CASE STUDY I SISENSE

Orca Security Alerts “Just Make Sense” to Sisense, Quickly Pinpointing Critical Vulnerabilities Across Hundreds of EC2 Instances

INDUSTRY	CHAMPION	CLOUD ENVIRONMENT
Cloud	Aaron Brown: Senior Cloud Security Engineer	AWS

> “We deployed Orca Security in seconds—literally. It took me less than three minutes to get a cloud environment up and running.”

Aaron Brown
Senior Cloud Security Engineer
Sisense

Cloud Security Challenges

- Continuously growing AWS estate
- Commercial, homegrown and native tools, but no comprehensive solution
- Lean security team requires actionable insights

Cloud Security Results

- Fast visibility into misconfigurations, vulnerabilities, exposed ports, outdated AMIs, secret keys, and more
- Eliminates manual work—pinpoints critical vulnerabilities for quicker remediation
- Extensible via open APIs to integrate with Slack, Jira, and AWS security tools

Sisense Helps Simplify Complex Data for 2,000+ Customers Worldwide

Sisense is a business intelligence and analytics platform for simplifying complex data preparation and analysis. Its hybrid cloud infrastructure enables data engineers, developers, and product managers to build analytic applications that deliver highly interactive user experiences. More than 2,000 global customers—including large enterprises, Fortune 500 companies, smaller startups, and nonprofits—rely on Sisense.

A key requirement was a solution's ability to perform attack surface monitoring across his entire cloud infrastructure. Brown says, "I wanted to identify vulnerabilities and review any exposed ports across all of our EC2 instances. Protecting ports is critical to keeping any infrastructure secure."

Scalable Cloud Security Solution Required

Many of Sisense's on-premises, self-hosted clients are evaluating switching over to its managed service offering, hosted on AWS. Brown had a pressing need for a robust cloud security solution—one featuring a high degree of automation and scalability. "Scaling our managed service business and acquiring new customers means managing more EC2 instances. We needed a solution that could accommodate such growth without draining security team resources and their time."

Other Security Tools Don't Meet Its Needs

Sisense leveraged available commercial, home grown and open source tools, but found challenges locating the right mix to provide total insight regarding its cloud security posture.

The team wanted deeper, workload-level visibility, better dashboards, and more automation.

Brown and his team considered using a Cloud Security Posture Manager (CSPM). "Most CSPMs are just wrappers around AWS Config, yet they are still very heavy tools. There is a lot of noise and distraction because they are unable to filter out non-critical alerts," he discovered.

> "Orca Security is unique in that it locates vulnerabilities with precision and delivers tangible, actionable results- without having to sift through all of the noise."
>
> **Aaron Brown**
> Senior Cloud Security Engineer
> Sisense

SideScanning™ Increases Visibility with No Impact to the Production Environment

Orca's patented SideScanning™ technology, delivered as SaaS, reads cloud block storage out-of-band—none of its code runs within the cloud environment. With that and cloud account metadata, it builds a read-only view that includes all operating systems, applications, and data. Orca then scans the view for vulnerabilities, malware, misconfigurations, secret keys, weak passwords, lateral movement risk, and high-risk data such as PII.

Fast Implementation, Deeper Visibility, Actionable Results – And No Noise

Once Brown's team had deployed Orca, Sisense began seeing benefits straight away. "We deployed Orca Security in seconds—literally. It took me less than three minutes to get a cloud environment up and running."

Orca surfaces all metadata—such as the account, where an instance resides, and the direct path to issues that need fixing. Brown reports, "Orca is unique in that it locates vulnerabilities and delivers tangible, actionable results. Whereas other tools may provide an IP address—which requires us to run a script to pinpoint the misconfiguration or vulnerability—Orca provides a clear and immediate path."

"Orca looks at all EC2 instances across the entirety of Sisense cloud environments. With respect to AMIs, it lets us consider vulnerabilities that might lie within. It focuses on those areas of real concern—such as finding private keys stored alongside a public key pair. Examining all of our cloud accounts and production instances, we've discovered other issues—such as finding data that should be ephemeral, is actually persisting within our containers."

Easier Patches and Updates

Orca helps Sisense with automated patching, too. Brown explains, "In AWS you can set up your own operating system, such as Ubuntu, for a system to run on, and if the OS is stable, it'll roll that version within the AMI. An older OS version might have vulnerabilities within that AMI. Orca Security surfaces those OS-related vulnerabilities so our engineers know when to send an update, a patch, or switch to a new AMI."

Open APIs Enable Valuable Extensibility

For Brown, another big benefit Orca provides is its ability to integrate with other technologies via open APIs. Leveraging these, Brown plans to simplify regulatory compliance by creating a dashboard that provides a unified view of relevant data. "Being an engineer myself, it's great to know we're able to build on top of its platform to enhance our chosen solution—one that further solves all of our challenges now and in the future." Brown says he plans to integrate Orca with Slack and Jira so as to receive alerts and create tickets.

“Orca gives us insight into everything that’s being spun up and AWS assets that may be misconfigured. Orca heightens our awareness of potential threats in the cloud environment, and helps us in making sure it’s secure.”

Orca Security Delivers Cross-Functional Benefits

Orca Security provides benefits not only for Sisense’s security team, but also its platform team, cloud operations team, and its architects.

“Anybody in an engineering organization or who is deploying artifacts into a cloud environment will benefit from Orca Security. It gives us insight into everything that’s being spun up and anything that may be misconfigured. Orca heightens our awareness of potential threats in the cloud environment, and helps us in making sure it’s secure.”

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