EMPOWER YOUR CLOUD:
MASTERING CNAPP SECURITY

How security professionals can manage threats in the cloud with a unified approach to AWS, Azure and Google Cloud environments

Table of Contents

INTRODUCTION: IT'S TIME TO DEMYSTIFY CNAPP

You're a security professional. Maybe you have identity and access management down cold. Maybe you've been focused on vulnerability management. Or perhaps you've been securing on-premises environments for a while.

Either way, you know your stuff. But all this talk about Cloud Native Application Protection Platforms (CNAPPs) has you more than a bit puzzled.

So, why does a CNAPP make sense now? When you think about it, the classic perception of security—the company as a fort with a well-protected and patrolled perimeter—is outmoded. The cloud has broken that model and security hasn't kept up. Sure, there are solutions that might solve one aspect of the challenge, but that's part of a larger fragmentation problem that adds to the complexity of securing a cloud environment.

A cottage industry of security tools has popped up to handle tiny slivers of the challenge. The end result is tech fatigue. In the age of limited resources, when your day job has you focused on threats like ransomware and trying to ensure compliance, there are only so many alerts and systems you can pay attention to. After a while it's just all noise.

Cloud security requires a new approach—a CNAPP that looks at the problem holistically.

In this eBook, we'll bring you up to speed and let you in on the CNAPP story. We'll define it, we'll dig into why CNAPP is the right solution, we'll share exactly how it works, and we'll look at how a CNAPP can help you.

A CLOUD OF UNCERTAINTY

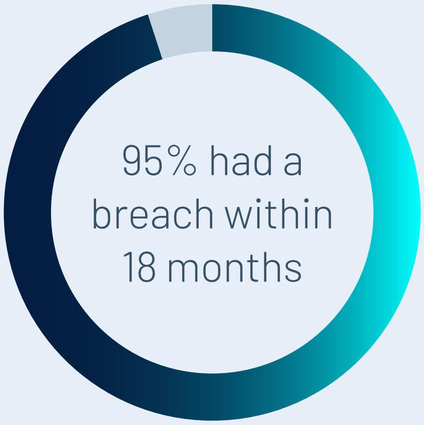
Although there have always been some blind spots, the cloud has introduced new levels of uncertainty into security. On-premises resources were a known quantity because all the gear was owned by the company and sat under the watchful eye of on-site staff. They knew what they were dealing with and traditional security tools were up to the task.

Many companies that moved away from on-premises environments, seduced by the promise of limitless possibilities, may have assumed they could get by in the cloud with a similar set of tools.

Surely, the cloud provider would be more secure. On the contrary, a new report from Tenable, Cloud Security Outlook, includes a survey of 600 global security professionals in which 95% of respondents reported a cloud breach within the past 18 months–with an average of 3.6 breaches per respondent.

Cloud breaches are almost universal

Source: Tenable Cloud Security Outlook, 2024; n=600



Alarmingly, IBM reported in 2022 that it took an average of 277 days for businesses to identify and report a data breach and 327 days to identify compromised credentials. Do the math on that – almost every company has a breach at some point and it can take the better part of a year to find – and the problem is clear.

Shared responsibility model = mainly your responsibility

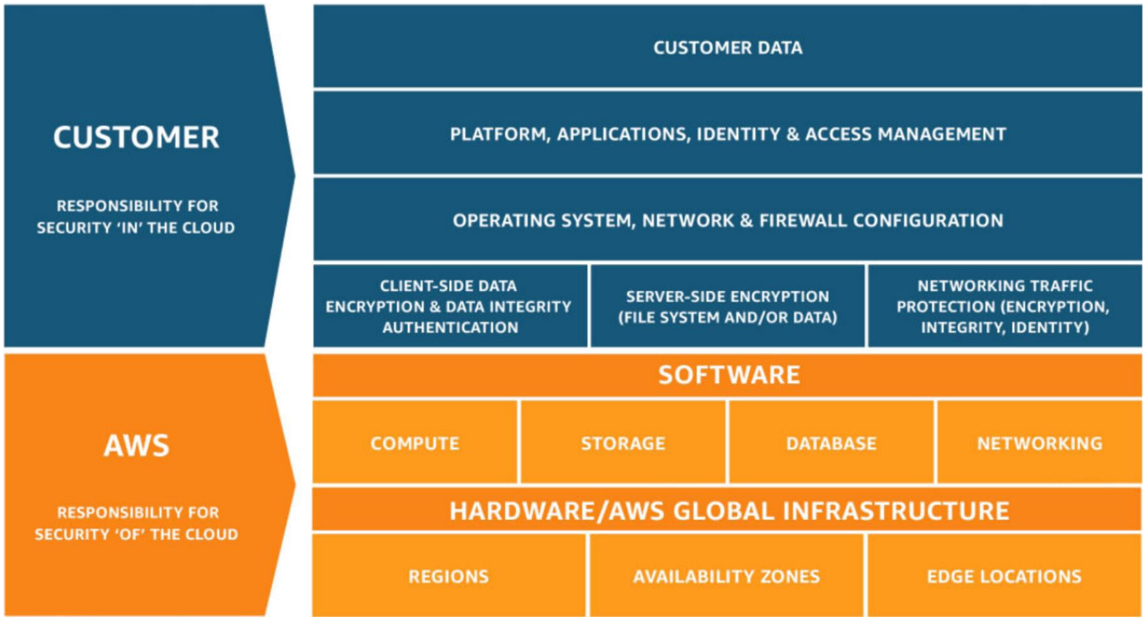
In the cloud, providers chant their "shared responsibility model" mantra, which can give comfort to security teams until they realize that the actual responsibilities are out of balance. Shared responsibility might be better characterized as a "split responsibility model" because it simply designates where responsibilities lie. None of the responsibility is really "shared"; that word is misleading. And, the truth is that the onus is on the customer, not the provider.

For example, AWS delineates the split responsibility this way:

- AWS is responsible for "Security of the Cloud" – essentially the infrastructure you pay them for every month.
- The customer is responsible for "Security in the Cloud" – in other words, all the services you use, applications you run, and every scrap of data you put in the cloud.

Here's the graphic AWS uses to outline those responsibilities. It seems pretty equitable until you drill down into the items at the top. You're responsible for the overwhelming majority of the security risk.

Amazon's Shared Responsibility Model



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

Source: AWS, 2024

It's a multi-cloud world

Even if a cloud provider did help with security, should you really trust one provider over another? If yours is like most enterprises, you've embraced a multi-cloud world so you can get the best services from each provider–and you've learned the hard way to avoid vendor lock-in.

Because cloud provider security tools are often limited to their own cloud, managing heterogeneous cloud security across multiple clouds that don't talk to each other is close to impossible. All of this has given rise to the need for third-party security that includes the entire cloud native application rather than the infrastructure layer alone. The end result: an evolution from cloud security posture management (CSPM) to CNAPPs.

Without control of identities, cloud security is not complete

Managing identities and permissions in the cloud is a challenge. At the same time, ensuring a user or service has "least privilege" – that is, only the access they need for a required task and nothing more – can be an administrative headache. Doing all of that, continuously, for thousands of human and service identities across multiple clouds is a daunting task. Industry trends reveal a staggering figure: more than 90% of identities are using less than 5% of permissions granted.

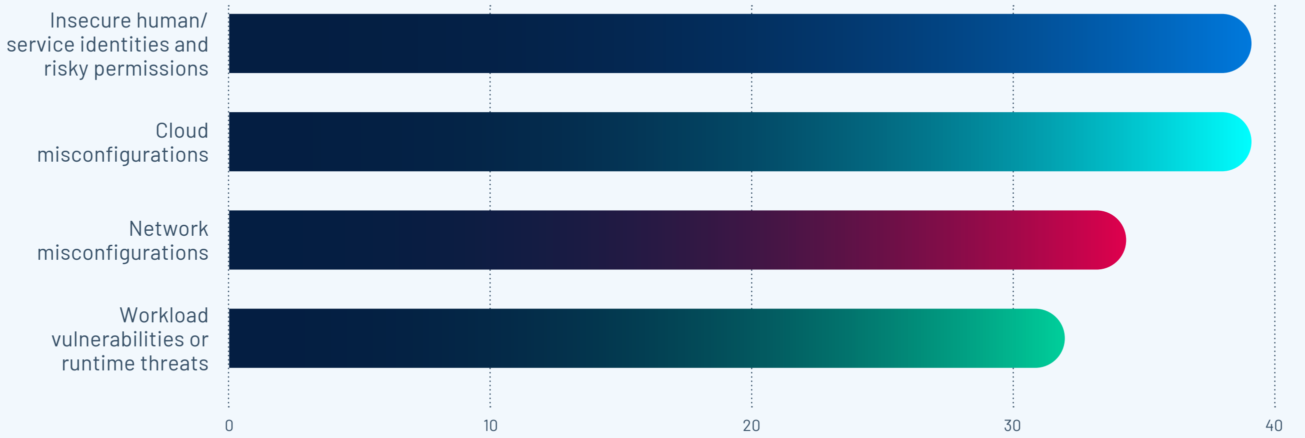
In the cloud, without control of identities, security is not complete. Think of it this way: as everything (even things that had been traditionally physical) became logical (i.e., when they moved to the cloud), the assigned permission to perform a specific action is really the only thing needed to be able to do it. That brought rise to a new cliche you'll probably hear a lot in the coming years: "identity is the new perimeter."

We all know how important the perimeter has been in security. Identity is just as important, if not more so, as we move to the cloud. And the numbers show that.

In Tenable's Cloud Security Outlook report, 39% of respondents said that the number one security risk reported for cloud infrastructure was insecure human/service identities and risky permissions. Anyone who's tried to secure human or service identities in environments like AWS, Azure and Google Cloud won't be surprised by that figure.

Top risks to cloud infrastructure

Source: Tenable Cloud Security Outlook, 2024; n=600



The complex interplay of policies and configurations that enable access can often leave loopholes for attackers to penetrate. In fact, the Verizon 2024 Data Breach Investigations Report shows that 31% of all breaches over the past decade have involved the use of stolen credentials. In early 2024, IBM reported a 71% increase in attacks that exploit identity. Even more alarming, in 2022, a survey from the Identity Defined Security Alliance showed that 84% of respondents had experienced an identity-related breach in the past year.

Once breached, cloud environments are wide open for bad actors to move at will.

Stopping identity-driven breaches in the cloud takes a new approach. An entire product category has sprouted to secure identities – Cloud Infrastructure Entitlement Management (CIEM).

A CIEM platform discovers all identities (including human, service, native/IAM, federated, and third party) and their complex permissions. Plus, a CIEM can identify all the resources being accessed and activities in your cloud environment, giving deep, contextualized visibility into the state of entitlements.

In addition, every user entity – human or services – has a unique identity. Users that need access to anything in the cloud need an assigned role, with accompanying permissions and entitlements. That role determines a user's access. Risks happen when users and roles have over-privileged access or excessive entitlements.

Vulnerability management lets security team focus

Legacy vulnerability management tools haven't kept pace with the way the modern attack surface has changed. Add in the vast quantities and the diversity of today's vulnerabilities, and the story gets even more dire.

Security and IT teams are buried with more work than they can handle, as they struggle to address all vulnerabilities that the Common Vulnerability Scoring System (CVSS) classifies as "high" or "critical."

Risk-based vulnerability management, as part of a CNAPP, can give security teams the context they need to focus on the vulnerabilities and workloads that matter most, while deprioritizing the vulnerabilities that attackers are unlikely to ever exploit. For example, a workload with a vulnerability that has no network exposure or permissions attached to it is nowhere near as important as a workload with a vulnerability that has public access and excessive permissions.

When it comes to vulnerability management in the cloud, there's a significant advantage over on-premises environments: A CNAPP can deploy cloud security solutions without the need for an agent.

Exposure management provides visibility across and beyond clouds

As part of a CNAPP, exposure management should help your organization gain visibility across clouds, with a focus on preventing likely attacks resulting from the toxic combination of vulnerabilities, misconfigurations, and excess permissions. Exposure management accurately communicates cyber risk to support optimal business performance with broad vulnerability coverage spanning all cloud resources.

WHAT IS A CNAPP?

CNAPP solutions replace a patchwork of siloed products that often cause more problems than they solve, such as multiple false positives and excessive alerts. Those products usually provide only partial coverage and often create overhead and friction with the products they're supposed to work with. Most importantly, CNAPPs allow businesses to monitor the health of cloud native applications as a whole rather than individually monitoring cloud infrastructure and application security.

A comprehensive CNAPP solution includes a wide variety of essential capabilities, some of which we mentioned earlier, including:

- ✓ **Cloud Security Posture Management (CSPM)**, which is a proactive way to seek out and fix misconfigurations within your cloud environment. CSPM is an important element in the battle over the modern attack surface because legacy approaches for on-premises infrastructure don't work well in cloud environments – mainly because there are thousands of configuration settings in cloud environments that are very different from on-premises. With CSPM, you can monitor threat exposure risk by continuously reviewing and assessing cloud environment settings and configurations. CSPM also assesses discovered risks against security standards and policies to attain and maintain compliance with regulations across multi-cloud environments.
- ✓ **Cloud Infrastructure Entitlement Management (CIEM)**, which is the most comprehensive and accurate solution for managing identities in cloud infrastructure environments and achieving least privilege at scale. The solution offers visibility into human and service identities, their roles, and assigned permissions and entitlements. It knows the critical services they can access and whether they have excess entitlements or privileges beyond what their work requires by using continuous automated scanning of multiple cloud accounts. CIEM can also spot unusual access patterns compared to similar identities and it helps teams get access entitlements under control with prioritization and auto-remediation of risky privileges and excessive permissions.
- ✓ **Cloud Workload Protection (CWP)**, a scalable, low-friction solution for securing cloud workloads and mitigating risk from vulnerabilities and violations that commonly occur during rapid development cycles.
- ✓ **Kubernetes Security Posture Management (KSPM)**, which adds depth to CSPM by addressing the security posture and associated risks unique to Kubernetes environments.
- ✓ **Infrastructure as Code (IaC) Scanning**, which is an essential tool for identifying risk with automated code in the development and integration stages to prevent security issues from being pushed into production. In addition, you can now combine application code security with IaC scanning to provide a complete picture of a cloud application's security posture.
- ✓ **Cloud Detection and Response (CDR)**, which adds capabilities that provide log and traffic analysis and identification of suspicious behavior patterns so security teams can see if they have a vulnerability in their current assets.
- ✓ **Data Security Posture Management (DSPM)**, which provides a better understanding of data and its sensitivity to contextualize and prioritize data risks that arise from misconfigurations, vulnerabilities, and over-permissive access.

Who does a CNAPP help?

Pretty much anyone who’s involved in cloud security can benefit from a CNAPP. Security, DevOps, DevSecOps, IAM, and IT teams can use a CNAPP to work collaboratively and continuously improve cloud security posture. A CNAPP can help those groups govern access more effectively without adverse impact to application availability or time to market.

What can an enterprise gain from a CNAPP?

Enterprises gain many benefits from a CNAPP, including:

- **Visibility:** DevOps, security, DevSecOps, IT and other stakeholders can understand their cloud resources and inventory–including cloud infrastructure, identities and workloads–to identify, control, prioritize and remediate risk.
- **Enhanced and consistent security posture:** The CNAPP lifecycle approach provides security consistency and context from coding to runtime, ensuring improved identification and remediation of risk.
- **Cloud infrastructure health:** The platform streamlines security hygiene for virtual machines, containers, Kubernetes clusters and other components, and leads to fewer misconfigurations during development and in production.
- **Minimal overhead:** The integrated tooling solution offers simplicity and nearly effortless usage compared to management of separate tools and vendors.
- **Seamless integration:** Notification and remediation of the findings integrate easily into the SDLC, developer pipelines, SIEMs, and ITSM on the production side–all with the goal of making findings actionable.
- **Shift-left security:** A CNAPP applies broader, more overarching security protection starting in development, which improves protection from development to runtime.
- **Insights and observability:** A CNAPP’s capabilities enable analysis and governance of attack paths as well as better understanding of permissions and configurations.
- **Holistic security:** A CNAPP breaks down the silos of multiple domains, including network, identity, workload protection, posture, etc., to use them together for analysis that can find toxic combinations and prioritize the most significant findings.
- **Simplification:** A CNAPP simplifies complex infrastructure and security concepts to democratize cloud security practices. It also creates a common language across teams so they can work together even across multiple cloud environments with vastly different concepts.
- **Cloud-native security:** A CNAPP is designed for the cloud from the ground up, rather than typical on-premises security poorly adapted to the cloud.

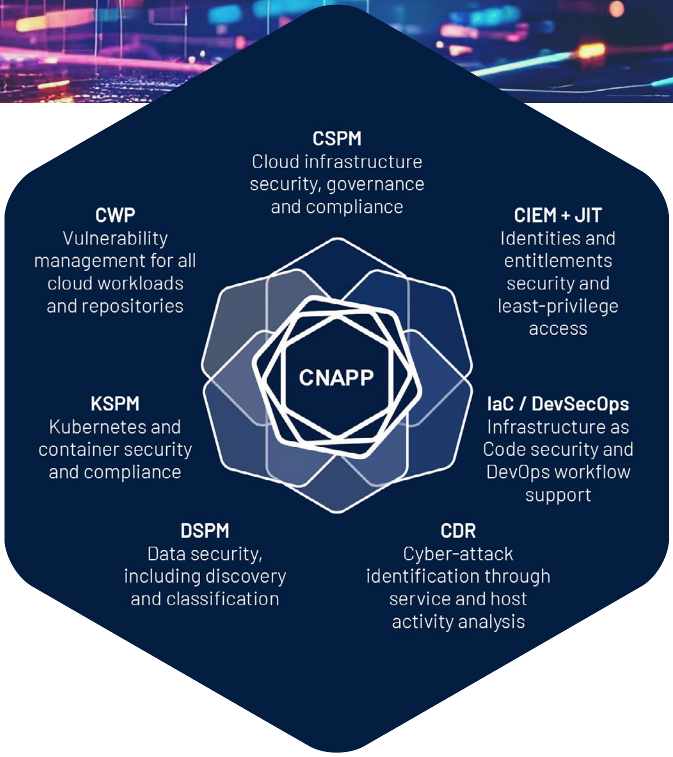
How does a CNAPP work?

With threats coming from the cloud, on-premises environments, and operational technology (or a hybrid of the three), along with misconfigurations arising from confusion about the shared security responsibilities between providers and their customers, the attack surface is exponentially larger.

So a CNAPP platform has to have breadth. It can't be a mere collection of point products that work independently. Independent analyst Tom Croll of Lionfish Tech Advisors, co-author of the original research on CNAPP, has said that "security for cloud-native applications requires an integrated approach."

CNAPP offers a holistic view of cloud risk and gives security, DevSecOps, DevOps and engineering teams the visibility, actionable findings and contextual alerts they need for comprehensive protection and an improved security posture of cloud native applications. A CNAPP includes six required capabilities: IaC scanning, container scanning, CWPs, CIEM, CSPM, and CDR.

Each one of these capabilities is consolidated into a single platform rather being delivered separately or from different vendors.



CSPM
Cloud infrastructure security, governance and compliance

CWP
Vulnerability management for all cloud workloads and repositories

CIEM + JIT
Identities and entitlements security and least-privilege access

CNAPP

KSPM
Kubernetes and container security and compliance

IaC / DevSecOps
Infrastructure as Code security and DevOps workflow support

DSPM
Data security, including discovery and classification

CDR
Cyber-attack identification through service and host activity analysis

A CNAPP functions continuously, seamlessly and from a single point of access. It understands the relationships and connections for all human and service identities. It looks for vulnerabilities, can oversee provisioning, and can handle on-demand policy generation.

Importantly, a CNAPP can work effortlessly across a multi-cloud environment. These abilities enable CNAPPs to deliver on their promise of finding and remediating risks at scale.

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at www.tenable.com.

CONCLUSION: A CNAPP SHOULD SIMPLIFY YOUR CLOUD SECURITY

The CNAPP category was defined only a short time ago. A rush of vendors seized on it and steered it to their strengths. The result was a complex security puzzle.

A true CNAPP should reduce complexity and protect your company's assets wherever they are by monitoring the security of cloud native applications as a whole, rather than being restricted to the infrastructure layer.

It should seek out and fix misconfigurations; manage identities in your cloud infrastructure and give you least privilege access at scale; secure cloud workloads; handle Kubernetes or container risks; and prevent security issues from being pushed into production.

Contact Us:

Please email us at sales@tenable.com or visit tenable.com/contact