JOINT SOLUTION BRIEF

zscaler™ + Orca SECURITY

Gain End-to-End Visibility, Enrich Risk Prioritization, and Streamline Remediation with Zscaler and the Orca Cloud Security Platform

INTEGRATION HIGHLIGHTS

- Sharpen risk prioritization in Orca with ZPA context for trusted access
- Enrich UVM vulnerabilities with comprehensive cloud intelligence from Orca
- Accelerate time to investigate & remediate vulnerabilities

The Market Challenge

Today's enterprise technology stacks are complex – with distributed applications, users, and endpoints, an ever-expanding list of IoT devices, and new sanctioned/unsanctioned tools being deployed daily. As attack vectors multiply, from endpoints to networks to the cloud, security teams struggle to secure their valuable assets inside & outside the traditional network perimeter.

The more security controls that security operations teams deploy, the more alerts they get, but the signal often gets buried in noise. Security analysts are forced to pivot between tools that do not integrate and fail to connect the dots across the entire technology stack. As a result, security data is collected and analyzed in isolation, without any context or correlation, creating gaps in what security teams can see and detect, leading to longer dwell times.

This complexity has necessitated a new approach to centralized vulnerability management.

The Solution

Together, Orca Security & Zscaler connect the dots between access control and risk to your cloud native application assets, while enriching vulnerability management with Orca intelligence.

The **Orca Cloud Security Platform** helps organizations identify, prioritize, and remediate risks to protect cloud native apps across the entire software development lifecycle—from pre-deployment through runtime.

By integrating **Zscaler Private Access (ZPA)** with Orca, customers connect the dots between trusted access and suspicious activity alerts to eliminate false positives and drive better risk prioritization.

By ingesting Orca intelligence into **Zscaler Unified Vulnerability Management (UVM)**, customers enrich UVM findings with vulnerability intelligence from Orca, resulting in deeper visibility, more effective prioritization, and faster remediation.

Together, Orca Security & Zscaler connect the dots between access control and risk to your cloud native application assets, while enriching vulnerability management with Orca intelligence.

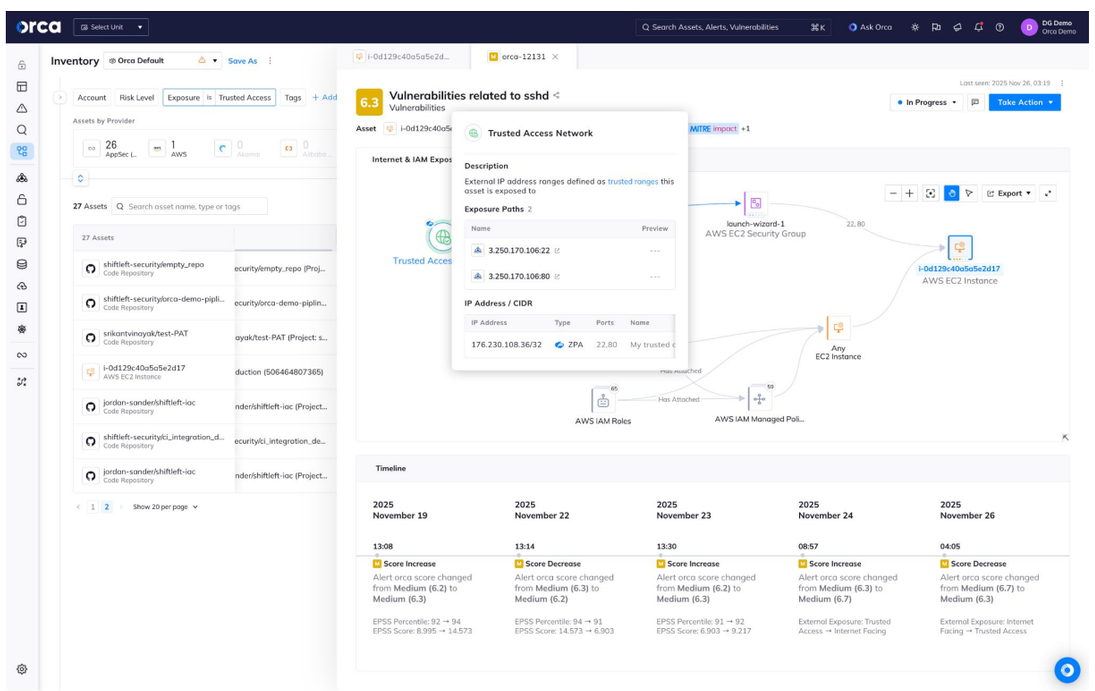
Solution Components Deep Dive

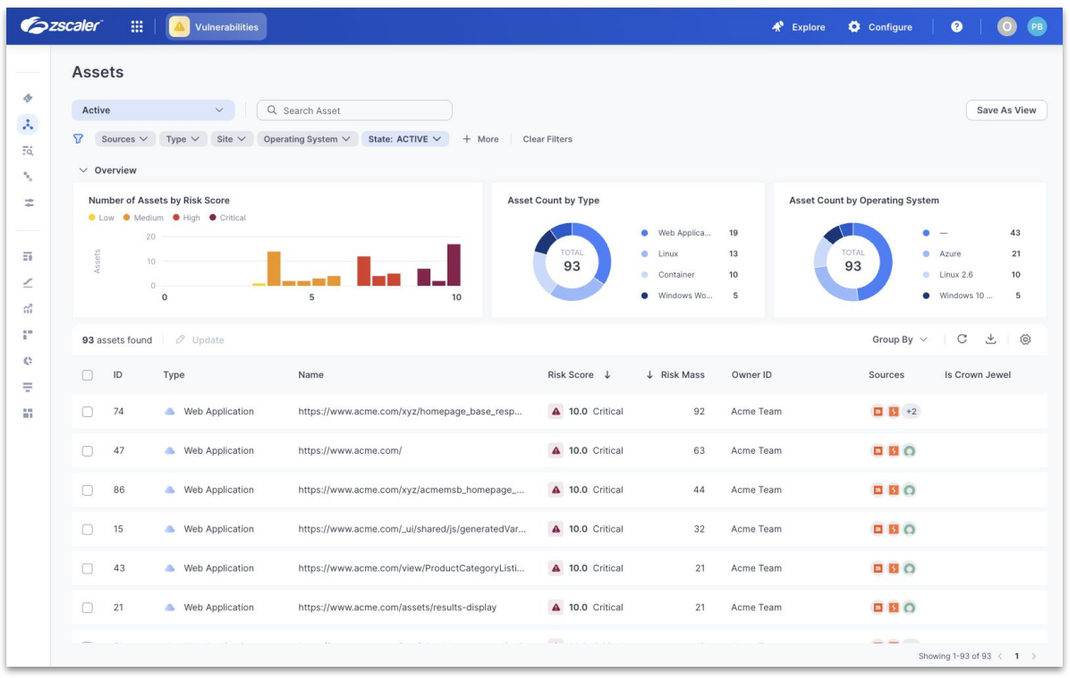
Orca scans the entire cloud estate, including VMs, containers, Kubernetes clusters, serverless functions, and more. The Orca Platform leverages 20+ vulnerability data sources to discover & prioritize vulnerabilities across your cloud environment.

Contextualize External Exposure for More Precise Risk Prioritization

Orca runs an external scanner to automatically discover web and API assets in your cloud environment, then systematically assesses their external exposure from the public internet by sending HTTP GET requests and analyzing the responses.

When Orca flags a "malicious or suspicious IP" alert, it now checks whether that IP belongs to a ZPA managed/egress pool or is tied to a private-app connector. If the destination is verified by ZPA context, Orca can dynamically lower severity or suppress alerts, freeing security teams to focus on the truly unknown or untrusted risks.





Enrich Vulnerabilities for Deeper Visibility and Faster Remediation

Intelligence passed from Orca to Zscaler UVM includes:

- **Vulnerabilities**: A full, prioritized list of vulnerabilities across your cloud estate, enriched with CVSS data, fix availability, asset & account information, trending status, exploitability, CISA Kev status, EPSS score, and much more.
- **Alerts**: Prioritized, contextual risks that include a numerical & dynamic risk score; detailed analysis across 14 risk factors; affected assets; graph visualizations of attack paths, exposures, & blast radiuses; vulnerable packages; CVSS details; remediation instructions; and more.
- **CVEs:** Enriched CVE data, including trending status, EPSS probability, CISA KEV assignment, affected asset information, associated packages, CVSS details, related alerts, and more.
- **Assets:** Comprehensive asset intelligence, including system & workload metadata, associated & prioritized risks, attack paths, IAM & configuration data, software inventory with reachability context, compliance posture, network exposure, forensic snapshots, cloud logs, and more.

"Together, Orca Security & Zscaler deliver deep, unified visibility across cloud & network environments - enabling customers & partners to identify, prioritize, & respond to risks faster & with greater confidence."

John Tavares

SVP, Worldwide Partner & Alliances Sales, Orca Security

KEY USE CASES

Prioritize cloud & application risk in the larger security context across the business

Customers can ingest Orca's detailed analysis of security issues across 14 different risk factors, centralize vulnerability management, & customize risk scoring in Zscaler UVM, allowing security operations to standardize risk prioritization across more security domains.

Accelerate remediation with Cloud-to-Dev tracing & deep cloud infrastructure intelligence

Reduce the time spent on hopping between tools to investigate cloud-native application security issues & propose remediation steps. Enrich Orca's deep analysis of running workloads & the code repos that originate security issues with other data sources in Zscaler UVM.

Zscaler + Orca Security Benefits

ACTION	DESCRIPTION
Improve risk prioritization	Integrating ZPA with the Orca Platform removes false positives from suspicious activity alerts, automatically deprioritizing or suppressing alerts. Pushing Orca intelligence to Zscaler UVM shares cloud context to support remediation.
Customize risk scoring with more context	Use Zscaler UVM to modify risk scoring using fields & risk factors from the Orca Platform. Adjust the scoring model to reflect your business context so that cross-functional teams are aligned to a common calculation of risk.
Reduce time to investigate & validate risk	Bringing Orca intelligence into Zscaler UVM centralizes, harmonizes, & deduplicates security findings while unifying the context necessary to validate the risk & establish remediation steps.
Accelerate remediation with unified context	Eliminate the usual time-intensive hunt-&-summarize cycle that team members follow to propose remediation steps, test solutions, and close out alerts.

Conclusion

Make vulnerability remediation faster & more impactful with Zscaler & Orca Security. Unify security across your organization and extend risk prioritization across cloud infrastructure, application security, network, endpoint, and beyond with Zscaler & Orca Security.

Learn more at **www.zscaler.com/partners/technology**

zscaler™ | **Experience your world, secured.™**

About Zscaler: Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, & secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks & data loss by securely connecting users, devices, & applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

©2025 Zscaler, Inc. All rights reserved.