The Rise & Future of CNAPP

One of the rising new categories of tooling in cloud security that's starting to get buzz is CNAPP. CNAPP, or Cloud-Native Application Protection Platform, represents a consolidation and evolution of multiple cloud security technologies, including Cloud Security Posture Management (CSPM), Cloud Workload Protection Platforms (CWPP), Cloud Infrastructure Entitlement Management (CIEM), Infrastructure as Code (IaC) scanning, and more.

As every organization becomes more and more of a cloud organization, applications are becoming the heartbeat of business.

The cloud provides a level of innovation and advancement that businesses must take advantage of to stay ahead of the curve. The increasing push to the cloud has highlighted some weaknesses of traditional infrastructure security approaches and sparked the emergence of new approaches like CNAPPs.

Let's take a look at some of the specific drivers and trends behind the emergence of CNAPP, why CNAPP is well suited to address those trends, and what they mean for the future of CNAPP as it continues to take shape and evolve.

Eight security trends behind the emergence of CNAPP

The cloud security space has reached a breaking point. Security teams are tasked with handling several very different types of complexity: one of coverage and knowing what is in the environment, one of prioritization and identifying what must be remediated first, and one of friction and balance with developer and operations teams to ensure that processes are followed and issues are remediated. They must achieve complete visibility and coverage of their cloud environments without causing too much friction with DevOps and slowing down the business. This is not a simple challenge! CNAPP is moving into the forefront to help security teams address these needs. The reason for the rise in CNAPP can be attributed to eight broader trends in security.

01. The evolution of risk in the cloud

For years, security teams have taken a one-to-one approach to security. Each specific issue type got its own dedicated scanning tool: one for misconfigurations, one for secrets, and so on. Each tool and the team in charge of it operated in their own silo. This worked fine in the pre-cloud world, but the cloud is driving a change here.

In the cloud, different issues are not isolated, and different resources are increasingly becoming more correlated and intertwined. This means that risks in the cloud are now made up of combinations of issues across multiple layers. This has caused a shift for security teams, and now many teams are responsible for cloud security end-to-end. They are faced with a need to consolidate their view across layers and their respective tooling to more accurately reflect the nature of risk in the cloud.

In today's world, security teams must be able to understand two things: the toxic combinations of issues that make up the most critical risks in the cloud, and which of those issues they have compensating controls in place for. Figuring these things out has become an intensive manual process for teams, and does not scale to the speed and size of cloud environments today. A pressing need to do this correlation and prioritization out of the box is one of the main drivers behind the emergence of CNAPP.

02. The changing place of compliance

Given the regulatory and legal necessity behind them, compliance frameworks and benchmarks have been a common starting point for security teams to indicate to the market that they're adopting a strong security posture. However, teams have started to realize that compliance alone is not sufficient. Frameworks will create a checklist of security activities but are not able to communicate priority and why items on the checklist matter.

If your compliance framework tells you something is not optimally configured, you don't have a way to tell if that actually matters for the overall security of your environment. Being compliant is not the same thing as being secure. You can be 100% compliant with a framework and still have security holes.

Security organizations are starting to treat compliance differently in today's world, as a necessary but not sufficient step towards a stronger security posture. The need to look beyond compliance benchmarks and frameworks has led teams to look beyond CSPMs towards more holistic security solutions like CNAPP that can combine compliance with a contextual understanding of risk. Joining these together allows teams to understand and prioritize their compliance efforts properly.

03.

The sharing of security responsibility with development and operations

The cloud is an extremely collaborative space. Many teams across engineering, DevOps, and security interact with the cloud, but cloud ownership really belongs to developers, across the entire stack. The trend is only going to shift more in this direction as developers become increasingly responsible for coding more of the computing stack in the cloud. This means that security teams must work with developers to improve security. They're the only ones who can implement security improvements in the cloud at the resource level. Nobody else can restart a production machine that's owned by a development team, for example, because there's no way to see the impact of doing so. Only the development team owner knows.

For years, developers used to get lists of findings from security teams in an email with what they needed to fix. Organizations are realizing that this process doesn't work. It takes too much time, is too overwhelming for developer teams, and incurs too much overhead. And most importantly, it doesn't give context to developers on why something needs to be fixed.

The industry is recognizing the need to move from tools dedicated solely to security to ones that provide value for security and DevOps teams. Not only because developers own the remediation and response, but also because it's the only way to scale security up, given the common discrepancy in team sizes between security and DevOps. Security tooling that allows developers to easily understand the state of security for their resources and provides the information they need to proactively remediate issues is a must, and something that CNAPP is well positioned to offer.

04.

The move from post-breach to pre-breach security

This trend speaks to the growing maturity of cloud security. The more breaches we see, the more we realize that containing and responding to a breach is so much more expensive and time-consuming than preventing it in the first place. And since many breaches happen via ways we could have prevented, security teams are realizing that investing more in pre-breach prevention has a higher ROI than post-breach detection tools.

Preventing breaches rather than responding to them seems like an obvious insight, but part of the reason that pre-breach security hasn't been as prevalent is because it's been too slow and expensive to deploy fixes in the past. Because of this, we relied on compensating controls to monitor the environment as a best resort. Now that we can deploy updates every minute, it opens up the possibility of preventing breaches by shrinking mean time to remediation. This shifts the value that security tooling should deliver towards a pre-breach prevention focus, which CNAPPs are designed to do.

05.

The unification of development and runtime security

The next trend is one that has been discussed for a long time: shifting left. If we know about an issue at the time of coding or deployment, then why deploy something that's vulnerable? Why not fix it before it hits production? Today, we have the automation and speed of deployment necessary to perform CI/CD scanning and test everything in the pipeline, and organizations are starting to implement it.

The promise of shifting left is not new, but what's changed is the capability to do so properly. To shift left, you need to know the impact of any policies you release. If you can say with certainty what policies will do and who they will impact, and give development teams notice, then you're in a position to successfully shift left. Predictability and certainty remove the friction that organizations have experienced in the past with shift left attempts. Teams are now able to understand their policies in the runtime cloud environment, so they can know what any given policy will do and the impact it will have for particular resources should they apply it to the development pipeline as well.

A desire to apply one policy across the pipeline drives teams to consider unified solutions like CNAPPs. Having separate security tooling for development and runtime causes friction and silos that no longer make sense as the consolidation of cloud responsibilities and speed continue to evolve.

06.

The consolidation from a suite of products to a unified platform

Security teams are changing their view on security tooling. They've learned that buying a portfolio of security products, even from the same vendor, can lead to friction and silos if they are not well integrated, creating visibility and security gaps in the cloud. To keep pace with the dynamic and ever-growing nature of the cloud, security teams need a unified data model across their security tooling. In other words, the tools must talk to each other out-of-the-box. Otherwise, it creates a large degree of operational friction in the form of correlating across tools manually.

Manual correlations and integrations lead to a worse security posture and a lot of headaches. Teams are striving to find ways to avoid portfolios of tools and move towards single unified platforms that work across cloud layers in a single data model. The trend towards consolidation is not just a matter of consolidating vendors, as a portfolio of tools from one vendor may still struggle to work well together, but rather a matter of consolidating capabilities into one solution. CNAPP represents the outcome of this consolidation, and successful CNAPPs must present a singular view, not a collection of separate analyses.

07.
The addition of context to alerts

We are good at sending alerts in the security industry. In fact, many security teams have alert overload. What's challenging is measuring the impact of alerts and getting to a place of understanding them in a simple way so that even non-security experts can understand the point and impact. Security teams are realizing that it's not a matter of creating more security alerts, but rather a matter of increasing visibility and context that alerts have so that they are useful and anyone can fix the issues. The driver behind this is the desire to democratize the ability to deal with security issues. If teams have a bottom line of what someone needs to do, why, and how they need to do it, then security operations can scale to meet the needs of large cloud environments.

Visibility and context in alerting comes from understanding your cloud environment across layers. The industry has learned that isolated, binary alerts don't provide what teams actually need to know to take action: the "so what?"

Should CNAPPs allow you to scale security operations by contextualizing and connecting different risk factors into unified alerts, removing the need to manually sift through and correlate thousands of isolated alerts.

08.
The elimination of security friction

Legacy security tooling introduced a lot of friction for security and development teams. There are many examples of this. Agent-based deployments caused friction because development teams were the ones that needed to deploy security agents, which created a disconnect and limited the coverage of security tools. Complicated onboarding and usability restricted the potential of tooling by limiting the number of people who could use them successfully. Floods of alerts and low fidelity security reports created pushback among development teams.

Security teams have realized that they must strive to ruthlessly remove friction from the security process and work security into developer workflows. They cannot depend on ongoing engineering work from developers to maintain visibility into the cloud, and without developer support and buy-in, security teams will be left in the dark and face an uphill battle to remediate what they do find.

The shift towards removing friction has created a demand for agentless and unified approaches like CNAPPs.

Why organizations are looking to CNAPP

The trends above impact security across many facets, but the common thread behind them is unification and removal of friction. First generation cloud security tooling has created silos, leading to fragmentation and friction across security data and cloud teams. CNAPP addresses these problems by unifying data across the cloud estate and making security something that teams across the organization can get their own value out of. Let's take a look at some of the reasons why security teams are using CNAPPs today.

01.
To keep up with the cloud

To keep up with the pace and scale of the cloud, security teams need to have full stack visibility into what's deployed and what changes. This cannot be done with narrowly focused tools that require manual correlation, or with agent-based solutions that are too slow and difficult to deploy. CNAPPs leverage cloud provider APIs to scan the full stack of the cloud estate and deep into every workload, providing security teams with a full asset inventory and visibility into correlated risks across vulnerabilities, misconfigurations, network exposure, exposed secrets, malware, and more. The breadth and depth of CNAPP's agentless scanning allows security teams to understand their cloud environments and stay on top of changes so they can ensure they're not missing anything.

02.
For context and prioritization

With cloud infrastructure security data spread across multiple tools, security teams have to rely on painful, manual correlation efforts to understand their cloud risks, and have no way of knowing what crucial context slips through the cracks between tooling. CNAPPs unify interconnected risk factors into one view, giving security teams the context they need to properly explore and prioritize risks in the cloud. By being able to identify, for example, all VMs with critical vulnerabilities, admin access to key resources, and public exposure to the internet, security teams have everything they need to empower developers to quickly remediate the highest priority risks in their environment.

03.
To make security proactive

The only way to move fast and have security keep pace with the speed of deployment is to democratize security across developers, operations, and security teams. Each team involved with the cloud must have a stake and a role to play with securing it. The trends above speak to this: shifting left, moving security pre-breach, empowering DevOps. The only way to do this is to remove the friction that security has traditionally brought into the software development lifecycle. CNAPPs do this in three main ways: applying one policy across the pipeline, providing dedicated views for developers and operations of their areas of ownership with all the remediation context and information they need to be proactive, and by automating the routing of high priority risks to the right teams at scale through workflow integrations.

What purpose should a CNAPP serve?

With these trends sweeping the industry, the reasons for the rise of CNAPP are clear. The question then becomes what exactly a CNAPP should do and be in order to help security teams address these trends. We see that question as a straightforward one. CNAPPs should address a simple question: where do I have the biggest risks in my cloud and what do I need to do to fix them?

CNAPPs should tell security teams what the most pressing risks are that they have in the cloud or application in production or that they're planning to deploy. This is the foundation for everything. This means that CNAPPs must cover the breadth of your cloud workloads and architectures, including containers, VMs, serverless, PaaS, and function across cloud service providers. They should cover the development lifecycle from artifacts to runtime. And this breadth and depth of coverage must be unified into a single view and data model.

From this starting point, the next concern for CNAPPs is helping security teams figure out how to address their biggest risks efficiently. CNAPPs should enable security teams to take action at scale – by implementing detection and prevention capabilities in the deployment process and production. Protection comes from a place of understanding. Understanding comes from visibility and context. The purpose of a CNAPP is to provide visibility into the cloud environment and context around risks so security teams can work at the speed and scale of cloud.

When in place, CNAPPs should provide security teams with visibility across their entire cloud estate and into each workload. With this full asset inventory, CNAPPs should then analyze across layers to identify the interconnected risks across resources, help security teams accurately prioritize those risks, and provide all the information and context necessary to remediate them. By unifying these capabilities, CNAPPs help organizations reduce complexity, break down silos, and improve the security interconnection between developers and security teams.

The future of CNAPP

CNAPP is a relatively new market category today, representing the consolidation of several technological capabilities and a unification of purpose. Naturally, this means that the category is going to be noisy. However, CNAPP offers the industry an opportunity to build a more robust environment that lets security move faster at a lower cost. Over time, CNAPP will be the way that a cloud developer ensures that they are doing well on the security front. Since CNAPPs are usable and consumable by developers and operation teams, they will allow those teams to be more proactive with the security of their resources.

Today, security teams have very few opportunities to tell if they're in a good state with their security. They don't have a way to tell if they've taken the right steps to secure the cloud, or if they've left some areas wide open. CNAPPs will allow any cloud developer to see that they are taking the right steps for securing their applications and resources, and for security teams to validate the state of security across their cloud applications without gaps.

As cloud adoption continues to increase, and teams leverage more cloud technologies, implementing cloud-native security is becoming more crucial. Shifting trends across the security industry are highlighting the need to address more comprehensive risks and approaches, reduce friction and complexity, and democratize security across multiple teams and stakeholders. The rise of CNAPP is a direct response to these trends and needs. As with any nascent space, it's easier to market than deliver, so ensure that any CNAPP you consider is able to adequately address the underlying drivers and changes that are causing your team to explore such a solution.