SOLUTION BRIEF

Enhance Security Intelligence By Integrating Orca Security's Comprehensive Cloud Security Data Into Your Snowflake Security Data Lake.

Establish a modern security data lake by integrating Orca's context-rich cloud security data and telemetry into Snowflake's Data Cloud to enable powerful analytics, accelerated detections, and speedy investigations.

Big Data and Cloud Security Challenges

As enterprises move to the cloud, traditional security solutions are unable to keep up with the scale and complexity of infrastructure, application, and data security. The resulting limitations and visibility gaps make it difficult to effectively identify and remediate risks. Early attempts to solve this problem failed to collect, combine, correlate, and format the data into actionable use cases for security teams.

On the other hand, modern cloud data platforms are built for cost-effective analytics at a massive scale but lack the security integrations and out-of-the-box analytics that security teams require.

The Solution: Orca + Snowflake

Orca Security and Snowflake have partnered to enable organizations to seamlessly integrate Orca's context-rich cloud security data for visibility, analytics, and intelligence-based incident response with other security and business data that is stored in Snowflake for near-unlimited time. With this integration, customers can use the Orca Cloud Security Platform for complete coverage across cloud risks — spanning misconfigurations, vulnerabilities, identity, data exposure, insecure APIs and advanced threats. All of this data is populated into a unified data model, which automatically prioritizes the attack paths - or toxic combinations of interrelated risks - that pose the greatest impact on the organization, and stores it on top of their existing Snowflake Data Cloud.

Orca Security and Snowflake have partnered to enable organizations to seamlessly integrate Orca's context-rich cloud security data for visibility, analytics, and intelligence-based incident response with other security and business data that is stored in Snowflake for near-unlimited time.

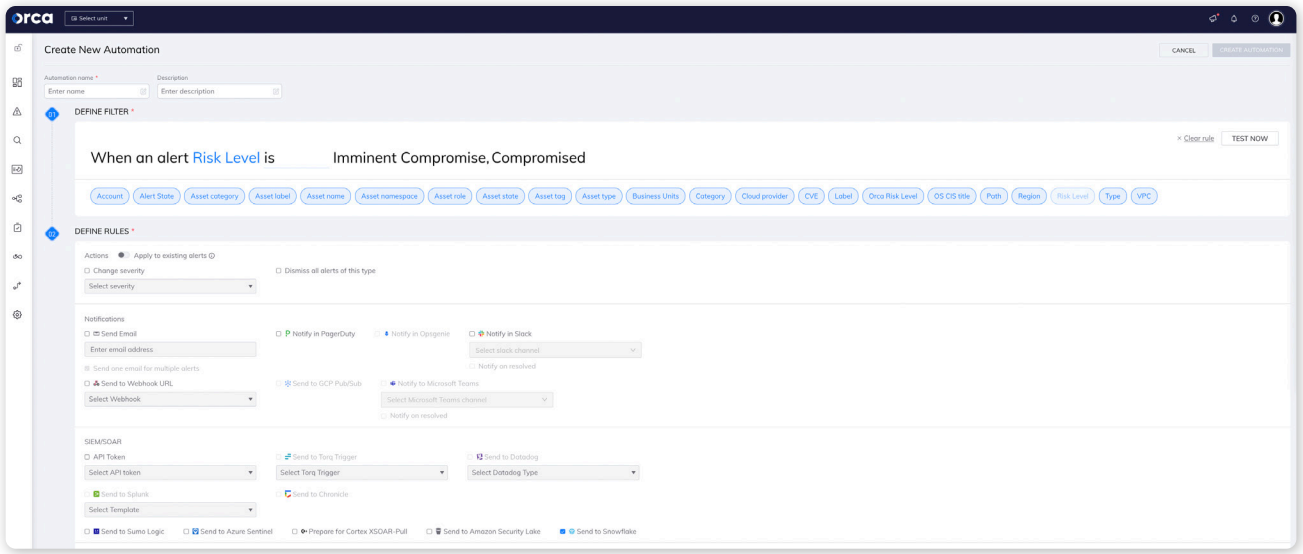
Unlike traditional siloed cloud security solutions that require multiple tools and deployed agents to gather and consume their security data, Orca and Snowflake have joined to leverage Orca's unique Agentless approach to gathering all of the valuable cloud security data and telemetry, and positioning it to be optimally stored within the Snowflake Data Cloud for longer periods of time, helping customers get the most value out of their security data. With the solution, organizations can consolidate their entire cloud estate, enterprise and security data into a single location and take advantage of advanced analytics for detection and response spanning across the entire organization's security footprint.

- **Collection:** All of the customer's cloud security data and telemetry can be collected through a single-source, and stored in a single place — removing the friction that comes from working through multiple, siloed integrations.
- **Enrichment:** Customers will be able to conduct advanced forensic security incident analysis as well as optimized threat hunting with access to historical data.
- **Correlation:** Orca's unique security data can be stored in customers' Snowflake accounts to enable them to consume it, while expediting correlation efforts with other existing company data the customer may already have in their Data Cloud (e.g. company employee HR information, etc).
- **Action/Response:** Customers utilizing this solution may experience faster and more accurate responses, enabling data-based decisions.

Solution Benefits

Consolidate Your Security Data in One Place: Unify your logs and enterprise data in a single place and store virtually unlimited amounts of data for years.

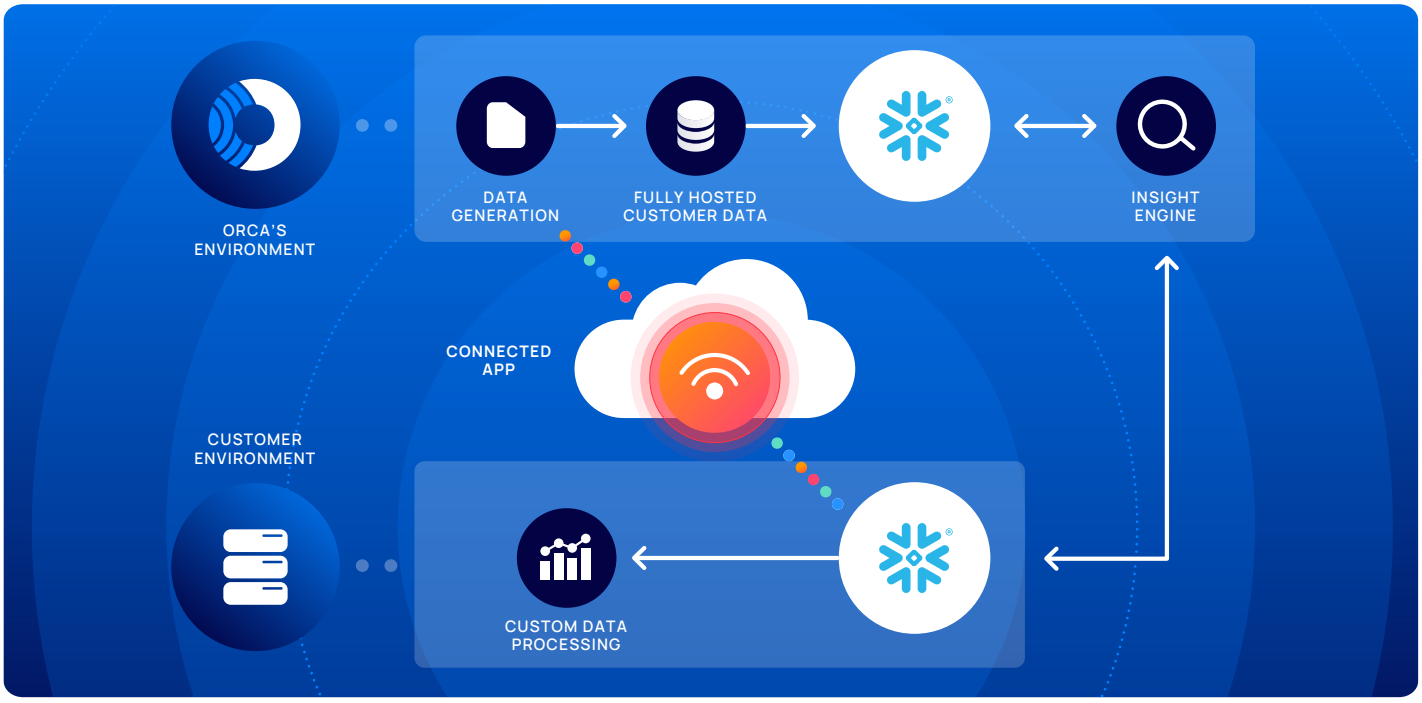
ORCA + SNOWFLAKE OUTCOMES	CUSTOMER BENEFITS
Run Advanced Analytics Like Never Before: Customers can combine business data sets, not normally sent to a SIEM, with contextual cloud security data to achieve better fidelity and automate correlation. Combine the latest attack path context from Orca Security to identify new or emerging threats that put your organization's most critical assets at risk.	**More efficient analytics, correlation, and response to your most important risks**
One Platform, Many Cloud Security Use Cases: Integrate Orca's comprehensive context and telemetry for faster risk prioritization and response. You can take advantage of up-to-date context to identify the latest sophisticated attack vectors, vulnerabilities, and misconfigurations.	**Improved overall security intelligence and confidence**
Elastic Compute Power and Instant Scalability: The Snowflake Data Cloud's separation of compute and storage allows investigations to run at groundbreaking speed. By automatically scaling compute resources up and down, you only pay for what you use. This allows you to focus on mission-critical activities without worrying about concurrency, resource contention, compute power, scalability, or cost.	**Cost optimized security data storage with faster triage**
Avoid Siloed Security Data: No longer maintain, manage, and govern separate enterprise and security data repositories. Centralize your data management for more control, correlated intelligence, and ease of use.	**Better visibility, comprehension and prioritization of organizational security risk**



Deployment Architecture Details

Orca has adopted Snowflake's connected application architecture which enables Orca to function as the customer's front end for cloud security coverage, context, and consumable data and telemetry, while storing all of the data and insights in customer's Snowflake for long term retention. Furthermore, customers have the ability to sign into Snowflake natively to use Orca's insights for additional analysis, ad-hoc investigations, threat hunting and more.

Customers can utilize Snowflake's scalable architecture for cost-effective and optimized cloud storage and data retention. Compute power is virtually unlimited and can be scaled as needed for rapid investigations across terabytes and petabytes of data. Additionally, Snowflake's consumption-based pricing means that you only pay for resources when used, which translates into significant cost savings overall.



Orca Security + Snowflake for Detection and Response

Integrating Orca's cloud security data with Snowflake allows customers to centralize the management of the entire data lake. Seamlessly merge your Orca cloud security data with other 3rd party security data within Snowflake for more readily accessible and actionable data. By combining Orca with the rest of your security data in Snowflake's central repository, organizations will remove the data silos and have access to more holistic visibility across their data which will give teams greater insight, forensics, and analysis of their entire security posture.

Gain complete visibility, actionable insights, better automation, and significant savings using Orca Security with Snowflake.

Quickly comprehend and centralize complete security coverage of your entire cloud estate with Orca Security and Snowflake. Learn more here: https://www.youtube.com/watch?v=AnPKGOwGoFE

ABOUT Orca Security

Orca Security is the industry-leading Cloud Security Platform that provides complete coverage and centralized context of your entire cloud estate, enabling security practitioners to spend less time correlating long lists of disconnected alert and focus on remediating the actual risks that have the most impact on the business. Founded in 2019, Orca is trusted by hundreds of customers globally.

orca.security

ABOUT Snowflake

Organizations use Snowflake's Data Cloud to unite siloed data, discover and securely share data, and execute diverse analytic workloads across multiple clouds and geographies. Organizations, including 573 of the 2022 Forbes Global 2000 as of January 31, 2023, use the Snowflake Data Cloud to power their businesses. Learn more:

snowflake.com