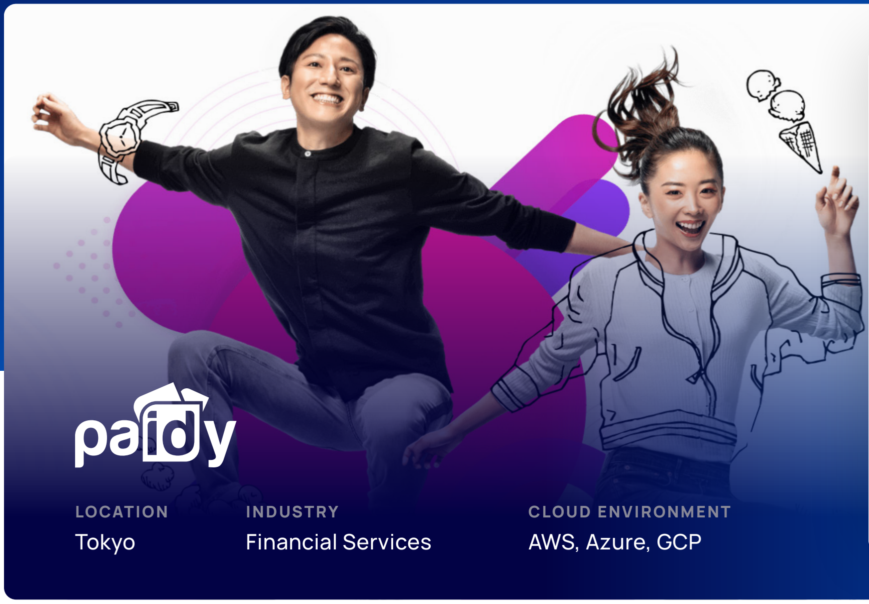
# Paidy Turns to Orca Security for Multi-Cloud Visibility, Saves Two FTEs and $500,000/Year in Cloud Security Management Costs



LOCATION
Tokyo

INDUSTRY
Financial Services

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

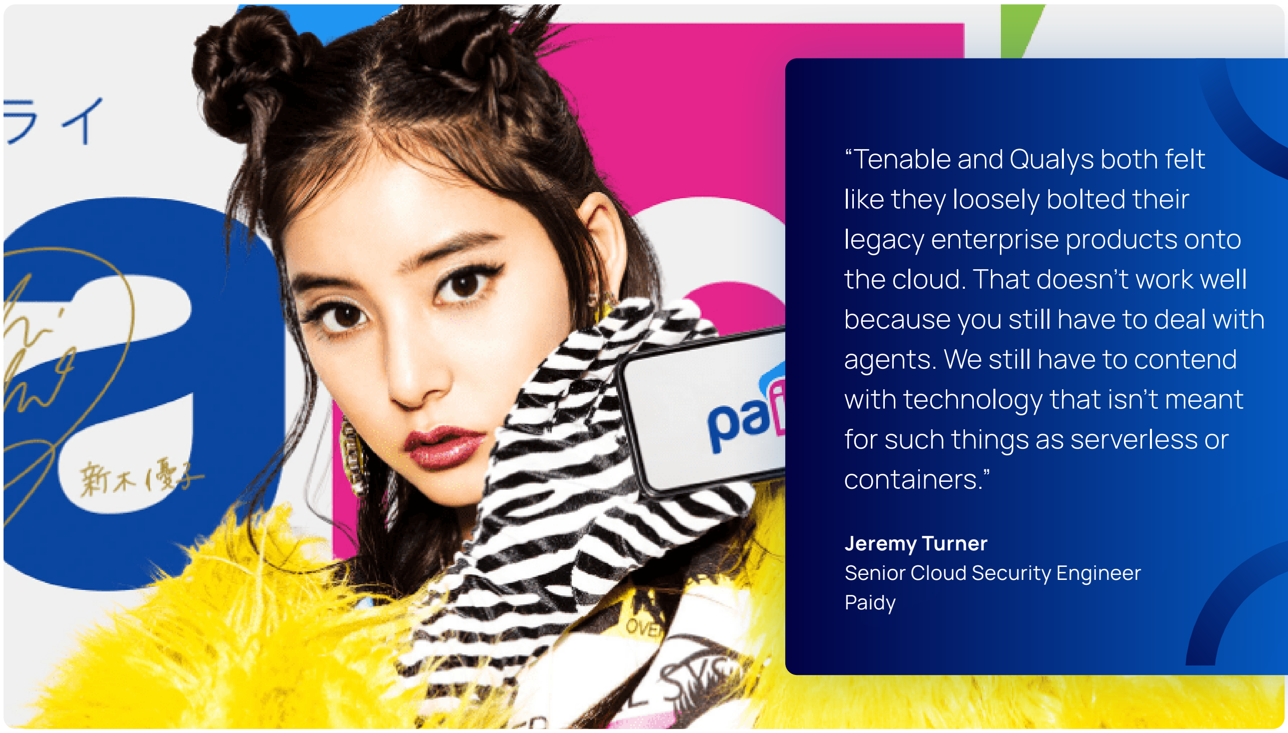
The Paidy security team had experience with a variety of legacy tools adapted for the cloud. Turner says, “I’ve used Trend Micro, Qualys, and Tenable, either in an enterprise environment or in testing. Tenable and Qualys both felt like they loosely bolted their legacy enterprise products onto the cloud. 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.”

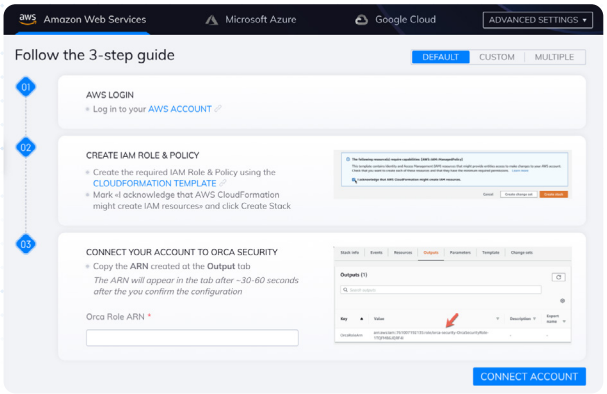
Cloud providers such as Amazon do provide security scanning tools. “Amazon’s AWS Inspector, a vulnerability scanner, requires an agent. Usually it’s baked into the Amazon AMI, but it only works with certain AMIs,” he continues. “AWS GuardDuty ticks the box for a vulnerability scan and compliance check. 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

AWS LOGIN
- Log in to your AWS ACCOUNT

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

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.

## 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