TAG

RETURN ON INVESTMENT (ROI) ANALYSIS:

ESTIMATING RETURN ON INVESTMENT FOR THE ORCA CLOUD SECURITY PLATFORM

DR. EDWARD AMOROSO, FOUNDER & CEO, TAG
THE TAG ANALYSTS

orca SECURITY

RETURN ON INVESTMENT (ROI) ANALYSIS:

ESTIMATING RETURN ON INVESTMENT FOR THE ORCA CLOUD SECURITY PLATFORM

DR. EDWARD AMOROSO
THE TAG ANALYSTS

EXECUTIVE SUMMARY

This updated 2026 TAG Return on Investment (ROI) analysis evaluates the modern Orca Cloud Security Platform, now significantly expanded since our prior TAG ROI on this enterprise security solution in 2023.[1] Key innovations that have emerged since this earlier analysis include agentless reachability analysis, deep AppSec, CIEM enhancements, the Orca Sensor, and the integration of Opus Security's AI-based investigation and automation capabilities.[2]

These additions to the Orca Cloud Security Platform, combined with the new Orca AI Assistant, create a unified platform that provides end-to-end cloud security coverage across hybrid cloud environments, AppSec pipelines, identities, data, and runtime risk. It is thus reasonable for readers to request information about how this impressive platform provides both qualitative and quantitative return to buyers. That is the motivation driving this updated ROI.

As will be explained in the report below, using TAG's ROI methodology, most organizations will be transitioning from an agent-based, multi-tool cloud security approach to Orca's unified platform. This multi-tool pre-condition is viewed as the most common cloud security arrangement in our work at TAG.[3] In that context, they can expect to achieve considerable benefits in cost and a material improvement in risk posture.

[1] This video provides an overview of the prior ROI assessment which resulted in the identification of a 207% return for security teams operating under reasonable enterprise cloud usage assumptions: *https://www.youtube.com/watch?v=bbwXWWTb3UU*.

[2] See *https://orca.security/resources/blog/orca-security-acquires-opus-agentic-ai-cnapp* for the acquisition announcement of Opus by Orca Security, resulting in a new agentic AI capability integrated into Orca's CNAPP.

[3] Much of our research in cybersecurity originates with our advisory practice for CISOs and their teams where we have a broad and extensive vantage point for understanding what practitioners are using to protect their enterprise, including the budget allocated and savings derived by deploying tools such as Orca. Throughout this report, any references to trends being observed relate to that practice.

In the analysis below, we will show specifically, based on modernized assumptions, that a representative mid-sized enterprise can produce an annual cloud-security ROI of 198.33%, compared to typical existing approaches. They will also eliminate significant person-hours associated with multi-console operations, alert triage, and coordination across point solutions. Again, these are commonly found attributes for in-house schemes.

We also leverage new case studies provided to our team from Orca that offer documented experiences from actual enterprise customers. These case studies further illustrate to readers how reducing noise, consolidating tooling, and applying context-rich attack-path analytics accelerate remediation and measurably reduce cloud exposure. Our observation is that they dovetail with our ROI analysis nicely.

INTRODUCTION

Enterprises today must secure expansive cloud environments under intense time pressure. Cloud workloads now span VMs, containers, serverless functions, data stores, identities, APIs, and complex CI/CD pipelines. But adversaries increasingly combine cloud misconfigurations, exposed identities, and reachable workloads to develop multi-step attack paths that traditional tools fail to detect. To keep pace, modern cloud-security programs therefore require:

- **Visibility** – Unified visibility is required for cloud security to span compute, identity, data, endpoints, and application code paths.
- **Scanning** – Agentless scanning is an important component of cloud security to help eliminate operational overhead.
- **Analysis** – Context-driven attack-path analysis is a key security method to ensure that protection tasks prioritize what actually matters.
- **Workflow** – Automated investigation and workflow support is required since cloud is now so essential to organizational infrastructure.
- **Decisions** – AI-augmented assistance is now a key requirement in cloud security programs to accelerate human decision-making.
- **Lifecycle** – Full lifecycle AppSec coverage from code to cloud is demanded by modern enterprise security teams.

The good news is that Orca Security supports all elements of this unified model through a single platform that eliminates friction, accelerates remediation, and reduces security spend, while improving coverage and reducing exposure. This ROI report provides quantitative analysis based on TAG's structured methodology as well as qualitative evidence from customers, updated to reflect Orca's latest platform capabilities and strategic direction.

It is worth re-emphasizing that modern enterprise teams, perhaps unlike their counterparts several years ago, no longer require guidance on the advantages of implementing cloud security. That issue is no longer debated. Instead, the ROI question has shifted to how existing cloud security measures can be improved – in this case, using Orca Security – to produce meaningful quantitative and quantitative advantages.

ORCA PLATFORM COMPONENTS

A fresh review of the commercial Orca platform reveals modules that align well with modern functional requirements and security needs from enterprise security teams in all sectors and across organizations of all sizes, shapes, and geographies. Let's review each of these platform modules, recognizing that many align with acronyms that have been established by the industry analyst community to reference common functions.

The Cloud-Native Application Protection Platform (CNAPP) is Orca's flagship offering. It consists of a unified platform that converges multiple cloud security solutions into a single data model. Orca states that its CNAPP delivers "100% cloud security coverage and attack path analysis," enabling organizations to detect and prioritize risks across cloud infrastructure, workloads, data, identity, and applications, all from one place.

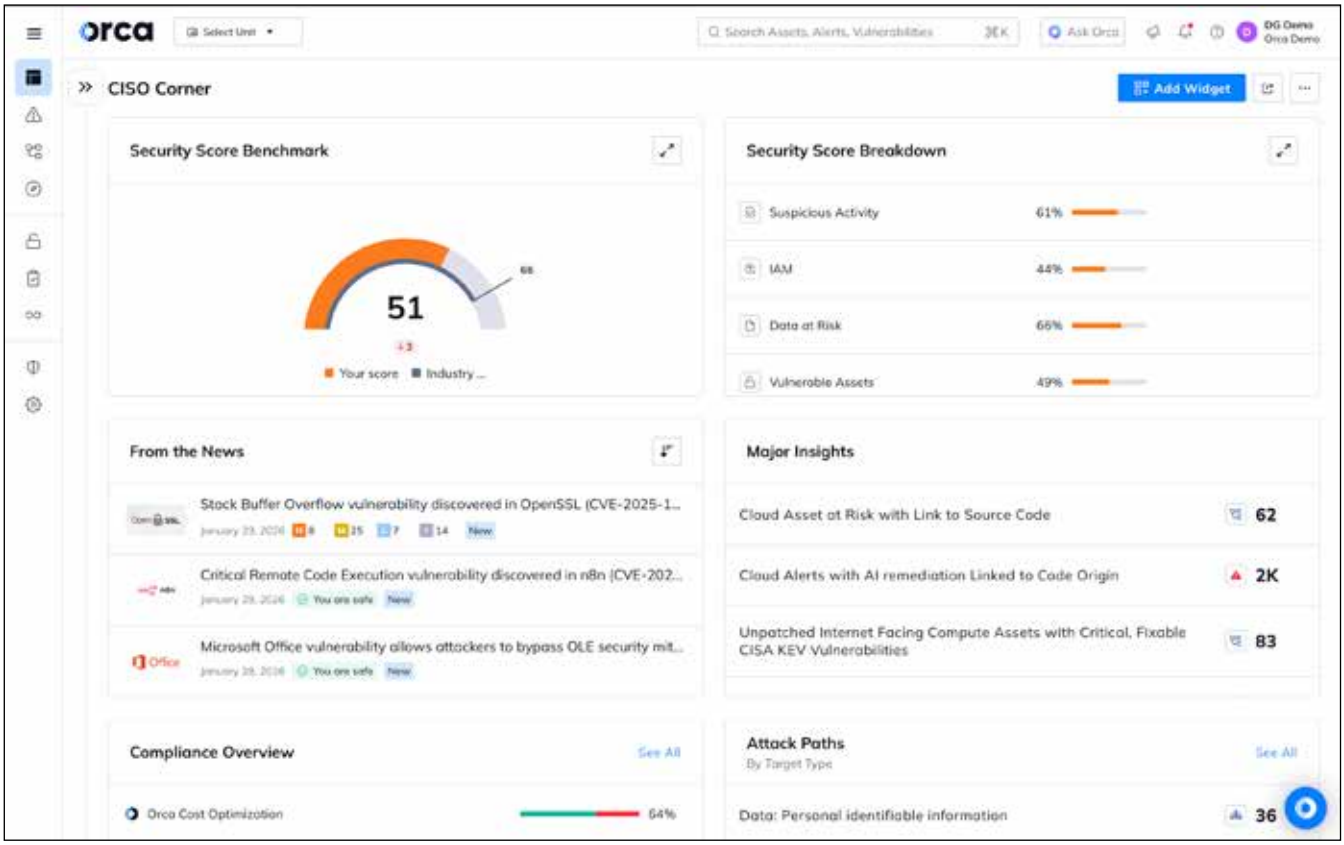

Figure 1. Orca CNAPP Dashboard[4]

Under CNAPP, security teams get full-stack visibility including cloud misconfigurations, workload vulnerabilities, identity/entitlement issues, data risks, API exposures, and more. By converging what traditionally required many point-products (e.g., CSPM, CWPP, CIEM, DSPM, container/Kubernetes security, etc.), Orca reduces complexity and enables more strategic remediation, focusing teams on the much smaller number of alerts that truly matter.

The Orca flagship CNAPP offers an excellent means for combining and integrating key features that are required in modern enterprise cloud security environments. As will be shown below, such consolidation can save considerable operating expense (i.e., license and maintenance costs) as well as qualitative time and effort by security teams. This establishes an important basis for our ROI analysis. Here are the Orca components – and the list is long:

- **Orca CSPM** – The Cloud Security Posture Management (CSPM) capability within the Orca platform continuously monitors cloud infrastructure for misconfigurations, policy violations, and compliance risks. It offers an integrated means within the Orca platform to build and maintain a comprehensive cloud-asset inventory, track compliance posture, and identify drift or deviations from security policy across public clouds.[5]

[4] This screenshot and much of the general and background information on Orca's CNAPP is derived from the publicly available resources hosted at *https://orca.security/resources/blog/what-is-cnapp/*.

[5] During the past three years, since our prior Orca ROI, we have noticed at TAG that CSPM has become an almost assumed component of any cloud security program. To that end, it has shifted from an add-on feature to the foundation of CNAPP. This is the case for Orca's platform.

- **Orca CWPP** – Cloud Workload Protection Platform (CWPP) in Orca delivers deep, agentless-first protection for cloud workloads, including virtual machines (VMs), containers, Kubernetes pods, and serverless functions. Rather than relying on installing agents, which can be brittle, inconsistent, and resource-heavy, Orca's CWPP instead uses its patented SideScanning technology to deliver full-stack workload visibility.[6]

- **Orca CIEM** – The Cloud Infrastructure Entitlement Management (CIEM) capability within the Orca platform helps organizations manage identity and access risks across their cloud environments. Orca tracks relationships between identities (i.e., users, roles) and cloud resources and highlights permissive identities, entitlements, or risky permissions.[7]

- **Orca DSPM** – Data Security Posture Management (DSPM) in Orca gives visibility and control over data stored across cloud estates. Orca continuously discovers and inventories data stores, including databases, storage buckets, virtual-machine disks, and container storage, and classifies them for sensitive content (e.g., PII, PCI, PHI).

- **Orca Container & Kubernetes Security** – The Container & Kubernetes Security capability within the Orca platform is specifically geared toward containerized and orchestrated workloads. Using SideScanning, Orca can inspect container images, Kubernetes clusters, and container runtime environments without requiring the use of agents.

- **Orca Multi-Cloud Compliance** – Orca Multi-Cloud Compliance helps organizations enforce security compliance across multiple cloud providers and environments. Orca can continuously monitor cloud assets, configurations, workloads, data stores, identities, and more, ensuring compliance with regulatory and industry frameworks by applying consistent security policies across modern heterogeneous cloud infrastructure.

- **Orca Vulnerability Management** – Orca Vulnerability Management gives continuous, agentless vulnerability scanning across cloud workloads and resources. This includes focus on detecting exploitable vulnerabilities in VMs, containers, and Kubernetes, across major public clouds (i.e., Amazon Web Services, Microsoft Azure, GCP, Oracle, Alibaba Cloud) and container orchestration environments.[8]

- **Orca API Security** – Orca API Security provides agentless, cloud-native API security capabilities. Orca claims to be among the first platforms to bring API security into a unified CNAPP — merging API posture with infrastructure, data, identity, and workload security for holistic risk assessment.

- **Orca CDR (Cloud Detection & Response)** – Orca Cloud Detection & Response (CDR), is part of the runtime protection and response capabilities that complement the static posture and vulnerability tools. Orca's runtime monitoring, telemetry collection, and alerting enable detection of malicious behavior, unusual activity, or compromise.

- **Orca Application Security** – Orca Application Security brings security earlier in the software development lifecycle, enabling "shift-left" practices. Orca offers SCM posture management, static code analysis (SAST), software composition analysis (SCA), secrets detection, IaC scanning, and container-image scanning, all integrated into CI/CD workflows.

---

[6] Readers should interrogate cloud security vendors who claim both CSPM and CWPP, because implementation of these functions demands different support and functional platform capabilities. Runtime protection of workloads demands the ability to handle execution environments and behaviors, which is dramatically different than static CSPM scans. We have been impressed with Orca's ability to handle both cases.

[7] It has been interesting to observe as security teams have come to recognize the importance of integrating identity with cloud security. Early attempts at CIEM (e.g., Addalom) were pioneering but clumsy. We've seen this function evolve to a required aspect of any CNAPP.

[8] Reference is made in this report to agentless operation. Agentless cloud security provides frictionless visibility across cloud accounts without requiring software installation, which eliminates deployment overhead and avoids operational issues tied to agent maintenance, versioning, and performance impact. It also ensures broader, more consistent coverage—especially for ephemeral or auto scaled resources that agents often miss, while still enabling deep configuration, posture, and workload analysis through native cloud APIs and metadata.

- **Orca AI-SPM** – Orca AI SPM (AI Security Posture Management) extends Orca's coverage to AI-enabled assets and cloud-based AI services. As cloud usage of AI grows, AI-SPM helps detect and manage risks associated with AI models and related infrastructure, integrating them into the same risk-prioritization and compliance framework as traditional assets.

ORCA PLATFORM TECHNOLOGY

The technology that underpins the Orca CNAPP and the various solution offerings described above is rooted in both practical day-to-day requirements from enterprise customers, as well as recent advances in machine and deep learning. Here is a brief overview of the more salient aspects of this technology foundation:

- **Orca AI** – Orca AI refers to the AI-driven capabilities embedded within the Orca Platform to simplify and accelerate cloud security operations. Orca AI helps generate remediation steps (for misconfigurations or IaC issues), provides conversational cloud-asset search (natural language search), and helps guide remediation workflows such as automatic code fixes or pull requests.
- **Orca Side-Scanning Technology** – SideScanning is the technology that enables Orca's agentless-first approach. Instead of deploying agents inside each workload (which can be resource-intensive), SideScanning collects data directly from cloud configuration metadata and the runtime block storage of workloads, reconstructing the workload's file system (OS, applications, data) as a virtual, read-only view.
- **Orca Sensor** – Orca Sensor is the runtime component of Orca's platform that enables dynamic detection, runtime protection, and Cloud Detection & Response (CDR) capabilities. When deployed, Sensor delivers real-time visibility into workload behavior, enabling detection of malicious activity such as privilege escalation, container escapes, "living-off-the-land" attacks, reconnaissance, and other runtime threats.

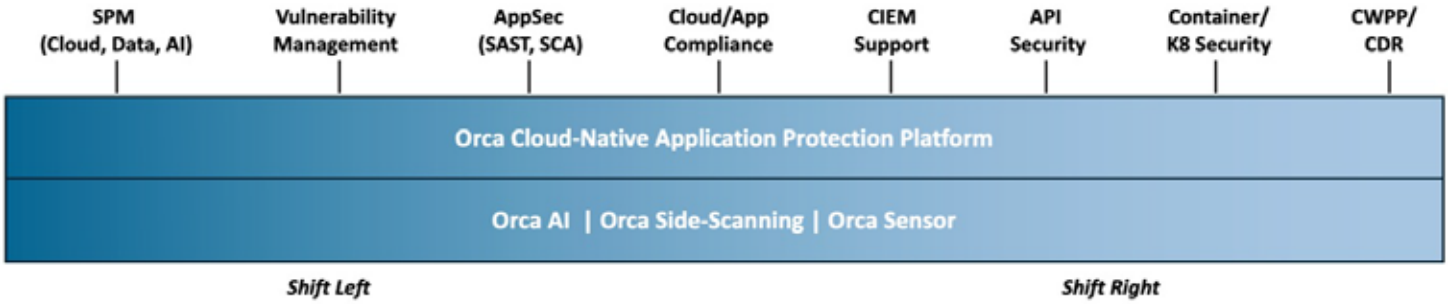

Figure 2. Orca CNAPP Solution Offering and Underlying Technology

QUALITATIVE PLATFORM BENEFITS OVERVIEW

As alluded to in the discussions above, the Orca platform unifies all of the major cloud-security controls demanded today by enterprise security into a single coverage model. This has the effect of unifying tasks that were once only possible using separate tools. The consolidation of CSPM, CWPP, CIEM, DSPM, AppSec, API security, and cloud response reduces complexity and improves response in significant ways.

Now – when we do an ROI, we try to separate quantitative benefits which result in actual reductions in the budgets managed by security leadership (i.e., usually the CISO) from qualitative benefits that just make life easier or save time for team members. We try to avoid the common ROI trap of assuming that by reducing hours spent on a task in the SOC, that CISOs will fire staff and save on salary budget. This rarely happens, if ever.

To that end, we will list below the major areas in which we see significant qualitative benefits for cloud security practitioners before we dive into the more quantitative returns. These qualitative benefits are 100% meaningful, tangible, and impactful, for sure – but they generally do not result in a numeric adjustment to the top line budget allocated to a CISO from their finance team. Here are the top qualitative advantages we have identified:

QUALITATIVE BENEFIT: OPERATIONAL RELIEF:

Teams spend less time maintaining agents, correlating alerts, switching consoles, and manually pivoting across tools.

Operational relief emerges as one of the most immediate and tangible qualitative benefits of adopting Orca's unified cloud-security platform. In traditional agent-based environments, teams spend large portions of their week deploying, updating, troubleshooting, and retiring agents across fragmented cloud workloads, an effort that grows exponentially with scale, ephemeral infrastructure, and multi-cloud diversity.

This friction is compounded by the need to toggle between separate tools for posture management, vulnerability scanning, CIEM, DSPM, workload protection, and runtime monitoring, each with its own schemas, alert formats, dashboards, and investigation workflows. By shifting to a consolidated, agentless-first platform, teams recapture countless hours otherwise lost to maintenance and coordination.

Equally important, operational relief includes the simplification of investigations and daily security routines. Instead of pivoting across consoles to reconstruct context, Orca provides a single source of truth for cloud assets, identities, data stores, misconfigurations, vulnerabilities, runtime behaviors, and their relationships. Analysts no longer waste effort aggregating disparate telemetry sources or reconciling contradictory signals between point tools.

The resulting reduction in cognitive burden is significant. That is, teams can work faster, will make fewer mistakes, and should avoid the fatigue and burnout that accompany constant triage under noisy conditions. While not a direct budget-line savings, this operational benefit is one of the qualitative outcomes that CISOs consistently value because it stabilizes their security programs and improves team performance.

QUALITATIVE BENEFIT: HIGHER-FIDELITY PRIORITIZATION

Agentless reachability and attack-path context will reduce triage noise by identifying what is actually exploitable.

Higher-fidelity prioritization represents one of the most strategically valuable benefits of Orca's platform, especially given the near-universal problem of alert fatigue in cloud security environments. Traditional tools tend to surface issues in isolation, flagging vulnerabilities without considering exposure, misconfigurations without identity context, or toxic permissions without linking them to reachable assets.

Orca's agentless reachability analysis changes this equation by mapping which assets can actually be accessed from the internet or through lateral movement paths. When combined with attack-path analysis, the platform surfaces only those risks that create real, exploitable conditions. The result is a dramatic reduction in triage noise and a far more defensible focus on the handful of issues that materially influence cloud risk.

This context-rich triage model also strengthens planning and governance. Security leaders can prioritize remediation based on evidence rather than assumptions or theoretical severity scores that do not reflect real-world exploitability. Engineering teams appreciate the improved accuracy. That is,

instead of being overwhelmed with large volumes of low-impact vulnerability tickets, developers and cloud engineers receive highly curated, actionable remediation tasks.

QUALITATIVE BENEFIT: FASTER REMEDIATION AND INCIDENT RESPONSE

The AI Assistant and Opus automation significantly reduce time spent investigating issues and coordinating fixes.

Faster remediation and incident response come from the combination of Orca's unified telemetry, deeply contextual analytics, and the automation capabilities integrated through Opus Security and the AI Assistant. Because investigations no longer require analysts to pivot across multiple tools, each incident begins with a much clearer picture of the affected assets, identities, data exposure, and reachable paths.

Instead of wasting minutes or hours (or even days) collecting forensic inputs, security analysts can move immediately to focus more on interpretation or data and telemetry, hopefully leading to some sort of meaningful action. The AI Assistant further accelerates this timeline by summarizing findings, generating remediation guidance, or automatically proposing fixes such as code changes or configuration updates.

The new Opus-driven automation amplifies this speed advantage for analysts by coordinating and executing standardized workflows. For example, once something like a risky entitlement or exposed workload is identified, teams can route tasks to the correct engineering owners, initiate runtime containment, validate fixes, and close out documentation without manual orchestration.

This whole process advantage reduces incident-handling cycles, minimizes dwell time, and prevents issues from resurfacing due to unclear ownership or incomplete remediation. While these efficiencies do not necessarily eliminate staff, they materially improve security operations tempo, reduce stress on the team, and significantly strengthen an organization's resilience to fast-moving cloud threats.

QUALITATIVE ADVANTAGE: BETTER ALIGNMENT WITH ENGINEERING AND DEVOPS

Because Orca covers AppSec and cloud, teams can collaborate earlier in the lifecycle and thus eliminate redundant tooling.

Better alignment of the security organization with Engineering and DevOps teams arises from Orca's ability to unify AppSec and cloud security within a single platform, a capability few competing models provide. In addition, AppSec teams have operated separate SAST, SCA, IaC, container-scanning, and compliance tools, while cloud-security teams managed entirely different CSPM, CIEM, CWPP, and DSPM platforms.

These parallel toolchains produced inconsistent risk signals, duplicate tickets, and conflicting security truths, straining collaboration and slowing delivery velocity. By consolidating these functions and their data into one system, Orca gives teams, both within the CISO organization and beyond, a coherent, lifecycle-spanning view that aligns security findings from code commit to cloud deployment.

The resulting alignment also ensures that platform engineers receive earlier, clearer feedback on issues, whether misconfigurations, vulnerabilities, or exposed identities. Because all issues stem from the same unified risk graph, cross-team discussions become simpler and more productive. DevOps leaders benefit as well, since they no longer need to maintain redundant AppSec toolchains or manage integration brittle points in CI/CD pipelines.

UPDATED ROI ANALYSIS MODEL

The approach taken to demonstrate the quantitative benefits for using Orca focuses on advantages that can lead to real reduction in budget needs for a CISO. The strategy recognizes two key elements of how budgets work: First, we understand that the idea of reducing full-time equivalent (FTE) hours, thus leading to reduced need for people is a reasonable way to reduce contract labor, managed service, or to fill staff gaps – so this is reasonable to include.

However, we have not seen in practice – nor do we expect to see soon, an approach where a tool such as Orca results in a reduction on payroll-based FTE employees, whether newly hired with less experience or more mature staff with many years of experience. Up-skilling the new hires and adjusting work assignments for experienced FTEs is the norm, so we do not include reduction of FTEs as a savings in our models.

Second, the primary benefits that we see, in addition to reduced need for consulting or managed services, involves lower costs via consolidation of multiple platforms and tools, as well as lower risk, which allows most security teams to adjust down their allocated and planned for response costs. Ultimately, the only real reason any security team improves their tooling is to reduce risk, so we acknowledge response cost as a real budget driver.

To that end, we can list below the primary cost drivers that will be used to create a representative ROI model for readers to leverage as a baseline for investigating how their own local circumstance would apply. These cost drivers are consistent with our observations above, and certainly connect with the experiences we see in our day-to-day research and advisory practice at TAG with enterprise customers:[9]

COST DRIVER 1: POSTURE, APPSEC, AND CIEM TOOL CONSOLIDATION

Consolidation of tools for cloud security is a major driver of reduced operating costs leading to strong ROI for using Orca.

A major contributor to Orca's ROI is the consolidation of multiple overlapping cloud-security and AppSec categories, specifically CSPM, CWPP, CIEM, DSPM-adjacent functions, and parts of SAST/SCA visibility, into a single unified platform. Most enterprise cloud programs today maintain a fragmented stack of tools that duplicate functionality or rely on complex integrations that drive up cost and operational overhead.

By replacing these discrete products with Orca's consolidated posture, AppSec, and identity-centric controls, organizations can meaningfully reduce annual software spend, vendor management burden, and integration labor. While actual savings will depend on current contract terms, discount structures, and enterprise procurement constraints, the consolidation impact remains one of the most predictable and material contributors to ROI.

COST DRIVER 2: REDUCED ALERT INVESTIGATION TIME VIA AI ASSISTANT

The time spent addressing alerts and related tasks by staff, consultants, and managed service teams can be significantly reduced, thus leading to cost savings.

Orca's AI Assistant significantly decreases the amount of human time required to investigate and triage alerts, leading directly to measurable analyst-hour savings. Instead of manually correlating signals across cloud assets, identities, vulnerabilities, and runtime behavior, analysts receive enriched and ranked findings with narrative explanations, remediation steps, and contextual evidence.

[9] Note that the 2025 ROI model from TAG incorporated traditional inputs such as staff salaries and fully burdened FTE costs, number of cloud assets, number of agents deployed, time to manage agent friction, support case overhead, and breach likelihood tied to visibility. We are assuming in this updated ROI that most of these benefits, driven by the original goal of implementing commercial cloud security platforms, have already been achieved. Obviously, if readers are just now implementing their first cloud security program, then the ROI here will be even greater. Our choice here is to be more conservative in our estimation for the typical reader.

This enables junior analysts to complete tasks previously requiring senior expertise and allows teams to handle a greater volume of issues without hiring additional headcount. Over a year, even modest per-alert time reductions compound across thousands of findings, creating a highly defensible operational efficiency gain. It also allows for reduction in costs for consultants, managed services, and other non-payroll staff.

COST DRIVER 3: REDUCED ATTACK SURFACE VIA REACHABILITY-BASED PRIORITIZATION

Fewer urgent cases can lead to fewer emergency escalations, which in turn reduces t he costs of workflow and other processes and infrastructure components.

Orca's reachability-based risk analysis reduces the volume of issues requiring urgent attention by focusing remediation on vulnerabilities that are truly exploitable given network paths, identity privileges, and application dependencies. This allows teams to avoid costly emergency escalations, late-night patch cycles, and executive-level incident mobilization triggered by false-critical alerts.

By shrinking the actionable attack surface and eliminating noise-critical findings that plague traditional scanners, the organization sees material reductions in labor hours, fatigue-related errors, and cross-team coordination costs associated with classic vulnerability firefighting. Again, this will not likely result in reduced payroll FTE, since these staff will be reskilled or assigned to other tasks. External support (e.g., consultants) often will be reduced, however.

COST DRIVER 4: REDUCED CLOUD SPEND THROUGH UNUSED RESOURCE DISCOVERY

Orca's platform directly identifies wasted cloud spend, which can lead to reduced spend on cloud services by enterprise IT teams.

Because Orca continuously inventories cloud resources and detects unused, idle, misconfigured, or abandoned assets, including compute instances, storage volumes, snapshots, IP allocations, and shadow services, the platform directly drives measurable reductions in wasted cloud spend. These savings are rarely included in the CISO budget, so we do not include this in our ROI analysis, but the savings to the overall organization can be tangible and significant.

Note also that these savings can appear quickly, since organizations routinely uncover dormant workloads, excessive permissions, orphaned storage, or legacy environments that continue incurring charges. Orca's unified visibility enables finance, DevOps, and security teams to collaborate on cleanup actions that translate into immediate and recurring cost optimization across AWS, Azure, and GCP footprints.

COST DRIVER 5: REDUCED CI/CD SECURITY FRICTION THROUGH INTEGRATED APPSEC

With the use of Orca, there is no longer the need to maintain separate SAST, SCA, IaC, and container scanning tools, thus leading to savings.

By delivering integrated AppSec scanning for SAST-equivalent code issues, SCA vulnerabilities, IaC misconfigurations, container image risks, and pipeline governance, Orca reduces the need to maintain separate testing tools and the operational friction those tools introduce into CI/CD workflows.[10] Like the earlier driver on tool consolidation, this can have a significantly positive impact on overall ROI.

[10] It is important to recognize that Orca does a good job of consolidating a surprisingly large number of existing tools, systems, and platforms. This author has had the experience of helping to manage a large commercial security platform in telecom, and there is always a balance between having many features (requires a lot of product management attention) and having fewer features (keeps the platform simpler) With its extensive collection of capabilities, Orca has made the decision that a more feature-rich approach is worth the additional effort – and buyers thus experience more opportunities to drive ROI by replacing existing tools, systems, and platforms.

The key here is that teams benefit from a single policy engine, unified reports, and automated guardrails that prevent insecure deployments without forcing developers to navigate multiple portals or contradictory findings. This simplification improves developer velocity, lowers tool maintenance overhead, and reduces the hidden labor cost of reconciling divergent AppSec outputs across different stages of the software lifecycle.

COST DRIVER 6: LOWER INCIDENT RESPONSE AND BREACH-RELATED COSTS

Opus automation accelerates resolution and reduces downstream cost exposure, thus leading to improved ROI.

With Opus Security integrated into the platform, Orca accelerates incident response by orchestrating investigation steps, evidence gathering, enrichment, and recommended remediation paths. Faster containment and shorter dwell time directly reduce the tangible and intangible costs of cloud security incidents from potential data exposure and regulatory penalties to staffing surge requirements and business-operations disruption.

Automated workflows also minimize reliance on expensive external IR retainers and reduce the likelihood that a minor misconfiguration escalates into a costly breach. The result is a meaningful reduction in both the frequency and financial impact of cloud security incidents. As will be shown below, this is considered an important component of the annual savings for improving security via use of Orca.

QUANTITATIVE ROI: UPDATED CASE STUDY

Using the same methodological rigor applied in TAG's original analysis, we can now update the variables to reflect modern cloud environments. As with our prior analysis, we can make some reasonable assumptions about the target environment, although our experience is that these assumptions do not have major impact on the ROI. Instead, we see excellent return even as these assumed variables go up or down. That said, here are some assumptions we make:

- **Cloud-Based Assets Across Multi-Providers** – We assume here a total of 1,000 cloud assets that are scattered (presumably based on architectural and operational planning) across AWS, Azure, GCP.
- **Agent-Based Processing for Cloud Workloads** – In an agent-based processing environment, we can assume the need for roughly 2-3 agents per workload, which is highly consistent with traditional environments.
- **Security Practitioner Salary Estimates** – While consultants and externally-managed staff might be a bit more, we will assume that the average loaded full-time equivalent (FTE) cost in US dollars to be $190,000.
- **Consultants and Managed Staff** – We will assume that multiple salaried staff (FTE) are assigned to cloud security and that additional consultants are also employed to provide day-to-day operational assistance (at the assumed FTE rate).
- **Alerts Requiring Manual Support** – We will assume that 30–50% of alerts in this agent-based systems require manual triage – and this makes no distinction between the severity or length of time spend on alerts.
- **Opportunities for Consolidation** – Rather than focus on the overlap in expenditures for redundant tools, systems, and platforms, we will view the security tools in use today as being opportunities for Orca replacement.
- **AppSec Time and Effort** – While we would not expect to see reduced AppSec FTE salary costs through Orca deployment, it is worth noting that we assume 500–700 engineering hours per year devoted to AppSec toolchain maintenance.

• **Average Cloud Breach Cost** – We will assume that the organization expects to see roughly one major cloud breach per year at an estimated $1.3M in costs (e.g., legal, response, forensic, reporting) depending on the environment.

These assumptions are made to suggest a non-trivial enterprise environment, but one that could easily be adjusted upward or downward without too much mathematical effort. Salary estimates are based on average FTE numbers for 2025, and the various assumptions that we make with respect to the savings are also highly commensurate with both our experience at TAG in working with enterprise practitioners, as well as common sense determinations.

A reasonable ROI estimate can be obtained regarding the selection, installation, and deployment of the Orca platform into the environment described above. This is done by reviewing and estimating the cost impacts of such usage on each of the assumptions listed, using the cost drivers discussed earlier as important analysis factors. This results in an ROI that also can be easily tailored up or down depending on local environment circumstances.

We should also say that our bias in the development of an accurate ROI is toward cost drivers that have a tangible and measurable impact on the CISO-managed budget. This tends to reduce our emphasis on "hours saved," even though this is a meaningful qualitative improvement. Rather, we emphasize savings in terms of reduced incident costs, reduce contractor costs, and consolidation of tools. Here are the ROI impact estimates for the relevant factors:

1. **Reduced Contractor Costs** – This will be included as a likely driver in our analysis below. Readers who prefer to reduce staff costs through FTE or managed services (e.g., staff augmentation) can easily adjust the numbers to match any negotiated rates.

2. **Reduced Response Costs** – This is an important cost driver in the analysis below because the whole idea of upgrading any security platform is to reduce the likelihood of serious incident. We therefore include reduction in response costs as a useful ROI component.

3. **Savings Through Tool Consolidation** – The reduction that comes from consolidation of existing tools and platforms represents the third major component of the quantitative analysis we include below (based on reasonable existing tool assumptions).

A simple portion of the overall CISO budget can be used to demonstrate how the quantitative ROI is obtained. Figure 1 below shows a simple spreadsheet with assumed costs before the decision is made to install and use the overall Orca platform. We do not include unrelated costs in the overall budget since our ROI analysis involves savings measured against Orca platform cost, which we estimate below based again on reasonable assumptions.[11]

[11] It is critically important to emphasize that the assumed Orca license fee used here in the spreadsheet is not intended to be used as a guide for buyers to benchmark or compare their own licensing arrangement. Every situation is different and every license fee is based on factors that transcend a general ROI. This implies, obviously, that all aspects of an ROI, including the Orca fee used, are intended to provide general guidance on the direction of return and the types of quantitative and qualitative benefits that will accrue from use of the platform.

Portion of CISO Budget		Operating Expense (USD K / Annual)	Description
Cloud Security Platform Budget			**Tools used specifically to reduce cloud security risk**
SAST Platform		$350,000	Used to scan application code for vulnerabilities
SCA Platform		$350,000	Used to develop compositional views of software
CSPM Platform		$450,000	Provides posture analysis for multi-cloud environments
CWPP Platform		$450,000	Provides runtime protection for cloud workloads
	Subtotal	$1,600,000	
Cloud Security Staff Budget			**People involved in cloud security**
Payroll FTE Staff		$950,000	Employees assigned to work muti-cloud security
Non-Payroll Consultants		$380,000	Contractors to augment payroll FTEs
	Subtotal	$1,330,000	
Incident Response Budget			**Response costs expected during year**
Annual IR Retainer		$400,000	Fee paid as a retainer for rapid IR assistance
Major Incident Response		$900,000	Set aside in budget in advance of need to handle expected major incident
	Total	$1,300,000	
Portion of CISO Budget (Total)			**Baseline on which we will calculate ROI for Orca deployment**
	Total	$4,230,000	

Figure 1. Representative Budget Before Implementation of Orca

As can be seen in the spreadsheet in Figure 1, the security team is using three tools for cloud security, to which we assign highly representative license fees. The team is also using two contractors to assist with day-to-day cloud-related security, and a significant set-aside has been made to handle the inevitable cybersecurity incidents (it is unfortunate that CISOs are forced to budget for this type of sadly predictable situation).

The basis for our ROI is that by investing in the Orca platform (again, using a fee estimate that is not intended as a benchmark or baseline for any negotiated rates being discussed with Orca by readers), the existing tools licenses, the contractor fees for day-to-day assistance with cloud security, and the set aside to handle major incident response, reporting, and other fees can all be reduced.

By comparing the reduction of new fees shown in the spreadsheet in Figure 2 below, we can arrive at a reasonable quantified ROI for this case. As we have mentioned repeatedly above, we interact with many of Orca's customers on a routine, daily basis – and much of the sanity checking for these estimates and savings comes from our experience helping these teams to optimize and rationalize their budgets.

Portion of CISO Budget		Operating Expense (USD K / Annual)	Description
Cloud Security Platform Budget			**Tools used specifically to reduce cloud security risk**
Orca Platform		$600,000	Unified coverage of multi-cloud security functions
	Subtotal	$600,000	
Cloud Security Staff Budget			**People involved in cloud security**
Payroll FTE Staff		$950,000	Employees assigned to work muti-cloud security
Non-Payroll Consultants		$190,000	Reduce contractors augmenting payroll FTEs by one (1)
	Subtotal	$1,140,000	
Incident Response Budget			**Response costs expected during year**
Annual IR Retainer		$300,000	Fee paid as a retainer for rapid IR assistance
Major Incident Response		$400,000	50% reduction in budget in advance of need to handle expected major incident
	Total	$700,000	
Portion of CISO Budget (Total)			**Baseline on which we will calculate ROI for Orca deployment**
	Total	$2,440,000	

Figure 2. Representative Budget After Implementation of Orca

The specific ROI calculation we can make here is quite straightforward – and we assume throughout that since the last ROI calculation we created for Orca several years ago that security teams have become more efficient. So, while the qualitative ROI has arguably grown since then, the quantitative ROI is slightly more modest – albeit still quite impressive. Here is the calculation we used:

1. The purchase of Orca was assumed to be $600,000.

2. Its implementation resulted in a savings of $1,190,00 in operating expenses.

3. This can be viewed as a return on investment (ROI) of approximately 198.33%.[12]

In our view as analysts, this type of savings represents a meaningful improvement in an annual operating budget. The obvious trend in CISO budgeting in 2026 and beyond involves rationalization and reduction in overall security budget, which implies that any initiative that can help to drive operating costs down will be not only important, but in some environments, an absolute requirement.

SAMPLE INSIGHTS FROM MODERN ORCA CASE STUDIES

To illustrate the ROI analysis in real-world experience, primarily from a qualitative perspective, TAG reviewed some enterprise case studies published by Orca that illustrate how the platform performs under operational conditions. While each organization's environment will differ, the two examples below show consistent themes around noise reduction, operational efficiency, and accelerated remediation, all referenced in this report.

SWIGGY CASE STUDY – ALERT REDUCTION AND OPERATIONAL EFFICIENCY

Swiggy is a large, cloud-native digital services company that operates at significant scale. The company adopted Orca to address growing alert fatigue and limited visibility across its expanding cloud footprint. This type of company with this type of experience in security operations is precisely the type of customer that is directly in the crosshairs of Orca's cloud security platform.

Prior to Orca, Swiggy's security team claims to have relied on multiple tools that generated large volumes of unprioritized findings, forcing analysts to spend disproportionate time on manual triage. By deploying Orca's agentless CNAPP with reachability-based prioritization and attack-path analysis, Swiggy reported reduction in cloud security alerts by approximately 75 percent, focusing attention only on risks that were actually exploitable.

Equally important from an ROI perspective, Swiggy operationalized a unified cloud-risk dashboard in a matter of days, eliminating lengthy integration and accelerating time-to-value. Investigations that previously required pivoting across tools were streamlined using Orca's contextual findings and AI-assisted triage, shortening investigation cycles to keep pace with rapid cloud change without adding headcount or external support.

These outcomes align directly with TAG's modeled assumptions around reduced alert investigation time, improved prioritization, and lower operational friction. We would expect that readers with local conditions comparable to Swiggy's would experience similar types of qualitative advantages. The manner in which this would influence budget would be dependent on the local operating and staffing situation.

[12] The formula used here is the ROI equals the net return divided by the cost of investment times 100%. Thus, net return is $1,490,000 - $600,000 which equals $890,000. Dividing this by $600,000 and multiplying by 100% produces 148.33%.

LATITUDE FINANCIAL CASE STUDY – TOOL CONSOLIDATION AND POST-INCIDENT MATURITY

Latitude Financial, a major financial services organization, turned to Orca following a high-profile security incident that exposed limitations in its fragmented cloud-security stack.[13] Operating across multiple cloud platforms and Kubernetes environments, Latitude faced challenges maintaining consistent visibility, correlating risks across tools, and executing coordinated response workflows.

By deploying Orca, the organization gained comprehensive, agentless visibility across its multi-cloud estate, including workloads, identities, data stores, and Kubernetes resources, all within a single platform. From a financial and operational standpoint, Latitude was able to consolidate several point solutions into Orca's unified CNAPP, reducing both licensing costs and the overhead associated with managing multiple vendors and integrations.

The platform also strengthened incident-response workflows by providing clearer attack-path context and faster access to remediation guidance, helping the organization mature its cloud-security posture post-breach. These outcomes closely mirror the ROI drivers highlighted earlier in this report, particularly tool consolidation, reduced response costs, and improved resilience against future incidents.

CONCLUDING REMARKS

As should be evidence from our extensive discussions and ROI analysis above, the 2025 Orca Cloud Security Platform delivers significant value to enterprise security teams. By combining agentless cloud protection with full-spectrum AppSec, CIEM, DSPM, agentless reachability analysis, Opus workflow automation, and the new AI Assistant, Orca stands as one of the industry's most comprehensive cloud-native security platforms.

For enterprise teams seeking measurable reductions in cloud-security operating costs, simplified workflows, and a meaningful improvement in cloud risk posture, Orca offers a strong and demonstrable return on investment. TAG recommends that enterprise teams explore their local environment using Orca's updated ROI calculator and map their own agent overhead, tooling spend, and remediation workloads to quantify the savings opportunities.

---

[13] Details on the incident can be found here: *https://www.latitudefinancial.com.au/latitude-cyber-incident/*.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence.