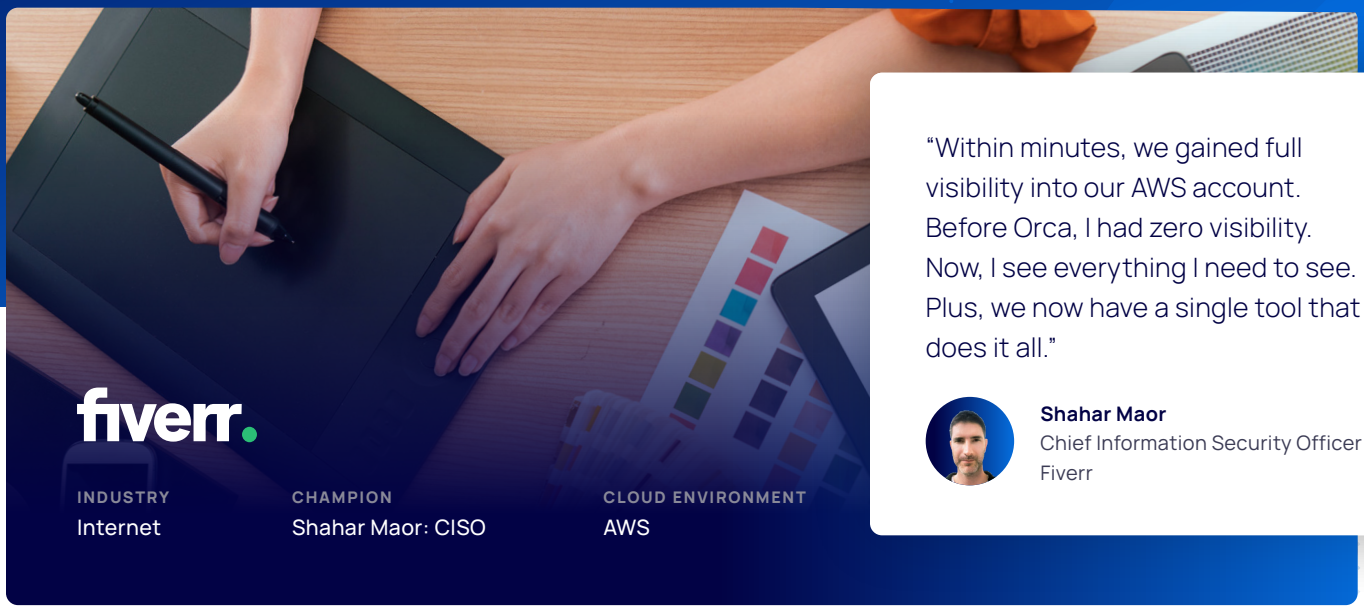
# Fiverr Replaces Multiple Tools with Orca Security to Gain Immediate and Complete Visibility into AWS Assets



fiverr.

INDUSTRY
Internet

CHAMPION
Shahar Maor: CISO

CLOUD ENVIRONMENT
AWS

"Within minutes, we gained full visibility into our AWS account. Before Orca, I had zero visibility. Now, I see everything I need to see. Plus, we now have a single tool that does it all."



**Shahar Maor**
Chief Information Security Officer
Fiverr

## Cloud Security Challenges

- No way to understand the full context of what was happening across AWS
- AWS and open source tools were time-consuming and ineffective
- Flooded with thousands of alerts that nobody has time to review

## Cloud Security Results

- Deep cloud inspection identifies malware, misconfigurations, "secrets", weak passwords, and PII
- Saves hours of work per week, less reliant on DevOps, and no overlooked assets
- Alerts now prioritized based on environmental context, pushed to Slack, and resolved

## Rapid Global Expansion Calls for AWS Cloud Security at Scale

Founded in 2010 and headquartered in Tel Aviv Fiverr (NYSE: FVRR) is a vast online global marketplace for freelance services. Its platform enables freelancers to offer services to customers worldwide while helping businesses find services they need simply by browsing a catalog or conducting a search.

Fiverr's platform has served over 5.5 million businesses and facilitated over 50 million transactions. With so many people accessing the platform, maintaining a secure AWS infrastructure is crucial.

## Fiverr's CISO Shahar Maor Knew that Securing Cloud Environments is a Complex Affair

"I was the first full-time security professional Fiverr hired," reveals CISO Shahar Maor. "Although security was already deeply embedded in Fiverr's culture."

Maor's initial analysis of the AWS infrastructure pointed to potential attacks from external vectors, hackers, malicious bots, and viruses. But he knew that in a cloud environment, there's more than meets the eye.

"Often, organizations assume that if they protect the perimeter, that's sufficient, and the cloud infrastructure is often overlooked," Maor said. "You might not think about the fact that a misconfiguration on the platform itself could be an issue. It's a misconception to think that if you have a cloud-native infrastructure that you see it more clearly. There are a lot of complexities when securing cloud environments."

Maor had concerns about platform users having weak passwords, and the potential for malware to be run on AWS servers. "When I first mapped the risks against our high-value assets, it was evident we had blind spots. Plus, I was spending way too much manual time monitoring assets—especially the AWS S3 buckets—to make sure nothing was exposed. It was very tedious."

## The Ideal Solution Needed to Provide Deep Visibility Across All AWS Assets

With specific requirements in mind, Maor set out to find an AWS cloud security solution. We needed a solution that could provide complete visibility

"Often, organizations assume that if they protect the perimeter, that's sufficient, and the cloud infrastructure is often overlooked."

**Shahar Maor**
Chief Information Security Officer
Fiverr

into our AWS environment while also scanning for malware, identifying misconfigurations, and protecting PII."

The optimal cloud security tool would be a comprehensive solution for identified risks, as well as provide actionable insights and value across IT, DevOps, and engineering. Additional goals and requirements for an AWS security solution included:

- No agents to manage
- Complete visibility; no overlooked assets
- Search for and protect PII
- Perform health checks on servers
- Identify weak passwords
- Find misconfigurations
- Look for "secrets" left in existing code
- Monitor exposed assets, such as S3 buckets
- Simplify regulatory compliance, particularly for PCI

"We needed a solution that could provide complete visibility into our AWS environment while also scanning for malware, identifying misconfigurations, and protecting PII."

**Shahar Maor**
Chief Information Security Officer
Fiverr

## Native Tooling, Legacy Scanners, and Agent-based Approaches Weren't Going to Cut It

Maor understood that Fiverr's cloud environment had unique requirements that many available cloud security tools couldn't meet. "Native tools such as Amazon Inspector or GuardDuty provide basic functionality, but they don't correlate logic with incidents or understand the full context of what's happening. You still have to analyze logs and invest more time to make sense of the data. They're better than nothing, as are open-source tools, but there's no workflow for delivering findings to your teams to take action."

Maor added that scanners and agent-based tools are very limited. "Some commercial tools scan a server for vulnerabilities, but that's it. In short, these tools create more work, and they require domain expertise and additional tools to work effectively."

## Single Tool Does It All

Maor sees Orca Security as a one-stop-shop for reducing risks hiding inside Fiverr's AWS infrastructure. "Orca provides a holistic solution for mitigating risk in Fiverr's datacenter. The unique method Orca uses to scan AWS proved to be the most suitable for us, and it won over our DevOps team. Plus, we now have a single tool that does it all."

## Orca SideScanning™ Eliminates Need for Agents, Has No Impact on Performance

Running security agents on individual virtual machines requires ongoing management and administration. Instead of that approach, Orca runs as a SaaS service with read-only access to the customer's AWS, Azure, and/or GCP workloads' run-time block storage. It reconstructs bits and bytes from the snapshot to build out a virtual, read-only view of the operating systems, applications, and data—then scans them for vulnerabilities and risks.

"Orca is extremely lightweight and has no impact on the network whatsoever," says Maor. "You get visibility without any interference with the instance itself. Orca simply creates a copy, reads it, analyzes findings, then presents them in a dashboard for us to review."

## Meaningful, High-Value Alerts without the Noise

Orca Security's patented SideScanning™ technology automatically discovers every asset in a customer's environment. This provides security teams with immediate visibility into compromised resources, vulnerabilities, malware, and misconfigurations. By combining such information with environmental metadata, Orca sends alerts within context to enable effective prioritization.

"Orca sends meaningful, actionable alerts in real-time to bring our attention to a threat, instead of creating tons of logs and thousands of alerts that nobody reads or has time to review. We get Slack alerts on every critical finding. If Orca uncovers a new vulnerability, we know about it immediately."

## Simplifying Regulatory Compliance

Additionally, Orca Security simplifies regulatory compliance. "PCI requires us to scan our environment—and because it's serverless, that presents unique challenges. Orca's solution lets us scan both EKS and ECS containers, providing good coverage for PCI."

"Orca Security sends meaningful, actionable alerts in real-time to bring our attention to a threat. If Orca uncovers a new vulnerability, we know about it immediately."

**Shahar Maor**
Chief Information Security Officer
Fiverr

## Complete Visibility, Minimal Effort

Soon after implementation, Orca surfaced vulnerabilities that Maor's team was able to address. "Orca Security delivers valuable insights and the ability to extend Fiverr's security posture. Before Orca, I had zero visibility. Now, I see everything I need to see."

For Maor, that was validation that Orca Security is all he needs. "I still have both Orca and a CASB implemented, but on my next renewal, I'll be removing the CASB because it's not providing any insights," he said. "I'll be relying solely on Orca for monitoring the AWS production environment, end-to-end."

## Saving Hours per Week, No Need to Rely on DevOps

Maor now spends half the time he used to on cloud security work. "Orca has eliminated hours of work every week with regard to cloud security maintenance and administration work. Plus, I don't have to rely on DevOps for support."

As an added bonus, Maor is able to rely on Orca Security's team for recommendations and expertise. "The Orca team brings an extensive background and practical knowledge in security, together with amazing agility and flexibility. We're already seeing tons of value from Orca, and we're excited to grow with it as our main AWS security platform."

## 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)