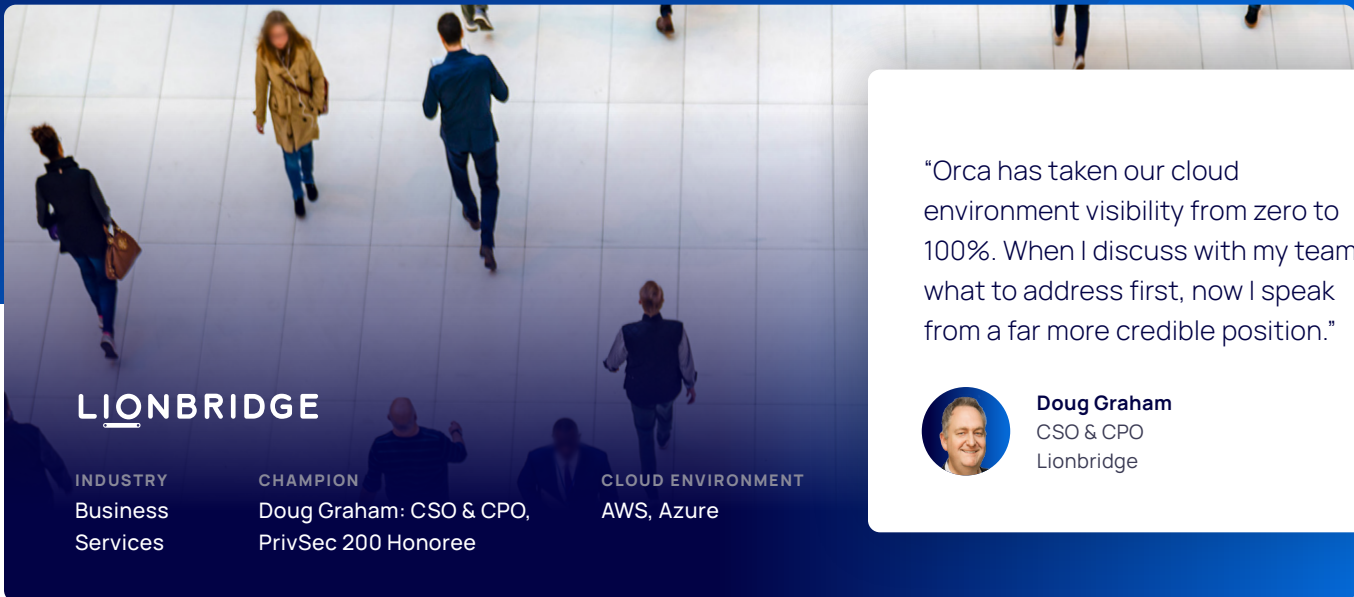


Lionbridge Achieves 100% Visibility into AWS and Azure Environments with Orca Security




LIONBRIDGE

INDUSTRY
Business Services

CHAMPION
Doug Graham: CSO & CPO, PrivSec 200 Honoree

CLOUD ENVIRONMENT
AWS, Azure

“Orca has taken our cloud environment visibility from zero to 100%. When I discuss with my team what to address first, now I speak from a far more credible position.”

 **Doug Graham**
CSO & CPO
Lionbridge

Cloud Security Challenges

- ✗ Needed holistic vulnerability management for multi-cloud environment having multiple accounts and subscriptions
- ✗ Different business units and technology solutions across multiple cloud providers made it difficult to establish standards or implement CIS security controls
- ✗ Legacy tools would require deploying cumbersome agents

Cloud Security Results

- ✓ Gained 100% visibility to assets—to the workload level—and prioritized risks in minutes across multiple clouds and accounts
- ✓ Based on the criticality of vulnerabilities, able to prioritize fixes for fast resolution with far less effort
- ✓ Orca Security integration with Axonius provides a more complete, accurate asset inventory

About Lionbridge

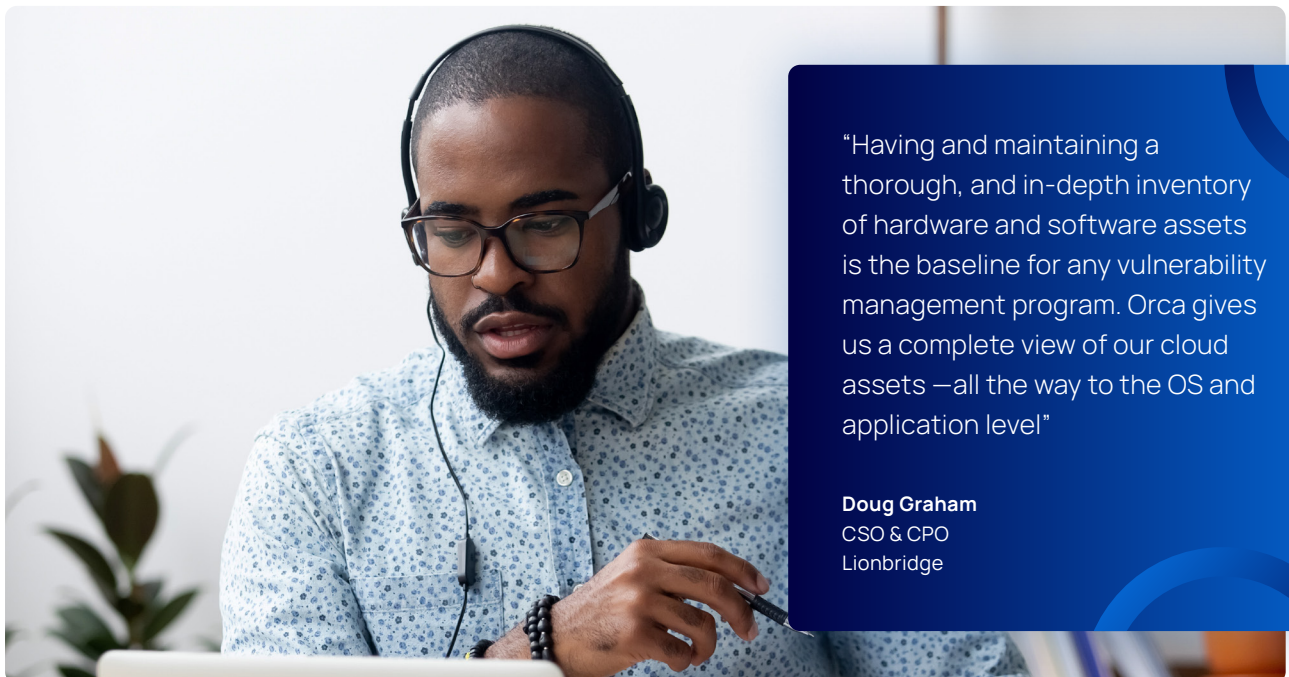
Lionbridge partners with brands to break barriers and build bridges all over the world. For more than 20 years, they have helped companies connect with global customers and employees by delivering localization and training data services in 350+ languages. Through their world-class platform, they orchestrate a network of one million passionate experts in 5000+ cities, who partner with brands to create culturally rich experiences. Relentless in their love of linguistics, they use the best of human and machine intelligence to forge understanding that resonates with their customers' customers. Based in Waltham, Mass., Lionbridge maintains solution centers in 26 countries.

Lionbridge's cloud estate includes multiple AWS accounts and Azure subscriptions. It's a diverse environment requiring strong oversight.

Doug Graham is relatively new as its chief security officer. Coming into the role, he immediately noticed the cloud estate was a diverse environment that included multiple AWS accounts and Azure subscriptions that required strong oversight. Immediately Doug needed to know which assets he was responsible for, how well they were configured, and how effectively they are maintained. "I really needed to understand the state of our infrastructure and have a consolidated view across both our AWS and Azure environments—and I needed it fast," he says.

Understand Assets to Control Vulnerabilities

Graham subscribes to the critical security controls framework established by the Center for Internet Security.



"Having and maintaining a thorough, and in-depth inventory of hardware and software assets is the baseline for any vulnerability management program. Orca gives us a complete view of our cloud assets—all the way to the OS and application level"

Doug Graham
CSO & CPO
Lionbridge

“Control number one, which we can argue is the most critical security control, is that you have to know what your assets are in order to be able to protect them. The next thing you need to know is what’s running inside them from both a software and application perspective. You can’t just protect things at a host level; you have to protect at an application, service and software level, and that dictates what you have to do.”

Orca is the exclusive feed for configuration and vulnerability data for the company’s cloud assets because it’s the definitive source of all things cloud-related.

Orca fills two critical needs for Lionbridge: cloud asset management and vulnerability management via a single pane of glass. “With a very simple configuration that took just minutes to put in place, Orca showed us exactly what’s running in our clouds and the security status of our environments. There’s little upfront work required for a very fast turnaround time to get detailed visibility of what we need to protect, and what we need to do to eliminate the vulnerabilities and reduce risk,” says Graham.

Orca Fulfills What Cloud Computing Has Promised

“The promise of cloud computing is that you’re not doing any manual configurations of devices. Everything should be deployed by scripts or automation and orchestration tools. You should have a CI/CD and immutable images. Infrastructure should be run as code so everything is deployed that way,” Graham says.

“That’s the nirvana everybody is trying to get to, but the reality is that everyone has some aspects of the

cloud that are spun up or configured manually. This lack of automation means resources get created, abandoned, and forgotten. Yet they’re still taking up workload and space. They have real costs and risks associated with them. Orca addresses this problem in full.

“Orca does what the concept of cloud and its automation, scripting, and orchestration have promised us,” he says. “It’s reading the workloads’ run-time block storage, and it’s enumerating the types of hosts based on what’s deployed. It’s highly accurate and very fast because Orca does what it promises—read the configurations back to you with a high degree of accuracy and reconstituting the picture of what you’ve got deployed.

“Then Orca organizes the information in a way that’s useful to analyze from a security perspective. Orca prioritizes alerts based on the reachability of the asset, criticality of vulnerabilities, the difficulty of potential attack, and any presence of an exploit kit.

“Orca represents the next generation of vulnerability management,” Graham says. “Sure, anyone can say ‘Okay, the device has a vulnerability’, but Orca also asks, ‘Is it accessible? Can it be exploited?’ With Orca, you can leap into the analysis of what you have, which then leads to our action plan.”

Easy Deployment and Use Without Agents

Before deploying Orca, Lionbridge had limited visibility into its two cloud environments, but now they’re 100% visible. Graham appreciates the ease of deployment—especially Orca’s lack of reliance on agents. “If I hadn’t come across Orca, I would

still need some way of collecting cloud asset and configuration information. It would've taken much more time to build the picture. I probably would have tried using the native tools of AWS and Azure; that would've required deploying agents and I would still need to reconcile the two cloud environments."

Graham says Orca has saved them a lot of resources. He speculates he would have had to devote a full-time staff member to build and then maintain a system to gather the data Orca produces in minutes. "Even if we built our own tool to gather information across our clouds, someone would have to take the results, and do some sort of risk filtering, and then assign them to people in a prioritized manner to have the issues fixed. With Orca's approach, it's already prioritized in a risk model based on the accessibility of the asset and the criticality of the vulnerability—not just CVSS scores."

More Than a Security Tool – Orca Also Provides Value to DevOps Team

At Lionbridge, those running the cloud infrastructure also have full access to Orca. Graham says, "Our philosophy is that the orchestration we get from our security tools have to be available to everyone doing the work."

As Orca was deployed, all DevOps teams and infrastructure engineers were able to use it to drive their own process and application assurance. Now Graham's security team can verify what they're doing with a 'trust and verify' approach. This helps Lionbridge "shift left" with an approach that incorporates security in the earliest stages of development.



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.



Connect your first cloud account in minutes and see for yourself: [Visit orca.security](https://www.orca.security)

