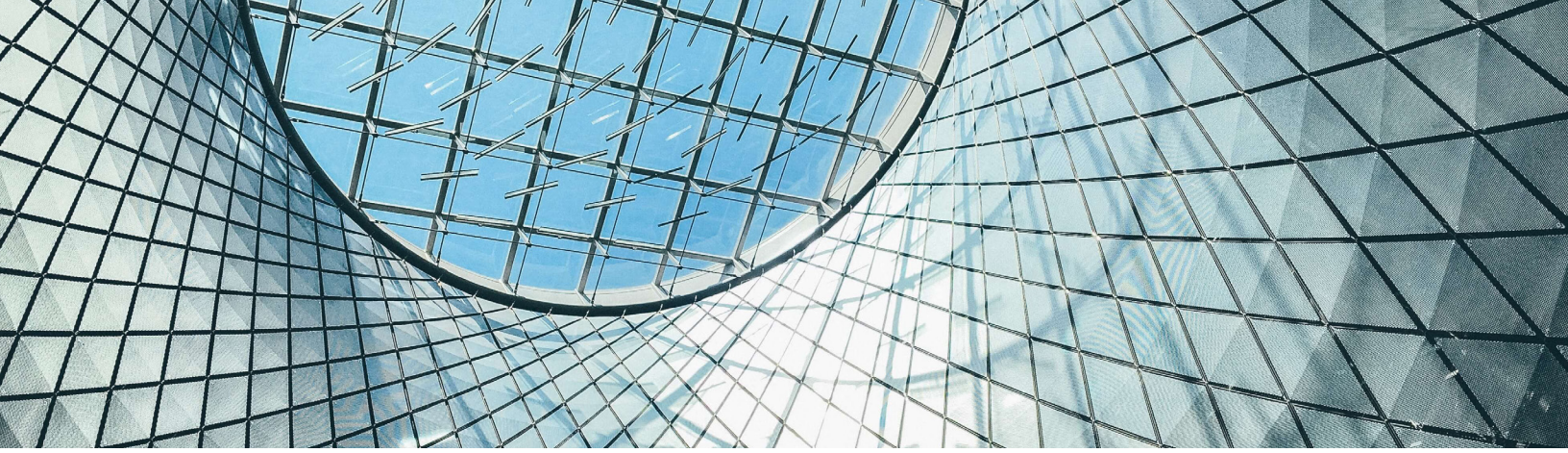


451 Research Market Insight Report Reprint

Orca Security continues its CNAPP momentum

May 13, 2024

by Mark Ehr

The company is making inroads into the cloud security market by expanding its organically developed cloud-native application protection platform, supporting all major cloud hyperscalers and providing coverage from development through production deployment. A partnership with Aqua Security will further strengthen Orca's runtime protection capabilities.

S&P Global
Market Intelligence

This report, licensed to orca, developed and as provided by S&P Global Market Intelligence (S&P), was published as part of S&P's syndicated market insight subscription service. It shall be owned in its entirety by S&P. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from S&P.

Introduction

Orca Security has steadily evolved since we began covering the company in 2022, organically growing its cloud-native application protection platform, adding new customers and expanding its footprint within existing accounts. Morphing from an entirely agentless to an agentless-first strategy has allowed the company to offer the additional capabilities that agents provide, to better compete with other top players in the cloud security space. Orca is also known as an early innovator in cloud security, and customer feedback is typically positive.

THE TAKE

Orca's approach is attractive for several reasons: Its comprehensive suite of security capabilities, cloud-native architecture, multicloud support, graph technology, search capabilities and compliance capabilities allow it to satisfy use cases that span detection, investigation, response and compliance. The company provides a wide set of capabilities through its platform. These include cloud workload protection (CWP), cloud detection and response (CDR), cloud security posture management (CSPM), data security posture management, cloud infrastructure entitlement management (CIEM), container and Kubernetes security, and API security. It also features flexible graph technology, attack path visualization and advanced search capabilities that share a common unified data model. Orca has added support for ThreatOptix's agent-based technology, which adds deep virtual machine, container and Kubernetes Linux telemetry to its platform.

Context

Orca was founded in 2018 in Israel, and is now headquartered in Portland, Ore. It has raised a total of $632 million in venture funding, with the last round, a $550 million series C, led by Temasek, in 2021. Other investors include CapitalG (Alphabet Inc.'s venture growth fund), Redpoint Ventures, GGV, ICONIQ Capital, Splunk Ventures and SAIC. The company reports hundreds of customers, primarily medium-sized to large enterprises, and over 350 employees.

Orca's founders and executives are information security industry veterans, many with a heritage at Check Point Software Technologies Ltd., including co-founders Gil Geron (CEO), Avi Shua (chief innovation officer), Arie Teter (chief product officer) and Yoav Alon (chief technology officer). The company has also attracted leaders from its competitors: Meghan Marks (chief marketing officer, from Palo Alto Networks Inc.) and Raf Chiodo (chief revenue officer, from Lacework).

Products

True to its cloud-native heritage, Orca addresses common challenges that cloud teams face. For developers, security operations and production (IT) operations teams, it provides a DevSecOps platform that solves issues that span development to deployment and runtime. Challenges that Orca looks to solve include a lack of visibility into cloud environments (amplified in multicloud organizations), skills shortages and knowledge gaps, high rates of environmental change, and rapidly evolving compliance requirements. These teams struggle with alert overloads and reduced productivity due to a prevalence of and lack of integration between multivendor toolsets.

©Copyright 2024 S&P Global Market Intelligence. All rights reserved.

Orca lends itself to rapid deployment due to its agentless architecture. It scans production environments through its patented SideScanning technology, which collects data from workloads' runtime block storage, creates a read-only reconstruction of the workload's file system, and performs a detailed risk analysis (typically within 24 hours), with no performance impact on the scanned systems. It can also detect and adapt to changes in monitored environments. The company supports all three dominant cloud hyperscalers (AWS, Google Cloud Platform and Microsoft Azure), plus Alibaba Cloud and Oracle Cloud, providing a wide range of CNAPP (cloud-native application protection platform) capabilities. Orca's platform was organically developed, with the exception of native API security and external exposure capabilities that were led by the RapidSec team, acquired in January 2022.

Orca's CSPM and CWP capabilities provide core capabilities including file integrity monitoring, malware detection and vulnerability scanning. Vulnerability risk scoring aids teams in prioritizing remediation based on context, such as being exposed to potential attackers via a valid attack path. These features also aid in addressing compliance requirements because several compliance regulations require vulnerability management, including PCI DSS, HIPAA, GDPR and FISMA. Orca's platform also provides CDR. Based on its ability to gather, normalize and correlate security data across multiple cloud environments, Orca's security graph technology visualizes the relationship between events in the environment, determining attack paths and recommending remediation actions.

The company has also made significant strides on the DevOps side of its CNAPP offering. As a standard part of CI/CD (continuous integration/continuous delivery) workflows, scanning can be performed on a developer's desktop, container images and infrastructure-as-code templates, along with deployment registries and runtime environments. Vulnerabilities and misconfigurations can be traced far "left," such as where a specific container image came from, down to the Git repository level.

Like many security vendors, the company has embedded artificial intelligence into its offerings for some time, applying so-called classic AI and machine-learning technologies to detect anomalies and derive data-driven metrics. Also like many vendors, Orca has added a generative AI-powered security copilot, designed to aid with staff skill shortages and improve productivity through automation and acceleration of tasks and up-leveling analyst skill levels.

This includes a natural language search interface that enables analysts to quickly investigate potential incidents or security exposures and initiate remediation steps. For example, an analyst can view top detected vulnerabilities by risk, have the AI generate a high-level description of the recommended remediation, and then provide detailed instructions, such as the specific command-line-interface commands required. Orca has also built AI into other components of its platform, such as CIEM, which can examine policies and recommend new ones to eliminate unused or overprovisioned permissions.

The company has also gained credibility through its research arm, known as the Orca Research Pod, which has discovered over 20 major public cloud platform vulnerabilities. Company researchers use data captured from billions of cloud assets on all major cloud providers, which are scanned by the Orca Cloud Security Platform, and publishes the findings through the company website and its State of Cloud Security report. The Research Pod aims to improve collaboration across the cloud-native ecosystem to enhance security outcomes for users.

©Copyright 2024 S&P Global Market Intelligence. All rights reserved.

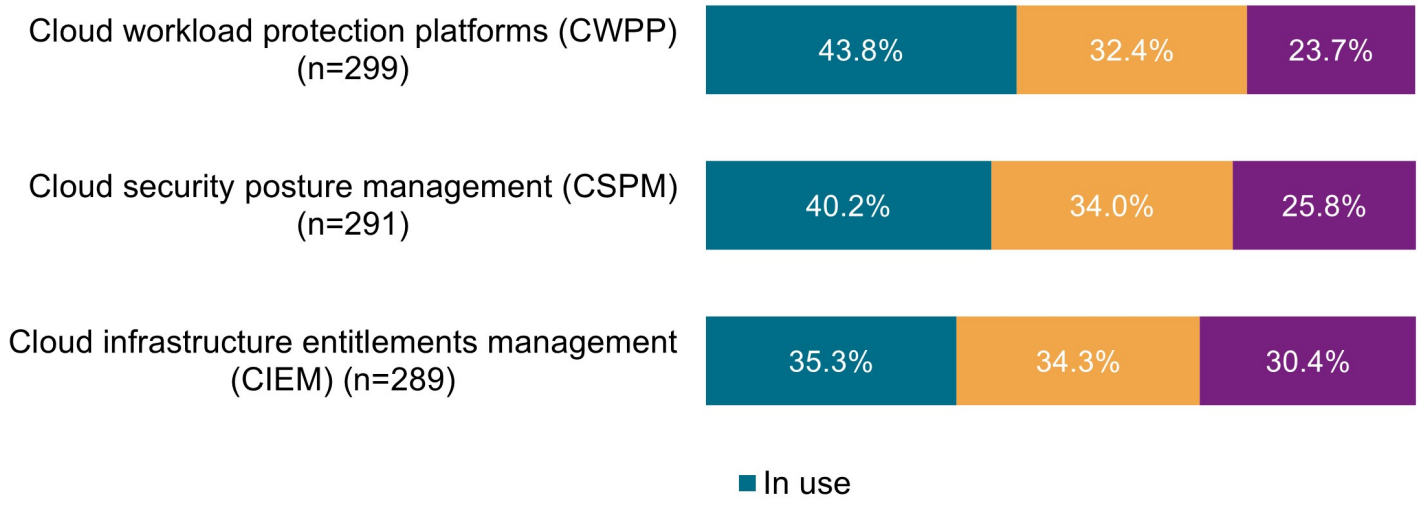
Market

The cloud security market is characterized by rapid growth, tight competition and confusion around what exactly qualifies as a CNAPP. We consider CNAPP table stakes, to include CSPM, cloud workload protection platforms and CIEM at a minimum. Interestingly, many CNAPP vendors are missing some of these capabilities, which they look to provide through partnerships or integrations.

Orca is one of the few cloud-native pure-play vendors that can claim to have an organically developed CNAPP, which could provide competitive advantage over CNAPPs that were built through acquisitions and third-party integrations. CNAPP market consolidation is very active: 15 acquisitions since December 2021 — 10 of them in 2023 alone — and six were over $100 million. We fully expect this consolidation trend to continue as larger vendors seek to flesh out their CNAPPs and expand their customer footprint.

451 Research's Information Security, Cloud Security 2023 study showed that 40% of respondents' total information security tool spending was allocated to securing off-premises cloud architectures, up 7 percentage points from the 2022 survey (33%) and 14 percentage points from 2021 (26%), indicating strong growth in the segment. Our research has also shown that most organizations have two or more cloud providers in use, and yet respondents indicated that only half (49%) of their third-party security tools/services are multicloud, presenting a significant opportunity for vendors that provide multicloud solutions.

Hosted cloud security technology adoption



Q. Which of the following security technologies have you implemented or plan to implement in your hosted cloud (IaaS, PaaS)?
Base: Respondents whose organization uses off-premises cloud architectures.
Source: 451 Research's Voice of the Enterprise: Information Security, Cloud Security 2023.

©Copyright 2024 S&P Global Market Intelligence. All rights reserved.

Strategy

Orca's agentless-first strategy represents a bit of a shift from its original fully agentless approach. We view this as a positive, because it allows the company to continue with its agentless architecture while selectively embracing agent-based telemetry when needed, such as when deeper or more real-time data feeds are required. This gives it a hedge against competitors that are primarily agent-based, while staying true to its heritage.

As organizations increasingly move mission- and business-critical workloads to the cloud, Orca's multicloud agentless architecture will continue to see traction. And while adding generative AI capabilities to the platform is becoming table stakes among security vendors, Orca's copilot shows promise in addressing skills shortages and increasing analyst productivity by automating routine tasks, as well as automatically providing background data and performing incident enrichment, which previously would have been performed manually.

Competition

Orca's biggest direct competitor is Wiz Security, another highly funded startup that is also based on an agentless, graph-based cloud security platform. Other competitors include Palo Alto Networks Prisma Cloud, which offers agentless workload protection, and Lacework, a data-driven platform based on behavioral ML technologies.

Orca recently announced a partnership and integrations with Aqua Security's platform, which will provide enhanced multicloud visibility, integrated views, deployment of Aqua runtime workload protection and drift prevention, ensured immutability, and the ability to block malicious malware across cloud-native workloads using real-time behavioral detection. We are currently tracking over 30 vendors that offer CNAPP capabilities, including large security vendors (Crowdstrike Holdings Inc., Check Point, Palo Alto Networks Inc., Rapid7 Inc., SentinelOne Inc., Symantec/Broadcom Inc., Tenable Holdings Inc. and Trend Micro Inc.), cloud hyperscalers and many startups.

SWOT Analysis

STRENGTHS

Orca's field-proven agentless cloud security offering is well positioned, and has received good feedback in terms of rapid deployment and the depth/breadth of its CNAPP. Multiple-cloud support across its portfolio is also a key advantage, as is the strategy to acquire telemetry from agents.

WEAKNESSES

Orca's agentless technology, while flexible, lacks the depth of a full agent-based architecture. While the company has made some advances by supporting some agents, lack of real-time telemetry could be an issue for some customers.

OPPORTUNITIES

Orca can exploit weaknesses in other security vendors' portfolios, including unwieldy agent-based architectures and inability to provide a complete single-vendor, multicloud CNAPP. As more organizations move to a cloud-first strategy and increasingly shift critical and sensitive workloads to the cloud, Orca is well positioned to satisfy a full set of cloud security use cases, even more so as its partnership with Aqua matures.

THREATS

Intense competition combined with uncertainty in the CNAPP market could cause potential customers to seek out large incumbent security vendors or leverage hyperscalers' built-in CNAPP capabilities, particularly those with enterprise "all you can eat" licensing agreements.

©Copyright 2024 S&P Global Market Intelligence. All rights reserved.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html

Copyright © 2024 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global keeps certain activities of its divisions separate from each other to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.