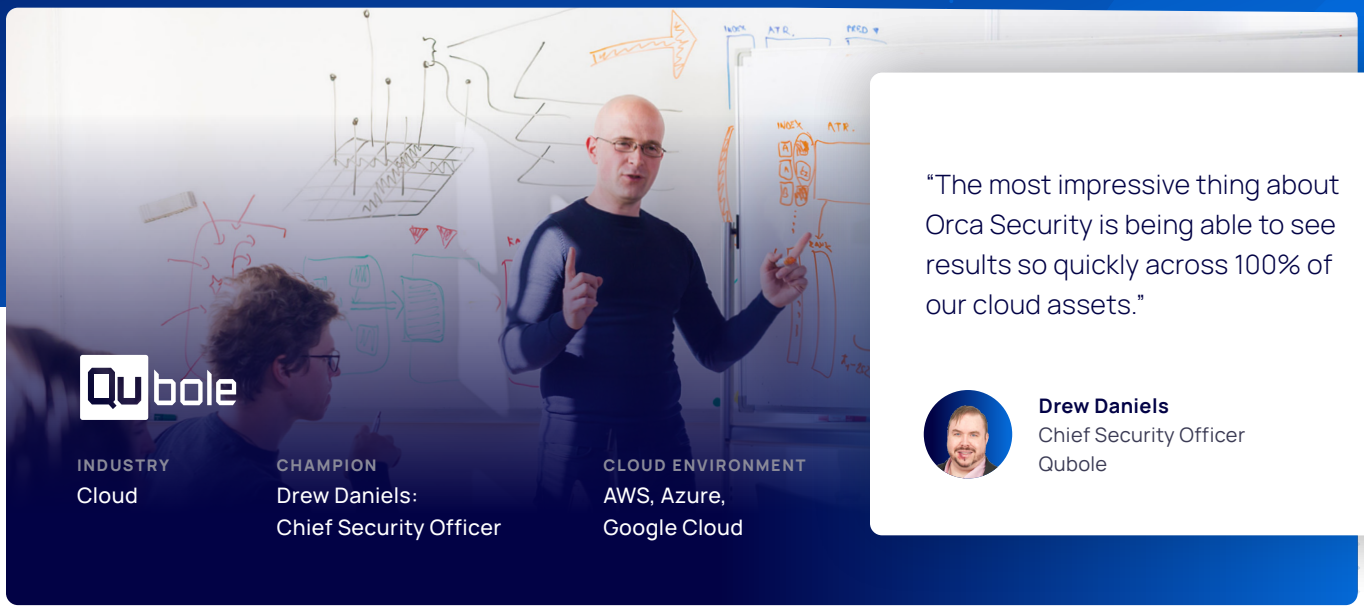
Qubole Protects Its Multi-Cloud Environment with Orca Security



INDUSTRY
Cloud

CHAMPION
Drew Daniels:
Chief Security Officer

CLOUD ENVIRONMENT
AWS, Azure,
Google Cloud

"The most impressive thing about Orca Security is being able to see results so quickly across 100% of our cloud assets."

Drew Daniels
Chief Security Officer
Qubole

Cloud Security Challenges

- Agent-based solutions took an average of nine months to implement and were ineffective
- Tedious per-asset integrations and maintenance burned up 33% of an FTE
- Competing solutions had side effects that impacted performance

Cloud Security Results

- A few hours to configure, and live in two weeks – 95% faster than competing solutions
- No performance hit on live environments
- Complete coverage across the cloud environment

Qubole is the #1 Cloud-Native Data Platform

Qubole provides a cloud-native data platform for analytics and machine learning that quickly activates large quantities of data for all users while lowering costs. It provides freedom of choice: customers can use any engine, any tool, and any cloud. Cloud security is a critical function of Qubole's platform.

Qubole's CSO Drew Daniels Tried One Tool After Another

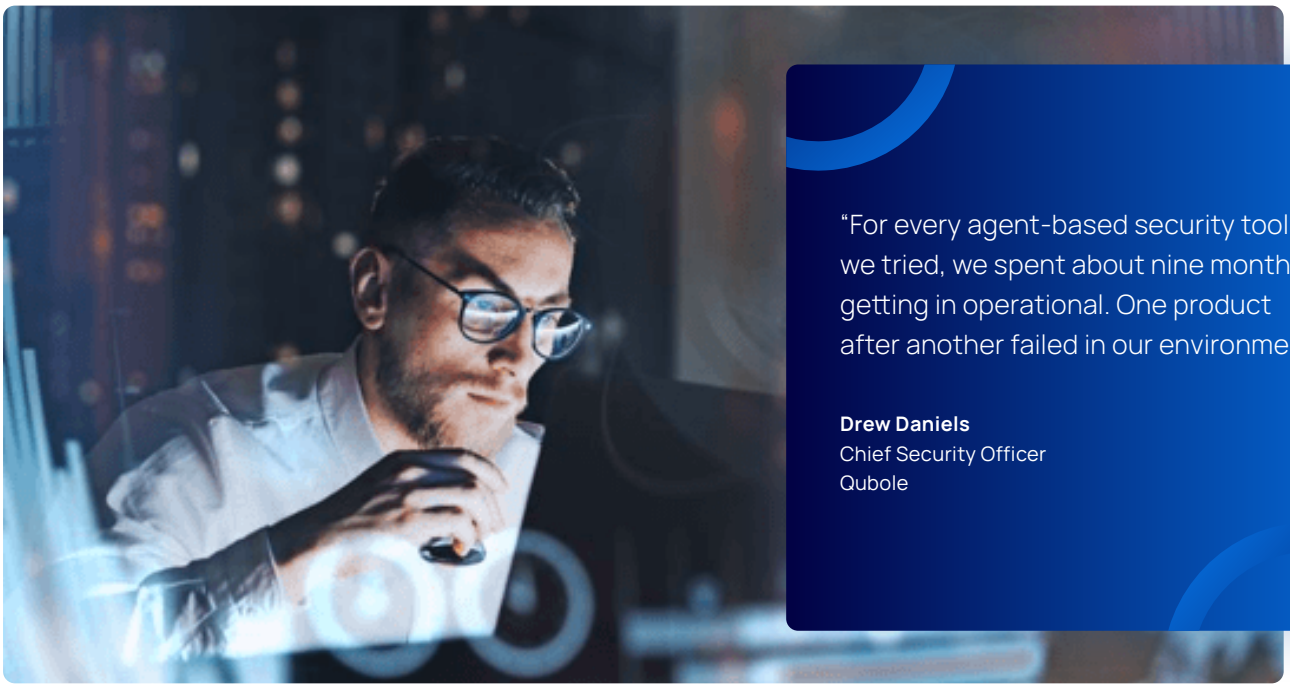
Many of Qubole's customers analyze petabytes of data every day. As a result, Qubole processes over an exabyte of data every month– across Microsoft Azure, AWS, and Google Cloud Platform. Customers such as Oracle, Expedia, Gannett, Roku, and others expect strong security to be an inherent feature of the Qubole platform.

Qubole CSO Drew Daniels had tried numerous security tools, but had abandoned most of them. "Traditionally, my customers were asking me to do risk detection in our cloud infrastructure," Daniels said. "That's what I was trying to solve as we tried one tool after another."

Agent-Based Security Tools Too IP-Centric, Didn't Scale for Cloud

The virtual nature of cloud computing is fundamentally different from traditional physical computers. With the latter, an installed software agent can scan for misconfigurations, vulnerabilities, cyber threats, and other risks on each machine. Agents track their steady state of health, pointing to specific machines or IP addresses where a problem exists.

That practice doesn't translate well to the cloud. "In a cloud environment, you're frequently scaling utilization up and down—possibly thousands of



"For every agent-based security tool we tried, we spent about nine months getting in operational. One product after another failed in our environment."

Drew Daniels
Chief Security Officer
Qubole

times per hour across multiple clouds—all within a CI/CD pipeline that builds your infrastructure," said Daniels. "When dealing with containers and VMs, agents can be challenging." Agent-based approaches often track hosts and systems by an IP address or network; that's not scalable when you're launching thousands of hosts an hour. "The database fills up quickly, making data analysis difficult."

Identifying vulnerabilities by virtual machine or IP address is ineffective, because they change all the time. "A given IP address might point to 60 different machines in any given month," says Daniels. "It's useless to get a report identifying a vulnerability at a certain IP address because the VM in that location during the scan is probably long gone."

> "With Orca's approach, no workloads get overlooked because the cloud infrastructure is aware of all systems attached to that account."
>
> **Drew Daniels**
> Chief Security Officer
> Qubole

Competing Tools Took an Average of Nine Months to Implement and Were Ineffective

Daniels has tried numerous tools over the years, starting with AlienVault. "We would kill it on a regular basis because it was trying to track all the different states of these ephemeral virtual machines," he says.

"We ran into the same problem with CloudPassage.

It was just difficult to deploy on such a large scale and not have it break anything. With Qualys, we spent a whole year writing scripts and figuring out ways to tease out the information we needed because it was focused on machines and their IPs. Well, that doesn't do me any good because that machine's gone already. With Threat Stack, the experience was the same. One product after another failed in our environment."

There were two main issues with most of these tools: installing and maintaining the agents and operationalizing the data they collected.

"For every agent-based tool we tried, we spent about nine months getting it operational. One product after another failed in our environment," Daniels said.

"Every time there was an agent update, we had to resoak those images in our QA environment."

Tedious Agent Deployment and Maintenance Burned Up One-Third of an FTE

In Qubole's mature cloud infrastructure, each security tool required about a third of an FTE to operationalize images and agent distribution. New agents come out all the time; each has to be soaked and tested, then go through a verification process to make sure it's not going to break anything. Then the Ruby Chef recipes have to be updated to deploy to the various Qubole platform tiers. As a last step, someone has to ensure that the image or agent gets deployed in a release cycle or a hotfix process. Daniels laments the waste of time and effort put into each product they've tried and abandoned.

Orca SideScanning™ "Out-of-band approach is a Breath of Fresh Air"

Learning about Orca Security through a CISO colleague, Daniels was intrigued by its agentless approach to scanning cloud environments. Instead of installing agents on virtual devices, Orca reads cloud block storage out-of-band, from the side — hence the term SideScanning™. No code runs within the cloud environment. Orca then reconstructs a read-only model of the cloud environment — including operating systems, applications, data, and metadata — which it then scans for malware, misconfigurations, secret keys, weak passwords, lateral movement risk, and high-risk data such as PII. It's all done without any impact to the active runtime environment.

Orca's ease of deployment and non-invasive approach are invaluable to Qubole's business model. "Orca is obviously different," Daniels said. "I wanted a tool I could deploy quickly and without risk to my services—Orca definitely checked that box. With Orca working out-of-band, I can attach it to the cloud account and let it do its thing on the side. That's a breath of fresh air."

No Performance Impact, No Overlooked Workloads

Qubole's service is all about performance with sub-second latency, so it's critically important that the security tool doesn't impact performance on a live environment. Orca doesn't.

"Almost everything we do uses SSH, so we can't get in the middle of, or block, those critical communications," Daniels said. "Other tools sometimes want to control that access. When you're doing that tens of thousands of times an hour, it could cause a blockage that makes our service stop responding. That's a critical failure."

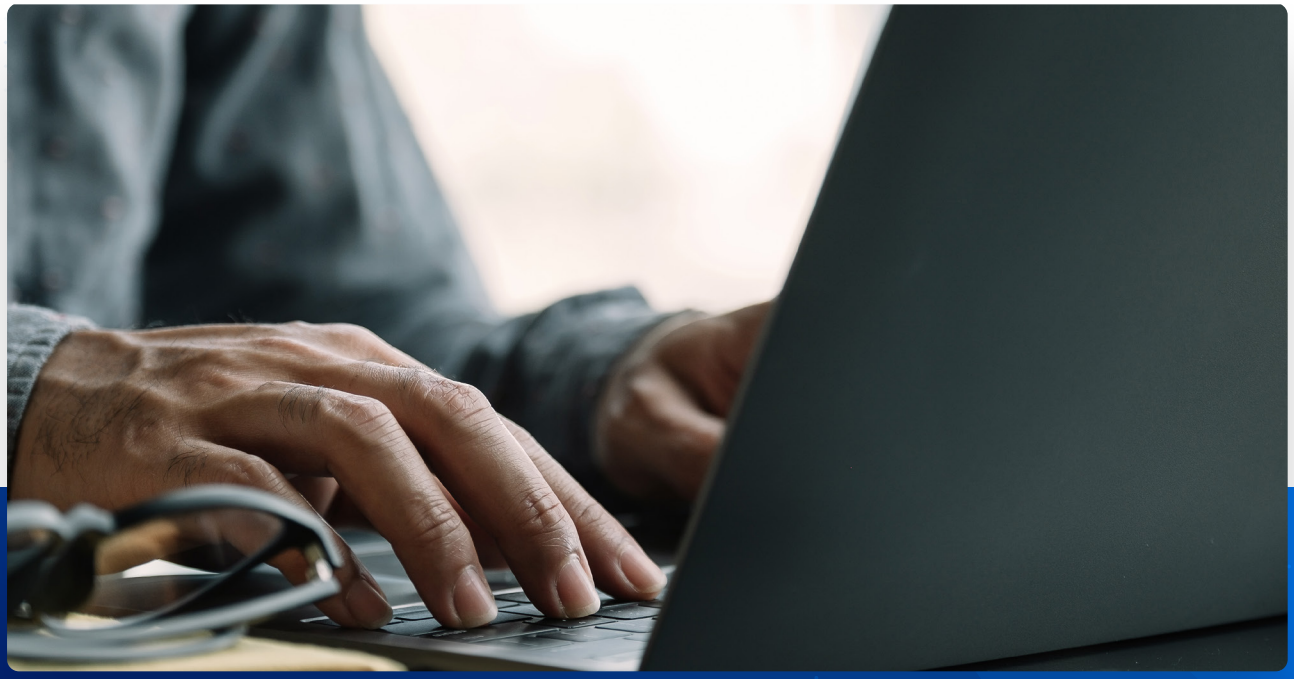
Perhaps most important to Daniels, "With Orca's approach, no workloads get overlooked because the cloud infrastructure is aware of all systems attached to that account."

Orca Cuts Average Deployment Time by 95% – From Nine Months to Two Weeks

Orca has saved Qubole considerable deployment time. "We were able to deploy Orca across 17 cloud accounts in two weeks," Daniels said. "We probably could have done it in one day if I had assigned a dedicated resource. But we first had to figure out the privileges needed and then get the operations team to create those roles on the various accounts."

Next Up? Bringing Orca's Security Insights to Multiple Departments

From the GRC team responsible for trust certifications to security operations, Daniels expects that several departments will interact with—and benefit from—Orca's security scans. "Orca is useful for incident response and helps us focus on the most critical issues. DevOps is even starting to use it as a quality control tool."



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)