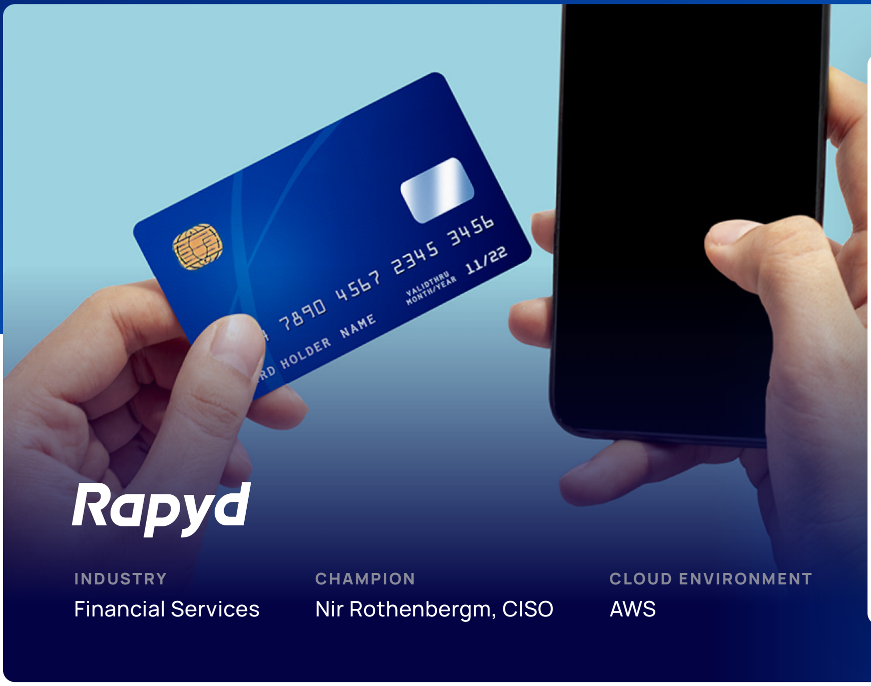
orca security

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



Rapyd

INDUSTRY
Financial Services

CHAMPION
Nir Rothenbergm, CISO

CLOUD ENVIRONMENT
AWS

> "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
Chief Information Security Officer
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 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 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.”

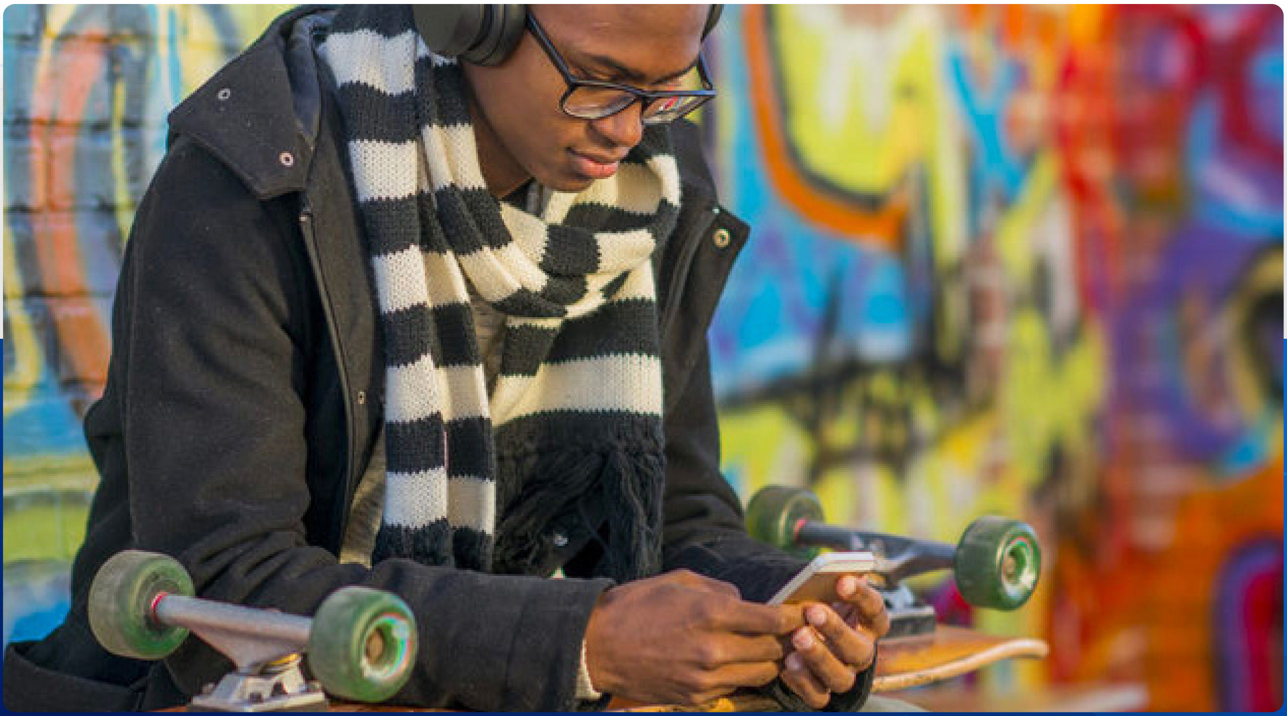
In previous years, Rapyd tracked vulnerabilities in Excel spreadsheets. Orca has eliminated that process. “Now everything is automated and has a CI/CD pipeline. The next time we face an audit, I can show our Orca and Jira reports to show the risks we’re tracking and what we’re doing to remediate them,”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

> “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**
> Chief Information Security Officer
> Rapyd

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.

orca security

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