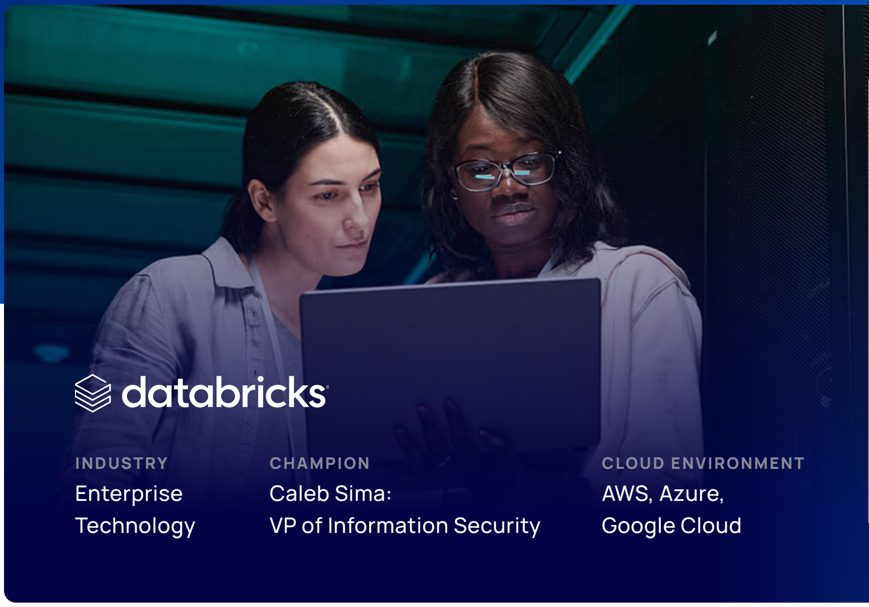
Orca Security Is a No Brainer Choice for Databricks



INDUSTRY
Enterprise Technology

CHAMPION
Caleb Sima: VP of Information Security

CLOUD ENVIRONMENT
AWS, Azure, Google Cloud

> “Orca Security provides similar capabilities to what agents on boxes do and more, but with no impact on engineering. It’s beautiful. Exactly what I want.”

Caleb Sima
VP of Information Security
Databricks

Cloud Security Challenges

- ✗ Gain visibility into everything that’s running without having to deploy agents
- ✗ Accurately assess vulnerabilities and risks, prioritizing them for remediations
- ✗ Support for a multi-cloud estate
- ✗ Avoid friction with software engineering

Cloud Security Results

- ✓ Gained visibility through risk-prioritized alerts that are accurate, actionable, and in context
- ✓ Able to address all major security issues; now monitoring smaller ones
- ✓ A single out-of-band tool provides vulnerability identification, asset inventory, monitoring, and detection of what’s happening on all cloud systems
- ✓ The technology is totally within the security team’s control

Databricks Manages Risk to Help Customers Succeed

Databricks is a leading data analytics and machine learning company. Today more than five thousand organizations worldwide – including a range of Fortune 500 companies – rely on Databricks to enable massive-scale data engineering, collaborative data science, full-lifecycle machine learning, and business analytics. The company has hundreds of global partners, with notables such as Microsoft, Amazon, Informatica, and Cap Gemini among them.

As an enterprise technology company that is part of its customers' and partners' supply chain, Databricks places a premium on monitoring and managing its own risks to earn and retain their trust. It invests in top-quality security products and vendors to provide that assurance.

Databricks operates a multi-cloud environment using AWS, Azure, and GCP. Operating on all three platforms makes it difficult to use the cloud operators' native tools for uniform security across the board. Thus, selecting the right tools to maintain a secure environment is paramount.

Security Entrepreneur Calls Orca "Simple and Brilliant"

Caleb Sima heads up the company's Vice President of Information Security. For much of his career, he was a serial entrepreneur who launched, developed, and sold several cybersecurity companies. A few years ago, Sima pivoted his career from founder and entrepreneur to become a defender inside of companies. This gives him a unique perspective on the best types of technologies to deploy to defend and protect Databricks' applications and cloud environments.

> "The entrepreneur in me said, 'That's it!' This is so obvious and simple, but just brilliant. It's a no-brainer."
>
> **Caleb Sima**
> VP of Information Security
> Databricks

“When I joined Databricks, I had the opportunity to build my security team from scratch. Together we evaluated and chose the tools for our security stack,” he says. An important criterion was to stay out of the way of Databricks’ software engineering team. “We’re a fast-moving company and I wouldn’t want to do anything to slow our engineers’ progress. Our technology stack is changing so fast that installing agents on resources would be challenging and complex.”

“Once I heard about it, I really wanted to see the Orca demo. What piqued my interest was learning how it works by basically taking disk snapshots and analyzing them for activity and vulnerabilities.”

Agents Create Complexity; Complexity Adds to Risk

Sima knew he didn’t want a product that uses agents on machines especially when it comes to critical infrastructure and hosts.

> “Orca risk-prioritizes alerts in a way that’s very actionable in terms of both the information that is provided and the level of security that is given. This is top-notch and pure magic.”
>
> **Caleb Sima**
> VP of Information Security
> Databricks

“It’s a lot of wasted effort – for both security and engineering – to make an agent-based solution work,” he says. “Every vendor with an agent says they are lightweight. The issue is not about CPU power but about adding more risk. The more things you load into a system, the more complexity you add, and the more risk that something can go wrong.”

Orca’s Value Was Obvious Right Away

Databricks signed up for a POC and quickly had Orca up and running. All it had to do was set up some cloud account permissions. Within hours, Orca was showing results in its dashboard. Sima and his security colleagues couldn’t believe what they were seeing. “I remember looking through the alerts and being amazed,” says Sima. “At first we thought we were looking at false positives. Then we checked for ourselves and learned that every alert was spot-on.”

Databricks had several challenges it was hoping to solve with a solution such as Orca. The initial push was to get visibility on everything that’s running without having to install agents on boxes. They were also looking for a tool that could help with cloud monitoring, detection, and response. And it wanted to identify risks in all of its cloud environments. “Somehow Orca has struck a balance among these needs, meeting all of our criteria. “That all cloud environments can communicate together – and with Orca – gives us a higher-level picture of our overall risk.”

“Our top pain point was around visibility of our cloud workloads, instances, and machines,” Sima reports. “The POC showed us that not only could we see what is happening, but that Orca could also tell us that something might happen. That is, ’Here are lateral movements that could occur and the kind of resources an attacker could potentially access.’ Such insights are incredible, so we saw the value right away.”

Sima most appreciates Orca’s accuracy and level of depth on findings. “You can do things like detecting that there’s a large amount of failed SSH logins on this box that also happens to contain keys, which access these boxes, which also contains an AWS credential that can access this infrastructure. Clearly, this box is under attack and it’s also over-privileged, which is all true. And you can do that and communicate that in a fairly understandable way to anyone in the organization,” says Sima. It’s super helpful.”

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