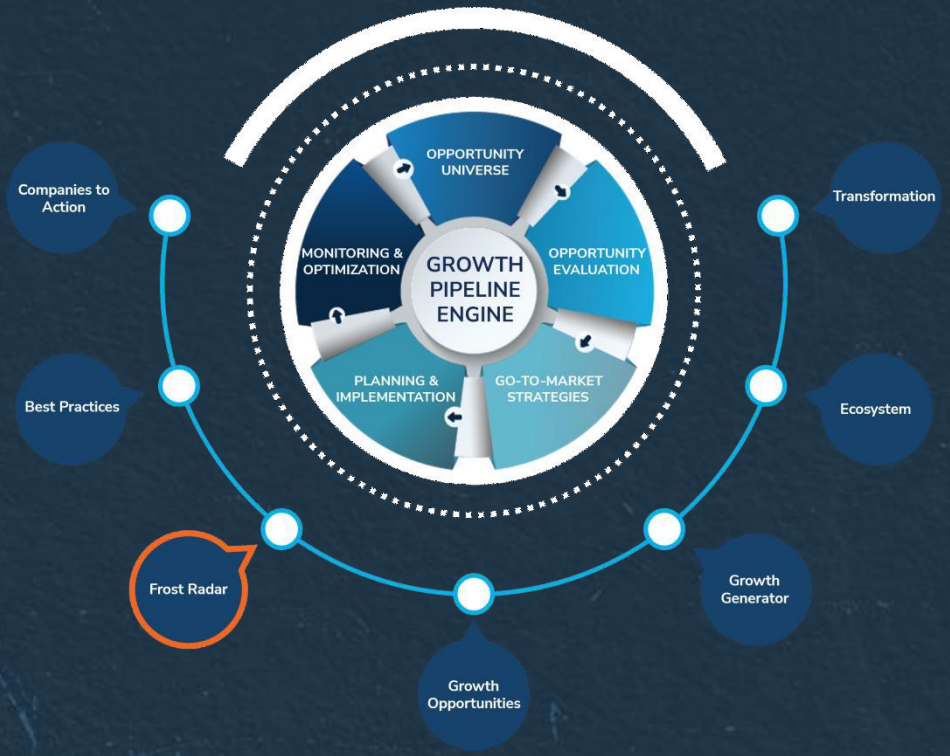
FROST & SULLIVAN

Frost Radar™: Cloud/Application Runtime Security, 2026



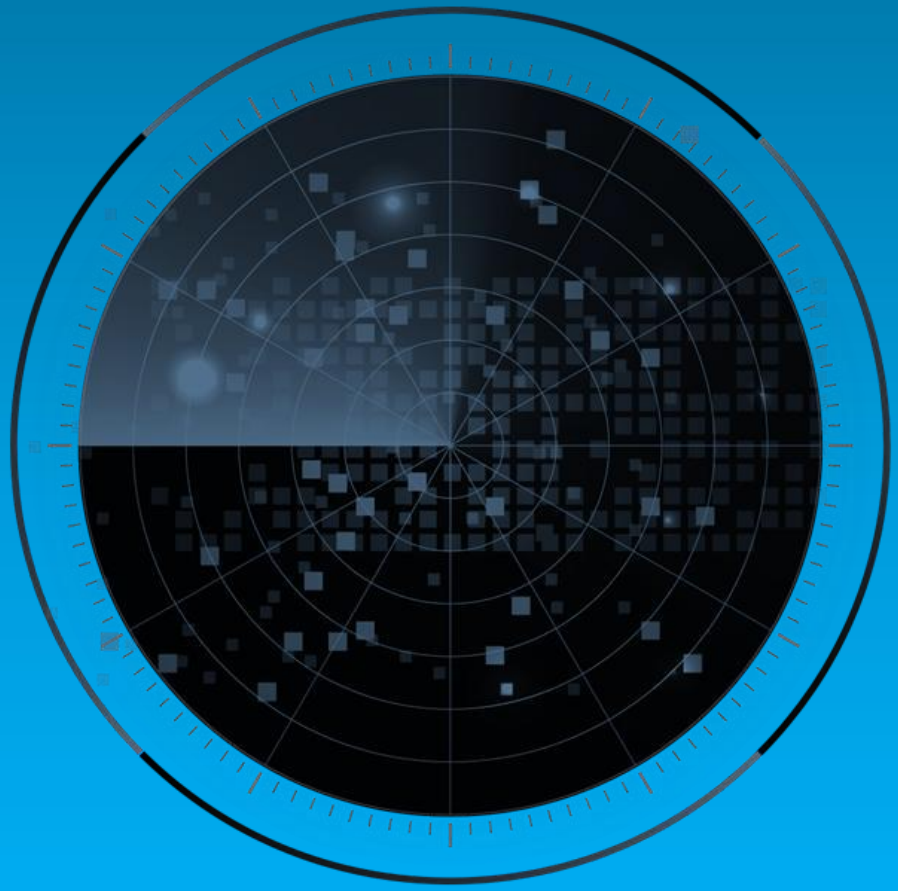
A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines

Authored by: Anh Tien Vu
Contributor: Jarad Carleton

PLYY-74
June 2026

FROST & SULLIVAN

Strategic Imperative and Growth Environment



List of Abbreviations

- **ADLC:** Application Development Lifecycle
- **ADR:** Application Detection and Response
- **AI SPM:** AI Security Posture Management
- **APA:** Attack Path Analysis
- **APAC:** Asia-Pacific
- **API:** Application Programming Interface
- **AppSec:** Application Security
- **ARR:** Annual Recurring Revenue
- **ASM:** Attack Surface Management
- **ASPM:** Application Security Posture Management
- **AWS:** Amazon Web Services
- **BFSI:** Banking, Financial Services, and Insurance
- **CARS:** Cloud/Application Runtime Security
- **CDR:** Cloud Detection and Response
- **CI/CD:** Continuous Integration and Continuous Delivery
- **CIEM:** Cloud Infrastructure Entitlement Management
- **CIO:** Chief Information Officer
- **CISO:** Chief Information Security Officer
- **CloudSecOps:** Cloud Security Operations
- **CNADR:** Cloud-Native Application Detection and Response
- **CNAPP:** Cloud-Native Application Protection Platform
- **CNDR:** Cloud-Native Detection and Response
- **CSP:** Cloud Service Provider
- **CSPM:** Cloud Security Posture Management
- **CTO:** Chief Technology Officer
- **CWPP:** Cloud Workload Protection Platform
- **DAST:** Dynamic Application Security Testing
- **DevOps:** Development and Operations
- **DevSecOps:** Development and Security Operations
- **DSPM:** Data Security Posture Management
- **eBPF:** Extended Berkeley Packet Filter
- **EDR:** Endpoint Detection and Response
- **EMEA:** Europe, the Middle East, and Africa
- **EPSS:** Exploit Prediction Scoring System
- **FIM:** File Integrity Management
- **GCP:** Google Cloud Platform
- **GRC:** Governance, Risk, Compliance
- **GTM:** Go-to-Market
- **IaaS:** Infrastructure as a Service
- **IaC:** Infrastructure as Code
- **IAST:** Interactive Application Security Testing
- **ICAP:** Internet Content Adaptation Protocol
- **IDE:** Integrated Development Environment
- **ISPM:** Identity Security Posture Management
- **IR:** Incident Response
- **ISV:** Independent Software Vendor
- **ITSM:** IT Service Management
- **JIT:** Just in Time
- **K8s:** Kubernetes

Source: Frost & Sullivan

List of Abbreviations (continued)

- **KSPM:** Kubernetes Security Posture Management
- **LLM:** Large Language Model
- **MCP:** Model Context Protocol
- **MDR:** Managed Detection and Response
- **ML:** Machine Learning
- **MSP:** Managed Service Provider
- **MSSP:** Managed Security Service Provider
- **MTTD:** Mean Time to Detect
- **MTTR:** Mean Time to Remediate/Mean Time to Respond
- **NAS:** Network-Attached Storage
- **NG-SIEM:** Next-Generation Security Information Event Management
- **NHI:** Non-human Identity
- **OCI:** Oracle Cloud Infrastructure
- **OSS:** Open-Source Software
- **PaaS:** Platform as a Service
- **PaC:** Policy as Code
- **RASP:** Runtime Application Self-Protection
- **ROI:** Return on Investment
- **SaaS:** Software as a Service
- **SAST:** Static Application Security Testing
- **SBOM:** Software Bill of Materials
- **SCA:** Software Composition Analysis
- **SCM:** Source Code Management
- **SDK:** Software Development Kit
- **SecOps:** Security Operations
- **SI:** System Integrator
- **SIEM:** Security Information and Event Management
- **SMB:** Small and Medium-Sized Business
- **SOAR:** Security Orchestration, Automation, and Response
- **SOC:** Security Operation Center
- **SSCS:** Software Supply Chain Security
- **SSPM:** SaaS Security Posture Management
- **TDIR**: Threat Detection, Investigation, and Response
- **TDR:** Threat Detection and Response
- **USPM:** Unified Security Posture Management
- **UVM:** Universal Vulnerability Management
- **VAR:** Value-Added Reseller
- **VM:** Vulnerability Management
- **WAAP:** Web Application Firewall and API Protection
- **WAF:** Web Application Firewall
- **XDR:** Extended Detection and Response
- **YoY:** Year Over Year

Source: Frost & Sullivan

Strategic Imperative

- Global cloud and AI adoption are expanding the runtime attack surface across multicloud infrastructure, containers, K8s, serverless, APIs, and AI applications in ways that static posture, scanning, and traditional AppSec tools cannot fully capture or control. Modern SecOps teams need continuous runtime visibility into how cloud/AI workloads and applications actually behave in production.
- This has elevated the importance of CARS solutions. CDR, ADR, and converged CNADR/CADR capabilities are becoming crucial to this shift, while CWPP, API runtime security, app network analysis, and runtime vulnerability validation are critical supporting capabilities in modern cloud security programs.
- CDR, ADR, and CWPP are becoming critical layers in the cloud-native security stack as well as modern cloud security and SecOps workflows. They ingest high-fidelity telemetry from cloud services, workloads, and application runtimes to detect anomalous behavior, prevent active exploits, and automate detection and containment/response (with human in the loop) effectively. These capabilities transform CNAPP, AppSec, and SIEM/XDR platforms from static risk management to unified SecOps/SOC workflows that drive rapid detection, investigation, and response in the SOC environment, reducing dwell time and helping teams focus on risks that are truly reachable and exploitable in production instead of wasting hours on irrelevant posture alerts.
- As runtime security matures, the market is shifting toward CNADR, where CDR, ADR, CWPP, and other runtime security capabilities (API and AI security) are unified into a single runtime fabric that spans cloud infrastructure, workloads, applications, and AI services under a common data lake and workflow layer. In this operating model, posture and vulnerability findings are continuously validated against real runtime behavior, attack paths, and incident context, with AI-assisted investigation and automated playbooks orchestrating response across cloud and application layers to support SecOps/SOC operations in the cloud- and AI-native era.

Source: Frost & Sullivan

Growth Environment

- The CARS market is entering a high growth phase as organizations recognize that CNAPP and static scanning alone cannot provide runtime context and high-fidelity insights needed for effective TDIR. Many traditional CNAPP solutions fail to deliver deep runtime capabilities, forcing security teams to look for runtime-first solutions that can detect active attacks, identify exploitability, and provide immediate remediation.
- CDR is increasingly treated as a mandatory control layer in cloud security roadmaps and becoming a must-have capability on enterprises' cloud security short lists. This is directly fueling market expansion as enterprises invest more in cloud-native detection and response instead of treating it as an add-on to CNAPP tools. Organizations now evaluate cloud security platforms on their ability to translate large volumes of cloud telemetry and attack path insights into SOC workflows to facilitate incident response, which is favoring vendors that package CDR as an integrated service.
- In parallel, ADR has gained traction over the last 2 years because of its ability to address challenges associated with application risk reduction and threat management that legacy WAF/RASP and static AppSec tools fail. ADRs help reduce false positives, verify exploitable vulnerabilities, and support compliance and audit management. The rise of AI-accelerated exploitation is increasing the importance of ADR because organizations need to know which application vulnerabilities can actually be reached, exploited, attacked, or blocked inside the running application. These make ADR relevant for AppSec and SOC teams, creating a new, fast-growing area.
- The rapid adoption of AI workloads, AI agents, LLM applications, RAG pipelines, plugins, and autonomation workflows is also creating a new, structural growth vector as organizations seek to extend runtime controls to these AI assets. Security vendors that can integrate cloud/app security, AI-SPM and AI-DR into a unified runtime security platform for cloud, application, and AI are well positioned to capture this opportunity.

Source: Frost & Sullivan

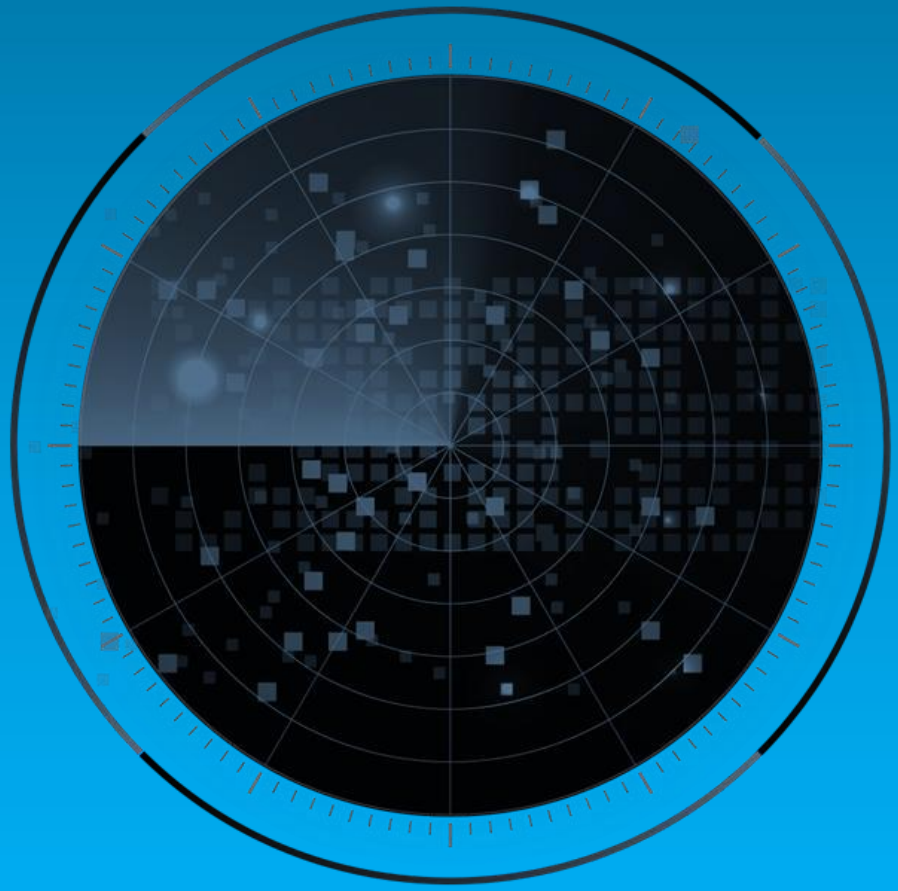
Growth Environment (continued)

- Runtime security demand is also growing for capabilities that secure the execution layer of cloud-native environments, including workload runtime security, API security, and application network analysis. As enterprises scale their cloud stack, security teams need real-time telemetry to understand cloud workload behavior, process activities, file access, network connections, API activity, and workload drift in production. This is driving the adoption of lightweight runtime technologies, such as eBPF, memory analysis, and workload sensors, to provide evidence to validate exploitability, detect lateral movement, identify workload or agent compromise, and support faster investigation and remediation.
- CISOs expect investments in these runtime technologies to reduce alert fatigue, accelerate MTTD/MTTR, and provide better risk prioritization across cloud, workload, application, and AI services. This requires platforms that can correlate runtime telemetry with posture and identity context to deliver explainable, low-noise detection that maps to real business processes and integrates tightly with SOC, IR, and audit workflows, which favors vendors offering a unified code-to-cloud-to-SOC framework.
- Regional adoption patterns influence the growth trajectory for CARS. North America remains the most mature and platform-driven market, with buyers consolidating around CNAPP, XDR, and CDR fabrics and demanding measurable risk reduction outcomes, faster MTTD/MTTR, and strong integration with existing cloud, data, identity, and SOC ecosystems. EMEA growth is equally strong but more compliance-driven, with deal cycles shaped by sovereignty, data residency, and regulatory assurance requirements.
- APAC is the fastest-growing region for cloud security overall, with India, Southeast Asia, and Australia leapfrogging to cloud-first and AI-heavy architectures. Though the actual adoption and market size of runtime security, particularly CDR and ADR, remains low because of the emphasis on posture and vulnerability management, regional regulators and industry bodies are pushing for stronger cloud incident management, driving adoption of lighter-weight, cost-efficient runtime security.

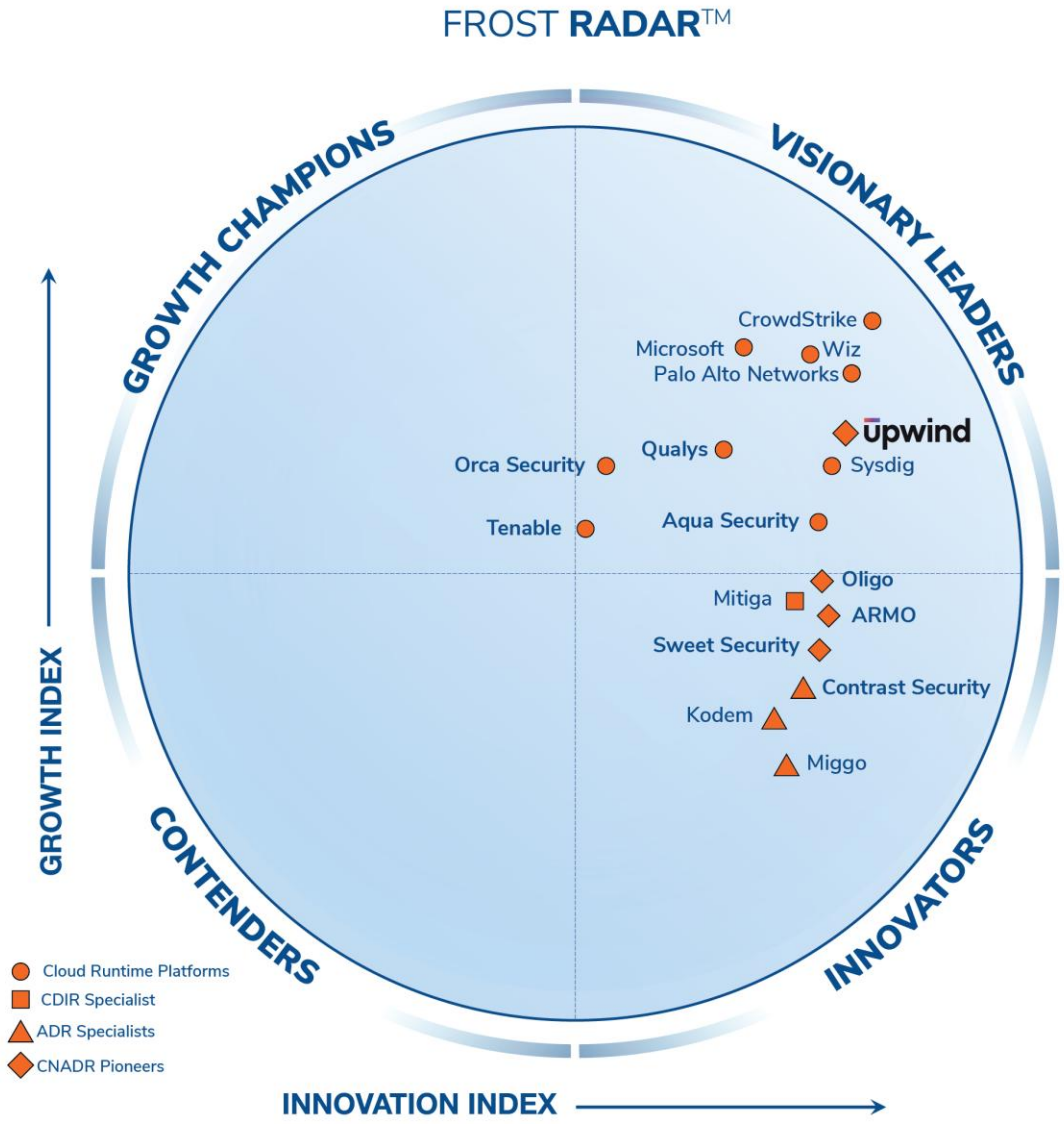
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Cloud/Application Runtime Security



Frost Radar™: Cloud/App Runtime Security



In a highly competitive CARS market with more than 25 qualified participants meeting inclusion criteria, Frost & Sullivan independently evaluated the landscape and selected just 17 companies to be benchmarked in this Frost Radar™. It evaluates the market, with the primary focus on CDR, ADR, converged CNADR/CADR, and adjacent runtime capabilities, such as CWPP, K8s runtime security, API security, and AI security. It assesses capabilities to validate vulnerabilities and their exploitability, prioritize risk, detect active threats, and support investigation and response across cloud infrastructure, workloads, APIs, microservices, AI services, and applications in production.

This evaluation is led by Frost & Sullivan's experienced global analyst team, combining deep domain expertise with a rigorous, fact-based approach using our proprietary, multidimensional benchmarking methodology, applied consistently and validated by analysts. Frost & Sullivan ensures a fair, globally comparable, and defensible assessment of true market leadership.

FROST & SULLIVAN

Source: Frost & Sullivan

Frost Radar™: Competitor Categories

GROWTH CHAMPIONS

- Achieve significant market growth through effective execution.
- Leverage proven technologies and scalable business models.
- Maintain competitiveness via operational efficiency and customer focus.
- Require increased innovation investment for sustained leadership.

VISIONARY LEADERS

- Market leaders with strong balance of innovation and growth.
- Deliver transformative technologies, business models, and processes.
- Influence industry direction and set new benchmarks.
- Combine strategic vision with operational excellence for market dominance.

CONTENDERS

- Emerging players with modest market presence and cautious strategies.
- Often new entrants or niche participants establishing their position.
- Emphasizes continuous improvement and ensures operational reliability.
- Hold potential for growth through innovation, alliances, and market expansion.

INNOVATORS

- Drive technological advancement with disruptive ideas and solutions.
- Prioritize R&D, IP development, and pioneering concepts.
- Strong innovation foundation with opportunities to accelerate commercialization and scale.
- Benefit from strategic partnerships and targeted go-to-market strategies.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- Vendors featured in this Frost Radar™ analysis met the following criteria:
  - Generated at least $5 million in ARR by May 2026
  - Have CDR, ADR, CNADR, and other runtime security capabilities, either as part of CNAPP or as stand-alone solutions
  - Have business presence in at least in 2 regions (North America, EMEA, APAC, or Latin America)
- Other vendors were not included in this analysis because of one or more reasons:
  - Declined participation
  - Were unable to provide direct input
  - Insufficient data was available from secondary research to conduct a thorough analysis
- The evaluation relies on information, vendor performance, and market conditions as of 31 May 2026.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- As enterprises scale their business, they need runtime visibility into process activity, system calls, network connections, workload drift, privilege escalation, and lateral movement across their cloud, application and AI environments. This is creating requirements for lightweight runtime technologies, such as eBPF and runtime sensors, to provide workload runtime insights with low performance impact and support stronger detection and response across cloud environments.
- Many runtime security vendors are CNAPP-first players that embed CDR, CWPP, and other runtime context into broader cloud security platforms to improve risk prioritization, investigation, and remediation. They typically correlate cloud control plane activity, workload telemetry, identity behavior, application and network activity, misconfigurations, data exposure, and attack paths to identify and prioritize risks in runtime. More mature platforms are extending these capabilities into SOC workflows through MITRE mapping, incident timeline construction, attack path analysis, threat hunting, SIEM/SOAR integration, and guided response for better active threat management.
- ADR specialists focus more deeply on application-layer runtime risk. They use different architectural approaches, including eBPF-based telemetry, library-level behavioral monitoring, application instrumentation, code path analysis, API behavior monitoring, memory analysis, and exploit behavior detection. Their value lies in seeing how applications, libraries, functions, APIs, and business logic behave during execution, allowing teams to validate whether vulnerabilities are reachable, exploited, or actively attacked in production. While many ADR vendors focus on runtime visibility, anomaly detection, and remediation context, the more advanced players extend into in-application blocking or runtime-informed mitigation, which distinguishes ADR from cloud-centric runtime players that often lack inside-application execution context.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- A growing group of vendors is positioning around a broader runtime security convergence where CDR, ADR, CWPP, API security, and application context are unified into a cloud-native detection and response fabric (CNADR/CADR) to facilitate SOC teams in cloud TDR. These platforms enable SOC, CloudSec, AppSec, and DevSecOps teams to work from a shared runtime source of truth, helping them validate vulnerabilities and exploitability, understand full attack storylines, and detect and respond to active threats across cloud infrastructure, workloads, and production applications.
- Cloud-centric runtime platforms and CNADR vendors are generally stronger in cloud, workload, identity, K8s, and SOC correlation. While many of these vendors are expanding into AppSec, most still provide application runtime visibility mainly at the API, Layer 7, service-to-service, or traffic behavior layer and do not match ADR specialists in deep application instrumentation, code execution visibility, library/function-level analysis, or in-application attack blocking. By contrast, while ADR specialists deliver stronger application runtime visibility, exploit validation, and in-application TDR, they often lack broader cloud, workload, K8s, identity, and cloud posture security capabilities. This can limit their role in full CNADR deployments, where enterprises need cross-layer detection and response across cloud infrastructure, workloads, APIs, applications, identities, data, and AI services.
- Architecturally, most vendors differentiate through agentless telemetry, eBPF and kernel-level sensors, application instrumentation, cloud graph correlation, and AI-driven analytics for investigation, prioritization, and response. Larger CNAPP and exposure management platforms are embedding runtime security and CDR into existing cloud security stacks, while newer entrants focus on cloud/workload runtime, ADR, cloud investigation and forensics, and runtime protection for AI workloads and agents.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

Cloud-centric runtime security platforms

- CrowdStrike is the visionary leader in this analysis, scoring highest on the Growth and Innovation indices by combining mature CDR with a scaled XDR/MDR platform. Its Falcon Cloud Security ingests cloud logs and workload telemetry in near real time and applies adversary-driven analytics and attack path correlation informed by CrowdStrike's threat intelligence team. The runtime-first approach is strengthened by cloud detection logic derived from real-world adversary tradecraft, enabling detections that continuously evolve alongside attacker behavior. Coupled with strong marketplace traction and a broad partner ecosystem, it enables CrowdStrike to sustain robust growth in its cloud security portfolio.
- Palo Alto Networks is also positioned as a visionary leader on the Frost Radar™, driven by its integration of CDR into Cortex Cloud and Cortex/XSIAM. Its CDR capabilities are part of its code-to-cloud-to-SOC vision, leveraging cloud-native telemetry, graph-based context, and automated playbooks to deliver real-time TDR across multicloud environments, tightly coupled with SIEM analytics and automation. The company's ability to connect posture, workload protection, CDR, and broader AI-assisted SecOps workflows differentiates it for large enterprises looking for full-stack platform consolidation spanning network, endpoint, cloud, and SOC.
- Wiz is a leader on the Innovation and Growth indices. It has evolved its platform with a high velocity of innovation over the last few years, transforming from agentless CNAPP into a broader exposure management and emerging runtime platform with Wiz Defend, expanding Wiz's flagship security graph into runtime-powered prioritization and threat detection. This allows the platform to correlate vulnerabilities, misconfigurations, identities, data and network paths, and runtime insights across the cloud environment, making posture findings more actionable for SOC teams. Wiz's rapid product cadence and strong enterprise momentum give it outsized influence in how CNAPP-first vendors expand and evolve into CNADR.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Aqua Security and Sysdig are visionary leaders, scored highly for deep runtime protection and their role as runtime-powered CNAPP providers. Sysdig builds on Falco-based kernel telemetry to deliver real-time detection of container and K8s threats, correlating system calls, K8s audit logs, and cloud logs to provide SOC teams with full forensic and investigation capabilities and rapid response actions. It has increasingly positioned runtime as the starting point for CNAPP, with posture and vulnerability management layered around it. Aqua emphasizes enforcement-first runtime controls across containers, K8s and VMs, delivering excellent correlating capabilities of posture, identity, and runtime signals to prioritize toxic combinations of misconfigurations and exploitable vulnerabilities while expanding AI workload runtime security.
- Orca Security is an agentless CNAPP and cloud exposure management vendor that has continued to extend into runtime and CDR-adjacent capabilities. Orca's strength remains in broad cloud visibility, unified risk context, and SideScanning-based assessment, giving it strong appeal for customers focused on exposure reduction and attack path analysis rather than deeper SecOps-centric detection and response differentiation.
- Microsoft remains a notable player and is positioned as a visionary leader because of its established cloud runtime security capabilities, the scale of its hyperscale ecosystem, operational breadth of Defender for Cloud when integrated with Defender XDR, and huge customer base from its Azure business. Its value is driven more by platform breadth, ecosystem integration, and SecOps workflow convergence while improving its technology innovation CDR, workload runtime security, attack-path analysis, managed detection capabilities, and expanded recommendation coverage across major hyperscalers.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

Runtime-first CNADR leaders

- Upwind, ARMO, Oligo, and Sweet Security are rapidly growing, runtime-driven CNADR innovators with strong runtime capabilities across the cloud stack, but their differentiation is not identical.
- Upwind stands out for its inside-out, runtime-first approach, using runtime workload behavior, API activity, and data flows to validate risk in production and drive prioritization. Its runtime converges CDR, CWPP, API security, vulnerability prioritization, data security, and application runtime context into a unified CNADR concept. This positions Upwind as a strong runtime-powered CNAPP player and CNADR leader that helps cloud security, AppSec, and SecOps teams reduce alert noise, facilitate faster threat investigation, and prioritize remediation based on real production behavior rather than theoretical risk.
- Sweet Security differentiates itself through a unified cloud-native detection and response platform with SecOps-centric capabilities that brings together CDR, ADR, and CWPP with deep application profiling, eBPF-based behavioral baselining, and AI-generated incident storylines, positioning it as a consolidated SecOps layer for cloud environments that delivers rapid contextual investigation and noise reduction.
- ARMO has evolved beyond its K8s-centric security into a broader behavioral CNADR platform, using eBPF-based runtime telemetry, function-level anomaly detection, and code-to-cloud explainability to connect suspicious behavior from the exploited line of code through APIs, containers, clusters, and cloud resources, with automated responses using seccomp policies, network controls, and soft quarantine.
- Oligo, as an ADR pioneer, has evolved to be positioned as a CNADR leader. Oligo has extended its ADR platform across libraries, APIs, workloads, software supply chain exposure, and emerging AI runtime use cases. While remaining strong with deep exploit detection inside running applications, the platform can now connect application-layer insights with cloud-native runtime context to support cross-layer detection, investigation, and response.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

ADR innovators

- Contrast Security, Miggo, and Kodem form the ADR cohort in this analysis. These specialists have shown meaningful technological innovation and market disruption in application runtime protection, but with more limited market penetration and narrower coverage across the full CARS stack. Their strengths are more concentrated in application-centric detection, reachability, exploit validation, and prevention than unified cloud-to-application runtime security. However, their future growth depends on how they can commercialize their innovations at scale to sustain growth and become market leaders.
- With Oligo positioned as a CNADR player, Contrast Security is the strongest ADR innovator in this assessment, supported by its depth in application instrumentation, in-application attack detection, and runtime blocking. Its platform combines ADR, runtime vulnerability validation, exploit detection, attack blocking, and code-level remediation context, helping teams determine which application risks are reachable, exploitable, or actively attacked. By covering both preproduction application security and production runtime protection, Contrast gives AppSec and SecOps teams a stronger bridge between vulnerability discovery, runtime-confirmed exploitability, and real-time application defense.
- Miggo and Kodem are the more innovation-forward challengers, with momentum driven by adaptive runtime protection, library behavior analytics, vulnerable function monitoring, and exploit path validation that align with modern ADR buying criteria around production validation and risk prioritization. Miggo shows stronger upward momentum through adaptive protection and increasing relevance in AI-first application environments, while Kodem differentiates through memory analysis, runtime-based exploitability validation, using vulnerable-function monitoring, full execution-path mapping, and AI-assisted attack path analysis to improve reachability and exploitability-based prioritization in production.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

Exposure management-based players

- Tenable and Qualys form the exposure management-based cloud security group, leveraging their established VM, posture management, and broader exposure management capabilities while extending into emerging CDR and workload runtime security use cases. Both vendors are able to capture certain growth opportunities among large enterprise accounts that have already used their posture and exposure management solutions.
- Qualys has a strong TruRisk-driven runtime/CDR profile, combining eBPF-based threat detection, agentless cloud network and audit logs analysis, zero-day malware detection, container/K8s runtime security, application/API security, and QFlow automation. Qualys's strength lies in its ability to correlate runtime detection insights with posture and vulnerability findings to help prioritize risks and accelerate response and remediation across cloud, workload, and application environments, making it relevant for TDR in SecOps/SOC environments and earning it a higher innovation position in this analysis.
- Tenable has a more exposure-centric runtime security approach, using CDR insights, workload exposure, CIEM, JIT access, DSPM, AI-SPM, and attack path analysis to identify breach paths. Its runtime security is most relevant for identity-aware prioritization and exposure reduction, but has limited capabilities for deep workload telemetry, cloud forensics, or application-layer detection, which reduces its popularity in SecOps/SOC environments.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

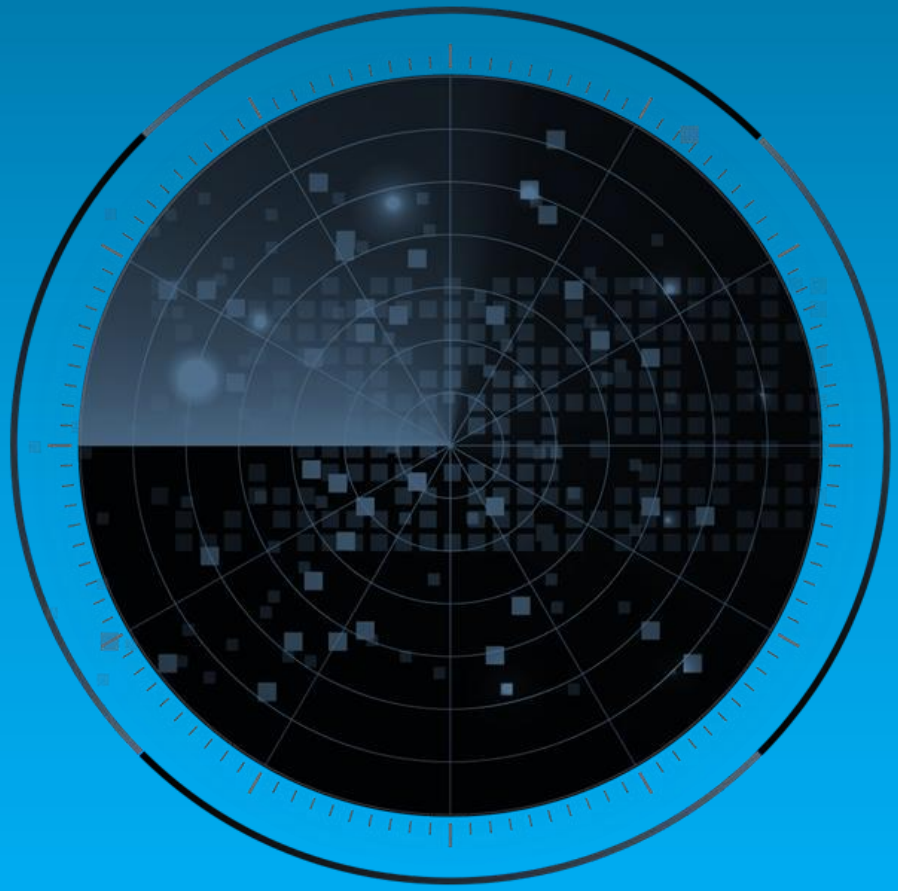
Cloud detection, investigation and response (CDIR) specialist

- Mitiga is positioned as a leading CDIR specialist in this analysis, differentiated by its focus on cloud, SaaS, identity, and AI detection, investigation, and response for SecOps teams and preemptive runtime security. The platform delivers advanced TDIR and forensics across cloud control planes, SaaS applications, identity systems, AI services, CI/CD pipelines, and data environments. Its Security Data Lake, automated forensic collection, AI-driven event correlation, MITRE mapping, and Cloud Attack Scenario Library provide analysts with strong insights to reconstruct attack timelines, investigate identity abuse and SaaS misuse, and reduce MTTR across complex cloud-native attack paths. Expansion into SaaS Detection and Response, AI Detection and Response, and Agentic SOC positions the company as a leading specialist in TDR across across cloud-, SaaS-, identity-, and AI-driven environments.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Companies to Action



Upwind

VISIONARY LEADER

INNOVATION SCORE **4.75**

GROWTH SCORE **4.30**

INNOVATION

- Upwind is positioned as a strong visionary leader in the CNADR category with a runtime-first cloud security architecture that converges CDR, workload protection, application/API security, posture, and exposure prioritization capabilities, operating from a common data and context layer, delivering excellent risk prioritization and detection and response across cloud-native environments.
- What makes Upwind stand out is that, instead of starting with static inventory, configuration checks, or vulnerability scanning like other traditional cloud security competitors, Upwind uses runtime data as the single source of truth for its platform operation to identify risk and detect threats in runtime. This gives Upwind a clear advantage in environments where security teams already have visibility but still struggle to detect critical risks from background noise of theoretical vulnerabilities and irrelevant alerts.
- The unified runtime fabric and inside-out runtime security philosophy makes Upwind a leader in runtime security. The platform uses a lightweight, advanced eBPF runtime engine to enable deep, real-time correlation between configuration findings, actual workload activity, network traffic, application, and identity behavior visibility to validate posture, vulnerability, API, and data findings in production, allowing teams to focus on actual risk from alert noise.
- Upwind is particularly strong in CDR. It combines cloud activity, workload telemetry, network and application flows, cloud logs, and cloud APIs into a single security platform. It delivers automatic baselining of cloud activity, rapid investigation, cloud-native forensics, and cross-layer correlation, enabling security teams to understand blast radius, exploitability, and APA without manually stitching together siloed findings or alerts. The deep context combination enables Upwind to increase risk prioritization and active prevention capabilities, dramatically reducing noisy alert as much as 95% and accelerating remediation.

Source: Frost & Sullivan

Upwind (continued)

VISIONARY LEADER

INNOVATION SCORE **4.75**

GROWTH SCORE **4.30**

INNOVATION

- Upwind's runtime security is not limited to CDR, CWPP, or ADR, which primarily focus on cloud infrastructure, workloads, identities, and runtime activity, or application and API behavior. Upwind offers unified runtime security capabilities across cloud and application layers by correlating cloud and application runtime context in one platform, giving it a broader detection and response model of CNADR than competitors that specialize in only one side of the runtime security.
- As cloud-native attacks move across infrastructure, identity, workload, API, and application layers, this distinction is becoming more important. Upwind's ability to connect cloud and application runtime insights helps security teams understand how exposure, runtime activity, API behavior, and sensitive data flows form real risk, making the platform more relevant as enterprises move toward more integrated cloud-native detection and response models.
- The platform also has strong security coverage across modern cloud-native environment, extending across containers, K8s, serverless, and managed compute services, including AWS Fargate, AWS Lambda, Google Cloud Run, and Azure Container Apps. This breadth enables it to gain traction as enterprises need runtime security to cover hosts, containers, serverless functions, managed services, APIs, and application-centric workloads.
- Upwind's recent product expansion and roadmap shows its commitment to innovation by extending the platform beyond workload runtime protection into a broader runtime-driven CNAPP and CNADR architecture. The expansion across managed compute, serverless, API security, data security, AI security, code security, and attack surface validation strengthens the platform's ability to correlate production behavior across cloud infrastructure, applications, identities, data flows, and build pipelines.

Source: Frost & Sullivan

Upwind (continued)

VISIONARY LEADER

INNOVATION SCORE **4.75**

GROWTH SCORE **4.30**

GROWTH

- Upwind is one of the most dynamic emerging players in the cloud security market, standing out through its runtime-powered CNAPP platform. It witnessed explosive revenue growth of more than 4,000% YoY in 2024, maintaining exceptional growth momentum in 2025 and into 2026. It has become one of the best-performing players and has gradually become a significant contender in the CNAPP space.
- Upwind has grown its enterprise client base, with notable traction among technology, financial services, and SaaS organizations seeking a comprehensive cloud security solution with robust runtime capabilities. It is especially well suited to cloud-first and application-centric enterprises with heavy use of K8s, containers, serverless, APIs, microservices, and managed cloud services, many of which are midsize to large enterprises in North America, where it is executing an aggressive sales strategy.
- Upwind is expanding its enterprise client base globally, notably among Fortune 150 and G5000 companies, while driving mid-market growth through cloud marketplaces. Its channel-centric model is driven by MSSP partnerships, especially in Latin America and APAC, where 50% of regional revenue already flows through managed service partners.
- Upwind's CNADR positioning gives it a broader growth path than CDR or ADR specialists. As buyers seek to bring cloud runtime and application runtime security into a single operating model, Upwind's ability to connect infrastructure, workloads, APIs, applications, identities, and data strengthens its relevance for cloud-native detection and response.

Source: Frost & Sullivan

Upwind (continued)

VISIONARY LEADER

INNOVATION SCORE **4.75**

GROWTH SCORE **4.30**

GROWTH

- The company has doubled down on expansion efforts to scale its regional footprint to meet demand for its platform in APJ region, establishing offices in Mumbai, Bangalore, Pune, Singapore, Tokyo, and Sydney, and has added local SaaS instances across India, Australia, Singapore, and Japan to address regional data residency, performance, and operational requirements. Regional buildout helps strengthen Upwind's infrastructure and business presence in the region and improves its ability to serve regulated and cloud-maturing enterprises that require local support, faster performance, and stronger alignment with local market conditions.
- Upwind's overall GTM strategy combines enterprise direct engagement with marketplace and partner-driven expansion. This momentum is strengthened by its February 2026 integration with the Extended plan for AWS Security Hub, where Upwind became a Select CNAPP partner, giving customers a simplified AWS-aligned procurement path with one contract, one bill, consolidated support, and flexible pricing while embedding Upwind more directly into the AWS security operating model.
- These developments will help Upwind tap larger market opportunities by strengthening regional execution and CSP-driven business simplification and huge customer bases. Combined with its multicloud product support, marketplace presence, and runtime-driven CNAPP value proposition, Upwind is well positioned to compete for larger enterprise cloud security programs, which will help it increase its footprint and drive its exceptional growth momentum in the years to come.

Source: Frost & Sullivan

Upwind (continued)

VISIONARY LEADER

INNOVATION SCORE **4.75**

GROWTH SCORE **4.30**

FROST PERSPECTIVE

- Upwind stands out as one of the most architecturally differentiated emerging vendors in the cloud security market, differentiating itself through an inside-out runtime-powered architecture that provides powerful and comprehensive runtime capabilities across cloud, workload, and application layers, enabling excellent risk prioritization and effective TDR in the modern cloud-native environment.
- Upwind's runtime cloud security platform is an evolution of modern cloud security, well aligned with the market shift from visibility to active runtime TDR, from static scanning to runtime validation, and from separate posture, workload, API, and application tools to one unified runtime security model that supports modern cloud security from code to cloud and to SOC with robust runtime capabilities, accurate risk prioritization, and precise detection, investigation, and response across the cloud stack.
- Upwind is positioned as one of the few credible CNADR vendors, making it a visionary leader that converges CDR, CWPP, and API security, setting it apart from other CNAPP platforms and CDR and ADR specialists. As organizations seek to converge cloud and application runtime security, Upwind's ability to connect runtime context across infrastructure, workloads, APIs, applications, identities, and data gives it a strong fit for customers that want one operating model for risk prioritization, detection, investigation, and response in the cloud environment.
- Upwind is not replacing SOAR and SOC tools but acting as the cloud-native investigation layer, offering analysts visibility into runtime behavior, API activity, identity usage, execution paths, affected assets, and blast radius. It is well positioned to complement and support these systems for modern CloudSecOps. It gives organizations, particularly SecOps teams, an important complement for their entire SecOps strategy with deeper cloud and application runtime context.

Source: Frost & Sullivan

Upwind (continued)

VISIONARY LEADER

INNOVATION SCORE **4.75**

GROWTH SCORE **4.30**

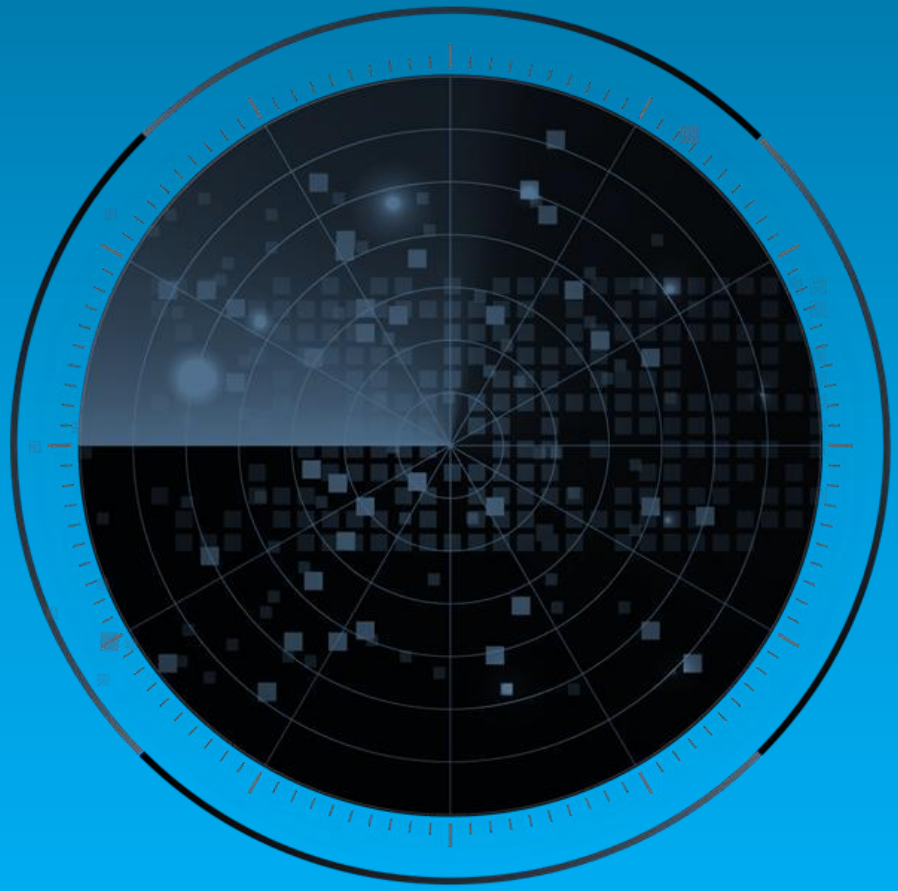
FROST PERSPECTIVE

- While Upwind is highly regarded for its runtime capabilities, it should continue maturing its SOC relevance to strengthen adoption among large enterprises. Priority areas include more standardized detection formats, MITRE ATT&CK mapping, investigation timelines, SIEM/SOAR integrations, response playbooks, and remediation ownership workflows that can support coordinated action across SOC, DevOps, AppSec, and compliance teams. At the same time, Upwind should deepen its ADR capabilities beyond API and application traffic investigation, with stronger inside-app monitoring, business logic detection, and function-to-function detection and response.
- Upwind's unified runtime security capabilities have supported rapid growth since its inception and will sustain the momentum over the next few years as the company continues investing in human resources, GTM execution, and product innovation. Its channel expansion, geographic push in APJ, and selection as a CNAPP partner in the Extended plan for AWS Security Hub are anticipated to help strengthen global customer outreach and support growth.
- The next test is enterprise-scale operationalization at a global level. Upwind has demonstrated operational maturity through deployments with Fortune 50, 100, 200, and 500 customers, but it still needs broader brand recognition, a larger partner ecosystem, and a wider enterprise customer base to build confidence among large global buyers.
- Upwind still competes against vendors with larger installed bases, stronger field coverage, deeper channel ecosystems, and more mature SOC workflows. Its technical differentiation is strong, but becoming a durable enterprise standard in large, regulated, multicloud environments will require more than technological innovation. Compliance depth, support maturity, SOC integration, platform reliability, and global execution will be equally important to sustaining its growth trajectory.

Source: Frost & Sullivan

FROST & SULLIVAN

Best Practices & Growth Opportunities



Best Practices

1. Security leaders should avoid adopting runtime security, particularly CDR or ADR, as isolated point solutions. Runtime telemetry becomes more valuable when correlated with posture findings, identity risk, data sensitivity, code ownership, and threat intelligence as it provides context to connect prevention, detection, investigation, and remediation into one risk reduction workflow.

2. Organizations should close the runtime visibility gap by collecting real-time data from cloud control planes, containers, K8s clusters, serverless workloads, APIs, inside-app behavior, processes, files, and identities. Lightweight technologies, such as eBPF and runtime sensors, should be used where appropriate to provide a source of truth with minimal performance impact and improve detection quality across cloud-native environments.

3. Security teams can adopt CDR, ADR, and CNADR in stages based on maturity and risk priorities. Many organizations should begin with CDR and workload runtime security to improve cloud threat detection, then add ADR for application-layer exploit visibility and progress to CNADR when they need unified investigation and response across cloud, workload, API, identity, data, and application layers.

Source: Frost & Sullivan

Growth Opportunities

1. As organizations move beyond posture management, vendors have opportunities to turn runtime security into the next expansion layer of CNAPP, XDR, and SecOps platforms. Buyers increasingly need CDR, ADR, CWPP, K8s runtime security, API security, and workload telemetry to validate exploitability, detect active threats, and support investigation and response, creating new growth areas for cloud security players.

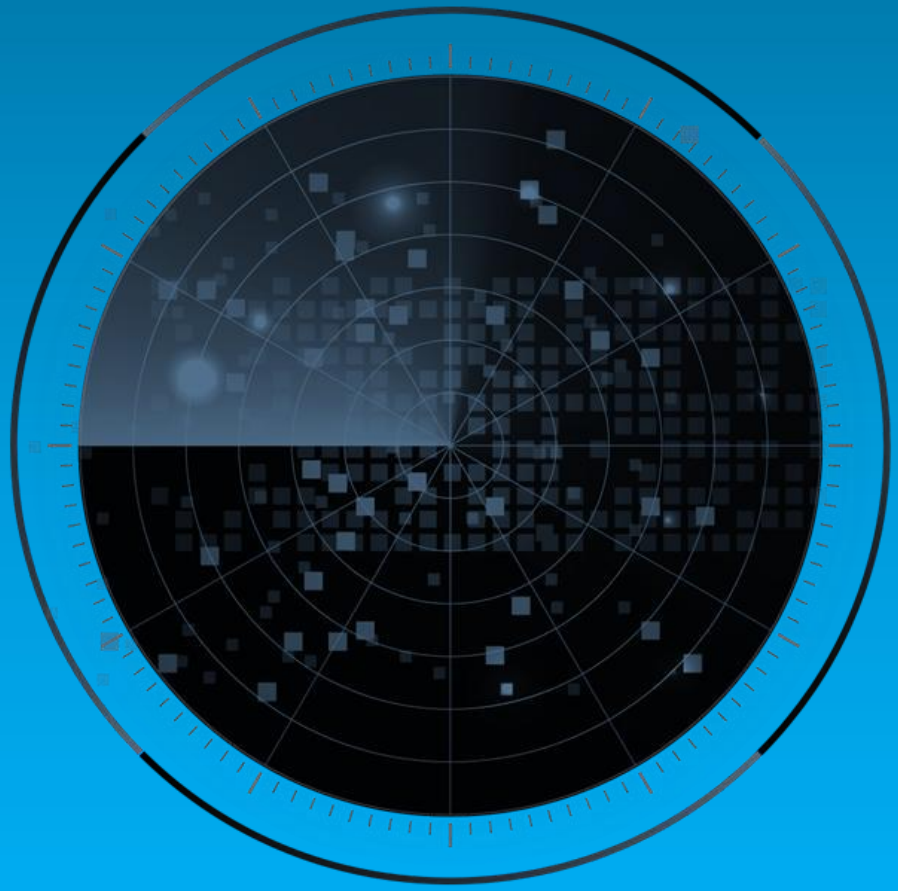
2. MSSPs, MDR providers, and incident response firms can benefit from the demand for cloud-native detection and response services. Many organizations want TDR outcomes but often lack the internal cloud forensics, detection engineering, and response expertise to operate these capabilities effectively. This positions them to package runtime security into managed cloud threat detection, investigation, response, and remediation services integrated with SIEM, SOAR, ticketing, and cloud operations workflows.

3. AI workloads, agentic applications, and API-driven architectures create a new growth opportunity for runtime security vendors. As organizations deploy AI agents, LLM applications, autonomous workflows, and machine identities in production, they need visibility into model behavior, API activity, data flows, identities, and workload interactions. Cloud security vendors can extend runtime security into AI runtime security and sensitive data protection to capture emerging AI security investment.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Analytics



Frost Radar™: Benchmarking Future Growth Potential
2 Major Indices, 10 Analytical Ingredients, 1 Platform

Growth Index

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline system; and effective market, competitor, and end-user focused sales and marketing strategies.

GI1

MARKET SHARE (PREVIOUS 3 YEARS)
This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.

GI2

REVENUE GROWTH (PREVIOUS 3 YEARS)
This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar™.

GI3

GROWTH PIPELINE
This is an evaluation of the strength and leverage of a company's growth pipeline system to continuously capture, analyze, and prioritize its universe of growth opportunities.

GI4

VISION AND STRATEGY
This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?

GI5

SALES AND MARKETING
This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Source: Frost & Sullivan

Frost Radar™: Benchmarking Future Growth Potential
2 Major Indices, 10 Analytical Ingredients, 1 Platform (continued)

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive megatrends) that are globally applicable, are able to evolve and expand to serve multiple markets and are aligned to customers' changing needs.

II1

INNOVATION SCALABILITY
This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.

II2

RESEARCH AND DEVELOPMENT
This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.

II3

PRODUCT PORTFOLIO
This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.

II4

MEGATRENDS LEVERAGE
This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of megatrends can be found here.

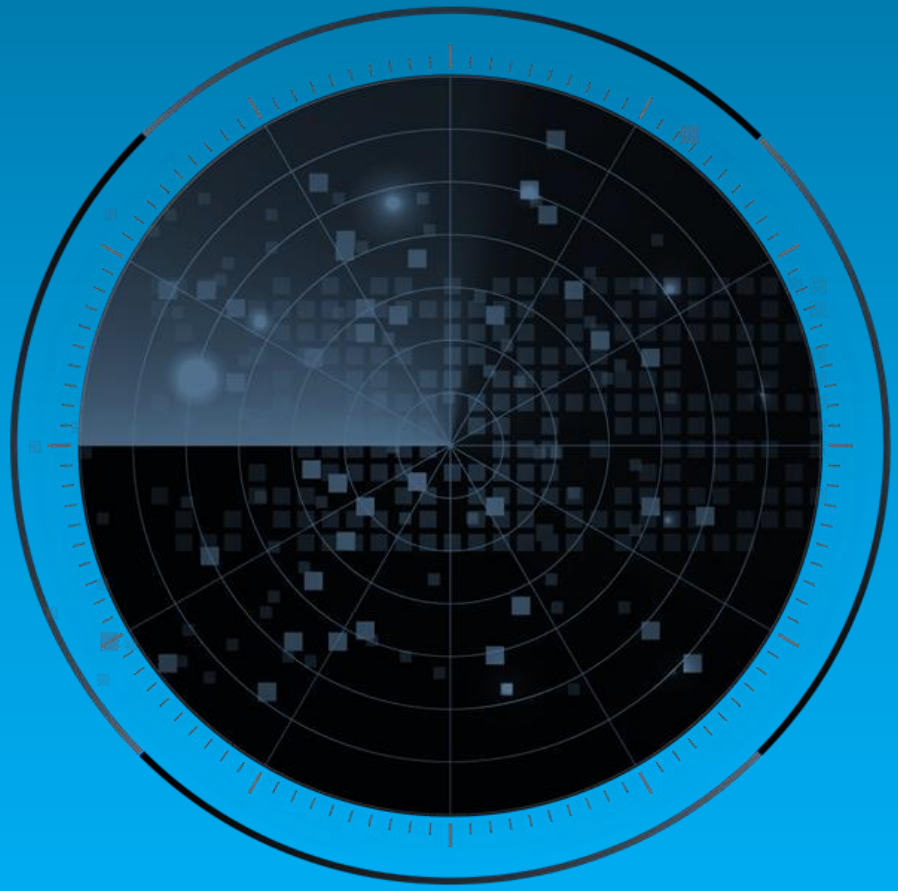
II5

CUSTOMER ALIGNMENT
This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Source: Frost & Sullivan

FROST & SULLIVAN

Next Steps: Leveraging the Frost Radar™ to Empower Key Stakeholders



Significance of Being on the Frost Radar™

Companies plotted on the Frost Radar™ are the leaders in the industry for growth, innovation, or both. They are instrumental in advancing the industry into the future.

GROWTH POTENTIAL

Your organization has significant future growth potential, which makes it a Company to Action.

BEST PRACTICES

Your organization is well positioned to shape Growth Pipeline™ best practices in your industry.

COMPETITIVE INTENSITY

Your organization is one of the key drivers of competitive intensity in the growth environment.

CUSTOMER VALUE

Your organization has demonstrated the ability to significantly enhance its customer value proposition.

PARTNER POTENTIAL

Your organization is top of mind for customers, investors, value chain partners, and future talent as a significant value provider.

Source: Frost & Sullivan

Frost Radar™ Empowers the CEO's Growth Team

STRATEGIC IMPERATIVE

- Growth is increasingly difficult to achieve.
- Competitive intensity is high.
- More collaboration, teamwork, and focus are needed.
- The growth environment is complex.

LEVERAGING THE FROST RADAR™

- The Growth Team has the tools needed to foster a collaborative environment among the entire management team to drive best practices.
- The Growth Team has a measurement platform to assess future growth potential.
- The Growth Team has the ability to support the CEO with a powerful Growth Pipeline™.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline™ Dialogue with Team Frost**

Source: Frost & Sullivan

Frost Radar™ Empowers Investors

STRATEGIC IMPERATIVE

- Deal flow is low and competition is high.
- Due diligence is hampered by industry complexity.
- Portfolio management is not effective.

LEVERAGING THE FROST RADAR™

- Investors can focus on future growth potential by creating a powerful pipeline of Companies to Action for high-potential investments.
- Investors can perform due diligence that improves accuracy and accelerates the deal process.
- Investors can realize the maximum internal rate of return and ensure long-term success for shareholders
- Investors can continually benchmark performance with best practices for optimal portfolio management.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Opportunity Universe Workshop**
- **Growth Pipeline Audit™ as Mandated Due Diligence**

Source: Frost & Sullivan

Frost Radar™ Empowers Customers

STRATEGIC IMPERATIVE

- Solutions are increasingly complex and have long-term implications.
- Vendor solutions can be confusing.
- Vendor volatility adds to the uncertainty.

LEVERAGING THE FROST RADAR™

- Customers have an analytical framework to benchmark potential vendors and identify partners that will provide powerful, long-term solutions.
- Customers can evaluate the most innovative solutions and understand how different solutions would meet their needs.
- Customers gain a long-term perspective on vendor partnerships.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Growth Pipeline™ Diagnostic**
- **Frost Radar™ Benchmarking System**

Source: Frost & Sullivan

Frost Radar™ Empowers the Board of Directors

STRATEGIC IMPERATIVE

- Growth is increasingly difficult; CEOs require guidance.
- The Growth Environment requires complex navigational skills.
- The customer value chain is changing.

LEVERAGING THE FROST RADAR™

- The Board of Directors has a unique measurement system to ensure oversight of the company's long-term success.
- The Board of Directors has a discussion platform that centers on the driving issues, benchmarks, and best practices that will protect shareholder investment.
- The Board of Directors can ensure skillful mentoring, support, and governance of the CEO to maximize future growth potential.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**

Source: Frost & Sullivan

Next Steps

JOIN:
Growth Council

APPLY:
Companies to Action

ENGAGE:
Growth Dialog

PARTICIPATE:
Growth Council Think Tank

Does your current system support rapid adaptation to emerging opportunities?

Source: Frost & Sullivan

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com