Brought to you by Informa Tech
OMDIA

Publication date:
23 Mar 2022
Author:
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: Orca Security Adds Web and API Security with RapidSec Buy

Summary

Catalyst

Orca Security is a provider of cloud security technology, having started with vulnerability management and cloud security posture management (CSPM). Most recently, it has added client-side web security with its first acquisition, namely a start-up called RapidSec.

Omdia view

Digital transformation projects have been dramatically accelerated by the coronavirus pandemic, resulting in a greater enterprise dependence on online channels for interacting with customers, partners, and employees. That also raises even further the profile of such channels for threat actors, who can target them to disrupt an organization's operations or to steal valuable information.

The RapidSec acquisition gives Orca more capabilities to offer to its existing cloud security customers who will now be able to get agentless detection of network security risks and API exposure from the Orca platform.

Why put Orca on your radar?

Orca's core value proposition is the delivery of security posture management and threat detection for cloud assets from an agentless platform. As it integrates the RapidSec technology into its platform, that same platform will be able to discover managed and unmanaged APIs and identify exposure risks associated with an organization's APIs.

Market context

Web security was once a separate activity from enterprise application security (AppSec), with tools such as web application firewalls (WAFs) and runtime application self-protection (RASP) developed specifically to address the requirement. However, the two fields have been converging in recent years as more interactions with customers, partners, and employees have moved online thanks to digital transformation, and even private (i.e., employee-facing) applications increasingly residing in environments such as public clouds and content delivery networks (CDNs). Effectively, all applications are becoming web apps, such that web app security is being subsumed into AppSec.

Thus, security vendors have begun to offer both types of functionality from a single platform. For instance, after building an extensive runtime AppSec portfolio comprising services such as DDoS mitigation, WAF, bot management, and API security, Akamai acquired Guardicore to offer protection for its customers' cloud workloads. Meanwhile, Palo Alto Networks, having assembled a comprehensive set of cloud security tools (many of them through acquisition), now also offers WAF, bot, and API security from its Prisma Cloud platform.

Thus it makes sense for Orca to add RapidSec's client-side web security capabilities to its platform, particularly as both companies offer the ability to strengthen security posture before any attacks have taken place. Its acquisition of RapidSec brings it into the web security market and complements its broader cloud security platform.

Product/service overview

Orca's main claim to fame in cloud security—and the core technology underpinning its product offering—is its so-called SideScanning technology which is its out-of-band (and thus passive) approach to gathering data/telemetry from a customer's cloud estate. It is this data that it analyzes and uses to produce the alerts and recommendations it delivers to customers regarding what they need to do to tighten up their security posture and bolster their defenses. It champions its approach to data gathering as better than the widespread use of software agents in cloud security.

Orca offers the following capabilities delivered by its Cloud Security Platform:

- **Vulnerability management**, where Orca's agentless technology creates a software inventory of a customer's cloud environment, leverages 20+ vulnerability data sources to identify vulnerabilities in it, and prioritizes the riskiest vulnerabilities by considering accessibility and potential business impact.

- Identification and remediation of **misconfigurations**, where the platform inspects the customer's cloud infrastructure, comparing it against some 600 configuration controls across 15 categories, including authentication, data protection, logging and monitoring, network configurations, and system integrity as well as against 40+ industry and regulatory frameworks, including a wide range of CIS control benchmarks, triggering automated alerts to enable a return to compliance.

- Detection of **malware**, using both signature-based and heuristic approaches. Here Orca examines cloud workloads for malware out-of-band, which it argues avoids the operational hit of agent-based scanning. It does this via snapshots taken outside the running environment, detecting malware, and prioritizing it for remediation based on its criticality.

- Discovery of **sensitive data that is at risk** within the customer's cloud infrastructure. Orca detects such data across both the workload and control plane, pinpointing the location and providing masked samples of the data to ease remediation. It leverages context such as the location and accessibility of the assets containing the data, the idea being to identify the greatest risks and reduce unnecessary noise.

- Identification **of lateral movement risk**; where Orca finds unencrypted keys and other exposed credentials with the potential to enable attackers to move around a target's infrastructure to seek sensitive or confidential information and exfiltrate it without being detected.

- **IAM risk**, where the platform detects, prioritizes, and continuously monitors for common and obscure identity and access management (IAM) misconfigurations across the customer's public cloud estate. This includes poor password hygiene, such as commonly used passwords, complex passwords that are reused across multiple applications and services, and highly secure passwords that have been leaked. Orca also checks for excessive permissions.

- **Attack Path Analysis** to automatically show a chain of attack vectors with an integrated Business Impact Score to aid security teams in prioritizing and remediating the greatest risks to their cloud environments. Orca's interactive dashboard allows security teams to explore each attack chain, as well as crown jewel assets, with guidance on how to "break" the attack path and reduce risk to their environments.

Now, with the RapidSec acquisition, Orca adds **web and API security**. More specifically, while technologies such as WAF and RASP focus on the server-side to secure websites and web apps, RapidSec brings Orca monitoring to generate strong headers and content security policies (CSPs) to protect against client-side threats such as cross-site scripting (XSS), clickjacking, formjacking, and Magecart attacks. Importantly, Orca plans to bring in API security capabilities via the acquisition via its existing SideScanning technology to focus on network attack vectors and API risks.

Company information

Background

Orca was founded in 2018 by CEO Avi Shua, CPO Gil Geron, and Chief Architects Liran Antebi and Matan Ben Gur. Shua was previously chief technologist at Israeli firewall heavyweight Check Point, while Geron was also there, most recently as Director of Cybersecurity Gateway and Cloud Products. Antebi and Ben Gur are also Check Point alumni, their last roles there being as architects.

Orca has raised $632m over five funding rounds, most recently announcing a $340m Series C round in October 2021 led by Singapore-based Temasek Holdings. Other investors include Splunk Ventures, an arm of the security incident and event management (SIEM) heavyweight with whom Orca also has a technical integration, and CapitalG, the independent growth fund of Google parent Alphabet.

Current position

The Orca Cloud Security Platform is cloud-delivered and started out providing vulnerability management and CSPM capabilities. However, it has since expanded into contiguous areas such as cloud workload protection (CWPP) and cloud permissions management (CPM) to the point where the vendor now refers to it as a cloud-native application protection platform (CNAPP), using the more recently coined term for a comprehensive set of security technologies for infrastructure- and platform-as-a-service (IaaS and PaaS) environments.

Until recently, additional functionality brought to the platform was internally developed, but in January 2022, the vendor broke with tradition by buying Israeli start-up RapidSec to access its API security capability. The RapidSec technology is now being added to the platform.

As for its charging mechanism, Orca adopts a very straightforward model whereby it charges an annual or three-year subscription for the platform, based on the average number of workloads the customer will be protecting with it. Where the customer has a containerized environment, it charges on a per-host virtual machine rather than by individual container. The fee is an all-in-one (i.e., once the customer buys into Orca, it gets the right to use all and any of the services available on the platform).

Future plans

Orca aims to offer breadth and depth for customers securing multicloud environments. Recently, the company announced several features that are designed to improve an organization's ability to measure and respond to risks, including:

Orca Security Score

Orca Security Score helps security and compliance teams demonstrate the state of their security controls and progress to auditors, top management, the board, investors, and cyber insurance companies. Organizations can use it to benchmark their cloud security against industry peers or across business units, as well as to measure their progress over time. The Orca Security Score is based on factors such as suspicious activity, lateral movement risk, data at risk, vulnerable assets, and the time taken to remediate critical security issues.

From the News Widget

The From the News Widget feature aims to provide organizations with a quick and seamless way to measure the impact of new Common Vulnerabilities and Exposures (CVEs) once new vulnerabilities have been announced. It is a central "window" for viewing press announcements and newly disclosed vulnerabilities mapped to a user's environment. This helps security teams report on the impact of a CVE in a timely fashion and see if their environment is at risk with a few clicks.

Key facts

Table 1: Datasheet: Orca Security

Product/service name	Orca Cloud Security Platform	**Product classification**	Cloud security (CSPM, CWPP, CPM etc.)
Version number	n/a	**Release date**	n/a
Industries covered	All	**Geographies covered**	Global
Relevant company sizes	All	**Licensing options**	Per workload/asset
URL	https://orca.security/	**Routes to market**	Direct and channel
Company headquarters	Portland, OR, US	**Number of employees**	±275

Source: Omdia

Analyst commentary

Thanks to the agentless approach it calls SideScanning, Orca has been a rising star in the cloud security market in recent years. It has already expanded its Orca Cloud Security Platform beyond its origins in CSPM and vulnerability management and is clearly en route to offering a full CNAPP (i.e., a comprehensive set of security capabilities for IaaS and PaaS environments). Bringing it client-side web security, the RapidSec acquisition is a logical extension of that process.

Once the RapidSec technology is fully integrated into the Orca platform, it will give the vendor the opportunity to upsell its existing customers to the new capability, potentially replacing any dedicated web security or API security platforms they may already be using. We should also expect to see Orca appearing in forums where web and application security is still discussed in isolation from cloud security in an effort to raise its profile among potential customers who may not be aware of its foray into applications and APIs.

As detailed in this report, both the cloud and web security markets are busy spaces with increasing overlap. Orca has certainly made waves in the cloud world, and there is clearly the potential for it to do something similar in the applications space, extolling the virtues of getting security delivered from the same platform that currently enables customers to improve the posture of their cloud asset.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Omdia Market Radar for Next-Generation Application Security: Pipeline (Pipeline NGAS) (July 2021)

Fundamentals of Next-Generation Application Security for the Dev Pipeline (Pipeline NGAS) (June 2021)

Omdia Market Radar for Next-Generation Application Security: Runtime (December 2020)

Fundamentals of Next-Generation Application Security (December 2020)

Cloud security – IaaS and PaaS (December 2019)

"Google enters NGAS for runtime" (May 2021)

"The landgrab in CSPM continues apace" (June 2021)

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com