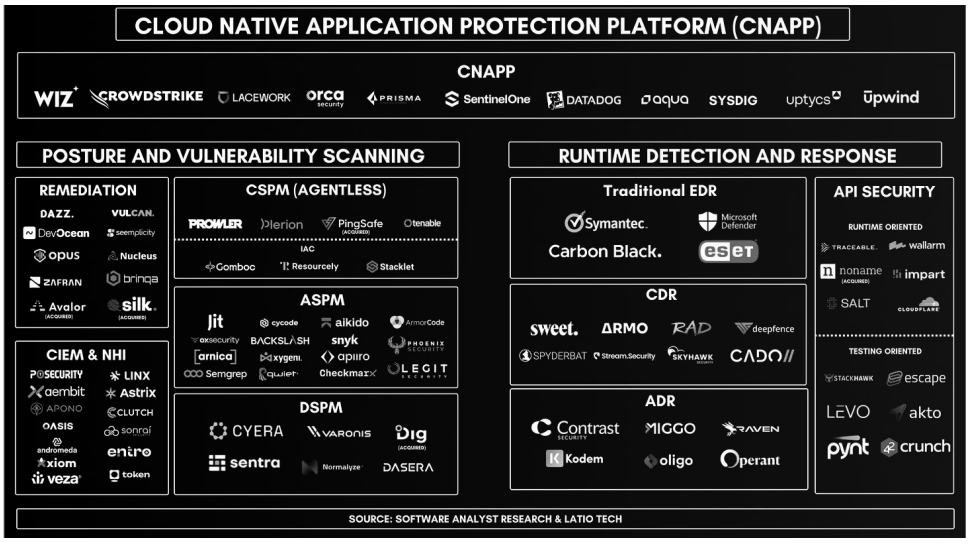
Redefining CNAPP: A Complete Guide To the Future of Cloud Security

This report provides a holistic view of cloud security's evolution and provides a framework for redefining the future of cloud security.

FRANCIS ODUM AND JAMES BERTHOTY
SEP 12, 2024

75 13 6 Share

Readers, today I'm incredibly excited to publish one of the biggest reports I've ever done within any cybersecurity industry. This report provides a holistic view of cloud security's evolution, tracing its major milestones, a detailed breakdown of the key vendors today, and evolving market shifts. It presents a new framework for redefining Cloud Native Application Protection Platforms (CNAPP), addressing its limitations and contradictions while offering a comprehensive roadmap to navigate the future of cloud security. James Berthoty and I have been working for months to make this report happen today. We hope you enjoy every part of it.



Authors of the report

- Francis is the founder of the software analyst research platform that helps security leaders understand emerging themes and industries in cybersecurity.
- James is the founder of the Latio Tech platform and newsletter, which helps engineers find & understand security tools.

Key Actionable Summary

If you only have 5-minutes to read the report, here are the key takeaways:

Wiz - EXHIBIT 1125
Wiz, Inc. v. Orca Security Ltd.
IPR2024-00865

1. This report explores the evolution of cloud security vendors over the past 14 years - taking you through how we got to this critical juncture, and using historical context to build a vision for the future.
2. We discuss the consolidation trends, as cloud security vendors merge adjacent solutions, particularly in Application Security and SOC operations, and analyze why some vendors have outperformed others.
3. We provide in depth analysis of companies like Wiz, CrowdStrike, SentinelOne, Orca, Upwind, Sweet Security, Palo Alto Prisma Cloud, Jit, Rad, Armo, and Dazz, as representative players in the evolving nature of the CNAPP market.
4. Beyond merely categorizing vendors, we discuss limitations of the current conception of CNAPP as an all in one security platform. We propose some new perspectives to try and address the following contradictions on the market:
    - **Increased spending, decreased satisfaction**: Despite rising cloud security budgets, end users remain dissatisfied.
    - **Feature overload**: The most successful CNAPP platforms offer fewer features, even though demand for functionalities has grown.
    - **Agentless vs. agents**: Companies that once championed agentless solutions are now all building agents.
    - **Developer vs. Security Analyst persona's**: CNAPP tools are used by developers and analysts, despite these personas having vastly different needs.
    - **Old innovations in new packaging**: Code scanning and runtime security are being hailed as breakthroughs, but they've been around for years. The market wasn't ready for them yet, is it ready now?
5. The Cloud Security market continues to grow and proves to be an unavoidable reality for legacy providers - who push forward acquiring their way into the market. Wiz added $150M over two quarters! CrowdStrike grew by double over the past two years. Other large enterprises continue to acquire cloud startups to augment their offerings, such as SentinelOne and PingSafe, or Tenable and Ermetic.
6. The CNAPP feature set continues to expand, with analysts both lamenting the complexity while pushing for the category to be an all in one solution. CNAPP also struggles to span across posture and runtime, as enterprise security companies struggle to address all aspects of security in a single platform
7. There is still demand for cloud security tools, with companies viewing these solutions as the cornerstone and beginning of their security program. However, practitioners and CISO's alike are frustrated with the tools they have. There are too many tools, and too few results.
8. Practitioners are frustrated by a lack of context, alert fatigue, and the general pain of having small teams manage the security tests and detections for teams 100x their size. They're being expected to understand the details of an impossible number of infrastructure configurations.
9. CISOs are frustrated with the wasted time and developer complaints, all without much to show for it. Their teams have to spend hours troubleshooting alerts, and

many cloud breaches go totally undetected by their CNAPP.

10. This is our first report on the market's state. In our next report, we'll explore future trends, themes, and predictions of how we think the market will evolve.

Our report offers an honest assessment of where the market stands today and where it's headed, helping you navigate the complex and ever-evolving world of cloud security.

If you found both of these reports helpful, please subscribe below:

Thanks for reading The Software Analyst Newsletter! Subscribe for free to receive new reports on Identity, SOC, Cloud & AppSec and support my work.

Type your email... Subscribe

Latio Pulse
Weekly insights into Cloud, Application & Product Security
By James Berthoty

Type your email... Subscribe

Brief History of Cloud Security

The core of pre-cloud security was only two solutions: endpoint detection response (previously antivirus) and network security via firewalls. These core technologies birthed the largest mass market companies as their leaders, CrowdStrike and Palo Alto Networks. To be sure, there were plenty of additional vendors outside of these core functions, from e-mail security to vulnerability scanning, SIEM for the enterprise, but the core of the mass market was split between EDR and firewalls, technologies businesses of any size could justify an investment in. Even SMBs would have a firewall in front of, and an EDR running on, their servers.

In the early day of cloud, vendors rushed to deploy their existing solutions into this new environment. After all, Palo Alto firewalls can be deployed as virtual appliances, and a server is a server - whether in your datacenter or Amazon's. Only early visionaries saw that the transition to cloud actually opened a section of the datacenter to security that was previously unavailable: the end to end configuration of the resources themselves.

As security teams evolved, the question became less “how can I take my existing tool and run it in the cloud” and more “how can I figure out what the heck is going on up there?” Discovery and context became more urgent needs than porting existing tools that never quite worked right. Basic EDR functionality and basic network protection now also came out of the box with GuardDuty, Security groups, and other native capabilities in AWS.

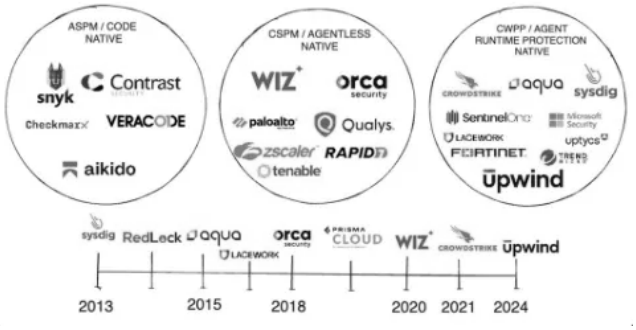
What was really happening with this transition was from traditional architectures to containers. Security teams were frankly late to the party, realizing only later that the workloads themselves in the cloud were shift from servers to containers. Existing players had massively invested in Windows protection, with very little support for Linux at the time, never mind the container layer. Beyond just needing Linux support, teams needed deeper visibility into containers.

Evolution of Cloud Security

Innovators saw the opportunity across two areas: access to the cloud APIs for visibility and the need for container insights. Cloud Security has changed massively in the past 10-14 years, trying to evolve and maximize the power of these two seemingly simple innovations. Early vendor “CSPM” products quickly became commoditized, as interrogating cloud APIs for misconfigurations became common fodder for open-source projects like Prowler or ScoutSuite.

Even in these early days, the split between posture and runtime was apparent but never fully understood by the industry. Sysdig launched container runtime protection with Falco, its posture-based foil being the kube-bench from Aqua. CSPM experiments like ScoutSuite, focused on auditing, had more complex workload-focused alternatives like Cloudmapper.

Rather than positing some hidden genius behind the approaches of these early companies, it’s more likely that a combination of luck, agility, and connections helped cement the early discussion of cloud security into agent vs. agentless instead of posture vs. runtime. While cutting edge developers were ready for container runtime solutions, the broader security market was still exploring general visibility and trying to catch up to their developer counter parts. Unlike these early days, when people hear “CSPM” in 2024, they assume some level of workload visibility comes with it - that is the core of the transition from generation one cloud security to generation two, the assumption that the workloads are along for the ride.



Pivotal Moments in Cloud

The 2010-2014 (CSPM and the Shift to Cloud)

- **Dome9 was founded in 2010**, while they weren't named a direct cloud security vendor, they were focused on compliance checks and governance solutions for cloud environments. They were eventually acquired by Check Point Software Technologies in **2018**.
- **Evident.io** was founded in **2013** by Tim Prendergast and Justin Lundy. The company focused on compliance monitoring for public cloud infrastructure, and helping organizations detect misconfigurations.
- **RedLock** was founded by Varun Badhwar and Gaurav Kumar. They started out focusing on providing visibility into VPN flow logs and network visualization. However, customers started to pull in RedLock to help identify misconfigurations and manage compliance for cloud environments. In 2018, it was acquired by Palo Alto Networks.
- **Qualys, Tenable and Rapid 7**: It's important to acknowledge that these vulnerability management providers existed to help companies find misconfigurations primarily within on-prem environments before subsequently moving to the cloud. However, Tenable found early success in cloud environments due to the network based scanning of Nessus being much more scalable than agent deployments. This was perhaps the only hint of the agent vs. agentless scanning debate that would come to define the later years.

2015 - 2018 (Innovations in Workload Security)

- **Twistlock**: Founded in **2015** by Ben Bernstein and Dima Stopel. Twistlock was an early player in container security, specializing in securing cloud-native applications, containers, and microservices. It was acquired by Palo Alto Networks in 2019, and has kept Prisma Cloud competitive even with minimal feature updates.
- **Sysdig Security**: Although Sysdig was formally founded in 2013, the company rose to prominence in 2015 when they launched "the first and only container-native" solution. Sysdig was founded with a focus on **container runtime security**, enabling users to monitor and secure cloud-native environments with containerized applications using an agent.

- **Aqua Security:** They were founded in 2015 with a similar vision to secure cloud-native applications, particularly focusing on containers, serverless computing, and Kubernetes environment. Aqua's open source solutions, especially their vulnerability scanner Trivy, have been lovingly adopted by their customers and competitors alike (Trivy silently powers many of the vulnerability scanners out there, especially early on!).

Post 2018 (Synergies around CNAPP)

- **First Cloud Security Consolidation:** Palo's acquisition of Twistlock and Redlock is one of the pivotal moments in cloud security. Palo Alto Networks deserves a lot of credit for the vision of CNAPP, and taking a big bet to enter the space from day one. By acquiring RedLock and Evident.io in 2018, then later in 2019 acquiring Twistlock, Palo created the first truly consolidated cloud security offering (aka, what we call now CNAPP). By duct taping together RedLock and Twistlock, Palo Alto put forward a hypothesis still unproven: that customers want one platform for runtime and posture. Due to their size, Palo quickly defined the market around what they were doing, moving the conversation from CSPM vs. CWPP, to the consolidated CNAPP. They could also justify their massive valuations on the product offering, as many companies just wanted visibility, but were convinced to buy container and cloud visibility in the same place. Another overlooked piece of early sales was companies looking to offload the shockingly high cost of ingesting cloud logs into their SIEM.
- **Orca**: Introduced the concept of **agentless side scanning**, which allowed for deep visibility into cloud environments, and workloads, without the need to install agents on each workload. CSPM can be defined by pre and post-Orca: the ability to view workload data without an agent was a genuinely genius innovation - utilizing the nature of cloud APIs being accessible to vendors.
- **Wiz**: Wiz pushed agentless scanning to new limits, most importantly by introducing the intuitive graphing of asset relationships to security teams, and building their entire UX around that capability. They also showed publicly accessibly resources, and pushed what visibility was possible without an agent. They evolved to build upon the agentless approach, by building around the graph and providing a uniquely low time to value. During this time, other vendors were slow to recognize that agentless scanning was a major gap in their capabilities, and now almost every major vendor offers the capability with different maturities.
- There's a conversation worth having about how difficult it was for older providers to come to terms with the success of agentless scanning. They were absolutely right to be skeptics: from a security perspective, agentless scanning was nothing compared to what attacks they were able to detect and protect. They missed however that security teams were not yet in the weeds of these architectures, and didn't know what they didn't know. Agentless scanning was the first step of a security journey, and that's why everyone needed it in order to stay competitive.
- Wiz's true strength is in their ability to come to market at exactly the right time to meet customers where they're at. Rather than sit on their agentless success, they introduced an agent when people started asking for it. They improved their DSPM

capabilities as teams cared about it. Most recently, they announced Wiz Code just as security teams are catching onto the power of ASPM capabilities. Wiz is frightening to the market precisely because they're not just a history lesson stuck in what they invented, but continue to release just the right features at just the right time to appease the majority of the market.

Summary of the evolution

Phases of Innovation: Cloud security has evolved in three clear phases:

1. The era of cloud posture and misconfigurations (2010-2015). This was the era of exploring scanning cloud APIs for misconfigurations.
2. The era of runtime experimentation (way ahead of its time) as containers, and microservices grew in adoption (2013-2018).
3. Finally, the era of agentless scanning and consolidation (2019-2023)

What does 2024 and the future hold? Teams are fundamentally frustrated with two competing ideas:

1. They have too many tools
2. They have bad tools, creating noise instead of solving their problems

The next great question of Cloud Security is asking what teams want more - further consolidation or better results with fewer features.

Deployment options for cloud security (Agent vs Agentless)

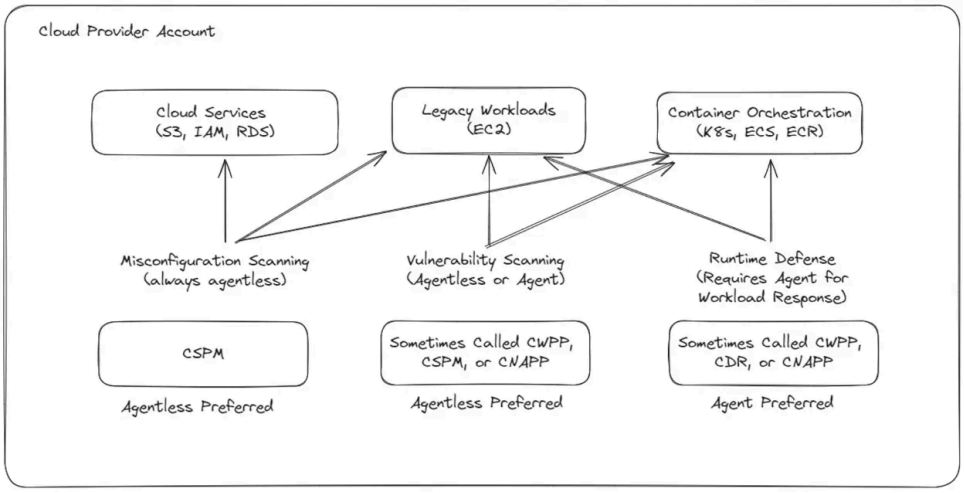
One of the central discussion points about the evolution of cloud security is how much the role of agents and agentless played throughout the history, and how relevant the question is today. There is no doubt, the pivotal moment was the introduction of **agentless** scanning by companies like Orca and Wiz. Agentless scanning was a turning point - but anyone who tells you they knew it at the time is lying. We're old enough to remember when these tools were finding their messaging foothold - trying everything from risk based prioritization to compliance scanning. This was a subtle industry move that wasn't appreciated until years later, in no small part due to how Wiz used it to define the CNAPP conversation.

We especially love a quote from one former marketing professional at a Wiz competitor - "We allowed Wiz to define the conversation around agent vs. agentless scanning, where all we did from marketing to sales was defend the benefit of an agent. This focus stopped us from focusing on the real message and what we actually did better: securing the cloud." Wiz made every sales call revolve around time to value and the ease of agentless, instead of trying to touch the complexities of containerized workloads - **something security teams still have resisted learning.**

Let's set the context and understand some basics. When organizations move to the cloud, their first problem is visibility - AWS just shows them a bunch of EC2 instances without even names to identify what they're doing. They have two deployment options to scan for vulnerabilities, and just get general insights into these workloads:

1. Agent
2. Agentless

The below chart gives a glimpse into the complexity of the decision between agent and agentless, with solutions having complex tradeoffs depending on workload types. Instead of digesting this complexity, many security teams made a much more simple calculation: do I want to bother developers or not? Combined with complex messages in the market about "how to secure Kubernetes," agents became "something to do later" rather than "something I need now."



Source: LatioTech Substack

Evaluating Agent-based solutions in 2024 (The Return of Agents?)

Agents are super challenging to get objective data on. Step one for evaluation is deploying a Kubernetes cluster, so many security teams are already unable to get meaningful results in a PoC. Latio provides a testing repo to try and help security teams accomplish this, but testing comparative agents in this evolving landscape is almost unheard of.

Here's what matters for professionals thinking about agents in 2024: performance has gotten better, insights have improved, and installation has gotten easier. In the dark days, agent deploys required multiple manual rollout commands from DevOps teams. Now, modern solutions are all helm charted, allowing for quick one line installs, or deployment via ArgoCD. It's essential to note that eBPF is safe but new - it won't crash the kernel, but it's the wild west of innovation, meaning no two agents will be exactly the same, in terms of both performance and visibility.

Pros

- **Agents can detect and mitigate threats in real time,** allowing security teams to respond to incidents faster. They are particularly useful for industries where rapid incident response is critical, such as finance and healthcare. This is also very relevant if an organization has workloads across cloud and on-prem systems.
- **Granular Data**. Agents are useful for everything from reachability analysis to looking for non-human identities in application contexts. Beyond reachability data, doing incident response in the cloud requires contextual data to be at all effective - too many solutions still don't give SOC Analysts the data they need to take effective response actions to cloud threats.
- **Deep Visibility and Control:** Agent-based solutions offer granular visibility into the behavior of the underlying workloads, processes, and system files. This allows for deeper insight into runtime environments, configuration issues, and active threats.
- **Containers. Period.** Containers are the infrastructure of the cloud, powering the vast majority of cloud workloads. Agentless solutions are severely limited in what they can show - they fake it with vulnerability data, but things like process executions, file access, and remediation contexts can only be gained with an orchestrated agent.
- **Emergent Application Layer Detections.** The most innovative agent based solutions are reaching deeper into the application running on workloads themselves, giving robust visibility security teams have never before had access to.

Risks

- **Deployment**: Traditional agents struggle with **complex deployment and maintenance.** No matter how good an agent deployment gets it, with many vendors now offering one line CLI commands to accomplish it, this is access the security team rarely directly has. Step one to showing value typically requires security to poke DevOps teams, something they're already hesitant to do. With modern vendors, this **is a bigger fear than any real technical issue.** Ambitious security teams should also use this as an opportunity to learn containers, rather than fearing the learning.
- **Performance Questions**: Container monitoring solutions rely on new implementations and experimentations with eBPF and other telemetry solutions. eBPF is incredibly flexible, with no default paradigm for keeping performance at acceptable levels. While it won't crash the system, this flexibility leads to wildly divergent performance implications between vendors, which are difficult to assess.
- **Workload Edge Cases**: At this point, most vendors support Kubernetes, and self hosted container deployment solutions. However, there are workload edge cases such as serverless and PaaS where agents struggle to accomplish much. Even these have their use cases though, with vendors experimenting with different methodologies to cover these edge cases.
- **Response Anxiety:** Many companies tense up when it comes to the idea of allowing automated response actions, due to bad histories with other vendors or

solutions - from WAF to EDR. No one trusts agents to break their production web app.

How Agentless Scanning Emerged

As discussed earlier, Orca launched the first version of **agentless side scanning**, which allowed deep visibility into cloud workloads without the need to install agents. Subsequently, Wiz was able to make the experience more intuitive with the graph and more fully bring the approach to market. There's a lot you can do without an agent, and with most security teams already overwhelmed by that work, it's hard to argue they're looking for even more to do.

Pros

- **Quick deployment and rapid-time to value**: Agentless solutions are easier to deploy since they do not require installing software on each workload. They leverage cloud APIs to snapshot underlying instance hard disks, copy them into the security vendors account, where they're hooked up on the vendor's side and scanned. This creates an elegant "like magic" approach - where you get full visibility into the workload, without any instrumentation.
- **You can get good context without an agent.** Beyond the snapshot scanning, agentless solutions are able to build full cloud attack graphs, look at network traffic with flow logs, perform secrets scanning, and really function as full asset management systems. While you don't get as much total context without an agent, it would be disingenuous to say you get nothing.
- **Suited toward multi-cloud and multi-OS**: Agentless solutions are particularly suited for organizations that operate across multiple cloud platforms (AWS, Azure, GCP, etc.) with multiple workload types (Windows and Linux). They provide a unified view of security posture without the complexity of managing agents across various platforms. Additionally, one easy scanner across all your workload types is a lot simpler to manage than specific deployments for different types of workloads. Windows is another elephant in the room, as most CNAPP vendors have opted to focus on containers and Linux.

Limitations

- **Agentless solutions are fundamentally work generators.** Agentless solutions discover all sorts of problems - some of which are real, some of which aren't. But ultimately, they don't independently solve a single problem.
- **Containers are ephemeral**. Agentless scanning doesn't fit the containerized world well, because many containers run for only seconds at a time. No matter how "real time" agentless scanning gets, the insights will always be limited. To be clear, agentless vendors have gotten good at faking some of this visibility, but they can never know the real time activity of containers in detail.
- **Efficacy and high false positives**: Agentless solutions rely on data collected from cloud APIs which don't have workload data, and sometimes are missing relevant security data altogether. This can lead to inaccurate or incomplete results.

Companies complain that while they appreciate the ease of deployment of agentless solutions, they still experience a higher false-positive rate compared to agent-based systems, particularly when monitoring for deeper threats.

- **Hidden lack of support.** Agentless scanning of underlying system volumes is amazing!...when systems have underlying volumes. Unfortunately, security teams who dig deep will find a surprising number of workload types that don't have volumes - whether cloud workloads with nvme drives or RDS clusters.
- **Hidden costs.** Snapshot storage and network transfers (depending on configuration) ain't free! AWS doesn't mind the extra price, and security vendors certainly don't go out their way to let you know that a small increase in cloud costs is coming along with their agentless magic.

Overall, the story of CNAPP is the story of security teams looking for agentless visibility solutions, before maturing into agent based ones as they learn that their cloud is mostly containers. Security teams start wanting visibility, and quickly realize that they don't have as much as they thought. This is precisely why Wiz didn't just "used to lead" the market, but still does. Their choice to invest in an agent allows them to continue to meet security teams where they're at - offering the right amount of visibility as their customers want it. Conversely, the decision by runtime providers to build agentless scanning hasn't moved the needle as much for them because their buyers were already farther along in their journey.

It's worth briefly noting that most major players now have agentless scanning as well as agent based offerings, and what we're really talking about is interface of interacting with those features, the depth of their capabilities, and how those features translate into a complete user experience.

Frameworks For Understanding Cloud Security Today

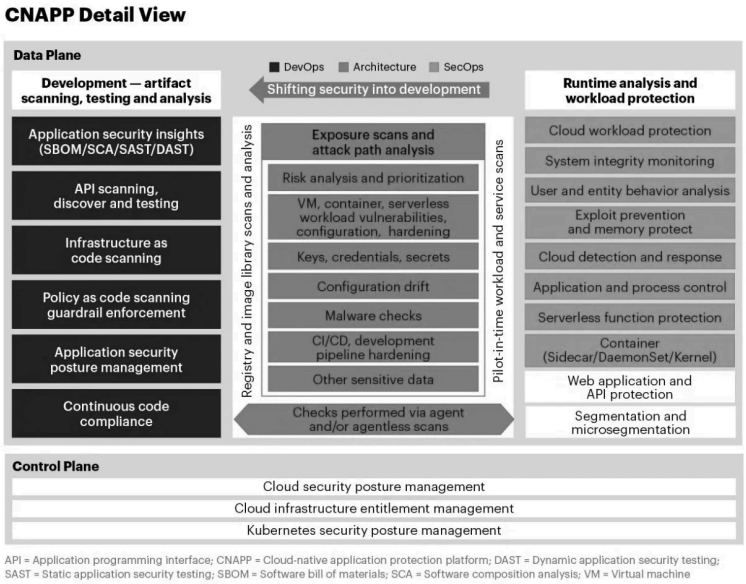
CNAPP by Gartner

We have some disagreements around how CNAPP got its start - Palo Alto had a hypothesis that people wanted Twistlock and Redlock in one place and forced their will upon the industry. A less cynical approach is that most CISOs wanted protection for their cloud. That protection started with visibility into the cloud, and visibility into containers. This fundamental logic is sound; indeed, it's what drove James' decision to be an early adopter of Prisma Cloud (as much as he hates to admit it). Security teams needed something to help them tackle the cloud - whether that mean learning their containerized environment, or finding unencrypted databases their compliance team was asking about them.

It's only recently that CNAPP has gotten to the point of almost comical bloat - would we have ever talked about a "data center application protection platform?" Enterprises,

along with analyst firms, continue to push the idea that CNAPP means all in one security.

One fascinating dichotomy are these articles from Forrester which we'd argue contradict. The first argues that CNAPP is crowded and bloated (we agree). The second argues that CDR doesn't exist as a category because it's part of CNAPP. This is exactly the innovation stifling the first article complained about! If CNAPP is really what Gartner describes, there are no other categories. If we want real solutions here, we need to look beyond the mystical "no more problems" CNAPP promises. Let's start by breaking down the component categories.



Source: Gartner

Cloud Security Posture Management (CSPM)

Gartner explains that CSPM as tools are designed to identify misconfiguration issues, gaps in security policy enforcement, and compliance risks in the cloud by comparing cloud environments against a predefined set of best practices stated policies, and known security risks. One selling point continues to be reporting on compliance statuses for less technical GRC teams.

As we've discussed for much of the article, CSPM can really be segmented to pre and post-workload visibility capabilities. Early CSPM looked only for misconfigurations, new CSPM looks also at workload level misconfigurations. At this point, we argue CSPM can be simplified to asset management and vulnerability scanning in the same place, with misconfiguration detection layered on top. While this market is largely considered eclipsed by CNAPP, there is still room down the market, as CNAPP pricing has ballooned to unacceptable levels for scrappy teams.

Cloud Workload Protection Platforms (CWPP)

CWPP was always a weird category, because it was just EDR but it worked on containers. To be fair, it had a few additional benefits like vulnerability scanning and

experiments with network layer visibility. What makes this category weird is there was never a defined set of capabilities to what made something count. Vendors often call themselves CWPP while only providing vulnerability scanning. Other vendors call themselves CWPP with only runtime defense solutions. What counts as "workload protection" has always been unclear. In a phrase, CNAPP = Redlock (CSPM) + Twistlock (CWPP). CSPM provides the cloud visibility, CWPP provides the container visibility. This term has grown less commonly used because of the lack of clarity. We prefer Cloud Detection Response (CDR), meaning providing detection and response across cloud and workload layers.

Limitations of CNAPP

James once described CNAPP as saying, "**I am CNAPP, destroyer of startups. Let's do everything, but a little bit worse."** CNAPP at this point has become bloated to the point of mockery. I've seen demos where vendors click 6 screens deep to show a giant table of application layer vulnerabilities. Finally, what practitioners have always wanted, even more vulnerabilities that don't matter. The key problems of security right now are:

1. Too much noise
2. Not enough value

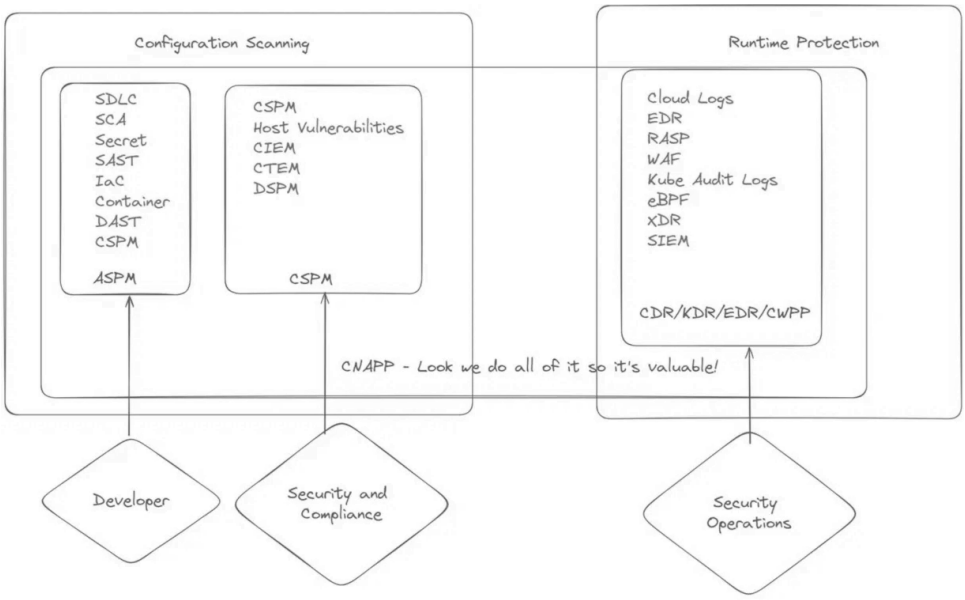
Here's why James argues CNAPPs create more problems than they solve:

Developers and Security Operations don't want the same things

Developers want (or are forced) to see vulnerabilities in their code, and how those vulnerabilities were picked up in production. A developer does not care about a runtime exploit alert, they're too busy assigning story points and taking midday rejuvenation breaks in their nap pods while complaining about project managers. Developers receive tickets, their performance is assessed based on tickets, and they work out of IDEs and pull requests.

Conversely, security operations teams live in the SIEM. They query logs to respond to attacks and put stories together. They take response actions to attackers, and figure out blast radius. These are things developers would pay not to be involved in.

The only thing that unites these teams is the need for context; however, everything else - from UI, to workflow, to the data they care about is radically different.



Source: Latiotech

Defining a Security Engineer?

No two security engineers are really alike. The line between "appsec" and "cloudsec" is slowly disappearing into "product security," with one primary function being "vulnerability management," which is slowly becoming its own discipline. Product security paves paths, vulnerability management helps patch, the SOC responds to threats, and GRC creates and audits policies. CNAPPs have really only served cloud security engineers by providing asset visibility, but will really struggle to appease more holistic practitioners who have evolved deeper into application security.

The Future of CNAPP?

CNAPP has created a crappy version of too many standalone products and is at a serious breaking point. Providers have forced themselves into having to dive head first into runtime protection and ASPM at the same time. They risk getting caught in the middle and made obsolete by both.

We are open to the idea that a CNAPP can pull this off, but no one has a UX that really delights the SOC and Developers at the same time. Wiz is well positioned to do this due to the flexibility of the graph with Wiz code and the Gem acquisition alongside their agent, but the execution will matter.

Another elephant in the room: Amazon GuardDuty and inspector keep getting better, with inspector now also supporting agentless scanning. There may be a play for vulnerability management as an "AWS cost/force multiplier."

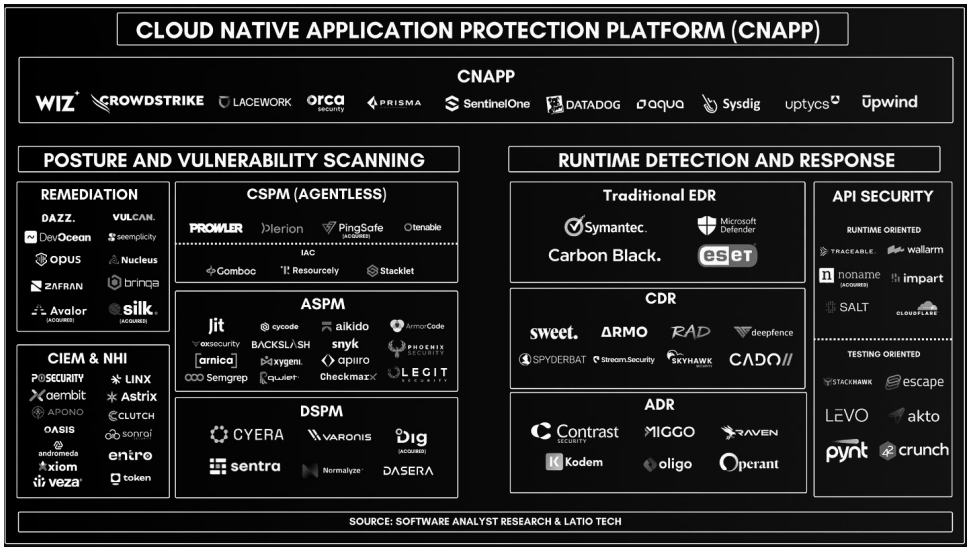
Based on their valuation and adoption, the most successful CNAPP right now is also the one with the least features. Execution around use cases matters more than Gartner feature checkboxes.

How We Should Think of CNAPP

This is our proposition for the CNAPP mental model: a series of functionalities aligning either to vulnerability detections, or aligning to runtime exploit detections. CNAPP product decisions are a complex nightmare of tradeoffs, which is why so many enterprises end up with more than one. At the highest level though, there are only two fundamental capabilities - either you're detecting vulnerabilities, or you're responding to threats. Security teams can opt to try and get all these features in a single place, but will face very real usability tradeoffs by doing so. Fundamentally, we believe these are the two areas:

1. **Posture and vulnerability scanning:** This area primarily focuses on proactively identifying misconfigurations and vulnerabilities in cloud environments before they can be exploited. This ensures a secure baseline and helps meet compliance requirements by scanning cloud resources and applications for weaknesses. The ICPs for these functionalities are all product related, with a bunch of titles in flux, such as developers, devops, devsecops, cloud security, or product security.
2. **Runtime detection and response:** This primarily monitors cloud workloads and applications in real time, detecting active threats and anomalies as they happen. This reactive approach enables swift action to mitigate attacks but may introduce complexity and performance overhead. The ICPs for these functionalities are all tied to security operations teams, with cool hacker titles like threat hunters, detection engineers, and security researchers.

Both capabilities are essential for comprehensive cloud security—one focuses on prevention, while the other addresses live threats. We've grouped these into subcategories as either posture or runtime:



Across two of these categories, we believe there are further sub-market categories within cloud and application by which we can further analyze each of these areas. In general, the platforms have sub-par versions of each of these capabilities, with

practitioners leveraging point solutions where they most matter. We provide a brief breakdown of these markets below:

POSTURE & VUL SCANNING

Cloud security posture management (CSPM)

As discussed in most of this report, CSPM provides agentless visibility into cloud workload configuration and vulnerabilities. It provides broad coverage and visibility into your assets. While runtime can be provided, it's not the core of the platform. This will continue to be a core piece of the acronym.

Application Security Posture Management (ASPM)

ASPM provides all of the application security testing tools needed to thoroughly test and secure applications. There are a lot of scanners and languages, so companies are more likely here to have many different solutions, leading to vendors who are also purely on the orchestration and aggregation of findings from different scanning tools.

Unified Remediation

It's well known that the more of these tools you use, the more work you're creating for your teams. These platforms provide guidance, de-duplication, and data enrichment to make fixing and tracking things easier.

Cloud Identities: CIEM (Cloud Infrastructure Entitlement Management) & Non-Human Identities (NHI)

CIEM has evolved into NHI, but both focus on tracing different permissions and what they can do in the cloud. The reality is that CSPM tools always did enough identity stuff for most teams, so the NHI acronym allows these vendors to better differentiate their focus into APIs, SaaS, and workload identities, where CNAPPs have not yet extended.

Data Security Posture Management (DSPM)

Teams have always looked at DSPM hoping for data tagging, and walked away with mixed satisfaction from this combination of tools. At its heart, DSPM provides insights into your data platforms - from object storage like S3 to relational like RDS. However, there is a similar problem here to CIEM, where CSPMs can do some of this too, so the question is how much that differentiation matters to the specific team.

RUNTIME DETECTION & RESPONSE

As discussed, Runtime detection and response focus on monitoring cloud environments and workloads while they are running to detect active threats, anomalies, or attacks in real time.

Every runtime tool says they support containers, but the reality of their detection capabilities, and the amount of context they surface for security teams is all over the place. The lines of demarcation between these three cloud categories are rapidly

disappearing, as Latio argues by creating a new category, CADR. However, this is our analysis of the different categories as they exist today.

Traditional EDR

These tools are just EDRs that run in the cloud. They are best defined by focusing on static servers, and **file based detections**. One easily identifiable feature gap between this category and cloud detection response is if a Kubernetes visualization can be made rather than just a process tree.

Cloud Detection & Response (CDR)

CDR is detection and response built for the cloud. A small segment of this market (Gem, Stream, and Skyhawk) is committed to an agentless approach, thinking of cloud only as cloud APIs and flow logs. However, because the cloud runs on Linux and containers, it's our stance that the heart of CDR includes its workloads, making container security a cornerstone of what proper CDR means. For clarity, the agentless CDR players typically take an integration approach for visibility into those workloads anyways.

Application Detection & Response (ADR)

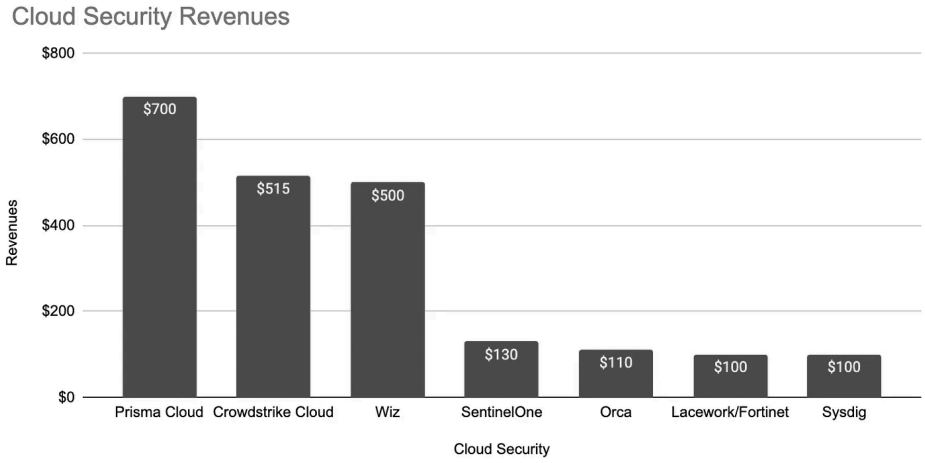
ADR is a rapidly emerging market with a ton of hype. These vendors are expanding outside of just the container, into application context more holistically. This market is new enough that each vendor's approach is radically different, what unites them though is their defense of the application layer without requiring any code changes. Code changes are what made RASP never take off, end to end application detection without a single code change clearly differentiates this market from EDR.

Vendor Landscape & Ecosystem Discussions

Based off the CNAPP acronym we have laid out above, we believe there are different vendors to depict different components of the market. The vendor list we have included at the bottom is not exhaustive list of all the vendors.

A core part of the vendor inclusion and criteria was based off the traction and growth traction on the market. If CNAPP means "every single security feature in the cloud," we'd have to spotlight thousands of vendors. In order to choose who we spotlighted, we focused primarily on covering the biggest revenue players, alongside some smaller ones that we're each personally excited about for different reasons. If you ever want the exhaustive list, it's on Latio's site.

Using all available sources on the market and earnings reviews, these are revenue metrics for the major players on the market. Prisma Cloud remains the largest vendor. However, CrowdStrike is closely followed by Wiz (which will be the next great war of the clouds, with many customers currently on both platforms due to their different historical focuses).



Source - Author: Public filings, Press releases and Estimates

Major Vendors

Wiz

Wiz launched in 2020 as the last major entrant to the CNAPP market, addressing the most basic yet essential cloud security need— cloud visibility via agentless vulnerability scanning. This simple requirement came with complex implementation challenges, but Wiz executed on it exceptionally well, outperforming its competitors at the time.

Wiz had a clear understanding of the core issues in cloud security, particularly the urgent need of security for cloud Visibility, with detection and response evolving later. It prioritized visibility as the foundation, building a user experience focused on delivering fast, clear insights into cloud environments.



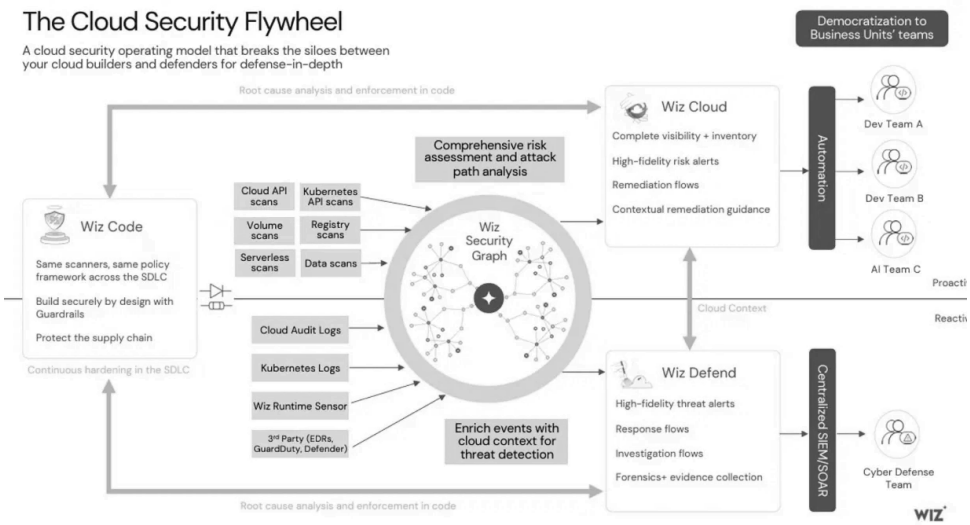
Despite entering the market later than many established players, Wiz quickly gained traction among enterprises seeking fast deployment and minimal upkeep. Additionally, the flexibility of their graph DB allowed them to easily add new types of assets and relationships as they evolved. The company grew rapidly, reaching over $500M in revenue within four years of its founding. Wiz differentiated itself by taking a graph-based approach to visibility, detection, high-fidelity risk prioritization alerts and an obsessive customer-driven approach, setting it apart from the competition. While the haters will attribute Wiz's rapid growth to strong marketing and the ease of implementation, that misses the core aspects that make Wiz the "lowest common

denominator" (that is, addressing the majority of needs for the majority of the market) of cloud security. Agentless asset and vulnerability management was what the early market really wanted.

Product Advantages

Graph User Experience

A core factor in Wiz's success is its graph-based architecture, from the actual database to the user experience. Cloud environments are composed of many interconnected entities like virtual machines, databases, and APIs. Wiz's graph model allows security teams to understand these complex relationships in a highly efficient way, querying the relevant information for the relevant teams.



This architecture provides deep visibility, enabling teams to analyze misconfigurations more effectively than competitors, and more importantly understand cloud contexts. For instance, security teams can easily create searches, and turn those searches into saved dashboards for other teams to use, driving product adoption across the organization. We believe a fundamental understanding of the graph is an underlying capability for their product success.

Evolving Beyond Agentless Scanning

It is widely known and should be emphasized Wiz launched a much more effective agentless scanner that helped teams identify vulnerabilities with incredible quick time-to-value and deployment for the largest enterprises. The underlying premise comes down to the fact that Wiz leveraged the graph to build out more advanced agentless visibility solution for software development teams to easily visualize threats across their network (internet-facing vs non-facing risks).

Underlying Wiz's true success has been meeting the market exactly on time as it evolves. Early on, cloud visibility was slow to become a problem for security teams, as they attempted to lift and shift their on prem tooling into the cloud. This problem was

much more prevalent between 2020-2021 when companies where companies rapidly moving to the cloud, but had to protect themselves attacks like Log4J and the CapitalOne breach. These incidents proved to be pivotal to Wiz success in that they had the right product for the right time.

Wiz offered a non-intrusive way to get that same visibility with agentless scanning, offering the basics when that's all security teams were ready for. Now, the market is evolving to see the pitfalls of a pure agentless approach - a lack of code context, and a lack of runtime defense. Rather than sit on their laurels and double down into the agentless approach, Wiz created an agent (almost two years ago), Github integrations, and expanded their DSPM. These individual components are not as advanced as some of their competitors; however, they continue to focus on user experience over features, with the features delivered right as their customers are needing it.

Attack Path Analysis

Wiz's graph-based system naturally supports attack path analysis. It can prioritize risks by evaluating the context of vulnerabilities and trace potential attack paths quickly. For example, it can map how an attacker might exploit a less critical vulnerability to move laterally across an environment, reaching more valuable assets. This context-driven analysis helps security teams focus on the most significant risks. To be sure, this feature has quickly become commoditized, as just about every CNAPP can make some pretty drawing of their cloud assets; however, Wiz continues to be rewarded for their early implementation, and how customized this can be with the graph search.

Effective Prioritization Engine

With CSPM in particular, security teams quickly became drowned with meaningless alerts that failed to drive business value. Wiz's prioritization engine was an early attempt to correct this problem. While competitors often scan individual assets in isolation, Wiz provides full context on how these assets interact and what risks those interactions pose. By using data clustering techniques and informed by the cloud attacker research of its' research team, Wiz ranks vulnerabilities, helping enterprises prioritize the most critical issues. Its low false positive rate ensures that teams aren't overwhelmed by unnecessary alerts, a notable advantage over rivals like CrowdStrike and Palo Alto, even if the other providers now have their own versions of this.

Customization and Ease of Collaboration

Customers (which are mostly developers and cloud-teams, not security teams) frequently highlight Wiz's user-friendly interface and automation features, which allow security teams to quickly prioritize critical issues, and create common dashboards with engineering teams. Its intuitive scanning engine detects vulnerabilities out of the box, requiring minimal customization. Wiz's scalability is another strength, as it easily adapts to increasing workloads and complex cloud-native use cases. While some customization is possible, the platform is designed to minimize the need for custom rule creation and manual intervention, handling common configurations natively.

Branding

While critics will define Wiz by "marketing fluff," they've actually done incredible work building a competitive brand to the likes of Palo and CrowdStrike through delivering real value and defining the conversation. First, Wiz has very few haters from a customer perspective, giving them a good industry reputation. Second, Wiz's marketing team effectively delivers real value - from their cloud security job postings site to their history of cloud breaches. Combined with genuinely helpful research led by the highly trusted Scott Piper and Alon Schindel, Wiz made meaningful community investments. Third, they're also really good at the marketing fluff, whether it's thoughtful gifts, custom shoes, or local events, Wiz runs a highly competitive marketing ground game. This frames any CNAPP evaluation with Wiz in the running. Combined with a little popular kid drama (who's Wiz buying or getting bought buy this week?), they stay in the conversation at all times.

Wiz has built a strong GTM organization around partners, CSPs, and unlocking large enterprise accounts. This is similar to what we saw in Endpoint security with Crowdstrike vs. SentinelOne.

A quote from a former competitive marketer offered deep insights when they said, "We allowed Wiz to define the conversation around agent vs. agentless scanning, where all we did was defend the benefit of an agent. This focus stopped us from focusing on the real message: securing the cloud." Wiz is continuing to define the conversation around their capabilities.

Areas To Watch

1. **Depth of Agent-based Capabilities**: While Wiz excels in agentless scanning, it has not fully matched the deep workload visibility and runtime protection offered by their competitors based off our customer discussions. It's worthwhile to note that Wiz has had an agent-solution for a longtime. Additionally, the ADR space continues to pick up steam, with these competitors having their own unique runtime offerings.. Most enterprise cloud environments are also mixed operating systems, where Wiz doesn't have a Windows offering, forcing them to supplement with Crowdstrike.
2. **ASPM and Code Scanning:** Other vendors have introduced their own SCA and SAST scanning, but this seems to have done little to move the market, as the offerings are really limited compared to full application security products. Additionally, many teams are turning to outside remediation platforms to provide code-to-cloud coverage and de-duplication. Wiz recently launched Wiz Code which covers most of the capabilities within ASPM. Most of this development was sped up by their earlier acquisition of Rafft at the end of 2023. Wiz Code leverages the security graph to scan code repos to CI/CD pipelines to cloud environments. The adoption of Wiz Code over competitors will be critical to watch over the next few months.
3. **Serving Multiple Personas:** Most CNAPP platforms have been built for cloud security engineers, who typically have systems engineering or DevOps

backgrounds. This has biased them heavily towards scanning and context. However, as detection and response capabilities become more prevalent, the user persona for these alerts will be Security Operations teams, who typically have very different preferences and requirements. No vendor has solved this split persona problem with a UX that can delight both personas. Although Wiz acquired Gem with their deep expertise in SecOps as former incident responders (IR)

4. **Pricing**: Though competitively priced, Wiz is not the cheapest solution. Early adopters benefited from discounts, but newer customers have found pricing less flexible. Midmarket teams looking for a basic cloud solution will be priced out.

Future Trends and Directions

As Wiz continues to grow, it has made several strategic moves to maintain its competitive edge. The company has expanded its capabilities beyond agentless scanning by developing an agent, enhancing its DSPM capabilities, introducing near real-time scanning, and integrating with GitHub and cloud event rules. This shift away from the original "agentless-only" model has been crucial in addressing new demands in cloud security, particularly with the rise of cloud detection and response (CDR).

The question remains whether Wiz can continue to extend beyond its agentless cloud security posture management (CSPM) strengths. As competitors evolve and the market becomes more crowded, Wiz's long-term success will depend on how well it adapts to new security challenges, particularly in areas like API security, identity, runtime protection, and DSPM. While it may not be the cheapest solution, Wiz's focus on automation, scalability, and ease of use makes it an attractive option for enterprises seeking fast, reliable cloud security. We highly recommend visiting the CNAPP Guide by Gartner on more details.

Crowdstrike

Crowdstrike launched their cloud security solution in October 2020. Over the past four years, they've successfully risen to generate over $515M ARR. CrowdStrike started as an EDR provider leveraging its Falcon sensor, and their entry into cloud was just installing that same sensor in cloud environments. Their cloud/container capabilities have slowly evolved over that time, but still lag far behind container specialists. That said, with many CISOs staffing a SOC around CrowdStrike, the advantage for their container offering is massive regardless of its actual capabilities.

Product Advantages

Windows-based environments

Practitioners like James have personally experienced the phrase, "Crowdstrike is the industry leader, we're going with them" in the face of contradictory evidence - or even no testing at all! Many security teams falsely assume that an agent is an agent, and that their existing CrowdStrike licenses can easily be expanded into the cloud. While in some cases this is true, especially in Windows environments, we believe it is not always

the case. Their massive existing install base that use the EDR agents with Windows workloads (that aren't going away any time soon) continue to be core to their success. With a few exceptions such as Sysdig, many CNAPP players have ignored Windows from a runtime perspective. This makes CrowdStrike or SentinelOne contracts almost a default need for most enterprises. Getting their foot in the door this way allows for easy expansion into cloud workloads. Additionally, the CrowdStrike contract will be seen as a non-negotiable for many teams who built their entire skillset around it.

Leveraging their strengths as an EDR and threat intel provider, Crowdstrike is able to detect and respond to behaviors that indicate advanced attacks. As a result, some customers have emphasized the accuracy of CrowdStrike's threat detection (AI-driven algorithms and behavioral analysis), citing a high true positive rate which makes it easier for security teams to prioritize real threats. CrowdStrike's access to global threat intelligence database gives it a significant edge in identifying new and emerging threats especially zero-day vulnerabilities and emerging malware.

While CrowdStrike has developed some API and agentless capabilities with its Falcon CSPM offering, Crowdstrike acquired bionic.ai to build out their own version of what an ASPM is. However, we believe it is lacking some core capabilities that define the category. To be clear, Bionic gave them an awesome technology - it detonates binaries to map out how applications work; however, calling such a capability runtime or an ASPM is really a mischaracterization of both capabilities. Bionic creates maps of what applications binaries **should be doing** at runtime - making it a theoretical map of a runtime state. It then imports vulnerabilities into that application map. This feature set allows them to say they have a competitive offering in ASPM, while offering neither true application security testing or true ADR capabilities.

Discounting

CrowdStrike was noted for offering flexible licensing options that allowed organizations to scale up or down based on changing needs. Unlike other vendors that require large, upfront investments, CrowdStrike provides more dynamic licensing, which appeals to organizations with fluctuating security needs. CrowdStrike's pay-as-you-go model has allowed companies to adjust their security coverage without requiring massive upfront investments. In general, we'll note that although, they offer customers lots of good deals, its pricing is seen as a disadvantage, with the platform being more expensive than competitors like Wiz and Orca, especially for organizations looking for more budget-friendly options.

Areas To Watch

Doesn't Meet Cloud Engineer Goals

CrowdStrike's entire user experience is built around a very specific user: operations teams responding to runtime threats via process trees, quarantining, and similar heuristics. Their UI doesn't measure up to CSPM's at providing asset context, ASPM's at providing developer insights, or Kubernetes providers at showing complete Kubernetes contexts. Genuinely expanding into these areas beyond acquisition plays will be a massive undertaking.

Overhead around agents

Despite its strengths, CrowdStrike's reliance on agent-based security solutions can increase operational complexity, overhead and costs, especially for DevOps teams that need to manage manual configuration for each cloud subscription or workload.

Limited cloud coverage

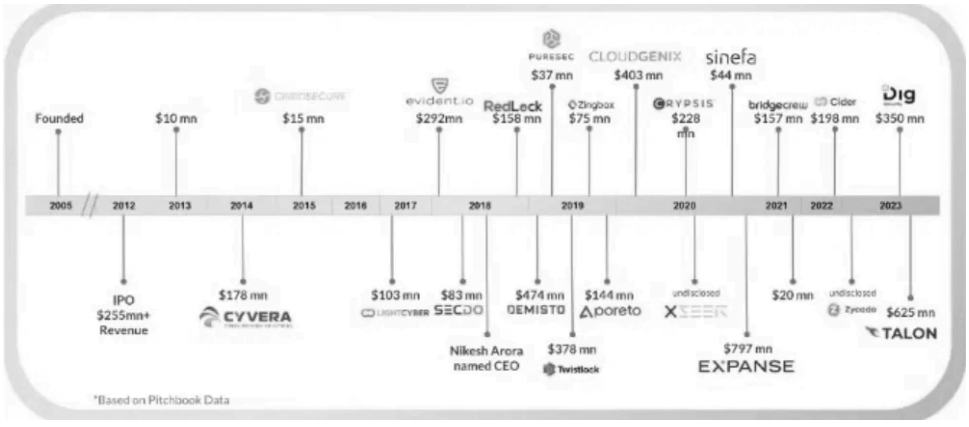
CrowdStrike's CSPM also suffers from limited cloud coverage, supporting only AWS and Azure. This makes it less appealing for organizations with multi-cloud environments, which require integration with platforms like Google Cloud or VMware.

Onboarding process

CrowdStrike's onboarding process has been noted as complex and time-consuming, requiring significant manual configuration, which can slow down deployment in dynamic cloud environments. James would like everyone to know that he can attest to this personally.

Palo Alto Networks Prisma Cloud

Palo Alto had the first vision of CNAPP. They paid $173M to acquire RedLock, one of the first cloud security vendors focused on identifying misconfigurations in cloud instances, and combined it with Twistlock, an advanced container security solution, creating an initial end to end vision of cloud security. They subsequently acquired Bridgecrew for IaC scanning, Dig Security for DSPM, and Cider to expand into application scanning more broadly. They used an acquisition-driven expansion strategy to build out a robust solution. To Palo's credit, each of these acquisitions were absolutely brilliant as far as the particular vendors they selected - each was way ahead of their time.



Source: Felicis

Comprehensive solution set

Prisma Cloud stands out as one of the most robust platforms (currently over 13+ modules across cloud and application security), offering security coverage across

multi-cloud environments, containers, workloads and code security with both agent and agentless solutions. It's storied brand name and longevity makes them easy to come into conversations. They've best been suited for enterprises in the Palo Alto Ecosystem. Prisma Cloud has been an ideal fit for organizations that are already leveraging Palo Alto's firewall or network security products, and their SOC solutions into a unified security platform.

Agent-based scanning built around their endpoint solution has seen success within organizations already on their install base. Their agent-based architecture provides deeper security insights into running workloads compared to agentless models, and Twistlock, even though behind on updates, has managed to remain competitive for a long time. Palo Alto utilizes RedLock Query Language (RQL) which enables users to create custom queries and rules for compliance and vulnerability detection. This allows users to tailor security monitoring to their specific needs. By defining unique policies and adjusting the security checks to a company's cloud infrastructure, an enterprise can ensure compliance with internal and external regulations.

This allows security teams to tailor Prisma Cloud's monitoring and reporting to meet specific compliance and operational needs. RQL is particularly useful for organizations with highly specific security and governance requirements, such as those in regulated industries. This customization sets Prisma Cloud apart from competitors like Wiz, which offer more automation but less granular threat hunting capabilities. RQL allows for deep flexibility and extensibility that security-conscious organizations often require.

Overall, Prisma Cloud is in a strong place because it's not incredibly bad at anything, it's just also not a delight at anything. It's hard to make a case against the platform from a feature perspective, because looking at feature checkboxes, they do more than most of their competitors; however, security teams are quick to tell you, "man I hate Prisma," due to the UI and feature bloat.

Areas To Watch

Lacking An Integrated and outcome driven vision

From what we've heard from practitioners, Palo still lacks a fully integrated risk view and they have higher false positive rates than competitors like Wiz and Orca. Some customers expressed frustration with Prisma's complex UI and the need for extensive customization to achieve desired outcomes, especially in earlier versions. Overall, it was noted that the platform still feels fragmented and lacks real-time consolidated risk reporting. Palo seems to have a cloud security strategy based on chasing Gartner acronyms for enterprise features. They tend to watch the market and try to acquire their way into success. This creates a disjointed platform driven by features rather than user experience.

Customization Comes at a Cost

While the flexibility through RQL (RedLock Query Language) allows for custom security policies, Prisma Cloud's heavy reliance on manual rule-based configurations makes it more resource-intensive. We heard that enterprises seeking a turnkey, automated

solution may find some of the agentless solutions like Wiz more streamlined approach preferable, as it reduces the need for hands-on management. RQL is also much less intuitive than graph searches or simple asset filters.

Higher False positives

We heard multiple times that Palo Alto also has more **higher false positive rate** than solutions like Wiz or Orca. Palo doesn't have the same agent as emerging vendors and therefore, deploying agents in Prisma Cloud can increase resource consumption, both in terms of cloud costs and operational maintenance, making it less cost-effective in some cases. Their CSPM engine also covers so many asset types, it's tough to call something a true positive finding when the "misconfiguration" is debate-able.

Orca

Orca Security made a big leap in cloud security with the introduction of its patented agentless SideScanning technique in 2019. This innovation introduced workload visibility without needing security teams to install an agent on endpoints or installing software on workloads for assessments.

They operate out-of-band by accessing cloud workloads at the runtime storage level, gathering crucial data through the cloud provider's APIs, while scanning disk snapshots. Their technology evaluates block storage bytes and reconstructs file systems, scans operating systems, and applications in a read-only mode, ensuring that virtual assets remain unaffected. This unique method allows companies to deploy Orca across their entire cloud environment without worrying about performance impacts or operational disruptions. For security teams, this means getting visibility into engineering workloads, without needing to bother them at all along the way.

Orca's SideScanning technology has proven highly effective for vulnerability assessments and scanning with a fast and unified database for attack paths especially for non-container assets. While Orca's advantages in agentless remains a key strength, it also has shown some limitations as cloud security teams start looking for more runtime data and visibility into their workloads. Critically, agentless scanning has always had difficulties being applied to ephemeral workloads, where what's on disk is changing minute by minute.

When it comes to its feature set and user experience, the comparison to Wiz is inevitable. Orca continues to go toe to toe with Wiz on its agentless feature set. There are real benefits to Orca: their data architecture is more scalable, they've continued to push agentless capabilities and offer very comparable risk graphs. However, going toe-to-toe with Wiz is exactly where most vendors we talk to are desperately trying not to be.

Orca's biggest challenges are twofold: brand and sales related. On the sales side, Wiz's graph search, and the ability to save those searches to per team dashboards, is such an organic experience of the capabilities that it's difficult to overcome on a sales call.

Once you're in the weeds investigating an alert, Orca and Wiz offer most of the same things, but the graph UX from Wiz makes the pitch really clear to first time buyers, especially someone coming from a bloated platform. On the brand side, Orca is in the unfortunate position of being directly compared to the undisputed marketing behemoth that is Wiz. Since they're forced to go toe to toe, they're also forced to bear the brunt of that constant comparison.

Recently, Orca expanded its capabilities by integrating source code scanning for platforms like GitHub and GitLab, helping companies identify risk hotspots, including code misconfigurations. As the emphasis continues to shift to cloud detection and response capabilities and containerized workloads, we believe Orca's most immediate challenge is the lack of an in-house agent.

SentinelOne

By acquiring PingSafe, SentinelOne is stepping into CNAPP with a big bet. SentinelOne and CrowdStrike have the same potential growth opportunities in the cloud, but the same difficulties as well. Both have powerful EDR platforms with massive install bases. Both have expanded into container security with mixed results, and then into the broader cloud context as well. Whereas CrowdStrike has built much of their CNAPP offering into their existing data structure, SentinelOne took a bold approach to ingest way more contextual data into their data lake.

The future of SentinelOne in CNAPP will be totally determined by their ability to execute on the power of their data. PingSafe as a CNAPP is inoffensive, with a few features that help it stand out from others. They have everything we've come to expect - vulnerability scanning, IaC, posture, etc. Their differentiator for SentinelOne is their ability to actually test exploits from the outside - cutting through the noise of CNAPP by validating the exploitability of resources. As a CNAPP, it's a competitive offering for existing customers to consider, but I don't see many people flocking to it over Wiz for example in a head to head comparison. Not that it's a substantially worse offering, it's just not 10x the way something needs to be to stand out in the space.

More core for SentinelOne's long term purposes, PingSafe's graph database of cloud and code assets can be leveraged for alert contextualization. SentinelOne has made massive data investments into their general cloud and asset architecture. If the PingSafe data can get fully integrated, SentinelOne has the potential for a truly innovative end to end data driven solution. While the CNAPP doesn't stand out right now, it has a lot of potential once it's all unified.

Sysdig

Sysdig has long been a go-to tool for DevOps engineers and enthusiasts. Many vendors in the CNAPP space struggle to expand beyond their original use cases, but Sysdig has stayed competitive. Sysdig's runtime focus undoubtedly comes in part from

their technical co-founder, Loris Degioanni, who co-created Wireshark and Falco. If you're familiar with Wireshark and appreciate its utility, you're likely to appreciate Sysdig's approach to cloud security as well.

Falco, the open-source container security runtime agent, was ahead of its time. Despite that, it remains the default option for eBPF security implementations in container workloads—a position that's quickly gaining recognition. Sysdig faced the challenge of developing a robust agent first, only to later add agentless CSPM features after initially underestimating the market's fast-paced evolution. Practitioners didn't fully grasp the value of Sysdig's agent compared to other options in the market. Unfortunately, many security teams first purchased a CSPM solution, only to later realize that tools with container insights like Sysdig was what they really wanted.

Sysdig's real advantage lies in its real-time contextual monitoring. While traditional security solutions offer static snapshots, Sysdig continuously monitors for critical vulnerabilities and threats using Falco. For example, its detection engine streams real-time insights, allowing teams to detect cloud-native threats, such as risky identity behaviors or configuration drifts, in action. Sysdig's expertise in Kubernetes, containers, and hybrid cloud security gives it a significant edge over more traditional security providers.

As the market shifts its focus from endless scanning to actively stopping attacks, Sysdig finds itself at a critical juncture. On one hand, innovations in eBPF and similar technologies have rapidly advanced, putting Falco at risk of being considered outdated. On the other hand, Sysdig remains the most mature solution with a runtime focus, positioning it well for the changing landscape.

Upwind

Upwind was founded in 2022, one of the latest cloud security vendors. Despite the many solutions before them, Upwind's value proposition is centered on providing real-time cloud security that leverages runtime data for threat detection and response. Their product is built around an eBPF-based agent (extended Berkeley Packet Filter) that allows for deep kernel-level monitoring and insights without the performance overhead typically associated with traditional agents.

Upwind's perspective on the market is that CNAPP needs a runtime-oriented facelift. As CNAPP features have exploded into bloated platforms, Upwind argues that the essence of results-oriented security is one oriented towards runtime defense. For Upwind, that means leveraging eBPF technology to monitor and filter system activities, network traffic, and file access at the kernel without heavy performance impact or risk of kernel panics. We should note that Upwind excels in environments running containers and Kubernetes, both for visualizing those relationships and doing threat detection. It focuses on detecting anomalies in real time by establishing baseline behaviors for network traffic, file operations, and process execution. For example, it can spot unusual activities like wrongly loaded libraries that could be indicators of compromised systems.

Unlike other CDR players, Upwind recently announced their agentless cloud scanners. This is useful for initial engagements or landing customers, especially for companies hesitant to deploy agents. This will prove critical for customers using Serverless containers, functions and virtual machines (VMs). Additionally, unlike other CNAPPs, they've made serious investments into API security using their network data - becoming legitimate competitors to standalone runtime API security.

Now, Upwind offers both agentless and agent-based solutions, allowing them to cater to diverse customer needs. They also integrate security throughout the CI/CD pipeline by leveraging build-time data to enhance overall cloud security. They can automatically discover and correlate CI/CD events with runtime data, providing an end-to-end view of vulnerabilities, risks, and the root causes of issues.

Their primary focus is on being results-oriented, real security for mid-market companies, which represent their core customer base. These customers are typically looking for tool consolidation and cost savings, making Upwind's comprehensive platform particularly attractive. The mid-market is where Upwind sees the most traction and growth, positioning itself as a company offering consolidated solutions rather than a fragmented, tool-based approach. Upwind has also found traction with enterprise buyers who are looking for cutting-edge runtime security, who often see Upwind as part of a larger suite of tools.

Overall, we like Upwind's approach providing the full library of solutions across CNAPP. The next key question will be derived on how well they can execute on their GTM within the mid-market. Almost every new cloud security provider is dancing the "are we a Wiz competitor" question, with only Upwind having the boldness to say, "yes, we're better."

Sweet Security

Sweet Security focuses on cloud-native runtime security. Their key offering utilizes an eBPF sensor designed to help organizations detect and respond to active cloud threats in real-time.

A key differentiator of Sweet Security is its **multi-layered approach** to cloud security, which integrates protections across the entire cloud stack—from infrastructure and applications to APIs, identities, and network interactions. This holistic coverage ensures comprehensive real-time protection across different layers of the tech stack. Combined with a robust anomaly detection engine within each of those layers, Sweet promises total runtime security across cloud workloads.

The multi-layered approach means that Sweet fits into several categories:

1. **Cloud Detection & Response (CDR):** Sweet Security's cloud detection and response solution monitors and analyzes logs from all major cloud providers—AWS, GCP, Azure, Oracle—as well as managed services and VMs, to deliver real-

time attack prevention across private, public, hybrid, and multi-cloud environments.

2. **Workload Protection**: Sweet Security uses an eBPF sensor to monitor cloud resources, such as hosts and virtual machines, detecting any abnormalities or vulnerabilities. They do vulnerability scanning with reachability analysis, and have unique innovations tying together workload and cloud alerts.
3. **Application Detection & Response (ADR):** Application layer detection capabilities are still being experimented with, but Sweet has enough visibility into function execution and code context to be one of the only cloud-centric companies to also fit in this category
4. **Network Detection and Response (NDR) & API Security**: Sweet's behavior analysis provides baseline monitoring of network activity, including Layer 7 interactions, which helps identify zero-day attacks and suspicious network patterns that may otherwise go unnoticed
5. **Vulnerability Management**: Sweet provides robust reachability data for vulnerabilities powered by the eBPF agent, which evaluates vulnerabilities according to critical criteria—such as whether they are loaded into the applications memory, are executed, public-facing, exploitable, or fixable— to hone in on threats that actually matter.

Sweet places particular emphasis on non-human identities (NHI), such as service accounts, API keys, and OAuth tokens in runtime to detect suspicious activities. They have deep visibility into these workload identities that are becoming an evolving focal point for security leaders.

At the core of Sweet's security platform is the bet that runtime is a better way to do cloud security. They're less concerned with who their competitors are from a CNAPP standpoint, and much more concerned with delivering real security value to teams big or small.

Example of Code to ASPM: Jit

In our initial report, we discussed ASPM solutions and their role in the broader code-to-cloud ecosystem. Jit is an ASPM (Application Security Posture Management) platform designed to empower developers to own the security of their code. This is the methodology behind "shifting left", and is achieved through orchestrating the power of OSS and commercial scanners (for SAST, DAST, SCA, secrets detection, CSPM, and more) directly into developers' workflows. Simply put, Jit is built upon the premise that developer ownership of secure coding practices is only achievable when they don't need to leave their coding environment.

In terms of developing and forwarding overall security posture, Jit addresses software supply chain security through its 'Security Plans,' which align security measures with business goals and requirements. These plans guide users toward achieving specific business objectives while ensuring certification readiness. Some notable plans include

AWS Foundational Technical Review (FTR), Jit MVS for AppSec, and the OWASP Top 10 compliance framework.

A key differentiator, particularly for organizations in regulated environments, is that Jit does not extract customers' source code from their SCM environment. Instead, Jit executes all security controls directly within the customer's SCM (e.g., using GitHub Actions). Moreover, recognizing the importance of future-proofing in today's economy, Jit built an open and extensible platform that allows users to integrate their own security tools, rather than developing proprietary ones. This ensures a unified security experience tailored to individual needs.

CSPM as Part of ASPM

An emerging trend among companies that began with shift-left security is the integration of CSPM (Cloud Security Posture Management) into their offerings. Jit is no exception.

Jit's CSPM integrates with Wiz, Prowler, and others, enhancing its security suite by helping cloud security teams and developers maintain secure and compliant cloud environments. It automates key security tasks, continuously monitoring cloud infrastructure for misconfigurations, policy violations, and compliance gaps across AWS, Azure, GCP, and other cloud providers.

Connecting Code to Cloud

In cloud-native enterprises deploying multiple microservices, security teams often struggle to ensure code from different development teams meets security standards. By integrating Jit's automated code scanning and vulnerability detection into CI/CD pipelines, cloud security teams can ensure security is applied consistently across all development teams.

Rather than waiting until after deployment for security checks and remediation, Jit integrates natively in the workflows of developers, ensuring security checks, vulnerability scanning, and configuration audits occur as code is developed and pushed.

In fast-paced DevOps environments, where rapid development cycles are the norm, manual security checks cause bottlenecks. Jit helps developers self-manage security checks while pushing new features by automating pre-approved security policies that are enforced during code commits. This approach reduces the burden on security teams while ensuring compliance and speed of deployment.

Other key vendors include Cycode, Aikido, Ox, ArmorCode and Apiiro. A full list is here. In earlier articles, Francis has written on Cycode and Aikido

Cloud Detection & Response (CDR)

Cloud Detection and Response tools detect malicious activities in common cloud workloads (containers & Kubernetes) and contextualizes them with other cloud services to create a single attack path across cloud environments. Read Latio's full exploration of CDR here.

Armo

ARMO provides protection from cloud runtime threats with both posture and runtime detection solutions. They uniquely **combine these capabilities to enrich both posture and runtime actionability**. One core value proposition is utilizing their container insights to inform the posture findings, from vulnerabilities to misconfigurations, and then using the posture insights to empower runtime defense with advanced attack prevention features.

Posture:

1. Detects misconfigurations across different kinds of cloud resources, with rich detections into Kubernetes. They use their runtime data to alert you to misconfigurations that can be corrected with zero impact. These findings are also mapped to most major compliance frameworks.
2. Detects vulnerabilities whether in CI/CD, Container Registry, or at runtime, and provide reachability analysis via the runtime sensor. They improve actionability with features like layer detection and vulnerability grouping.
3. Creates attack paths for prioritization, bringing together multiple insight layers from exposure, identity, and runtime.
4. Has advanced attack prevention mechanisms in the form of SecComp and Network Policies, generated automatically with their agent.

Runtime:

1. Has both anomaly and static based detection rules for workload attacks, as well as customizable rules.
2. Can detect threats against cloud resources more broadly, including how those threats tie back to the workload they started on
3. Gives users the preventative policies to block those kinds of attacks in the future

ARMO began with an early commitment to the Kubernetes ecosystem that has been unparalleled, with their open source project Kubescape being donated to the Cloud Native Compute Foundation (CNCF) - it continues to be the starting place to learn the security posture of your cloud environment. ARMO then made major strides into cloud security more broadly, and expanding the capabilities of their eBPF agent for actionable remediations and detection capabilities.

Rad Security

Rad security is an amazing growth story in CNAPP. Co-founder Jimmy Mesta wrote the OWASP top 10 for Kubernetes, and only ARMO has had as genuine a commitment to securing the core of cloud computing as Rad. Now, from re-brand to baselining with

an eBPF agent, Rad has their sights set on runtime cloud security more holistically. Rad continues to expand their cloud runtime protection abilities, while maintaining the Kubernetes innovations that DevOps teams have long loved them for. As the market continues to look for runtime compliments to their CSPM, Rad is well positioned to be that solution, while generating a lot of buzz for their baselining approach.

Other key vendors include Sweet and Upwind, who were mentioned earlier, along with Stream and SkyHawk on the agentless side. A full list is here.

Application Detection & Response (ADR)

Application Detection and Response (ADR) offers security teams visibility, detection, and response across their applications. It shows security teams how users are interacting with their application, service to service communications, how applications are interacting with their hosting containers, and provide tools to make investigating and responding to application threats possible for non-developers. They detect and correlate common application attacks, like the OWASP Top 10, fraud and abuse, and exploiting vulnerable libraries. Read Latio's full exploration of ADR here.

Miggo

Miggo is one of the only offerings in the ADR space to look at applications holistically by leveraging distributed tracing. They utilize either existing telemetry instrumentations, or leverage "no code" deployment methodologies to gather distributed tracing data. They then apply this data to security use cases, detecting exploits typically invisible to the SOC, such as injection or cross site forgery attempts. Their main differentiator is being able to show you the full attack scenario across application services.

Oligo Security

Oligo Security took an elegant approach to extend detection capabilities into applications, without requiring any app-level instrumentation. They baseline library activity into the kinds of syscalls they make, and then can detect deviations at runtime - leading to robust zero day exploit detection. Beyond detection, tools like Oligo also have a unique ability to block function level executions - stopping exploits in their tracks.

Raven.io

Raven has taken the approach of looking for application attacks by monitoring application and library activity. They're able to detect application exploits against libraries, and use runtime execution data to tune out vulnerability noise. Raven is taking a more holistic approach in terms of maximizing the data they're gathering at runtime, but can also directly stop active attacks, or proactively patch vulnerabilities.

Kodem

Kodem has built their own distinct solution in the ADR space that focuses on the local application context, but are more emphasizing how their runtime detection mechanisms can be used to reduce vulnerability false positives. They're the only runtime scanner to apply this reachability methodology not just to SCA, but also to SAST.

Operant

Like many vendors in this space, Operant could also easily fit within the API or CDR categories. Their endpoint agent gets rich visibility into containerized workloads, and uses that visibility for detection and response rules across your stack. Like others in this category, they are focused on being an end to end runtime detection response platform. They operate most closely aligned with the network layer, allowing for advanced microsegmentation features alongside CADR capabilities more broadly.

Other key vendors include Contrast, Traceable, Operant and Datadog. A full list is here.

Remediation

Dazz Security

While many companies have invested heavily in Cloud Native Application Protection Platforms (CNAPP), they often struggle to manage the flood of alerts and issues generated by cloud logs or the security tools themselves. Dazz offers a solution: a vendor-agnostic platform designed to map code-to-cloud pipelines, correlate security data, and drive remediation seamlessly within the developer's workflow.

Dazz's Core Differentiators

At the heart of Dazz's is its patented capabilities:

1. **Data Correlation and Root Cause Analysis** – Dazz excels at normalizing and correlating data from different development, infrastructure, and security tooling. With this correlated data, Dazz links alerts directly to their root causes.
2. **Remediation Guidance and fixes** – Dazz gives developers insights into security issues, recommended fixes, and actions to fast track remediation.

Unified Remediation & ASPM

Many enterprises use CNAPP tools like Wiz and Palo Alto, which excel at visibility and detection but often fall short when it comes to reducing alert noise and enabling efficient remediation. Dazz integrates seamlessly with leading CNAPP platforms and contextualizes them further with additional context from development, application security testing (AST), and other tools.

Dazz bridges this gap with its patented data correlation engine, tailored specifically for Application Security Posture Management (ASPM). By ingesting and correlating security data across the enterprise's cloud infrastructure and application layer, Dazz

analyzes the multitude of alerts and correlates them to key root causes—allowing security teams to prioritize the most critical vulnerabilities.

Root Cause Analysis: Fixing What Matters

Dazz's advanced root cause analysis capabilities help organizations address vulnerabilities efficiently. One standout feature is Dazz's root cause analysis for Terraform and Docker, which enables DevOps teams to trace cloud infrastructure vulnerabilities directly back to the source code. This significantly reduces remediation time and allows developers to resolve issues as part of their regular workflows, minimizing disruptions. By focusing on the remediation of CVEs, misconfigurations, and exposure risks, Dazz ensures that DevOps teams can effectively fix the vulnerabilities that pose the greatest risks.

Dazz is seeing increasing demand for its ASPM capabilities as enterprises seek tools that integrate into their development workflows. Dazz offers deduplication, remediation guidance, and alert aggregation, making it a preferred solution for organizations looking to streamline their security operations.

Other key vendors in this space include application oriented solutions like Phoenix and Armorcode, cloud oriented solutions like Opus, DevOcean, and Zafran, and generalist vulnerability management providers like Vulcan and Brinqa. The full list is here.

Rest of the market

Some vendors we didn't get spotlight but will certainly cover them in the future. However, we want to acknowledge that there are important vendors like Aqua security, Lacework (Fortinet), Datadog, Checkpoint Cloud Guard, Tenable, Qualys and Caveonix cloud and many more that are worth mentioning. That doesn't mean we don't like them or they're not worth your time, the full exhaustive list is on Latio's site, please visit to review all the vendors.

Concluding Thoughts

We believe the conversation around CNAPP will continue to evolve over the next few years, and the goal of this report was to help frame those future developments. CNAPP continues to dominate the cyber conversation, despite tinges of frustration: Security teams are saying they want less tools while they complain how noisy those giant bloated platforms are. The large CNAPPs have the money and distribution, but startups have the innovation.

Moving forward we believe there are some critical questions for the industry.

1. Are security teams truly ready to move beyond "just visibility?" Early runtime shifts proved not to win the market, but perhaps security teams are finally ready to take production security seriously.

2. Can you make a UX for developers and the SOC in the same platform? Developers and SOC analysts rarely agree on anything, besides that they're annoyed to have to annoy each other so often.
3. Lastly, the discussion around platform consolidation continues to evolve. Do customers want a product with both agent and agentless capabilities, with the same vendor providing all their AppSec and SOC tools in one solution? Or are customers fine with best-of-breed solutions? There is a consolidation of right and left, as well as application, cloud, and operations teams. Can all of their use cases really be covered in a single place? Should they be?

Ultimately, the vendors that solve these questions for customers will continue to win the market. Either way, this report serves to explain how we got here and the vendors that have all made a bunch of money making our cloud a little more...secure—or at least noisy!

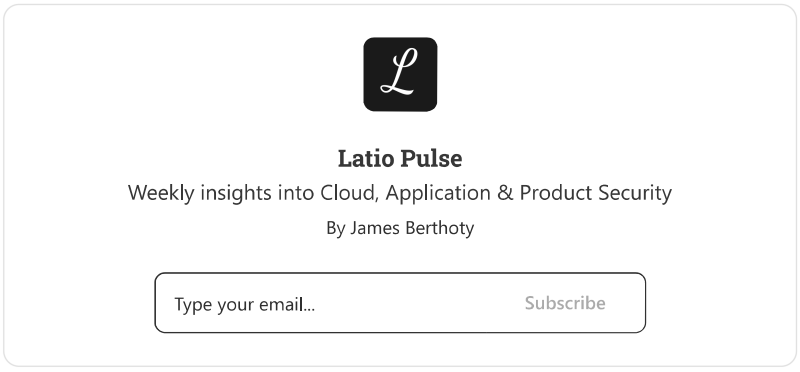
Thank you for reading!

We make this report freely available for everyone. If you find it helpful, please share it with a security leader or your software engineering team. To see our next episode on this Cloud & Application Security, feel free to subscribe below.

Type your email... Subscribe

Thanks for reading The Software Analyst Newsletter! I focus on Identity Secuity, The SOC (Pipeline, SIEM & Automation) And Cloud & App Sec Ecosystems. This post is public so feel free to share it.

Subscribe to James' newsletter here:



Subscribe to Francis's research:



The Software Analyst Newsletter

A newsletter focused on the analysis of software companies within cybersecurity and data infrastructure (AI/ML).

By Francis (Software Analyst)

Type your email... Subscribe

Thank you for reading this report. If you have comments or anything to share, please share below:

Type your email... Subscribe



75 Likes · 6 Restacks

← Previous Next →



A guest post by

James Berthoty

James Berthoty has been in technology for over 10 years across engineering and security roles. He built Latio Tech to help connect people with the right products.

Subscribe to James

Discussion about this post

Comments Restacks

Write a comment...



Daniel Sep 15

Liked by Francis Odum

- Check point CloudGuard. Also Tamnoon for remediation (managed remediation).

LIKE (2) REPLY SHARE



Matthew Oct 5

Liked by Francis Odum

Truly incredible research. I found this article to be the pinnacle of excellence. You are very right on some of your key points; you outlined the history to a tee, you provided analytics to draw correlations, and you foreshadowed the future based off of where we have gone. well done.

LIKE (1) REPLY SHARE

1 reply by Francis Odum

11 more comments...

© 2025 Software Analyst · Privacy · Terms · Collection notice
Substack is the home for great culture