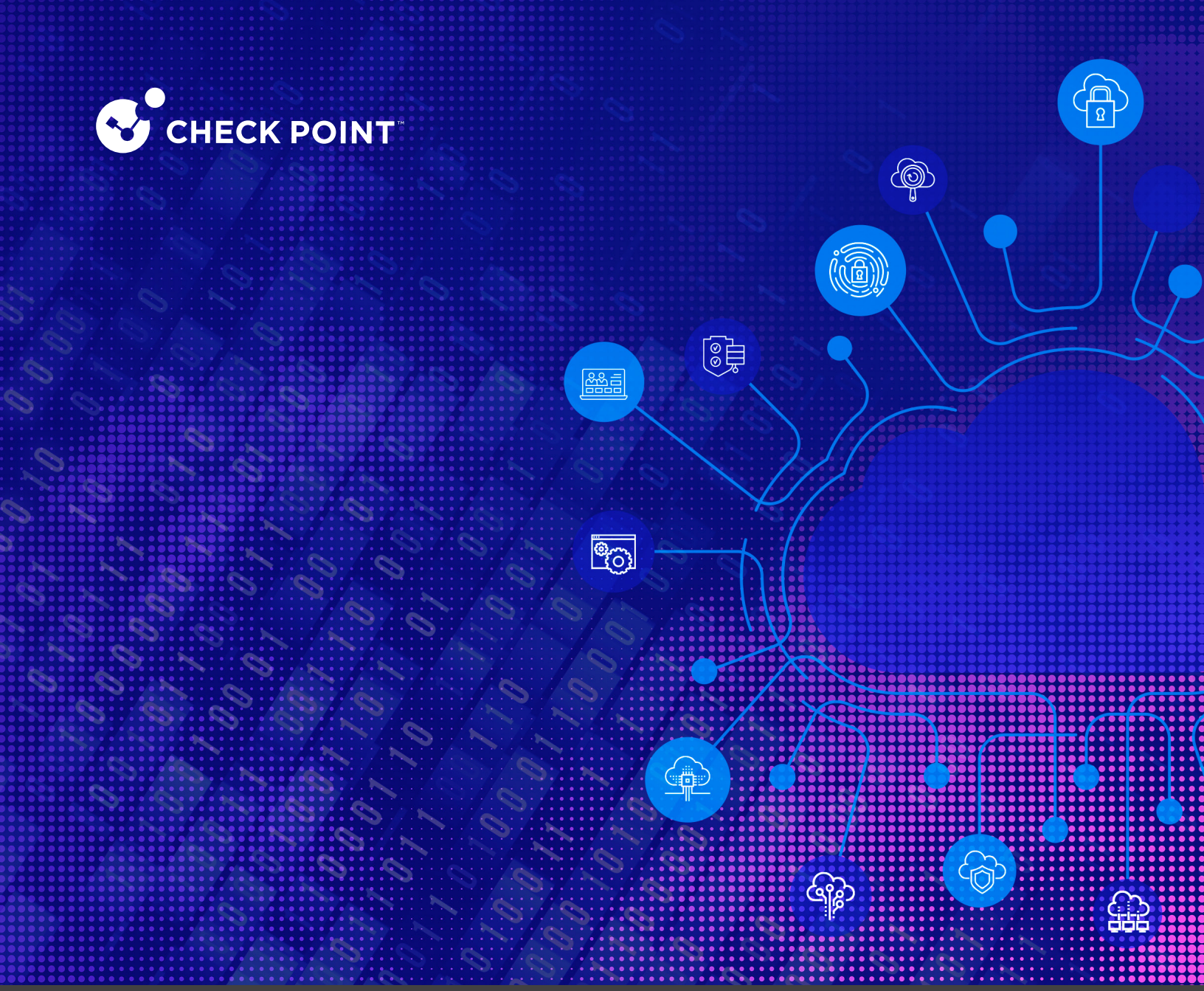


THE ULTIMATE BUYER'S GUIDE TO CLOUD-NATIVE APPLICATION PROTECTION PLATFORMS (CNAPP)

Introduction: What's the Weakest Link in Your Application Security?

You've heard the old adage: "A chain is only as strong as its weakest link." So what's the weakest link in the security of your software development supply chain?

Concern over application security is growing with the rise in open-source software, APIs, and other third-party components—all common practices in application development today. Businesses and governments around the world are waking up to the realization that a single compromised component—such as the Log4shell vulnerability in Apache's Log4j, an open-source logging framework—could put hundreds of millions of devices at risk.

Amid rising panic about software supply-chain vulnerabilities, U.S. government security agencies issued joint guidance for developers in September 2022 to crack down on the problem, saying, "supply chain compromise allows malicious actors to move throughout networks seemingly undetected. In order to counter this threat, the cybersecurity community needs to focus on securing the software development lifecycle [SDLC]."

The most widespread way to secure the SDLC has been "shift-left," an approach that moves security earlier and earlier in the SDLC. But too often this leads to buck-passing and doesn't solve the problem; it just moves it to another department.

That's a problem, given that most organizations can't meet their own application security needs: 39% say they're facing a severe skills gap, without the qualified personnel to implement coherent application security; 35% claim a lack of security awareness throughout their organization.

In a world where we are continuously developing, continuously integrating, and continuously releasing, we need a continuous, always-on approach to application security. And it must work for today's loosely coupled, highly distributed cloud applications, which are complex and unpredictable by nature.

All of which means that the methods used in application security are also long overdue for an overhaul. Static security checks aren't enough—today there's so much more that can go wrong, at a lot more points, in bigger ways, across your entire SDLC.

And the cost of not properly securing your applications against these risks is steeper than ever, as we've seen from Log4shell and other vulnerabilities, not to mention the rising number of malicious packages discovered in the popular Linux open-source code repository PyPi: financial and reputational damage to your business, your users, and the risk of running afoul of a wide range of regulatory guidelines.

One layer of protection also isn't enough, no matter where you situate it, or at what point in the SDLC. Security and compliance management is a business necessity across the entire infrastructure on which your application runs, including for network traffic, the application layer code, and the workload layer (VMs, containers, serverless).

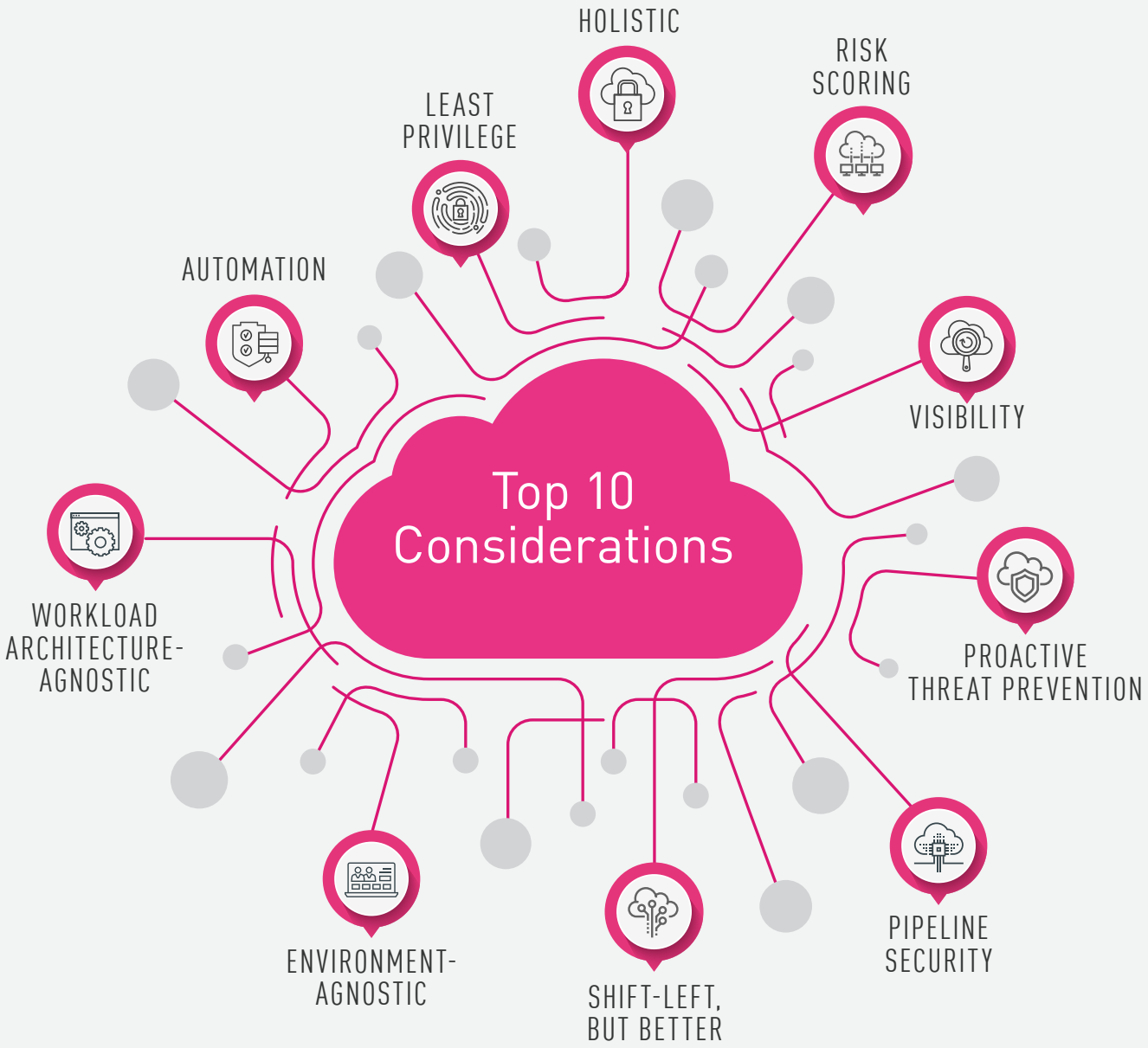
With all this complexity, many vendors have begun offering security scanning, monitoring, and observability tools for cloud-native workloads, all within a single unified platform instead of a loosely integrated set of single-purpose products.

First coined by Gartner, the term "cloud native application protection platform" (CNAPP) refers to "an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production." CNAPP solutions promise the ability to contextualize information based on end-to-end visibility across your entire application infrastructure.

But often, the promise of CNAPP doesn't quite line up with what vendors deliver. To help you choose a solution that will work for your business, this buyer's guide outlines the main considerations and questions to apply when choosing a third-party enterprise CNAPP solution.

The Top 10 Considerations for Evaluating a CNAPP Solution

So you're in the market for a CNAPP solution. Don't sign on the dotted line unless the solution you choose can deliver these Top 10...



1 

Holistic. Look for a "one-stop-shop" approach that secures the forest (the overall application) and the trees (the workloads) while integrating with the organization's existing stack. Application workload security is a complex set of activities carried out by multiple teams across the development lifecycle, from coding to runtime. It is not unusual for these teams to each have their own security tools, such as static and dynamic testing tools for the developers and a range of runtime vulnerability scanners for the operations team. These teams also tend to work in silos, and this fragmentation makes it very difficult for the security team to implement a seamless end-to-end application security process.

Your CNAPP platform must solve this by integrating deeply with the organization's existing application security stack and promoting a collaborative cross-team security process throughout the application's lifecycle and ecosystem.

2 

Visibility. You need end-to-end visibility of cloud environment assets and data flows. You are most likely running your cloud-native distributed applications in a multi-cloud/hybrid environment. Given the complexity and dynamic nature of the applications and the ecosystem in which they run, tracking assets and data flows can often feel like mission impossible. The bottom line is: You cannot secure what you don't see, or what you don't see in context.

Your CNAPP platform should provide all stakeholders with a centralized view of application security health—a view that is comprehensive, contextual, and real-time. For example, two-way integration with your organization's asset management and change management systems is essential.

3 

Least privilege. Don't choose any solution that doesn't let you uphold a zero-trust, least-privilege access security strategy. Application security is more than just application layer security; it begins with a shared responsibility model. The lines of responsibility between the cloud customer and the cloud provider change depending on the service model, from infrastructure as a service (IaaS) to fully managed software as a service (SaaS). At the IaaS level, the cloud provider is responsible for securing the infrastructure itself (hosts, operating systems, networks, and so on) while the customer must secure what runs on the infrastructure (authentication and access control, data governance, and so on).

Zero trust and least privilege have emerged as a basic standard cloud customers must uphold in order to meet their shared security responsibility. The application security platform must support a zero-trust security strategy that assumes that all traffic is suspect until it has been authorized, inspected, and secured. Your CNAPP platform should help you enforce least-privilege access that granularly tailors privileges to the user role, along with other best practices.

4 

Automation. Throughout the SDLC and in production environments, the platform must automate time-consuming, tedious, and error-prone manual application security processes throughout the development lifecycle and in production environments. It must, for example, automatically and dynamically enforce corporate security controls and industry best practices, as well as detect, alert to, and, where possible, remediate security misconfigurations, which are one of the leading causes of risky security gaps.

Advanced data technologies such as machine learning and artificial intelligence are changing the face of many sectors, from manufacturing and healthcare to logistics, financial services, and more. With large and diverse streams of real-time data coming in across all these industries, analytics and other technologies need to autonomously manage complex processes with minimal human intervention. Your CNAPP platform must provide automated enforcement of corporate security controls and industry best practices, automated and contextual misconfiguration remediation, and more.

5 

Environment-agnostic. Your CNAPP platform should work seamlessly everywhere you do—on-premises, across multiple cloud providers, and in hybrid infrastructures. It must be able to orchestrate monitoring and remediation across cloud providers and the organization's data center(s).

The public cloud is a large and highly attractive attack service for malicious actors. Although each cloud provider offers tools and services to help monitor and secure their cloud resources and services, it is up to you to manage security consistently in hybrid and multi-cloud environments. A CNAPP platform should help you do that efficiently and easily.

6 

Workload architecture-agnostic. Your CNAPP platform needs to be able to work with all of today's modern architectures—including microservices, containers, and serverless functions, enforcing security and governance policies automatically for all types of ephemeral runtime workloads.

Legacy security tools can't effectively enforce security controls across flexible and dynamic cloud workloads, which are launched and terminated at scale and at velocity with little or no human intervention. That's where CNAPP comes in, ensuring consistency in all your security policies.

7 

Pipeline security. A CNAPP platform should help you develop more quickly and securely by scanning templates, scripts, and images for security gaps before vulnerabilities can be propagated to all the applications or runtime environments that use the pipeline.

This gives you a security-as-code approach, creating a continuous application security pipeline based on CI/CD processes, infrastructure-as-code (IAC) templates and scripts, and function and container images.

8 

Shift-left, but better. We mentioned above that left-shifting isn't always the answer—but it can help, embedding security into builds while reducing development cycles and supporting a DevSecOps culture. This also reduces remediation costs, since it is far less expensive to fix a vulnerability during pre-production phases. Last but not least, a shift-left security culture facilitates continuous feedback so that application security and workload protection can be tweaked and optimized over time.

As part of a CNAPP platform, left-shifting security processes earlier in the SDLC can ensure robust security posture management for cloud-native applications, embedding security and governance controls into your organization's DNA and putting continuous testing in place for the design and build cycles.

9

Proactive threat prevention. Your CNAPP platform should go beyond early threat detection to proactively prevent threats in the first place. Detection-only policies give threat actors plenty of time to compromise your systems and assets (minutes or even hours) after detection and before remediation. That's why you need proactive protection to block malicious activity in near real-time before attackers can cause damage.

Look for robust threat intelligence and behavioral analytics capabilities that reliably pinpoint risk and trigger protective workarounds and other compensating controls—buying your security team time to conduct further investigation and remediation efforts as necessary.

10

Risk scoring. Dealing with numerous alerts from an entire suite of unconnected cloud security tools is complicated. To work "smarter, not harder," a CNAPP solution should provide effective risk management (ERM), using contextual AI to provide actionable recommendations, letting you focus on the highest priority risks.

Look for a platform that gives you deep context, letting you focus on the 1% of essential tasks that cannot be overlooked.

What Goes into a CNAPP Solution?

Make no mistake: Not every product marketed under the banner of CNAPP contains the same components—far from it. Since there's no standardization, vendors are free to provide some combination of the following components. It may seem like alphabet soup at first, but each of these components serves a separate and useful function in securing your entire development and production environment.

And often, there's no way to integrate all these moving parts and get them working together. That's a problem when you're evaluating 10 or more "lookalike" platforms and trying to evaluate what will work best for you.

Here are some of the features you may find in a CNAPP platform:

Basic Components—For Bare-Minimum Protection

The following should be considered "basic" features—in other words, the bare minimum you should look for when you're considering a CNAPP solution. Looking at this from a big-picture perspective, you should (at the very least) have the ability to monitor and control both your cloud security posture and your applications.

- **Cloud security posture management (CSPM)**
  An essential part of any CNAPP solution, CSPM solutions offer automated governance across multi-cloud assets and services. This covers the detection of misconfigurations, the enforcement of security best practices, and adherence to compliance frameworks, as well as the visualization and assessment of your overall security posture.

- **Cloud service network security (CSNS)**
  This is the cloud equivalent of traditional, perimeter-based network defenses used to secure on-premises infrastructure, such as traditional firewalls, since these do not function in the "perimeter-free" realm of cloud and therefore can't meet enterprise security requirements. CSNS allows companies to achieve the same level of security monitoring and threat prevention that exists in their on-premises environment—without the traditional on-premises perimeter. That lets you ensure total corporate cybersecurity and regulatory compliance using cloud network security and zero-trust network segmentation.

- **AI-based AppSec**
  This lets you replace legacy Web Application Firewalls (WAFs) with automation and intelligence. In return, you get precise threat prevention so you can stop OWASP Top-10 attacks, prevent bot attacks, and catch any attempt at malicious interaction with your apps and APIs—across any environment.

- **Cloud workload protection**
  With applications being built and deployed at the speed they are today, security is often an afterthought—leading to vulnerabilities and security compromises. Cloud workload protection discovers running workloads in real time, then performs a vulnerability scan to ensure that nothing has been missed, either due to poor coding practices or lack of correct network segmentation.

Advanced Components—For Next-Level Protection

The following are more "advanced" CNAPP components that are becoming available in some higher-functioning solutions.

- **Cloud infrastructure entitlement management (CIEM)**
  In the cloud, there's no perimeter, so permissions are more important than ever to protect sensitive assets. But it doesn't end there. Beyond ordinary users, we're also dealing with ephemeral entities like workloads (containers, serverless) that spin up and down on demand. To avoid problems around permissions, DevOps teams often assign excessive entitlements to foster agility, but that leaves your organization vulnerable.

  CIEM provides a true picture of your infrastructure and access management, eliminating the guesswork and automatically enforcing least privilege. A truly effective CIEM solution won't get in your developers' way—instead, it functions in the background to make their work even easier.

  Check Point's CloudGuard CNAPP with CIEM helps reduce your TCO with:
  - Automatic remediation of identity risk
  - Auto-enforcement of least privilege
  - Eliminates the need to manually search, find, and remove redundant user accounts
  - Enables you to easily adopt security best practices

  Plus, CloudGuard's CIEM offers machine learning to analyze permission paths and give you full visibility into entitlements. All without impacting functionality or the pace of development. You get all the security, all the insight, without the headache.

- **Agentless workload posture**
  Cloud workload protection (CWP) provides deep security posture visibility into all running processes: hosts, containers, and microservices. Many CWP solution vendors will tell you this can't be done without adding agents to workloads, but this adds a lot of work for developers and increases friction between dev and security teams. Since developer agility is a leading strategic goal of any software organization, you should ideally look for an agentless workload posture (AWP) solution that will work in the background, without interfering with existing DevOps processes; this ensures security while letting your teams continue to work normally.

  Check Point's CloudGuard CNAPP with AWP provides workload protection that builds security right into the cloud-native applications that drive your business, giving you:
  - Total coverage, from development through runtime and from code to cloud
  - Full automation to get up and running fast with zero trust and least privilege
  - Full security across all your cloud environments, within any workload architecture and across the entire application lifecycle
  - Easy access to set security policies, enforce and profile functions, and block malicious activity

CloudGuard AWP lets you embed security into the build with continuous scanning of code including infrastructure as code (IaC).

- **Pipeline security**
  The way we build code today has changed. Instead of building applications from scratch, developers piece them together from a hodge-podge of open-source components, libraries, and APIs. This introduces new types of vulnerabilities all the way along your software supply chain. Pipeline security offers you an easier, more efficient way to build in static application security testing (SAST) for source code, along with infrastructure-as-code (IaC) scanning. This way, when you shift left, you're not just passing the buck, you're actually doing security better from square one.

  Check Point's CloudGuard CNAPP with Spectral pipeline security offers you an easier, more efficient way to build in SAST for source code, along with IaC scanning, allowing you to:
  - Manage security policies from a single central dashboard
  - Enforce routine scanning of code and repositories
  - Protect applications from code to cloud seamlessly
  - Automate secret protection, malware, and vulnerability detection through the SDLC
  - Eliminate public blind spots and enforce policies throughout the SDLC

Spectral was created with developers in mind, so—as with the entire CloudGuard CNAPP suite—its focus is on letting them do their job.

ERM—Bringing It All Together

With all of the components we've explored so far in your CNAPP, you need the ability to bring all the information from all your security solutions together. You want to focus on the risks that matter to your business and not have your teams distracted by lower-priority issues.

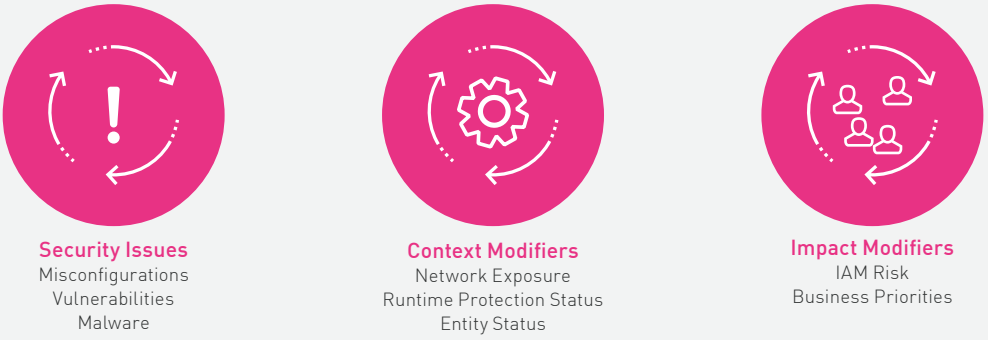
To help you do that more easily, Check Point's CNAPP offers effective risk management (ERM), providing you not only with data, but with deep context and insight that lets you take action fast. It provides:

- Contextual AI and risk scoring
- Reduced attack surface, so you can focus on the highest priority risks
- Auto-remediation based on "minimal effective dose" actions

What do we mean by "minimal effective dose"? This refers to resolving security issues by following "right-sized" recommendations: too little, and the resolution won't resolve the problem; too much, and you will be wasting resources on doing unnecessary work with lower ROI.

Optimize your security team's focus so you are protecting the assets and processes that matter most. It's just another way that Check Point CloudGuard CNAPP puts you in the driver's seat, with total control over your security, adapted to your priorities.

Here's a simple diagram of ERM considerations:



CloudGuard's CNAPP solution helps you understand your true risk posture—which is more than just a number. ERM goes beyond the numbers, taking into consideration:

- The type of security issue and its severity
- Context modifiers such as network exposure
- Impact modifiers such as its potential financial cost to your business

That information empowers your team to take action, bringing down total time to remediation (TTR) and ensuring greater end-to-end application security.

Five Questions You Must Ask When Evaluating a CNAPP Solution

The era of monolithic applications deployed on proprietary infrastructure is gone forever. Long live cloud-native, distributed applications that are essentially orchestrators of microservice, container, and serverless workloads deployed across multi-cloud/hybrid-cloud environments.

The following five questions are essential when assessing if a CNAPP solution is right for your organization.

1. **Does your CNAPP cover all layers: infrastructure, pipeline, workload, and microservices?**
   You must ensure that the solution under consideration offers a broad suite of features as well as a unified interface and centralized set of security and compliance guardrails. It must be an end-to-end platform that lets you apply your application workload security and compliance processes and policies consistently throughout the application lifecycle and across a fragmented environment. And it must also be able to respond automatically to dynamic workloads and infrastructure resources.

2. **Do you deliver single-pane, contextual visualization of cloud security issues and status?**
   Your security officers need to be able to understand the entire distributed application workload deployment in one place, with a single interface for setting and enforcing security policies. Make sure the application workload security solution that you choose delivers intelligent visibility and clear situational awareness of application security, including:

   - Continuous security and governance monitoring of all assets, traffic, workloads, users, and data usage across all environments
   - Support for all leading frameworks for application security best practices and benchmarks, as well as internal rules and guidelines
   - Runtime alerts to anomalous system or user behavior, with intuitive visualizations that encourage incident and risk investigations

3 **Do you support a shift-left DevSecOps strategy?**

Question the vendor carefully about the depth and breadth of their DevSecOps support. Do they automatically scan and test the application code itself? How about the open-source code (and other dependencies) called by the application, or the templates and images used to deploy workload and infrastructure instances? Are components that were scanned during the pre-production stages also scanned during runtime to ensure protection from tomorrow's threats?

4 **How much of the application security workflow are you intelligently integrating and automating?**

Smart, contextual automation is absolutely essential for achieving this objective. Make sure, for example, that the solution automatically aligns workloads when security and compliance rules change. Ensure that risk mitigation and remediation processes are triggered automatically if a misconfiguration or threat is detected.

One of the key motivations for implementing an application workload security solution is to achieve scale and reduce human error. Which is why it's so perplexing that many vendors offer what they present as comprehensive CNAPP "suites" or "platforms" that offer multiple capabilities, yet are not connected in a coherent way. Instead, these products work separately and are not integrated, meaning the security value they present to you as a whole is minimal. Often, these kinds of tools give you no way to extract intelligence and insight to make organizational changes.

5 **Do you provide proactive application threat prevention and protection in runtime environments?**

The whole point of application workload security is to block runtime threats before they can compromise data and systems. Be sure to run through the following checklist with the application security vendor:

- Global coverage (versus region-based protection)
- Context-aware, real-time anomaly detection and intrusion alerts, leveraging advanced threat intelligence capabilities
- AI-drive contextual risk scoring
- Tamper protection for asset configurations
- Granular IAM control, just-in-time privilege elevation
- Zero-trust approach, such as automatically locking egress rules for newly detected assets
- Automated remediation
- High-quality, actionable forensics based on context-enriched traffic

Conclusion

Today's modern cloud-based development demands security solutions designed from the ground-up for cloud. CloudGuard from Check Point is the only end-to-end cloud-native security platform. With protection for every layer of the application workload, from CI/CD to runtime, CloudGuard empowers security teams and DevOps teams to deploy simultaneously, with a zero-trust approach to security, while meeting all of the challenges of modern development:

- Effectively **securing fragmented APIs**, microservices, and containers at scale
- Dealing with **vulnerabilities in third-party and open-source components**
- Instilling a security mindset by proving to all your teams that **application security won't conflict with agile CI/CD** pipelines

We hope that you've found this Buyer's Guide useful as you consider which CNAPP solution is optimal for your organization.

Application security solutions aim to close security and compliance gaps by providing a unified and centralized security framework that delivers end-to-end visibility and consistent enforcement of security and compliance guardrails. The best application security solutions uphold a zero-trust security strategy, provide high levels of automation, and are both environment- and workload architecture-agnostic.

CloudGuard's CNAPP platform represents the next evolution of cloud-native application security, giving all your departments exactly what they need:

- More context
- Better security
- Less time to remediation

At Check Point, we know that effective CNAPP is more than the sum of its parts, bringing together best-in-breed tools and unifying them through a single powerful platform, built for the way modern software organizations work.

That means you'll get a serious security platform, backed by CloudGuard's decades-long reputation, giving you effective guardrails for all your developers—without slowing them down or interfering with their workflows.

Click here to get started free with CloudGuard CNAPP.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: 972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391

www.checkpoint.com