TAG CYBER

Vendor Landscape and TCO Analysis for Achieving Cloud-Wide, Workload-Deep Security and Compliance for Public Cloud Environments

A Comparison of Pre-Cloud Tooling, CSPM, CWPP, and Orca Security's Next-Gen Cloud Security Platform

PREPARED BY

Katie Teitler
Senior Analyst, TAG Cyber
katie@tag-cyber.com

Dr. Edward Amoroso
Chief Executive Officer, TAG Cyber
eamoroso@tag-cyber.com

ORCA_0261399
ORCAW_CP010_000171778

Orca Security Ltd.
Exhibit 2118
Wiz v. Orca
IPR2024-00863, -00864, -00865
Ex. 2118-001

TAGCYBER

Table Of Contents

Introduction and Background 1

Orca Security's Next-Gen Cloud Security and Compliance Platform 3

Using a Risk Calculator to Support Cloud Security Platform Decision-Making 6

Orca Security's Additional Benefits 12

Next Steps 15

Introduction and Background

Migration to public cloud has been slow but steady over the past decade. In the early days, businesses saw the productivity and cost benefits of moving infrastructure to the cloud, yet security teams were less enthusiastic about the control they would have over an outsourced environment. Over the years, cloud providers have improved the security of their environments, nonetheless, the shared responsibility model dictates that users implement the controls to secure their assets in those environments.

> "In a cloud environment, you're frequently scaling utilization up and down—possibly thousands of times per hour across multiple clouds—all within a CI/CD pipeline that builds your infrastructure. I tried numerous agent-based tools and they all failed miserably. Orca provides 100% coverage without burdening our DevOps team. It just works."
>
> Drew Daniels
> CIO and CISO | Druva, Inc.

Ex. 2118-003
ORCA_0261401
ORCAW_CP010_000171778

As more and more companies adopt public cloud, the responsibility on the user grows proportionally. Within the last year, given the mandates of operating on a fully remote basis, cloud adoption has had its most rapid increase in history, with greater numbers of companies sunsetting legacy environments in favor of public cloud which can be easily accessed and scaled on demand. With this rapid adoption, the pressure is on enterprise security teams to ensure that their cloud instances are configured correctly, that access is secure, that PII is controlled, that the environment is free of malware, and that attackers, should they somehow gain access to the cloud, can't move laterally and adversely affect the business by causing a disruption or breach.

The vendor landscape is rich with providers focusing on this exact problem. However, while vast, the vendor landscape for public cloud security is confusing, with each provider offering slightly different approaches. One challenge to present-day cloud security is that technologies built for on-premises environments are not effective in dynamic environments like cloud, containers, and serverless. Simply put, technologies that were adapted for cloud can't provide the holistic visibility and control over cloud-based environments that enterprises need.

> "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. 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
> Sr. Cloud Security Engineer | Sisense

CSPMs Haven't Kept Pace with Enterprise Business Requirements

But the challenge doesn't stop there. As befitting the ephemeral nature of the cloud, workload visibility has become a table stakes platform requirement. As has the need for platforms to fit seamlessly into continuous integration/continuous development (CI/CD) pipelines required by DevOps. These challenges cannot be overcome with first generation cloud security offerings like cloud security posture management (CSPM). Once considered "cutting edge," these products haven't kept pace with business requirements. As such, enterprises must now look at second generation cloud security platforms that combine CSPM with additional capabilities like cloud workload protection, file integrity monitoring, continuous discovery, and more.

This must all be accomplished in a scalable, resource-friendly solution that not only provides the technical capability, but also the ability to counterbalance the expense, staffing pressures, and potential lack of in-house expertise required to manage cloud securely.

Ex. 2118-004

ORCA_0261402
ORCAW_CP010_000171778

Orca Security's Next-Gen Cloud Security and Compliance Platform

In this paper, we explore Orca Security's next-gen platform and cost benefits of implementing their solution to achieve cloud-wide visibility—from the cloud infrastructure to the OS to applications and data—and demonstrate how Orca can strategically and operationally improve enterprise security teams' cloud security risk posture.

Workload-Deep Visibility and Risk Mitigation

Orca Security is a cloud-native SaaS solution that treats cloud deployments as an interconnected web of assets. Unlike other cloud and workload security products that use agents to scan and assess companies' cloud environments, Orca uses a patent-pending technique called SideScanning™, a read-only view of cloud workloads, which unobtrusively scans the run-time block storage layer—out of band—to extract valuable data about the environment and the assets communicating in it. This method produces a full snapshot of the environment—including a reconstruction of the file system, applications, data, and OS—that is used for correlation, contextualization, and analysis.

> **"I've been working with vulnerability assessment solutions for over 20 years. I even wrote a book on how to build a vulnerability management strategy. I've never seen anything like the Orca Security platform before. Within a couple of months I had it fully rolled out, protecting our more than 4,000 cloud customers. This product is a gem and must-have solution for businesses operating in the cloud."**
>
> Morey Haber
> CTO and CISO | BeyondTrust

Ex. 2118-005

ORCA_0261403
ORCAW_CP010_000171778

Bypassing the Challenges of Pre-Cloud Scanning Methods

Orca SideScanning bypasses the typical problems of better-known scanning methods like agent-based scanning and authenticated and unauthenticated scanning. For instance, with agent-based scanning, each asset must have an agent on it, or communicate with another asset with an agent, in order to be visible. Authenticated scanning requires the scanner to have privileged access on each scanned host, opening the possibility of exploitation if access to it were compromised. In addition, authenticated scanning and agents consume system resources and thus potentially produce lag. Unauthenticated scanning is less cumbersome on the system and eliminates the potential risk of compromise against privileged access, but it cannot collect the detailed information operators need to effectively understand system risk.

With SideScanning, workload performance is unimpacted while Orca quickly gathers all relevant data about deployed assets, including virtual machines, containers, databases, and datastores, along with information on configurations/ misconfigurations, vulnerabilities in software, weak or stolen credentials, risks of lateral movement, secret keys, weak passwords, and misplaced or unsecured PII. The platform also collects metadata from the cloud providers' APIs so that relevant information from integrated assets running outside but connected to the cloud environment is captured.
This complete dataset provides full visibility into assets communicating in the cloud and any known exposures. Next, Orca enriches and contextualizes that data with third-party threat intelligence, vulnerability, and exploit information and then uses advanced algorithms to assess the risk posture of every asset in the environment.

> "It's a lot of wasted effort – for both security and engineering - to make an agent-based solution work. Every vendor with an agent says they are lightweight. The issue is not about CPU power but about adding more risk. The more things you load into a system, the more complexity you add, and the more risk that something can go wrong. Orca's out-of-band approach isn't so much a performance benefit as it is a people-process benefit."

Caleb Sima
VP of Information Security | Databricks

Ex. 2118-006

ORCA_0261404
ORCAW_CP010_000171778

Orca Security's Unified Data Model for the Control Plane and Data Plane Provides a More Accurate Way to Prioritize

Orca goes beyond identifying vulnerabilities as "risk." The platform uses the true definition of risk—severity of underlying vulnerability x accessibility x business impact—as its measure to help assess risk in customers' environments. This assessment, therefore, is unique to each customer based on not only cloud assets, but also business criticality of each asset and its relationship to adjacent assets within the customer's cloud. By leveraging this contextualized dataset, Orca presents customers with a context map that allows them to quickly and easily identify the most likely attack vectors and targeted assets in the environment.

Through this process of data gathering and contextualization, customers can answer important risk-based questions such as:

- Is my cloud configuration secure?
- Which applications and operating systems are running and what are they vulnerable to?
- What data are we storing and is it properly secured?
- Am I meeting compliance mandates?
- Can I see my entire attack surface, across cloud, serverless, and container environments?
- Am I able to achieve true continuous risk assessment?
- Can I prioritize the latest risks based on business impact?

These are all fundamental business risk questions—not just cyber security questions—that can positively or negatively impact operations and help or hinder employees, partners, and supplier productivity. This context is extremely important in today's business environment, as a digital disruption or breach could cause long term consequences. This is why Orca Security takes a holistic approach to cloud asset inventory and analysis, focusing on all four cloud layers of the security stack—infrastructure, OS, applications, and data.

Without complete insight and contextualization of the data, businesses cannot properly understand and act upon infected workloads, misconfigured storage buckets, malicious lateral movement, and other vulnerabilities that threaten productivity, efficiency, and the ability to increase revenue streams.

The commercial market is filled with cloud security tools, but many of them work in silos, covering only some aspects of cloud computing. This is why disparate but related terms have emerged to describe cloud security. Cloud security posture management (CSPM) and cloud workload protection platforms (CWPP) have become popular in the past five years, but as standalone products, these cannot provide the holistic coverage necessary to accurately assess cyber risk from cloud deployments and protect the assets running in the cloud.

In contrast, Orca Security integrates then builds upon these capabilities to offer ubiquity across companies' entire cloud operating infrastructure. Their platform includes CSPM, CWPP, vulnerability scanning, file integrity monitoring, and asset discovery, but what they uniquely add to the mix is a new, patented technology called SideScanning, described above, which no other commercially available product can claim. The benefit of these integrated capabilities built on Orca's SideScanning is a platform that detects, contextualizes, and prioritizes cyber risk in any cloud environment, at both the workload and control plane level, yet doesn't impact performance in the customer environment.

Ex. 2118-007

ORCA_0261405

ORCAW_CP010_000171778

Using a Risk Calculator to Support Cloud Security Platform Decision-Making

A risk calculator model from Orca Security is shown to be effective in assisting enterprise security decision-makers regarding the important cost-benefit decisions that must be made regarding in-sourcing or outsourcing cloud security posture management, cloud workload protection, and related cloud security tasks. A typical case study is shown that uses typical industry averages to calculate the cost savings of moving from an agent-based approach to Orca-supported cloud security.

Overview of the Calculator

Given the expanding complexities of modern cloud-based computing, enterprise security decision makers require assistance in the selection of platforms to assist in their security risk management. Such decision makers include C-Suite corporate leaders, senior security leaders including the Chief Information Security Officers (CISO), and executives in adjacent organizations such as procurement.

The most important decision points for these leaders involves making accurate cost-benefit comparisons for the types of controls being deployed across cloud and hybrid enterprise architectures. In traditional areas such as finance and operations, leaders can fall back on practical experiences and empirical results from previous engagements to make such decisions. For new cloud security usage, however, no prior experience exists to guide decision makers.

To assist in this regard, the team from Orca Security has developed a risk calculator to help enterprise decision makers with their cost-benefit analysis of cloud security management tasks. The calculator focuses specifically on comparison of internally performed cloud security functions versus cost proposals by commercial vendors. The presumption is that this is a primary decision point for cloud security teams.

Ex. 2118-008

ORCA_0261406

ORCAW_CP010_000171778

This report outlines TAG Cyber's assessment of the calculator[1] and its potential use by enterprise leaders. As will be shown, the calculator, in TAG Cyber's view, offers a clear means for managers to perform a rapid quantification of their respective internal and potential external costs from a commercial vendor. Comparison of these two estimates provides insight as to the savings of one approach over the other (usually trending toward the commercial tool).

[1] TAG Cyber worked closely with the Orca Security team to perform the assessment and calculations including representative numbers offered by Orca to help ensure that the review and case study were within typical industry ranges. TAG Cyber's role was to review and validate the risk calculator approach and the cost savings conclusions drawn. https://resources.infosecinstitute.com/careers/cybersecurity-engineer/#gref

Underlying Risk Model

The Orca risk model driving the calculator includes a series of broad enterprise factors that cover the salient aspects of management decision making about cloud security that will influence cost-benefit implications of security decisions. The key components of the cost-benefit framework are listed below along with their role within enterprise security risk management for cloud-related assets.

- *Staff Costs* – This involves determining the salary costs for internal staff. It is best done using fully loaded and realized costs for any full-time equivalents (FTEs).
- *Cloud Assets* – The basic unit of cloud-related work involves assets hosted in the cloud. This will correspond to virtual machines but could involve other workload-related units.
- *Cloud Agents* – An additional important unit of work estimation involves software agents that are installed on cloud assets for management.
- *Management Time for Assets* – This involves the amount of time required on average to manage assets in the cloud.
- *Management Time for Agents* – This involves the amount of time required on average to manage agents on cloud assets.

Obviously, local considerations can apply to interpret any of these elements in a more granular or bespoke manner, or to add more factors to the model. For example, costs could be different for consultants or outsourced staff. Similarly, multiple cloud hosting environments might require different average times for asset or agent management. Such differences would require slight adjustments to how the model is used.

Ex. 2118-009

ORCA_0261407

ORCAW_CP010_000171778

How the Calculator Works

The specific elements of the Orca risk calculator include a series of variables, based on the risk model, that can be quantified by the local cloud security team, or through collection of data from empirical or sector-average results. These variables, which provide basis for the quantified analysis, are assigned values via a questionnaire that asks cloud security managers for information on the following factors:

- *Average salary of internal security staff* – This is locally determined, but a typical average might be $115,000 per annum for cloud management staff. These are positions that require skill [1].
- *Average realized cost ratio for internal staff* – A typical industry average multiplier for loaded fully realized costs is 1.7. If this data is not easily obtained locally, then average data is available from various public resources [2].
- *Number of cloud assets requiring visibility and hygiene* – The average number of cloud assets might be averaged over a month that are in need of visibility and ongoing hygiene will often measure in the hundreds or thousands.
- *Number of agents per cloud asset that require management* – This number of agents that provide operational information about patching, updates, and maintenance will typically be 2 or 3.
- *Number of cloud assets per different cloud environment* – Given an organization's different cloud environments (services, configurations, or images), a typical average of assets per environment might be in the 20-40 range.
- *Number of staff hours to manage agents per environment per year* – The number of staff hours to plan, design, test, and deploy agents per environment per year will be in the range of 60 hours.
- *Percentage of agents that require manual installation* – The percentage of all agents that require manual installation by security FTEs will be typically in the 30% range, but this can vary.
- *Average manual installation time in hours* – The typical manual installation time in hours, which should include factors such as travel, communication, and training, could be in the 2-hour range.
- *Percentage of agents requiring one support case per year* – The historical percentage of all agents that require at least one support case to be opened by the security team over a year might be in the 8% range.
- *Time for support cases to be completed* – The length of time to complete support cases for cloud assets can average roughly 3 hours, but this can be higher, and will include outliers that can drive the average higher.

In addition to these calculator factors, the local team can provide software costs for agents, and information about assets that might not have agents, which can be as high 50% in a typical environment (25% is used in the model below). The goal is to collect information on all the locally relevant factors, and the Orca risk calculator supports flexible adaptation to a customer environment.[2]

[2]The TAG Cyber team ran several manual spreadsheet-based exercises with the model changing the values and adding or removing different sample local factors. The model looked to include the right factors for calculating baseline costs for manual operation without a tool such as Orca. https://web.mit.edu/e-club/hadzima/how-much-does-an-employee-cost.html

Ex. 2118-010

ORCA_0261408

ORCAW_CP010_000171778

Case Study Model Shows a 32% or $184,831 Reduction in TCO and Risk Using Orca Security vs Agent-Based Tooling: ACME Enterprise Cloud Assets

To illustrate the use of the risk calculator to compare local manual costs with the usually lower costs associated with the Orca commercial platform, we include below some typical calculations. Readers can peruse the sample numbers to get an idea of how this might be performed locally with relevant variable data to make decisions about whether to invest in the Orca toolset.

The assumption here is that ACME Enterprise is a typically average organization operating a group of cloud-based assets, most of which have agents installed, supported by local FTE staff. The calculations are made in the context of variable assumptions that include average breach costs of $500,000 [3]. The table below lists the quantitative assumptions made for our case study.

Figure 1. Case Study Variable Assumptions

DESCRIPTION	AMOUNT
IT ENGINEER SALARY PER ANNUM	$ 115,000.00
IT ENGINEER FULLY-LOADED COST (YEARLY)	$ 195,000.00
INFOSEC ENGINEERING HOURLY COST	$ 93.99
NUMBER OF ASSETS PER DIFFERENT ENVIRONMENT	35
PER YEAR	60
PERCENTAGE OF AGENTS THAT REQUIRE MANUAL INSTALLATION	30%
MANUAL INSTALLATION TIME (HOURS)	2
PERCENTAGE OF AGENTS THAT REQUIRE AT LEAST ONE ANNUAL SUPPORT CASE	8%
AVERAGE SUPPORT CASE TIME (HOURS)	3
CSPM PRICE PER ASSET PER ANNUM	$ 110.00
AGENT PRICE PER ANNUM	$ 11.00
CHANCE OF BREACH FOR "UN-AGENTED", UNCOVERED ASSET	0.25%
BREACH COST	**$ 500,000.00**

Ex. 2118-011

ORCA_0261409

ORCAW_CP010_000171778

Figure 2. Case Study Cloud Environment Data

ENVIRONMENT	AMOUNT
NUMBER OF MACHINES	1,200
AGENTS PER MACHINE	2
NUMBER OF AGENTS	2,400
NUMBER OF ENVIRONMENTS	34

The questionnaire used for our ACME Enterprise case study included estimates for number of assets (machines), agents per asset (machine), number of total agents, and number of cloud environments. This information, which includes numbers in the typical industry ranges, is shown in Figure 2.

Using this information, the risk calculator could be used to estimate existing, agent-based costs for the case study cloud environment. These calculations result in a total cost, including a risk-based cost estimate that integrates the percentage of breaches due to lack of visibility, expected lack of visibility, and average breach cost. Figure 3 shows the case study calculation of $569,625 in total annual costs for the baseline agent-based cloud approach.

Figure 3. Case Study Calculation for Existing Agent-Based Approach

DESCRIPTION	AGENT BASED
EXPECTED SECURITY COVERAGE	90%
OPERATIONAL / PERFORMANCE IMPACT OR RISK	LOW
DESIGN & PLAN TIME (HOURS)	2,040
MANUAL INSTALLATION TIME (HOURS)	1,440
SUPPORT TIME (DOWNTIME: IT HOURS FOR RECOVERY)	576
TOTAL HOURS	**4,065**
TOTAL COST OF SOLUTION ENGINEERING	**$ 381,225.00**
SOLUTION / LICENSE COST PER ANNUM	$ 26,400.00
AGENT / SCANNING CAUSED ENDPOINT DOWNTIME/SLOWDOWN COST	$ 12,000.00
TOTAL COST OF OWNERSHIP	$ 419, 625.00
TOTAL COST OF OWNERSHIP - PER MACHINE	$ 349.69
RISK COST DUE TO LACK OF VISIBILITY - % OF BREACH DUE TO LACK OF VISIBILITY / EXPECTED LACK OF VISIBILITY BREACH COST	$ 150,000.00
TOTAL COST + RISK COST	**$ 569,625.00**

This defines costs per year for "competitive" solutions

Ex. 2118-012

ORCA_0261410

ORCAW_CP010_000171778

The Orca team provided comparable numbers for a commercial installation. As one would expect, many factors are no longer relevant in the case study. This allowed us to zero out a few of the factors, to list coverage at 100%, to use a total estimated time of 51 hours (supplied by Orca), and to assume other typical platform costs. Figure 4 shows the comparison calculation.

This simple case study obviously includes numbers generated for the sample calculation, but the general idea should be clear. That is, through a reasonable entry of data that could be justified as typical for most environments, the calculation shows a savings of $184,831 per year in operating expense savings.[3] This is good news for the typical cloud security team, who can direct their existing staff toward higher value activities than day-to-day maintenance.

[3]The Orca team provided TAG Cyber with additional data for more granular deployment cases that might be of interest to enterprise cloud security teams (e.g., CSPM only, unauthenticated, authenticated). Interested readers can be in touch with the Orca team to go through these calculations using local information. https://www.helpnetsecurity.com/2019/07/24/data-breach-cost/

Figure 4. Case Study Calculation for Orca Commercial Approach

DESCRIPTION	AGENT BASED	ORCA SECURITY
EXPECTED SECURITY COVERAGE	90%	100%
OPERATIONAL / PERFORMANCE IMPACT OR RISK	LOW	NONE
DESIGN & PLAN TIME (HOURS)	2,040	51
MANUAL INSTALLATION TIME (HOURS)	1,440	0
SUPPORT TIME (DOWNTIME: IT HOURS FOR RECOVERY)	576	0
TOTAL HOURS	**4,065**	**51**
TOTAL COST OF SOLUTION ENGINEERING	**$ 381,225.00**	**$ 4,793.51**
SOLUTION / LICENSE COST PER ANNUM	$ 26,400.00	$ 380,000.00
AGENT / SCANNING CAUSED ENDPOINT DOWNTIME/SLOWDOWN COST	$ 12,000.00	$ -
TOTAL COST OF OWNERSHIP	$ 419, 625.00	$ 384,793.51
TOTAL COST OF OWNERSHIP - PER MACHINE	$ 349.69	$ 320.66
RISK COST DUE TO LACK OF VISIBILITY - % OF BREACH DUE TO LACK OF VISIBILITY / EXPECTED LACK OF VISIBILITY BREACH COST	$ 150,000.00	$ -
TOTAL COST + RISK COST	**$ 569,625.00**	**$ 384,794.00**
This defines costs per year for "competitive" solutions		
DELTA RELATIVE TO ORCA	$ 184,831.00	$ -

Ex. 2118-013

ORCA_0261411

ORCAW_CP010_000171778

Orca Security's Additional Benefits

Orca provides important additional benefits, but didn't have a large enough dataset from which to make statistically sound assumptions for their calculator. Yet these benefits should be considered in any cloud security platform vendor evaluation.

Reduce Alerts to the Few that Actually Matter

Understanding risk context is critical; it's the difference between effective security and alert fatigue. Security teams today receive an average of 10,000+ alerts for every 100 cloud assets they manage. They simply can't keep up. These alerts lack prioritization and actionable details, leaving security teams to do all the heavy lifting.

Be wary of solutions that consider only one dimension of risk such as the severity of the underlying security issue (e.g., CVSS score). These solutions will ignore its accessibility and business impact. The result is a long list of security issues that divert attention from real problems. Attackers don't look for or care about independent vulnerabilities. Instead, they seek the easiest and most direct routes into the cloud environment. They use any vulnerabilities and relationships between assets to access their target.

Orca Security's approach visualizes security issues in context, just like an attacker. Orca's context engine combines deep workload discovery, including the workload's host configurations (e.g., running services, firewall configurations) with cloud configuration details (e.g., IAM roles, VPC's, security groups) and presents the cloud estate as a detailed asset inventory.

Orca identifies the role each asset plays in the environment (e.g., what permissions does each asset have) as well as connectivity such as which VPCs allow inbound internet traffic. This visual representation of the cloud environment immediately surfaces potential security issues and their root cause without overwhelming security teams with thousands of meaningless alerts.

Ex. 2118-014

ORCA_0261412

ORCAW_CP010_000171778

> "Orca tells me I have 28 things I need to focus on today. Out of 25 cloud accounts with about 840 compute assets, VMs, and thousands of other assets, true risk comes down to 28 things to take care of today. We can manage that."

Peter Robinson
Director of Cybersecurity and Business IT | Zip

Reduced Friction with DevOps

DevOps is a rapid development model that has taken on a life of its own. It now not only describes the process of software development and IT operations integration, but implies a team of engineers working together to build and deploy software which serves internal and external customers by increasing satisfaction and thus revenue.

DevOps has become a very powerful business driver. The main advantage of DevOps is time-to-market, therefore, anything that slows the process is perceived negatively; executive teams will prioritize DevOps teams' needs over conflicting needs. This has been the main source of tension between DevOps teams and security teams over the past decade—DevOps' need to go fast and security's need to check for vulnerabilities. For so long, the tools and processes used by security teams were not compatible with either the DevOps lifecycle or the platforms used for software development.

From inception, Orca was built to fit into the DevOps workflow and reduce friction between DevOps and security teams. Because SideScanning occurs out of band, software engineers and operations professionals won't even be aware of its execution; it's only when the results of the risk analysis are complete and fed into developer friendly tools like Jira that DevOps teams can see and then fix vulnerabilities and misconfigurations in the cloud environment.

In addition, because Orca is DevOps friendly, the platform's bi-directional reporting for alerts allows engineers to continue working in their native environments and with native tools like Jira, Slack, ServiceNow, and various other development tools via simple APIs. The ease of integration into developers' workflows creates more secure environments without the traditional arguments that accompany adding security to DevOps.

> "Even though DevOps reports directly to me, they still have their own way of working. I've been waiting six months for them to write a rule in another security product. But when I gave them Orca, they loved it. I've never seen adoption like this."

Jack Roehrig
CISO | Turnitin

Ex. 2118-015
ORCA_0261413
ORCAW_CP010_000171778

Fewer Meetings

A direct result of reduced friction between IT, development, and security teams is fewer intra-departmental meetings. When all vulnerability data and analysis is readily available to all parties, there is less need for discussion around findings and concerns. A centralized source of contextualized data means that conversations can abstract to a higher level and focus on fixing problems rather than identifying them.

Better Tracking

Orca's SideScanning technology identifies and alerts on known vulnerabilities, providing the precise path to remediation. Users no longer have to guess at where or how to go about fixing a vulnerability or eliminating unnecessary access. Once a user has patched a vulnerability, Orca can then close out a vulnerability and issue an updated assessment of the environment, across the entire stack, from OS to applications and running services.

> "Knowing the tasks and associated risks at any moment, we can prioritize what we send to DevOps so they don't get overwhelmed. To assign the work, we simply click the 'send-to-Jira' button. If we get audited, we can show, 'This is our pipeline, this is our work plan.' It's all in Jira and everything has an audit trail. it just becomes very simple to demonstrate patching and compliance."

Nir Rothenberg
CISO | Rapyd

Simplified Compliance Audits

Compliance audits are traditionally point-in-time and limited to the specified project scope. Project scope becomes especially tricky when the enterprise's networks are spread across multi-cloud environments. These limitations may fulfill compliance obligations but in reality do very little to reduce the cyber risk to an organization or accurately reflect whether the business is compliant on an ongoing basis. In addition, point-in-time audits can be costly and burdensome on IT infrastructure.
Orca was built to provide continuous, cloud-wide, and workload deep visibility for 100% of cloud-based assets—whether the enterprise is deployed in AWS, Azure, Google Cloud Platform, or any combination thereof. This means that enterprises can not only demonstrate cloud-wide compliance after an audit, but will remain compliant and even exceed baseline compliance requirements day after day. Because Orca

Ex. 2118-016
ORCA_0261414
ORCAW_CP010_000171778

runs continuously, automatically, and autonomously, data is always available to auditors or anyone responsible for reducing cyber risk at any time.

This always-current dataset lessens audit complexity and cost, and goes beyond what's required to unearth what's important in the cyber risk equation.

In addition, Orca meets all standards included in major compliance frameworks such as AWS CIS, SOC2, PSD2, PCI-DSS, NIST CSF and more. This framework alignment means that businesses won't miss adherence to any major requirement and find themselves dealing with an expensive and time-consuming audit failure. With Orca, businesses can easily and quickly demonstrate the ability to systematically identify vulnerabilities, malware, insecure configurations, and critical attack vectors, then use that information to remediate problems before they become breaches.

> **"Orca has helped reduce my audit effort; for example, I can run reports that show we maintain least privilege controls and that we use multi-factor authentication. Orca is great at detecting potential exposure of credit card data, email addresses, and social security numbers or other national IDs. These are priority issues that we can quickly remediate."**
>
> Jonathan Jaffe
> CISO | Lemonade

Next Steps

Enterprise teams who manage cloud assets today and who seek ways to reduce maintenance cost and free up staff for higher value activities would be advised to connect with Orca Security to try out the risk calculator methodology described above. The TAG Cyber team found this easy to learn and follow, and we would expect that enterprise teams would enjoy working through their own local case to determine their possible cost savings.

Contact Orca Security

info@orca.security

orca.security