The Complete Guide to CNAPPs

CROWDSTRIKE

What You'll Learn in This Guide

Throughout this guide, we look at how CNAPPs help security, DevSecOps and DevOps teams excel by providing them with the capabilities they need to decipher the massive datasets CNAPPs capture and analyze every day.

This complete guide is your roadmap for understanding CNAPPs. You'll get firsthand knowledge of how CNAPPs deliver business benefits by eliminating blind spots and reducing breach risks while increasing productivity. You'll see how CNAPPs integrate security throughout the software development life cycle (SDLC), simplifying the process of monitoring, analyzing and acting on cloud security threats. A major goal of this guide is to provide an introduction to how CNAPPs work, including their many moving parts.

You'll also get a clear view of the many challenges that CNAPPs address, such as the challenge to keep up with constant innovation while ensuring security — an issue many DevSecOps and DevOps teams face.

Table of Contents

Chapter 1

Defining CNAPP

Cloud applications are the rocket fuel that keeps companies growing, empowering them to serve customers in new, exciting and personalized ways. The most innovative and fast-moving companies on the planet have turned cloud app development into an art form. It’s core to who they are. Their cloud apps and the experiences they deliver are in their DNA.

Securing the development process for cloud apps is a critical part of fueling constant innovation. That’s where cloud-native application protection platforms (CNAPPs) come in. These platforms are designed to close the security gaps that have emerged from piecemeal cloud security adoption, which often involve multiple siloed solutions.

As organizations continue to build out their cloud infrastructure, the threat to cloud environments grows. Today’s adversaries are on the hunt for any weakness they can exploit to access an organization and its systems, applications and data — and more often, they are targeting the cloud. Shutting them down with a CNAPP solution is a must to protect your company’s most valuable assets and resources. Customers trust you more when your cloud applications are secure.

A solid cloud security strategy helps accelerate application development and delivers higher-quality code. When a CNAPP is in place, protecting the workflow of application creation — often called the continuous integration/continuous delivery (CI/CD) process — DevSecOps and other teams benefit from a secured workspace to move quickly and build new apps.

Terms to Know

DevOps is the convergence of development and operations. It is defined as a software engineering methodology that aims to integrate the work of development teams and operations teams by facilitating a culture of collaboration and shared responsibility.

DevSecOps is DevOps with security embedded throughout every stage of the software development life cycle. This is an approach to culture, automation and platform design that integrates security as a shared responsibility.

CI/CD is a software development practice in which code changes are continuously tested, compiled and deployed to production. Think of CI/CD as the workflows that guide how cloud apps are built.

What Is a CNAPP?

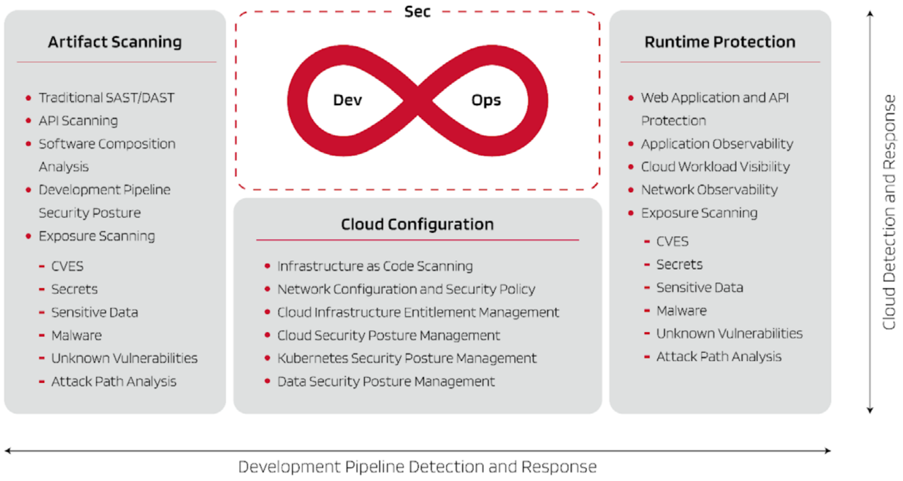
A CNAPP is best defined as an all-in-one cloud-native software platform that simplifies monitoring, detecting and acting on potential cloud security threats and vulnerabilities. Think of a CNAPP as the glue that keeps a wide variety of security apps all unified on a single platform, sharing data and insights in real time.

A CNAPP is a tightly integrated set of security and compliance capabilities designed to protect cloud-native applications throughout development and production. The popularity of CNAPPs is growing because they provide what DevSecOps and DevOps teams need to keep their app development secure and moving smoothly through the CI/CD process. The goal of a CNAPP is to bring visibility to the blind spots that attackers take advantage of to break into cloud systems' databases — or inject malicious code into DevOps coding cycles.

CNAPPs are security solutions that consolidate various security capabilities such as container scanning, cloud security posture management (CSPM), cloud workload protection (CWP), infrastructure-as-code (IaC) scanning, cloud infrastructure entitlement management (CIEM), application security posture management (ASPM), data security posture management (DSPM), runtime cloud workload protection and runtime vulnerability/configuration scanning. Figure 1 shows how CNAPPs orchestrate threat data using artifact scanning, cloud configuration apps and a series of runtime protections, all aimed at providing real-time threat detection and response.

DevSecOps teams are “all in” on CNAPP because it keeps their fast-moving code efforts secure and allows them to keep moving new apps and features through to testing and launch. At the core of the CNAPP architecture is CI/CD, the infinite loop shown at the top center of Figure 1.

CNAPP Detailed View



Sec
Dev
Ops
Cloud Detection and Response
Development Pipeline Detection and Response

Artifact Scanning

- Traditional SAST/DAST
- API Scanning
- Software Composition Analysis
- Development Pipeline Security Posture
- Exposure Scanning
  - CVES
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

Cloud Configuration

- Infrastructure as Code Scanning
- Network Configuration and Security Policy
- Cloud Infrastructure Entitlement Management
- Cloud Security Posture Management
- Kubernetes Security Posture Management
- Data Security Posture Management

Runtime Protection

- Web Application and API Protection
- Application Observability
- Cloud Workload Visibility
- Network Observability
- Exposure Scanning
  - CVES
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

CVEs = common vulnerabilities and exposures

Figure 1. Detailed view of CNAPP capabilities as defined by Gartner
Source: Gartner, Market Guide for Cloud-Native Application Protection Platforms, 14 March 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

As more organizations adopt DevSecOps, they seek ways to ensure cloud-native application security, protect business-critical workloads and streamline operations. A CNAPP combines multiple tools and capabilities into a single solution to minimize complexity and enable continuous innovation. It automates tasks and scans configurations and infrastructure for potential risks, thereby reducing threats and risk while improving productivity and response times.

10 Reasons Why CNAPPs Are the Future of Secure Innovation

Peering into a crystal ball, it's clear that CNAPPs are essential to securing every aspect of software developed in the cloud. CNAPPs are the future of secure innovation because they consolidate several powerful features into a single platform to provide better visibility and deeper insights.

Here are the top 10 ways CNAPPs strengthen the security of applications built and run in the cloud:

1. **For modern DevOps and DevSecOps teams, visibility is essential.** By providing a bird's-eye view of cloud-native applications' security postures, CNAPPs deliver a holistic view of a cloud estate. This is invaluable when it comes to making both minor course corrections and big changes — like redefining an entire application architecture.

2. **CNAPPs consistently establish and enforce security policies** across distributed teams and environments, reducing the risk of cloud and app misconfigurations that lead to security gaps.

3. **CNAPPs simplify your security architecture.** When you have a single cloud security platform, it's easier to manage and maintain. This saves valuable time and reduces the learning curve for both security and development teams.

4. **CNAPPs excel at remediating security incidents.** By providing a unified view of security events, enabling teams to quickly identify and address potential threats, a CNAPP can help remediate existing threats and prevent potentially damaging situations from escalating.

5. **Integration with application development and deployment practices makes CNAPPs invaluable.** From their "shift left" role in the CI/CD process to allowing organizations to more effectively integrate security into their development workflows, CNAPP integration capabilities are core to the future of cloud security.

6. A CNAPP simplifies regulatory compliance and accelerates related audits and reporting — two capabilities DevSecOps and DevOps teams have been looking for. A CNAPP is purpose-built to help maintain compliance with industry standards and regulations and generate consolidated security reports.

7. CNAPPs are quickly becoming the go-to accelerators for security management by providing a centralized interface for monitoring, configuring and responding to security issues across the entire application life cycle.

8. A CNAPP eliminates redundant capabilities across security tools, defending and monitoring the CI/CD life cycle. It's designed to avoid overlap between different tool categories and even cloud provider offerings.

9. CNAPPs are effective at reducing costs. By centralizing cloud security through a CNAPP, you can avoid the duplicative costs of point solutions as contracts renew for CWP and CSPM, software composition analysis (SCA) and container security offerings.

10. CNAPPs' built-in security and scalability enables integrated workflows and reduces friction between teams that are spread across different locations and employ a different development methodology.

Chapter 2

Integrating Security into Development

In the relentless race to innovate, DevOps teams are looking for any edge they can get. Shipping new apps and features securely and on time must be a core part of any company's strategy to drive growth. Every DevOps team is focused on how their code can contribute — it's how they define success. Their goal is to gain an extra edge to more quickly deliver new cloud apps and create new customer experiences at scale.

In organizations where security has not been integrated into the SDLC, teams face obstacles in quickly developing and deploying secure code. Security testing and reviews are often tacked onto the end of schedules when time is tight or launch deadlines have already passed. As a result, these crucial steps are often rushed or sometimes skipped altogether, raising the risk of deploying vulnerable applications.

Security as a Differentiator

When security teams find new vulnerabilities, they must be able to share them in real time with software development and other teams. Culling false positives, reprioritizing vulnerabilities based on risk, capturing sufficient context and informing the right project stakeholders of the risks saves all participating teams valuable time.

Integrating a CNAPP into CI/CD pipelines is an essential step. The goal must be to integrate security throughout the process and reframe the entire project so it is more efficient, more focused and based on established guardrails or policies. The tighter the integration between CI/CD pipelines and the CNAPP, the faster risks can be identified and acted on, and the faster development can progress. When security is expanded across DevOps and DevSecOps, code is cleaner, apps get more coding cycles and deadlines are met with time to spare.

With security built in, DevOps teams are also able to gain greater context, prioritization and remediation guidance to fix issues related to the resources they're relying on and sharing in the CI/CD pipeline. Context and prioritization enable developers to stay agile and move quickly while staying secure. CNAPPs provide guardrails for the development process and aid in the organic integration of security, allowing developers to automate, build and deploy as fast as they want — as long as it's all within the constraints of the security guardrails.

Security as an Accelerator

CNAPPs are flattening the speed bumps that stand in the way of getting more cloud apps launched. They're turbocharging development by making security a core part of the CI/CD pipeline.

But it doesn't stop there. CNAPPs expand security across all teams, giving them the time and flexibility they need to unleash their creativity and productivity while shortening time-to-market. The more security is integrated, the more customers win — they'll see more innovative, state-of-the-art and trusted apps they can rely on. CNAPPs turn security into rocket fuel, propelling apps through development faster and ultimately delivering them with security built in from the start.

CNAPPs are the force multipliers DevOps and DevSecOps teams have been looking for. Integrating security throughout the development process, and enabling earlier risk identification and remediation while apps are in development, helps DevOps and DevSecOps teams innovate faster and deliver more secure and reliable applications.

Security as a Risk Mitigator

The typical DevOps team within a medium- to large-scale enterprise handles hundreds of different projects in various stages at any time. There are new apps under development for sales teams, pricing apps and new customized revenue management systems, and large-scale eCommerce apps designed to propel companies into new digital-first revenue models for years to come.

DevOps teams are often under pressure to rush through security reviews and do everything possible to get an app launched. Compensation plans for CIOs, DevOps leaders and their teams prioritize time-to-market performance, driving the intensity to beat schedules. Though the focus is on speed, the risk of releasing vulnerable apps goes up when a CNAPP hasn't been integrated into the CI/CD pipeline from the start.

Security teams take on a big risk when they sign off on apps that haven't been tested across the SDLC. CNAPPs were created to help reduce risks by improving real-time collaboration and providing guardrails to minimize risk. Every phase of development includes a security review when a CNAPP is part of the CI/CD pipeline. Team members across a project gain a full view of vulnerabilities and can fix them in order of priority.

10 Ways CNAPPs Can Help You Win

Much like the racing teams that compete on the Formula 1 Grand Prix circuit, DevOps and DevSecOps teams have a need for speed. The pressure to make every second count and deliver apps on time, or even ahead of schedule, is like the countdown clock on race day. Time ticks away relentlessly on a Grand Prix course the same way it does when DevOps and DevSecOps teams are racing to meet a deadline.

In cloud app development and Formula 1 racing, the time shaved off every turn and code revision can lead to a win. For DevOps and DevSecOps teams, the victory is delighting customers with new apps and seeing how their contributions drive revenue growth.

Here are the top ways CNAPPs help teams win:

1. **Sharing responsibility:** When implemented right, CNAPPs create a culture of shared responsibility where everyone owns security. This model has become essential to cloud-native security operations, where ownership and responsibilities are distributed among stakeholders, including developers and security operations teams.

2. **Detecting risks early:** By integrating with CI/CD pipelines, CNAPPs enable early risk detection throughout every phase of the development process. This is particularly important with cloud-native workloads, which change quickly throughout development.

3. **Reducing false positives:** CNAPPs help cull false positives, reducing alert fatigue and enabling teams to focus on genuine threats. This is crucial because the rate of change in cloud security is high and requires agile approaches to manage security risks.

4. **Prioritizing risks:** CNAPPs aid in reprioritizing issues based on risk, helping teams focus on the most critical issues first.

5. **Adding business context:** CNAPPs provide developers with context to help them understand and address security issues related to the resources they manage and own. Many organizations do not fully leverage the benefits of cloud capabilities, and CNAPPs can help bridge this gap.

6. **Guiding remediation:** CNAPPs provide specific remediation guidance to help developers fix identified issues that put code and projects at risk.

7. **Establishing guardrails:** CNAPPs provide security guardrails for the development process, ensuring developers can move fast while remaining secure. This aligns with the shift toward DevSecOps, where security controls are automated and integrated into the development pipeline.

8. **Integrating security:** CNAPPs aid in the organic integration of security into the development process, making security a core part of DevOps. Having a CNAPP integrated into the CI/CD pipeline is crucial to scaling cloud-native services development.

9. **Empowering developers:** CNAPPs empower developers to take ownership of security issues related to the resources they own. This is in line with the trend toward federated ownership of cloud-native security operations between well-defined teams.

10. **Broadening security initiatives:** By reducing the number of issues that reach production, CNAPPs allow security teams to focus on broader initiatives. As cloud security platforms continue to evolve and deliver advanced functionality, security teams must adapt and be able to focus on strategic initiatives.

Crossing the Finish Line

CNAPPs are setting up DevOps and DevSecOps teams for success. By integrating security across the development process, these teams can ensure they have what they need to accelerate past every stage gate or review and stay secure. With CNAPPs, DevOps teams won't have to take an extra lap for security at the end of the race. Taking on security challenges during each lap — or sprint — is how DevOps teams can win the race to deploy apps.

Chapter 3 Challenges that CNAPPs Address

Every DevOps team is racing to out-innovate competitors by delivering apps, platforms and tools that delight customers, deliver lasting value and drive revenue. Knowing the obstacles to achieving these goals is critical. Having a unified, real-time view of security posture across multi-cloud and hybrid cloud environments is essential for strong code to be created. That's where CNAPPs come in.

DevOps teams take a major performance hit when attackers target vulnerabilities or misconfigurations of cloud infrastructure and APIs that provide access to software supply chains. CNAPPs reduce these risks by simplifying overall cloud complexity and boosting defense across growing attack surfaces.

Managing Complexity

Think of DevOps, DevSecOps and product management like the racing teams and pit crews tasked with finding new ways to shave minutes off turnaround times for race car drivers. In comparable terms, a CNAPP's job is to tackle the cloud- and security-based roadblocks, delays and challenges so DevOps can code quickly and securely.

And just like a racetrack covered in fog makes it difficult to break speed records, the growing complexity of multi-cloud configurations impedes DevOps productivity. Pit crews compensate for track condition challenges and risks by reflexively working with each other. The best DevOps and DevSecOps teams have the same level of intensity and reflex response — and their code and shipped apps show it.

The cloud enables speed. It allows DevOps teams to add new resources on demand, from virtual machines and serverless functions to containers. New services are constantly added and integrated into the dynamic and scalable DevOps environment. Of course, it's challenging to secure an environment that can grow and change in minutes. CNAPPs address this growing complexity by ensuring multi-cloud and hybrid cloud configurations are safe so DevOps teams can speed on. They protect the engine parts of every DevOps effort, including Kubernetes containers, code repositories, integration points and every threat surface that could slow down development.

Fast-moving DevOps teams deploy cloud-native apps several times a day. By bringing together previously siloed tools and systems, CNAPPs unleash the full value of cloud security for DevOps and DevSecOps teams. CNAPPs deliver container scanning, CSPM, IaC scanning, CIEM, and runtime workload, application and data protection.

In the race to ship new features at a record pace, CNAPPs keep the track clear of multi-cloud configuration errors and potential security risks and delays. DevOps, DevSecOps, platform engineering and security operations teams all keep development secure and on schedule. Cloud security practices and CNAPP stakeholders must be well-coordinated to help DevOps teams overcome challenges now and in the future.

7 Ways CNAPPs Keep Cloud Complexity Under Control

The greater the complexity of cloud configurations, the greater the security risks. Getting multi-cloud and hybrid cloud security right from the start gives DevOps teams greater agility to adapt to quickly changing cloud services, containers and tools.

Formula 1 and IndyCar drivers are known for their exceptional reflexes — they need to anticipate track conditions in a split second and course-correct constantly. Similarly, DevOps and DevSecOps teams need a high level of agility and risk awareness to keep their projects on schedule and win the time-to-market race against competitors.

Here are seven ways CNAPPs help DevOps, DevSecOps and product teams reduce security risks, remove roadblocks and accelerate development.

1. **Simplifying and scaling cloud configurations:** CNAPPs keep the complexities of cloud services across multi-cloud and hybrid environments under control. They provide the tools and support DevOps teams need to provision secure cloud infrastructure in an efficient and repeatable way by using templates, enforcing policies and managing images.

2. **Streamlining your team's security toolset to a single toolbox:** CNAPPs streamline security by consolidating myriad tools into a single unified platform, saving DevOps teams hours and making the security process more efficient. CNAPPs are purpose-built to ensure no critical vulnerability is left unchecked.

3. **Providing continuous security coverage from start to finish:** In auto racing, every component of the car is scrutinized and optimized before it touches the track. CNAPPs mirror this high level of preparation for cloud applications, as they are involved in everything from the coding phase to deployment. This built-in security is like fine-tuning your engine to help avoid unexpected breakdowns when you're gunning for the finish line.

4. **Prioritizing risks with laser focus:** Just as race car drivers need to know which areas of the track will test their limits, DevOps and DevSecOps teams must also know their risks. That's where CNAPPs prove especially valuable, as they're designed to prioritize risks and spotlight the most critical issues.

5. **Boosting team collaboration to increase the odds of winning:** CNAPPs foster collaboration between security and development teams by providing a unified platform and view of security posture. This makes it easier to coordinate efforts and address issues, ensuring the team is well-coordinated and in sync.

6. **Staying current on new knowledge and technologies:** There are always new challenges to securing cloud infrastructures and apps. Through a platform approach, CNAPPs provide DevOps and DevSecOps teams the broadest possible protection and incorporate new security capabilities as they emerge.

7. **Protecting the software supply chain:** Cloud-based apps and workloads need evolving security measures to stay safe, especially when they're part of the supply chain. CNAPPs can handle the security of containers and Kubernetes — as well as the security of serverless functions — to ensure apps and workloads stay secure.

Defending a Growing Attack Surface

Every time a new feature or service is added to a cloud environment, it can improve performance — but it can also make it easier for adversaries to attack. CNAPPs are always ready to spot issues, helping ensure your cloud environment is fast and secure.

There are a few key ways that CNAPPs help scale security across growing attack surfaces:

Unified, real-time visibility: Managing cloud security across multiple services without a dashboard is like driving blindfolded. CNAPPs reveal risks and help you fix them before an incident occurs. They also integrate cloud security tools to monitor performance and strengthen security.

Continuous change: When you add new virtual machines and serverless functions, it's like tweaking your car during a high-speed race. CNAPPs help ensure every change is reflected for an accurate view of your attack surface.

Growing identity and access risk gaps: When it comes to cloud security, having control over access is essential. CNAPPs act as security guards, ensuring only authorized users and entities can access the most critical resources. Furthermore, CNAPPs ensure only the right team members can adjust the settings of your cloud platform. This enables security teams to spot and fix security holes in real time, keeping your cloud platform safe from unauthorized access.

Enforcing security and compliance through policies: Enforcing security rules can be tough in the cloud. If you don't do it right, you might face penalties. CNAPPs ensure everyone plays by the rules and keeps your cloud secure.

Prioritization: CNAPPs are like race technicians — they help quickly spot which car component (aka security issue) could cause the biggest problem if it's not fixed ASAP.

Closing the skills gap: By providing an all-in-one security solution, CNAPPs help address the broad lack of cloud security skills many organizations face. For teams that lack the expertise they need, this technology helps their cloud stay secure as it evolves.

Crossing the Finish Line

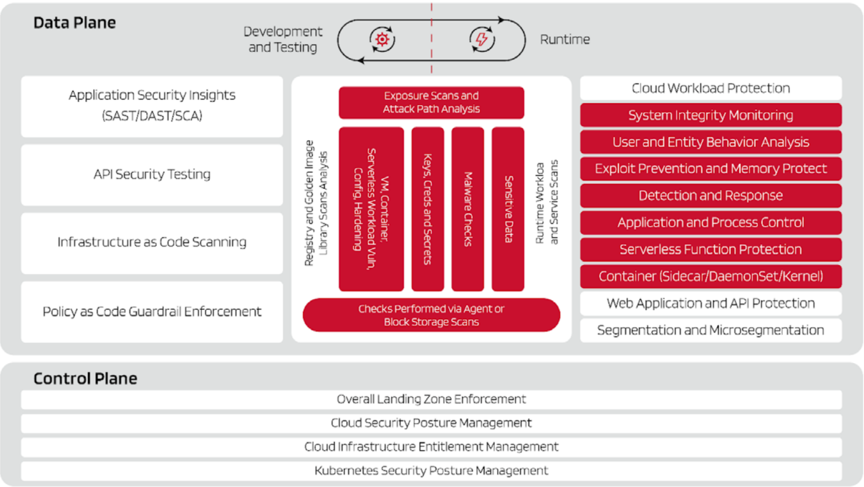
CNAPPs ensure your cloud environment runs smoothly and securely, even as new services and resources appear. They provide a unified dashboard for real-time visibility, which is crucial for navigating today's multi-cloud and hybrid environments. They continuously scan for vulnerabilities and misconfigurations, manage cloud identities and consolidate security findings to reduce the risk of breaches. By enforcing security posture and compliance, CNAPPs help organizations avoid penalties and prioritize incidents, ensuring your cloud vehicle is compliant and ahead of the competition.

Chapter 4
Core CNAPP Capabilities

CNAPPs are designed to adapt to the complex requirements of multi-cloud and hybrid cloud environments. They are built to deliver greater speed by ensuring hardened security across entire supply chains.

Figure 2 shows how CNAPPs support development, testing and runtime. Through the core parts of their architecture, CNAPPs allow development teams to produce high-quality, secure code faster.

CNAPP Capabilities


Data Plane
Development and Testing
Runtime
Application Security Insights (SAST/DAST/SCA)
API Security Testing
Infrastructure as Code Scanning
Policy as Code Guardrail Enforcement
Registry and Golden Image Library Scans Analysis
Exposure Scans and Attack Path Analysis
VM, Container, Serverless Workload Vuln, Config, Hardening
Keys, Creds and Secrets
Malware Checks
Sensitive Data
Runtime Workloa and Service Scans
Checks Performed via Agent or Block Storage Scans
Cloud Workload Protection
System Integrity Monitoring
User and Entity Behavior Analysis
Exploit Prevention and Memory Protect
Detection and Response
Application and Process Control
Serverless Function Protection
Container (Sidecar/DaemonSet/Kernel)
Web Application and API Protection
Segmentation and Microsegmentation
Control Plane
Overall Landing Zone Enforcement
Cloud Security Posture Management
Cloud Infrastructure Entitlement Management
Kubernetes Security Posture Management

CNAPP-cloud-native application protection platform; DAST dynamic application security testing: SAST static application security testing: SCA software composition analysis; VM virtual machine

Figure 2. These CNAPP capabilities are like a cutaway of a racing engine — every part of a CNAPP has a role to play in securing multi-cloud configurations and reducing risk factors.
Source: Gartner 2024 Planning Guide for Security, published October 4, 2023

Leading auto manufacturers pursue new car and engine designs with competitive intensity to design the world's safest, most finely tuned cars for their drivers, and the same is true for DevOps teams. Security and safety for DevOps, DevSecOps and product teams center on making sure cloud infrastructure is as solid, secure and risk-free as possible.

Each CNAPP feature is comparable to the precisely engineered parts of a race engine. Let's take a look under the hood of a CNAPP to see how each of its major features stops threats and contributes to faster, more secure development cycles and hardened CI/CD pipelines.

Cars and Planes

There are two main axes for racing: planning and execution. Similarly, CNAPPs have two important planes: a control plane and a data plane.

Think of the data plane as the physical parts of an engine you work with (e.g., when you change the oil or replace an air filter in your car). The data plane is where you execute and get your hands dirty working directly with cloud applications and data, performing checks and scans to ensure everything is secure. The control plane is a lot like planning for a race — researching technology and best practices to ensure you have the best opportunity to win.

The Full Race: Security from Development to Runtime

In addition to the data and control planes, CNAPPs span the entire software development life cycle. In Figure 2, development and testing are part of the data plane shown at the top left. Runtime is on the right. Notice how both are connected by an oval, like a racetrack.

Think of development and testing as the qualifying round for a high-stakes, high-speed race — only the stakes for DevOps and DevSecOps are shipping and updating applications early. CNAPPs identify potential security issues before applications go live. Once the race is on, CNAPPs monitor all cloud configurations, applications and integration points in real time, looking for and responding to any security threats.

CNAPP Capabilities that Span the Race

Just like car designers working on next year's upgrades, developers must also know what's new so they can compete.

Every component and code base that supports a feature has to be faster, safer and more reliable than the competition's. This is core to earning the trust of every customer using an app. Getting to this level requires a complete CNAPP that all teams can trust to continuously secure everything built and run in the cloud.

IaC Scanning

This part of a CNAPP checks and validates that each cloud configuration is legitimate, accurate and safe. It's where the blueprints for how the CNAPP connects to cloud configurations are stored. Code scanning is invaluable in identifying potential design and security flaws early.

Policy-as-Code Enforcement

Every CNAPP has a governance module that enforces policies to ensure every cloud configuration is secure. And like any world-class racing event, security is always tight. This is the CNAPP component that keeps the car and racing engine safe and secure.

Cloud Security Posture Management (CSPM)

CSPM flags misconfigurations early so they can be fixed. It is also designed to automate remediation to guard against an accidental misconfiguration that could lead to a breach. CSPM gives DevSecOps teams vigilance and visibility so they can keep apps on track and on time to beat competitors to market.

Cloud Vulnerability Management

High-performance racing engines need to be fine-tuned for each race, and the same holds true for the hybrid and multi-cloud infrastructure and tech stacks that help deliver next-generation apps. Racing teams know down to the tool level how much torque an engine component can take. It's the same with DevOps and DevSecOps when it comes to managing applications to prevent buffer overflows and injection flaws while ensuring optimal performance.

Cloud vulnerability management helps organizations identify, report and remediate vulnerabilities in the cloud. It can identify improper access, insecure interfaces and APIs and detect compromised third-party components to prevent supply chain attacks by analyzing past vulnerabilities.

Cloud Workload Protection (CWP)

DevOps, DevSecOps and product teams use CWP to protect their cloud-based assets from vulnerabilities, malware and misconfigurations. CWP provides visibility into cloud workloads and helps reduce risk across diverse cloud environments without bogging down the network with agents. Cloud workloads are scanned for vulnerabilities, secrets and malware while their configurations are continually checked for misconfigurations and CI/CD pipeline vulnerabilities. CWP is also lightweight, relying on an agent to detect real-time threats.

Cloud Infrastructure Entitlement Management (CIEM)

CIEM maintains cloud security and efficiency like a track marshall monitors race course conditions and traffic breaks. It guards the cloud, ensuring everyone has the right amount of access — no more, no less. Access control precision protects confidential data and helps DevOps teams deliver apps on time without security issues.

CIEM prevents data leaks by optimizing the cloud landscape and managing least-privilege permissions. It’s like having a high-tech security system that monitors every track move and restricts engine starting to qualified drivers. CIEM is essential for securing cloud entitlements and ensuring innovation runs smoothly.

Kubernetes Security Posture Management (KSPM)

KSPM checks your Kubernetes containers, hosts and clusters for vulnerabilities, misconfigurations and permission issues.

Keeping your cloud applications running smoothly and safely as you speed toward the finish line is key. With automated security and compliance checks, KSPM provides complete visibility into your Kubernetes environment. It analyzes risks like exposed secrets and networking issues and prioritizes fixes to keep you ahead. KSPM uses the “shift left” approach to catch security issues early in development. This means less time fixing problems and more time developing winning applications.

Application Security Posture Management (ASPM)

ASPM is like having an accurate and updated map. It provides guidance and insights needed to stay fast and resilient in the face of complex track challenges. Think of ASPM as the advanced diagnostics a race crew uses to inspect every car part — from the engine to the diagnostics software — for safety and performance. Effective risk management steers DevOps around cyber vulnerabilities and helps boost performance.

ASPM lays out the full architecture of the race, ensuring the race team has accurate visibility. This real-time visibility helps DevOps teams continuously identify, prioritize and remediate critical application risks.

The best racing strategies are tightly integrated across every aspect of the race. The same is true with ASPM. Development and operational tools are integrated with the goal of identifying, correlating and prioritizing emerging threats.

Data Security Posture Management (DSPM)

Think of DSPM as your secret racing strategy for cloud data security success. DSPM helps you understand where your sensitive data is, how it's being used and where it may crash into security risks.

Your apps and data are like high-performance race cars competing on different tracks. DSPM monitors each car to prevent data breaches and pileups. It searches your data storage for sensitive data, classifies it by value or risk, and monitors who has access.

DSPM doesn't just watch — it detects vulnerabilities and gives DevSecOps teams what they need to know, complete with plans for responding to threats before they need them. Having this in place saves valuable time and avoids breaches in the middle of busy DevOps cycles.

Crossing the Finish Line

The digital race for innovation and customer acquisition is relentless. CNAPPs have become a key solution for DevOps, DevSecOps and product teams under pressure to outperform competitors. Similar to how precision engineering and strategy help win a professional race, CNAPPs' carefully designed components secure cloud infrastructure and enable safe, fast application deployment. With CNAPPs, organizations are turning the tables on digital competition and getting apps out ahead of schedule.

Chapter 5

Get on the Fast Track to CNAPP Benefits

DevOps and professional racing are among the most intensely competitive fields on the planet. There's no question that the best DevOps teams bring an exceptional level of intensity, focus and passion to everything they do.

The secret to excelling at both is pretty simple: Bring your intensity and get as much out of every system, process and component as possible. Just as professional drivers develop an intuitive sense of how hard and fast they can push their cars, the same holds for DevOps, DevSecOps and product teams developing new code.

Balancing Security Risk with the Need for Speed

Professional drivers and DevOps professionals know they always need to be faster. For DevOps teams, this means getting every possible benefit out of CNAPPs. Professional drivers know how fast they can take a turn, and DevOps and DevSecOps teams need to have the same intuitive sense of how hard they can push.

For professional racers, gaining speed is a relentless quest — but it needs to be balanced with safety. It's the same for anyone in DevOps and product management. Getting products out on schedule and delivering on commitments to other teams and — most importantly — customers is paramount, and security teams need to ensure deployments do not create unacceptable levels of risk.

Here's a look at the core business and practitioner benefits that CNAPPs provide.

Business Benefits

Eliminating blind spots that drain energy and time: In racing, missing a blind spot can mean victory or failure. Like the best spotters, CNAPPs provide a 360-degree view of your cloud environment. They detect and prevent multiple threats, including malware, phishing attacks, DDoS attacks and insider threats from malicious or negligent employees. CNAPPs integrate technologies like CSPM, CIEM, CWP, ASPM and DSPM to detect and respond to a broad range of threats.

Having a strong security posture to prevent cyberattacks and maintain compliance: CNAPPs are crucial for identifying risks like unauthorized access, regulatory compliance issues and misconfigurations that could result in data breaches. A CNAPP optimizes a DevOps team's security through three of its main components: CSPM, ASPM and DSPM.

CSPM identifies and fixes public cloud misconfigurations and compliance violations. ASPM prevents misconfigurations and compliance violations at the application layer, and DSPM does so at the data layer. When combined into a CNAPP, these three components help create a strong security posture at every layer so DevSecOps teams can harden their cloud security, automate compliance using policies and streamline audits.

Setting a quick pace when it comes to compliance: A CNAPP helps organizations achieve and maintain compliance with regulations. A CNAPP automates paperwork so team members can focus on their areas of expertise. Additionally, CNAPPs automate compliance checks and generate reports to show compliance with regulations like GDPR, CCPA/CCRA, HIPAA and more.

Making quick decisions with automated analytics: When building a new app or platform, DevSecOps is focused on securing it from attacks and works nonstop to keep DevOps cloud platforms stable. Threat intelligence-based apps and systems within CNAPPs help DevSecOps teams quickly identify and fix the weakest areas of cloud infrastructure, helping to keep those threats away from DevOps teams so they can continue working. CNAPPs use behavioral analytics and AI-based indicators of compromise (IOCs) to detect anomalies early and take action on them.

Knowing what risks are critical: CNAPPs help DevOps and DevSecOps teams prioritize and address the most critical security risks they face in building and launching apps and platforms. CNAPPs also automate security policy enforcement throughout the application life cycle and provide a complete security posture view to accelerate development and operations.

Streamlining operations to reduce total cost of ownership (TCO): CNAPPs reduce costs by centralizing everything. DevSecOps teams can maximize impact and contribution from the tools they use for the minimum price. That's why the CISOs and CIOs are saving on costs by consolidating tools. Choosing to consolidate with a single provider ensures all of the tools work together well. Reducing TCO starts by choosing what to consolidate and finding a CNAPP provider who can go the distance with your DevOps, DevSecOps and product teams.

Empowering security and DevOps teams to fix and prevent issues: CNAPPs deliver the high-octane boost DevSecOps and DevOps teams need to keep ahead of schedule. One of the more powerful aspects of a CNAPP is its ability to align security and development teams to tackle security issues through real-time collaboration. A CNAPP is the platform of choice for enabling DevOps and DevSecOps teams to rapidly develop, deploy and operate secure cloud-native applications.

Protecting sensitive data: CNAPPs protect your company's most valuable data. With ASPM and DSPM capabilities, CNAPPs show you where sensitive data is and ensure it isn't at risk of being stolen or misused. With CIEM, CNAPPs use the principles of least-privilege access and Zero Trust to protect the cloud infrastructure that your applications are running on and the data connected to those apps — both at rest and in transit.

Shipping faster with built-in security: CNAPPs are the force multipliers DevOps and DevSecOps teams are looking for, as they consolidate cloud security tools critical to streamlining DevOps timelines while protecting CI/CD pipelines. But what makes them so valuable from a speed standpoint is the tight integration among the core capabilities and throughout the SDLC.

Practitioner Benefits

Preventing cybersecurity threats by decreasing the number of cloud misconfigurations: CNAPPs continuously scan the cloud infrastructure, looking for cloud misconfigurations and cybersecurity threats. They're also capable of scanning security across multiple cloud services so DevOps teams can continue working without security disruptions or distractions.

Increasing code reliability and reducing human error by automating security tasks: CNAPPs help DevOps teams find new ways to gain more speed. Designed into the core of a CNAPP is the ability to automate security tasks, which helps reduce human error and makes your cloud applications more reliable.

Providing a cloud security dashboard that can track output and results: CNAPPs deliver detailed, in-depth cloud security analysis that identifies threats and vulnerabilities. With a CNAPP, you don't just avoid security risks — you predict them and navigate around cloud security's hazards at high speed. CNAPPs scrutinize every aspect of your cloud environment, ensuring your digital assets perform securely while DevOps teams race to deliver apps.

Boosting productivity and collaboration: The higher the quality of real-time data shared across teams, the greater the productivity and collaboration. Siloed systems are dangerous for DevSecOps teams because they create too many duplicative or irrelevant alerts, making it difficult to track and triage across tools and teams. Having a centralized view of all CNAPP activity reduces the likelihood that an alert will be ignored and lead to a breach. Furthermore, it simplifies and streamlines communication. Having a definitive source of truth that both security and development teams can trust to guide their risk remediation will reduce friction and accelerate mean time to recovery.

Crossing the Finish Line

By embracing CNAPPs, organizations can secure their cloud-native applications more effectively and gain a competitive edge in the fast-paced DevOps race. CNAPPs offer a winning formula for navigating the complexities of hybrid cloud and multi-cloud security. CNAPPs are like high-octane fuel for your DevOps and DevSecOps teams, helping them speed through the development cycle with precision and security.

Chapter 6

Using Threat Intelligence and Threat Hunting to Go Full Throttle with CNAPPs

The phrase “knowledge is power” takes on an entirely new meaning in DevOps and professional racing. When a millisecond can make the difference between a win and a loss, no amount of data capture and intelligence is too extreme.

Racing teams rely on hundreds of sensors positioned on their car to gain the real-time intelligence necessary to deliver a competitive edge. This information is invaluable — when the car comes in for refueling or new tires, the pit crew knows exactly what it needs to do. With each new race, crews have new data they can use to better predict how they can get more speed out of their car while keeping the driver and car secure.

Managed Services Combines Speed and Intelligence to Make DevOps Bulletproof

The world’s top professional racing drivers have that innate split-second skill to maneuver a car through a course. But it’s the intelligence they gain from sensors and their team that gives them the edge to plan a strategy in their heads as they speed down a course.

It's the same with DevSecOps, DevOps and product teams. They have to know the conditions of the cloud platforms and infrastructure they rely on. Identifying patterns that could indicate an intrusion or breach is critical. Indicators of attack (IOAs) and IOCs are essential for teams to stay in the race.

IOCs and IOAs act like a racing car's sensors, providing invaluable real-time data. IOAs focus on detecting an attacker's intent and trying to identify their goals, regardless of the malware or exploit they use. IOCs provide the forensic evidence of a breach occurring on a network. IOAs must be automated to deliver accurate, real-time data on attack attempts so teams can understand attackers' intent better and kill any intrusion attempt.

To get the most out of threat hunting, threat intelligence, IOAs and IOCs, it would benefit teams to rely on their CNAPP provider's trained and experienced threat hunting specialists — sometimes called managed detection and response (MDR) or cloud detection and response (CDR).

CDR provides visibility into cloud infrastructure services, APIs and workloads so DevOps and DevSecOps teams can stay ahead of cyber threats, giving them the ability to navigate configuration or security challenges with virtual machines, containers, serverless technologies and Kubernetes clusters.

CDR identifies threats, analyzes them and acts quickly to keep the cloud security race on track. CDR also provides endpoint detection and response (EDR) and extended detection and response (XDR) data and intelligence to DevOps and DevSecOps teams while focusing on hybrid and multi-cloud challenges. It's like having a dedicated team with the tools and expertise to ensure every DevOps phase gets done securely by out-navigating breaches, intrusion attempts and rapid shifts in cloud configurations.

Managed services offers DevOps teams a deep bench of threat hunting and threat intelligence experts. These experts know how to spot a potential threat and can shut it down immediately. They are constantly monitoring every cloud instance — and every part of a cloud infrastructure. Expert services teams can effectively stop major breach attempts.

When you're considering a CNAPP solution, make sure the potential providers you're looking at have a dedicated team of highly qualified research staff that continuously adds coverage for new vulnerabilities and threat actors. Your DevOps and DevSecOps teams need to be notified of new detections to immediately identify workload exposure to the latest vulnerabilities. A strong services provider does this automatically and for no additional charge.

Expert Threat Insight

Getting completely blindsided by an intrusion or breach is devastating. After going off schedule, DevOps and DevSecOps teams must perform damage assessments and make sure any malicious code is eradicated from every cloud instance.

This is why so many DevOps and DevSecOps teams are partnering with managed services providers. They want to have greater threat hunting, better threat intelligence and deeper expertise when it comes to understanding IOAs and IOCs.

Having this expertise on your team can help shut down breach attempts early and keep on schedule. Let's take a look at how DevOps and DevSecOps teams can get in the driver's seat of threat hunting and threat intelligence.

Expert Threat Hunting

A managed services team worth its retainer will have experienced threat hunters on staff. Visibility isn't enough — you need a team of trained experts who are proactively threat hunting to deliver truly comprehensive protection. These experts need to know how to operate and navigate cloud infrastructure, applications and more. They should be able to quickly scope your cloud estate, identify the tools you need to protect your infrastructure and apps, and identify when an intrusion is worth paying attention to. Best of all, hiring a services team puts DevSecOps and DevOps teams into a more aggressive, proactive security stance. You're no longer sitting and waiting for an attack to happen — you're relying on dedicated experts to find it first.

Delegating threat hunting to a service provider that has automated systems to proactively identify threats is necessary for many organizations, given the complexity of attacks and scarcity of security professionals. In cloud-native environments and applications where configurations and code change often, these threat hunters are a must-have for many organizations that don't have in-house expertise.

Managed Detection and Response and Adjacent Services

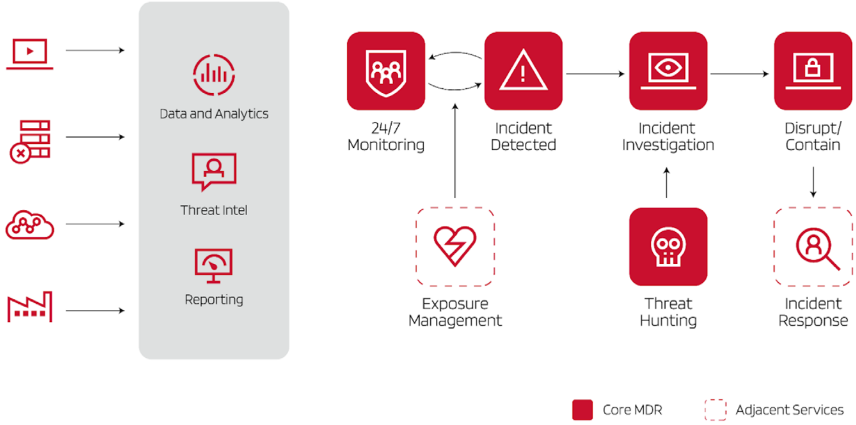


Figure 3. MDR services are designed to adapt quickly to enterprises' evolving hybrid cybersecurity needs by integrating AI and machine learning (ML) models within each core component to capitalize on real-time monitoring and telemetry data.
Source: Gartner, Market Guide for Managed Detection and Response Services, 14 February 2023, Pete Shoard, Al Price, Mitchell Schneider, Craig Lawson, Andrew Davies

Expert Threat Intelligence

DevSecOps and DevOps leaders need to go all in on securing CI/CD pipelines and realize threat intelligence is critical to success. The threats no one sees coming are the ones that can annihilate a timeline, project schedule or even a product.

Only the best CNAPPs have threat intelligence designed into their core. For DevSecOps teams looking to turn security into a strategic strength, it's a necessity. Of the teams that have adopted a CNAPP, many say what makes it valuable is its ability to collect data on known threats and provide a 360-degree view of attacker tactics, techniques and procedures. DevSecOps teams use CNAPPs to aggregate data from myriad channels — including global threat databases and industry reports — and continuously integrate that data into security processes. In short, CNAPPs ensure defenses are always aligned with the latest threat landscape.

Chapter 7

CrowdStrike Falcon Cloud Security: The Most Complete CNAPP Built on Leading Threat Intelligence

CrowdStrike is the first provider to offer AI-based IOAs to help identify threats early and take action on them. AI-powered IOAs work in conjunction with existing layers of sensor defense, including sensor-based machine learning and existing IOAs.

CrowdStrike is unique in how it uses AI-based IOAs to combine cloud-native machine learning and human expertise on a common platform. These patterns were discovered during testing and implemented into the CrowdStrike Falcon® platform for automated detection and prevention.

AI-Powered Indicators of Attack

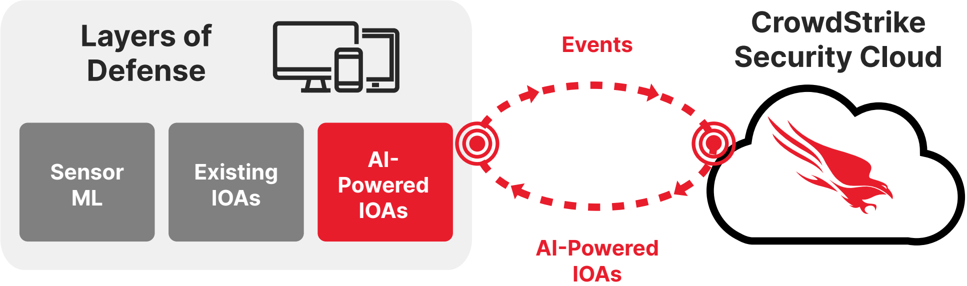


Figure 4. CrowdStrike's AI-powered IOAs collect, analyze and report network telemetry data in real time, offering a continuously recorded view of all network activity.

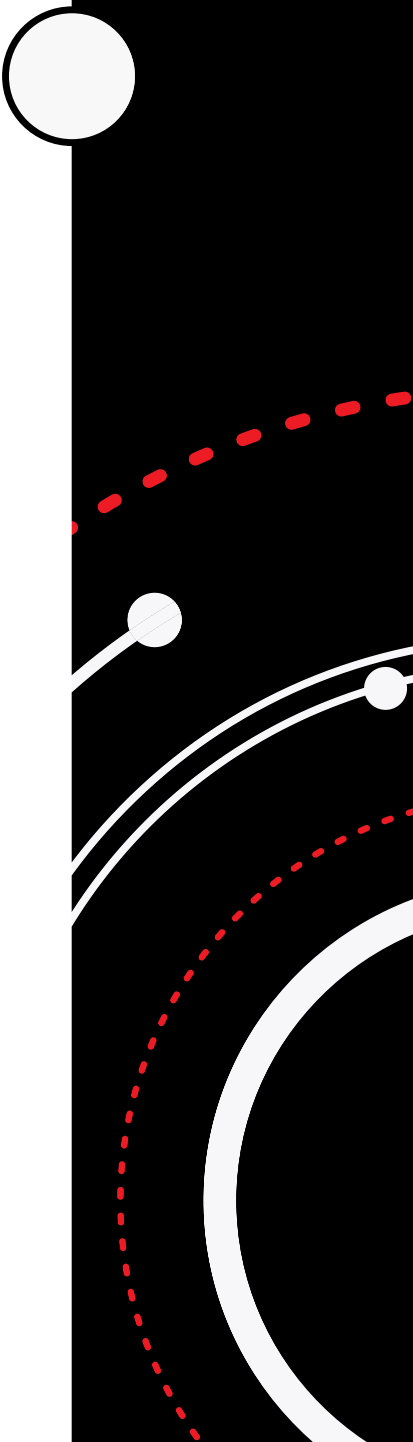
Source: CrowdStrike

Managed Services Offers a Competitive Edge

Sometimes DevOps, DevSecOps and product teams need the expertise of managed services to fully realize the benefits that CNAPPs are capable of offering. A big part of this is combining threat intelligence, threat hunting, IOAs and IOCs into a single, unified view of the security posture of a DevOps cloud infrastructure.

Managed services teams can watch all cloud resources and are skilled at understanding cloud-oriented IOAs and indicators of misconfiguration (IOMs). With the help of experts, you can get actionable alerts along with global insights and tailored recommendations so you can understand and act faster.

For many organizations, this orchestrated approach is the only way to truly stop breaches. As part of an MDR team, threat hunting experts go the last mile to keep your cloud environment secure.



Conclusion

In the high-energy world of professional racing, having the data and insights needed to keep excelling and improving is critical to win. DevOps, DevSecOps and product teams face these same challenges when racing against ever-tighter deadlines to deliver world-class cloud apps.

Teams rely on CNAPPs for real-time insights into their cloud security and use these signals to continuously improve and refine security measures with every development cycle. CNAPPs act as the advanced telemetry system of cloud security, providing real-time feedback and automated responses that enable teams to fine-tune their defenses and accelerate secure application delivery.

Just as racers adapt to fast-changing road conditions and twists in a racetrack, CNAPPs adapt to the evolving cloud landscape, ensuring security is not a one-time checkered flag but a series of victories in the race against threats. With CNAPPs and the power of end-to-end cloud security automation, companies can address critical risks and uncover threats in a fraction of the time — no point solutions needed.

Having a CNAPP is like having an experienced pit crew that is available 24/7, constantly scanning for vulnerabilities and misconfigurations. It's a unified platform that not only identifies potential hazards but suggests the best course of action to take. The goal is to help DevOps teams stay ahead of the pack, making informed decisions on the fly and pushing toward the finish line with confidence that their cloud applications are as secure as they are fast.

CROWDSTRIKE

Get a Free Cloud Security Health Check

What to expect:

- Engage in a one-on-one session with a cloud security expert
- Evaluate your current cloud environment
- Identify misconfigurations, vulnerabilities and potential cloud threats

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram