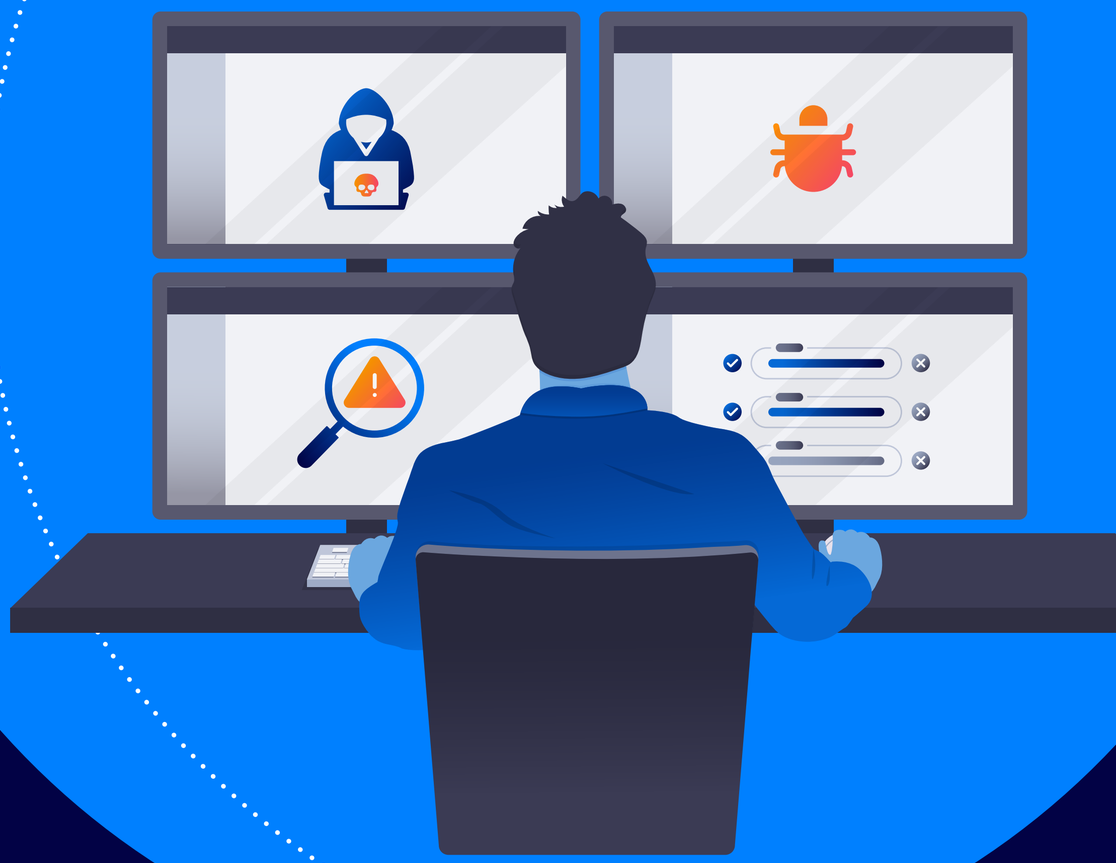
orca security

EBOOK

The Essential Guide to Cloud Detection and Response



Introduction

Cloud Detection and Response (CDR) is an emerging category of solutions that focuses on detecting active attacks in cloud environments and provides organizations with the information and tools needed for security teams to investigate and respond to these attacks.

In this guide, we explain the current types of detection and response solutions available today, and why a new Cloud Detection and Response category is needed for the cloud. In addition, we describe what defines a CDR solution, the benefits of using CDR, and key features.

For organizations wanting to learn more about CDR, or are starting to evaluate CDR solutions, this guide will provide insights on how CDR helps security professionals, Security Operations Centers (SOCs), and Incident Response (IR) teams detect and prevent cloud attacks.

The State of the Cloud Threat Landscape

The adoption of public cloud infrastructure to build, store, and deploy applications and workloads continues to increase, with Gartner predicting a 20.4% increase in worldwide spending on public cloud services in 2022. With the advent of cloud native application architectures, such as containers, Kubernetes, and serverless, it is now even easier for organizations to deploy their applications in the cloud, and enjoy benefits such as reduced costs and increased agility.

In 2021, 98% of companies experienced a cloud data breach in the last 18 months, up from 79% in 2020

However, organizations are starting to understand that they cannot just use their on-premises security solutions for the cloud. According to an IDC survey, in 2021 98% of companies experienced a cloud data breach in the last 18 months, up from 79% in 2020. In a recent survey conducted by 451 Research, 46% of respondents said that security and compliance concerns represent the top concern of using cloud-native technology.

When it comes to securing cloud workloads, many cloud security tools are focused on identifying and alerting to potential risks, such as control plane misconfigurations, workload and application vulnerabilities, permission and entitlement risks, insecure secret management, and compliance violations. However, to detect and respond to cloud attacks, organizations have had to rely on using traditional, on-premises tools for the cloud that only provide limited insight and can therefore lead to missed attacks and high rates of false positives.

What is Detection and Response?

In larger organizations, the **Security Operations Center (SOC)** or **Incident Response (IR)** team is tasked with 24/7 monitoring of systems to ensure smooth operations and protect against attacks. In smaller organizations, the IT team typically will be tasked with this, or the functions could be outsourced, such as to an **MDR (Managed Detection & Response)** services offering.

SOC and IR Team Frameworks

MITRE ATT&CK (MITRE Adversarial Tactics, Techniques, and Common Knowledge) is a framework for understanding cyber adversary behavior and the different phases of an attack lifecycle to improve threat detection. For cloud attacks, they maintain a separate framework, called MITRE ATT&CK Cloud Matrix.

NIST Cyber Security Framework (CSF) is a set of guidelines that help organizations detect, respond, prevent, and recover from cyber attacks.

Detection and Response Solutions

There are several types of security solutions that help organizations detect threats and respond to cyber attacks in progress. For all of these solutions, “D” stands for detection, i.e., the ability to identify a threat, and “R” is for response, the broadly defined capability to isolate, prevent, expel, and/or remediate the threat.

Threat detection solutions available today include:

Endpoint Detection and Response (EDR)

EDR solutions focus on endpoints, primarily on-premises workstation computers and servers, considering each as a potential attack vector. EDR solutions use agents to record activity taking place on the endpoint, and then use this data to detect potential threats through anomaly detection, machine learning, and other approaches. These tools also offer a varying range of response capabilities, which may include actions that trigger alerts, isolating the machine from the network, rolling back to a known good state, deleting or terminating threats, or generating forensic evidence files.

Network Detection and Response (NDR)

As opposed to focusing on the endpoint, NDR detects threats through an analysis of data observed from the network traffic that flows through the organization. NDR vendors most commonly use a network sensor (a physical or virtual appliance) to look for potential threats based on anomalous or unauthorized protocols, port utilization, odd timing and transfer sizes, and more.

Threat Detection & Response (TDR)

TDR typically is divided into two categories — endpoint TDR and analytical TDR, with both looking to solve big data challenges and gather information most relevant to a current threat. Unlike full-scale EDR platforms, endpoint TDR tools record data only after a credible threat is occurring or only check in on specific events or processes most likely to reveal a threat. Analytical TDRs on the other hand leverage existing data and apply analytics to decipher what is actually a threat.

Extended Detection & Response (XDR)

A hybrid of EDR and NDR solutions, XDR platforms ingest endpoint agent data, network level information, and in many cases device logs. This data is correlated, and detections can be made from one or many sources of telemetry. The advantage of XDR is its ability to combine multiple sources of telemetry, including data from endpoints and their relationships, to achieve a big picture overview.

Why a New Approach is Needed for the Cloud

Many organizations have deployed one of the above solutions to the cloud.
However, they are finding that these solutions don't scale in the cloud for the following reasons:

Unsuitable for dynamic environments

Existing detection and response systems are focused on on-premises networks and endpoints; these systems were not built for the cloud with its ever-changing and ephemeral cloud-native workloads.

Agent-based with limited visibility

EDR, TDR, and XDR solutions rely on agents to obtain workload telemetry and can only achieve limited coverage. Since it is virtually impossible to deploy agents everywhere, and agents do not support every operating system, these solutions will inevitably lead to blind spots in the cloud estate. On average, Orca Security research found that less than 50% of assets are covered by cloud workload protection solutions.

No insight into the control plane

EDR, TDR, and XDR solutions only detect risks at the cloud workload level - not the control plane. This lack of insight results in the inability to understand which events are truly dangerous, and which events produce false positives that slow down investigation efforts and remediation.

What is Cloud Detection and Response (CDR)?

Given the shortcomings of existing solutions, a new category of solutions is emerging, specifically designed for detecting and responding to attackers in the cloud. The main objective of **Cloud Detection and Response (CDR)** is to detect cloud attackers who have breached the perimeter controls of cloud resources and applications. By continuously providing SOC and IR teams with contextualized data on potential malicious activity in the cloud environment, CDR accelerates investigation, triage, and response to cloud attacks.

Collect Analyze Detect

Agentless versus Agent-based

CDR solutions detect cloud threats by ingesting and analyzing logs and feeds to detect when anomalous events and behaviors may indicate an attack in progress. Feeds can include cloud service provider logs, VPC flow logs, Kubernetes audit logs, instance logs, and threat intelligence feeds. In order to process this vast amount of data, CDR tools use machine learning and AI to analyze large volumes of 'big data', including accounts, privileges, configurations, and activity from cloud services to provide insights, situational context, and visibility.

There are two types of CDR solutions:

Agent-based CDR solutions that utilize an agent installed on the workload to access workload data, and combine information from the endpoint, traffic analysis, cloud workloads (those that have an agent deployed), cloud traffic and audit logs, as well as data available from the cloud service providers.

Agentless CDR solutions that utilize a snapshot scanning approach that collects data externally from the workloads' runtime block storage (data plane) and retrieves cloud configuration metadata via APIs (control plane). All of these combined are used to gain a contextual understanding of the most urgent cloud threats.

How does CDR work?

As with traditional on-premises detection and response solutions, there are typically four stages in which CDR brings value to customers:

1. **Detection -** continuous or frequent monitoring for attacks across cloud services feeds with alerting capabilities

2. **Investigation -** review of attack steps, techniques, and timelines, and analysis of available data to determine a needed response to the threat

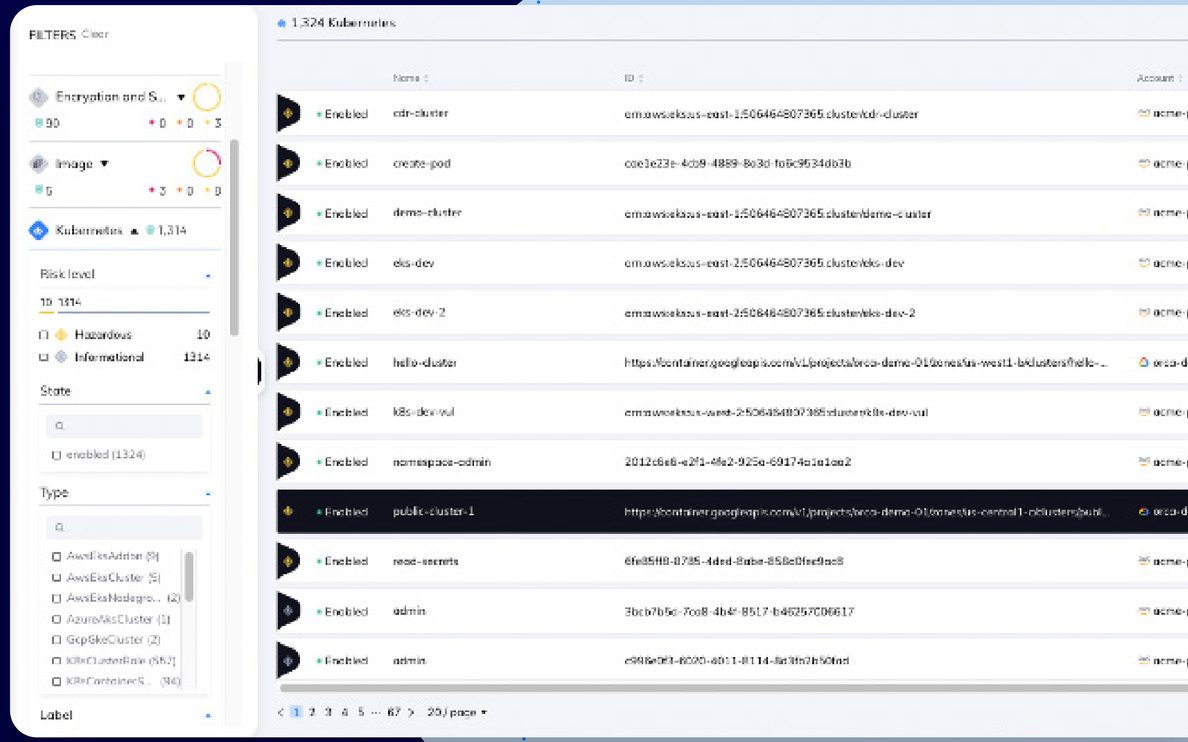
3. **Response -** capabilities that focus on ensuring cloud threats are contained before they can do damage, such as auto-remediation or automatic forwarding to ticketing systems

4. **Resilience -** post-mortem investigation, conclusions, and potential remediations. That is, based on available data, identifying—and fixing—the sources and vulnerabilities that led to the attack in order to help prevent future threats and strengthen security. A good analogy of this would be when you identify a leak on a boat: you will first try to patch the leak through whatever means available, and then once the immediate danger is stemmed, go back and try to find out why the leak occurred and how it can be prevented in the future. Likewise, following the threat mitigation, you would investigate the root cause, and take actions—patching, encryption, stricter IAM policies—that would harden your cloud environment.

5 Essential CDR Capabilities

1. Complete Asset Coverage

An effective CDR solution needs to cover all of your cloud assets, whether they are VMs, containers, or serverless, and automatically include new resources as your cloud estate expands. A primary challenge of agent-based solutions is the inability to provide complete coverage, since it is simply impossible to install an agent on every asset, either due to the fact that operating systems do not support agents, or because IT systems can simply not keep up with the speed at which cloud assets are being spun up and torn down on demand. However, an agentless solution automatically covers all cloud assets and adds new ones as they are added. Agentless CDR solutions also discover and monitor idle, paused, and stopped workloads, orphaned systems, and devices that don't support agents.

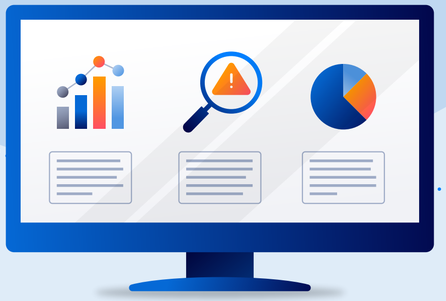


2. Depth of Visibility

Awareness of existing risks and threats across every layer of your cloud estate is important in order to get a complete understanding of what goes on inside the entire cloud environment: the infrastructure level, operating systems, applications, identity, APIs, and data. By combining this information with active events and behaviors, the CDR solution will gain a deep understanding of which activity is potentially malicious and could pose the biggest danger to the environment.

- **Cloud Infrastructure Level -** All assets run on top of this layer. Clear visibility here provides answers to the following questions: Which assets are running on which networks? Who is allowed to access them? Solutions that came from protecting on-premise environments and that focus on endpoints generally don't have any (or at least limited) visibility into the cloud infrastructure layer.
- **Operating System Level -** Common issues like remote code execution vulnerabilities (e.g., Microsoft Windows SMB Vulnerability) exist in this layer. It is vital to see which OS is in use, and when it was last updated or patched. Is it secured sufficiently or is it wide open? What is the configuration setup? Are user privileges in compliance? Have you applied all required patches?
- **Application Level -** This layer is where the vast majority of vulnerabilities reside. One example is the 2017 breach at Equifax that exposed the personal information of nearly 150 million consumers, resulting in up to $700 million in fines and compensation. It is vital to see all installed applications and their configurations, as well as know if they've been patched appropriately.
- **Identity Level -** As companies add more cloud services to their environments, the process of managing identities is getting more complex. Getting visibility into the identity level should go beyond healthy identity hygiene (MFA, principle of least privilege, etc.), and also include detecting anomalies in user and role behaviors, indicating possible malicious activity.
- **API Level -** APIs are an attractive attacker target, as they retrieve and modify information (often sensitive functions and data). Gartner has predicted that API abuses will become the top attack vector for most companies in 2022. By detecting possible malicious behavior and understanding how an attacker could exploit existing API vulnerabilities and risks in the environment—such as broken object-level authorization or excessive data exposure—dangerous attack paths can be identified.
- **Data Level -** This layer includes all data inventory and where it is housed. Clear visibility is critical in order to determine where the organization's crown jewels are stored, and which servers include sensitive data such as PII or payment information.

CDR solutions should be able to detect threats at all cloud layers including identities, configurations, workloads, applications and data-related behaviors. Having deep visibility into all of these layers is critical to detecting and analyzing malicious activity.



3. Comprehensive Cloud Telemetry

To detect threats, your solution needs to collect data. As each security layer mentioned in the previous section contains varying types of data, a CDR platform collects cloud telemetry from a variety of sources that it will then utilize to form a contextual “big picture” of current threats.

It’s important to note that when diving into cloud telemetry, all of the leading cloud service providers (CSPs) offer their own built-in cloud threat detection capabilities. CDR solutions, depending on integration levels, access many of these services. Most CSPs use a combination of telemetry sources to identify attacks, including network flow logs that leverage analytics and supplemental sources of threat intelligence. One well-known example is AWS GuardDuty, which analyzes continuous metadata streams generated from your account and network activity found in AWS CloudTrail Events, Amazon Virtual Private Cloud (VPC) Flow Logs, and DNS Logs.

Examples of cloud telemetry sources include:

Event logs like AWS CloudTrail logs, Google Cloud Audit Logs, and Azure Activity logs - describe certain types of actions performed on a cloud account (i.e., API calls inside the account itself) with a record of administrative activities and accesses within your cloud resources. These logs help you answer “who did what, where, and when?” within your cloud resources.

VPC Flow Logs - enable you to capture information about the IP traffic going to and from network interfaces in your VPC.

DNS Logs - allow you to record and view back and forth communication between browser users and the websites and services they are using.

Instance Logs - record VM-based activities, including access logs, Bash history, system logs, system calls, logins, and more.

Kubernetes Audit Logs - record chronological lists of all requests made to the Kubernetes API. Kubernetes stores the actions generated by each user, as well as by the control plane. The audit logs can tell you what happened and when, as well as who initiated it, where the request was observed, where it was initiated, and where it was going.

When looking at CDR or other detection and response options, it’s important to recognize the value in having a single, centralized platform that ingests, aggregates, analyzes, and presents data and telemetry with context. There is a lot of data available, but analysts need the right data, presented in the moment of need, in a way that is consumable and actionable. Be cautious of vendors that have “bolted” together previously separate tools, each presenting a series of siloed risks and threats in multiple dashboards, which significantly complicates investigations.

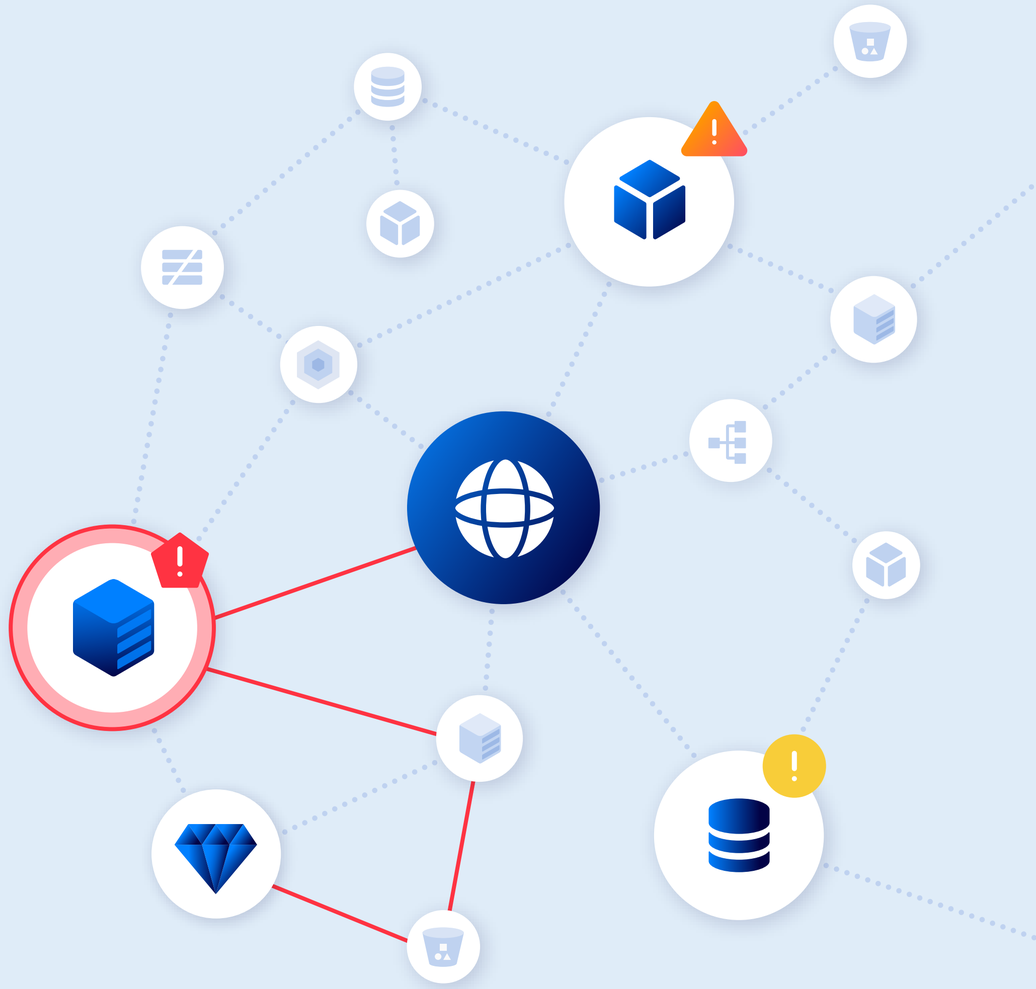
4. Contextual Intelligence

A unified CDR platform, with a highly contextual and prioritized view of all the different threats in the cloud environment, empowers security organizations to immediately understand and remediate their most critical threats.

This includes representing potential attack paths (i.e. lateral movement options that an attacker potentially could take to move to other workloads) in a visual graph with data on all relevant cloud entities and their risks across vulnerability status, misconfiguration risks, trust and authorization, and data as well as the relations between them. In addition, the ability to identify the location of crown jewel assets—housing Personal Identifiable Information (PII), secrets exposure, intellectual property, financial information, and other sensitive data—relative to where active threats are operating from is essential to understanding the threat context, and which threats are most dangerous.

This allows security teams to immediately understand which attack paths are the most critical to the business, so they can remediate those first. For this to be truly beneficial, it is essential that the cloud security platform utilizes a unified data model that collects and correlates contextual data on each asset, including information on potential risks in the cloud workload and configuration as well as external and internal cloud connectivity.

Finally, a weak contextual understanding of the threat landscape by a CDR tool can lead to false positives, alerting on activity that is not currently a pressing threat.



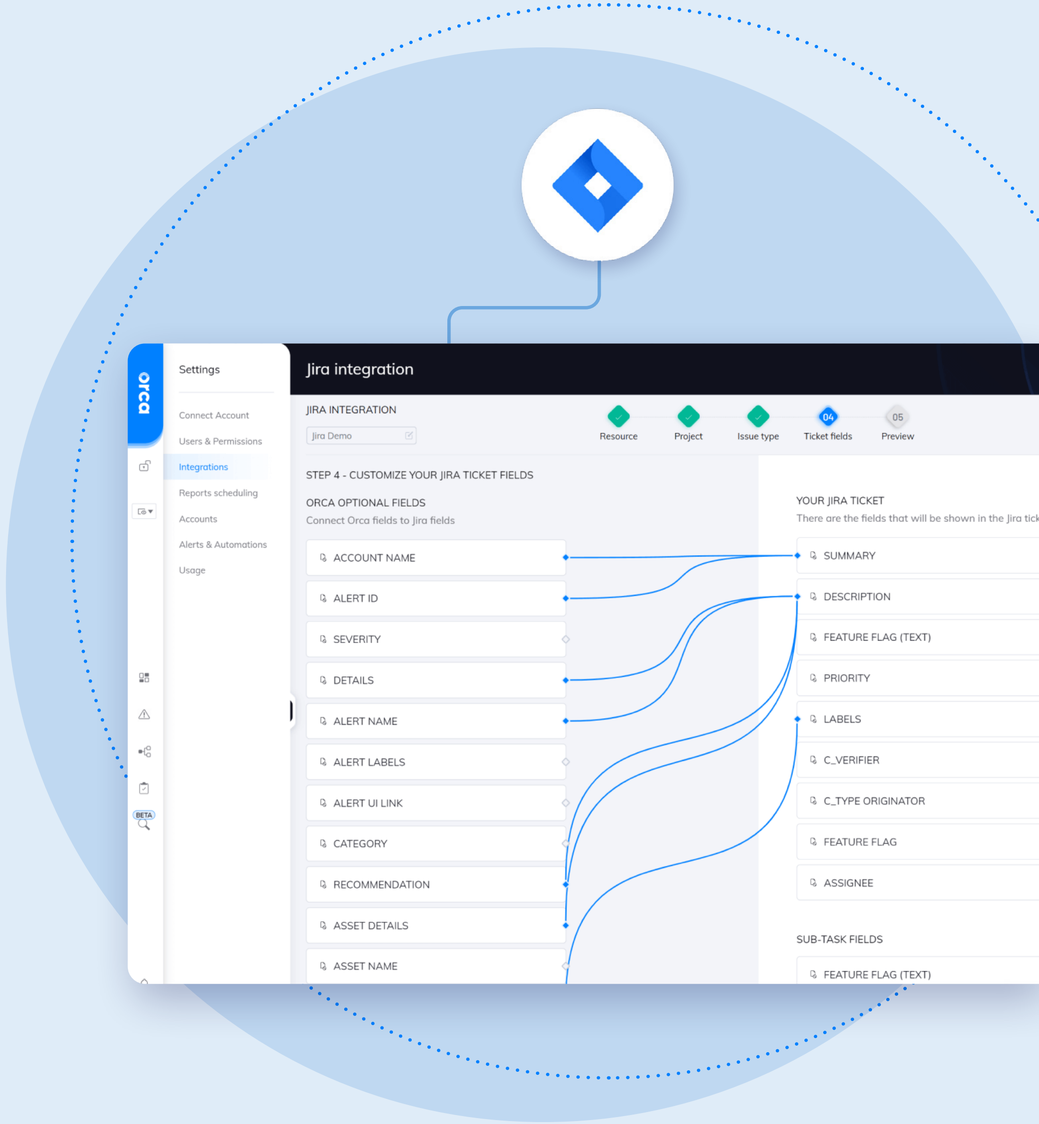
5. Workflow Integrations

When an attack is in progress and an alert has been generated, time is of the essence. Often, understaffed incident response teams must execute many separate collection processes and mine volumes of incident data. It's essential that the CDR platform provides teams with the required information to quickly investigate and make smart decisions to determine the best course of action.

The steps for investigation and support for incident response that a CDR solution provides includes guidance on how to quickly remediate the attack in the fastest way. This guidance can come with each individual alert, or in a big-picture graph or module that demonstrates necessary actions.

The CDR should also leverage technology integrations to give SOC and IR teams the power to increase automation, improve efficiency, and expedite remediation. These integrations should enable security teams to prioritize, customize, and integrate automated alerts into existing workflows.
These integrations may include:

- Ticketing systems (Jira, Azure DevOps, ServiceNow)
- SIEMs (Splunk, SumoLogic, AzureSentinel, Datadog, IBM QRadar))
- SOARs (Cortex XSOAR)
- Notification offerings (Slack, PagerDuty)
- Remediation orchestration (Torq, Tines, Brinqa)



Conclusion

As cyberattackers increasingly target applications and information stored in the cloud, Cloud Detection and Response (CDR) capabilities should represent an integral part of cloud security operations.

As SOC and IR teams are already overloaded, CDR platforms must provide clear and actionable information about active threats, and enable rapid investigation and response, without creating extra noise.

About the Orca Cloud Security Platform

Orca's Cloud Detection and Response capabilities help organizations quickly identify and respond to cloud attacks by continuously collecting and analyzing intelligence from cloud feeds, workloads, configurations, and identities.

Orca Security is the industry-leading agentless Cloud Security Platform that identifies, prioritizes, and remediates risks and compliance issues across your cloud estate spanning AWS, Azure, Google Cloud and Kubernetes. Instead of layering multiple siloed tools together or deploying cumbersome agents, Orca delivers complete cloud security in a single platform by combining two revolutionary approaches: SideScanning, which enables frictionless and complete coverage without the need to maintain agents, and a Unified Data Model, which allows for centralized contextual analysis of your entire cloud estate.

Orca's agentless platform connects to your environment in minutes and provides 100% visibility of all your assets, automatically including new assets as they are added. Orca detects and prioritizes cloud risks across every layer of your cloud estate, including vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and overly permissive identities.

For more information, visit https://orca.security