5 Integrations that Make CNAPP Ideal for Cloud Environments

Key Takeaways

- CNAPPs unify CSPM, CWPP, and DSPM to secure multi-cloud environments across AWS, Azure, and GCP.
- Five essential integrations—cloud APIs, CI/CD pipelines, SIEM/SOAR, EDR/XDR, and compliance frameworks—enable real-time threat detection and automated remediation.
- These provide comprehensive visibility, tackling risks traditional tools miss.
- 61% of organizations cite security barriers to cloud adoption, while 64% lack confidence in real-time detection.
- Fidelis Halo® deploys rapidly with agentless and microagent architecture for 2026 scaling.

Cloud-native application protection platforms (CNAPPs) converge cloud security posture management (CSPM), cloud workload protection platform (CWPP), data security posture management (DSPM), and vulnerability management. They secure cloud infrastructure across multi-cloud environments. As 2025 progresses, organizations continue to battle increasing cloud security challenges, where security and compliance issues remain the primary barriers to cloud adoption, cited by 61% of organizations[1].

CNAPPs integrate multiple security tools for cloud environments. They unify cloud detection, runtime security, and attack path analysis. Security teams gain comprehensive visibility into cloud assets and workloads, tackling risks that traditional security tools miss.

Key CNAPP integrations simplify operations, spanning cloud provider APIs to compliance frameworks. Real-time threat detection and automated remediation follow. Development and operations teams reduce security gaps in cloud native applications through this unified approach.

How CNAPP Integrates Multiple Security Tools for Cloud Environments

CNAPPs pull together disparate security capabilities. They blend CSPM for cloud configuration scans with CWPP for runtime protection. DSPM adds data security layers across cloud services.

This unification breaks data silos. Cloud security issues like overprovisioned entitlements get prioritized. Attack surface mapping reveals paths from misconfigurations to sensitive data exposure.

In practice, CNAPPs ingest logs from cloud provider APIs. They correlate them with runtime telemetry from Kubernetes clusters and serverless functions. Security operations (SecOps) teams see the entire cloud estate in one view.

Gartner’s 2025 CNAPP Market Guide stresses this integration depth. Mature platforms handle cloud infrastructure entitlement management (CIEM) alongside vulnerability management. They prioritize risks based on exploitability in runtime environments[2].

Forrester’s Q3 2025 landscape confirms the need. CNAPPs must cover the development lifecycle from code repositories to production cloud workloads. This shift-left approach cuts operational overhead[3].

Cloud statistics underline urgency. 61% of organizations cite security and compliance as primary cloud adoption barriers, while 64% lack confidence in real-time threat detection.

Fidelis CloudPassage Halo® exemplifies this. Its agentless and microagent architecture unifies CSPM, CWPP across AWS, Azure, GCP. Patented centralized framework offloads processing to Fidelis Halo® Cloud.

1. Cloud Provider APIs: Essential for Seamless Multi-Provider Coverage

Cloud provider APIs enable CNAPP to scan AWS, Azure, and Google Cloud Platform (GCP) natively. Agentless access delivers continuous visibility into cloud configurations and entitlements.

Security teams query APIs for Compute Engine, EC2, and AKS resources. Public buckets, open ports, and IAM drifts trigger alerts. This forms the base for cloud security posture management across the entire lifecycle.

Attack path analysis thrives here. A weak GCP firewall rule maps to downstream cloud workloads. Prioritization uses context like runtime access patterns.

In multi-cloud environments, normalization unifies findings. Cloud assets commonly carry dozens of vulnerabilities, often from excess permissions.

Comparisons Across Providers:

Provider Key API Integrations Benefits for CNAPP AWS S3, EC2, EKS APIs, CloudTrail, IAM IaC scanning, bucket security, encryption keys Azure AKS, Storage APIs, Key Vault Entitlement audits, hybrid views, network security GCP GKE, Cloud Run APIs, Cloud KMS Serverless protection, KSPM, VPC monitoring

These connections support cloud integrations for real-time threat detection. Automated remediation closes gaps via API writes. Teams enforce security policies without manual console switches.

Fidelis Halo® Cloud Secure uses proxy-aware API connectors. It covers IaaS/PaaS like Lambda, Azure Functions, App Engine without agents. Continuous inventory hits every heartbeat.

To find platforms with comprehensive CNAPP integrations, look for native API depth across all three providers plus Kubernetes. This ensures coverage for cloud native application security in dynamic setups.

Cloud Security Essentials Powered by Fidelis Halo®

- Agentless Multi-Cloud Visibility
- Microagent Runtime Protection
- Automated Compliance (CIS, NIST, PCI, HIPAA)
- Continuous Monitoring & Rapid Remediation

Get the Full Halo® Solution Brief

2. CI/CD Pipeline Tools: Top Integrations for Development Lifecycle Security

CNAPPs integrate with CI/CD pipelines like GitHub Actions, Jenkins, and GitLab CI. Scans run on infrastructure-as-code (IaC) like Terraform and Helm charts pre-deployment.

Vulnerable containers halt builds. Secrets detection blocks exposed keys. This shifts vulnerability

management left in continuous integration workflows.

Development teams get inline feedback. Policy-as-code enforces cloud security standards. Runtime previews flag Kubernetes pod risks early.

Pipeline plugins enable early vulnerability detection. Multi-cloud IaC normalizes across CDK and ARM templates.

Best CNAPP Integrations for CI/CD Pipelines:

- **GitHub Actions:** SBOM generation, PR scans
- **Jenkins:** Gate enforcement, IaC validation via native plugin
- **GitLab CI:** Container image checks, compliance mapping

These simplify compliance management in pipelines. Custom rules align with CIS benchmarks. SecOps gains visibility into attack surfaces from day zero.

For cloud native applications, this covers serverless functions and containers. It reduces cloud threats from supply chain issues heading into 2026.

Fidelis provides CI/CD SDK, Jenkins plugin, deployment scripts. Microagents embed in gold images for Chef, Puppet, AMIs. DevSecOps shifts left seamlessly.

3. SIEM and SOAR Platforms: Seamless Connections for Incident Response

CNAPPs forward cloud detection data to SIEM systems. Platforms handling enterprise logs correlate runtime threats with network events.

Anomalous API calls enrich alerts with attack path details. Behavioral analytics prioritize cloud risks. SOAR automates quarantines via cloud provider APIs.

Security Tools that Integrate Well with CNAPP Solutions:

- **SIEM:** Log aggregation, ML scoring for misconfigs
- **SOAR:** Workflow orchestration, incident response capabilities
- **Ticketing:** ServiceNow for remediation tracking

Gartner highlights SOC integrations for advanced persistent threats. Cloud logs reveal lateral movement in cloud workloads. 64% lack confidence in real-time threat detection.

Look for CNAPP integrations that offer seamless SIEM and EDR—those with bi-directional APIs for telemetry and actions. This unifies security operations across hybrid cloud applications.

Runtime protection feeds threat intelligence. Teams handle data exfiltration in serverless without silos.

Fidelis Halo® integrates natively with SIEM/SOAR. REST API delivers JSON events. Curated threat intelligence enhances cloud detection.

4. EDR and XDR Solutions: Hybrid Runtime Protection

CNAPPs link with EDR/XDR for endpoint-to-cloud coverage. Runtime threats in cloud workloads

blend with VM telemetry.

Kubernetes cryptojacking correlates across layers. Attack path analysis spans endpoints to cloud assets. Workloads represent a primary attack target.

List of Integrations for Real-Time Threat Detection:

- EDR: Behavioral endpoint data for cloud VMs
- XDR: Unified dashboards, automated isolation
- CWPP: Container runtime security

In Google Cloud and multi-cloud setups, normalization helps prioritize risks. Incident response speeds via shared views.

This beats traditional security tools for runtime environments. Forrester notes hybrid compliance gains.

Fidelis Halo® Server Secure microagents (2MB Linux/Windows) deliver CWPP. They self-install, monitor file integrity, logs, and firewall. They quarantine rogue assets at cloud speed.

5. Compliance and Governance Frameworks: Top-Rated for Multi-Cloud Control

CNAPP map to NIST, PCI DSS, HIPAA, and CIS benchmarks. Automated scans flag drifts in cloud configurations and Kubernetes.

CSPM dashboards track security posture. DSPM discovers sensitive data across providers. Kubernetes security posture management (KSPM) enforces pod policies.

Essential CNAPP Integrations for Governance:

- **CIS/NIST:** Policy mapping, drift detection
- **PCI/HIPAA:** Data flow audits, compliance violations alerts
- **Custom:** Policy-as-code for serverless

Yes, CNAPP integrations simplify multi-cloud compliance via unified reporting and remediation. Regulatory needs are met without per-provider tools.

Governance controls attack paths tied to non-compliant resources. Teams maintain security posture amid scaling.

Top-Rated CNAPP Integrations for Governance and Control:

Framework CNAPP Role Multi-Cloud Benefit CIS Benchmarks Config validation Standardized checks across AWS/Azure/GCP NIST 800-53 Risk prioritization Attack path alignment PCI DSS Data security Sensitive data protection

Fidelis offers 10,000+ out-of-box rules for CIS, HIPAA, PCI, SOC2. Continuous monitoring, audit-proof records. Remediation scripts route to owners.

Fidelis Security: Unified CNAPP for 2026 and Beyond

Fidelis CloudPassage Halo® delivers CNAPP with these integrations baked in. Halo® Cloud

Secure handles agentless CSPM via native APIs for AWS, Azure, GCP IaaS/PaaS.

Halo® Server Secure provides CWPP with microagents for servers/workloads. Halo® Container Secure secures full-stack containers, Kubernetes.

Cloud provider APIs feed network detection and response. CI/CD scans align with runtime protection via SDK, Jenkins plugin. SIEM/SOAR flows enhance incident response. EDR/XDR extends to hybrid cloud resources. Compliance frameworks ensure regulatory compliance.

Deploys in under an hour. Adds accounts in seconds. No security tax—zero added compute costs. Security teams protect cloud native applications end-to-end. Comprehensive visibility cuts cloud risks. Fidelis fits enterprises scaling into 2026.

Reference:

1. ^2025-Cloud-Security-Report-Fortinet.pdf
2. ^Gartner Reprint
3. ^The Cloud Native Application Protection Solutions... | Forrester