FROST & SULLIVAN

Frost Radar™: Cloud Workload Protection Platforms, 2025

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

Authored by: Anh Tien Vu
Contributors: Jarad Carleton

PG3M-74
September 2025

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Source: Frost & Sullivan

List of Abbreviations

- **ADR:** Application Detection and Response
- **AI SPM:** Artificial Intelligence Security Posture Management
- **API:** Application Programming Interface
- **AppSec:** Application Security
- **ASPM:** Application Security Posture Management
- **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
- **CloudSecOps:** Cloud Security Operations
- **CNADR**: Cloud-Native Application Detection and Response
- **CNAPP:** Cloud-Native Application Protection Platform
- **CSP:** Cloud Service Provider
- **CSPM:** Cloud Security Posture Management
- **CWPP:** Cloud Workload Protection Platform
- **DAST:** Dynamic Application Security Testing
- **DevOps:** Development and Operations
- **DevSecOps:** Development and Security Operations
- **eBPF:** Extended Berkeley Packet Filter
- **EDR:** Endpoint Detection and Response
- **FIM**: File Integrity Management
- **IaC:** Infrastructure as Code
- **IAST:** Interactive Application Security Testing
- **IR**: Incident Response
- **KSPM:** Kubernetes Security Posture Management
- **LB:** Large Business
- **MSSP:** Managed Security Service Provider
- **MTTR**: Mean Time to Remediate
- **OSS:** Open-Source Software
- **PaaS:** Platform as a Service
- **RASP:** Runtime Application Self-Protection
- **SAST:** Static Application Security Testing
- **SBOM:** Software Bills of Materials
- **SCA:** Software Composition Analysis
- **SCM:** Source Code Management
- **SDK:** Software Development Kit
- **SecOps:** Security Operations
- **SIEM:** Security Information and Event Management
- **SMB:** Small and Medium-Sized Business
- **SOAR**: Security Orchestration, Automation, and Response
- **SOC**: Security Operation Center
- **SQL:** Structured Query Language
- **SSCS:** Software Supply Chain Security
- **TDR:** Threat Detection and Response
- **VM:** Virtual Machine
- **WAAP:** Web Application Firewall and API Protection
- **WAF:** Web Application Firewall
- **YoY:** Year Over Year

Source: Frost & Sullivan

Strategic Imperative

- Organizations worldwide continue to accelerate their cloud adoption in 2025; multicloud and hybrid cloud strategies are becoming the norm as businesses diversify their strategies and migrate a greater volume of workloads to cloud environments. Cloud migration is also driven by the surge in adoption of AI-native applications and services, as on-premises systems are not designed to support them.
- The broad adoption of cloud has exposed new security challenges, such as inconsistencies in controls across cloud platforms and gaps in workload risk and threat visibility, which attackers have been quick to exploit. This has driven a corresponding rise in demand for cloud workload protection solutions to manage these complex environments and provide comprehensive visibility and security protection for cloud workloads, applications, and data.
- Many businesses realize that they must adopt CWPP to protect their critical workloads in these complex cloud environments by enabling automation, deep visibility, and detection of misconfiguration, vulnerabilities, secret exposure, policy violation, compliance misalignment, anomalous behavior and threats across diverse cloud workloads, such as containers, K8s clusters, and serverless functions.
- A CWPP, which is normally agent-based, is a server workload-centric security solution to protect computing workloads in cloud environments (private, public, hybrid, and multicloud) from cybersecurity risks and attacks, regardless of the workload's location. Typical workloads that CWPPs secure include cloud/edge servers, hosts, VMs, containers/K8s, serverless functions, databases (SQL and NoSQL), APIs, and AI models.
- By providing critical pre-deployment security checks, such as scanning of IaC templates, virtual machine and container images, and compliance management, CWPPs can provide better workload misconfiguration and vulnerability management across workloads, repositories, CI/CD pipelines, and application codes and automate remediation to reduce exposure to supply chain attacks.

Source: Frost & Sullivan

Strategic Imperative (continued)

- As VM-based workloads are gradually displaced by containers, the need for integrated container security in CWPP solutions is set to grow, with increased focus on visibility into K8s environments, protection for container images, and application components in CI/CD pipelines.
- CWPP is often used as a part of CNAPP and/or CNADR and integrated with other security tools, such as vulnerability management, SCA, CI/CD pipeline security, K8s protection, CSPM, DSPM, API protection, and broader exposure management platforms with automated remediation capabilities, creating a holistic approach to cloud-native environment protection.
- As a result, modern CWPPs are evolving and extend security capabilities beyond foundational features, such as workload discovery, misconfiguration detection, visibility, compliance, and vulnerability management, to deliver robust runtime security, automated remediation, and advanced TDR. Many CWPPs now can monitor workloads in runtime, detect and block threats in real time through the integration with CDR and EDR, and use behavior-based analytics to identify anomalies and malware as they occur.
- There is an increasing need for seamless integration with SecOps and SOC workflows to automate remediation and streamline incident management enables security teams to quickly act on prioritized risks with contextual insights. This allows organizations to gain visibility from code to cloud to better manage dynamic, multicloud environments effectively while helping to transform modern SecOps to maintain strong, proactive defenses against increasingly sophisticated cloud-native threats, and reflects a broader trend toward proactive, dynamic threat management in response to escalating supply chain and runtime attacks.

Source: Frost & Sullivan

Growth Environment

- The CWPP industry is in a growth phase and has evolved rapidly, with vendors prioritizing real-time threat detection, runtime protection, and cloud-native workload visibility. Many LBs invest heavily in cloud security technologies and their workforce to secure workloads, applications, and data to avoid service disruptions and data breaches and adhere to regulatory compliances.
- The CWPP market is expected to generate revenue of $6.43 billion in 2025, representing YoY growth of 25.4%. Revenue is set to hit $15.54 billion in 2030 (a compound annual growth rate of 19.3% from 2025 to 2030).
- Customers in the BFSI and tech industries are the largest adopters of CWPP, requiring robust cloud security solutions to manage compliance, shift-left security, vulnerability/risk management, and runtime protection/threat management. They take a proactive approach to cloud security and cyber-risk management as they accelerate their cloud migration for critical workloads.
- The growth of cloud spending, better awareness of the cloud threat landscape, and heightened accountability of CISOs and their teams are driving CWPP adoption globally. The use of multicloud, hybrid cloud, and containerized environments in modern application development exacerbates inherent cloud security challenges that create gaps in visibility and control in the supply chain.
- Simultaneously, as organizations are maturing their DevSecOps culture, there are requirements for integration of CWPP with the CI/CD pipeline to enable automated security and compliance checks. This integration provides granular visibility into the entire application development lifecycle.

Source: Frost & Sullivan

Growth Environment (continued)

- Adoption patterns have shifted from a narrow focus on misconfiguration and compliance toward real-time risk management and active workload protection. Organizations recognize that preventive controls alone are insufficient, shifting their focus to runtime security, anomaly detection, and automated remediation.
- CISOs continue to face significant challenges that are shaping adoption patterns. Alert fatigue and tool sprawl remain major pain points, while fragmented tools are creating blind spots and overwhelming SOC teams, making their SecOps less effective. This has driven a push for consolidation, with enterprises seeking unified platforms that integrate security posture management, workload runtime protection, identity and data security, as well as AI security with a single data lake for better risk management and SecOps efficiency.
- Adoption barriers persist because of misconceptions about the shared responsibility model, underdeveloped DevSecOps cultures, and challenges integrating with legacy infrastructure. Concerns regarding total cost of ownership, performance, and compliance obligations contribute to enterprise hesitancy in expanding cloud usage or adopting new workload security tools.
- Despite these challenges, the market is set to maintain a robust growth trajectory with increasing demand for unified, runtime-focused, and developer-friendly cloud security solutions. Enterprises are finding ways to balance innovation with resilience in an increasingly complex cloud landscape.

Source: Frost & Sullivan

Growth Environment (continued)

- Frost & Sullivan studies related to this independent analysis:
  - Global Cloud-native Application Protection Platform Growth Opportunities
  - Growth Opportunities in Global Cloud Security Posture Management, 2024–2028
  - SaaS Security Posture Management (SSPM) and Data Security Posture Management (DSPM)
  - Global Software Supply Chain Security Growth Opportunities
  - Cloud Workload Protection Platform (CWPP) Market, Global, 2024–2028
  - Cloud-native Application Protection Platform (CNAPP) Market, Global, 2025–2029
  - Cloud/Application Runtime Security (CARS), 2025
  - Frost Radar™: Cloud/Application Runtime Security, 2025

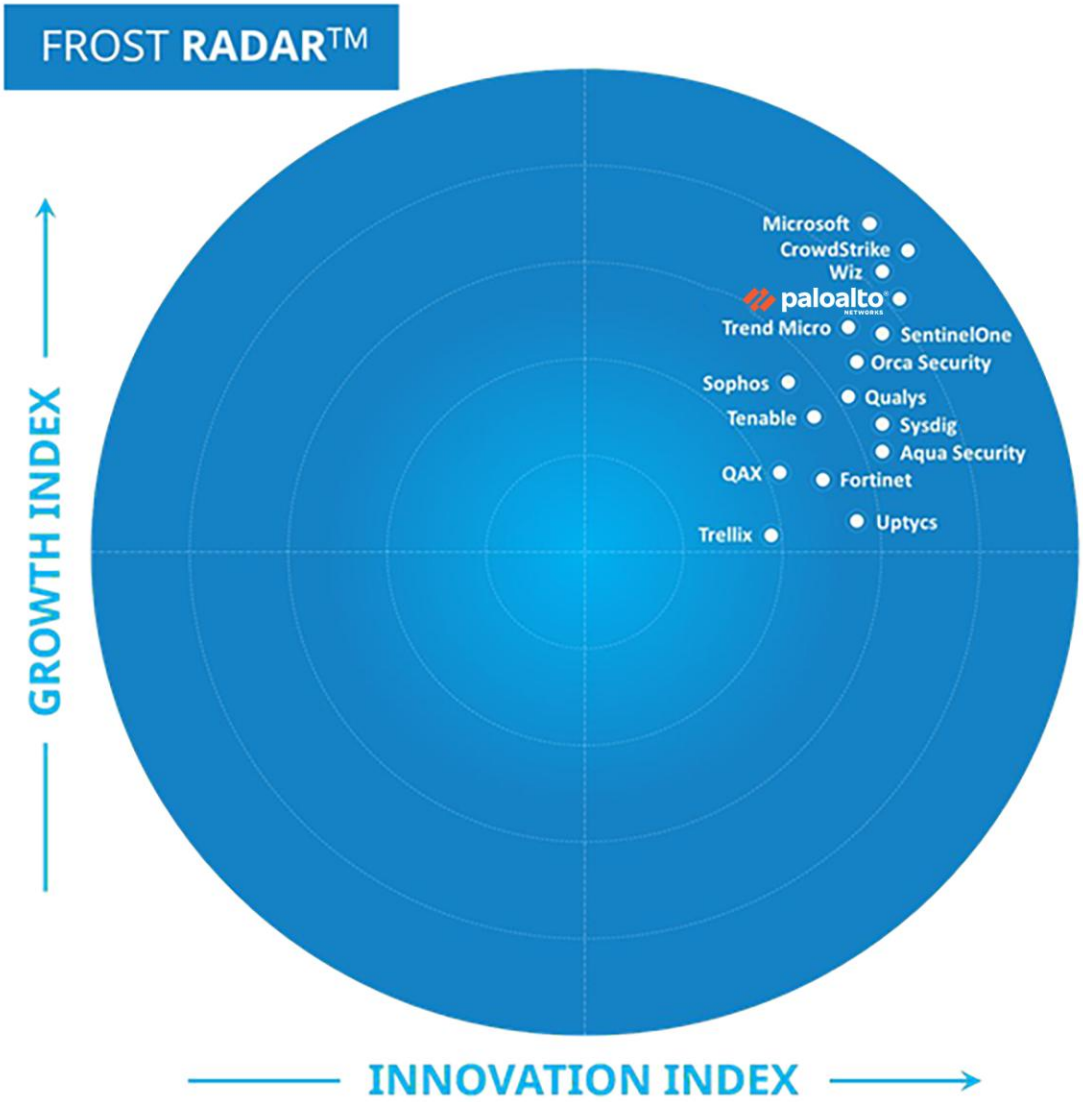
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Cloud Workload Protection Platforms

Source: Frost & Sullivan

Frost Radar™: Cloud Workload Protection Platforms, 2025



FROST & SULLIVAN

Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- Because CWPP is increasingly integrated with other security solutions, this Frost Radar™ does not solely assess CWPP solutions and their technological features and capabilities; it also evaluates the segment in the context of the broader cloud security industry, including CNAPP and CNADR.
- Vendors registering an estimated annual revenue of at least $50 million in 2025 are included in this analysis, including Aqua Security, CrowdStrike, Fortinet, Microsoft, Orca Security, Palo Alto Networks, QAX, Qualys, SentinelOne, Sophos, Sysdig, Tenable, Trellix, Trend Micro, Uptycs, and Wiz. Frost & Sullivan has identified these companies as the top technology players in the global CWPP industry.
- Frost & Sullivan also recognizes endeavors of Bitdefender, Caveonix, Rapid7, Skyhawk Security, Red Hat, Sonrai Security; other start-up companies, such as Sweet Security, ARMO, and Upwind; and Chinese vendors, including Asiainfo Sec, Tencent Cloud, TopSec, Hillstone Networks, and NSFOCUS. While these vendors demonstrated substantial technological advancements and market expansions, they were not included on this Frost Radar™ for one or more of the following reasons:
  - Their revenue is small and global market presence is relatively limited.
  - They declined to participate.
  - They were unable to provide direct input.
  - Secondary research alone was insufficient to deliver a robust analysis.
- While revenue estimates are based on CY2025, this analysis and vendor assessment are based on information available, vendor performance, and market conditions as of September 2025.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- With CWPP being increasingly integrated with the broader cloud security platform, vendors' innovation strategies revolve around CNAPP and CNADR to provide organizations with security capabilities from code to cloud and to SOC with comprehensive visibility, vulnerability, and risk management on the left and TDR in the runtime environment on the right.
- Most players are in the race to develop new technological features and capabilities to maintain competitiveness, focusing on automated compliance, workload vulnerability and risk prioritization, AI-guided remediation, and integration with DevOps and GitOps workflows for better CI/CD pipeline and software supply chain security.
- CWPP players are also focusing on integration with CDR, ADR, XDR, threat intelligence platforms, and SOC tools and workflows, such as SIEM, SOAR, and ticket system, to gain real-time visibility into the threat landscape and unlock threat detection, response, and investigation capabilities. As a result, top vendors are defined not just by breadth, but also by runtime protection and TDR.
- AI is becoming an integral part of cloud security solutions to enhance threat detection, investigation, risk prioritization, and remediation. Vendors are embedding AI assistants capable of natural language queries, guided investigations, and automated, role-specific security recommendations.
- AI/LLM workload security has also become a differentiator. Most vendors featured in this analysis are racing to add AI security to their cloud security platform, spanning AI security posture, model scanning, and AI runtime protection.
- Although technological features and capabilities remain key factors in evaluating CWPP solutions, customers also consider other factors when choosing a solution. These include the vendor's product ecosystem, sustainability, and support; and the solution's stability, ease of use, integration capability with existing and future technologies, and ROI.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Most top vendors stand neck to neck, investing heavily in technological innovation and bridging the gap in features and capabilities. Customers can benefit from the heated competition through unique innovation, faster feature development, and a variety of choices, from stand-alone products to address specific use cases to all-in-one cloud security platforms that are often designed to cater to different personas and use cases. Nonetheless, it is their responsibility to balance the need for specialized tools and features with the organization's business strategy, vision, and long-term support from vendors of choice.
- Wiz continues to experience explosive revenue growth, outpacing most competitors, and is positioned as a growth leader in this analysis. The company has become a strong choice for cloud infrastructure security, particularly for its risk management capabilities for cloud workloads. It has also shown its aggressive innovation pace by expanding its platform, from agentless posture management, exposure management, and AI security to deeper runtime insights, integrating real-time detection capabilities through its Wiz Runtime Sensor and Wiz Defend, marking a milestone for Wiz to strengthen its runtime security with the CDR capabilities. Wiz Defend is designed to bring cloud security operation into SOC, expanding its inherently leading CNAPP capabilities.
- Microsoft remains a leader in the CWPP market as the largest player in terms of revenue, with consistent and robust revenue growth over the last few years. By leveraging its diversified Azure customer base with LBs across various industries, the vendor continues expanding its Defender for Cloud business among those using Azure cloud services. It continues to enhance its workload protection by offering unified runtime protection across AKS, Azure VMs, and AWS/GCP workloads, adding eBPF-based detection and AI security and enhancing DevSecOps best practices for better workload vulnerability and risk management. It also enhanced the correlation of risk and threat insights with Defender XDR and CDR for richer investigation and TDR.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- CrowdStrike maintains substantial growth for its Falcon Cloud Security business, leveraging its superior brand perception and extensive customer base for its XDR platform and MDR services. With its strong capabilities of cloud runtime security, supplemented by its CDR, CrowdStrike is an excellent candidate for cloud workload security, particularly in Windows environments. It has added agentless workload visibility, cloud-native threat intelligence, and K8s runtime controls, enabling pre-deployment and runtime protection in a single platform. It is doubling down on XDR and CDR for cloud workloads, evolving Falcon Cloud Security into a unified platform that spans posture, runtime, identity, data, and AI-model protection.
- Palo Alto Networks is one of the largest cloud security players in revenue and maintains robust growth, leveraging its large customer base in network security, SASE, and XSIAM. Its Cortex Cloud (an evolution of Prisma Cloud) platform leads with its breadth, covering all major CNAPP functions from shift-left security to runtime with deep K8s and serverless protection. The company has added new capabilities, including real-time network anomaly detection and predictive runtime profiling for zero-day defense. Cortex Cloud is transforming security operations to cater to diverse user groups, including DevOps, cloud/app security, and SecOps teams, enabling them to handle cloud-native threats more effectively.
- SentinelOne remains one of the fastest-growing players in the market. Leveraging a growing customer base from its XDR and MDR service lines, it has increased its workload security penetration over the last two years. SentinelOne has strengthened cloud workload runtime security with new capabilities, such as behavioral AI-based detection for containers and cloud VMs and new integrations into DevOps workflows for proactive workload protection. Its workload security solution has integrated into the broader Singularity platform, providing cross-domain correlation, from endpoint, identity, and workload alerts in a single data lake, to offer a streamlined visualizations and AI integration (with its Storyline ™ and Purple AI™) for rapid threat hunting.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Sysdig remains a prominent pure-play CNAPP provider with a focus on solving issues in cloud-native, container, and K8s environments. Its Sysdig Secure has been widely adopted globally, particularly in North America, with most of its 700-plus clients from large enterprises and rapidly growing software companies in BFSI, high-tech, retail/eCommerce, and media/telco. Sysdig sharpens its edge in runtime security with Falco enhancements, eBPF performance improvements, and stronger integrations for real-time threat correlation, enabling its CWPP to detect threats in real time, with granular visibility into containers, servers, K8s, and serverless stacks.
- Aqua Security has been growing steadily over the last two years, maintaining a leadership position in the cloud-native security space. Aqua has more than 500 enterprise customers (many in the Fortune 100) with penetration in large organizations across key industries, including the US government, defense, BFSI, and technologies. However, its growth is lower than other competitors, causing it lose significant market share. Aqua has doubled down on its runtime observability over the last two years for granular attack path tracing and rapid protection using eBPF-powered enforcement. This helps teams detect and block zero-day exploits and live memory threats in production workloads.
- Orca Security has a robust and consistent growth trajectory. Orca's GTM strategy has been focused on its value proposition of "instant-on, agentless" security, which has resonated with security teams frustrated by agent fatigue and deployment delays. Its cloud workload protection leverages both agentless scanning and its lightweight eBPF-based Orca Sensor to provide real-time detection of threats such as container escapes, privilege escalation, and suspicious runtime activity. It supports workloads across VMs, containers, and serverless environments in AWS, Azure, and GCP.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Tenable's cloud security business has seen a recent uptick, leveraging its strong partner ecosystem and customer base exceeding 40,000 from Nessus and vulnerability management businesses. Its CWPP is integrated with identity-aware workload protection, leveraging AI-driven entitlement and privilege analysis that connects identity risk (e.g., AD, Azure AD) with workload vulnerabilities into Tenable One's unified exposure platform. Tenable has particularly strengthened runtime container protection with continuous eBPF monitoring, admission-controller management for K8s workloads, JIT access controls, and integrated IaC and vulnerability intelligence from build time through production.
- Qualys's cloud security business is growing fast, leveraging its customer base in its vulnerability management business, making it one of the fastest-growing vendors with a remarkable presence in the market. Over the years, Qualys has put more efforts to strengthen its cloud security portfolio and expand its business. Its workload security solution delivers unified visibility, vulnerability management, and runtime threat detection for VMs, containers, and cloud instances across hybrid and multicloud environments. Integrated into the Qualys TotalCloud platform, it offers APA, image scanning, CDR, and runtime behavioral monitoring, allowing organizations to prioritize and remediate risks across the workload lifecycle with minimal agent overhead.
- Trend Micro's cloud security business maintains a solid growth of double digits over the last four years, becoming one of the fastest-growing segments in its entire business portfolios. Its Cloud One platform usage has grown significantly, with the number of customers reaching the thousands. Its workload security solution has been popular among organizations for its runtime protection for VMs, containers, and serverless functions across hybrid and multicloud environments with strong integration with IPS, app control, FIM, log inspection, and risk-based vulnerability protection.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Fortinet's workload security business (through the acquisition of Lacework) has gone through a transformation as the cloud security business portfolio is now tightly integrated with its SASE business pillar. However, the sales strategy transition has taken time, with its cloud business exhibiting some stagnancy. Technology wise, Fortinet provides a solid workload security solution, using both agentless and agent-based monitoring across containers, VMs, and serverless workloads. Fortinet has unified workload protection into its broader FortiCNAPP offering, delivering runtime visibility, posture management, and threat detection in a single, cloud-native framework.
- QAX continues to evolve its workload security capabilities using big data and AI-powered runtime analytics, mainly to cater to the Chinese government and critical infrastructure industry. Its platform integrates runtime behavior detection with compliance automation. In China, QAX is emerging as a strong hybrid CWPP performer.
- Uptycs has seen an uptick in revenue in 2025 following a slow 2024, leveraging its reputation as a unified CNAPP/XDR player, which boosts its popularity among large, tech-savvy enterprises and medium-sized companies that prefer a unified cloud security platform. Uptycs has enhanced its cloud workload security with a slew of innovations, focusing on breach mitigation, agentless discovery, runtime behavior detection, remediation, root-cause code tracing, and CI/CD and workload hardening, risk prioritization, and threat response by contextualizing runtime telemetry using eBPF.
- Trellix offers a strong CWPP solution to protect virtual instances and cloud workloads across multiple public and private clouds from advanced threats, with capabilities such as application control, micro-segmentation, and malware protection, and integration with its XDR, managed through a centralized console for better visibility and control. However, Trellix has struggled to grow its CWPP business and has lost significant market share over the years. The lack of recent exciting innovation for its cloud security solution makes it a less attractive option relative to competitors.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Companies to Action

Source: Frost & Sullivan

Palo Alto Networks

INNOVATION

- Palo Alto Networks is evolving Prisma Cloud into Cortex Cloud, consolidating all CNAPP capabilities, including CWPP, CSPM, CDR, and other specialized security posture modules across identity (CIEM), data (DSPM/DDR), AppSec (SAST, IaC, SCA, and SBOM), AI-SPM, and CI/ CD pipeline into a single, integrated platform.
- Its CWPP solution supports Linux and Windows hosts, offering extensive security capabilities to protect modern cloud environments with robust features such as vulnerability assessment, compliance checks, access control, FIM, app control, WAAP, and network visualization. It can seamlessly integrate with existing DevOps and SecOps workflows to enable shift-left security for comprehensive protection for VMs, containers, K8s, and serverless functions running on both public and private clouds.
- By using an agent that supports kernel and eBPF modes, Cortex Cloud's CWPP stands out for its runtime protection capabilities, delivering comprehensive and real-time protection across multiple network layers (L3/L4/L7) and detailed contextual analysis of vulnerabilities and risks, enabling SOC teams to improve their remediation and response capabilities.
- Cortex Cloud can be tailored for different executives and operational teams for better collaboration, risk visibility, and faster TDR. Leveraging AI/ML, Cortex Cloud can contextualize security information across domains and translate them into actionable insights, aggregating security alerts into clearly defined "cases" that pinpoint actions to significantly reduce risk and enhance workflows for rapid remediation. The bidirectional tracking capability, from risk management to runtime protection to SOC operations, enables a more seamless and effective security operation lifecycle, reflecting its huge shift to align with the industry trends toward real-time threat detection, AI-driven automation, and rapid response.

Source: Frost & Sullivan

Palo Alto Networks (continued)

GROWTH

- Palo AIto Networks has established itself as the leading CNAPP player, bolstered by its robust cloud workload security module that has experienced accelerated growth from 2023 to 2025, solidifying the company's position as one of the largest pure-play cloud security vendors in the market.
- The company leverages its broad enterprise customer base and established network security dominance to cross-sell its cloud security solutions across various verticals, including BFSI, technology, retail/eCommerce, telecommunications, and healthcare. It supports organizations with small to very large cloud deployments, emphasizing compliance, risk reduction, and holistic visibility across multicloud and hybrid environments.
- With a customer base from its network security, SASE, and security operations that forms a massive community of 320,000 users globally, Palo AIto Networks is in the prime position to maintain its growth momentum.
- Its strategy to rearchitect the cloud security platform to fit in SOC/SecOps environments will help Cortex Cloud to gain popularity among SecOps teams and increase its revenue growth. Its GTM aligns with the shift toward DevSecOps that requires embedding security across the development lifecycle with integrations into DevOps pipelines and K8s/container environments, which helps it address security and developer audiences.
- The company benefits from a robust ecosystem of more than 8,000 partners with security expertise, including channel partners, GSIs, and CSPs. The extensive network increases industry penetration and ensures the delivery of comprehensive service coverage, capacity, and capabilities to end users.

Source: Frost & Sullivan

Palo Alto Networks (continued)

FROST PERSPECTIVE

- Palo Alto Networks is a pioneer in the cloud security industry and an innovation trailblazer for its complete CNAPP features and capabilities that help organizations manage security risks and protect their cloud infrastructure, workloads, and applications throughout the application development, deployment, and runtime lifecycle.
- The company's transformational vision to evolve Prisma Cloud into Cortex Cloud platform is a milestone in its cloud security journey, extending security coverage from cloud and on-premises workloads all the way through development pipelines and to SOC to strengthen its cloud runtime security and cloud-native TDR across different cloud environments.
- Palo Alto Networks' CWPP is one of the most well-known cloud workload security solutions in the industry, offering a full set of capabilities for protecting cloud infrastructure, workloads, and applications throughout the application development, deployment, and runtime lifecycle. The tight integration with Cortex Cloud benefits the workload security portfolio because it can offer organizations granular attack-path analysis and risk context and automated correlation of security signals across various domains, helping teams protect diverse workloads, identify and analyze complex attack paths, and gain deeper insight into potential attack vectors and enabling more effective risk mitigation strategies.
- Nonetheless, integrating Cortex Cloud with other modules may create an impression that its solution is fragmented because it spans different products, particularly with the SecOps portfolios. It should continue to improve platform integration and further redefine the platform dashboard to make it more intuitive, unified, and user-friendly to enhance the experience for DevOps, cloud/AppSec, and SecOps teams.

Source: Frost & Sullivan

FROST & SULLIVAN

Best Practices & Growth Opportunities

Source: Frost & Sullivan

Best Practices

1. Organizations seek CWPP platforms that provide unified code-to-cloud posture controls, runtime protection, and real-time TDR and across diverse cloud environments. Modern CWPP solutions must combine deep runtime visibility (via eBPF telemetry or CDR) with risk insights into a single, prioritized risk view, enabling security teams to detect and respond to advanced threats while managing cloud risks effectively.

2. Manual triage is no longer viable at cloud scale. Organizations demand CWPP solutions powered by agentic AI, real-time drift/vulnerability detection, and automated remediation. These capabilities reduce alert fatigue by contextualizing threats, prioritizing the most critical risks, and providing guided remediation workflows. This can be delivered through GenAI/AI assistants that can help trace runtime alerts back to root causes, recommend actions, and carry out remediation to cut MTTR significantly.

3. Tool sprawl and fragmented risk views remain major obstacles in security operations. Organizations are advised to consolidate CWPP into broader CNAPP/CNADR platforms that unify and correlate insights from other solutions to gain comprehensive visibility into risks and threats across the cloud stack. This convergence provides a single source of truth for cloud risk and threats, reduces operational overhead, and empowers SOC and SecOps teams to investigate threats with full attack-path context.

Source: Frost & Sullivan

Growth Opportunities

1. Vendors can capitalize on the demand for hybrid and multicloud runtime protection by extending CWPP capabilities beyond public cloud to private cloud and on-premises workloads. As organizations adopt hybrid strategies for compliance, sovereignty, and resilience, they require unified workload visibility and consistent runtime TDR across all environments. Vendors that deliver seamless protection coverage across these environments can differentiate themselves and gain more influence.

2. Bringing agentic AI, automated remediation and TDR into day-to-day SecOps can be a differentiator for vendors. Organizations need platforms that don't just detect but are able to correlate runtime signals with posture and identity context, understand alert context and prioritize them, generate guided fix/remediation, and respond to threats. Embedding AI into cloud security platforms and enhancing integration with SOC workflows can help vendors gain a competitive edge.

3. Safe adoption of AI/ML workloads is creating demand for AI security. Cloud security vendors can stand out by combining code-to-cloud controls with runtime protection with models and data risk detection, scanning of AI pipelines, and policy enforcement using policy-as-code before deployment. Combined with AI runtime threat detection, drift control, and least-privilege enforcement, it can deliver a smarter and unified approach to early risk management and threat response for all AI workloads and applications.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Analytics

Source: Frost & Sullivan

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 Mega Trends) 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

MEGA TRENDS 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 Mega Trends 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

Source: Frost & Sullivan

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 Rada™ 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

Engage:

Growth Dialog

Join:

Growth Council

Participate:

Growth Council Think Tanks

Apply:

Companies to Action

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

Source: Frost & Sullivan