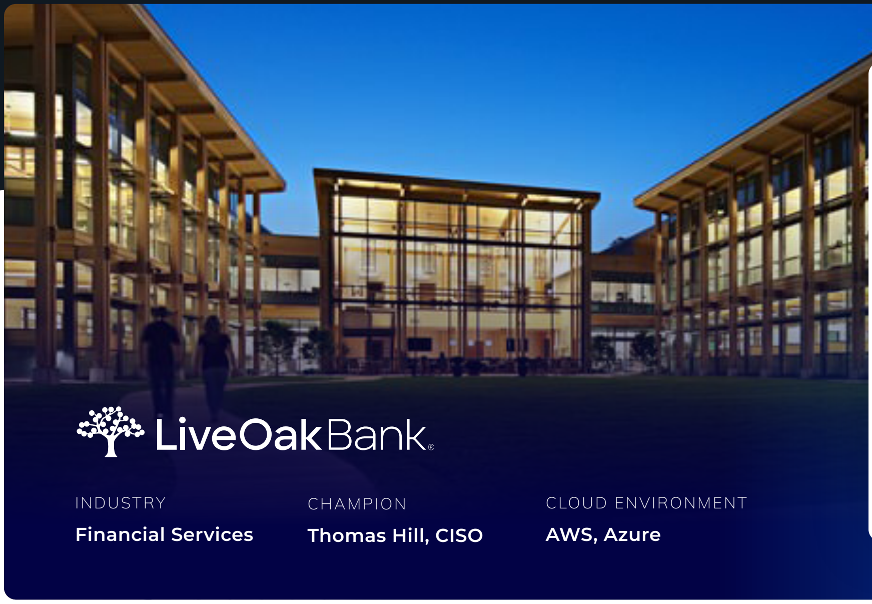
“When I talk to colleagues about Orca, I tell them it gives us insight across all our cloud environments—not only AWS, but also Azure and GCP. The more accounts we have, the more value we get because now we know what our people are running,” says Beatty.

About Orca Security

Orca Security is the industry-leading Cloud Security Platform that provides complete coverage and centralized context of your entire cloud estate, enabling security practitioners to spend less time correlating long lists of disconnected alert and focus on remediating the actual risks that have the most impact on the business. Founded in 2019, Orca is trusted by hundreds of customers globally.

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

Orca Security Helps Live Oak Bank Innovate While Facilitating Compliance with Data Privacy and Security Mandates



LiveOakBank.

INDUSTRY
Financial Services

CHAMPION
Thomas Hill, CISO

CLOUD ENVIRONMENT
AWS, Azure

> *"Orca is a great solution for us because we want to give developers the power to be innovative, but need to scan close to real-time without impacting the operations."*

Thomas Hill
Chief Information Security Officer
Live Oak Bank

Cloud Security Challenges

- ✗ Wants to perform security assessments as close to real-time as possible
- ✗ Needs to protect the cloud environment without constraining developers or getting contentious with IT
- ✗ Must meet FDIC compliance requirements for cloud security

Cloud Security Results

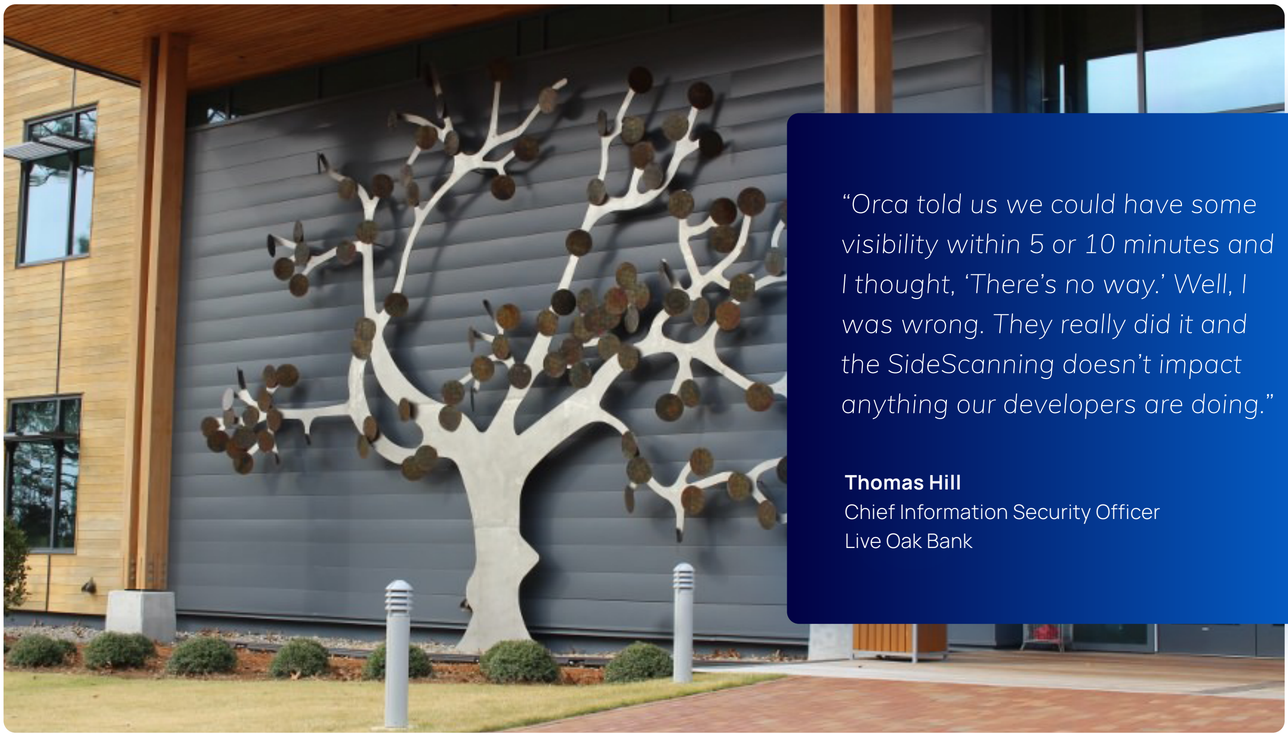
- ✓ Can now get full visibility of risks and vulnerabilities in near realtime
- ✓ Can support DevOps procedures without interrupting operational and production access, and without installation of agents
- ✓ Positioned to fully support FDIC guidelines and future requirements for cybersecurity in the cloud

Live Oak Bank's Homegrown Technology is a Big Differentiator

Live Oak Bank is different from most banks in many respects. Started as an internet bank, Live Oak continues to operate without physical locations. The company is focused on small businesses and has domain expertise in 20+ specific verticals—such as veterinary practices, pharmacies, agriculture, healthcare, and other industries. Unlike its competitors, Live Oak bankers get deeply involved in helping customers run—and succeed in—their own businesses. Its partnership approach has resulted in a loan default rate of less than 1%—far below the industry average of 3%.

The company has embraced the cloud from the beginning. Rather than build its business on a traditional, datacenter-based banking platform, Live Oak developed its own software. Some of the company's technology has been spun off into new software entities. Many of these fintech companies are still partnered with Live Oak Bank to create an in-the-cloud, API-driven core. Cloud technology is central to everything Live Oak does.

Thomas Hill joined Live Oak Bank six years ago as CIO. As the company grew and its homegrown technology portfolio expanded, there became a need to separate IT and security roles, so Hill assumed the CISO position. "We want our business to be fast, real-time. We want the business to be able to move and change at the speed of light," says Hill. "My job is to make sure we can do that securely and within the bounds of all regulatory constraints."



> *"Orca told us we could have some visibility within 5 or 10 minutes and I thought, 'There's no way.' Well, I was wrong. They really did it and the SideScanning doesn't impact anything our developers are doing."*
>
> **Thomas Hill**
> Chief Information Security Officer
> Live Oak Bank

Empowering DevOps (Without Getting in the Way)

Steeped in the heritage of a company that creates its own software, the DevOps team is encouraged to be bold and innovative. A traditional security leader can hamper DevOps by imposing demands on them to slow down and consider security every step of the way. But Hill refuses to be an impediment to the development team. “The last thing we want to do is constrain our developers,” he says. “We want them to think outside the box and create new things, so we give them the power to spin up what they need, but in a responsible way.”

“In the old days—and I literally mean three months ago—we were scanning our environment once a month,” according to Hill. “In the back of my mind, I worried about a developer spinning off a script that builds a whole environment, builds a new stack, and they start testing things. They could be one misconfiguration away from putting all that out on the internet. We need to detect that but scanning once a month wasn’t going to do it. When you work in real-time, you need to see everything in real-time.”

This is where Orca comes into play. “We want to be able to see our whole environment—not just the devices that have an IP address, that might be accessible, and that we know about,” says Hill. “Orca is a great solution for us because we want to give developers the power to be innovative, but need to scan close to real-time without impacting the operations.”

“The IT infrastructure team is happy, too, because we’re taking a view of the total environment, setting it aside, and doing the scanning completely offline. We aren’t asking them to do anything —like install agents—to support this process,” says Hill.

Orca Does the Work of Several Tools in the Security Toolbox

Hill’s team did a PoC with Orca and knew within days how useful it would be. The visibility it gives the security team is unlike anything other tools can provide—even those with agents installed on devices. “I can’t understate the importance of getting visibility of the whole cloud in an offline fashion so as not to interrupt any operational and production access. Orca’s SideScanning™ method is truly innovative,” says Hill. “It takes away any friction with our IT group.”

Live Oak had been using traditional industry leading vulnerability scanners for cloud assessments. Hill sees that Orca does a more complete job of scanning the cloud assets without the need for cumbersome agents. “The best practice for running agent-based tools is monthly. I’m not comfortable going that long between scans,” says Hill. With Orca, he can run it daily without any impact on production.

> *“The most important thing for a security person is to know what is there in order to extend the right controls to the right environment. Orca gives us that full visibility so we know where to focus our energy.”*
>
> **Thomas Hill**
> Chief Information Security Officer
> Live Oak Bank

Orca Facilitates Compliance with Federal Regulations for Financial Institutions

Live Oak Bank has a sprawling AWS estate. Hill says they have over a dozen orgs—each being its own AWS mini-datacenter. In addition, the bank has fintech partners that use both AWS and Azure, with Live Oak's systems interconnecting them.

As a chartered bank, Live Oak must comply with data privacy and security regulations. Here, the FDIC, as a member of the Federal Financial Institutions Examination Council (FFIEC), issued a statement addressing the use of cloud computing services and security risk management principles in the financial services sector. "The FDIC statement letter is just guidance today, but we expect it to become a requirement soon," says Hill. "Orca helps us convey the security posture of our cloud environments, which is extremely important for us as a bank. Our corporate risk group finds it very advantageous to have a tool like Orca to meet this need."

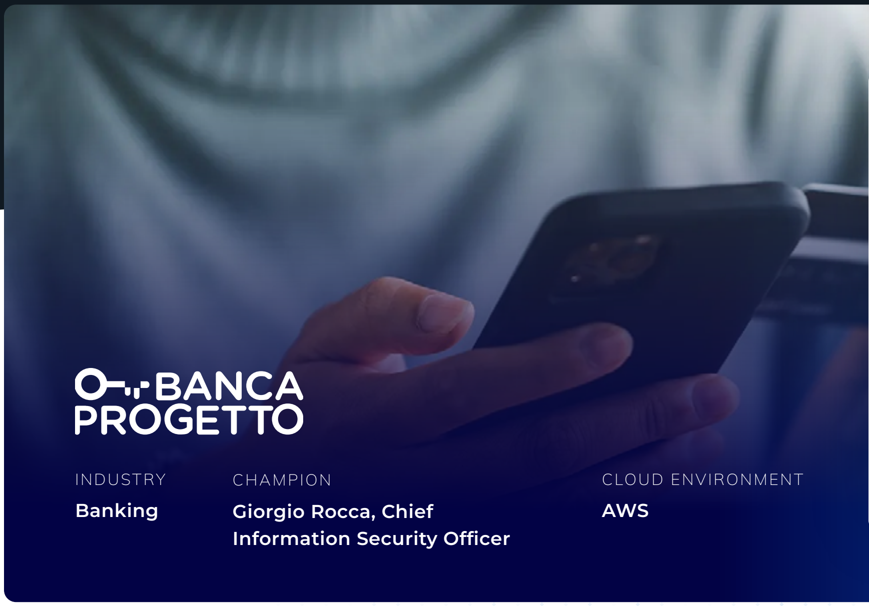
Due to regulatory requirements governing financial data, Live Oak uses a hybrid-SaaS version of Orca Security, called Orca Pod. It permits the bank to keep its data in its own environment while only transferring metadata to Orca.

About Orca Security

Orca Security is the industry-leading Cloud Security Platform that provides complete coverage and centralized context of your entire cloud estate, enabling security practitioners to spend less time correlating long lists of disconnected alert and focus on remediating the actual risks that have the most impact on the business. Founded in 2019, Orca is trusted by hundreds of customers globally.

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

Orca Enables Security Evolution for Banca Progetto, the First Italian Bank on AWS



BANCA PROGETTO

INDUSTRY
Banking

CHAMPION
Giorgio Rocca, Chief Information Security Officer

CLOUD ENVIRONMENT
AWS

> *"I tell my peers in the banking industry to try Orca. If they try it, they will surely keep it."*

Giorgio Rocca
Chief Information Security Officer

Cloud Security Challenges

- ✗ Need to monitor the security aspects of a complex cloud environment and identify vulnerabilities to the SOC for remediation
- ✗ Need to measure adherence to various security frameworks
- ✗ Need to support development efforts to catch issues before they go into the production environment

Cloud Security Results

- ✓ Orca integrates the security of the cloud environment with the classic SOC
- ✓ Orca's compliance reports identify key risk indicators and measure progress against security frameworks
- ✓ Massive cost savings because there are no integration costs, no need for six FTEs to find and prioritize risk, and Orca's pay-as-you-go licensing model only applied to assets actually in use

Banca Progetto Is Italy's First Bank to Operate Fully on AWS

Banca Progetto S.p.A., a fast-growing Italian challenger bank, born in 2015 from the reorganization of Banca Popolare Lecchese carried on by the Californian fund Oaktree, provides financing to households and corporates also through the digital channel. With branches in Milan and Rome and a commercial network operating through the whole country, Banca Progetto is specialized in products for small and medium-sized Italian companies and retail customers, in particular savings accounts products targeting private and retail customers.

Ever since, the bank has been undergoing a complete transformation of its business and operations. Today, the company has four primary business channels: lending to small and medium businesses in Italy as well as tax credits factoring and instant cash to PMI actual customers, savings accounts products such as deposit account and time deposit and in its most recent development, instant lending to non-customers retail clients.

In 2019, Banca Progetto started its cloud journey to unlock the full potential of its banking products. With the approval of the Italian regulator, Banca d'Italia, Banca Progetto worked closely with Amazon Web Services to deliver the best decoupling infrastructure and create a compliant ecosystem. By 2020, Banca Progetto had become the first Italian bank to operate fully in the cloud.

Among other key milestones for the bank, in 2020, the custom designed and developed Service Bus was launched on AWS, enabling customers to be onboarded in less than 10 minutes. In 2021, the core product of lending to small/medium enterprises went fully digital, making it possible for teams working across Italy to take advantage of a single platform to manage the entire lending process. The following year, Banca Progetto entered the Instant Lending market with Instant Cash PMI and the Cream application.

All these milestones represent a high rate of technological innovation for the bank. Having migrated all applications and infrastructure into the cloud, while building the new ones straight into it, allows the bank to be more responsive to customers' evolving needs and to quickly launch new products and services.

A Complex Cloud Environment Needs Security Governance

Banca Progetto has a complex yet manageable infrastructure in which the cloud environment developed by the bank itself coexists with various individual third-party environments connected to it. There are multiple accounts involving three regions in which the front ends for customers, the sales network, and the local instances used by the bank's back-office services are distributed. The middleware that enables communication among all components is the nerve center of this cloud environment.

Giorgio Rocca is Banca Progetto's Chief Information Security Officer and leader of the small security team. "Most of our work pertains to the governance of our security program," says Rocca. "We have a SOC and many aspects of our security are outsourced to other players. So, the focus of our work is typically partner monitoring and cloud monitoring."

The priority to monitor and audit all cloud environments is dictated by the cloud-centric nature of the bank's development and growth. This prompted the security team to look for a cloud security posture management (CSPM) solution that could identify existing vulnerabilities and communicate with the bank's SOC to properly monitor the operational scenario in real time. Particular attention was paid in finding a solution that works across multiple cloud providers. While most of the bank's infrastructure and accounts are in AWS, the company does have some back-office services in Azure Cloud, and there's always the potential for additional applications in other cloud environments in the future.

The Bank's Requirements for CSPM

Rocca says his team had a list of requirements for the cloud monitoring solution in addition to the ability to support multi-cloud environments. "We have a cloud native architecture that adds complexity from a security standpoint," he says. "We have virtual machines, containers, and even a serverless architecture for some applications. We need a solution that can scan all these components for vulnerabilities and configuration issues and report them to our SIEM."

The bank also needs to observe compliance with various security frameworks, such as NIST (the U.S. National Institute of Standards and Technology), the MITRE ATT&CK framework, and the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM). Any chosen tool must help the bank determine its compliance posture.

Ease of use was a paramount concern, given that the security team is so small. Some people with governance responsibilities don't have a technical background, so the cloud security tool had to have a simple user experience where all users can get the information needed as easily as possible.

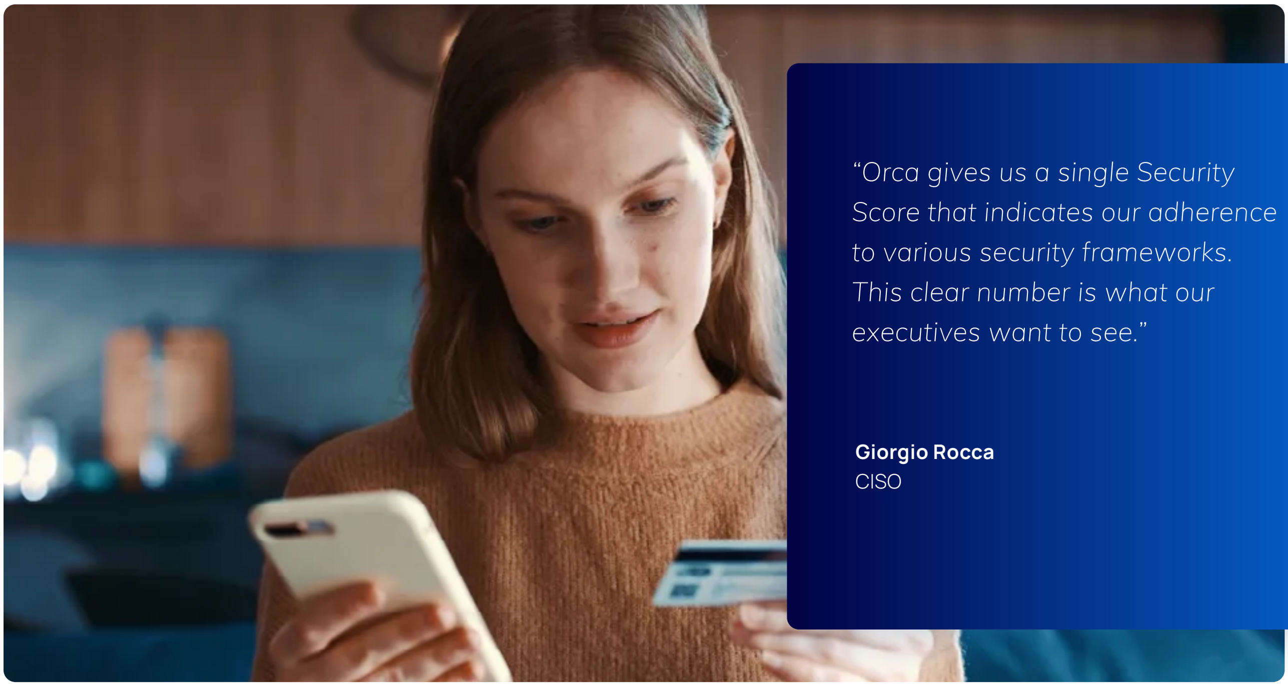
> *"Previous experience with CSPM tools clarified our requirements and processes needed to make the best use of these tools. Orca more than meets the challenge."*
>
> **Giorgio Rocca**
> CISO

The Orca Beats Out Prisma Cloud in a Side-By-Side Comparison

Banca Progetto already had experience with Palo Alto Networks Prisma Cloud. However, the license agreement for Prisma Cloud was expiring, so this seemed like the best time to test the market for other solutions. Mauro Restante of the cyber risk consulting firm Cybersel Group suggested Rocca's team try Orca Security, and so they began a week-long Proof of Concept. They were able to compare Prisma Cloud and the Orca Platform side-by-side.

"The Palo Alto Networks product seems more suited to companies with bigger infrastructure," says Rocca. "The system is quite technical, and the dashboard is harder to manage. Also, it requires the installation of an agent, which increases the friction we have in trying to get our engineers to support it. They don't necessarily want to change their processes to install and maintain agents."

Orca is a much simpler solution in terms of onboarding, licensing, user experience and integration with the bank's SIEM. "It took us just 5 minutes to onboard Orca," says Rocca. "Our architect did it with no external support. This was the first sign that we should adopt Orca. Another important aspect is that it natively integrates with Sumo Logic, our SIEM. The other product requires an API to talk to the SIEM. We'd need specialized architects or a systems integrator to make it work for us."



"Orca gives us a single Security Score that indicates our adherence to various security frameworks. This clear number is what our executives want to see."

Giorgio Rocca
CISO

Other important aspects of Orca sealed the decision to make it the bank's cloud security solution. "In many ways, Prisma Cloud and Orca are similar solutions," explains Rocca. "They both offer compliance reporting, but Orca's reporting is simple and concise for executives and the board to view. On top of this, Orca has MITRE compliance reporting for the totality of cloud infrastructure, applications, data, and identities, and that is an important security framework for us."

Parallel use of both Orca and Prisma Cloud highlighted Orca's greater accuracy in refining the search for critical issues, therefore producing a more meaningful overall security score. Orca has also a considerably simpler and more appealing user experience interface that allows ease of use even by staff who are not strictly technical but who are assigned to governance roles.

> *"Orca makes collaboration possible with IT, Dev and security giving a big value we get from this tool. We are working together to reach our objectives."*
>
> **Giorgio Rocca**
> CISO

Even more important is that Orca is not just a security tool but also a development instrument, allowing the bank's Dev team to "shift left" and build secure applications from the very beginning and not secure them afterwards. "Our Dev team uses Orca to verify the efficiency of updates before release in production, helping to optimize our development process. It is easier to understand the gap that we must remediate or mitigate before production and to secure the bank's infrastructure," says Rocca. "The other solution doesn't have a development integration process, so it is solely for security. By comparison, Orca provides much more value overall."

Orca's licensing approach is also much more attractive than that of Palo Alto Networks. "Orca provides simplicity in its licensing table. You can see what you want to spend or project to spend in the future because the licensing is tied to the virtual machine," says Rocca. "The other solution has a more complicated licensing scheme tied to the individual component, so for example, every new container or every new transit gateway has a price. This is not good when you want to have a strategic view of your company's expenses."

Orca Delivers Results for Banca Progetto

Banca Progetto has been using the Orca Platform for just under a year and the results have been encouraging. It made it possible to integrate the security perimeter of the cloud environment with the classic SOC, thus completing Banca Progetto's digital transformation in the security field. The amount of data in the compliance reports helps to identify specific key risk indicators, calibrated to the numbers provided by Orca, thus enhancing the internal security posture of the cloud environment, and complementing what had already been defined with security rating tools for the external side.

By supporting our architects in the shaping of Banca Progetto's cloud architecture with valuable indications and precise configuration, Orca helped us to optimize the overall environment.

Finally, Orca has helped to facilitate full governance of security aspects by the bank's IT security group, providing valuable feedback on the degree of security achieved.

About Orca Security

Orca Security is the industry-leading Cloud Security Platform that provides complete coverage and centralized context of your entire cloud estate, enabling security practitioners to spend less time correlating long lists of disconnected alert and focus on remediating the actual risks that have the most impact on the business. Founded in 2019, Orca is trusted by hundreds of customers globally.

orca SECURITY

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