REPORT REPRINT

Coverage Initiation: Orca Security looks to offer cloud security with a light, agentless touch

JUNE 8 2020

By Fernando Montenegro

Cloud security is a key concern for many organizations, and security teams want a comprehensive view of their environments with minimal friction. Orca Security is bringing to market an approach based on out-of-band scanning that aims to address this imbalance.

451 Research®
Now a Part of
S&P Global Market Intelligence

Introduction

When discussing how security teams can better support cloud environments, it is not uncommon to hear complaints from other stakeholders about just how much friction security adds to the process of securing cloud. For many security teams, there's also the struggle of being asked to evaluate cloud environments after they've been deployed to production, where retrofitting security controls may be an expensive proposition. Orca Security is bringing to market an approach to assessing the security of cloud environments that sidesteps some of the friction concerns by using out-of-band scanning of cloud resources.

451 TAKE

Security teams tasked with getting a grip on cloud security often struggle with two key issues: how to get proper visibility into the cloud environments, and how to do that without causing friction that would cause conflict with cloud engineering. Orca Security's approach of performing out-of-band scans via access to the underlying cloud storage, then using cloud metadata to better model and prioritize findings, provides an alternative to methods such as deploying agents or performing network-based scans. The company is aiming for security buyers looking for the quick time to value and lower friction of this alternative approach to broad coverage of cloud security, just as it also looks to expand its capabilities and support to more enterprise use cases and needs.

Context

Orca Security is an Israeli startup that was founded in 2019 by Avi Shua, Ety Hubara, Gil Geron and others. The company has approximately 40 employees split between Israel and the San Francisco Bay Area. Many of the original founders, including CEO Shua, hail from Check Point.

The company has raised approximately $27m, after announcing its $20m series A in early March. That round was led by GGV Capital, and included participation by YL Ventures, which had led Orca's earlier seed round, as well the new Silicon Valley CISO Investments group.

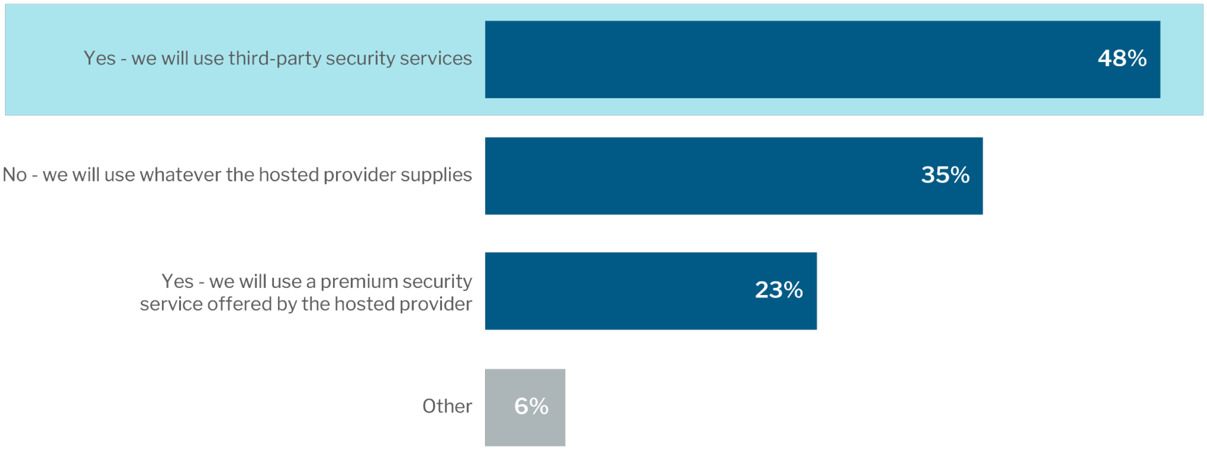
Market

Orca Security's offering falls into 451 Research's coverage of the cloud security market. We further divide this market into cloud access security brokers, cloud workload protection, cloud infrastructure security and cloud-native security. Orca's offering is aligned with Cloud Workload Protection, which revolves around understanding and securing cloud-based assets.

This particular subsector is affected by increasing overlap with cloud infrastructure security (validating cloud security posture from the perspective of cloud account configuration, not assets), some overlap with endpoint security (particularly in the context of server workloads) and growing adoption of technologies such as container-based applications and Kubernetes orchestration.

Data from 451 Research's Voice of the Enterprise research program indicates that, when it comes to cloud security, many customers are looking to complement existing features from their cloud providers with third-party security tooling.

Do you plan to acquire additional security services for your hosted architecture in 2019?



Source: 451 Research's Voice of the Enterprise: Information Security, Budgets and Outlook 2019

Strategy

Orca Security's main thesis is that it can leverage the underlying capabilities of cloud environments themselves – notably the access to the runtime storage components of cloud workloads, as well as the cloud management APIs – to provide security functionality with minimal friction and broad coverage.

The company's message is aimed primarily at security teams, although it often sees cloud engineering teams as key stakeholders. The company indicates that it has grown to dozens of customers of different sizes and verticals in North America, Europe and Asia-Pacific. Orca claims its midmarket customers value the overall security functionality, while larger customers appreciate the ease of deployment, which allows them to get broader coverage in fragmented organizations.

Moving forward, the company is planning to emphasize how it treats its offering as a platform, as well as to add more security functionality such as file integrity monitoring. It is also making progress on updating its user experience and enterprise integration features.

Technology

Orca Security aims to deliver security visibility and functionality to cloud environments via an out-of-band service that, without using agents, analyzes both the cloud environment metadata and the actual runtime state of the disk images associated with each workload. As the offering analyzes the metadata and disk images, it builds a model of how the cloud environment is configured and checks for many security issues, such as vulnerabilities, presence of malware, misconfigurations, and authentication issues due to weak credentials or sensitive data. Orca also verifies the cloud configuration and workloads for compliance with various frameworks, such as CIS.

The offering is aimed at providing insight into cloud security without the associated friction of installing workload agents or performing network scans. The most common scenario for deploying Orca is where a security team needs to obtain visibility and later control over a sprawling cloud environment that is being created and operated independently. The company mentions that it often comes across what it calls 'neglected workloads,' which are systems that, while still operational, haven't been properly maintained by the appropriate teams, sometimes for years, although they are being used by the business units.

Orca is deployed primarily as a SaaS offering. The typical deployment model is for customers to give Orca read-only access to their cloud environments. The company offers predefined AWS, Azure and GCP guidance on how to do this with features such as CloudFormation. The option exists for customers to also run a modified version of the service within their own cloud accounts, if needed.

Once deployed, the product will scan cloud metadata, cloud-based storage and container repositories. The company uses what it calls 'SideScanning' technology to leverage the inherent efficiencies of cloud-based block storage and access runtime disk images without performance penalties. As data is surfaced and analyzed, it can be visualized on a Web UI or integrated with other environments via Orca's own API.

Orca will scan the environment in two ways – it collects metadata on a regular/near-real-time basis, and will scan the disk images on a periodic basis (typically daily). It uses cloud metadata to understand which workloads may be internet-accessible or accessible given specific account permissions.

As it analyzes the disk images, it builds an asset inventory, then looks for a variety of security-relevant information: evidence of vulnerabilities, such as older components; misconfigurations on systems or artifacts; existence of sensitive information, such as credentials/keys; personally identifiable information; or other sensitive information.

As it catalogs and analyzes findings, Orca will use the insight from the metadata analysis to prioritize systems that may be more exposed or highlight how artifacts such as SSH keys can be used to perform lateral movement in an environment. As issues are discovered, they can be filtered in the UI or sent to additional systems for further processing.

Competition

The functionality that Orca is providing ends up translating to competition on distinct fronts. First and foremost, it compares to that of vulnerability scanners, be they agent-based or network-based. It also touches on some of the functionality from the cloud security-posture vendors that evaluate a company's cloud presence for issues. Finally, it touches on areas such as malware scanning and container security.

Rapid7, Qualys and Tenable are well known for their offerings in vulnerability management, whether agent-based or network-based. Additional vendors in the space include BeyondTrust, Tripwire and Acunetix. From an open source perspective, OpenVAS is one of the better-known options.

For cloud security-posture management, the field is quite broad and includes established security vendors such as Palo Alto Networks, Trend Micro, Sophos, Qualys and Rapid7 (via the recent acquisition of DivvyCloud). There are also several more recent entrants to the space, including but not limited to Aqua Security, Fugue, Turbot, Lacework, Cavirin and others.

For malware scanning, Orca will typically compete with agent-based offerings from vendors such as Trend Micro, Palo Alto Networks, Broadcom, McAfee, Crowdstrike and others. For container security functionality, it will compete with vendors such as Palo Alto Networks, Trend Micro, Aqua Security, Sysdig, NeuVector and others.

Orca is hoping to differentiate by combining the functionality and aggregated context of several disparate security tools with the ease of deploying its offering and the overall simplicity of an agentless approach.

SWOT Analysis

STRENGTHS

Orca's combination of SaaS delivery, SideScanning technology and access to cloud configuration APIs provides security visibility and context into different aspects of cloud security with less friction than agent-based approaches.

WEAKNESSES

Orca scans the environment periodically, so it may not be applicable to organizations that depend on real-time protection of their assets or use real-time information as part of their decision-making policies for security controls.

OPPORTUNITIES

Many organizations struggle with how to properly insert security functionality into cloud environments without undue impact to performance and agility, and are looking for approaches that can meet security needs with low friction.

THREATS

As more organizations mature their application architectures and security practices in cloud environments, they may favor deploying security controls elsewhere in the application lifecycle or using alternative controls.