Cloud Detection and Response Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031)
Industry: Cloud & Enterprise Software
URL: https://www.mordorintelligence.com/industry-reports/cloud-detection-and-response-market

Cloud Detection and Response Market Size and ShareMarket Overview

Study Period	2020 - 2031
Market Size (2026)	USD 3.72 Billion
Market Size (2031)	USD 8.68 Billion
Growth Rate (2026 - 2031)	18.47 %
Fastest Growing Market	Asia-Pacific
Largest Market	North America
Market Concentration	Medium
Major Players	*Disclaimer: Major Players sorted in no particular order

|
Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

Cloud Detection and Response Market Analysis by Mordor IntelligenceThe cloud detection and response market size is projected to expand from USD 3.21 billion in 2025 and USD 3.72 billion in 2026 to USD 8.68 billion by 2031, registering a CAGR of 18.47% between 2026 and 2031. Enterprises are moving beyond security tools that identify configuration issues after deployment and are seeking protection that monitors cloud workloads while they run. The cloud detection and response market is shaped by the need to connect workload, identity, and container signals within a common security process. Threat actors can move laterally through a network in an average of 48 minutes, which limits the usefulness of investigation processes that depend only on manual review. Vendors are responding by combining telemetry collection, alert prioritization, and response workflows across cloud environments. The cloud detection and response market also faces demand for tools that can address nonhuman identities, sovereign-cloud requirements, and attacks that use AI to shorten breach timelines.

Key Report Takeaways

* By component, solutions held 58.46% of the cloud detection and response market revenue in 2025, while services are projected to expand at a 24.16% CAGR through 2031.
* By deployment mode, public cloud held 57.29% of revenue in 2025, while hybrid and multi-cloud are projected to expand at a 23.46% CAGR through 2031.
* By organization size, large enterprises accounted for 64.73% of cloud detection and response market revenue in 2025, while small and medium-sized enterprises are projected to expand at a 24.81% CAGR through 2031.
* By industry vertical, BFSI held 26.69% of revenue in 2025, while healthcare and life sciences are projected to expand at a 22.84% CAGR through 2031.
* By geography, North America held 44.87% of the cloud detection and response market in 2025, while Asia-Pacific is projected to expand at a 23.59% CAGR through 2031.

Note: Market size and forecast figures in this report are generated using Mordor Intelligence’s proprietary estimation framework, updated with the latest available data and insights as of January 2026.

Global Cloud Detection and Response Market Trends and InsightsDrivers Impact Analysis*

DRIVER | (~) % IMPACT ON CAGR FORECAST | GEOGRAPHIC RELEVANCE | IMPACT TIMELINE |
Cloud and Multi-Cloud Workload Expansion | +5.2% | Global | Medium term (2-4 years) |
Identity-First Cloud Attack Growth | +4.5% | Global | Short term (≤ 2 years) |
Regulatory and Cyber-Insurance Control Requirements | +3.5% | North America and Europe, with spillover to Asia-Pacific | Medium term (2-4 years) |
Cloud-Native Application and DevSecOps Adoption | +2.8% | Global, with early gains in North America and Asia-Pacific | Medium term (2-4 years) |
Runtime Security for AI Workloads and Autonomous Agents | +2.0% | Global, concentrated in North America and Asia-Pacific | Medium term (2-4 years) |
Ephemeral Workload Telemetry Gaps Creating Demand for Agentless Detection | +1.5% | Global | Short term (≤ 2 years) |
Source: Mordor Intelligence |

Cloud and Multi-Cloud Workload Expansion

Organizations are running more workloads across hybrid and multi-cloud environments, and their security processes are adapting to this change. Fortinet reported that 88% of organizations operated hybrid or multi-cloud environments in 2026, compared with 82% in the prior year.[1]Fortinet, “2026 Cloud Security Report Data Reveals Complexity Gap,” Fortinet, fortinet.com. The same report found that 81% used 2 or more cloud providers for critical workloads. Each provider introduces its own control planes and data sources that security teams need to monitor. The cloud detection and response market benefits when buyers require a unified view of activity across AWS, Azure, and Google Cloud. Providers that ingest cloud telemetry directly and connect related activity across those environments are better positioned for this requirement.

Identity-First Cloud Attack Growth

Identity has become a central attack surface for cloud attacks because credentials, service accounts, and tokens can provide persistent access. Sophos found that 71% of organizations experienced at least 1 identity-related breach in the prior year, and affected organizations reported an average of 3 incidents.[2]Sophos, “71% of Organizations Suffered at Least One Identity Breach in the Past Year, Sophos Research Finds,” Sophos, sophos.com. Those organizations reported average recovery costs of USD 1.64 million, while 73% incurred costs of at least USD 250,000. CrowdStrike reported that 82% of its detections were malware-free and that valid account abuse appeared in 35% of cloud incidents. Permiso reported that 77% of organizations said identity compromise accounted for up to 75% of security incidents, while 46% reported comprehensive visibility over identities. The cloud detection and response market, therefore, favors platforms that integrate API keys, federated credentials, service accounts, and workload signals.

Regulatory and Cyber-Insurance Control Requirements

Regulatory requirements are reducing the time available to identify and respond to cloud incidents. The Digital Operational Resilience Act applied across European Union member states from January 17, 2025, and it requires covered financial entities to maintain ICT risk management arrangements. The framework includes a 4-hour timeline for an initial major-incident notification and requires threat-led penetration testing for qualifying entities. These requirements increase the importance of real-time detection instead of periodic cloud reviews. Cyber-insurance requirements in North America also make documented detection and response controls more relevant to coverage decisions. The cloud detection and response market is supported as compliance expectations move from financial services into other regulated operating environments.

Cloud-Native Application and DevSecOps Adoption

Containerized applications, serverless functions, and microservices can move fro

m code changes to production use quickly. Datadog found that modern applications commonly run in cloud-native, containerized systems, whereas static application security testing remained dominant prior to deployment. Static checks cannot fully capture behavior that only appears after a workload runs in production. Short-lived Kubernetes workloads can also create evidence gaps for security teams that rely on conventional agents. NIST guidance for DevSecOps addresses security activities throughout the software development life cycle, including operations. The cloud detection and response market gains relevance when monitoring extends from build outputs and image registries into runtime execution.

Restraints Impact Analysis*

RESTRAINT | (~) % IMPACT ON CAGR FORECAST | GEOGRAPHIC RELEVANCE | IMPACT TIMELINE |
Security Tool Sprawl and Integration Complexity | -2.5% | Global | Short term (≤ 2 years) |
Cloud-Security Skills Shortage | -2.0% | Global, most acute in Asia-Pacific and Europe | Medium term (2-4 years) |
Data Sovereignty and Cross-Border Telemetry Restrictions | -1.5% | Europe and Asia-Pacific, with spillover to the Middle East | Medium term (2-4 years) |
Short-Lived Workloads and Sparse Evidence Increasing False Negatives | -1.2% | Global | Short term (≤ 2 years) |
Source: Mordor Intelligence |
Security Tool Sprawl and Integration Complexity

Security teams often add cloud tools to existing systems for posture management, access control, endpoint security, and event management. Fortinet found that nearly 70% of respondents cited tool sprawl and visibility gaps as a primary hindrance to effective cloud security in 2026.[3]Fortinet, “Fortinet Report Reveals Cybersecurity Hiring Stalls as Nearly Half of IT Leaders Face Corporate Pushback,” Fortinet, fortinet.com. Separate tools can generate alerts that lack common context, creating more work for analysts. Integration also delays the point at which a new runtime detection tool delivers usable results. The cloud detection and response market can be constrained when buyers must connect a new product to a fragmented security stack. Consolidated platforms can reduce this barrier by lowering tool counts and simplifying investigation workflows.

Cloud-Security Skills Shortage

Cloud security platforms require personnel who understand cloud configuration, identities, alerts, and response procedures. Fortinet found that 74% of organizations reported a shortage of qualified cybersecurity professionals in 2026, and 56% of IT leaders identified skill shortages as a cause of breaches. ISC2 reported that 95% of organizations had at least 1 cybersecurity skill need, and 88% had experienced a significant event linked to a skills shortage in the prior 12 months. Cloud security engineering ranked among the top 3 skill deficits for 30% of hiring organizations in the research. The cloud detection and response market is better served by products that automate triage and provide response playbooks for analysts with general security backgrounds. Platforms that require extensive manual tuning can remain difficult to deploy where specialized staff is limited.

*Our forecasts treat driver/restraint impacts as directional, not additive. The impact forecasts reflect baseline growth, mix effects, and variable interactions.

Segment AnalysisBy Component: Solutions Lead Revenue, While Services Support Delivery

Solutions held 58.46% of the cloud detection and response market share in 2025,

reflecting enterprise demand for purpose-built CDR platforms. These platforms bring cloud telemetry ingestion, attack correlation, and alert triage into one operating environment for security teams. They help analysts assess related events rather than investigate isolated alerts from disconnected point products. Palo Alto Networks reported that 99% of organizations had experienced at least 1 attack on their AI systems during the prior year.[4]Palo Alto Networks, “Where Cloud Security Stands Today and Where AI Breaks It, State of Cloud Security Report 2025,” Palo Alto Networks, paloaltonetworks.com. This pressure supports demand for platforms that observe generative AI workloads alongside established cloud workloads.

Services are projected to expand at a 24.16% CAGR through 2031, the highest rate within the component split. Mid-market enterprises often select managed services when they cannot maintain continuous cloud monitoring with internal cloud security staff. Service providers support onboarding, telemetry mapping, and detection engineering across several cloud environments, which can shorten the time to use. Vendors are increasingly combining licensed software with managed services in subscription contracts, narrowing the distinction between the two categories. This can affect the positioning and margins of standalone managed security service providers within the cloud detection and response industry.

 By Deployment Mode: Hybrid and Multi-Cloud Gains Priority

Public cloud accounted for 57.29% of the cloud detection and response market in 2025, reflecting the concentration of workloads and security budgets in single-provider environments. Buyers with public cloud estates require monitoring of data, identities, workloads, and provider control planes as cloud usage expands. This installed base remains a substantial source of demand for cloud-native detection tools. It also makes interoperability with major public cloud services important for continued product adoption. Organizations that retain a single-provider design still need tools that connect security events with operational cloud activity.

Hybrid and multi-cloud deployment is projected to expand at a 23.46% CAGR through 2031. Enterprises are using operating models that combine on-premises systems, private cloud, and public cloud services across different business needs. Data sovereignty requirements in Europe and the Asia-Pacific can make this structure both a compliance response and an architectural choice. Providers that convert provider-specific APIs into a common data model can help teams apply consistent detection rules across environments. Private cloud also remains relevant for financial institutions and defense organizations with strict data classification requirements.

By Organization Size: Large Enterprises Remain the Core Buyer Base

Large enterprises accounted for 64.73% of the cloud detection and response market revenue in 2025. Their cloud scale, formal security operations center capacity, and board-level breach accountability support centralized runtime detection programs. These organizations often operate across several cloud environments and require unified visibility for security teams. Their early adoption has helped establish cloud detection and response as an enterprise security category. Large accounts will remain important for vendors that support complex integrations and large telemetry volumes.

Small and medium-sized enterprises are projected to expand at a 24.81% CAGR through 2031, the highest rate for organization size. Subscription-priced managed offerings can give smaller buyers cloud coverage without a dedicated team of cloud security engineers. Sophos found that organizations with 100 to 250 employees were nearly twice as likely as mid-sized peers to fail to detect an incident before damage occurred. Providers are developing lighter onboarding, prepared detection libraries, and automated response playbooks to address resource constraints.

The cloud detection and response market size for this group is supported by ransomware risk, cyber-insurance expectations, and delivery models designed for smaller organizations.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0. By Industry Vertical: BFSI Retains Scale, While Healthcare Expands Faster

BFSI held 26.69% of the cloud detection and response market share in 2025. Financial institutions operate cloud-hosted transaction workflows and API ecosystems, making identity and control-plane security central to risk management. The financial consequences of breaches and extensive regulatory oversight sustain spending on detection capability. American Banker found that enhanced security and fraud mitigation were the leading technology spending priority for 56% of surveyed banks in 2025.[5]American Banker, “Banks Increasing Tech Spend in 2025,” American Banker, americanbanker.com. Related investments in identity management, multifactor authentication, fraud analytics, SOAR platforms, and vendor risk management make runtime cloud detection part of a wider security program.

The healthcare and life sciences industry is projected to expand at a 22.84% CAGR through 2031. Electronic health record and medical imaging migration to large cloud providers increases the need to observe cloud access and workloads. Ransomware groups target hospitals because unavailable data can have direct clinical consequences. Government and public administration, industrial manufacturing, IT and telecommunication, energy and utilities, oil and gas, transportation and logistics, retail and e-commerce, media and entertainment, and education and research institutions also create demand. The cloud detection and response industry can support these settings by connecting identities with runtime activity around sensitive operational data.

Geography Analysis

North America held 44.87% of the cloud detection and response market in 2025. The region combines extensive cloud infrastructure, a high concentration of enterprise targets, and established security budgets. U.S. requirements related to HIPAA, SOC 2, GLBA, and SEC cybersecurity disclosures support formal security controls. Federal cloud initiatives and zero-trust requirements also create public-sector demand. Cloud security spending in North America advanced at a 16.76% CAGR as hybrid work revealed the limits of perimeter-focused security approaches.

Europe is a significant part of the cloud detection and response market, with spending increasingly guided by compliance requirements. DORA has been applied since January 2025 to banks, insurers, payment firms, and asset managers in the European Union. Its incident and risk-management requirements create demand for continuous detection and response capability. NIS2 obligations broaden the buyer base across energy, healthcare, transportation, and digital infrastructure. The United Kingdom, France, Germany, Italy, and Spain are the main spending bases, while South America shows emerging demand in Brazil and Chile despite infrastructure and skill constraints.

Asia-Pacific is projected to expand at a 23.59% CAGR through 2031, the fastest regional rate. Cloud-first infrastructure programs in India, South Korea, and Japan, ASEAN fintech expansion, and localization requirements support demand. China’s cybersecurity and data security rules require localized approaches and encourage country-specific deployment models. The Middle East is developing demand through sovereign-cloud security plans, while Africa remains at an earlier stage, led by South Africa and Nigeria.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

Competitive Landscape

The cloud detection and response market is moderately concentrated at the platform level, where Palo Alto Networks, CrowdStrike, Microsoft, and Wiz, now part of Google Cloud, influence enterprise procurement. The managed service layer is more fragmented, with Arctic Wolf, ReliaQuest, Expel, and SentinelOne competing through detection quality, response automation, and service delivery. Google completed its USD 32 billion acquisition of Wiz on March 11, 2026.[6]Google, “Google Completes Acquisition of Wiz,” Google, google.com. Wiz joined Google Cloud while retaining its multi-cloud commitment, combining its Security Graph with Google’s Mandiant threat intelligence and Unified Security Platform. The transaction places agentless cloud security capabilities within a hyperscale cloud offering, and pressures rivals to strengthen integrations.

CrowdStrike introduced adversary-informed cloud risk prioritization in March 2026 through Application Explorer, Timeline Explorer, and a Cloud Risk Engine. The product connected cloud exposures with active adversary tradecraft and live application behavior. Palo Alto Networks launched Prisma AIRS 3.0 in March 2026 to cover AI agent discovery, risk assessment, and runtime protection. These moves extend competition into AI workload protection, where standardized benchmarks have yet to emerge. The NIST AI Risk Management Framework remains a governance reference for buyers assessing these capabilities.

The cloud detection and response market has opportunities in sovereign cloud deployments that require in-country telemetry residency and identity-focused detection for smaller organizations. Unified workflows that connect a cloud alert with a security operations center investigation can reduce response delays. Sysdig, Orca Security, Mitiga, and ReliaQuest compete through agentless designs, zero-agent deployment, and AI-supported remediation. Competition will center on broad coverage, manageable deployment, and operating requirements that customers can sustain.

Cloud Detection and Response Industry Leaders* Palo Alto Networks, Inc.

* CrowdStrike Holdings, Inc.

* Microsoft Corporation

* Wiz, Inc.

* Arctic Wolf

* *Disclaimer: Major Players sorted in no particular order

Recent Industry Developments* April 2026: CrowdStrike expanded its real-time Cloud Detection and Response service to Google Cloud Platform at Google Cloud Next 2026, establishing unified CDR coverage across AWS, Azure, and Google Cloud simultaneously. The expansion positions Falcon Cloud Security as a cross-cloud detection plane, replacing posture-only tools with live runtime protection and direct adversary-tradecraft alignment.
* April 2026: Orca Security signed a strategic collaboration agreement with AWS to advance AI-powered cloud security, enabling organizations to gain deeper visibility into AI service usage and accelerate remediation across multi-cloud environments. The agreement deepens Orca's agentless-first architecture integration within the AWS ecosystem.
* March 2026: Palo Alto Networks launched Prisma AIRS 3.0, advancing its AI security platform to cover the full agentic AI lifecycle, including discovery, risk assessment, and protection of AI agents running across cloud environments, SaaS

platforms, and endpoints. The launch directly addresses the growing unmonitored attack surface created by enterprise AI agent proliferation.
* March 2026: SentinelOne announced a significant multi-year collaboration with Google Cloud to deliver autonomous, AI-powered security at a global scale, with the Singularity Platform now available across 3 strategic Google Cloud regions, North America, Frankfurt, and the Kingdom of Saudi Arabia, supporting in-country data residency and regional regulatory alignment.

Table of Contents for Cloud Detection and Response Industry Report1. INTRODUCTION

Global Cloud Detection and Response Market Report ScopeThe cloud detection and response market includes security platforms that continuously monitor, detect, investigate, and respond to threats in cloud-native environments, including public cloud IaaS and PaaS, containers, serverless functions, cloud identities, and SaaS applications. These solutions use cloud telemetry, API integrations, behavioral analytics, and machine learning to identify anomalous activity, misconfigurations, identity-based attacks, data exfiltration, lateral movement, and other cloud-specific threats across multi-cloud and hybrid environments. Key capabilities include cloud workload protection, cloud security posture management integration, identity threat detection, automated containment, forensic investigation, and compliance reporting. These platforms help security teams reduce mean time to detect (MTTD) and mean time to respond (MTTR), prevent data breaches, and maintain security visibility across dynamic cloud infrastructure that traditional on-premises security tools cannot adequately monitor or protect.

The Cloud Detection and Response Market Report is Segmented by Component (Solutions, and Services), Deployment Mode (Public Cloud, Private Cloud, and Hybrid and Multi-Cloud), Organization Size (Large Enterprises, and Small and Medium-Sized Enterprises), Industry Vertical (Government and Public Administration, Industrial Manufacturing, Retail and E-Commerce, Transportation and Logistics, Energy and Utilities, Oil and Gas, IT and Telecommunication, Media and Entertainment, Education and Research Institutions, Healthcare and Life Sciences, Banking, Financial Services, and Insurance (BFSI), and Other Industry Verticals), and Geography (North America, South America, Europe, Asia-Pacific, Middle East, and Africa). The Market Forecasts are Provided in Terms of Value (USD).

By ComponentSolutions |
Services |
By Deployment ModePublic Cloud |

Private Cloud |
Hybrid and Multi-Cloud |
By Organization SizeLarge Enterprises |
Small and Medium-Sized Enterprises |
By Industry VerticalGovernment and Public Administration |
Industrial Manufacturing |
Retail and E-Commerce |
Transportation and Logistics |
Energy and Utilities |
Oil and Gas |
IT and Telecommunication |
Media and Entertainment |
Education and Research Institutions |
Healthcare and Life Sciences |
Banking, Financial Services, and Insurance (BFSI) |
Other Industry Verticals |
By GeographyNorth America | United States |
 | Canada |
 | Mexico |
South America | Brazil |
 | Argentina |
 | Chile |
 | Rest of South America |
Europe | Germany |
 | United Kingdom |
 | France |
 | Italy |
 | Spain |
 | Rest of Europe |
Asia-Pacific | China |
 | Japan |
 | India |
 | South Korea |
 | Australia |
 | Rest of Asia-Pacific |
Middle East | Saudi Arabia |
 | United Arab Emirates |
 | Rest of Middle East |
Africa | South Africa |
 | Nigeria |
 | Egypt |
 | Rest of Africa |
By Component | Solutions |
 | Services |
By Deployment Mode | Public Cloud |
 | Private Cloud |
 | Hybrid and Multi-Cloud |
By Organization Size | Large Enterprises |
 | Small and Medium-Sized Enterprises |
By Industry Vertical | Government and Public Administration |
 | Industrial Manufacturing |
 | Retail and E-Commerce |
 | Transportation and Logistics |
 | Energy and Utilities |
 | Oil and Gas |
 | IT and Telecommunication |
 | Media and Entertainment |
 | Education and Research Institutions |
 | Healthcare and Life Sciences |
 | Banking, Financial Services, and Insurance (BFSI) |
 | Other Industry Verticals |
 | |

By Geography | North America | United States |
 | | Canada |
 | | Mexico |
 | |
South America	Brazil
	Argentina
	Chile
	Rest of South America
Europe	Germany
	United Kingdom
	France
	Italy
	Spain
	Rest of Europe
Asia-Pacific	China
	Japan
	India
	South Korea
	Australia
	Rest of Asia-Pacific
Middle East	Saudi Arabia
	United Arab Emirates
	Rest of Middle East
Africa	South Africa
	Nigeria
	Egypt
	Rest of Africa

Key Questions Answered in the ReportWhat is the cloud detection and response market size and forecast? The cloud detection and response market size is projected to expand from USD 3.21 billion in 2025 and USD 3.72 billion in 2026 to USD 8.68 billion by 2031, registering a CAGR of 18.47% between 2026 and 2031.

What is driving adoption in the cloud detection and response market? Multi-cloud expansion, identity-related attacks, regulatory requirements, and cloud-native application use are increasing demand for runtime security.

Which component has the largest cloud detection and response revenue share? Solutions held 58.46% of revenue in 2025, while services are projected to grow faster at a 24.16% CAGR through 2031.

Which deployment model is growing fastest? Hybrid and multi-cloud deployment is projected to expand at a 23.46% CAGR through 2031.

Which end-user vertical is expanding fastest? Healthcare and life sciences are projected to expand at a 22.84% CAGR through 2031, supported by cloud migration and ransomware exposure.

Which region is expected to grow fastest in the cloud detection and response market? Asia-Pacific is projected to expand at a 23.59% CAGR through 2031, supported by cloud infrastructure programs, fintech growth, and data localization requirements.