How to Assess and Improve Your CNAPP Maturity

20 May 2025 - ID G00823491 - 41 min read

By: Fred Sotolongo

Initiatives:Security Technology and Infrastructure for Technical Professionals

Security architects struggle to keep pace with evolving threats in cloud environments. The Gartner CNAPP maturity model provides a framework to enhance security practices, automate processes and embed security into cloud development processes for robust cloud-native protection.

Overview

Key Findings

- Cloud environments are highly dynamic and increasingly complex, with resources being continuously created, updated and deleted. Without a clear path to mature cloud security practices, organizations risk falling behind in protecting their critical applications.
- Organizations face difficulties in automating security processes and maintaining visibility across cloud-native environments. Manual security checks and limited monitoring slow down response times and increase vulnerability risks.
- At the initial levels of maturity, organizations struggle to integrate security consistently into their development processes. Security is often treated as an afterthought, leading to reactive approaches that leave gaps in protection.
- Organizations that reach the higher levels of maturity achieve high levels of automation of detection and response processes, including real-time threat detection and remediation. These advanced capabilities allow them to respond to threats immediately, maintaining a resilient and secure environment.

Recommendations

- Use the cloud native application protection platform (CNAPP) maturity model to progress through the levels of maturity — transitioning from initial, ad hoc approaches to optimized, resilient security strategies. This progression helps systematically strengthen security posture, improve automation, ensure continuous compliance and integrate security deeply into development processes.
- Automate routine security tasks such as vulnerability scanning, compliance checks and policy enforcement within CI/CD pipelines. Expand automation to include remediation and incident response to reduce manual effort and human error.
- Improve CNAPP maturity by starting at the bottom across all dimensions of the assessment to establish a firm foundation, then consistently improve all dimensions without leaving any behind.
- Make cloud security a core part of the organizational culture to achieve the highest maturity levels. Encourage cross-team collaboration between security, development and operations to ensure that security is everyone's responsibility.

Analysis

As organizations increasingly adopt cloud-native architectures, they face challenges in securing complex environments that include containers, microservices and dynamic workloads. Traditional security measures frequently prove inadequate, requiring more integrated solutions such as CNAPP to ensure comprehensive protection throughout the application life cycle.

However, many organizations struggle to implement and mature cloud-native security practices effectively. Integrating security into the DevOps pipeline is often fragmented, with limited visibility into the environment, and incomplete security automation. This disjointed approach can lead to increased exposure to cyberthreats, higher costs associated with manual security processes, difficulties in meeting regulatory obligations and increased mean time to resolution (MTTR) for remediation efforts.

The Gartner CNAPP maturity model provides a comprehensive framework that guides organizations through the stages of developing and enhancing their cloud-native security practices. By progressing through the various levels of maturity — from initial, ad hoc approaches to optimized, resilient security strategies — organizations can systematically strengthen their security posture, improve automation, ensure continuous compliance and integrate security deeply into their DevOps processes. This can assist in systematically lowering MTTR over time.

Cloud Native Application Protection Platforms

CNAPPs represent an evolutionary approach to securing infrastructure as a service (IaaS) and platform as a service (PaaS) cloud environments throughout development and production. Unifying many previously disparate capabilities, CNAPPs incorporate features such as container scanning, cloud security posture management (CSPM), infrastructure as code (IaC) scanning, cloud infrastructure entitlement management and runtime vulnerability or configuration scanning in one platform. In doing so, they can provide a more holistic view of cloud-native deployments (e.g., posture context for workload security assessments and workload insights in posture management views). This consolidation marks a departure from earlier, fragmented tools that required multiple vendors and often led to a lack of integration, creating an unclear view of risks and potential inefficiencies in developers' efforts to prioritize and remediate them.

A CNAPP combines stand-alone security tooling to build its functionality. This includes:

- Cloud workload protection (CWP)
- CSPM
- Cloud infrastructure entitlement management (CIEM)
- Kubernetes security posture management (KSPM)
- IaC scanning

See 5 Ways CNAPP Will Improve Your Cloud Security and Market Guide for Cloud-Native Application Protection Platforms for more details.

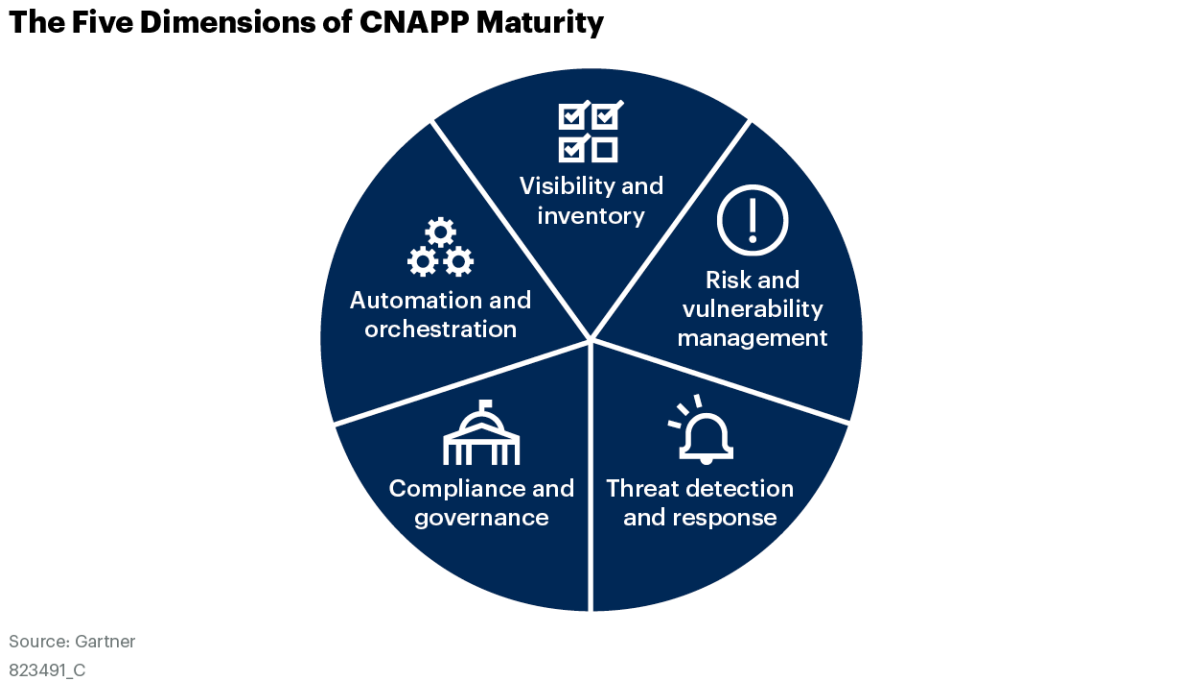
Gartner's CNAPP Security Maturity Model

The CNAPP maturity model is built around five dimensions that define an organization's ability to secure its cloud-native environments. Each dimension represents a critical aspect of cloud security, from gaining full visibility into assets and managing vulnerabilities to detecting threats, enforcing compliance, and automating security processes. As organizations progress through each maturity level, they transition from manual, reactive practices to integrated, proactive methods, establishing a more comprehensive and resilient security posture that aligns with the pace of modern cloud-native innovations.

The five dimensions for CNAPP maturity are (see also Figure 1):

- Visibility and inventory: Knowing what you have in your cloud environments (assets, workloads, configurations).
- Risk and vulnerability management: Defining how risks are identified, assessed and mitigated in cloud environments.
- Threat detection and response: Detecting and responding to malicious activity in your cloud environments and running workloads.
- Compliance and governance: Ensuring that your cloud environment meets regulatory requirements and internal security policies.
- Automation and orchestration: Automating security tasks to improve efficiency, reduce errors and enable faster response.

Figure 1: The Five Dimensions of CNAPP Maturity



For each of these dimensions, there are five maturity stages that indicate the level of advancement within them:

1. **Initial** — Basic cloud security with minimal visibility or controls.

2. **Developing** — Foundational security practices in place but limited automation and risk management.

3. **Intermediate** — Proactive security with improved threat detection, compliance and governance.

4. **Advanced** — Automated and integrated security controls with strong risk management.

5. **Optimized** — Security is fully integrated into the organization's cloud strategy and is continuously optimized.

With these progressive levels, the CNAPP maturity model guides organizations to advance from basic, ad hoc security practices to automated, proactive defenses in cloud-native environments. At the lower end, organizations often lack comprehensive visibility or risk management, relying on manual checks and piecemeal tools. As they progress, they embed security into CI/CD pipelines, establish real-time threat detection and adopt policy-as-code for consistent governance. Ultimately, at the optimized level, security is fully integrated across the organization, with increasing levels of automation, and advanced analytics, to prevent breaches before they occur.

Figure 2 illustrates the five dimensions of CNAPP security, along with the five stages of maturity against which each dimension can be measured.

Figure 2: CNAPP Maturity Model

CNAPP Maturity Model

CNAPP Pillars	Level 1 Initial	Level 2 Developing	Level 3 Intermediate	Level 4 Advanced	Level 5 Optimized
Visibility and inventory	Limited visibility into assets and workloads. Manual, often outdated inventory.	Basic discovery. Some cloud-native visibility, but gaps remain across clouds and asset ownership.	Asset discovery across all clouds; ownership tracked, context like dependencies may be missing.	Automated, real-time visibility across all cloud assets. Detailed context.	Continuous, dynamic discovery with full context, integrated with business risk.
Risk and vulnerability management	Reactive vulnerability scanning, infrequent and limited in scope. Manual remediation.	Basic vulnerability scanning for VMs and containers; patching in place but inconsistent.	Regular, automated scanning across clouds; basic risk prioritization (e.g., CVSS).	Comprehensive vulnerability mgmt: container scans, config, runtime. Risk-based with business impact.	Proactive scanning, predictive analysis, autoremediation, drift detection.
Threat detection and response	Limited cloud threat detection. Reliance on on-premises tools. Manual response.	Basic cloud monitoring (logs). Some alerts, high false positives, weak response plans.	Defined threat detection rules based on cloud attack vectors. Formal incident response.	Advanced threat detection: behavioral, anomaly detection. Autoresponse (e.g., workload isolation).	Proactive threat hunting/modeling. Automated, context-aware response.
Compliance and governance	Limited cloud security policies, compliance, or frameworks. Manual checks.	Basic cloud security policies. Some regulatory adherence. Manual reporting.	Defined policies/ frameworks aligned with best practices. Basic automated checks.	Comprehensive compliance automation with continuous monitoring. Basic PaC.	Heavy use of autoremediation of violations. PaC plays a large role in dev life cycle.
Automation and orchestration	Limited or no automation. Manual processes for security tasks.	Basic scripting for some security tasks (e.g., patching).	Significant security task automation (scanning, checks). Cloud-native tools.	Extensive automation across security life cycle. Orchestration of workflows.	Extensive IaC and PaC. Continuous optimization of processes. AI-driven automation.

Source: Gartner
823491_C

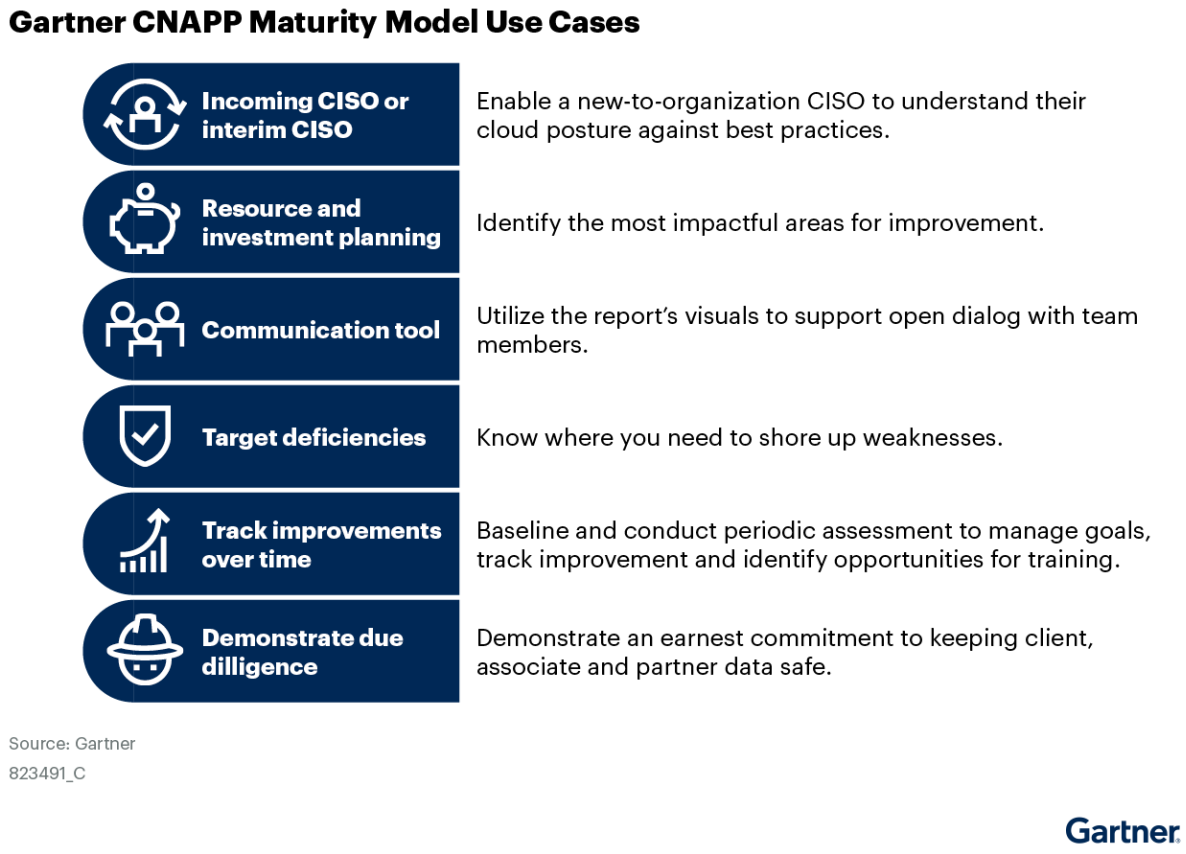
Gartner

CNAPP Maturity Model Use Cases

A CNAPP maturity model serves as a strategic tool to help organizations evaluate and advance their cloud security posture. For a new or interim CISO, the maturity model provides an essential health check, offering a clear, structured view of the current state of the organization's cloud security against industry-best practices. This insight equips leadership with the information necessary to make informed decisions early in their tenure and prioritize actions accordingly.

Beyond leadership transitions, the model plays an instrumental role in resource and investment planning by identifying the most impactful areas for improvement. It allows teams to identify specific deficiencies, prioritize remediation efforts and allocate budgets effectively. Regular assessments — conducted every six to eighteen months — enable organizations to baseline progress, track improvements over time and identify gaps in training or processes. Ultimately, using a CNAPP maturity model also supports broader compliance and trust objectives by demonstrating due diligence and a strong commitment to safeguarding client, associate, and partner data. See Figure 3 for list of use cases.

Figure 3: Gartner Maturity Model Use Cases



Visibility and Inventory

Back to top

Visibility and inventory in CNAPP refer to an organization's capacity to identify, track and monitor cloud assets across various cloud environments. This encompasses everything, from virtual machines, containers and serverless workloads to databases, IAM roles, and networking components. Without comprehensive visibility, organizations find it challenging to manage security risks, leading to misconfigurations, shadow IT and unauthorized access.

A well-defined visibility strategy ensures that security teams possess real-time insights into cloud workloads, the relationships between assets, the owner of the asset and potential security risks. The more mature an organization's visibility and inventory management, the easier it becomes to enforce security policies, maintain compliance, and detect anomalies before they escalate into breaches. Table 1 summarizes key aspects of each maturity level in visibility and inventory and is followed by more detailed information

Table 1: Rate Your Organization's Maturity in Visibility and Inventory

(Enlarged table in Appendix)

Visibility and Inventory

Level	Description
1Initial	■ Limited or no visibility into cloud assets and workloads. ■ Manual inventory management, often outdated. ■ Cloud assets are deployed without centralized oversight, creating gaps in visibility around ownership and security posture. ■ Security teams conduct point-in-time audits using CNAPP, which remain time-consuming and unreliable due to manual, fragmented asset discovery.
2Developing	■ Basic asset discovery. ■ Not all cloud environments in CNAPP. ■ Linking assets to their respective owners is also inconsistent. ■ Limited context; offers basic asset information (e.g., name, region, type), but lacks relationships and dependencies.
3Intermediate	■ Asset discovery and inventory across all cloud environments. ■ Infrastructure and application ownership is carefully monitored. ■ Improved CNAPP context, including information on ownership, configurations, tags, security groups and network connectivity.
4Advanced	■ Automated, real-time full life cycle tracking from build to runtime for every asset. ■ Detailed context, including application mapping, relationships and dependencies including capabilities such software composition analysis (SCA) and software bill of materials creation (SBOM). ■ Inventory data is integrated with other IT management systems, such as CMDB/ITSM, for a holistic view.
5Optimized	■ Fully automated discovery with continuous tracking, labeling and integration into CMDB or single source of truth. ■ Automated actions can be triggered based on inventory changes (e.g., quarantining a newly discovered, unapproved resource). ■ Visibility and inventory seamlessly feed other security functions (risk scoring, compliance checks and threat detection).

Initial (No Centralized Inventory and Limited Awareness)

At this stage, organizations lack a formal asset inventory and CMDB and rely on manual tracking methods, such as spreadsheets or ad hoc reports. Cloud assets are deployed without centralized oversight, resulting in a lack of visibility for security teams regarding the resources that exist, who owns them and their security posture. Additionally, there is no integration between cloud environments and security monitoring tools, CMDB, and ticketing systems, contributing to unmanaged cloud sprawl. Misconfigurations, excessive permissions and abandoned cloud resources often go unnoticed, significantly increasing the attack surface. Security teams often utilize CNAPP to conduct point-in-time audits, which are time-consuming and unreliable since asset discovery remains a manual and fragmented process.

Developing (Basic Asset Discovery and Limited Inventory Management)

Organizations are beginning to adopt measures to track cloud assets, but visibility remains partial and inconsistent. The inventory may only connect to certain areas of the multicloud environment, leaving gaps and blind spots. Additionally, linking assets to their respective owners is also inconsistent, meaning security teams struggle to assign the remediation of security findings to the correct owner.

While automated asset discovery is improving, organizations still lack visibility into asset relationships and dependencies. This hinders their ability to assess the impact of security changes, detect misconfigurations and manage risk effectively. Moreover, security teams may not have real-time monitoring, which leads to delays in identifying unauthorized changes or shadow IT deployments.

Intermediate (Comprehensive Asset Tracking)

At this level, organizations maintain a centralized asset inventory that integrates into all cloud workloads, configurations and relationships. Security teams utilize CNAPP's automated discovery capabilities and tagging frameworks to classify assets according to risk, business unit and compliance requirements.

CNAPP's are fully integrated into all cloud environments, automatically detecting security misconfigurations, unauthorized access and orphaned assets. Infrastructure ownership is carefully monitored to ensure that security findings are correctly assigned to the infrastructure owner and addressed appropriately. Asset metadata is enriched with contextual insights, enhancing risk assessment and policy enforcement.

Advanced (Automated Asset Discovery With Comprehensive Context)

The context now includes automated, real-time full life cycle tracking from build to runtime for every asset.

This gives a deep understanding of asset relationships, application dependencies, data flows and network topology (see Improve Application Security With Posture Management Tooling for more). Inventory data is integrated with other IT management systems, such as CMDB/ITSM, for a holistic view. Consistent tagging policies are enforced, enabling granular filtering and reporting.

Asset inventory is now completely automated and consistently updated. Organizations can now incorporate real-time telemetry, machine learning (ML), and behavioral analytics to identify asset anomalies and unauthorized alterations. Security teams can map dependencies between cloud resources, applications and identities, offering deeper insight into how security risks spread throughout the environment.

Optimized (Visibility Integrations)

At the highest maturity level, organizations engage in continuous, dynamic discovery and inventory, integrating full context with other security functions. Automated actions can be triggered based on inventory changes (e.g., quarantining a newly discovered, unauthorized resource). They utilize fully automated discovery with ongoing tracking, labeling and integration into the CMDB or a single source of truth. Visibility and inventory seamlessly support other security functions (risk scoring, compliance checks, threat detection).

Risk and Vulnerability Management

Back to top

Risk management in CNAPP includes identifying, assessing, prioritizing, and mitigating security risks such as misconfigurations, excessive permissions, vulnerabilities, and external attack vectors. An effective risk management strategy enables organizations to minimize security gaps, reduce the attack surface and maintain compliance with industry regulations.

Cloud risk management is particularly challenging because cloud environments are highly dynamic, and traditional security models do not always translate well to cloud-native architectures. Organizations must implement continuous risk assessment, leveraging automated scanning, security analytics and CNAPP's advanced risk prioritization capabilities. The more mature an organization's risk management approach, the better it can proactively address threats, mitigate risks and ensure continuous security enforcement.

CNAPPs bring together data from multiple capabilities that were previously siloed to improve risk prioritization and contextualization and share this contextual information with supplement tooling and ticking systems through structured workflows. A well-architected CNAPP solution will bring information from its various capabilities and use techniques such as a single data lake, data model, and unified graph database for all event logging, reporting, alerting, and relationship mappings, as illustrated in Figure 4. In addition, several CNAPP vendors offer capabilities for identifying and contextualizing sensitive data to enhance risk prioritization further.

Figure 4: CNAPP Risk Prioritization

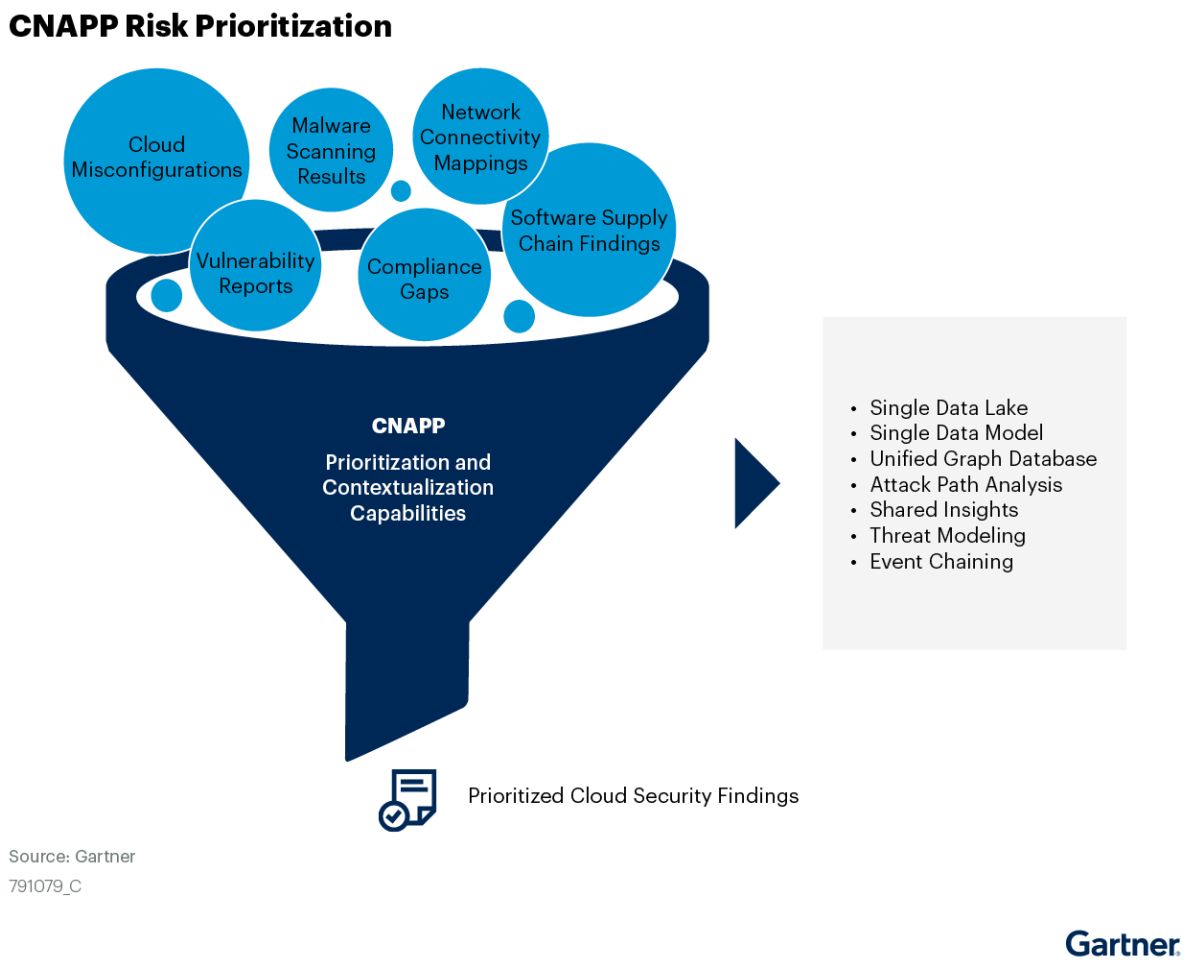


Table 2 summarizes key aspects of each maturity level in risk and vulnerability management, and is followed by more detailed information.

Table 2: Rate Your Organization's Maturity Risk and Vulnerability Management

(Enlarged table in Appendix)

Risk and Vulnerability Management

Level	Description
1Initial	■ No formal risk assessment framework for cloud-native environments. ■ Reactive risk identification and remediation, usually after incidents occur. ■ No visibility into cloud-specific risks (e.g., misconfigurations, overpermissioned accounts).
2Developing	■ Basic vulnerability scanning for cloud workloads. ■ Security policies exist but are inconsistently enforced. ■ Manual prioritization focusing on major known risks.
3Intermediate	■ Risk-based prioritization implemented for cloud vulnerabilities, guided by threat intelligence and business impact. ■ Defined risk tolerance levels for cloud security issues. ■ Automated misconfiguration scanning with policy enforcement.
4Advanced	■ Integration of risk management into the CI/CD pipeline and ticketing systems to augment and enrich initial workflows for remediation. ■ Automated policy checks and gating to prevent high-risk vulnerabilities from progressing. ■ Continuous risk scoring and reporting to stakeholders with near real-time updates.
5Optimized	■ Holistic, adaptive risk management, integrated with DevSecOps practices and real-time cloud posture management. ■ AI/ML-driven analysis for predictive risk assessment and autoremediation. ■ Ongoing lessons learned from postmortems and red-team exercises feed into improved threat modeling and more robust controls.

Source: Gartner (May 2025)

Initial (No Formal Risk Management and Reactive Security)

Organizations at this level lack a structured risk management process. Security teams use several point security tools that are not integrated and lack adequate context to prioritize security risks. Risks, such as open storage buckets, misconfigured IAM permissions and exposed APIs, go undetected until an incident occurs.

Security teams respond to security issues reactively without clear guidelines for assessing and mitigating cloud risks. There is no centralized risk assessment process, and security controls are applied inconsistently across cloud environments.

Developing (Basic Risk Assessments and Policy-Based Controls)

Organizations implement basic risk assessments and vulnerability scanning tools to detect security misconfigurations and policy violations. However, these assessments are performed manually or periodically, making it difficult to keep up with the dynamic nature of cloud security risks.

Security teams begin defining basic cloud security policies, but enforcement is inconsistent due to lack of automation. Risk prioritization remains unclear, meaning security teams struggle to differentiate between critical vulnerabilities and low-impact risks.

Intermediate (Automated Risk Analysis and Risk-Based Prioritization)

Organizations adopt automated risk assessments that continuously scan for misconfigurations, unsecure IAM policies and unpatched vulnerabilities. A risk-based prioritization framework is introduced, allowing security teams to focus on high-risk issues that pose the greatest threat. Risks are prioritized based on severity and exploitability, ensuring security teams focus on the most critical vulnerabilities first.

Risks become more visible at the organizational level and the remediation process becomes more structured with integrations to ticketing systems. This stage often marks the point where leadership begins to demand more consistent reporting on identified vulnerabilities and their resolution timelines.

Integration with ticketing systems for risk remediation are also present at this stage.

Advanced (Context-Aware Risk Mitigation and Continuous Monitoring)

At the advanced stage, risk management becomes proactive, incorporating context-aware risk analysis that evaluates business impact, compliance requirements and the likelihood of an attack.

Risk assessment transitions to a continuous process, spanning the entire life cycle of cloud assets — from build and deployment to runtime. Automated tools and processes prioritize risks dynamically, leveraging business impact analysis and real-time threat intelligence to focus on the most critical vulnerabilities.

Collaboration between development, security and operations teams is well-established, ensuring faster remediation and alignment with organizational priorities. Risk management is seamlessly integrated into the CI/CD pipeline and other supplemental and supporting tools used for DevSecOps. For instance, code scanning systems for context sharing, following a shift-left approach to identify and mitigate security risks earlier in the development process.

Security teams utilize automated remediation workflows, behavioral analytics and AI-driven threat intelligence to predict potential security threats before they escalate into incidents. Risk assessments are continuous, automated, and highly contextual, allowing organizations to maintain a resilient and adaptive security posture. Remediation workflows are integrated through formal ticketing and CMDB systems provide context, owners are identified and tagged for accountability and responsibility, prioritization of alerted events are generated based on risk levels.

Optimized (Continuous Feedback Risk Management)

At this stage, risk management is an ongoing, data-driven process, informed by advanced analytics, predictive modeling and continuous feedback from security incidents. Organizations in this stage can automatically reprioritize vulnerabilities as threat landscapes evolve, ensuring that emerging exploits or zero-day vulnerabilities receive immediate attention. The entire pipeline — from code commit to runtime — is enriched with risk analytics, so teams can respond to or even prevent issues before they impact production. Ongoing lessons learned from postmortems and red-team exercises feed into improved threat modeling and more robust controls. This loop of continuous improvement, combined with high automation and collaboration, enables a nearly self-regulating system that minimizes the likelihood and impact of security breaches.

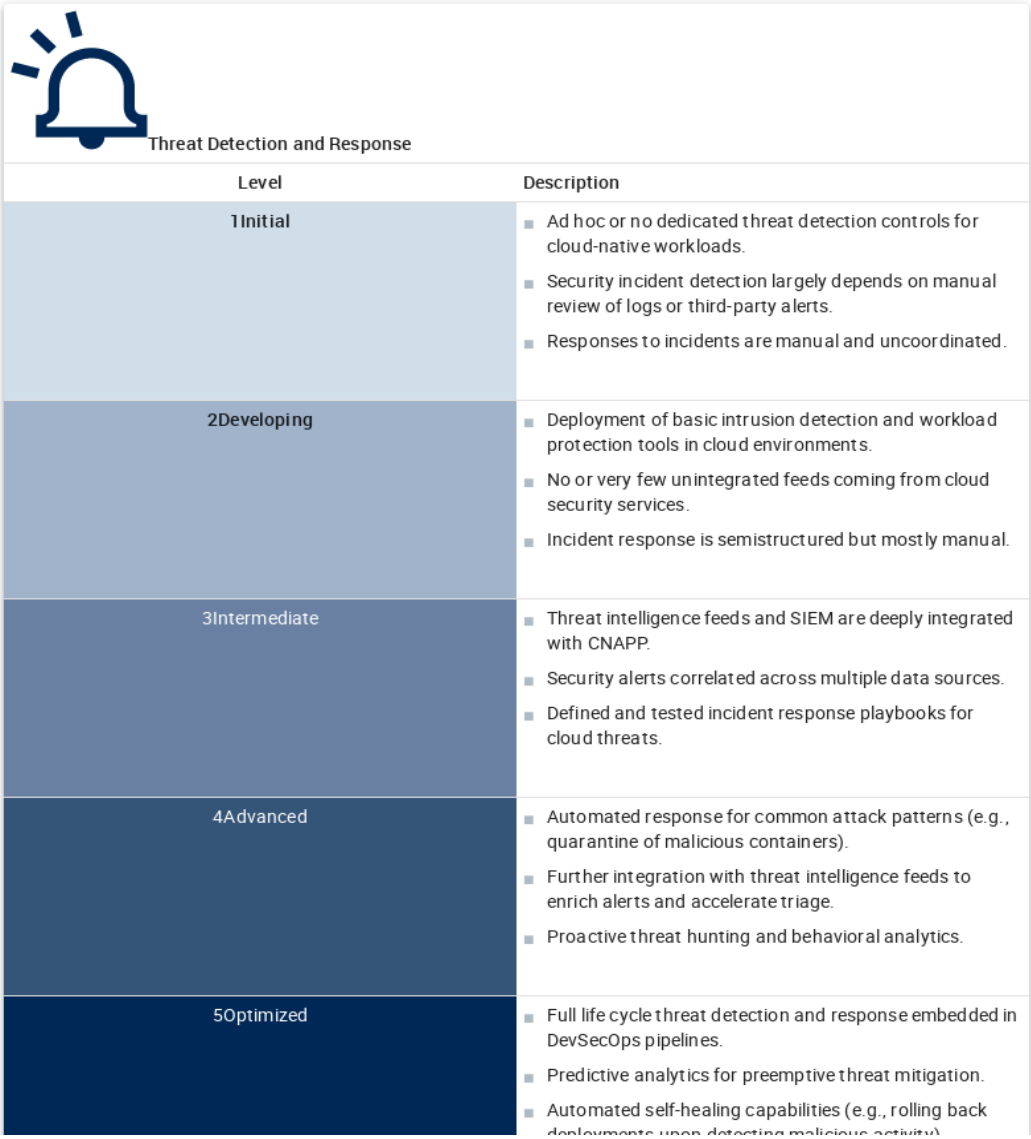
Threat Detection and Response

Back to topThreat detection and response in CNAPP is the practice of continuously monitoring cloud environments. It focuses on establishing processes and technologies that identify risks proactively, correlate security events across different layers of the stack, and initiate automated or well-practiced incident response measures. These capabilities typically include real-time log aggregation, visibility into the runtime states of workloads, anomaly detection and integration with threat intelligence to highlight the most critical threats.

Over time, organizations move from relying solely on reactive alerts to leveraging AI-driven analytics that can predict or pinpoint suspicious activity even before it triggers a traditional signature-based alarm. By evolving threat detection into a proactive discipline — and pairing it with swift, structured incident response — organizations can minimize the impact of cyberattacks, reduce MTTR and maintain confidence in their cloud-native deployments. Table 3 summarizes key aspects of each maturity level in threat detection and response, and is followed by more detailed information.

Table 3: Rate Your Organization's Maturity in Threat Detection and Response

(Enlarged table in Appendix)



Threat Detection and Response

Level	Description
1Initial	■ Ad hoc or no dedicated threat detection controls for cloud-native workloads. ■ Security incident detection largely depends on manual review of logs or third-party alerts. ■ Responses to incidents are manual and uncoordinated.
2Developing	■ Deployment of basic intrusion detection and workload protection tools in cloud environments. ■ No or very few unintegrated feeds coming from cloud security services. ■ Incident response is semistructured but mostly manual.
3Intermediate	■ Threat intelligence feeds and SIEM are deeply integrated with CNAPP. ■ Security alerts correlated across multiple data sources. ■ Defined and tested incident response playbooks for cloud threats.
4Advanced	■ Automated response for common attack patterns (e.g., quarantine of malicious containers). ■ Further integration with threat intelligence feeds to enrich alerts and accelerate triage. ■ Proactive threat hunting and behavioral analytics.
5Optimized	■ Full life cycle threat detection and response embedded in DevSecOps pipelines. ■ Predictive analytics for preemptive threat mitigation. ■ Automated self-healing capabilities (e.g., rolling back deployments upon detecting malicious activity)

Initial (No Formal Threat Detection and Manual Incident Handling)

At this level, organizations lack dedicated threat detection mechanisms including zero visibility of workload activity and behavior at the kernel level, relying only on cloud provider logs or basic security monitoring. Security incidents are handled manually, often going undetected until they cause significant damage.

Threat intelligence is not integrated, and security teams struggle to distinguish real threats from benign activities. There is no automated alert correlation, leading to slow response times and high-risk exposure.

Developing (Basic Security Monitoring)

In the developing stage, organizations implement basic security monitoring. There is a concerted effort to implement basic threat detection tools and techniques, often focusing on workload-based checks.

Security operations teams might consume threat intelligence feeds but lack the capabilities or processes to effectively correlate or contextualize this data across their diverse cloud services. Alerts typically trigger manual investigations, and response times can be slow as teams juggle multiple responsibilities.

While documentation and playbooks may be emerging, they tend to be incomplete or inconsistently applied, resulting in varying outcomes and potential gaps in coverage. While this improves visibility, alerts are often high-volume and lack context, overwhelming security teams. Moreover, they are not prioritized according to risk levels.

Intermediate (Threat Intelligence Integration and Automated Response Playbooks)

At this level, CNAPP deeply integrates with threat intelligence feeds and SIEMs, and automated security workflows are introduced. Security alerts are correlated across multiple sources, reducing false positives and improving incident prioritization.

Automated response playbooks start replacing manual intervention for common threats. Formalized incident response plans and playbooks provide step-by-step guidance, reducing confusion and delays when incidents do occur. In addition, teams may start experimenting with ML models or advanced analytics to detect unusual patterns of behavior, though these capabilities might still be in an early phase. The organization’s response process becomes measurably more efficient, as security personnel can quickly escalate or contain incidents based on documented procedures.

Advanced (Systematic Threat Hunting)

At the advanced stage, threat detection capabilities extend to threat-hunting activities, which systematically search for hidden threats or suspicious patterns in workloads. There is more automation introduced, such as automated responses for common attack patterns (e.g., quarantine of malicious containers). There is also further integration with threat intelligence feeds to enrich alerts and accelerate triage.

Real-time alerting mechanisms feed into established incident response playbooks that have been refined over time, and cross-functional cooperation between development, security, and Ops teams ensures quick, effective mitigation.

Security teams move away from manual log analysis and rely on ML models to detect novel attack techniques.

Optimized (Continuous Adaptation and Self-Improvement)

At the optimized level, threat detection and response reach a state of continuous adaptation and self-improvement.

Threat hunting becomes proactive, with AI-driven analytics continuously scanning for early attack indicators.

Many more response actions — such as blocking unauthorized network connections — are automated, freeing human analysts to focus on higher-level strategy and threat hunting.

The security team regularly updates detection rules and incident playbooks based on real-world incidents, threat intelligence and red-team exercises, creating an environment of perpetual refinement. This high degree of automation and integration makes it exceedingly difficult for malicious actors to remain undetected for long, significantly reducing the overall risk profile of the organization.

Compliance and Governance

Back to top

Compliance and governance in the CNAPP maturity model refers to the frameworks, policies and processes that ensure an organization's cloud-native environments meet both external regulatory obligations and internal standards. This dimension goes beyond merely checking boxes to satisfy auditors; it weaves compliance requirements and governance rules into every stage of the cloud-native life cycle. In traditional settings, compliance checks might happen late in a project's timeline or in response to audits, which often leads to rushed remediations and reactive governance measures. By contrast, cloud-native architectures demand a proactive, integrated approach to governance — one that is capable of adapting as new microservices, containers and serverless functions are continually deployed.

A core element of maturity in this dimension involves the automation of compliance checks and enforcement, reducing the opportunity for human error or oversight. This allows organizations to maintain continuous compliance, catch potential violations early, and provide real-time assurance to stakeholders and regulators. Beyond the technical controls, the compliance and governance dimension also emphasizes cross-functional collaboration, ensuring that development, security, operations, and compliance teams all share accountability for adhering to relevant standards and regulations. By embedding governance throughout the development process, organizations can maintain agility without sacrificing the rigor and reliability required in a dynamic cloud-native environment. Table 4 summarizes key aspects of each maturity level in compliance and governance, and is followed by more detailed information.

Table 4: Rate Your Organization's Maturity in Compliance and Governance

(Enlarged table in Appendix)

Compliance and Governance

Level	Description
1Initial	■ Compliance efforts are fragmented and driven by audits only. ■ Minimal mapping of controls to regulations (e.g., Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act [U.S.] (HIPAA), General Data Protection Regulation (GDPR) in cloud-native contexts. ■ Policies are inconsistent and rarely enforced.
2Developing	■ Basic mapping of essential regulatory requirements to cloud services and workloads. ■ Reactive exception handling. Deviations from policy handled on a case-by-case basis, often with no formal records. ■ Manual control checks for key regulatory frameworks. ■ Policy enforcement is inconsistent across cloud environments.
3Intermediate	■ Structured policy framework covering common compliance standards across cloud environments. ■ Automated compliance checks against defined baselines (e.g., CIS Benchmarks). ■ Governance committees or steering groups formed to oversee policy enforcement and exceptions.
4Advanced	■ Continuous compliance monitoring with real-time dashboards and alerting for policy violations. ■ Integration of compliance checks in CI/CD workflows. ■ Automated remediation of compliance violations.
5Optimized	■ Comprehensive governance model with automated policy as code (PaC) and real-time enforcement. ■ Compliance enforcement is fully automated. ■ Dynamic policy adjustments based on real-time threat intelligence.

Source: Gartner (May 2025)

Initial (Manual Compliance and No Real-Time Governance)

In the initial stage, compliance is handled manually, relying on spreadsheets, periodic audits and reactive assessments. Security policies are not consistently enforced, leading to frequent compliance violations.

Cloud resources are provisioned without proper security governance, meaning that configurations often fail to meet security benchmarks (e.g., United States Department of Commerce National Institute of Standards and Technology [NIST], Center for Internet Security [CIS], International Organization for Standardization [ISO] 27001, Payment Card Industry Data Security Standard [PCI DSS]).

Developing ("Out-of-the-Box" Policies With Reactive Exceptions)

At this stage, organizations begin to rely on default or “out-of-the-box” policies to govern their cloud-native environments, applying basic controls mapped to essential regulatory requirements. Because these policies are not tailored to the specific contexts of different teams or applications, exceptions and deviations frequently occur. In most cases, these deviations are handled reactively and on a case-by-case basis. As a result, any policy exceptions may remain undocumented, making it difficult to pinpoint systemic issues or track recurring patterns over time.

Organizations in the developing stage tend to conduct manual control checks to satisfy only the most pressing regulatory needs, leading to a patchwork approach to compliance. Policy enforcement is inconsistent across multiple cloud platforms and regions, leaving certain environments more vulnerable than others. While this approach may suffice when security requirements are minimal, it poses a significant risk if the organization must scale quickly or faces stringent compliance obligations. As the complexity of the cloud-native stack grows, these ad hoc methods can lead to gaps in visibility, heightened risk and compliance challenges that become harder to address without more proactive governance measures.

Intermediate (Introduction of Continuous Compliance Monitoring)

At this level, organizations begin to implement continuous compliance monitoring using their CNAPP in some environments, ensuring checks are embedded throughout the build, deploy and runtime phases. Security teams integrate automated compliance checks into CI/CD pipelines, issuing warnings or even blocking certain non-compliant deployments before they can reach production. A structured policy framework addresses common industry standards and automated checks against known baselines — like CIS Benchmarks — help maintain consistency.

Governance committees or steering groups formed at this stage oversee policy enforcement and review exceptions, aiming to balance flexibility with robust security practices. As a result, organizations can refine their policies over time based on real-world feedback, ultimately moving closer to a more mature, fully automated compliance posture.

Advanced (Fully Integrated Security Governance)

Organizations now enforce real-time compliance policies fully across multicloud environments, using automated policy enforcement mechanisms with limited exceptions. Security governance is fully integrated with CI/CD pipelines, automatically blocking non-compliant infrastructure deployments. Policies are defined and well-documented, and exclusions and rule changes are taking place when needed. PaC begins to play a role, enforcing security policy across cloud environments

Collaboration between development, security and operations teams is well-established, ensuring faster remediation and alignment with organizational priorities. Risk management is seamlessly integrated into the CI/CD pipeline, following a shift-left approach to identify and mitigate security risks earlier in the development process.

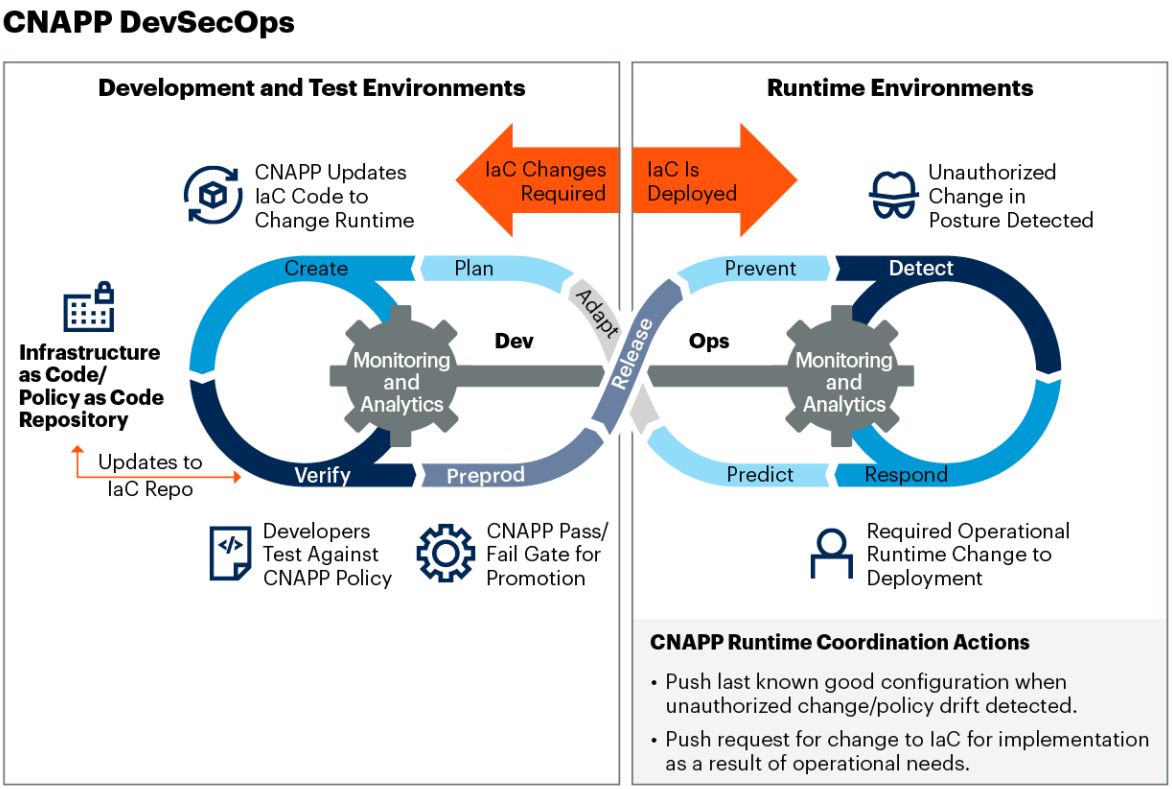
Optimized (Continuous Optimization of Compliance and Governance)

The ongoing process of reducing false positives and reviewing and changing new policies is proactively managed. Continuous compliance is deeply embedded into the organization's processes. Compliance frameworks are dynamically updated and enforced. Policies are continuously optimized based on operational data and threat intelligence. Policies are enforced in real-time, with minimal manual intervention required. PaC plays a significant role in enforcing security policy across cloud environments.

Features in CNAPPs permit the assessment of IaC and PaC configurations throughout the development life cycle. This gives CNAPPs an offline role that allows testing builds against policy before runtime deployment (see Using 'Policy as Code' to Secure Application Deployments and Enforce Compliance). When configured and tuned well, this approach can help to bring the remediation of misconfiguration, vulnerabilities and security issues up to the speed of the DevOps teams.

Figure 5 shows the key capabilities from creation to runtime monitoring. To assure runtime environment immutability, CNAPP actions in runtime must coordinate to update IaC and PaC in order to address operational issues, such as identified misconfigurations, changes to cloud provider settings and vulnerabilities. The updated IaC can then be pushed to runtime at a pace that is aligned with the urgency of the issue at hand. When an unauthorized change is detected, alongside an investigation into the incident, the last known good IaC can be pushed back into runtime to immediately remove potential vulnerabilities and attack paths. Remember that existing DevOps tools offering IaC capabilities, such as IBM (HashiCorp Terraform) and Helm, can also be used to deploy securely to the cloud. Contextual information from these tools should be integrated into CNAPP to enrich the alerts and tickets for communication consistency.

Figure 5: CNAPP DevSecOps



Source: Gartner
791079_C

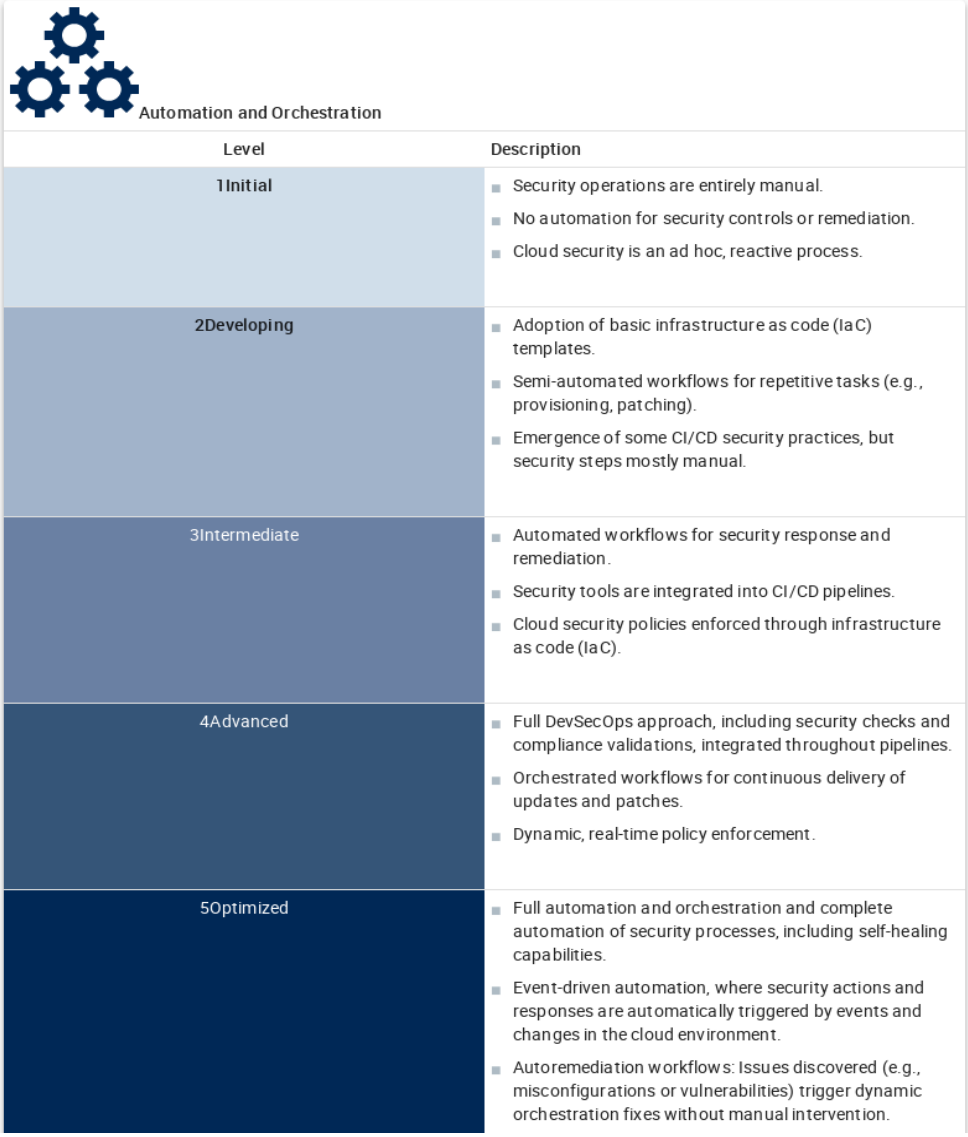
Gartner

Automation and Orchestration

Back to topAutomation and orchestration are essential elements of modern cloud security, aiming to reduce manual effort and enhance efficiency in security operations. The primary objective of automation and orchestration is to establish a self-healing security architecture that lessens the need for manual oversight, accelerates incident response, and guarantees consistent security enforcement across multicloud environments. As cloud platforms grow increasingly complex, organizations that neglect to integrate security automation frequently grapple with alert fatigue, prolonged remediation times and human errors. An effective automation and orchestration strategy can help eliminate repetitive tasks, standardize security enforcement, and facilitate quicker detection and response to threats. Nonetheless, many organizations encounter obstacles in embracing automation due to outdated processes, a lack of expertise, or fear of disrupting business operations. Table 5 summarizes key aspects of each maturity level in automation and orchestration, and is followed by more detailed information.

Table 5: Rate Your Organization's Maturity in Automation and Orchestration

(Enlarged table in Appendix)



Automation and Orchestration

Level	Description
1Initial	■ Security operations are entirely manual. ■ No automation for security controls or remediation. ■ Cloud security is an ad hoc, reactive process.
2Developing	■ Adoption of basic infrastructure as code (IaC) templates. ■ Semi-automated workflows for repetitive tasks (e.g., provisioning, patching). ■ Emergence of some CI/CD security practices, but security steps mostly manual.
3Intermediate	■ Automated workflows for security response and remediation. ■ Security tools are integrated into CI/CD pipelines. ■ Cloud security policies enforced through infrastructure as code (IaC).
4Advanced	■ Full DevSecOps approach, including security checks and compliance validations, integrated throughout pipelines. ■ Orchestrated workflows for continuous delivery of updates and patches. ■ Dynamic, real-time policy enforcement.
5Optimized	■ Full automation and orchestration and complete automation of security processes, including self-healing capabilities. ■ Event-driven automation, where security actions and responses are automatically triggered by events and changes in the cloud environment. ■ Autoremediation workflows: Issues discovered (e.g., misconfigurations or vulnerabilities) trigger dynamic orchestration fixes without manual intervention.

Initial (Manual Security Operations and Siloed Processes)

At this level, security operations remain entirely manual, with no automation implemented. Security teams must analyze security alerts, investigate incidents and enforce policies manually. This results in slow response times, human errors and operational inefficiencies. Cloud security is reactive, which means issues are addressed only after an incident occurs, rather than being managed proactively. Inconsistent security policies and misconfigurations are prevalent, which increases the attack surface.

Organizations at this stage generally lack integration among their security tools, meaning that tools operate in silos without centralized coordination. Consequently, security teams face alert overload and often miss critical threats due to excessive manual triaging and response efforts.

Developing (Basic Security Automation and Scripted Workflows)

At this stage, organizations begin adopting basic automation techniques to manage routine security tasks. Although automation is being introduced, it remains confined to specific use cases and lacks full integration across the security ecosystem. Orchestration is still missing, which means that security automation efforts are fragmented and not centrally managed. Organizations may also start utilizing security-as-code approaches, but policies are enforced inconsistently, and workflows still require significant human intervention.

At this stage, automation slightly enhances operational efficiency, but it does not significantly lessen the manual workload or improve incident response times. The organization continues to rely heavily on security analysts to review and validate security alerts, investigate incidents, and initiate remediation actions.

Intermediate (Integrated Automation and Policy Enforcement Through IaC)

As organizations mature, they progress toward centralized automation and policy-based security enforcement. At this stage, they integrate security automation into CI/CD pipelines, ensuring that security checks occur before workloads are deployed. A key characteristic of this stage is the adoption of IaC and PaC frameworks, such as Terraform, Amazon Web Services (AWS) CloudFormation and Open Policy Agent (OPA). This enables security teams to enforce security policies dynamically and consistently across cloud environments. Security workflows also become more streamlined and automated, minimizing the need for human intervention in repetitive security tasks. Organizations incorporate CSPM tools to automatically detect misconfigurations. Although automation is developing, incident response still necessitates human decision making, with security teams responsible for manually approving or modifying automated remediation actions.

Advanced (End-to-End Security Orchestration)

At the advanced maturity stage, organizations achieve full security orchestration, meaning that security tools and automation workflows are fully integrated and centrally managed. AI-driven security analytics assist in identifying emerging threats, correlating alerts across multiple sources and predicting potential attack vectors. Organizations also implement behavior-based anomaly detection to spot zero-day threats and insider attacks.

At this level, security automation is no longer confined to predefined scripts; it is adaptive, dynamic and responsive to real-time security events. Security policies are continuously updated based on threat intelligence feeds, compliance requirements and evolving risk landscapes. Furthermore, organizations achieve near real-time remediation of security threats, reducing the mean time to detect (MTTD) and mean time to respond (MTTR) to threats. Security teams transition from being reactive incident responders to proactive risk managers, concentrating on higher-level security strategies rather than manual security operations.

Optimized (Automated Preemptive Cloud Security Operations)

At the highest level of maturity, organizations achieve high levels of automation, meaning that security systems operate with minimal human intervention. Security automation at this level is not just reactive; it is predictive and preemptive. AI models analyze past attack patterns, environmental changes, and system behavior to anticipate potential vulnerabilities or breaches before they happen. This allows organizations to neutralize threats before they escalate into security incidents.

Compliance enforcement is also fully automated, dynamically adjusting policies to meet evolving regulatory requirements. Governance frameworks operate autonomously, ensuring that security configurations remain compliant across all cloud environments, business units and geographic regions.

At this stage, security teams prioritize ongoing optimization, proactive risk mitigation and innovative security solutions over manually managing routine security tasks. The organization's cloud security infrastructure is resilient, adaptable and continually evolving, ensuring it stays ahead of emerging cyberthreats.

What Level of CNAPP Maturity Is Most Suitable for Your Organization?

Determining the right CNAPP maturity level to target depends on several factors unique to your organization, including its size, industry, regulatory obligations and existing security posture. Smaller organizations or startups operating in less regulated sectors might initially aim for a mid-level maturity — such as Level 3 (Intermediate) — so they can balance basic security requirements with the need for agility. Conversely, enterprises dealing with strict compliance mandates or managing critical infrastructure may need to progress more rapidly toward higher levels, ensuring that advanced capabilities like automated detection,PaC and continuous compliance checks are fully implemented. It's ok to select a target profile that is less than all Level 5s to reflect all of these factors and organizational risk appetite.

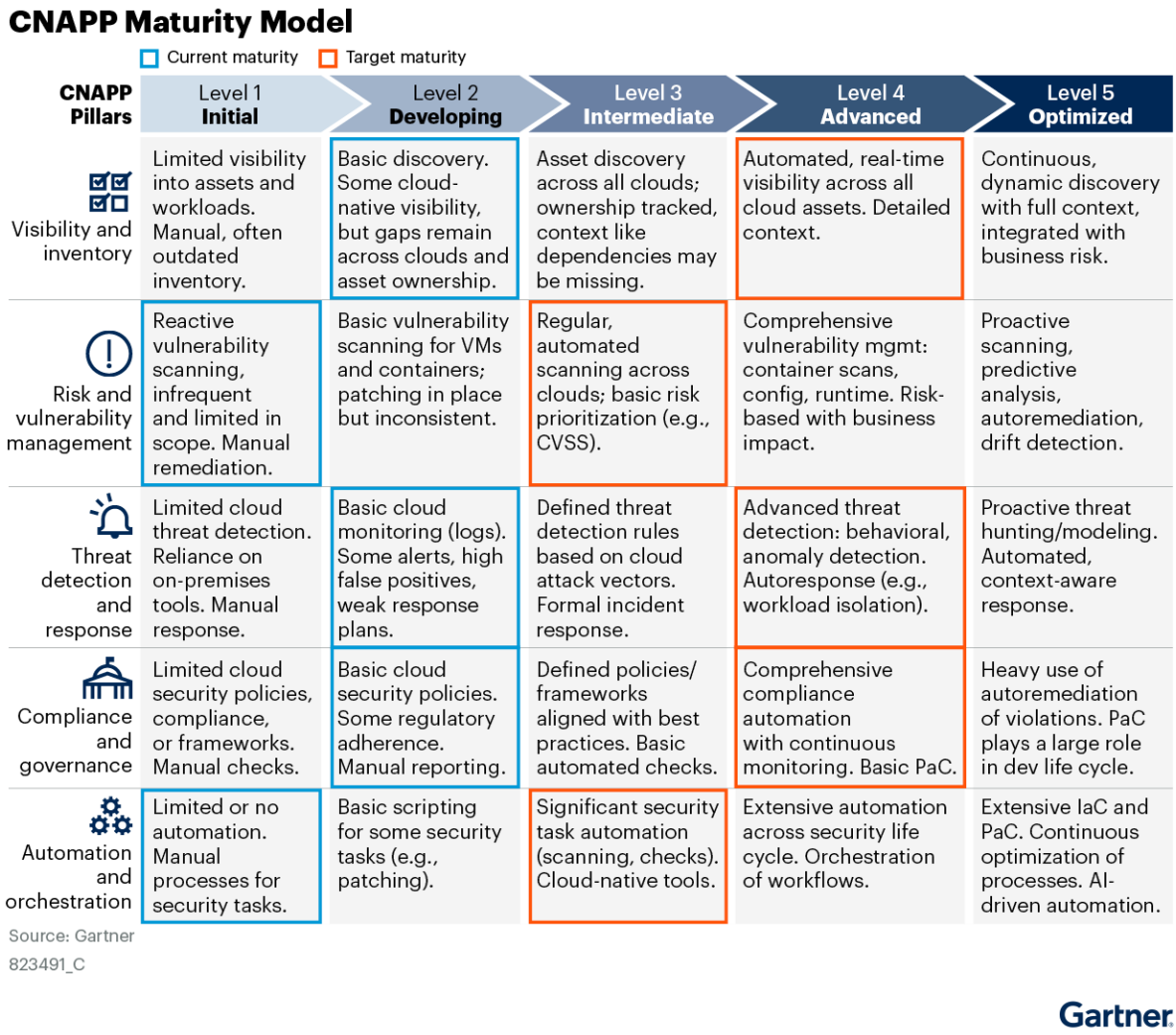
It's important to perform a thorough gap analysis against the CNAPP maturity model to identify areas of risk, inefficiency, or missed opportunities. This assessment helps you prioritize improvements based on available resources and the potential impact on your business. Keep in mind that organizations rarely advance uniformly across all dimensions at once — one team may already be advanced in threat detection while another still struggles with asset inventory. By targeting the CNAPP level that best aligns with your current capabilities and risk tolerance, you can build a clear, step-by-step roadmap for evolving your cloud-native security strategy over time, without overwhelming your team or sacrificing everyday operations.

This framework enables organizations to assess their current maturity, identify gaps and prioritize improvements across five dimensions.

Step 1: Assess Current Maturity Level

Figure 6 provides a sample maturity assessment by pillar, with the current level highlighted in blue and the target level in orange.

Figure 6: Sample Maturity Assessment by Pillar



CNAPP Maturity Model

Current maturity Target maturity

CNAPP Pillars	Level 1 Initial	Level 2 Developing	Level 3 Intermediate	Level 4 Advanced	Level 5 Optimized
Visibility and inventory	Limited visibility into assets and workloads. Manual, often outdated inventory.	Basic discovery. Some cloud-native visibility, but gaps remain across clouds and asset ownership.	Asset discovery across all clouds; ownership tracked, context like dependencies may be missing.	Automated, real-time visibility across all cloud assets. Detailed context.	Continuous, dynamic discovery with full context, integrated with business risk.
Risk and vulnerability management	Reactive vulnerability scanning, infrequent and limited in scope. Manual remediation.	Basic vulnerability scanning for VMs and containers; patching in place but inconsistent.	Regular, automated scanning across clouds; basic risk prioritization (e.g., CVSS).	Comprehensive vulnerability mgmt: container scans, config, runtime. Risk-based with business impact.	Proactive scanning, predictive analysis, autoremediation, drift detection.
Threat detection and response	Limited cloud threat detection. Reliance on on-premises tools. Manual response.	Basic cloud monitoring (logs). Some alerts, high false positives, weak response plans.	Defined threat detection rules based on cloud attack vectors. Formal incident response.	Advanced threat detection: behavioral, anomaly detection. Autoresponse (e.g., workload isolation).	Proactive threat hunting/modeling. Automated, context-aware response.
Compliance and governance	Limited cloud security policies, compliance, or frameworks. Manual checks.	Basic cloud security policies. Some regulatory adherence. Manual reporting.	Defined policies/ frameworks aligned with best practices. Basic automated checks.	Comprehensive compliance automation with continuous monitoring. Basic PaC.	Heavy use of autoremediation of violations. PaC plays a large role in dev life cycle.
Automation and orchestration	Limited or no automation. Manual processes for security tasks.	Basic scripting for some security tasks (e.g., patching).	Significant security task automation (scanning, checks). Cloud-native tools.	Extensive automation across security life cycle. Orchestration of workflows.	Extensive IaC and PaC. Continuous optimization of processes. AI-driven automation.

Source: Gartner
823491_C

Gartner

Step 2: Identify Key Gaps and Challenges

Once you've rated each dimension, document the gaps preventing progression to the next level.

Example:

- **Visibility and inventory:** Lack of real-time asset discovery and inventory across all cloud environments. Infrastructure and workload ownership is not carefully monitored resulting in a lack of accountability and responsibility.
- **Risk management:** No regular, automated vulnerability scanning across all cloud environments

- **Threat detection and response:** No defined threat detection rules and policies based on common cloud attack vectors or formalized incident response procedures. No automated threat response capabilities (e.g., workload isolation).
- **Compliance and governance:** No defined security policies and compliance frameworks aligned with industry best practices and regulations.
- **Automation and orchestration:** Limited security automation; remediation is manual.

Step 3: Prioritize Improvements Using an Impact Versus Effort Approach

Focus on high-impact, low-effort initiatives first. Use the impact versus effort matrix to prioritize actions. Prioritizing improvements using an impact versus effort approach allows organizations to concentrate on initiatives that offer significant benefits without consuming excessive time or resources. By plotting potential actions on the impact versus effort matrix, teams can quickly identify high-impact, low-effort opportunities that deliver rapid gains (see Table 6). Because each organization's environment, risk tolerance, budget and internal expertise differ, the outcomes of such an assessment will vary. A high-impact initiative for one company might be less urgent for another due to dissimilar infrastructure or compliance needs. Ultimately, this method ensures that investments in CNAPP maturity are optimized, driving meaningful progress before tackling more complex, resource-intensive projects.

Table 6: Prioritize Improvements Using an Impact Versus Effort Approach

(Enlarged table in Appendix)

Initiative	Impact (High/Medium/Low)	Effort (High/Medium/Low)	Priority (1-5,1=Highest)
Implement real-time cloud asset discovery	High	Low	1
Deploy automated vulnerability scanning across all cloud environments	High	Low	2
Carefully monitor Infrastructure ownership	High	Medium	3
Define threat detection rules and policies based on common cloud attack vectors.	Medium	Medium	4
Basic scripting for some security tasks	Low	Low	5
Formalized incident response procedures	Medium	Medium	6
Implement automated threat response capabilities (e.g., workload isolation).	High	High	7
Policy-as-code for consistent enforcement begins to play a role.	High	High	8

Source: Gartner (May 2025)

Recommendations

To improve their organization's CNAPP maturity, security architects must follow these key recommendations.

Starting Out — Early Wins at Level 1 (Initial) and Level 2 (Developing)

Organizations operating at Levels 1 (Initial) and 2 (Developing) typically face significant visibility and process challenges. However, there are several "early wins" that can quickly improve their security posture without requiring a complete overhaul of existing operations. For instance, establishing a basic but consistent asset inventory helps teams understand what resources they have and where potential risks may exist. Even a simplified, centralized log collection process can create a single source of truth for events, enabling quicker and more accurate root-cause analysis when issues arise.

Another area for early improvement is the adoption of lightweight security checks within existing workflows. Developers at these early maturity levels can integrate basic vulnerability scans into their CI/CD pipelines with minimal disruption, detecting issues before they propagate into production. Additionally, promoting cross-functional communication — through short, frequent stand-ups or shared dashboards — reduces silos and encourages a unified approach to addressing security gaps. While these steps alone won't solve all challenges at Level 1 or Level 2, they create the momentum needed to evolve toward more mature, proactive security practices in cloud-native environments.

Key Early Wins at Level 1 and 2

- **Achieve complete environment coverage:** Implement discovery tools to map every region and workload, ensuring full transparency in dynamic cloud environments.
- **Identify clear asset ownership:** Track ownership details (e.g., department, project, business unit), streamlining accountability and remediation.
- **Remediate the most severe issues:** Prioritize flaws with the highest likelihood of exploitation or largest potential impact to protect essential assets.
- **Utilize CNAPP capabilities to contextualize and prioritize:** Utilize advanced CNAPP features like attack path analysis that help contextualize and prioritize risk in new ways (as seen in Figure 6) to target the most severe risks (see 5 Ways CNAPP Will Improve Your Cloud Security for more on CNAPP prioritization capabilities).
- **Automation and orchestration:** Begin to look for ways to automate and orchestrate security. Start understanding your development pipelines and look for opportunities to start some basic scripting for some security tasks.

Improve All the Low-Maturity Dimensions to Level 3 to Lay the Foundations of CNAPP

Achieving Level 3 (Intermediate) maturity in all low-maturity CNAPP dimensions sets a crucial foundation for a secure, scalable and future-ready cloud environment. At this stage, organizations establish consistent processes and tools that enable them to maintain visibility, manage risk, detect threats, govern compliance and orchestrate workloads more reliably. By aligning each dimension to at least Level 3, teams move past ad hoc, siloed practices and embrace a systematic approach that cuts across development, operations, and security.

Leaving any single dimension at a much lower level than others, can create bottlenecks that stall progress in other areas, no matter how advanced they may be. For instance, lacking basic visibility or a centralized inventory of cloud assets can undermine effective risk management, since security teams cannot accurately assess vulnerabilities. Similarly, if threat detection remains reactive and underdeveloped, even robust automation or compliance processes may fail to catch critical issues in time. Each CNAPP dimension is interconnected — the shortfalls of one invariably weaken the others. Therefore, advancing to higher levels in one dimension frequently relies on laying at least a foundational maturity level in the others.

The transition to Level 3 often involves formalizing policies, integrating automated scans or checks into CI/CD pipelines, and consolidating tools for centralized logging and event management. Instead of merely reacting to issues, organizations begin to proactively identify and address emerging problems. For example, a single source of truth for asset inventory helps both security and operations teams rapidly spot misconfigurations, while a unified compliance dashboard ensures no critical gaps remain hidden. These capabilities reduce operational overhead by standardizing processes and clarifying responsibilities across departments.

From an organizational perspective, elevating all dimensions to Level 3 promotes collaboration and consistency. When security requirements are embedded from the start, developers and engineers spend less time fixing last-minute vulnerabilities or dealing with surprise compliance audits. Automated workflows enhance productivity and help maintain continuous, data-driven improvements. Ultimately, a solid Level 3 foundation lays the groundwork for higher levels of CNAPP maturity, where advanced analytics, self-healing systems and PaC solutions become attainable and sustainable.

Key Actions to Advance to Intermediate (Level 3)

- **Standardize risk assessment and prioritization:** Have regular, automated vulnerability scanning across all cloud environments. Ensure prioritization based on basic risk factors and business impact to prioritize remediation effectively.
- **Automate inventory and asset discovery:** Move from manual asset tracking to an automated discovery process that continuously updates cloud resources. Implement asset discovery and inventory across all cloud environments. Ensure that infrastructure ownership is carefully monitored.

- **Develop incident response procedures:** Set defined threat detection rules and policies based on common cloud attack vectors. Ensure integration with SIEM and formalized incident response procedures.
- **Compliance and Governance:** Set defined security policies and compliance frameworks aligned with industry best practices and regulations. Ensure automated compliance checks with basic reporting.
- **Integrate Security into CI/CD Pipelines:** Implement significant automation of security tasks (e.g., vulnerability scanning, compliance checks), ensuring security issues are addressed before deployment.

Mastering Cloud-Native Security: Achieving Maturity Levels 4 and 5 with Automation and Integration

Reaching Levels 4 (Advanced) and 5 (Optimized) within the CNAPP maturity model represents a pivotal shift from reactive security measures to a seamlessly integrated, proactive approach. At Level 4, organizations harness automation to continuously validate configurations, scan for vulnerabilities and enforce policies across multicloud or hybrid environments. Teams move beyond detecting issues in production by embedding security into every phase of the DevOps pipeline, including build, deploy and runtime stages. This deep integration of security controls, guided by agile collaboration between development and operations, accelerates responses to emerging threats while reducing the overhead of manual intervention.

By progressing to Level 5, organizations fully optimize their cloud-native security posture. At this level of maturity, governance committees and cross-functional teams use data-driven insights to refine policies continuously, ensuring minimal downtime and streamlined compliance. Level 5 environments thus embody a culture of constant evolution and adaptation, where security is not a separate process but an intrinsic aspect of cloud-native application development and operations.

Key Actions to Advance to Levels 4 and 5

- **Enhance cross-team collaboration:** Establish clear roles and responsibilities for security, development and operations teams, fostering a shared security culture through regular security reviews and training.
- **Fully integrated security in DevOps:** Embed security tests and checks at every stage of the software development life cycle (build, test, deploy and runtime), minimizing the risk of late-stage discoveries.

- **Dynamic policy enforcement:** Use policy-as-code frameworks to automatically apply security standards, preventing non-compliant workloads from being deployed.
- **Extensive automation:** Establish automation across the security life cycle, including threat detection, response and remediation. Ensure orchestration of security workflows.
- **Continuous validation of configurations:** Automate checks for configurations, policies and compliance requirements across multiple cloud environments to ensure immediate detection of misconfigurations.

Conclusion

The Gartner CNAPP maturity model offers a structured path toward robust, adaptable security in today's dynamic cloud environments. By advancing through stages of visibility and inventory, risk management, threat detection and response, compliance and governance, and automation and orchestration, organizations progressively reduce risk and enhance resilience. Each dimension's maturity evolves from basic, manual approaches to automated strategies. Constant assessment, clear roadmaps, and periodic reviews ensure continuous improvement and alignment with evolving threats from code to cloud.

Note 1: Sample Vendors

Table 7 has a list of sample vendors offering CNAPP solutions; it is not exhaustive nor does it indicate any Gartner endorsement.

Table 7: Example CNAPP Vendors

(Enlarged table in Appendix)

Vendor	Offering
Aqua Security	Cloud Native Application Security
CrowdStrike	CrowdStrike Falcon Cloud Security
Cyscale	Cyscale Cloud-Native Application Protection Platform (CNAPP)
Datadog	Datadog Cloud-Native Application Protection Platform (CNAPP)
Data Theorem	Cloud Secure
Fortinet	FortiCNAPP
Google Cloud	Google Cloud Security Command Center
Microsoft	Microsoft Defender for Cloud
Orca Security	Orca Cloud Native Application Protection Platform
Palo Alto Networks	Cortex Cloud
Qualys	Qualys TotalCloud
Rapid7	InsightCloudSec
SentinelOne	Singularity Cloud Security
Sophos	Sophos Cloud Native Security
Sysdig	Sysdig Secure
Tenable	Tenable Cloud Security
Trend Micro	Trend Vision One – Cloud Security
Uptycs	Uptycs Cloud-Native Application Protection Platform (CNAPP)
Wiz	Wiz CNAPP

Source: Gartner (May 2025)

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Reference Architecture Brief: Cloud Security

Secure Azure Resources Using Microsoft Defender for Cloud

5 Ways CNAPP Will Improve Your Cloud Security

How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB

Solution Criteria for Cloud Security Posture Management (CSPM)

Market Guide for Cloud-Native Application Protection Platforms

Advance Your Platform-as-a-Service Security

Essential Skills for Cloud Security Architects

Guide to Cloud and Infrastructure Security Concepts

Solution Path for Security in the Public Cloud

Table 1: Rate Your Organization's Maturity in Visibility and Inventory

Visibility and Inventory

Level	Description
1Initial	■ Limited or no visibility into cloud assets and workloads. ■ Manual inventory management, often outdated. ■ Cloud assets are deployed without centralized oversight, creating gaps in visibility around ownership and security posture. ■ Security teams conduct point-in-time audits using CNAPP, which remain time-consuming and unreliable due to manual, fragmented asset discovery.
2Developing	■ Basic asset discovery. ■ Not all cloud environments in CNAPP. ■ Linking assets to their respective owners is also inconsistent. ■ Limited context; offers basic asset information (e.g., name, region, type), but lacks relationships and dependencies.
3Intermediate	■ Asset discovery and inventory across all cloud environments.

	■ Infrastructure and application ownership is carefully monitored. ■ Improved CNAPP context, including information on ownership, configurations, tags, security groups and network connectivity.
4Advanced	■ Automated, real-time full life cycle tracking from build to runtime for every asset. ■ Detailed context, including application mapping, relationships and dependencies including capabilities such software composition analysis (SCA) and software bill of materials creation (SBOM). ■ Inventory data is integrated with other IT management systems, such as CMDB/ITSM, for a holistic view.
5Optimized	■ Fully automated discovery with continuous tracking, labeling and integration into CMDB or single source of truth. ■ Automated actions can be triggered based on inventory changes (e.g., quarantining a newly discovered, unapproved resource). ■ Visibility and inventory seamlessly feed other security functions (risk scoring, compliance checks and threat detection).

Source: Gartner (May 2025)

Table 2: Rate Your Organization's Maturity Risk and Vulnerability Management

Risk and Vulnerability Management

Level	Description
1Initial	■ No formal risk assessment framework for cloud-native environments. ■ Reactive risk identification and remediation, usually after incidents occur. ■ No visibility into cloud-specific risks (e.g., misconfigurations, overpermissioned accounts).
2Developing	■ Basic vulnerability scanning for cloud workloads. ■ Security policies exist but are inconsistently enforced. ■ Manual prioritization focusing on major known risks.
3Intermediate	■ Risk-based prioritization implemented for cloud vulnerabilities, guided by threat intelligence and business impact. ■ Defined risk tolerance levels for cloud security issues. ■ Automated misconfiguration scanning with policy enforcement.
4Advanced	■ Integration of risk management into the CI/CD pipeline and ticketing

	systems to augment and enrich initial workflows for remediation. ■ Automated policy checks and gating to prevent high-risk vulnerabilities from progressing. ■ Continuous risk scoring and reporting to stakeholders with near real-time updates.
5Optimized	■ Holistic, adaptive risk management, integrated with DevSecOps practices and real-time cloud posture management. ■ AI/ML-driven analysis for predictive risk assessment and autoremediation. ■ Ongoing lessons learned from postmortems and red-team exercises feed into improved threat modeling and more robust controls.

Source: Gartner (May 2025)

Table 3: Rate Your Organization's Maturity in Threat Detection and Response

Threat Detection and Response

Level	Description
1Initial	■ Ad hoc or no dedicated threat detection controls for cloud-native workloads. ■ Security incident detection largely depends on manual review of logs or third-party alerts. ■ Responses to incidents are manual and uncoordinated.
2Developing	■ Deployment of basic intrusion detection and workload protection tools in cloud environments. ■ No or very few unintegrated feeds coming from cloud security services. ■ Incident response is semistructured but mostly manual.
3Intermediate	■ Threat intelligence feeds and SIEM are deeply integrated with CNAPP. Security alerts correlated across multiple data sources.

	■ Defined and tested incident response playbooks for cloud threats.
4Advanced	■ Automated response for common attack patterns (e.g., quarantine of malicious containers). ■ Further integration with threat intelligence feeds to enrich alerts and accelerate triage. ■ Proactive threat hunting and behavioral analytics.
5Optimized	■ Full life cycle threat detection and response embedded in DevSecOps pipelines. ■ Predictive analytics for preemptive threat mitigation. ■ Automated self-healing capabilities (e.g., rolling back deployments upon detecting malicious activity).

Source: Gartner (May 2025)

Table 4: Rate Your Organization's Maturity in Compliance and Governance

Compliance and Governance	
Level	**Description**
1Initial	■ Compliance efforts are fragmented and driven by audits only. ■ Minimal mapping of controls to regulations (e.g., Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act [U.S.] (HIPAA), General Data Protection Regulation (GDPR) in cloud-native contexts. ■ Policies are inconsistent and rarely enforced.
2Developing	■ Basic mapping of essential regulatory requirements to cloud services and workloads. ■ Reactive exception handling. Deviations from policy handled on a case-by-case basis, often with no formal records. ■ Manual control checks for key regulatory frameworks. ■ Policy enforcement is inconsistent across cloud environments.
3Intermediate	■ Structured policy framework covering common compliance standards across cloud environments.

	■ Automated compliance checks against defined baselines (e.g., CIS Benchmarks). ■ Governance committees or steering groups formed to oversee policy enforcement and exceptions.
4Advanced	■ Continuous compliance monitoring with real-time dashboards and alerting for policy violations. ■ Integration of compliance checks in CI/CD workflows. ■ Automated remediation of compliance violations.
5Optimized	■ Comprehensive governance model with automated policy as code (PaC) and real-time enforcement. ■ Compliance enforcement is fully automated. ■ Dynamic policy adjustments based on real-time threat intelligence.

Source: Gartner (May 2025)

Table 5: Rate Your Organization's Maturity in Automation and Orchestration

Automation and Orchestration

Level	Description
1Initial	■ Security operations are entirely manual. ■ No automation for security controls or remediation. ■ Cloud security is an ad hoc, reactive process.
2Developing	■ Adoption of basic infrastructure as code (IaC) templates. ■ Semi-automated workflows for repetitive tasks (e.g., provisioning, patching). ■ Emergence of some CI/CD security practices, but security steps mostly manual.
3Intermediate	■ Automated workflows for security response and remediation. ■ Security tools are integrated into CI/CD pipelines. ■ Cloud security policies enforced through infrastructure as code (IaC).

4Advanced	■ Full DevSecOps approach, including security checks and compliance validations, integrated throughout pipelines. ■ Orchestrated workflows for continuous delivery of updates and patches. ■ Dynamic, real-time policy enforcement.
5Optimized	■ Full automation and orchestration and complete automation of security processes, including self-healing capabilities. ■ Event-driven automation, where security actions and responses are automatically triggered by events and changes in the cloud environment. ■ Autoremediation workflows: Issues discovered (e.g., misconfigurations or vulnerabilities) trigger dynamic orchestration fixes without manual intervention.

Source: Gartner (May 2025)

Table 6: Prioritize Improvements Using an Impact Versus Effort Approach

Initiative	Impact (High/Medium/Low)	Effort (High/Medium/Low)	Priority (1-5,1=Highest)
Implement real-time cloud asset discovery	High	Low	1
Deploy automated vulnerability scanning across all cloud environments	High	Low	2
Carefully monitor Infrastructure ownership	High	Medium	3
Define threat detection rules and policies based on common cloud attack vectors.	Medium	Medium	4
Basic scripting for some security tasks	Low	Low	5
Formalized incident response procedures	Medium	Medium	6
Implement automated threat response capabilities (e.g., workload isolation).	High	High	7
Policy-as-code for consistent enforcement begins to play a role.	High	High	8

Source: Gartner (May 2025)

Table 7: Example CNAPP Vendors

Vendor	Offering
Aqua Security	Cloud Native Application Security
CrowdStrike	CrowdStrike Falcon Cloud Security
Cyscale	Cyscale Cloud-Native Application Protection Platform (CNAPP)
Datadog	Datadog Cloud-Native Application Protection Platform (CNAPP)
Data Theorem	Cloud Secure
Fortinet	FortiCNAPP
Google Cloud	Google Cloud Security Command Center
Microsoft	Microsoft Defender for Cloud
Orca Security	Orca Cloud Native Application Protection Platform
Palo Alto Networks	Cortex Cloud
Qualys	Qualys TotalCloud
Rapid7	InsightCloudSec
SentinelOne	Singularity Cloud Security
Sophos	Sophos Cloud Native Security
Sysdig	Sysdig Secure

Tenable	Tenable Cloud Security
Trend Micro	Trend Vision One — Cloud Security
Uptycs	Uptycs Cloud-Native Application Protection Platform (CNAPP)
Wiz	Wiz CNAPP

Source: Gartner (May 2025)