Cloud-Native Application Protection Platform (CNAPP)

Market Guide

Volume 1, 2025

TABLE OF CONTENTS

METHODOLOGY

To produce a comprehensive and reliable analysis of the Cloud-Native Application Protection Platform (CNAPP) ecosystem for 2025, ISMG leveraged a proprietary, AI-powered methodology combining automation, structured data modeling, and editorial oversight. This edition, finalized as of October 1, 2025, incorporates advanced validation techniques to mitigate hallucinations in large language model (LLM) outputs, ensuring profiles are factually grounded and aligned with CNAPP-specific market dynamics.

AI-POWERED CNAPP VENDOR INTELLIGENCE

At the core of our methodology is ISMG's Apollo AI workflow engine, which gathers, structures, and analyzes CNAPP vendor data from diverse sources—including product pages, security blogs, analyst reports, investor filings, and regulatory disclosures. Vendor information is normalized to support consistent cross-comparisons, regardless of vendor size, region, or messaging sophistication.

GROUNDING IN VERIFIED DATA REPOSITORIES

Every output is anchored to trusted, validated sources. No speculative content or unverifiable assertions are permitted in the final vendor write-ups.

SUMMARIZATION FOR PRINT AND WEB

Vendor profiles are condensed for the print version of this guide while preserving core insights related to technical scope, integrations, and market fit.

SCOPE AND UPDATE TIMELINE

This guide reflects the state of the CNAPP market as of October 1, 2025, with vendor profiles selected based on relevance to major CNAPP categories including:

- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)
- Kubernetes Security Posture Management (KSPM)
- Cloud Infrastructure Entitlement Management (CIEM)
- Infrastructure as Code (IaC) Scanning
- Runtime Threat Detection
- Agentless and Hybrid Deployments

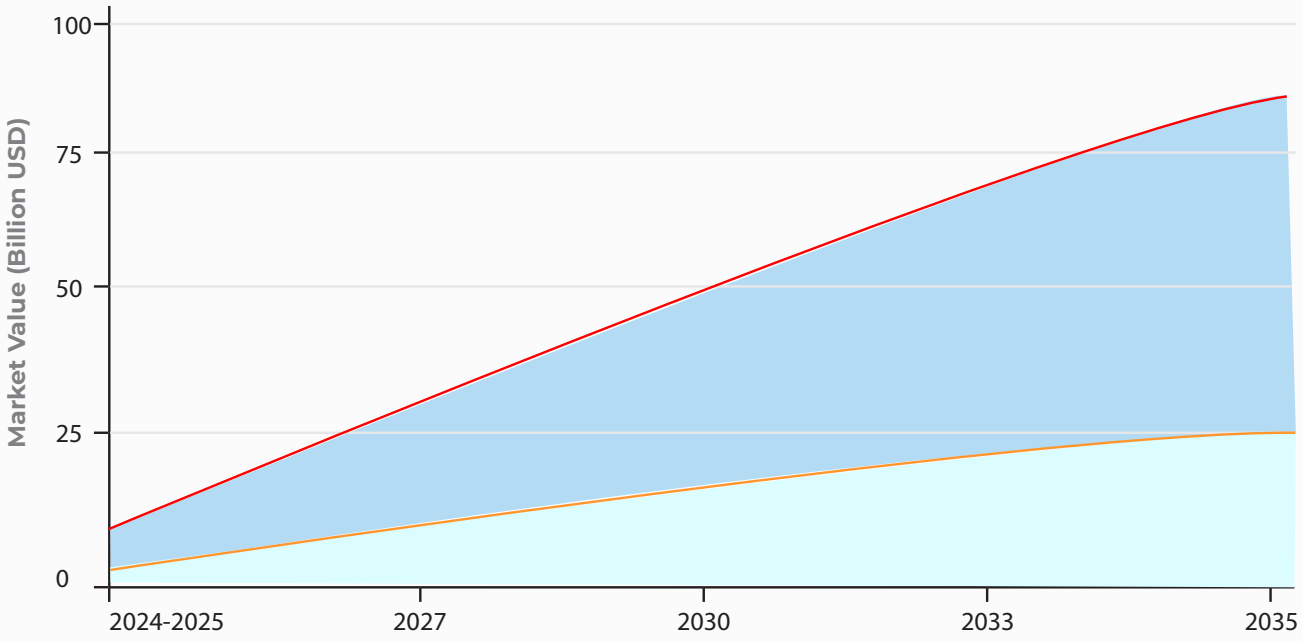
CNAPP VENDOR DIRECTORY (OCTOBER 2025 EDITION)

Comprehensive analysis of 19 leading cloud-native application protection platform (CNAPP) vendors categorized by deployment complexity and coverage breadth.

MARKET MOMENTUM: BEYOND THE HYPE CYCLE

The CNAPP market is experiencing explosive growth, with current valuations ranging between $3.4 and $10.69 billion and projections reaching $38 to $88 billion by 2030-2035. All research converges on 20% to 35% CAGR growth, positioning CNAPP among the fastest-growing cybersecurity segments. The U.S. market alone demonstrates this trajectory: $2.4 billion in 2024, accelerating to $17.5 billion by 2035 at a CAGR of 19.8%. This isn't incremental expansion - it's fundamental restructuring of enterprise cloud security.

Global CNAPP Market Forecast Range



Shaded area represents the range of market f orecasts from multiple research sources

THE PERFECT STORM DRIVING ADOPTION

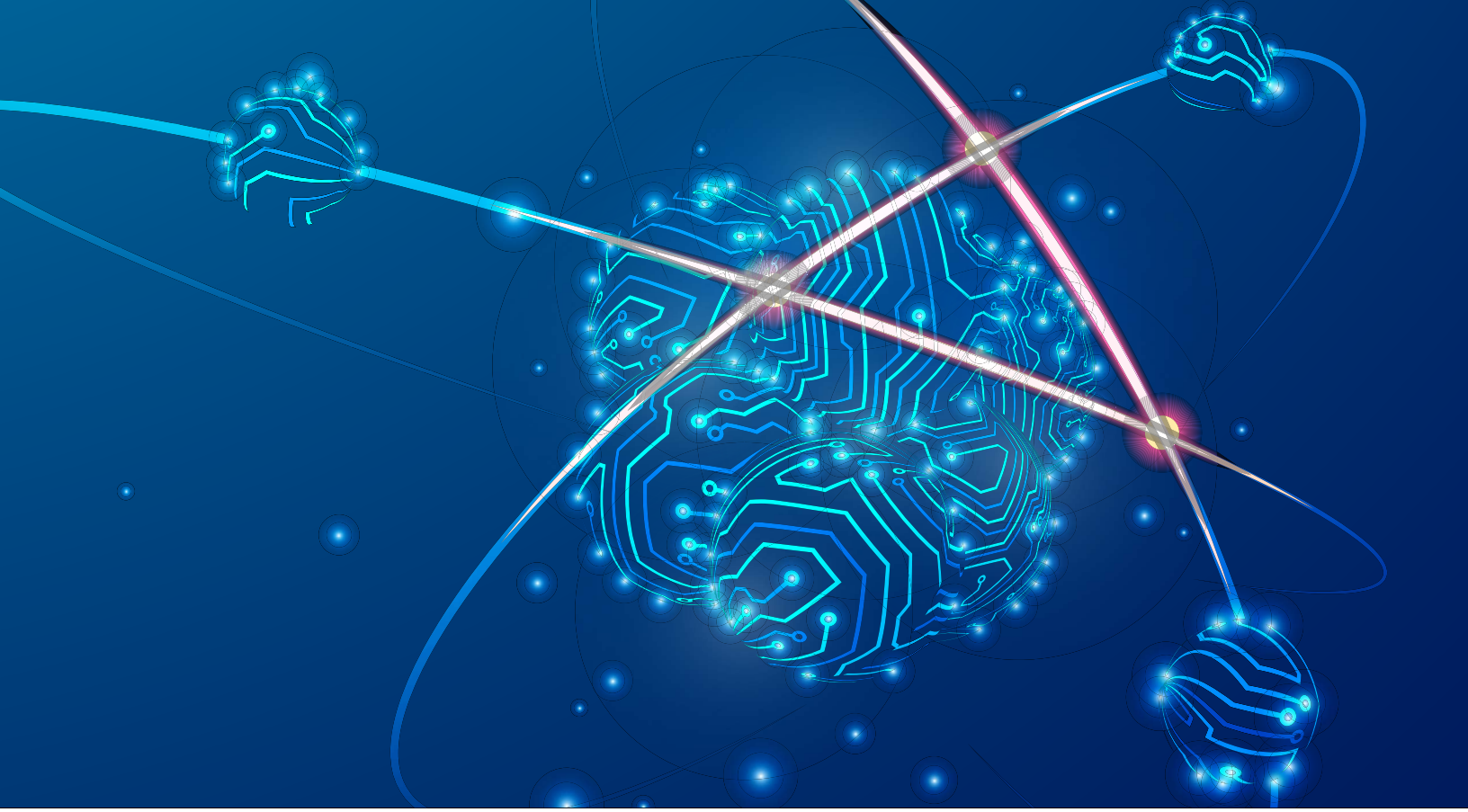
Tool consolidation has become a strategic imperative. Security leaders are abandoning fragmented CSPM, cloud workload protection platform (CWPP), CIEM and IaC scanning tools that create alert fatigue and visibility gaps. CNAPPs promise holistic risk visibility through unified platforms.

Cloud-native architectures are outpacing traditional security. Containerization, microservices, serverless and multi-cloud deployments have evolved faster than security tooling. CNAPPs provide development-to-runtime visibility that legacy perimeter-based tools cannot deliver.

Regulatory mandates demand continuous compliance. GDPR, HIPAA, PCI DSS and SOC 2 requirements have shifted from quarterly audits to continuous monitoring. CNAPPs automate compliance checking across more than 30 frameworks, transforming regulatory burden into automated workflows.

DevSecOps integration is non-negotiable. The "shift-left" movement demands security embedded in CI/CD pipelines without breaking developer velocity. For organizations practicing continuous deployment, this capability is table stakes.

The threat landscape has moved to the cloud. Attackers now target misconfigurations, identity compromise, supply chain attacks and runtime exploitation. CNAPPs provide contextual risk analysis across these surfaces that siloed tools miss by design.



TECHNOLOGY EVOLUTION: FROM DETECTION TO PREVENTION

AI integration has become mandatory. CNAPPs now embed generative AI for alert summarization, remediation guidance, attack path analysis and automated policy generation. Vendors without mature AI capabilities face existential competitive pressure.

Runtime protection supplants static scanning. The market is pivoting from agentless-only approaches toward runtime-powered solutions offering real-time threat detection and inline protection. Buyers increasingly demand proactive mitigation rather than reactive alerting.

Zero trust convergence is accelerating. By 2029, 40% of enterprises implementing zero trust in cloud environments will rely on CNAPP solutions, positioning CNAPPs as foundational infrastructure rather than point tools.

XDR integration creates unified response. CNAPP-XDR convergence enables unified threat detection across cloud, endpoint and network environments, accelerating incident response through comprehensive attack context.

MARKET SEGMENTATION: WHO'S BUYING

Large enterprises dominate CNAPP adoption due to complex multi-cloud environments, but SME adoption accelerates at the highest CAGR as cloud-native architectures become mainstream. Solutions represent over 70% of market revenue and will exceed $35 billion by 2034, but services are growing faster at 15.8% CAGR as organizations struggle to operationalize platforms amid cybersecurity skills gaps.

Hybrid cloud environments show the highest growth potential, requiring consistent security governance across on-premises and multiple cloud infrastructures. SaaS deployments lead at 15.7% CAGR, reflecting buyer preference for reduced operational overhead.

North America maintains largest CNAPP market share in 2025. Asia-Pacific demonstrates strongest growth at 16% CAGR through 2030, fueled by data sovereignty regulations and government-backed cloud initiatives. The European CNAPP market is also expanding substantially, driven by GDPR compliance, particularly in banking, healthcare and government.

The healthcare sector posts growth at 15.4% CAGR, driven by electronic health record migration and patient data protection requirements. Financial services shows high adoption due to regulatory mandates and sophisticated threat landscapes. Manufacturing and government sector adoption is increasing as digital transformation collides with strict security requirements.

MARKET CONSOLIDATION: THE LAND GRAB

- **Google's $32 billion Wiz acquisition** - the largest cybersecurity acquisition in history - instantly positioned Google Cloud as a credible enterprise security platform. Google stated it couldn't build equivalent capability fast enough.
- **Palo Alto Networks' $25 billion CyberArk acquisition** combines privileged access management with CNAPP, creating comprehensive identity-to-workload security. This reflects strategy of building integrated platforms rather than best-of-breed components.
- **Orca Security's Opus acquisition** focuses on agentic AI-driven automation and remediation, signaling market movement beyond detection toward autonomous response.

These acquisitions demonstrate that technology giants are buying rather than building CNAPP capabilities. As consolidation creates competitive pressure on independent vendors while validating the category's strategic importance, expect intensified M&A activity ahead.

PERSISTENT BARRIERS

The shortage of skilled cybersecurity professionals - particularly those with cloud-native expertise - limits market expansion. Organizations deploy CNAPP platforms but struggle to configure and operationalize them effectively, driving faster growth in managed services.

Integration complexity persists despite consolidation goals. Many organizations operate fragmented security tool environments, making CNAPP integration complex and potentially duplicative.

Multi-cloud management remains challenging. No vendor has achieved true parity across AWS, Azure and GCP, forcing buyers into uncomfortable compromises on cloud-agnostic capabilities.

BOTTOM LINE

CNAPP represents the most significant evolution in cloud security - consolidating fragmented point solutions into unified platforms addressing the full spectrum of cloud-native challenges. Organizations adopting comprehensive CNAPP strategies now will be positioned for the cloud-first future. Those delaying face compounding risk: deteriorating security posture, operational inefficiency and competitive disadvantage.

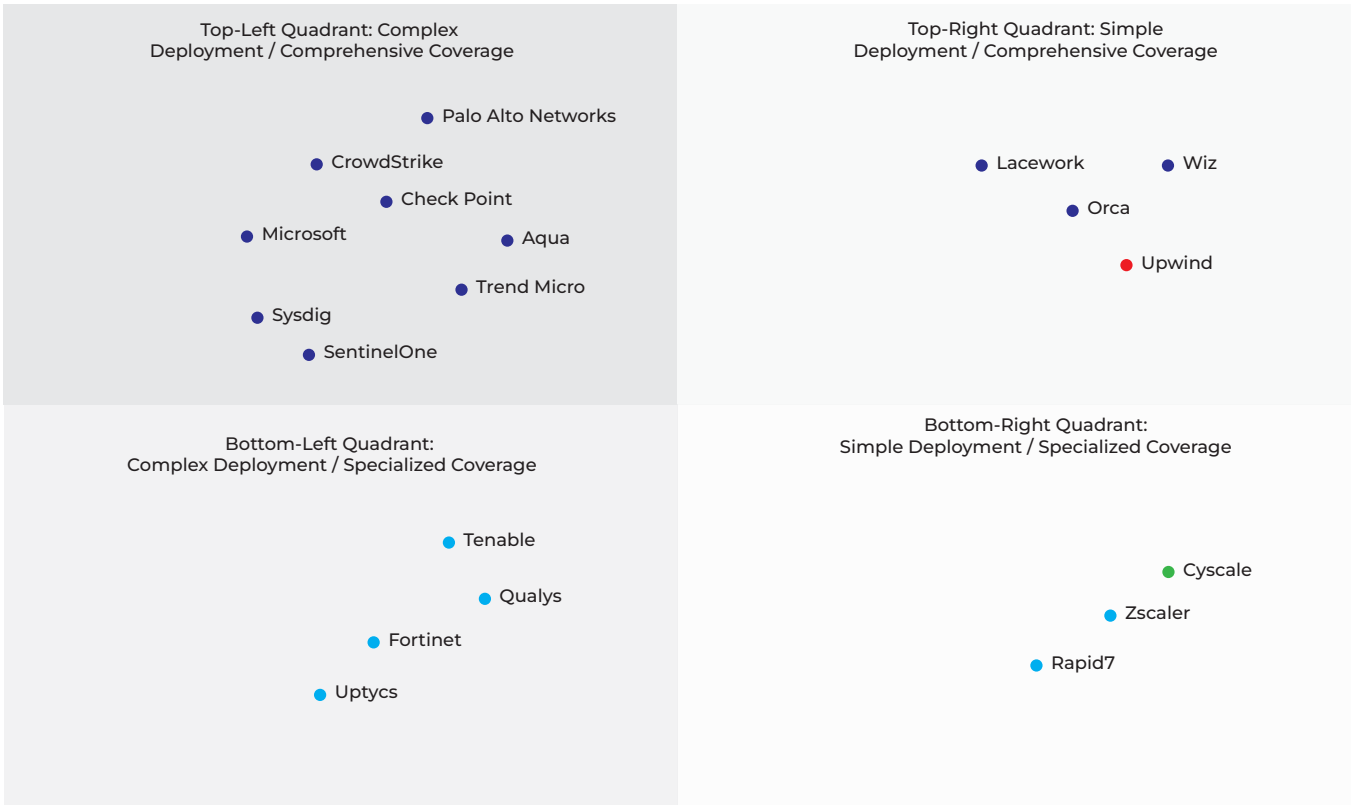
The question is no longer whether to adopt CNAPP, but which vendor strategy aligns with your organization's cloud trajectory and risk tolerance. This decision will define your security architecture for the next decade.

CNAPP VENDOR LANDSCAPE AND PROFILES (2025)

The CNAPP market in 2025 features a mix of established cybersecurity vendors, cloud platform providers and innovative startups. Notably, many large vendors have expanded their cloud security portfolios via acquisitions and development to offer full CNAPP suites, while several newer companies pioneered agentless cloud-native security and have grown explosively.

CNAPP Vendor Market Positioning

Strategic positioning by deployment complexity and coverage breadth



Vendor Categories

- Full CNAPP Suite (12 vendors)
- Specialized CNAPP (6 vendors)
- Regional (1 vendor)
- Emerging (1 vendor)

Architecture Types

- **Agentless:** API-based scanning, no performance impact
- **Agent-based:** Runtime protection with deployed agents
- **Hybrid:** Combined agentless + agent capabilities

Market Focus

- **Enterprise:** Large organizations, complex requirements
- **Mid-Market**: Growing companies, moderate complexity
- **SMB:** Small businesses, simplified deployment

Note: This chart is derived from AI analysis of deep research and full vendor profiles built using public vendor data.

TOP-RIGHT QUADRANT: SIMPLE DEPLOYMENT + COMPREHENSIVE COVERAGE

This quadrant features next-generation CNAPP innovators combining ease of deployment with full-spectrum protection. These vendors embody the shift toward agentless or lightweight architectures that deliver comprehensive visibility, risk prioritization and compliance with minimal operational overhead.

VENDOR PROFILES

WIZ (Full CNAPP, Now Part of Google Cloud)

WHAT IT IS

Wiz is an agentless, API-driven CNAPP that provides broad visibility and contextual risk assessment across multi-cloud environments. Founded in 2020 and acquired by Google Cloud in 2025 for $32 billion, it delivers comprehensive coverage without deploying agents.

CORE COVERAGE

- **CSPM:** Continuous monitoring for misconfigurations, excessive permissions and policy violations;
- **CWPP (agentless):** Vulnerability/ malware scanning of virtual machine and container snapshots;
- **Identity and secrets:** Analysis of over-privileged identities and exposure of secrets across clouds;
- **AppSec integrations:** Expands into code/pipeline scanning to help developers fix issues earlier.

WHAT MAKES IT DIFFERENT

- **Agentless by design:** Pure API connections enable rapid, low-friction deployment and scale;
- **Security graph:** Correlates assets, configurations, identities and exposures to map attack paths and prioritize exploitable risk;
- **Intuitive UX and fast time-to-value:** Visual, context-rich interface that's operational within hours.

BEST FIT

- Cloud-first and DevOps-driven organizations needing broad coverage with minimal operational overhead;
- Multi-cloud enterprises seeking unified visibility and prioritized remediation across AWS, Azure, GCP and Oracle Cloud;
- Teams that want to embed risk insights into CI/CD for shift-left remediation.

CAVEAT

Wiz's agentless model emphasizes rapid visibility and prioritization; organizations requiring real-time runtime containment often pair it with agent-based tools.

ORCA SECURITY (FULL CNAPP)

WHAT IT IS

Orca Security is an agentless CNAPP that uses its patented SideScanning™ technology to provide full visibility into multi-cloud environments without installing agents. The SaaS platform delivers comprehensive CSPM, CWPP, vulnerability management and IAM risk analysis with near-zero operational overhead.

CORE COVERAGE

- **CSPM:** Continuous posture assessment across AWS, Azure and GCP;
- **CWPP:** Snapshot-based vulnerability scanning of workloads and containers;
- I**AM and data security:** Contextual analysis of identity risk and sensitive data exposure;
- **Compliance:** Pre-built frameworks and continuous monitoring for standards such as PCI DSS and ISO 27001.

WHAT MAKES IT DIFFERENT

- **SideScanning™ technology:** Reads snapshots via cloud APIs for visibility, now complemented by agentless runtime detection capabilities that identify active threats without workload agents.
- **Contextual risk correlation:** Identifies "toxic combinations" of misconfigurations, vulnerabilities and access exposures;
- **Agentless simplicity:** Deploys in minutes through API connections, providing comprehensive visibility with minimal effort.

BEST FIT

- Enterprises seeking fast, full coverage across multiple clouds without agent management;
- Security teams that prioritize risk-based correlation over raw alert volume;
- Organizations extending posture management into vulnerability and identity risk domains.

CAVEAT

Orca focuses on agentless visibility and contextual prioritization; teams needing deep runtime protection or active defense typically pair it with agent-based solutions. Orca's CNAPP now includes DSPM and CIEM modules, broadening its coverage beyond posture and vulnerabilities.

LACEWORK (FULL CNAPP - HYBRID BEHAVIORAL ANALYTICS)

WHAT IT IS

Lacework is a data-driven CNAPP that unifies CSPM, CWPP and anomaly detection through its Polygraph® behavioral analytics engine. The SaaS platform learns relationships among workloads, users and configurations to establish a behavioral baseline and detect subtle anomalies across multi-cloud and Kubernetes environments.

CORE COVERAGE

- **CSPM:** Continuous configuration and compliance monitoring across AWS, Azure and GCP;
- **CWPP:** Runtime monitoring for workloads and containers with vulnerability and threat detection;
- **Behavioral analytics:** Polygraph® maps relationships between users, workloads and data flows to identify abnormal activity;
- **Kubernetes and container security:** Visibility into clusters, images and orchestrator-level events;
- **Compliance and IaC scanning:** Prebuilt policy checks and integrations with Terraform and other IaC tools.

WHAT MAKES IT DIFFERENT

- **Polygraph® technology:** Learns and models normal behavior to detect insider threats and novel attack paths;
- **Anomaly-first detection**: Focuses on deviations from baseline rather than static rule sets, minimizing false positives;
- **Automation and scalability:** Adapts to dynamic, ephemeral workloads common in modern DevOps environments.

BEST FIT

- Cloud-native and DevOps-driven organizations managing fast-changing environments;
- SaaS and technology companies using microservices or serverless architectures;
- Security teams seeking behavioral anomaly detection with minimal rule tuning.

CAVEAT

While Lacework provides exceptional behavioral depth, its policy and network control features are narrower than those of larger CNAPP suites.

UPWIND (EMERGING CNAPP - RUNTIME-POWERED)

upwind

WHAT IT IS

Upwind is a next-generation CNAPP that prioritizes runtime intelligence to correlate live workload activity with configuration and vulnerability data. Founded in 2022, it bridges posture management and real-time threat detection through a hybrid architecture using both agentless connections and lightweight runtime sensors.

CORE COVERAGE

- **Runtime-powered visibility:** Correlates real-time telemetry with configuration and IAM data to expose exploitable risks;
- **CSPM:** Continuous, context-aware misconfiguration detection across AWS, Azure and GCP;
- **CWPP:** Behavioral analysis of workloads, containers and Kubernetes clusters for privilege escalation or lateral movement;
- **AI-driven remediation:** Suggests or automates fixes for misconfigurations and vulnerabilities;
- **Compliance:** Maps risks to frameworks such as NIST, CIS and MITRE ATT&CK.

WHAT MAKES IT DIFFERENT

- **Runtime-first design:** Prioritizes real, observed threats over theoretical vulnerabilities;
- **Contextual correlation:** Merges configuration, identity and runtime data into unified, prioritized insights;
- **Balanced deployment:** Combines agentless speed with optional sensors for deeper runtime fidelity;
- **AI-assisted response:** Automates remediation and containment workflows for faster mitigation;

BEST FIT

- Cloud-native enterprises and DevSecOps teams that value signal over noise;
- Organizations seeking runtime-informed prioritization with minimal manual tuning;
- Mid-sized teams wanting full coverage without the burden of complex integrations.

CAVEAT

While emerging and highly innovative, Upwind's hybrid model still requires limited runtime component deployment - less friction than traditional CNAPPs, but not fully agentless.

TOP-LEFT QUADRANT: COMPLEX DEPLOYMENT + COMPREHENSIVE COVERAGE

Vendors in this quadrant are enterprise powerhouses offering deep, feature-rich CNAPP platforms. They trade deployment simplicity for unmatched coverage across posture, workload, identity and runtime protection - best suited for organizations with mature SecOps and integration capacity.

PALO ALTO NETWORKS - PRISMA CLOUD (FULL CNAPP - ENTERPRISE POWERHOUSE)

WHAT IT IS

Prisma Cloud is Palo Alto Networks' flagship CNAPP, securing applications "from code to cloud." It integrates CSPM, CWPP, CIEM, IaC scanning and container/Kubernetes security into a single platform, offering one of the most mature and feature-rich CNAPP suites available.

CORE COVERAGE

- **CSPM and CIEM:** Continuous posture assessment, identity analysis and compliance monitoring across AWS, Azure and GCP;
- **CWPP:** Runtime protection for workloads and containers using agentless and agent-based sensors;
- **IaC and DevSecOps:** Scans Terraform, GitHub, GitLab and Jenkins pipelines for early vulnerability detection;
- **Threat intelligence:** Leverages Palo Alto's Unit 42 and Cortex AI for global threat correlation;
- **Cortex Cloud (2025 update):** Integrates CNAPP with cloud detection and response (CDR)/XDR for automated, AI-driven prevention.

WHAT MAKES IT DIFFERENT

- **Breadth and depth:** True full-stack coverage - CSPM, CWPP and code security under one console;
- **AI-powered threat correlation:** Uses Cortex AI to unify insights from endpoints, networks and workloads;
- **Enterprise ecosystem integration:** Tight interoperability with Palo Alto's firewalls, Cortex XDR and SASE products;
- **Deployment flexibility:** Offers SaaS, hybrid and customer-managed components for regulated environments.

BEST FIT

- Large enterprises with complex, multi-cloud infrastructures;
- Regulated industries needing compliance automation (GDPR, HIPAA, PCI DSS and FedRAMP);
- Organizations with mature SecOps teams capable of managing a comprehensive platform.

CAVEAT

Prisma Cloud's unmatched coverage comes with deployment complexity and configuration overhead - best suited for enterprises ready to invest in deep integration and skilled operation.

CROWDSTRIKE - FALCON CLOUD SECURITY (FULL CNAPP - XDR-INTEGRATED)

WHAT IT IS

Falcon Cloud Security extends CrowdStrike's Falcon platform from endpoint protection into full CNAPP coverage, merging CSPM, CWPP and XDR under one architecture. It unifies threat detection and response across cloud workloads, containers and endpoints through shared telemetry and advanced behavioral analytics.

CORE COVERAGE

- **CWPP:** Real-time runtime protection for virtual machines, containers and Kubernetes clusters via the lightweight Falcon agent;
- **CSPM:** Continuous cloud configuration and compliance monitoring across AWS, Azure and GCP;
- **XDR integration:** Correlates data from endpoints, identities and networks for cross-domain threat detection;
- **Vulnerability and threat assessment:** Prioritizes remediation using real-time threat intelligence;
- **DevSecOps integration:** Hooks into CI/CD pipelines for early misconfiguration and vulnerability detection.

WHAT MAKES IT DIFFERENT

- **XDR-led CNAPP strategy:** Extends endpoint telemetry into the cloud for unified detection and response;
- **Single agent design:** Uses the same Falcon agent for endpoint and workload protection, simplifying management;
- **Real-time threat intelligence:** Backed by CrowdStrike's global graph analyzing trillions of events daily;
- **Low dwell time:** Advanced behavioral analytics detect and contain threats quickly;
- **Seamless ecosystem integration:** Works natively with Falcon Identity Protection, Falcon LogScale and Falcon Fusion SOAR.

BEST FIT

- Existing CrowdStrike customers seeking to extend Falcon protection to cloud workloads;
- Enterprises prioritizing real-time detection, response speed and integrated operations;
- Hybrid and multi-cloud organizations that need unified visibility across domains.

CAVEAT

While strong in runtime detection and XDR correlation, Falcon Cloud Security's CSPM depth is lighter than agentless-first CNAPPs like Wiz or Orca.

CHECK POINT CLOUDGUARD (FULL CNAPP - NETWORK-INTEGRATED)

WHAT IT IS

Check Point CloudGuard extends the company's trusted network security into cloud-native protection, delivering a full CNAPP suite that unifies CSPM, CWPP and DevSecOps security with enterprise-grade cloud network protection. It combines Check Point's threat prevention, firewall and intrusion detection expertise with cloud visibility and compliance monitoring.

CORE COVERAGE

- **CSPM and CWPP:** Continuous posture assessment, vulnerability detection and compliance validation across AWS, Azure and GCP;
- **Cloud network security:** Virtual firewalls and gateway defenses prevent lateral movement and external attacks;
- **Threat prevention:** Uses Check Point's ThreatCloud AI for real-time malware, intrusion and exploit blocking;
- **DevSecOps integration:** Embeds security in CI/CD pipelines with Terraform, Jenkins and GitHub scanning;
- **Compliance management:** Automated checks for PCI DSS, ISO 27001 and GDPR.

WHAT MAKES IT DIFFERENT

- **Network + CNAPP fusion:** Combines workload and network-layer defenses in a single ecosystem;
- **Infinity architecture synergy:** Shares policy and telemetry with Check Point's broader network and endpoint stack;
- **ThreatCloud intelligence:** Enriched with real-time global indicators for proactive defense.
- **Zero trust segmentation:** Enables microsegmentation across hybrid and multi-cloud environments;
- **Strategic Wiz partnership (2025):** Merges agentless visibility with CloudGuard’s prevention stack — not an acquisition but a technology collaboration.

BEST FIT

- Enterprises with hybrid infrastructures and existing Check Point deployments;
- Regulated industries needing high-assurance compliance and unified network/cloud governance;
- Security teams wanting policy consistency from data center to cloud.

CAVEAT

CloudGuard's multi-component architecture requires careful integration for gaining full value - optimal for organizations already invested in Check Point's ecosystem.

MICROSOFT DEFENDER FOR CLOUD (FULL CNAPP - AZURE-CENTRIC)

WHAT IT IS

Microsoft Defender for Cloud is a comprehensive CNAPP integrating CSPM, CWPP and hybrid protection within the Azure ecosystem. Evolving from Azure Security Center, it provides unified visibility and threat protection across Azure, AWS, GCP and on-premises environments. Deeply tied to Microsoft Defender XDR, Sentinel and Entra ID, it delivers seamless multi-domain defense and compliance automation.

CORE COVERAGE

- **CSPM:** Continuous configuration assessment and compliance monitoring across clouds and on-premises systems;
- **CWPP:** Vulnerability scanning, just-in-time VM access and advanced workload defense;
- **Threat detection:** Machine learning and global Microsoft threat intelligence detect privilege escalation, injection and lateral movement;
- **Compliance management:** Built-in frameworks for PCI DSS, ISO 27001, NIST and CIS with Azure Policy integration;
- **Hybrid coverage:** Azure Arc extends Defender's capabilities to AWS and GCP for consistent policy and posture management.

WHAT MAKES IT DIFFERENT

- **Deep Azure integration:** Unified visibility and automated compliance through Azure Policy, Arc and Resource Manager;
- **Native Microsoft ecosystem synergy:** Works seamlessly with Sentinel, Defender XDR and Intune;
- **Machine learning analytics:** AI-driven detections across cloud and on-premises layers;
- **Built-in compliance templates:** Reduces time-to-audit with preconfigured regulatory mappings;
- **Enterprise scalability:** Backed by Azure's global cloud infrastructure for performance and data sovereignty.

BEST FIT

- **Azure-first enterprises** seeking tight platform integration;
- Organizations operating **hybrid or multi-cloud** environments needing centralized management;
- **Regulated sectors** requiring continuous compliance and automation.

CAVEAT

Best suited for Microsoft-centric organizations.
Multi-cloud users may face added complexity managing non-Azure integrations.

AQUA SECURITY - AQUA PLATFORM (FULL CNAPP - CONTAINER- AND KUBERNETES-FOCUSED)

WHAT IT IS

Aqua Security's Aqua Platform evolved from a container security pioneer into a full CNAPP, delivering end-to-end protection for containers, Kubernetes and cloud workloads across the software development life cycle. It unifies developer pipeline security, posture management and runtime defense for containers, virtual machines and serverless environments - available as SaaS or self-managed deployment.

CORE COVERAGE

- **Container and Kubernetes security:** Runtime defense against container escapes, privilege escalation and anomalous activity;
- **Developer pipeline protection:** Scans infrastructure-as-code (IaC) templates, container images and dependencies pre-deployment;
- **Image assurance and supply chain protection:** Enforces signed, trusted images to prevent tampering and supply chain risk;
- **CSPM:** Posture management across cloud accounts and Kubernetes clusters;
- **Runtime protection:** Monitors workloads in real time for integrity changes and unauthorized execution;
- **Secrets management:** Protects credentials and enforces least-privilege policies within containers.

WHAT MAKES IT DIFFERENT

- **Deep Kubernetes expertise:** Purpose-built controls provide granular runtime protection for containerized workloads;
- **Open-source leadership:** Creator of Trivy (vulnerability scanning) and Kube-bench (Kubernetes CIS compliance);
- **Flexible deployment:** Supports both SaaS and on-premises options for regulated industries;
- **Supply chain security:** Integrates scanning, artifact signing and image assurance across CI/CD pipelines;
- **Active DevSecOps ecosystem:** Native integrations with Jenkins, GitHub and GitLab streamline policy enforcement.

BEST FIT

- **Kubernetes-heavy enterprises** requiring deep runtime and container life cycle protection;
- **DevSecOps-driven organizations** embedding security early in CI/CD workflows;
- **Regulated sectors** needing robust compliance automation and data sovereignty options.

CAVEAT

While its runtime and container security depth is unmatched, Aqua's CSPM and CIEM functions are still maturing compared to generalist CNAPP peers.

TREND MICRO - TREND CLOUD ONE (FULL CNAPP - MODULAR ARCHITECTURE)

WHAT IT IS

Trend Cloud One is a modular CNAPP suite that delivers unified protection across workloads, containers, storage and configurations in hybrid and multi-cloud environments. Designed for scalability and flexibility, Cloud One lets organizations adopt modules incrementally, balancing operational simplicity with comprehensive runtime protection powered by Trend Micro's global threat intelligence.

CORE COVERAGE

- **Posture management (conformity):** Continuous multi-cloud visibility and compliance assessment;
- **Workload security:** Agent-based runtime protection for virtual machines, containers and hybrid workloads with anti-malware and intrusion prevention;
- **Container image scanning:** Detects vulnerabilities in container registries and CI/CD pipelines;
- **File storage security:** Scans cloud storage (e.g., S3 and Azure Blob) for malware and compliance violations;
- **Automation and DevOps integration:** Auto-protects new resources and integrates with Terraform, Jenkins and GitHub Actions;
- **Threat intelligence:** Backed by Trend Micro's global research network for proactive threat detection.

WHAT MAKES IT DIFFERENT

- **Modular adoption:** Organizations can roll out CNAPP capabilities in stages without losing integration;
- **Runtime prevention strength:** Deep workload protection combining anti-malware, IPS and behavioral analysis;
- **Automation-first design:** Automatically secures new assets as they deploy;
- **Global threat intelligence:** Real-time insight from Trend Micro's vast research network;
- **Hybrid coverage:** Equally effective for cloud, private and on-premises workloads.

BEST FIT

- **Enterprises and mid-market firms** with hybrid or multi-cloud operations;
- **Regulated industries** (e.g., finance, telecom and healthcare) needing compliance assurance;
- Teams pursuing **incremental CNAPP maturity** with modular rollouts and strong runtime defense.

CAVEAT

While modularity offers flexibility, managing multiple components adds deployment and maintenance complexity - optimal for teams with mature DevSecOps processes.

SYSDIG SECURE (FULL CNAPP - CONTAINER AND KUBERNETES EMPHASIS)

sysdig

WHAT IT IS

Sysdig provides a container-native CNAPP built around its open-source Falco runtime detection engine, offering deep visibility and protection for containerized and Kubernetes environments. It unifies CSPM, CWPP, runtime defense and compliance into a single SaaS platform, helping security and DevOps teams collaborate on real-time detection and response.

CORE COVERAGE

- **Runtime threat detection (Falco):** Monitors system calls and kernel-level behavior to detect anomalies, privilege escalation and container escapes;
- **CSPM:** Continuously evaluates configurations and compliance across AWS, Azure and GCP;
- **CWPP:** Scans images and hosts for vulnerabilities, isolates compromised workloads and enforces runtime controls;
- **Kubernetes and container security:** Deep visibility into cluster configurations, workloads and network activity;
- **Risk prioritization:** Correlates vulnerabilities, configurations and runtime telemetry for contextual risk scoring;
- **Forensics and incident response:** Captures detailed runtime data for replay and root-cause analysis.

WHAT MAKES IT DIFFERENT

- **Falco-powered runtime depth:** Cloud-native computing foundation (CNCF)-adopted, open-source runtime detection delivering unparalleled visibility;
- **Unified security and performance telemetry:** One agent captures data for both operational and security use cases;
- **Forensic replay capabilities:** Enables replay of captured system activity post-incident;
- **Open-source credibility:** Active contributor to CNCF projects like Falco, promoting transparency and innovation;
- **Runtime specialization:** Built specifically for detecting in-motion threats across containers and Kubernetes.

BEST FIT

- **Enterprises running containerized or Kubernetes workloads** in production;
- **DevOps-driven teams** uniting security and operations through shared telemetry;
- **Regulated industries** requiring real-time compliance and incident forensics.

CAVEAT

Sysdig Secure requires agent deployment and Kubernetes expertise, making it more complex than agentless CNAPPs - but unmatched for deep runtime observability and detection accuracy.

SENTINELONE - SINGULARITYTM CLOUD NATIVE SECURITY (FULL CNAPP - AI-NATIVE PLATFORM)

SentinelOne

WHAT IT IS

SingularityTM Cloud Native Security extends its AI-driven security platform into the CNAPP domain, unifying agentless CSPM, agent-based CWPP, CIEM and Kubernetes Security (KSPM) into a single, autonomous solution. Built on the same Singularity XDR architecture, it brings AI-driven exploit validation, threat detection and remediation across hybrid and multi-cloud environments.

CORE COVERAGE

- **CSPM:** Agentless visibility into AWS, Azure and GCP to detect misconfigurations and compliance drift;
- **CWPP:** Uses the SentinelOne agent for runtime defense, anomaly detection and exploit prevention;
- **Offensive security engine:** Simulates and validates attack paths via Verified Exploit Paths™ for prioritized remediation;
- **Purple AI assistant:** Conversational AI that summarizes incidents, explains alerts and guides response steps;
- **CIEM:** Detects excessive permissions and enforces least-privilege principles;
- **KSPM:** Scans and secures container clusters and nodes;
- **XDR integration:** Correlates cloud, endpoint and identity telemetry across the SingularityTM ecosystem.

WHAT MAKES IT DIFFERENT

- **Verified Exploit Paths™:** Distinguishes exploitable vulnerabilities from theoretical risks;
- **AI-first automation:** Purple AI accelerates triage and remediation through natural-language workflows;
- **XDR-unified defense:** Single data fabric correlating cloud, endpoint and identity telemetry;
- **Offensive-defense balance:** Proactively tests and validates cloud attack surfaces;
- **Autonomous remediation:** Automates configuration fixes and policy enforcement.

BEST FIT

- **Enterprises using SentinelOne XDR or EDR,** seeking unified endpoint and cloud protection;
- **Security teams focused on exploitability -** not static vulnerability counts;
- **Hybrid and multi-cloud organizations** prioritizing automation and AI-driven insights.

CAVEAT

Agent deployment adds complexity for runtime defense but delivers unmatched exploit validation and AI-assisted response for mature SecOps teams.

BOTTOM-RIGHT QUADRANT: SIMPLE DEPLOYMENT + SPECIALIZED COVERAGE

Vendors here deliver focused solutions designed for rapid deployment and ease of use. They emphasize simplicity and targeted coverage - ideal for mid-market and SMB organizations seeking immediate posture and compliance visibility without full CNAPP complexity.

RAPID7 - INSIGHTCLOUDSEC (SPECIALIZED CNAPP - POSTURE AND AUTOMATION FOCUS)

WHAT IT IS

Rapid7's InsightCloudSec is a cloud security posture and automation platform designed to provide unified visibility, risk assessment and compliance management across multi-cloud environments. Originally built from the acquisitions of DivvyCloud and Alcide, it integrates into the broader Rapid7 Insight Platform, offering seamless connectivity with Rapid7's SIEM (InsightIDR) and SOAR (InsightConnect) capabilities.

CORE COVERAGE

- **CSPM:** Continuous discovery and configuration analysis across AWS, Azure, GCP and Kubernetes;
- **Kubernetes Security (KSPM):** Inherited from Alcide, it provides network policy enforcement, runtime monitoring and audit visibility;
- **Automation bots:** Customizable bots automatically remediate common issues (e.g., open S3 buckets or misconfigurations);
- **Compliance and governance:** Out-of-the-box policy templates for standards like CIS, PCI DSS and GDPR;
- **Integration with the Insight Platform:** Unified with Rapid7's detection and automation tools (InsightIDR, InsightVM and InsightConnect).
- **Workload security:** Basic workload coverage focused on configuration rather than runtime defense.

WHAT MAKES IT DIFFERENT

- **Automation-first design:** Self-healing remediation via bots reduces manual workload;
- **Ease of use:** Streamlined SaaS deployment and intuitive dashboards for mid-market teams;
- **Unified ecosystem:** Natively integrates with Rapid7's SIEM and SOAR products for end-to-end visibility;
- **Multi-cloud scalability:** Single control plane across diverse environments;
- **Continuous compliance:** Automated policy enforcement and real-time drift detection.

BEST FIT

- **Mid-market enterprises** using Rapid7's Insight Platform;
- **Security teams prioritizing posture management** and automated remediation over runtime analysis;
- **Organizations seeking rapid deployment** and integration into existing detection and response workflows.

CAVEAT

Lacks full CWPP or deep runtime protection - best used for continuous posture, compliance and workflow automation rather than runtime threat defense.

ZSCALER POSTURE CONTROL (SPECIALIZED CNAPP - ZERO TRUST INTEGRATED)

WHAT IT IS

Zscaler Posture Control extends Zscaler's Zero Trust Exchange platform into the cloud security domain, offering a lightweight, agentless CNAPP focused on posture management, IaC scanning and compliance. It provides cloud visibility and risk prioritization by correlating cloud configuration data with identity and network telemetry already managed through Zscaler's platform.

CORE COVERAGE

- **CSPM:** Continuous assessment of cloud configurations across AWS, Azure and GCP;
- **IaC Scanning:** Identifies misconfigurations early in the development life cycle;
- **Identity context correlation:** Enriches cloud posture findings using identity and network data from Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA);
- **Compliance monitoring:** Maps misconfigurations to industry standards (e.g., CIS, NIST and ISO);
- **Unified dashboard:** Integrates with Zscaler's Zero Trust Exchange for centralized risk management.

WHAT MAKES IT DIFFERENT

- **Zero trust integration:** Leverages Zscaler's secure access and identity data for cloud posture insight;
- **Agentless architecture:** Simplifies deployment via cloud APIs - no workload agents needed;
- **Identity-aware posture management:** Correlates cloud misconfigurations with user and application context;
- **SaaS-native simplicity:** Fully cloud-delivered with minimal operational overhead;
- **Continuous compliance:** Real-time monitoring and auto-remediation recommendations.

BEST FIT

- **Enterprises already using Zscaler** for access and internet security;
- **Organizations adopting zero trust** looking to extend visibility into their cloud environments;
- **Teams seeking agentless posture and compliance management** without runtime complexity.

CAVEAT

Not a full CNAPP - limited runtime and workload protection. Best as a complementary posture tool for Zscaler customers - not a stand-alone runtime defense solution.

CYSCALE - CLOUD PLATFORM (SPECIALIZED CNAPP - SMB AND MID-MARKET FOCUS)

Cyscale

WHAT IT IS

Cyscale is a European cloud security platform that delivers a unified, agentless CNAPP for small and mid-sized businesses (SMBs) and mid-market enterprises. Headquartered in London, it provides comprehensive visibility, compliance monitoring and protection across multi-cloud and Kubernetes environments, focusing on ease of use and rapid deployment for teams without large security operations.

CORE COVERAGE

- **CSPM:** Continuous scanning for cloud misconfigurations, vulnerabilities and compliance violations;
- **KSPM:** Automated discovery and risk analysis for Kubernetes clusters and workloads;
- **CWPP:** Agentless workload visibility covering virtual machines, containers and serverless functions;
- **IAM and data security:** Analyzes permissions, roles and exposed assets to reduce privilege risk;
- **Compliance and reporting:** Automated assessments aligned to NIST, CIS and GDPR standards;
- **Real-time risk intelligence:** Prioritizes findings and provides actionable remediation guidance.

WHAT MAKES IT DIFFERENT

- **SMB-first design:** Built for smaller security teams needing enterprise-grade visibility without complexity;
- **Agentless simplicity:** Deploys via cloud APIs - no agents or infrastructure changes required;
- **Unified interface:** Consolidates CSPM, KSPM and CWPP into a single, intuitive dashboard;
- **Regulatory focus:** Emphasizes compliance automation and GDPR readiness;
- C**ontextual risk scoring:** Highlights issues by severity and business impact for faster remediation.

BEST FIT

- **SMBs and mid-market organizations** migrating to or expanding within the cloud;
- **Teams with limited security staff** seeking automation and simplicity;
- **Organizations requiring GDPR and NIST alignment** with minimal setup.

CAVEAT

Focused on accessibility and posture management rather than deep runtime protection or advanced workload analytics. Best for smaller teams prioritizing ease of deployment and compliance visibility.

BOTTOM-LEFT QUADRANT: COMPLEX DEPLOYMENT + SPECIALIZED COVERAGE

This quadrant includes established specialists extending their legacy strengths in vulnerability, exposure or network security into the cloud. These solutions offer valuable depth for specific use cases but require greater integration and management overhead.

TENABLE CLOUD SECURITY (TENABLE.CS) (SPECIALIZED CNAPP - EXPOSURE-CENTRIC APPROACH)

WHAT IT IS

Tenable Cloud Security (Tenable.cs) extends Tenable's well-established vulnerability management expertise into the cloud through acquisitions such as Accurics. It focuses on preventative and exposure-based security, offering unified visibility across infrastructure as code (IaC), workloads and configurations to help organizations understand and reduce total exposure across hybrid environments.

CORE COVERAGE

- **CSPM:** Continuous assessment of misconfigurations across AWS, Azure and GCP;
- **IaC Security:** Scans Terraform, CloudFormation and other IaC templates for security violations before deployment;
- **Vulnerability management integration:** Correlates on-premises and cloud vulnerabilities using Tenable.io and Nessus;
- **Exposure management:** Links vulnerabilities and misconfigurations into a unified exposure score;
- **Visualization and risk context:** Graph-based visualization of cloud resources, relationships and risk paths;
- **Compliance reporting:** Automated mapping to frameworks like NIST, CIS, PCI DSS and GDPR.

WHAT MAKES IT DIFFERENT

- **Exposure-centric approach:** Focuses on connecting cloud misconfigurations and vulnerabilities to overall business risk;
- **Integration with Tenable ecosystem:** Seamlessly combines Tenable.io and on-premises Nessus insights for hybrid visibility;
- **Strong IaC governance:** Prevents misconfigurations before deployment through policy-as-code;
- **Agentless and agent-based flexibility:** Offers both scanning and optional agents for deeper visibility;
- **Preventative security posture:** Prioritizes misconfigurations and vulnerabilities by exploitability rather than volume..

BEST FIT

- **Enterprises already using Tenable** for vulnerability management;
- **Security and DevOps teams** seeking unified IaC and cloud security enforcement;
- **Organizations focused on exposure management** rather than runtime defense.

CAVEAT

Not a full runtime CNAPP - strong in prevention, posture and compliance, but often paired with other CWPP tools for runtime threat detection and response.

QUALYS TOTALCLOUD (SPECIALIZED CNAPP - UNIFIED AGENT ARCHITECTURE)

WHAT IT IS

Qualys TotalCloud extends Qualys' renowned vulnerability management and compliance capabilities into the cloud, unifying asset visibility, posture management and workload security. Built on the Qualys Cloud Platform, it delivers CSPM, CWPP and vulnerability management using a single lightweight agent across on-premises, hybrid and cloud environments.

CORE COVERAGE

- **CSPM:** Cloud resource inventory, configuration checks and continuous compliance validation;
- **CWPP:** Workload and container protection via the Qualys Cloud Agent for virtual machines, containers and endpoints;
- **Vulnerability management:** Continuous scanning and risk prioritization for all connected assets;
- **Policy compliance:** Automated checks against regulatory and security benchmarks (such as PCI DSS, HIPAA and GDPR);
- **Container security:** Image scanning, runtime protection and compliance enforcement in containerized environments;
- **Unified Agent Model:** One agent covers vulnerability, configuration and compliance use cases across infrastructures.

WHAT MAKES IT DIFFERENT

- **Single-agent deployment:** Minimizes agent sprawl while providing broad asset and workload coverage;
- **Proven scalability:** Supports millions of assets globally through Qualys' mature SaaS platform;
- **End-to-end visibility:** Integrates traditional IT, cloud and container security into one console;
- **Compliance-driven architecture:** Built around enterprise reporting and continuous compliance enforcement;
- **Flexible deployment:** Available as SaaS or private cloud instance, catering to regulatory environments.

BEST FIT

- **Large enterprises and government organizations** extending existing Qualys deployments into cloud;
- **Security teams prioritizing compliance and vulnerability management** across hybrid environments;
- **Organizations seeking a unified, low-footprint solution** for vulnerability and posture management.

CAVEAT

While strong in assessment, compliance and prevention, TotalCloud lacks advanced runtime analytics and behavioral threat detection found in newer CNAPP architectures. Best suited for organizations emphasizing visibility and compliance over real-time runtime protection.

FORTINET - FORTICNP (SPECIALIZED CNAPP - FEDERATED CLOUD SECURITY PLATFORM)

WHAT IT IS

FortiCNP (CNP - cloud native protection) extends Fortinet's Security Fabric into the cloud, unifying findings from multiple Fortinet products and cloud-native tools to deliver contextualized risk insights. Rather than being a stand-alone CNAPP, it serves as a centralized intelligence layer, aggregating signals from FortiGate, FortiEDR and cloud posture tools to provide actionable, prioritized security guidance.

CORE COVERAGE

- **CSPM:** Continuous cloud configuration and compliance scanning across AWS, Azure and GCP;
- **Risk resource insights (RRI):** Proprietary scoring model that prioritizes cloud risks based on contextual analysis from multiple telemetry sources;
- **Multi-source correlation:** Consolidates data from FortiGate firewalls, FortiAnalyzer, FortiManager and cloud-native APIs;
- **Vulnerability and misconfiguration management:** Identifies and prioritizes cloud exposures through unified dashboards;
- **Compliance Reporting:** Maps findings to frameworks such as NIST, CIS and PCI DSS for audit readiness.

WHAT MAKES IT DIFFERENT

- **Federated data model:** Merges findings from Fortinet and third-party sources into a single risk-centric view;
- **Integration-first approach:** Designed to enhance existing Fortinet deployments, leveraging shared telemetry across network, endpoint and cloud layers;
- **Contextual risk prioritization:** Uses RRI to identify which resources pose the greatest real-world exposure;
- **Cloud-to-network visibility:** Extends Fortinet's network defense and segmentation intelligence into cloud environments.

BEST FIT

- **Organizations already invested in Fortinet's Security Fabric;**
- **Enterprises seeking unified cloud and network risk visibility;**
- **Teams emphasizing compliance and contextual prioritization over stand-alone runtime defense.**

CAVEAT

FortiCNP relies heavily on existing Fortinet infrastructure for full value and is more of an aggregation and prioritization engine than a full-featured CNAPP. Deployment complexity is higher for organizations integrating multiple Fortinet tools but delivers strong risk correlation across network and cloud layers.

UPTYCS (SPECIALIZED CNAPP - UNIFIED TELEMETRY AND THREAT ANALYTICS)

WHAT IT IS

Uptycs is a cybersecurity analytics platform that delivers unified visibility, detection and response across cloud workloads, endpoints and containers. Founded in 2016 and headquartered in Waltham, Massachusetts, Uptycs helps organizations manage hybrid cloud risk by providing continuous monitoring and analytics-driven threat detection. The platform focuses on cross-domain telemetry and correlation, empowering security teams to identify vulnerabilities, detect threats and respond effectively across diverse infrastructures.

CORE COVERAGE

- **Security analytics:** Centralized visibility and correlation of data across cloud, container and endpoint environments;
- **Asset discovery and risk assessment:** Continuous inventory and risk scoring for hybrid cloud assets;
- **Threat detection and response:** Behavioral analytics for detecting anomalous activity and coordinated attacks;
- **Access control and data security:** Enforces least-privilege policies and protects sensitive data;
- **Continuous monitoring:** Real-time visibility into vulnerabilities, configuration drift and compliance posture.

WHAT MAKES IT DIFFERENT

- **Unified telemetry model:** Built on osquery, enabling standardized data collection across endpoints and cloud workloads;
- **Cross-domain correlation:** Connects data from workloads, containers and endpoints to uncover complex attack paths;
- **Flexible deployment:** Available as SaaS or on-premises to support regulatory and operational needs;
- **Integration ecosystem:** Natively integrates with SIEM, SOAR and third-party security tools for centralized visibility.

BEST FIT

- Enterprises operating hybrid or multi-cloud environments that require unified analytics across domains;
- Security teams emphasizing visibility, telemetry correlation and threat hunting;
- Organizations prioritizing forensics and investigation capabilities over automated CNAPP remediation.

CAVEAT

Uptycs emphasizes analytics and visibility rather than full CNAPP automation or AI-driven remediation. Agent deployment and integration expertise are required for maximum effectiveness, making it best suited for mature security teams with hybrid visibility goals.

About ISMG

IInformation Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of its 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Its annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800)944-0401 · sales@ismg.io

902 Carnegie Center · Princeton, NJ · 08540 · ismg.studio