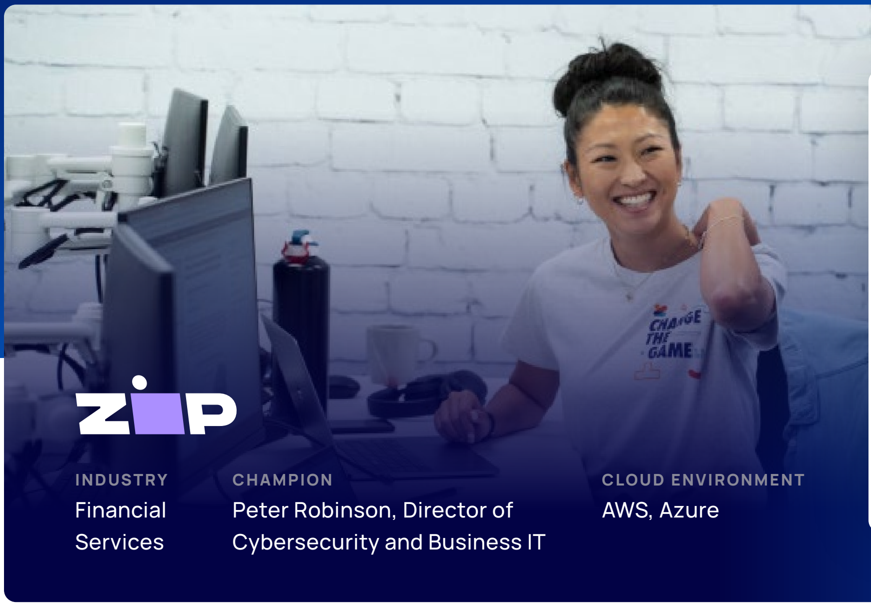
CASE STUDY I ZIP

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



INDUSTRY
Financial Services

CHAMPION
Peter Robinson, Director of Cybersecurity and Business IT

CLOUD ENVIRONMENT
AWS, Azure

> "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

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.

> "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

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.

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.”

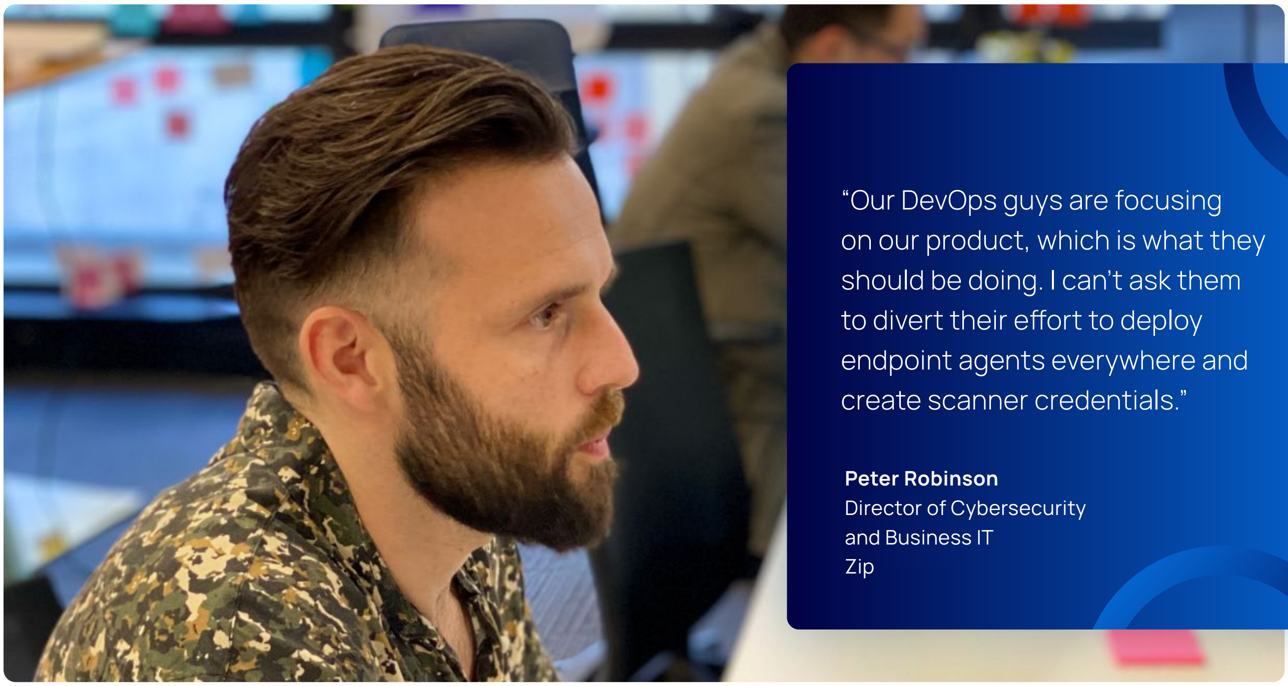
Robinson’s Zip team is small, so it needs to rely on tools to help them achieve their goals. “With Orca, all the automation, the prioritization, the correlation, and the zero-impact deployment to our production environments is just gold. It’s fantastic,” he says.

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." 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.

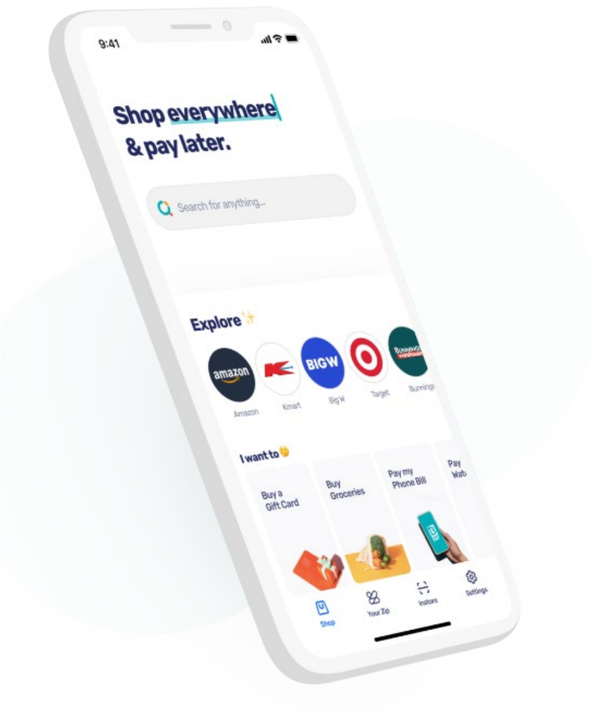


"Our DevOps guys are focusing on our product, which is what they should be doing. I can't ask them to divert their effort to deploy endpoint agents everywhere and create scanner credentials."

Peter Robinson
Director of Cybersecurity
and Business IT
Zip

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.”

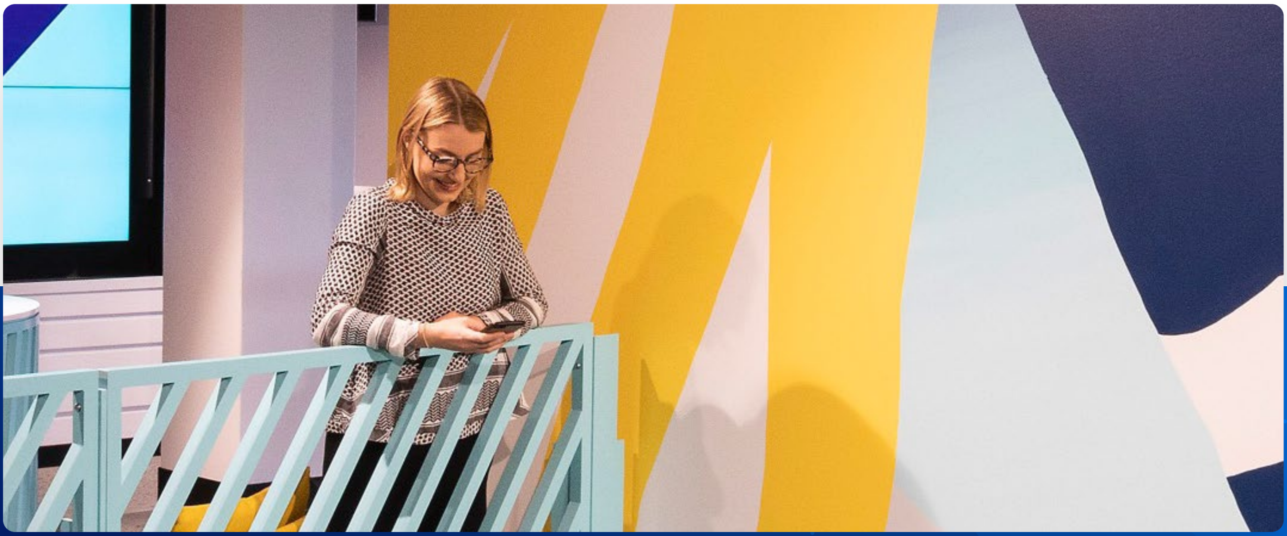
A unique feature of Orca is that it’s auto-solving. If it identifies a problem and it gets resolved, Orca notes that it has been remediated. “Before, the guys would have to run a manual assessment and a test to see if this thing has actually been remediated or not. Whereas Orca just says, ‘It’s gone. 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 bugbounty 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.

orca security

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