HOW 6 FINSERV CISOS *NAILED*

IAAS SECURITY & COMPLIANCE FOR AWS, AZURE & GCP

orca security

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

"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
CISO | 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 real-time
- 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

LiveOakBank

INDUSTRY
Banking

CHAMPION
Thomas Hill
CISO

CLOUD ENVIRONMENT
aws Azure

"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
CISO | Live Oak Bank

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."

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 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
> CISO | Live Oak Bank

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.

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

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 https://orca.security

orca security

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

"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
CISO | 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

INDUSTRY
Insurance

CHAMPION
Jonathan Jaffe
CISO

CLOUD ENVIRONMENT
aws

Lemonade is Revolutionizing the Insurance Market

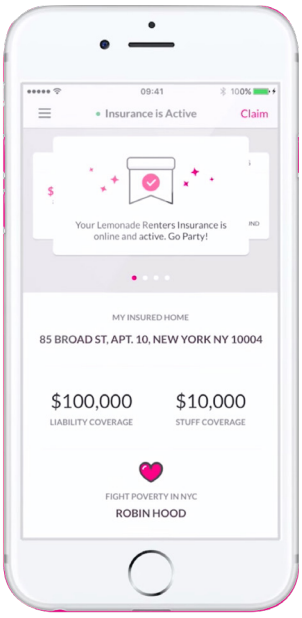
Lemonade provides insurance in the US and Europe. It's part of the "insurtech" market, whereby insurance providers use advanced technology to offer innovative products and services that traditional entities can't match. As a relatively young company, Lemonade has a cloud-native technology stack that 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.

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 Laceworks, 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."

> "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

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. 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."

> "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
> CISO | Lemonade

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."

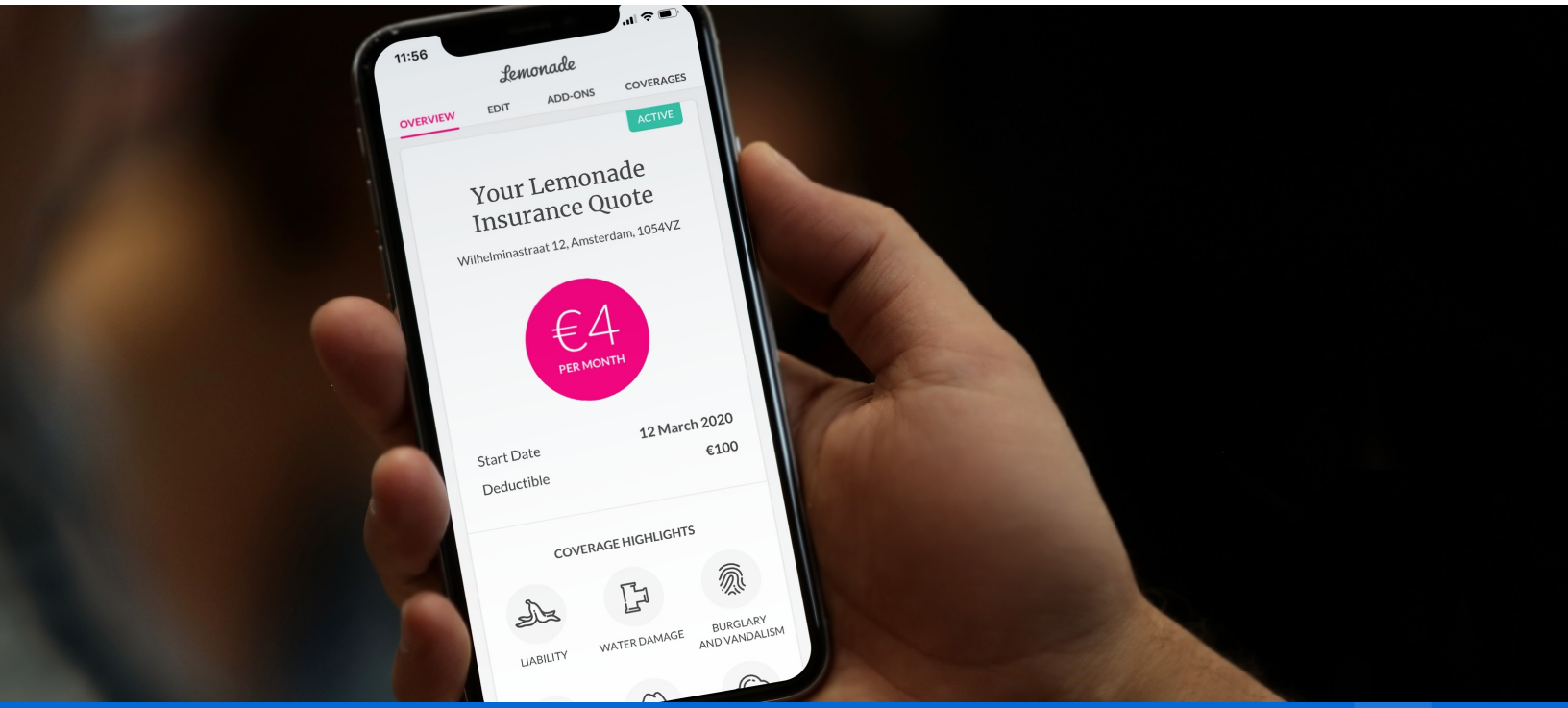
Orca also alerts Jaffe if there are potential data loss issues or if personal data is exposed in risky areas. The Lemonade team can remediate such issues long before they become a problem that would show up in audit reports. "Orca is great at detecting potential exposure of credit card data, email addresses,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

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.”



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 https://orca.security

orca security

Rapyd Uses Orca Security's Deep Cloud Visibility to Protect Global Payments Systems

"Orca is huge for helping us work with DevOps. My sys admin can now show and explain to DevOps what we've found. We're now more collaborative and helpful to them. It's a big step toward DevSecOps—the organizational friction between DevOps and my security team is gone."

Nir Rothenberg
CISO | Rapyd

Cloud Security Challenges

- Get full context visibility to drive prioritized patch management
- Demonstrate good governance and regulatory compliance to auditors
- Simplify security

Cloud Security Results

- Gained immediate and full visibility of its cloud infrastructure
- Integrated Orca with Jira to automate the CI/CD pipeline for security-related tasks
- Created a collaborative environment with DevOps to shift to DevSecOps

Rapyd

INDUSTRY
Financial Services

CHAMPION
Nir Rothenberg
CISO

CLOUD ENVIRONMENT
aws

Rapyd Breaks Down Barriers to Universal Payments

Rapyd is tackling the fragmentation that exists in the global payments industry. It builds the technology that removes the backend complexities of cross-border commerce while providing local payments expertise.

Global ecommerce companies, technology firms, marketplaces, and financial institutions use Rapyd's fintech-as-a-service platform to seamlessly embed localized fintech and payments capabilities into their applications in a simple way. The Rapyd Global Payments Network lets businesses access the world's largest local payment network, which has over 900 locally preferred payment methods. These include bank transfers, e-wallets, and cash in more than 100 countries.

Orca Takes the Pain Out of Patch Management

Every global digital payment system today has to have a relentless focus on security. It's what drives Nir Rothenberg, Rapyd's CISO, who manages IT and security operations. While his company has good security practices in place, proving that to auditors has been a challenge.

"Our business is payments, so we must be PCI DSS compliant—and we are," says Rothenberg. "Each year the auditors want to see we have a good patching process in place. We patch relentlessly, but it's never 100% for various reasons. Having everything documented to show we're on top of this was a real pain point before we found Orca."

Rapyd fully operates in the cloud, with everything on AWS. Rothenberg wanted an intelligent tool to provide full visibility into those servers truly in need of a patch. He sought a prioritized list with everything in context. Many tools can scan and list what needs a patch, but without context the list is long and much of it is meaningless.

"Native AWS tools lack intelligence. An AWS Inspector scan can give us results, but those results don't always fit our context," Rothenberg says. "We'll get a list of a thousand patches, all of them deemed critical. But some can't be deployed because they don't match our distribution, or they're for offline servers where patching

doesn't matter. If I show such a report to an auditor, they would think we're not taking care of business. Say there's a server with a critical vulnerability. There's a patch that works on Ubuntu 18.4, but we have 18.9. So in that context, we can't patch. Not only that, but the server isn't internet-facing, so it's not really important anyway. Orca tells us, 'Critical patch, medium risk.' I can show that to an auditor to justify our actions."

Rothenberg evaluated various AWS tools including GuardDuty, Inspector, and Detective, as well as traditional agent-based security tools and network scanners. He learned that it takes a lot of overhead to make those tools work—too much to approximate what Orca delivers right off the shelf.

"For agent-based tools, we'd have to create servers, deploy an agent, write and run scripts, know our environment, and configure a dashboard to show what we want to see. We'd have to teach it what is and isn't a risk, plus do a lot of the analysis work ourselves. And we'd always be tweaking it because risk is dynamic; it changes. All of those steps are all automatic with Orca."

> "Orca's scans return a meaningful and actionable report that puts everything in context. Besides its findings, it provides peripheral considerations to guide our patch management process."
>
> Nir Rothenberg
> CISO | Rapyd

Orca Identifies Nonconformity to CIS Controls and Risk to PII

Rothenberg oversees Rapyd's adherence to the Center for Internet Security Controls. For this, too, he tried native AWS tools and found them lacking. "We have to figure out for ourselves what their scan results mean. But with Orca, the scan results are all digested and focused. We can immediately see the non-conformity to CIS that we should deal with first. We've integrated Orca with Jira—to assign the work to DevOps, we simply click a button."

Rothenberg says creating tickets is essential for internal task tracking. "Knowing the tasks and associated risks at any moment, we can prioritize what we send to DevOps so they don't get overwhelmed. If we get audited, we can show, 'This is our pipeline, this is our work plan.' It's all in Jira and everything has an audit trail."

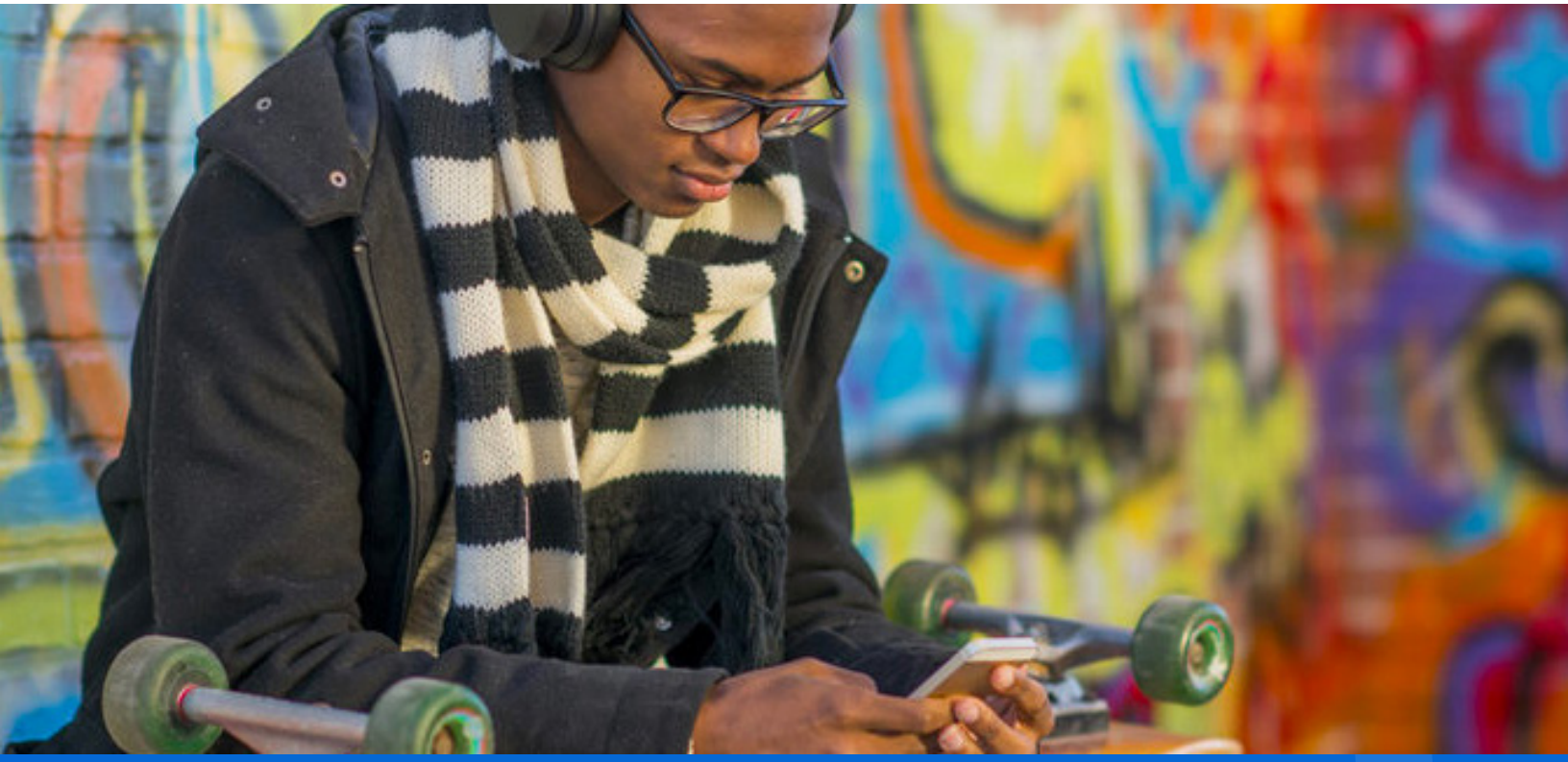
The CISO also looks to Orca to identify situations where PII is at risk in files that might not be properly protected. "As a payments company, we're very sensitive to PII exposure. If a server contains PII, or encryption keys are exposed, Orca picks that up right away and gives us the risks based on that machine and the specific asset. We're able to quickly remediate the occurrence."

In previous years, Rapyd tracked vulnerabilities in Excel spreadsheets. Orca has eliminated that process. "Now everything is automated and has a CI/CD pipeline. The next time we face an audit, I can show our Orca and Jira reports to show the risks we're tracking and what we're doing to remediate them," says Rothenberg. "With how we monitor our assets today, it just becomes very simple to demonstrate patching and compliance."

Simplicity Leads to Better Security

Orca has simplified life for Rothenberg's security team. "Right after we connected Orca to our environment, it immediately found a lot of interesting stuff. Without Orca, we would never have this visibility."

"Orca is huge for helping us work with DevOps," says Rothenberg. "My sys admin can now talk to DevOps eye to eye. He can explain what we've found, he can show them. This helps us become more professional, to see the environment better, to understand it better. Now we are more collaborative with DevOps and more helpful to them. It's a real step toward DevSecOps. Now we're one well-oiled machine. The organizational friction between Security and DevOps is gone."



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 https://orca.security

orca security

Orca Security Takes Zip from 18% Visibility of Risk to 100% Coverage in Less Than a Day

"We went from years' worth of pain to full visibility in a single afternoon. Take it from a guy who is in the trenches—that is profound."

Peter Robinson
Director of Cybersecurity and Business IT | Zip

Cloud Security Challenges

- Rapid expansion of the company is resulting in rapid growth of the cloud estate
- Ephemeral nature of the infrastructure makes it hard to scan for vulnerabilities
- Different environments are run by several people across multiple countries

Cloud Security Results

- 100% coverage of cloud accounts with full visibility, asset inventory, and prioritized remediation—all with zero impact on production environments
- Reduced dependence on DevOps while garnering their full support for prioritized remediations
- 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

INDUSTRY
Financial Services

CHAMPION
Peter Robinson
Director of Cybersecurity and Business IT

CLOUD ENVIRONMENT
aws Azure

Zip Believes in Relentless Innovation

Zip Co is a leading player in the next generation of retail finance and payments industry. The company offers point-of-sale credit and digital payment services to the retail, home, health, automotive, and travel industries. Founded in 2013 and headquartered in Sydney, Australia, Zip has grown rapidly and now has operations across Australia, New Zealand, South Africa, the UK, and the US. Further expansion in North America, Europe, and the Middle East is planned.

Zip's computing platform is entirely digital and hosted in the cloud. The platform leverages big data in its proprietary fraud and credit-decisioning technology to deliver real-time responses. Mirroring company growth, the cloud estate is also expanding rapidly. A year ago there were six AWS accounts. Today there are 22 AWS accounts and nine Azure accounts—with more on the way.

Peter Robinson is the director of cybersecurity and business IT, responsible for the company's cyber risk and security postures. "Zip was born in the cloud, and it's a challenging environment for securing our assets because traditional security tools don't work well here," he says. He has spent most of his two years at Zip looking for the right combination of tools that will provide good visibility into the vulnerabilities and risks Zip faces and the means to mitigate them.

> "Prior to Orca, we had maybe 18% vulnerability assessment coverage of our entire scope. Orca took us to 100% in less than a day."
>
> Peter Robinson
> Director of Cybersecurity and Business IT | Zip

From Little Visibility to 100% in One Afternoon

Zip's platform is on the cutting edge of cloud technologies. "We've moved heavily toward serverless computing and infrastructure as code," says Robinson. "The ephemeral nature of our environment puts us in a position where we can't get agents onto these devices before they're gone. We can't network scan them in the traditional sense, and there's no way to connect to these machines to assess their security status when they're not running."

"We also have an issue of having many environments run by different groups. We have six DevOps teams working on different chunks of infrastructure and other things. Getting them to deploy anything to do risk assessment is almost impossible," says Robinson. "Orca immediately solved this problem for us."

Robinson learned about Orca Security from LinkedIn articles. "We were skeptical about Orca's claims at first, but we gave it a try. We went from years' worth of pain to full visibility in a single afternoon. Take it from a guy who is in the trenches—that is profound."

Orca Far Outshines Competitive Tools

Robinson spent two years evaluating traditional vulnerability scanning tools and others that were specific to container-like environments. "They all had the same problems. One, they required too many resources to deploy agents and scanners. Two, they require credentials to actually authenticate, which makes the licensing model a failure in our perspective. And three, none of the tools automatically prioritize and track remediations."

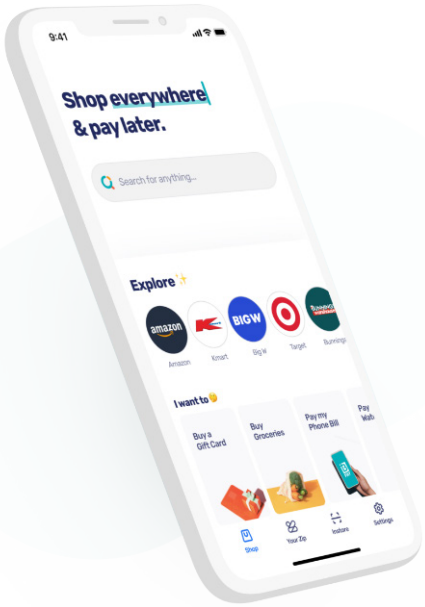
The licensing issue is also a big negative for these tools. "With those other vendors, I would have to buy a full-blown, infinite asset license. As soon as a license is used—albeit on an ephemeral asset—we have to pay for it. A server was only up for six hours and now it has consumed a license. To do the job with these tools would cost me five times more." Robinson reports that licensing this way would have cost him a quarter-million dollars a month.

The main problem with all these tools is that there's no prioritization of risks. For example, Robinson says there might be 129 rules that fail, they're on 2,000 assets, and the tool turns out six or eight pages listing the failures. "You can't drink from that firehose. It's not actionable. Even the SIEM came back with 55,000 failures these past seven days. You can't even assess that."

Orca overcomes all these drawbacks. Deployment is zero-touch and only requires the creation of one role, taking mere minutes. No agents need ever be installed. Licensing is much more manageable and is based on assets actually in use.

However, where Orca really stands out is in its prioritization capabilities. "Orca tells me I have 28 things I need to focus on today. Out of 25 cloud accounts with about 840 compute assets, VMs, and thousands of other assets, true risk comes down to 28 things to take care of today," says Robinson. "We can manage that."

Robinson's Zip team is small, so it needs to rely on tools to help them achieve their goals. "With Orca, all the automation, the prioritization, the correlation, and the zero-impact deployment to our production environments is just gold. It's fantastic," he says.



Orca Improves IT Security and DevOps Cooperation and Productivity

Robinson says the DevOps teams move fast to get their products out to market. He can't ask them to stop building a Zip product to deploy agents and network scanners. Orca takes that burden away. In fact, the DevOps teams are the ones who supported him most in adopting the Orca Security platform.

"The main thing is our DevOps guys don't have to do anything. They create a role and it's done, and they never have to do anything in the future. There's no deployment, no network rules, no security groups they need to change, no endpoint application or agent deployment, no credentialing—nothing. That has changed my world," says Robinson.

IT security and DevOps teams now work well together. "I can come to them with prioritized remediations Orca recommends. There are very clear instructions about issues that are super important," says Robinson. "And it's not just an endpoint asset thing. For example, say we have a problem with the security group of this network ACL, this load balancer, and this endpoint. Orca provides a map. Our people say, 'Oh, Orca shows how it's possible to bypass CloudFlare and the internal load balancers. It shows multi-path routing.' We know that's not supposed to occur because it means someone is bypassing our WAF."

> "Our DevOps guys are focusing on our product, which is what they should be doing. I can't ask them to divert their effort to deploy endpoint agents everywhere and create scanner credentials."
>
> Peter Robinson
> Director of Cybersecurity and Business IT | Zip

Robinson says that type of information is unattainable from other sources. "Orca provides deep insight into their misconfigurations. They can visually see it. They know they need to change it or firm up the security groups so you can only come through the load balancer. And the load balancer only takes input from CloudFlare, and you can't hit the load balancer directly from the internet. This kind of insight is incredibly helpful in reducing our workload," says Robinson.

Orca supports enterprise-grade features such as role-based access control. "What's really good is that when we add people, we can assign accounts to them. I can set it such that my Quadpay guys in the US can only see Quadpay data and work on

Quadpay accounts, as opposed to seeing the entire company. They get to see only what they need to see," Robinson says.

If Zip weren't using Orca throughout the company, Robinson estimates they'd need to have at least one full-time person in each of its six jurisdictions. "We'd probably need six additional FTEs to crawl through a long, non-prioritized list of vulnerabilities, figure out what to work on, create tickets for remediations—all while trying to get agents onto boxes and everything else. So, it's more than just a risk management thing. There's a time, cost, and effort thing as well," says Robinson. "Orca kills two birds with one stone—risk is immediately taken care of, at least from a visibility perspective, and costs are taken care of straight away."

Orca Fits into Zip's Risk Management Process

Robinson has a method for discovering issues —whether it's a penetration test, external vulnerability scanning, internal scanning, observations, incidents, or other means—and driving them through a risk management process into Jira. "We have a risk board in Jira where we evaluate inherent risk. We then assign a sub ticket or a task to the responsible owner and evaluate the remediation needed," says Robinson. "Orca's integration with Jira is on point, so that's definitely working for us." A unique feature of Orca is that it's auto-solving. If it identifies a problem and it gets resolved, Orca notes that it has been remediated. "Before, the guys would have to run a manual assessment and a test to see if this thing has actually been remediated or not. Whereas Orca just says, 'It's gone. Thank you.' We can put our residual risk at zero and close the ticket," says Robinson. "It's quite a time saver."

When Zip recently acquired a company, Robinson was asked to bring their assets under his management. "It took me literally minutes and two brand new Amazon accounts were fully under my vulnerability management scope—100%."

Orca Wins the ROI and Business Case

Zip has tools that scan their assets from the outside. “We throw domain names at it, it does discovery, and uses bug-bounty techniques to assess our external vulnerabilities,” says Robinson. “But internal assessments were more of a challenge before we found Orca. I fought to get the internal scans we needed. We reworked budgets and tried to put a cost on effort, labor, and detraction from our Zip product. I wrote up the business case to include those intangibles. I told our executives about the time it takes in distracting people from doing their regular jobs to deploy agents and set things up, and the time it takes to crawl through vulnerabilities to find the ones that are important and do all that manual correlation. It takes huge amounts of time. Also, integration costs are enormous.”

He says that with Orca, risk is vastly reduced because coverage is 100%. And time savings are pretty much 100% compared to any other product. “Deployment takes 20 minutes and it’s integrated with Jira on the backend,” says Robinson. “From a sys admin, infrastructure, or DevOps perspective, there’s nothing else to do—forever. The business case for Orca is a strong one.”

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 https://orca.security

orca security

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

"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.

INDUSTRY

Financial Services

CHAMPIONS

Felix Beatty
CISO

Jeremy Turner
Senior Cloud Security Engineer

CLOUD ENVIRONMENT

aws Azure Google Cloud

"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 – 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."

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

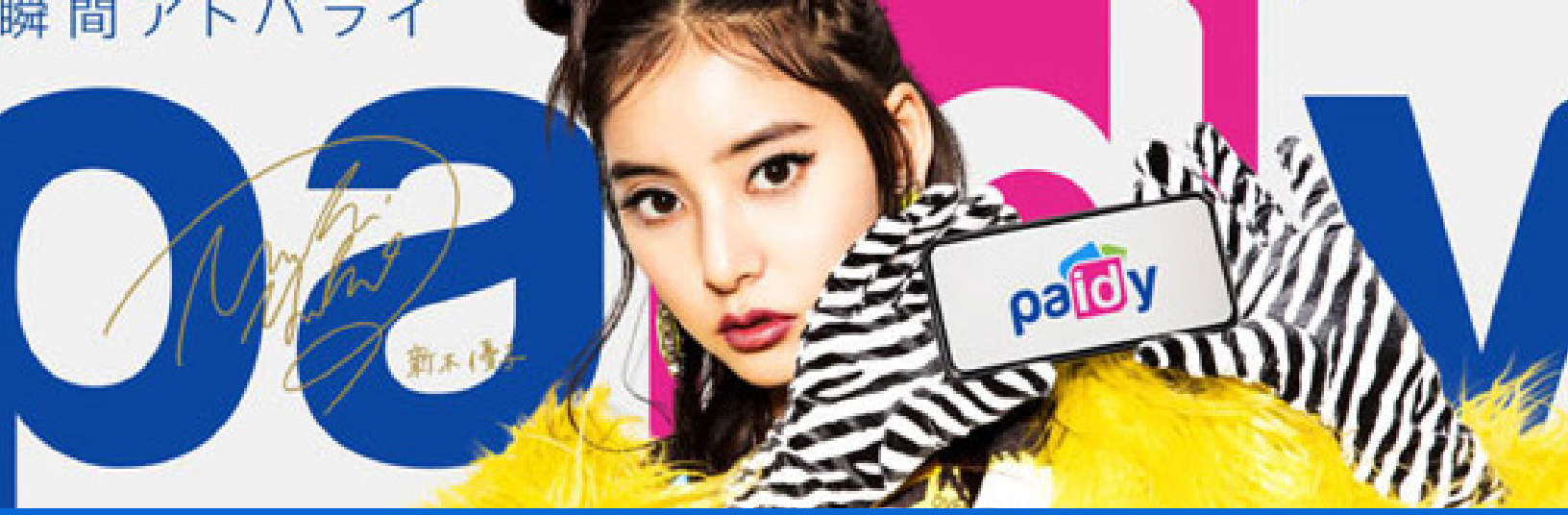
Gaining visibility into everything on the Paidy platform is one of his top challenges. "We have a large and complex cloud environment; it's difficult to manage all these dynamic assets," Beatty says. "We have hundreds of developers trying to push microservices as fast as possible into the cloud, spinning 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.



> "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

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.

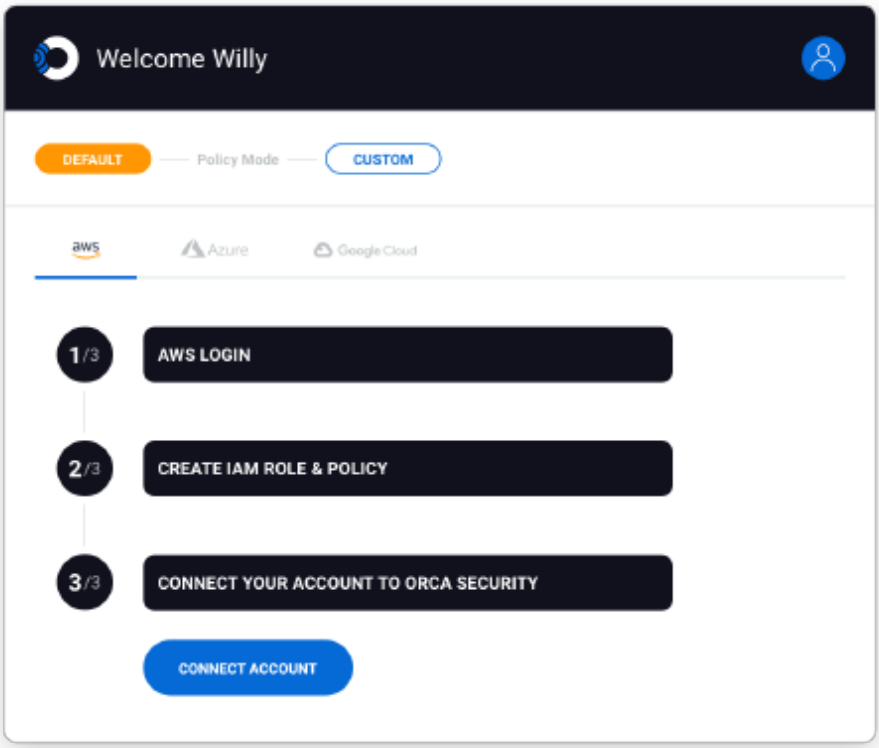
"Authenticated scanners might provide you with more vulnerability data, but still require lots of work to configure, as well as elevated privileges. This opens your enterprise up to risk because you essentially have another shared account and password."

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 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.

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.

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 https://orca.security

orca security

Online Payments Innovator Fast Gets Cloud Security Confidence with Orca Security

"There's no silver bullet when it comes to cloud security, but Orca provides the coverage so security professionals know they've done their best from a security visibility standpoint."

Anshu Gupta
VP, Security | Fast

Cloud Security Challenges

- Eliminate the noise of too many alerts; and focus on critical issues that could lead to a security incident or data breach
- Get comprehensive coverage for different use cases for Fast's cloud-native infrastructure—all applications are fully containerized, with Kubernetes orchestrating the workloads
- Assess compliance with key benchmarks, such as CIS and PCI

Cloud Security Results

- 100% coverage of cloud accounts with full visibility and prioritized remediation—all with zero impact on the production environment
- Gained coverage for use cases—including vulnerability management, asset inventory, regulatory/benchmark compliance, file integrity monitoring, incident alerting, and prioritized remediation
- Dashboards provide a quick assessment of compliance to benchmarks

Fast

INDUSTRY

Financial Services

CHAMPION

Anshu Gupta
VP, Security

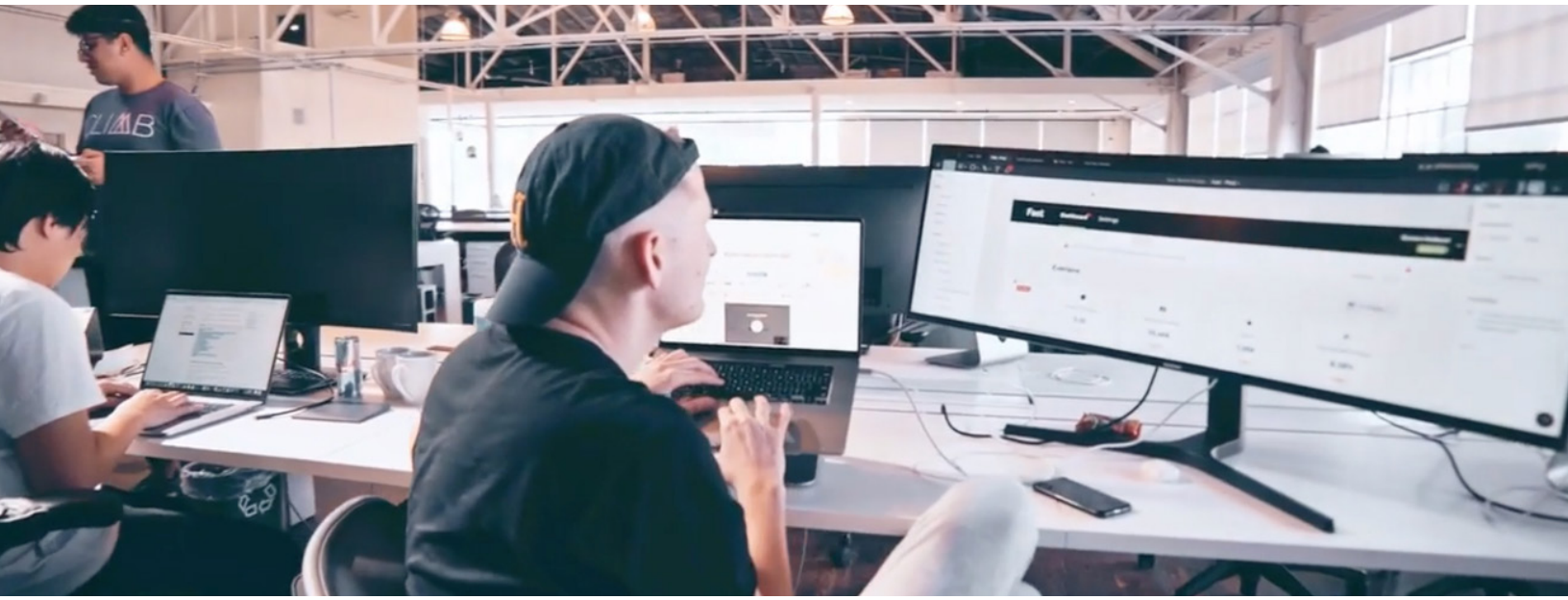
CLOUD ENVIRONMENT

aws

Securing Customer Data Is Inherent in Fast's DNA

Headquartered in San Francisco and backed by several venture capital firms, Fast is a privately held fintech startup established in March 2019. Its mission is to make buying online faster, safer, and easier for everyone. Its Fast Login and Fast Checkout products work on any browser, device, or platform, enabling a single-click sign-in and purchasing experience that makes it easier for buyers to buy and merchants to sell in a consistent, stress-free manner. Fast is entirely consumer-focused and invests heavily in its users' privacy and data security.

Anshu Gupta is its VP, Security. "As a financial services company, we have a strong need for continuous security and compliance," says Gupta. "We're always looking for best-in-class security partners to help us in letting people make online payments in a secure fashion, where they have trust in our product and know we're working with state-of-the-art technology to secure our customer data."

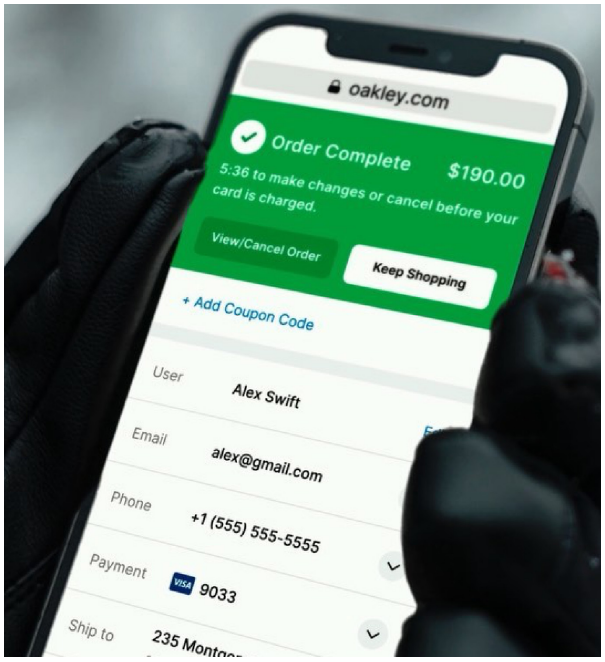


Orca Security Provides Value from Day One for Fast's Cloud-Native Infrastructure

Fast is a cloud-native company running 100% on AWS. All applications are fully containerized, with Kubernetes orchestrating the workloads. Gupta says they looked at various solutions for securing this dynamic cloud environment. "At first we looked at Amazon's inherent security tools such as Security Hub. Although it has a lot of capabilities, it falls short in unifying information within a single-pane dashboard and telling us what we really need to focus on," says Gupta. He looked at a cloud security posture management (CSPM) product, but it wasn't mature enough to meet Fast's needs. Another tool—derived from open-source—yielded too many alerts that didn't make sense. Gupta really needed an enterprise-grade tool that could fit many use cases and prioritize alerts so his security team knows what to work on first. Upon testing Orca, he knew he had found the best cloud security platform.

Orca checked the box on a number of use cases, providing comprehensive coverage. It satisfies Fast's need for vulnerability management, asset inventory, regulatory/ benchmark compliance, file integrity monitoring, incident alerting, and prioritized remediation.

Gupta says Orca provided value from day one in helping Fast protect its infrastructure. He showed his executive team the extent of help the security and DevOps teams get from it, especially when it comes to remediation. "They immediately saw the value and gave us purchase approval," he says..

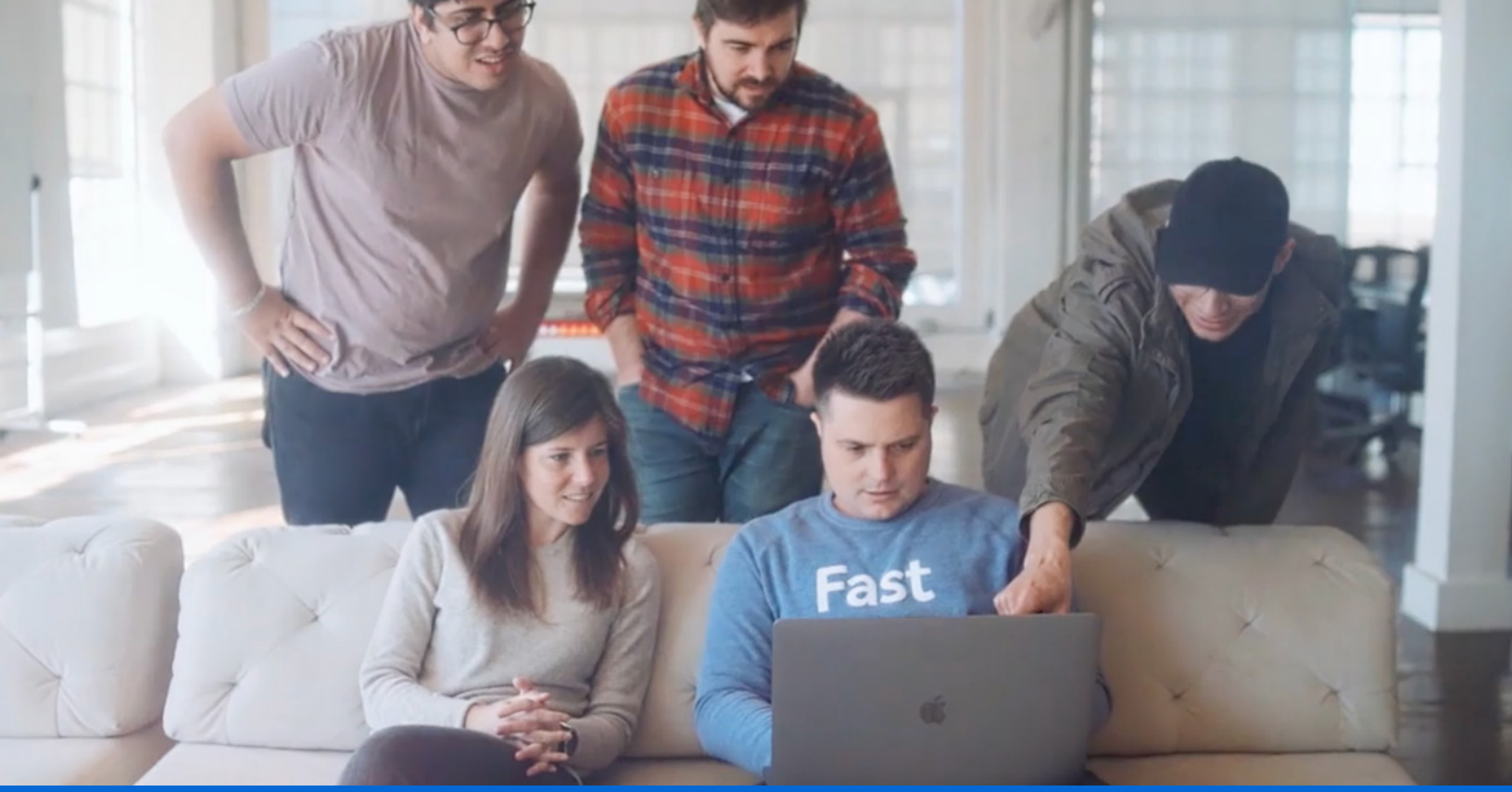


> "I can confidently say that Orca is an enterprise-grade tool that's doing its job when it comes to securing our infrastructure and giving us the visibility we need."
>
> Anshu Gupta
> VP, Security | Fast

Orca's Ability to Distill and Prioritize Alerts Enables Fast to Focus on What's Most Important

Other tools provide far too many alerts to be of any value. "Some issues are of low impact and aren't worth acting upon right away," says Gupta. "Orca tells us straight away what we should focus on in relation to what's urgent for Fast. When we look at alerts, whether they're remediation advisories or interactions between infrastructure components, we can immediately visualize their real impact. Orca helps us triage and prioritize issues."
Fast is still early in its journey with Orca, but both the DevOps and security teams are getting good value from its findings. "Orca has helped us reduce operational incident management time significantly. And now we aren't dealing with so many issues because our environment has been sufficiently hardened," says Gupta.

One area where he struggled with other tools is in recognizing when an issue had been remediated. With Orca's near-real-time visibility, it's quickly reflected in the dashboard when an issue gets fixed. "One time when I was showing Orca in a presentation, we witnessed an issue disappear from the dashboard in real-time—an engineer had easily pushed code into production that fixed it."



"In the financial services space, a single incident can be catastrophic, so we simply can't afford to make mistakes. That's where Orca provides us with total confidence we don't have pending issues we need to be worried about."

Anshu Gupta
VP, Security | Fast

Meets Multiple Controls to Satisfy Compliance Needs

Given its role in financial services, Fast is strictly held to regulatory standards for protecting customer data. "For PCI compliance, we've ideally been looking for a single solution that helps us meet multiple controls, be they vulnerability scanning, file integrity monitoring, system hardening, or compliance with frameworks such as CIS. Being feature-rich, Orca is one of the few available tools that help us meet our compliance requirements —including PCI," says Gupta.

Orca reports show proof to auditors that vulnerabilities have been found and remediated. They show that Fast has its security program under control.

Orca Innovation

"One of the things I like most about Orca is that it's constantly innovating," says Gupta. "When Orca's CEO frequently reaches out for our feedback, I take that as a sign he wants his product to be the best. He really listens to security professionals who constitute his customers to incorporate our ideas into the product. I'm glad we're part of Orca's journey, just as it's part of ours."

Gupta's advice to his fellow CISOs is, "Give Orca a shot. If you're evaluating multiple solutions for cloud security and haven't looked at it, you're doing yourself a disservice. Orca is easy to deploy and use; it doesn't disrupt your production environment and you realize great value early on."

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 https://orca.security

orca security