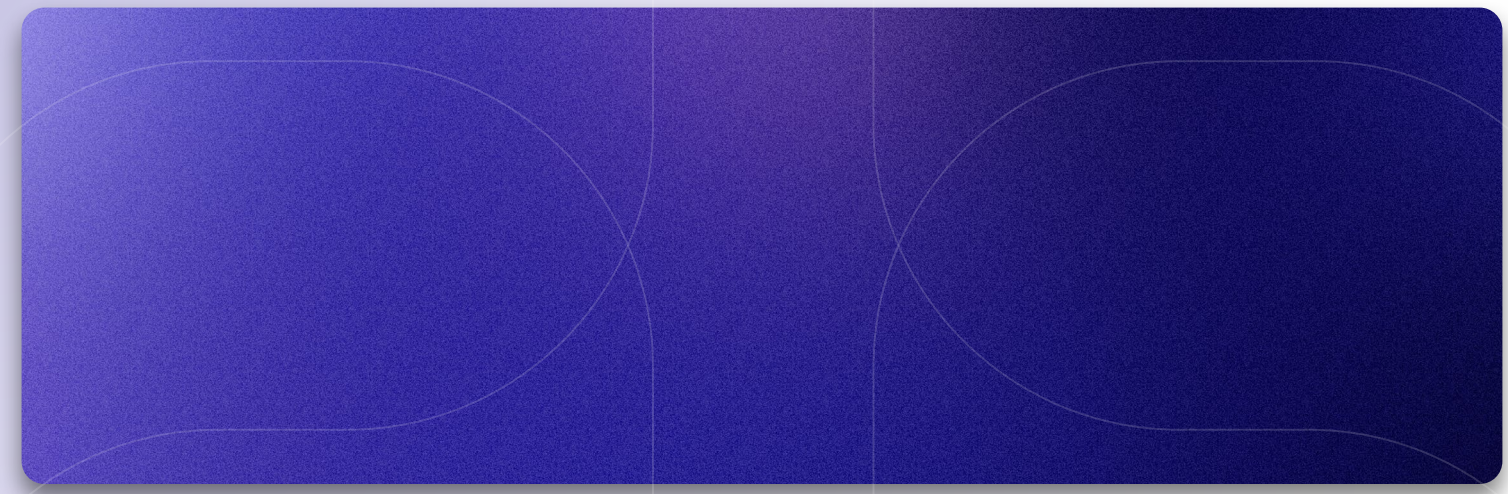
SentinelOne

A Buyer's Guide to CNAPP

Solving Cloud Security Challenges

Table of Contents



Executive Overview

A multitude of point-specific solutions has complicated cloud security operations, increased friction, and impaired achievement of objectives. These tools often emphasize risk mitigation within pre-production environments while neglecting protection in runtime. A cloud-native application protection platform (CNAPP) addresses many of these concerns by consolidating functional capabilities and leveraging a single security data lake. This document is intended to raise awareness of how a CNAPP helps, as well as what characteristics to look for as organizations seek to transition to a comprehensive CNAPP.

The Cloud Presents Unique Security Challenges

68% of cloud security professionals surveyed in the 2025 SentinelOne Cloud Security Report indicate that their organization generates so much cloud security data that they struggle to derive and prioritize actionable insights. Looking at the confluence of various factors, it is not hard to understand why.

- **Constant Change**
  Your organization likely went to the cloud to innovate quickly and create competitive advantage. Whether it's by multiple dev teams accelerating updates via automated CI/CD pipelines, your multi-cloud footprint is ever-expanding and rapidly evolving. Has cloud security operations kept stride? Many cloud security professionals complain about inefficient manual processes.

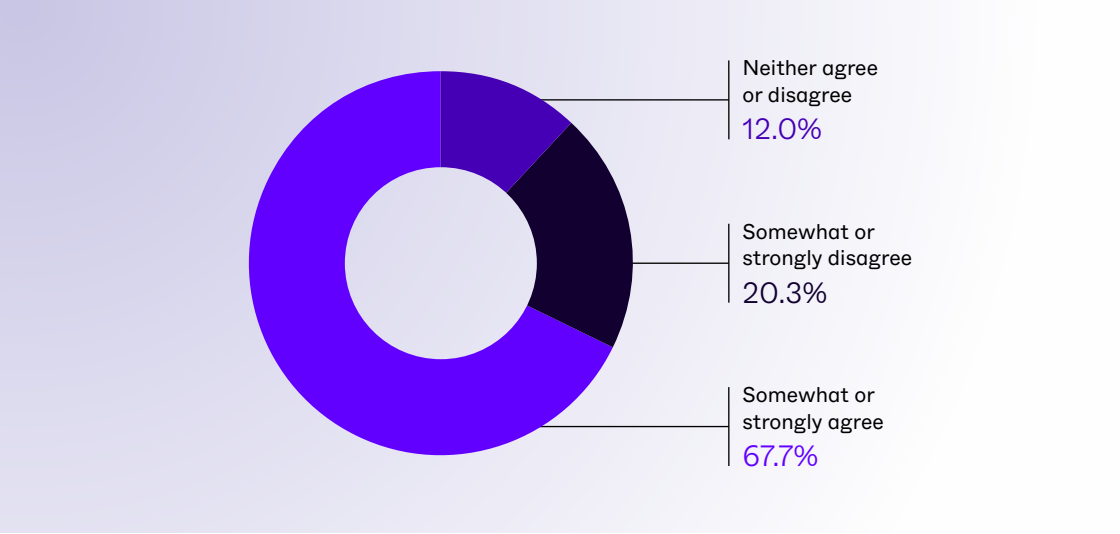
- **Multiple Point-specific Tools, Data Silos**
  Many security solutions are now mainstream. CSPM, CDR, CWPP, and vulnerability management, just to name a few. Not to mention that cloud breaches don't always start in the cloud, so EDR, ITDR, and Email Security. The complicating factor is that each of these specialized solutions typically exist in isolation. The data they create are locked away in their own data silos.

- **An Avalanche of Alerts and False Positives**
  Each of these solutions create alerts. But with the context behind each alert locked within its own data silo, obscuring a clear view of an incident's root cause and complicating the job of the research analyst. In fact, the aforementioned 2025 SentinelOne report indicates that nearly half of alerts are false positives.

- **Too Few Experienced Hands**
  While this problem is not unique to securing the cloud, finding and retaining cloud security talent continues to strain multi-cloud operations.

In summary, a cloud security stack of multiple point-specific solutions has not achieved the desired results. Security staff are stretched thin, desensitized by noise, and scrambling to find needles spread among multiple haystacks (ie, data silos). A CNAPP can help address these challenges.

Figure:
Agreement that their organization generates so much cloud security data that they often struggle to derive and prioritize actionable insights.



A CNAPP Should Solve These Pain Points

A cloud-native application protection platform (CNAPP) is a tightly integrated set of security and compliance capabilities intended to secure and protect cloud-native applications across development and production environments. CNAPPs bring together what were previously siloed functional capabilities to improve cloud security outcomes.

- **A CNAPP simplifies multi-cloud operations and improves risk management.**
  Replacing a patchwork quilt of point solutions diminishes complexity and unifies risk visibility through a single consolidated security data lake. The underlying data is more readily accessible, and streamlines investigation through automatically derived context.
- **A CNAPP slashes time to remediation.**
  Better context helps practitioners better prioritize their backlog based upon risk severity, probability of exploitation, and impact to the business. It also informs remediation action and promotes information sharing with the owner of implementing the fix.
- **A CNAPP realizes a closed-loop feedback system from runtime back to build time.**
  It facilitates collaboration between security practitioners and cloud-native application developers through improved information sharing and mutual understanding of risk. Security guardrails from a CNAPP enhances consistent enforcement. This reduces friction and shifts security left, to help accelerate innovation along said guardrails.

Capabilities To Look For

- Cloud Security Posture Management (CSPM)
- Kubernetes Security Posture Management (KSPM)
- Infrastructure as Code (IaC) Scanning
- Cloud Infrastructure Entitlement Management (CIEM)
- Secrets Scanning
- Agentless Vulnerability Scanning
- Attack Path Analysis
- Cloud Workload Protection Platform (CWPP)
- Cloud Detection & Response (CDR)
- CI/CD Integration
- DSPM
- Consolidated Security Data Lake

Key Capabilities

Cloud Security Posture Management (CSPM)

CSPM pinpoints misconfigured cloud resources and monitors compliance to industry standards. Not only does a CSPM check for proper configuration, but can also be used in risk analysis. Graphical relationship mapping of resources helps security practitioners in said risk analysis. (See section, "Attack Path Analysis.")

As organizations transition from a multitude of point-specific solutions, including CSPM, to a comprehensive CNAPP, they will quickly discover platform benefits outweigh the costs and complexities stemming from attempts to confederate so many data silos. This speaks to the convenience and context derived from a singular security data lake.

> "
>
> CNAPPs provide better identification, prioritization, and remediation of cloud-native application risk through a centralized and unified platform providing actionable insight... as organizations shift to a CNAPP-based approach, the synergy of an integrated platform will provide more benefits than a best-of-breed strategy that is difficult to scale.
>
> Gartner® Market Guide for Cloud-Native Application Protection Platforms, July 2024

CAPABILITIES TO LOOK FOR

- Built-in and custom configuration checks
- Asset inventory
- Graph analytics of attack paths
- Compliance frameworks supported
- Compliance dashboard
- Prioritization assistance

Kubernetes Security Posture Management (KSPM)

Similar to CSPM, KSPM focuses on the complexities and nuances of Kubernetes security. It assesses risk and monitors K8s clusters against security policies, finding misconfigurations such as insecure pods, overly permissive roles, exposed APIs, and insufficient network policies.

CAPABILITIES TO LOOK FOR

- Support for self-managed and managed K8s services
- View interdependencies of clusters, services, images
- Pinpoint exact vulnerable components
- Visualize risk analysis and propagation
- Streamline compliance and audit processes

Infrastructure as Code (IaC) Scanning

Infrastructure as Code (IaC) scanning inspects cloud infrastructure provisioning templates for security flaws, for example, misconfigurations. By identifying issues early in the software development lifecycle, the potential cost and impact of security failures can be mitigated. Moreover, such issues identified in production can be linked back to their root cause in the template.

CAPABILITIES TO LOOK FOR

- Support most common IaC frameworks
- Assign issues to owners
- Label issues
- Change severity
- Compliance monitoring

Cloud Infrastructure Entitlement Management (CIEM)

CIEM focuses on identity management and permissions to access cloud resources. Managing cloud identities is complicated not only by the ever-expanding number of cloud services, but especially by the granularity of machine identities used in managing access to them. CIEM helps you understand your identity risk, enforce least privileges, and detect suspicious access patterns.

CAPABILITIES TO LOOK FOR

- Multi-cloud support
- Discover overly permissive human and machine identities
- Curtail risk of privilege escalation
- Pinpoint toxic permission combinations
- Remove unused identities

Secrets Scanning

Compromised credentials remain a leading cause of cloud security failures, providing easy entry for unwanted intruders. Threat actors have automated means of identifying access keys, tokens, and credentials hard-coded (clear text or encrypted) within software posted to code repositories. A secrets scanning capability within a CNAPP pinpoints these hard-coded secrets, so you can change the locks and prevent unauthorized access to your cloud environments.

CAPABILITIES TO LOOK FOR

- Types and quantity of discovered secrets
- Inspect repos, both public and private
- Inspect developer & organization repos
- Determine of whether a key is still valid
- Detection speed

Vulnerability Scanning

Agentless scanning cloud-native application source code for known vulnerabilities (CVEs) is a vital functional capability for closing the security loop from operations back to development. Multiple factors such as CVE severity, exploit probability, affected container images, and resource misconfigurations help develop a shared understanding of relative priority among SecOps, DevOps, AppSec, and Developers.

CAPABILITIES TO LOOK FOR

- Local container image scanning
- Software Bill of Materials (SBOM)
- Assign exploit probability to known CVEs
- Map vulns to affected resources, misconfigurations
- Support for self-managed K8s

Attack Path Analysis

Understanding the relationships between the cloud assets that compose a cloud-native application is fundamental. Beyond simply graphing the relationships into so-called Attack Paths, a CNAPP should offer analytics which help security practitioners more fully appreciate risk of the system as a whole. Examples of such capabilities may include mapping software vulnerabilities and resource misconfigurations to specific elements, as well as severity and risk of exploitation.

Prioritize CNAPP offerings with deep graph analytics expertise.

CAPABILITIES TO LOOK FOR

- Graphical relationship mapping
- Link misconfigurations to resources
- Link known CVEs, their severity, and exploit risk
- Graphical query of a security data lake

Cloud Workload Protection Platform (CWPP)

Agentless CWPP, usually part of a CNAPP, periodically inspects snapshots of cloud compute instances for malware. It's a simple shortcut, but hindered by its limitations: no real-time threat detection, and no kernel-level observability and response.

In contrast, a CWPP agent provides **real-time threat** detection and response. Only an agent can observe and record kernel process-level workload telemetry - a **forensic data record** which proves priceless during investigation and threat hunting.

A CWPP agent serves a complementary role to an agentless CNAPP, protecting workloads in real time from runtime threats such as ransomware, zero-days, and memory injection exploits.

CAPABILITIES TO LOOK FOR

- Real-time cloud workload protection
- Broad Linux distribution support
- eBPF architecture, for stability and efficiency
- Support for servers, VMs, containers, and serverless containers
- Record detailed workload telemetry

Cloud Detection & Response (CDR)

CDR continuously monitors cloud infrastructure audit logs and API calls over time to detect suspicious activity. Illustrative examples might include but are not limited to unauthorized access (attempts to hijack cloud accounts), evade detection (modify snapshots), and establish persistence.

CAPABILITIES TO LOOK FOR

- Presents detailed evidence of findings
- Applies context for threat prioritization by impact and severity
- Uses advanced analytics to suppress noise and FPs

Data Security Posture Management (DSPM)

Data Security Posture Management (DSPM) provides visibility into where sensitive data is stored or kept – including cloud data. It aims to help organizations improve their cloud security posture, cloud data movement, and cloud data protection. DSPM ensures that sensitive data is shared only with authorized recipients and identifies potential vulnerabilities associated with data storage, transmission, and retrieval. CSPM and DSPM are often used in tandem to secure both the underlying cloud infrastructure and the data stored within.

CAPABILITIES TO LOOK FOR

- Automatic data discovery of cloud and self-hosted data stores
- Ruleless data classification based on data similarity
- Enforce least privilege access control
- Multi-cloud compliance support for standards such as HIPAA, PCI-DSS, and NIST

Singularity™ Cloud Security

Verify exploitable risk and stop runtime threats with a comprehensive, AI-powered CNAPP

Stop runtime threats at machine speed

Leverage the power of multiple AI-powered detection engines providing machine-speed protection and response.

Delete and prioritize exploitable risk

Reduce your cloud attack surface with automated asset discovery and align Dev, SOC, and IT with verified exploitable risk.

Accelerate response with unified visibility

Simplify investigations with generative AI to and action cross-surface alerts from cloud endpoint, and identity in a unified data lake.

SentinelOne Singularity Cloud Security is an AI-powered, multi-cloud CNAPP that provides buildtime-to-runtime protection for your cloud estate by combining proactive risk reduction with autonomous detection and response. It presents evidence-backed findings to cut through noise allowing SOC, IT, and DevOps teams to prioritize exploitable risk, while AI-powered detection engines maintain uptime by autonomously blocking attacks.

- **Singularity Cloud Native Security** is our agentless CNAPP that shifts security left to detect vulnerabilities, misconfigurations, and exposures before they reach production. It uses a unique Offensive Security Engine™ that analyzes and probes identified issues using benign attack payloads to present evidence-backed Verified Exploit Paths, to help you focus on exploitable issues that pose imminent risk to your business.
- **Singularity Cloud Workload Security** is our AI-powered CWPP that delivers real-time detection of runtime threats that other security controls miss and/or were never intended to detect like ransomware, zero-day exploits, and memory injection attacks. Built using eBPF, the highly stable and efficient agent that operates with no kernel dependencies, includes 5 distinct detection engines to stop known and unknown threats in their tracks at machine-speed.
- **Singularity Cloud Data Security** is AI-powered malware protection for NetApp and cloud data stores. Detect threats in milliseconds and streamline threat response with automatic quarantine of malicious objects. And, all file scans are local, meaning no data leaves your network.

Singularity Cloud Security is built on top of the Singularity Platform. Cloud workload telemetry and third-party data feeds are ingested and normalized within a cloud-native Security Operations platform for better visibility, interoperability, and speed. This data is accessible by PurpleAI which leverages natural-language queries and event summaries to remove the complexity and effort from cloud investigation and threat huntings.

KEY BENEFITS

- Rapid deployment and insights
- Highly performant and easy to use
- Multi-cloud protection with more than 20 cloud log integrations
- Verified Exploit Paths™, backed by evidence, for better prioritization
- Market-leading runtime protection built on eBPF since 2019
- Inventory, assess, and visualize AI workloads with AI-SPM
- Unified data lake to correlate and action all your security data
- Data ingestion from 3rd party solutions
- Purple AI for natural-language queries and threat hunting
- Hyperautomation for no-code automation of security workflows automated response

Conclusion

Eager to learn more about our comprehensive, AI-powered CNAPP, but not sure about speaking with a human just yet? We get it. Here are some more resources for your consideration.

- 1-Minute Video
- Solution Web Page
- Customer Case Studies
- Competitive Comparison

And when you are ready to discuss your CNAPP needs, we are ready to listen.

- Ask About a Rapid Cloud Security Assessment

PeerSpot

“

I’ve used other CNAPP’s. CNS has many advantages, including reduced false positives and detection time.

★★★★½

CISO

SOFTWARE COMPANY

PeerSpot

“

Straightforward, powerful, saves time. Increases collaboration between Security & Dev.

★★★★½

DevSecOps Engineer

TECHNOLOGY COMPANY, 1K+ EMPLOYEES

CNAPP POC Checklist

Artifact Scanning

- [ ] Secrets Scanning
- [ ] IaC Scanning
- [ ] Vulnerability Scanning
- [ ] Container Image Scanning
- [ ] Malware Scanning
- [ ] SBOM

Configurations

- [ ] CSPM
- [ ] KSPM
- [ ] AI-SPM
- [ ] Compliance
- [ ] Inventory
- [ ] CIEM

Runtime Security

- [ ] CWPP
- [ ] CDR

Other Considerations

- [ ] Multi-Cloud
- [ ] Security Data Lake
- [ ] Partner Integrations

Data Security

- [ ] DSPM
- [ ] Threat Detection for Data Stores

Innovative. Trusted. Recognized.

The Most Awarded CNAPP Solution
Over 240 awards—and counting

Industry-leading ATT&CK Evaluation
+ 100% Detections. 88% Less Noise
+ 100% Real-time with Zero Delays
+ Outstanding Analytic Coverage, 5 Years in a Row

98% willing to recommend
CNAPP customers rank SentinelOne highly in satisfaction, innovation, and performance

Contact Us

techpartners@sentinelone.com
+1-855-868-3733

sentinelone.com

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

25_MKTG_PMM_WhitePaper_013_CNAPP_Buyers_Guide_r2.1_07102025