orca security

CASE STUDY I FOURKITES, INC.

Orca Delivers Near Real-Time Cloud Security Visibility to FourKites

FOURKITES

INDUSTRY
Supply Chain Platform

CHAMPION
Charles Poff: VP of Information Security

CLOUD ENVIRONMENT
AWS, Azure

> "If you work for a company that's in the cloud, Orca Security provides you with a robust security visibility that is second to none."

Charles Poff
VP of Information Security
FourKites, Inc.

Cloud Security Challenges

- ☒ Need to build security visibility across all public cloud platforms
- ☒ Transition from reactive to proactive security
- ☒ Cost of security toolset escalates as the company scales
- ☒ Quicker assessment of the security posture of acquired companies

Cloud Security Results

- ✓ Does the work of several security tools, enabling cost savings & management
- ✓ Provides intelligence to an orchestration layer for remediation automation and playbooks
- ✓ Streamlines the due diligence process in acquisitions of companies
- ✓ Scales as cloud estate grows

Supply Chain Visibility Platform FourKites Is Growing Rapidly

FourKites is the #1 supply chain visibility platform, using real-time data to make global supply chains more efficient, agile, and sustainable. Working with over 1,000 of the world's most recognized brands, FourKites tracks more than 2.5 million shipments each day across more than 185 countries. In light of the global economic downturn, capacity shortages, and trade tensions, logistics professionals are accelerating their move to FourKites' solutions to better manage their operations and ensure timely delivery of shipments via real-time supply chain visibility. In 2021 the company saw 105% growth in total shipments, having tracked over 112 billion miles and computed over 5 billion estimated times of arrival.

FourKites leverages patented artificial intelligence to process more than 150 factors — weather, traffic and real-time data from GPS, ELD telematics networks, mobile devices, AIS and more — and provide insights and recommendations based on trillions of data points. The company was born in the cloud and fully operates its business within AWS and Azure.

Charles Poff recently joined the company as its VP of Information Security. With 25+ years in cybersecurity, he has a track record of building world-class, high-performance security programs. Poff joined FourKites to take the company's security program to the next level while the company experiences extensive growth.

"We have some of the largest companies in the world as customers. I was brought in to align a proactive security strategy with the growth and scale of the organization," says Poff.

Orca Fills the Role of Several Products in the Cloud Security and Compliance Toolbox

"Building a world-class security program starts with having a strong foundation in your security visibility fabric, that allows us to see everything in our environment in near real-time," says Poff. "We're taking a defense-in-depth approach to get a good grasp on our situational awareness. One question I like to ask any organization is, 'If we had a breach today, would we be able to detect it? Would anyone know?' If the answer is no, then we know what our top priorities are."

One of Poff's first purchases as head of Information Security was Orca Security. "The SideScanning™ technology is unique to Orca. It's not in the critical path, so the level of effort to get it installed and operational is literally just a few minutes," Poff says.

> "With Orca, there are so many features and functionalities combined into one non-intrusive tool. It saves us from having to buy a bunch of separate products that cost a lot and don't provide full coverage."
>
> **Charles Poff**
> VP of Information Security
> FourKites, Inc.

Beyond the simplicity of getting started, Poff says Orca provides value from a lot of different angles — vulnerability scanning, infrastructure configuration scanning, endpoint scanning for malware, Docker container scanning and reporting that actually ties together. "This means I don't have to invest in multiple tools, each of which has its own licensing and cost models that don't scale well with hyper-growth companies. There are tremendous cost savings with Orca."

Adding to Orca's value is that it works across multi-cloud environments. "We could use each cloud service provider's native tools, but that adds to the cost and complexity, leaving us with no unified view of our security status," he says.

> "Agents often provide a false sense of security. There are gaps in coverage where you can't install and use agent-based security products in the cloud. At any given time, there are 10-15% of agents that are broken, need reinstallation, or cause stability issues."
>
> **Charles Poff**
> VP of Information Security
> FourKites, Inc.

Agent-Based Products Don't Meet the Need

Poff sees the limitations of the use of agent-based products in the cloud. For starters, agents can't be deployed everywhere in the cloud, so you'll never have 100% coverage. Things like serverless, compute, Kubernetes, and others can't have agents installed, or it just doesn't make sense. "Once you get past your scale pain point threshold, the costs around managing agents are not easily justifiable," Poff says.

Poff has worked with other endpoint security products at previous companies, where the licensing costs were not aligned with the company's growth strategy. In some instances, licensing costs went from $160K in year 1 to more than $800K by years 2 and 3. That's an unsustainable cost increase and only covers licensing. It didn't account for staffing increases to maintain the endpoint agents.

"With Orca Security, I don't have to beg for DevOps' time to install anything. We now get 100% complete visibility across our entire cloud infrastructure, even on systems where agents can't be installed. We can easily benchmark our entire infrastructure against CIS Security Standards and many other compliance programs. In addition, we tied Orca back into our SOAR platform for easy alerting and automation around remediation tasks. Orca figured out the gaps in the industry and tied it all together into one product," according to Poff.

Innovative Uses for Orca Security

Poff has used Orca Security in previous organizations and takes advantage of the Orca Security reporting and results in innovative ways. For example, he's delighted with a feature that shows neglected assets and Orca's ability to support custom policies. “We’re able to tell from the way Orca Security articulates the number of vulnerabilities associated with a system if it hasn’t been touched in a while. That tells me if our patch management practices are out of compliance,” he says. “This level of security insights and optics is a must-have for any vulnerability management and remediation program. This is basic security hygiene that can be hard to see and understand. We use Orca’s reporting to drive better compliance and ensure that we are seeing everything.”

Poff doesn’t see SIEM technologies as being the focal point of any security program anymore — they’re too costly and by the time that data is normalized (log delays / queuing), the malicious activity has already happened. Instead, he feeds Orca Security intelligence directly into an orchestration layer through an API. “The data is already normalized and accessible via Orca Security’s rich APIs. We can ingest it into our orchestration layer that has the fingers to go into the environments and remediate or manage the risk,” he says. “Orca’s real-time data helps us move from a reactive to a proactive stance, and that’s where we want to be.”

To increase transparency and establish credibility with stakeholders, Poff gives them complete access to the Orca Security platform. “If I just gave them a report of vulnerabilities, they’d get defensive and push back on making the required changes. Instead, I reinforce that security is an extension of their teams — the DevOps, TechOps, CloudOps, and other engineering groups. They can see what is a high priority and what can wait to be fixed because Orca Security provides factual information that is not only classified by severity but is actionable. This helps create a partnership rather than an adversarial relationship, and it puts us in a continuous remediation cadence,” explains Poff.

“The intelligence that comes out of Orca Security is accurate. And it’s global. It crosses everything in your cloud environment.”

Charles Poff
VP of Information Security
FourKites, Inc.

Orca Security Provides a Win for M&A Due Diligence

FourKites is growing rapidly, including both organic growth and strategic acquisitions. Orca Security plays an important role in evaluating acquisition targets, both before and after deals close. "Instead of having to partner with an M&A due diligence firm to conduct compromise assessments, installing agents that auto-delete, uploading data, then getting a report a week later as to whether or not the target company has been compromised, I can plug in Orca Security and have very acute situational awareness of the company's security status within 24 hours," says Poff. "That's a tremendous win for us. We get instant gratification on their security posture and how mature they are in terms of a security program."

Contrast this with a traditional kind of due diligence security review. Multiple rounds involve many hours and resources spent on completing questionnaires, conducting audits, and reviewing documentation.

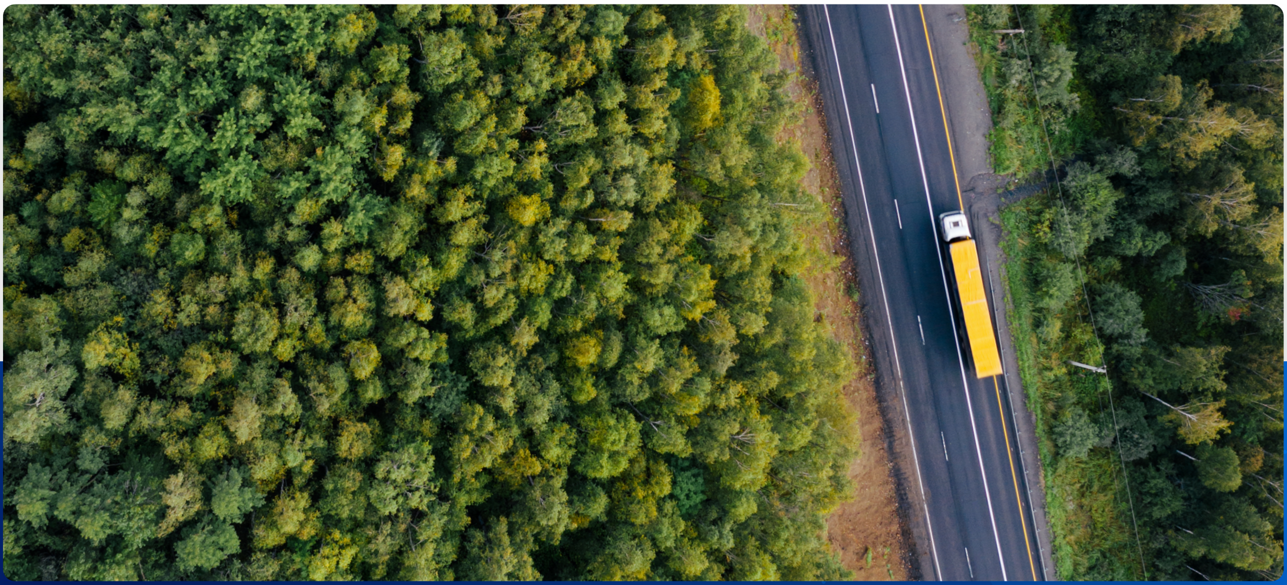
"That stuff is great, but we can speed up the process if we just snap in Orca Security. Now we can see the misconfigurations, the malware infections, any potential backdoor lateral movement, and the like," says Poff. "We can understand if patch management is aligned with our security policies and SLAs. And we get all that in a matter of hours."

Visibility post-acquisition can be even more crucial. Poff has seen a lot of M&A activity; in his experience, an acquired company immediately becomes a target of hackers when a deal is signed and announced. "The new company becomes an entry point into the mothership," says Poff. "It's a precarious time because there's not much you can do in the short term from a security perspective without disrupting operations. Snapping in Orca Security will give us high value at a low impact. Within a day, we can start to understand the risks to the organization and prioritize how to address them."

Orca Security's Value to FourKites

Overall, Poff is pleased with Orca Security's value. He gets a wide range of features and functionality, enabling him to ditch more expensive tools. He gets a unified view across FourKites' entire cloud estate without the hassle of deploying agents everywhere. And Orca Security puts the organization on the path to proactive security, even as the company experiences tremendous global growth.

> "With M&A activity, Orca Security gives us a level of comfort — a level of confidence — about the company we're acquiring. We can assess the security risks and determine its security posture within a day."
>
> **Charles Poff**
> VP of Information Security
> FourKites, Inc.



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