



Supercharge Your Alerts with Contextual Intelligence from Orca Security and AWS GuardDuty

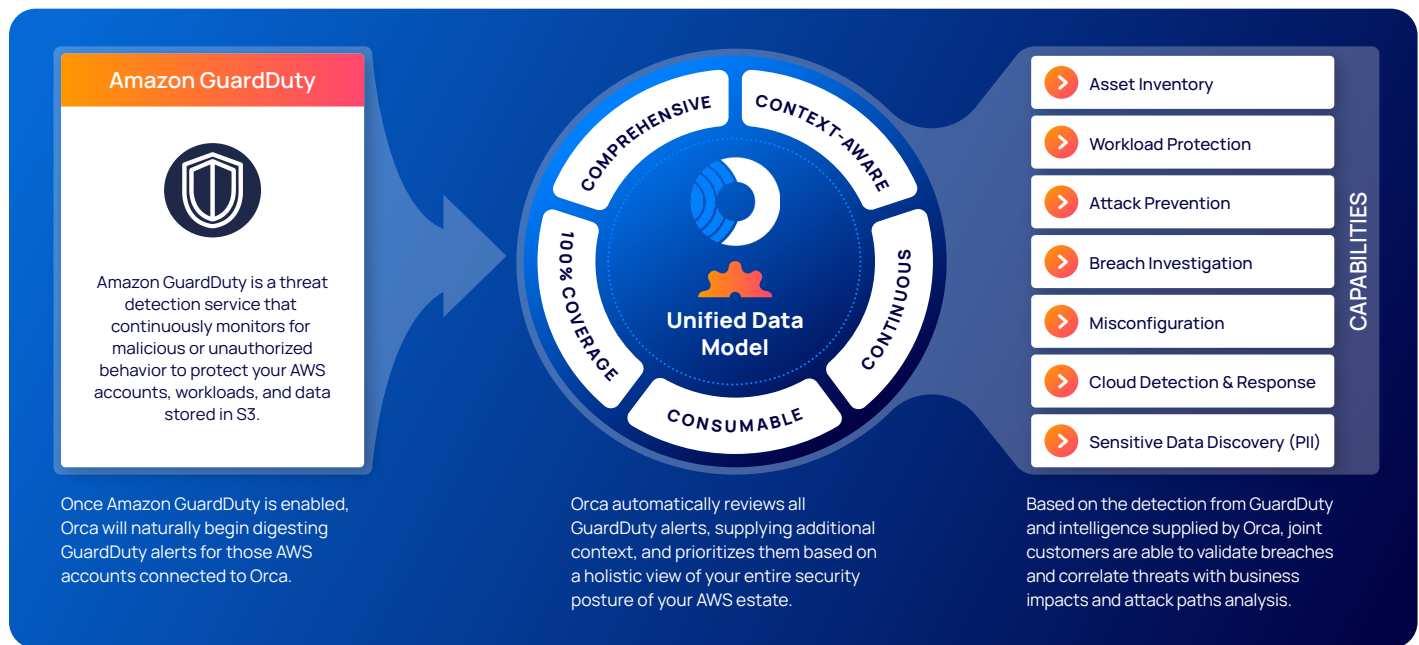


Amazon Web Services (AWS) offers many security services to help users protect their data and environments. One of the more well-known services for continuous security monitoring and threat detection is Amazon GuardDuty.

Amazon GuardDuty is a continuous threat monitoring service available to AWS customers that works by consuming CloudTrail logs (AWS native API logging), Virtual Private Cloud (VPC) flow logs and DNS logs. Since GuardDuty is gathering intelligence from a multitude of public and AWS-generated data feeds and is powered by its machine learning capabilities, GuardDuty is able to analyze billions of events in pursuit of trends, patterns, and anomalies that are turned into recognizable signs that something is amiss.

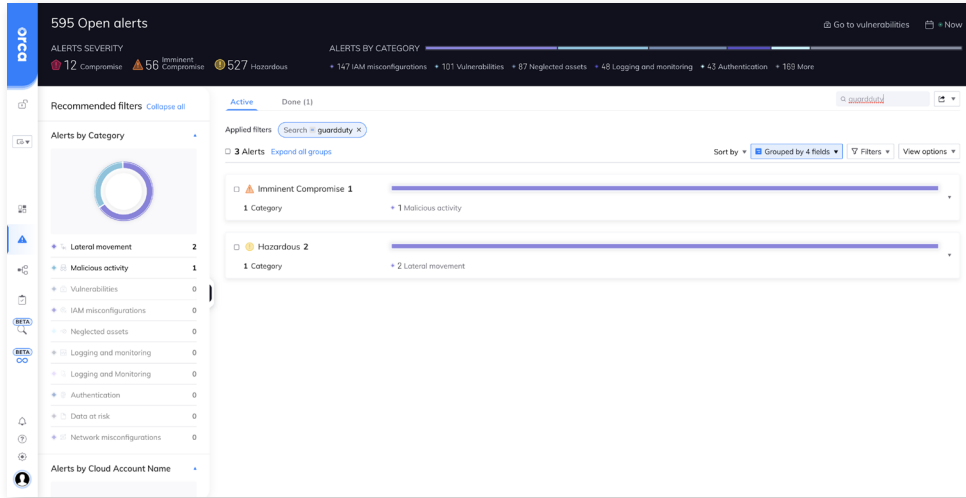
AWS GuardDuty operates completely on AWS infrastructure and does not affect the performance or reliability of your workloads. Similar to the Orca Cloud Security Platform, users do not need to install or manage any agents, sensors, or network appliances in order to activate powerful risk prioritization and threat detection capabilities.

Understand the full story around **malicious activity detected by GuardDuty** and what further **impact or risk it poses to your AWS environments with Orca.**



Orca Security + Amazon GuardDuty: Better Together

The Orca Cloud Security Platform leverages Amazon GuardDuty as supplemental triggers for alerts to help customers prioritize cloud events and respond effectively. Together, the platforms allow mutual customers to continuously monitor malicious activity and unauthorized behavior in your AWS accounts, workloads, and data stored in Amazon S3.



Orca digests alerts from GuardDuty, and layers on comprehensive contextual information around the alert to provide the basis for triage and prioritizing responses. AWS GuardDuty alerts are evaluated by Orca to prioritize those alerts that should be responded to first, based on selected compliance frameworks, attack path analysis, sensitive data, etc. Orca provides investigative content and rules for sorting these alerts, derived from our patented SideScanning and our Unified Data Model.



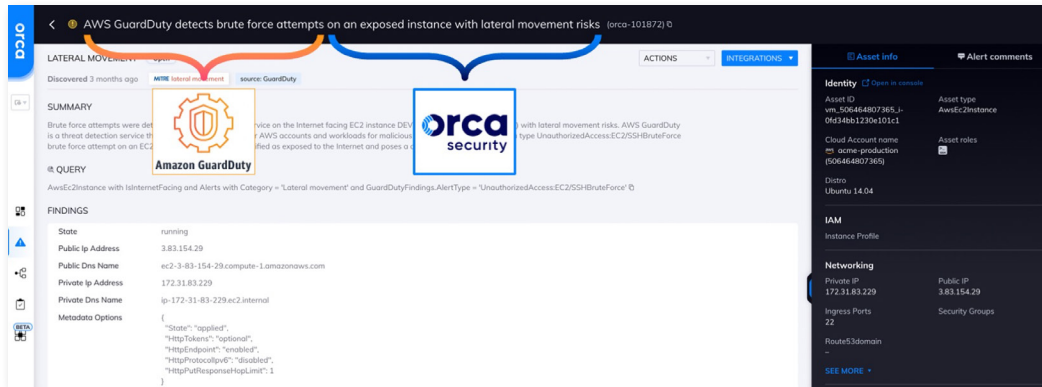
“This integration delivers a lot of value. GuardDuty helps us discover what is actually happening, while Orca can correlate those discovered incidents into what the potential risk is based on our environment. It helps us understand the full scope of the attack or potential attack, and see the full story and impact on our business.”

- Opher Hofshi, Cyber Security Architect | Wix

ORCA ADDED FEATURES	CUSTOMER BENEFITS
<p>Better Visualization: See how this alert might play a role in a much larger attack path that could lead to the compromise of more sensitive data.</p>	<p>Better prioritization of risk</p>
<p>More Context: Understand why an alert matters with a summary digest, along with recommended remediations.</p>	<p>More efficient remediation of risks</p>
<p>Accurate Classification: Group GuardDuty and other AWS alerts together based on compliance, severity, asset or risk type.</p>	<p>Improved alert intelligence</p>

Escalating the severity of a GuardDuty alert based on Orca's holistic intelligence


In this scenario, AWS GuardDuty detected brute force attempts to access an EC2 instance. Furthermore, the Orca Platform recognized that this was indeed an internet-facing asset that could pose additional lateral movement risk.



Orca received the initial SSH alert from GuardDuty, and added additional context and enrichment that actually increases the prioritization of this alert, moving the finding from a behavior anomaly to an increased level of detected risk.

Combining GuardDuty malicious and threat behavior alerts with Orca's posture analysis provides shared customers with more intelligence for better prioritization and more efficient risk classification. By correlating GuardDuty's alert with Orca's context-rich platform, customers are able to correlate the RDP brute force attempts to the state of the asset/machine, confirming if the brute force attempt worked, and if the asset became compromised.

Orca can also provide a series of additional risks associated with this asset, such as sensitive data (PII, Social Security Numbers), service vulnerabilities, and unsupported host operating systems that could also prove hazardous to this asset. Furthering the customer visibility, Orca also illustrates the potential attack chains, as well as displays login history and other important data regarding all the risks associated with this EC2 instance.

 **Quickly comprehend and centralize complete security coverage of your entire AWS cloud estate with GuardDuty and Orca**

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 alerts, and spend more time remediating the actual risks that have the most impact on the business.

ABOUT AWS GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.



Connect your first cloud account in minutes and see for yourself at: <https://orca.security>

