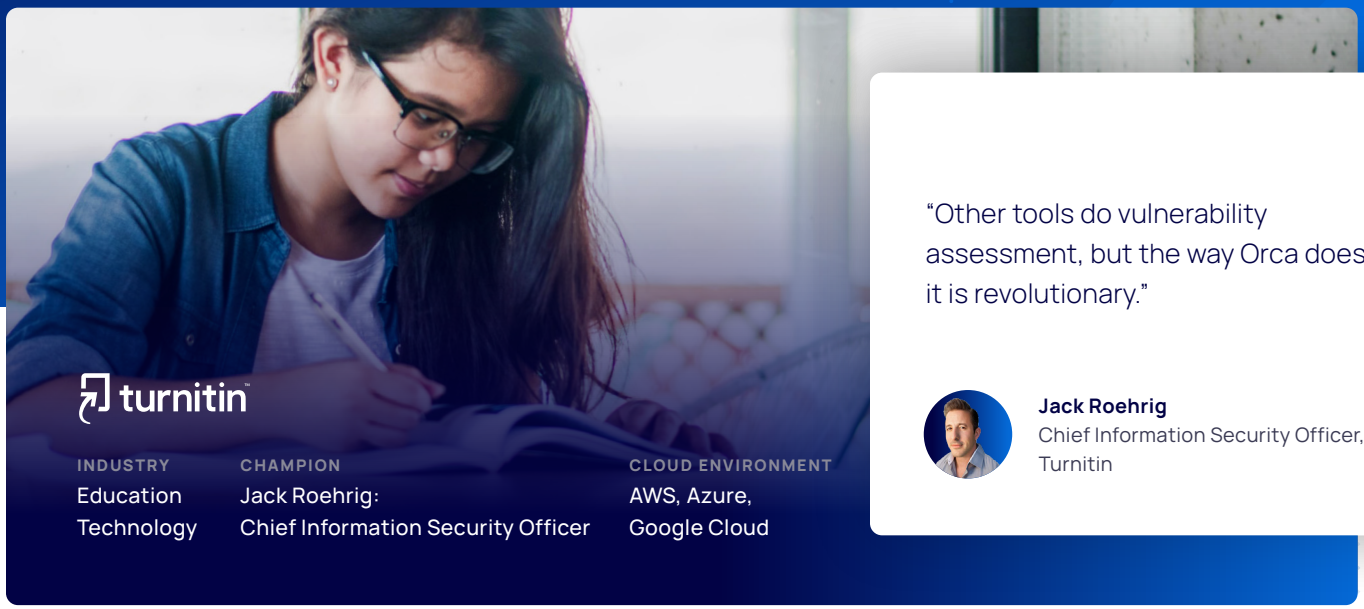
Orca Security Helps Instill Security Discipline and Governance for Turnitin's Multi-Cloud Estate



turnitin

INDUSTRY
Education Technology

CHAMPION
Jack Roehrig:
Chief Information Security Officer

CLOUD ENVIRONMENT
AWS, Azure, Google Cloud

"Other tools do vulnerability assessment, but the way Orca does it is revolutionary."

Jack Roehrig
Chief Information Security Officer, Turnitin

Cloud Security Challenges

- Need to support the company's M&A strategy and regulatory compliance efforts
- Improve security governance, close gaps, and reduce the potential attack surface
- Agent-based security tools miss high-risk aspects of the cloud estate

Cloud Security Results

- Provides quick assessment of M&A targets to support due diligence analysis
- Demonstrates a proper security program to regulators
- Gets ahead of governance with better visibility and more security discipline
- Agentless implementation provides 100% visibility of multi-cloud estate

30+ Million Students Use Turnitin Services Worldwide

Turnitin is a global SaaS company dedicated to ensuring the integrity of education and research while supporting the development of original thinking skills. The company provides instructors with tools to engage students in the writing process, provide personalized feedback, and assess student progress. Turnitin is used by more than 30 million students at 15,000 institutions in 140 countries.

Orca Tames the M&A and Compliance Processes

Turnitin has an acquisition strategy to help grow the company and Jack Roehrig is involved in the security due diligence process. "I've worked on M&A activity for more than a decade, and I know how to do the security assessment. I build a mock security program for a prospect company, then I run an actual security program after the acquisition. Today, all companies have something in the cloud. Orca makes it very easy for me to do a quick assessment to see if they're doing things that are reckless."

Regulatory compliance is another area under Roehrig's purview. GDPR, CCPA, PCI DSS—all are regulations of interest to Turnitin, especially given the amount of PII in the company's databases. With GDPR in particular, one of the most important principles is a demonstration of a proper security program. "With Orca, I can easily demonstrate passing cadence. I can demonstrate vulnerability assessment, proper governance of machines, and separation of duties," Roehrig says. "Orca in itself would convince any EU judge that a company has a more than reasonable security program."

"With Orca, I can easily demonstrate passing cadence. I can demonstrate vulnerability assessment, proper governance of machines, and separation of duties. Orca in itself would convince any EU judge that a company has a more than reasonable security program."

Jack Roehrig
Chief Information Security Officer
Turnitin

Orca Helps Turnitin Improve Discipline and Governance

Roehrig also has a strong DevOps background; this experience enables him to raise security and governance awareness with his DevOps team.

"We're several years into a massive cloud migration project," Roehrig says. "Turnitin is focused on getting our cloud applications into production with the highest levels of security. Until Orca, I couldn't find a vendor that would advance our security posture."

Roehrig came across Orca Security at an RSA Conference and liked what he saw. "The product was just elegant." His team soon ran an Orca PoC against Turnitin's SaaS application that was still in development. He used the results from the Orca scan to create greater security awareness among company executives and justify an increase in its security budget.

With Orca, Nothing Gets Overlooked

Roehrig has dual responsibilities at Turnitin. In addition to heading up security, he also leads the DevOps team. "I've been evangelizing our need to have fewer AWS accounts due to pricing models and associated overhead. I believe we have more AWS accounts than we need, so I began to inventory our assets by asking my development team for a node count. I wanted to know how many block storage devices related to EC2 instances are in production. The responses were between 150 and 400. But Orca showed we actually have 650. That revealed a lack of governance over our assets."

Roehrig finds this disconnect on asset inventory particularly troubling. "The one area where you need to have security controls the most is where you don't know the assets exist because they are ungoverned in other ways, too."

This is one reason why Roehrig prefers not to use risk assessment or vulnerability scanning software that require agents. "If I'm using agent-based software, then I'd be relying on the determinism of my agent deployment system, whether it's Chef, Puppet, Ansible, or something else. I'd have to rely on my asset management database being whole, encompassing everything. And I'd be relying on my identity and access management system to properly govern every asset."

Roehrig tells of one experience in deploying an agent-based security system. Logging into the product's console, he saw only 300 machines. Yet his infrastructure contains about 3,500. Auto-scaling microservice infrastructures and other edge

> "Orca helps us get ahead of governance issues. It can expose risk on any machine that lacks governance. I can take that finding and ensure the machine is being governed by the same security controls as everything else."
>
> **Jack Roehrig**
> Chief Information Security Officer
> Turnitin

cases weren't receiving the agent. This created a huge gap in visibility.

"Then Orca came along," Roehrig says. "Orca doesn't depend on agents, so it deploys on everything in the cloud. It picks up all edge cases and high-risk instances. That's critical—nothing gets overlooked."

"I gave the DevOps team access to Orca and they loved it. I've never seen an adoption like this. Within minutes, they had a dashboard where they could see real risks with 100% visibility. That's just remarkable. Orca helps the team know where to spend their time."

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](orca.security)