

The CISO Guide to Cloud-Native Application Protection

Strategies for Protecting Multi-Cloud
Environments in a Hybrid World



Executive Summary

**Your cloud perimeter is already breached.
You just haven't found the entry point yet.**

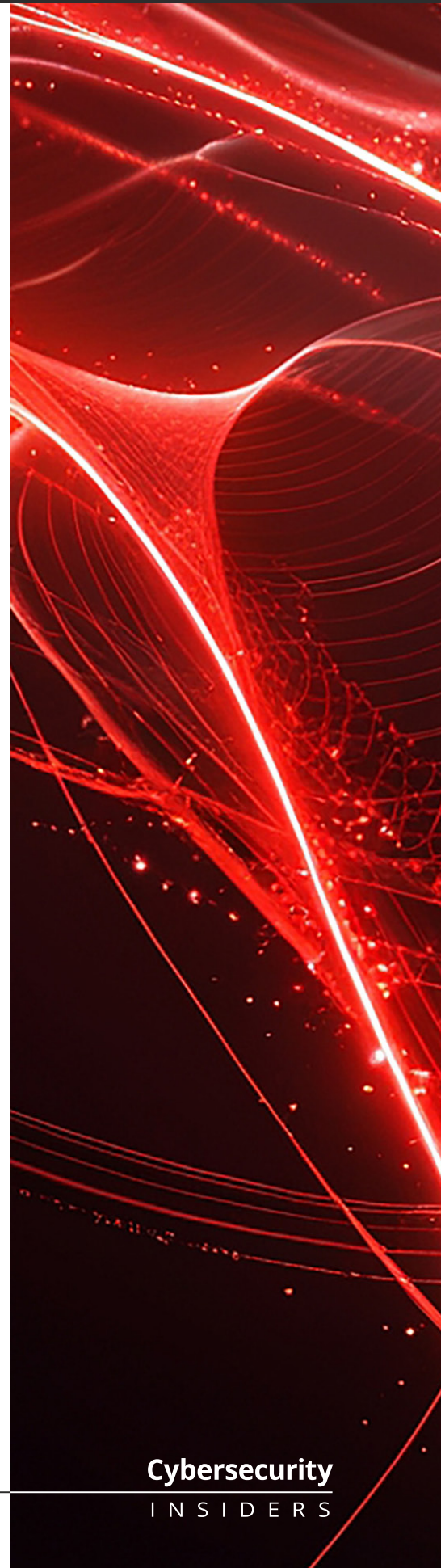
Cloud-native architectures have delivered speed and scale, but have expanded the attack surface exponentially. Identities (machine and human) constantly evolve, and APIs create new vulnerabilities. Gartner reports identity-driven attacks now outnumber perimeter breaches nearly 3-to-1, with cloud misconfigurations still the primary breach vector.

Traditional security tools like SIEMs and legacy SOC platforms weren't built for the scale and complexity of cloud environments. They overwhelm teams with low-value alerts, provide limited visibility into cloud activity, and lack the contextual insight needed to correlate risk with behavior or automate a timely response. That's what today's cloud-native threats demand—and what legacy tooling fails to deliver. Cloud-Native Application Protection Platforms (CNAPP) address these gaps. Fortinet's Lacework FortiCNAPP is built natively for the cloud from Lacework technology and integrated into the Fortinet Security Fabric. Its architecture ensures fewer false positives, faster threat investigations, significantly reduced operational noise, and enhanced developer productivity.

Independent reports validate these outcomes:

- › **Up to 80% faster threat investigations**
(Fortinet internal case studies, 2024)
- › **95% fewer false positives**
(validated customer deployments, 2024)
- › **Just 1.4 critical alerts per day on average**
(Fortinet industry metrics, 2024)

As cloud environments become increasingly complex, adopting a CNAPP strategy isn't optional. It's imperative.



A New Model for a New Era

The conventional cloud security model remains reactive and fragmented:

CSPM tools detect misconfigurations, CWPP detects malware, and CIEM manages entitlements, but none connect the dots.

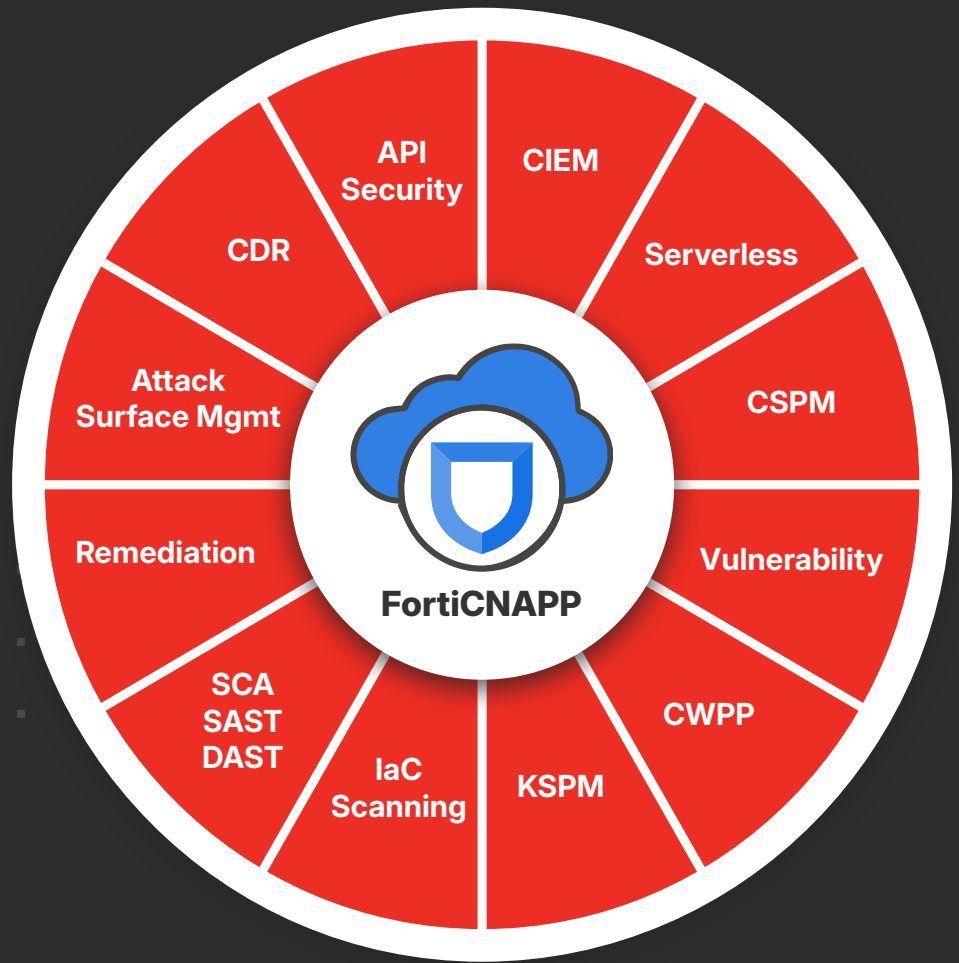


Figure 1: CNAPP unifies a variety of cloud security tools

Modern Cloud-Native Application Protection Platforms (CNAPP) Require More Than Visibility

Modern CNAPP, such as Lacework FortiCNAPP, stand apart by correlating static and dynamic signals, creating rich contextual awareness and automating responses across the cloud application lifecycle. Rather than reacting to alerts, FortiCNAPP enables proactive intervention to contain and eliminate threats before they cause significant harm.



Code-to-Cloud Lifecycle Security

Effective cloud security must begin before code deployment. Lacework FortiCNAPP integrates directly into Infrastructure-as-Code (IaC) pipelines, enabling early detection of leaked secrets and misconfigurations, and enforcing security policies. Built-in Static Application Security Testing (SAST), Software Composition Analysis (SCA), and Software Bill of Materials (SBOM) tools ensure robust and secure development without disrupting workflows. Unlike vendors that rely on loosely integrated acquisitions, FortiCNAPP is natively architected, delivering seamless coverage from code to cloud with superior scalability, tighter integration, and significantly reduced complexity.

Risk + Threat Correlation

Not all risks are equal. Effective CNAPP correlates posture findings with live threat telemetry, pinpointing actively exploited vulnerabilities in your environment.

By combining CSPM, CWPP, and CIEM, FortiCNAPP delivers prioritized insights into exploitability and impact, significantly reducing alert fatigue and enabling fast, confident responses.

AI-Powered Behavioral Analytics and Orchestrated Response

Sophisticated attackers no longer rely on known exploits to evade signature-based detection. FortiCNAPP employs a powerful AI-powered data platform to model normal user and entity behavior, enabling the rapid detection of unknown threats – including zero-day threats, compromised credentials, insider threats, ransomware, and cryptojacking – without needing static signatures or predefined rules. This behavioral approach is augmented by orchestrated response capabilities with the Fortinet Security Fabric. Automated integrations with FortiSOAR and FortiGuard enable real-time threat containment, remediation, and escalation, cutting attacker dwell time from days to seconds.



Operationalizing CNAPP

Real-World Scenarios

CNAPP value is clear when context replaces confusion. Consider these documented cases:

Upstream Risk Prevention

A leading healthcare provider integrated FortiCNAPP directly into their DevSecOps pipelines. Non-compliant IaC configurations in GitHub and Terraform were identified and blocked pre-deployment, preventing three significant compliance breaches in Q1 alone.

Triage and Alert Reduction

A global manufacturer overwhelmed by thousands of daily alerts implemented FortiCNAPP to correlate CSPM data with runtime activity. Only 2% of flagged misconfigurations were actively exploited, enabling security teams to strategically focus resources and reduce operational noise dramatically.

Behavior-Based Threat Detection

During a penetration test at a Fortune 100 firm, FortiCNAPP identified a container scanning sensitive storage and making outbound connections. FortiCNAPP's automated response contained and escalated the threat within 60 seconds, without relying on traditional threat signatures.

Coordinated Response in Hybrid Environments

A financial institution experienced unauthorized lateral movement within Kubernetes clusters. FortiCNAPP leveraged Kubernetes Security Posture Management (KSPM) to detect and isolate the compromised pod, automatically updated policies, and maintained comprehensive audit logs—all executed in minutes.

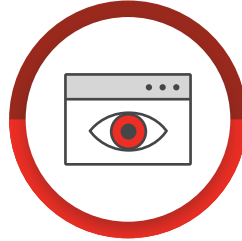
These scenarios demonstrate FortiCNAPP's critical role in reducing complexity, streamlining operations, and decisively protecting hybrid environments.

CNAPP Benefits



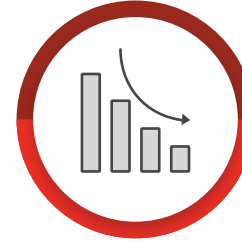
Minimize Attack Surface

Gain comprehensive visibility, proactively reduce vulnerabilities, misconfigurations, and excessive privileges without slowing down development.



Continuously Monitor Risks

Continuously assess virtual machines, containers, and Kubernetes workloads to address active risks before they are exploited.



Reduce Threat Impact

Quickly detect, investigate, and respond to unusual behaviour and active threats including the use of compromised credentials, cloud ransomware, and cryptomining.

Figure 2: How a CNAPP Enhances and Supports Core Security Tasks

Evaluating CNAPP Maturity: A Strategic Framework

To build an effective CNAPP strategy, CISOs need more than a list of features—they need a roadmap. Cloud-native security maturity isn't binary; it evolves across interconnected capabilities like visibility, threat detection, and automation.

This framework breaks down CNAPP maturity into five progressive stages, mapped across the dimensions that matter most: visibility and inventory, risk and vulnerability management, threat detection and response, compliance and governance, and automation and orchestration. Use it to benchmark where you are today, expose gaps that introduce risk or inefficiency, and prioritize the capabilities that will drive the biggest security and operational gains in your environment.

STAGE 1

Fragmented Control

(Initial / Ad Hoc)

At this stage, cloud security efforts are reactive and siloed. Tools like CSPM or CWPP may exist but are isolated, producing uncorrelated alerts with high noise and little context.

- **Visibility and Inventory:**
Incomplete or manual; limited to periodic scans or siloed dashboards.
- **Risk and Vulnerability Management:**
Posture is static; risks are logged but not linked to exploitability or runtime data.
- **Threat Detection and Response:**
Signature-based detection only; no behavioral analytics; slow manual triage.
- **Compliance and Governance:**
Point-in-time audits dominate; compliance gaps are discovered post-incident.
- **Automation and Orchestration:**
Minimal to none; manual playbooks dominate.

STAGE 2

Connected Visibility

(Foundational)

Security teams consolidate monitoring across cloud accounts and begin integrating basic tools.

- **Visibility and Inventory:**
Centralized inventory and asset discovery across cloud environments; real-time visibility still lacking.

- **Risk and Vulnerability Management:**
Misconfigurations and vulnerabilities surfaced more consistently, but triage remains manual.
- **Threat Detection and Response:**
Some basic anomaly detection begins to augment rules; few false positives are filtered.
- **Compliance and Governance:**
Improved visibility helps with audit readiness, but ongoing compliance remains difficult.
- **Automation and Orchestration:**
Alerting workflows begin to feed into ticketing systems or SOAR tools, but not dynamically driven by real risk.

STAGE 3

Contextual Prioritization

(Proficient)

Organizations begin correlating posture with real-time threat telemetry.

- **Visibility and Inventory:**
Dynamic inventory with continuous updates; coverage across workloads, containers, and APIs.
- **Risk and Vulnerability Management:**
CNAPP correlates static posture risks with exploitability data and attack paths; teams can focus on what matters most.
- **Threat Detection and Response:**
Runtime activity enriches findings; behavioral baselining identifies emerging threats earlier.
- **Compliance and Governance:**
Posture mapped to compliance frameworks; teams can spot drift before it leads to violations.
- **Automation and Orchestration:**
Policy-based triage; early integrations with CI/CD and runtime systems begin influencing prevention.

STAGE 4

Automated Protection (Advanced)

Security programs become adaptive, combining AI-driven detection with response orchestration.

- **Visibility and Inventory:**
Complete and continuously updated view across code, cloud infrastructure, identities, and data flows.
- **Risk and Vulnerability Management:**
Risks not just identified but contextualized and prioritized by actual attacker behavior and blast radius.
- **Threat Detection and Response:**
Advanced analytics detect unknown threats including zero-days and insider threats; automated containment is common.
- **Compliance and Governance:**
Continuous compliance with active controls; policy violations trigger automated guardrails or enforcement.
- **Automation and Orchestration:**
CNAPP triggers full remediation workflows—quarantine, kill, escalate—based on confidence and severity.

STAGE 5

Strategic Control Plane (Optimized)

CNAPP becomes the nerve center of cloud security operations.

- **Visibility and Inventory:**
Unified observability from development to production; enriched with business context and access insights.
- **Risk and Vulnerability Management:**
Risks inform threat models and prevention strategies upstream (e.g., in IaC); threat intel feeds reinforce prioritization.
- **Threat Detection and Response:**
Fully integrated with SOAR, SIEM, EDR, and identity systems for closed-loop detection and remediation.
- **Compliance and Governance:**
Proactive governance through embedded policy-as-code; audit-readiness is built-in.
- **Automation and Orchestration:**
Autonomous workflows maintain posture, block threats, enforce compliance, and reduce noise—empowering security teams to operate at scale with precision.

By clearly identifying your current stage and targeting improvements, CISOs can ensure their CNAPP evolves and scales effectively to address modern cloud security challenges.

CNAPP as the Strategic Control Plane

Security teams don't need more alerts. They require actionable intelligence and unified control. CNAPP shouldn't add another product, it must serve as the operational foundation of cloud security.

Fortinet's Lacework FortiCNAPP exemplifies these capabilities through its natively architected, fully integrated security fabric, contrasting sharply with fragmented, bolted-on solutions. FortiCNAPP simplifies continuous compliance by automatically mapping assets to standards like PCI DSS, HIPAA, SOC 2, and ISO 27001, significantly streamlining audits and reducing compliance fatigue.

The strategic question isn't whether CNAPP will become the central pillar of cloud security. It's whether your current cloud strategy is strong enough to withstand tomorrow's targeted, automated threats.

Critical Questions for Evaluating CNAPP Providers:

- *Do they provide real-time correlation of posture and active threat behavior?*
- *Is their platform unified across code, workloads, APIs, and identities?*
- *Can they detect and respond to threats without relying solely on predefined signatures?*
- *What automation is built into threat detection, containment, and resolution?*
- *Does their solution significantly reduce operational complexity and overhead?*

Explore Further

[Learn More](#)

[Request a Demo](#)

[Get a tour of FortiCNAPP](#)

