Brought to you by:

WIZ

CNAPP

for dummies®

A Wiley Brand

Consolidate tools

Reduce complexity and cost

Simplify risk reduction

Wiz Special Edition

Rob Shimonski

Hello readers!

Before you wave your wand and go to the next page, here's what you need to know about us at Wiz.

Founded in 2020, Wiz is the fastest growing software company in the world.* Our mission is to make cloud environments secure for companies, no matter what cloud provider they use and no matter how big or small they are. Use Wiz to provide your security and development teams with full-stack visibility and exact accuracy to fix critical risks in your cloud.

Yours,
Assaf Rappaport
CEO of Wiz

*Frost & Sullivan: 2023 Entrepreneurial Company of the Year Recognition

CNAPP

Wiz Special Edition

by Rob Shimonski

for dummies®
A Wiley Brand

CNAPP For Dummies®, Wiz Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-20694-0 (pbk); ISBN 978-1-394-20695-7 (ebk)

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor:
Amy Lupold Bair

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Client Acct. Mgr: Cynthia Tweed

Content Refinement Specialist:
Saikarthick Kumarasamy

Introduction

The changing landscape of technology has really impacted the world. They did it this time! The public Internet and the architecture that makes it up is filled with clouds. These clouds are quickly becoming critically important to every modernized organization in existence. While the cloud environment may not be new, the rapid rush toward the cloud is nothing short of remarkable. If your organization is like most, it is heading into the cloud or already there.

This is not a negative! A move toward the cloud is actually a great thing because it allows millions of people to experience a greater velocity in technological advancement. With the use of cloud and now DevOps (the fusion of development and operations teams), the capability to create technology quickly and efficiently has become the norm.

Herein lies the actual problem: The change has come too quickly for some. Security teams have not caught up with the changing landscape of security risks. In fact, many are in a state of shock, some frozen into inaction, unsure how to catch up. CNAPP is here to help.

Cloud native application protection platform (CNAPP) is the view from the stars, able to zoom down into the deepest recesses of the cloud to help identify security issues in real time — as they happen — and report them to users. CNAPPs reduce noise and help to consolidate toolsets, making life easier with a single pane-of-glass view of all cloud and development security.

It’s time to embark on a brief learning journey to help better understand the digital transformation leading to the need for a cloud native security such as CNAPP!

About the Book

This book is your introduction to the concepts of using cloud native security and a toolset called a CNAPP. It explains the background of cloud native security, why the security model for the different attack surfaces is needed more than ever, and why a toolset like CNAPP may be your only hope in helping with this imminent danger.

Foolish Assumptions

In writing this book, I'm working from a few assumptions about you, the reader:

- You could be an engineer, or you might even have an office in the C-suite (this topic is relevant for a lot of different roles).
- You may have heard a bit about CNAPP but it's still kind of a fuzzy mystery.
- You're concerned that CNAPP may be too complex and too prescriptive and would be glad to find out otherwise.

Icons Used in This Book

Check the margins of this book and you'll observe some icons, which are guideposts to key points:

REMEMBER

This isn't a lengthy novel, but if you're short on time and need to skim, don't miss the paragraphs marked with this icon.

TIP

The whole idea here is to learn something you can act upon, and the Tip icon points to a helpful bit of advice.

TECHNICAL STUFF

There's much to consider when implementing a CNAPP, and the Technical Stuff icon points to something you should know about the technology that goes a little more in depth.

Beyond the Book

There's more to this topic than will fit in a 48-page book. Here are a couple of places to turn to for more details:

- `https://www.wiz.io/solutions/cnapp`
- `https://www.wiz.io/blog/how-cnapps-identify-and-prioritize-excessive-risk-in-a-single-platform-gartner`

IN THIS CHAPTER

- » Introducing cloud native security
- » Looking at different roles
- » Defining the 4Cs

Chapter 1 What Is Cloud Native Security?

This chapter delves into what you need to know about cloud native security, which is a step in the right direction when you want to ensure a high security posture for your environment. Additionally, this chapter discusses some of the reasons why cloud native security is helpful when you want to make sure security is baked into every aspect of work so no threats emerge that can't be handled.

This book focuses on CNAPP tools and what they offer the CISO, DevSecOps/DevOps teams, and cloud security operation teams, who are the main personas for CNAPP. However, before starting out on any adventure, it's important to first lay the groundwork!

Defining Cloud Native Security

Before setting out on a journey on the seas of CNAPP (and you will definitely NOT be C-napping throughout this book — I promise to keep it interesting), it's important to be on the same page — or in the same boat — in regard to what cloud native security is and why it's important. After all, CNAPP is, at its most basic, a platform that provides you with the capability to achieve cloud native security.

And, what is *cloud native security?* Cloud native security is a security approach in which steps to ensure security are taken throughout the distinct life cycle of cloud native applications, from the infrastructure planning phase to client delivery and maintenance. With the cloud, teams can simply spin up an environment and go. The danger of that may be apparent, but just to be clear: With this flexibility comes an urgent need for a security model just as flexible and elastic as the cloud itself. You want to make sure that you can deploy security into this new cloud model quickly and maintain it. *Enter cloud native security with its own theme music!* Our hero, cloud native security is here to help you keep your cloud native applications secure.

TECHNICAL STUFF

Cloud native security plugs into the architecture based on elastic cloud services and the framework for agility, all while maintaining cloud security services, a security posture, and the capability to respond to and handle threats in real time. Cloud native security products provide the immediate security needed as you're working in the cloud.

Examining the Need for Cloud-Based Security Solutions

To fully understand cloud native security, it's important to first take a look at changes in application development and how those changes play into the bigger picture of maintaining a high security posture against threats.

As the shift from on-premises software to cloud architecture takes hold, more and more development is now done in the cloud on cloud-based platforms such as containers and *PaaS* (platform as a service) and *SaaS* (software as a service) solutions, just to name a few. Development teams continue to push forward with this model (called DevOps) because it's the most efficient and timely way to get products and services to clients and customers who expect them.

What role does security play in this shift? As developer teams embrace cloud native technologies, security teams find themselves scrambling to keep up. As more organizations embraced DevOps and developer teams began to update their application development pipelines for consistent and continuous small-batch code pushes, security teams quickly realized their old tools were ill-suited for the developer-driven, API-centric, infrastructure-agnostic patterns of cloud native security.

REMEMBER

With developers now coding directly on a fast-moving pipeline of continuous integration and continuous deployment (CI/CD), security needs to be integrated at all stages of the work from development until the big push to production.

Decentralized IT and the constant updates of services from cloud providers can create security concerns. Developers tend to create shadow IT organizations to use new tools and features without deploying security to approve (and secure) these new tools.

Security teams have evolved immensely over the past two to three decades. As technology has evolved, so have the threats and so have the security teams assigned to handle the threats. A paradigm shift over the years made sure that now security gets "baked in," which is just a simple way of saying that security issues are addressed as applications are being developed, not after. This is important because it allows for a proactive and less reactive approach to vulnerabilities, threats, exploits, attacks, and other alarming issues. Security teams now use new toolsets, models, workflows, and architectures to ensure security is not an afterthought but instead has evolved with the current technology of cloud.

Spelling Out the 4 Cs of Cloud Native Security

A cloud structure has millions of moving parts, which makes securing cloud-based applications especially challenging. This is where the 4 Cs of cloud native security come to the rescue! Together they provide security measures that protect applications — and the data included within those applications — running in cloud-based environments.

When moving forward with evolving cloud technology, both security and development teams should know about the 4Cs of cloud native security:

- **Cloud:** The cloud layer consists of the infrastructure that runs your cloud resources. When you set up a server with a cloud service provider (CSP), the provider is responsible for most infrastructural security. However, you're responsible for configuring the services, securing your data, and overseeing security. You should also know which cloud platforms are available, including infrastructure as a service (IaaS), PaaS, and SaaS.
- **Cluster:** The cluster layer consists of the Kubernetes components making up the worker nodes and control plane. It is at this layer that you secure your *Kubernetes* — or automated task — workloads. Kubernetes components use encrypted communication, requiring TLS certificates to authenticate with each other.
- **Container:** The container layer consists of container images, which may contain vulnerabilities for which you can scan. Organizations commonly overlook issues such as image security, the use of unknown sources, and weak-privilege configurations. It is important to keep containers regularly updated to minimize exposure through known vulnerabilities. You should also scan and verify any application running in your containers.
- **Code:** The code layer, also known as the application layer, provides the highest level of security control. You can restrict exposed endpoints, ports, and services to manage security risks. You should protect communication between both internal and external services using TLS encryption.

Understanding this model of security measures allows for a shift in how you approach securing your development environment while also exposing where you need to focus your efforts. Knowing the 4 Cs and how they help you carve out the areas of focus for security is just the beginning to understanding cloud native security.

IN THIS CHAPTER

- » Understanding the importance of collaboration
- » Creating a collaborative culture
- » Integrating various teams
- » Including cloud native security to mitigate risk

Chapter 2 Understanding DevOps and Shared Security Responsibility

In order to fully understand security in a cloud-based development world, it's important to first take a closer look at the development process and the role security plays in that process. Gone are the days of engineers, security teams, and DevOps — or integrated software development and operations teams — working separately. In order to keep up with the fast pace of working within a cloud environment, teams must unite in a collaborative space, fusing development, security, and operations together, also known as *DevSecOps*.

To get the best out of development, including security measures throughout the development process, teams need to work together in new value streams, breaking down older siloed methods of work and embracing a new paradigm. To do so there needs to be a level of shared responsibility. This is where cloud native security comes in.

Collaborating to Provide Improved Security Measures

First, let's break down and disassemble the traditional working model of the pre-cloud world. Most organizations were used to various teams working in siloes, each focused on its specific area of expertise. The development team focused entirely on the various aspects of application development and launch with little to no interaction with the security team. Even within the security team, there was very little collaboration. For example, one security team might be in charge of creating a tool to scan for misconfigurations while another security team created a tool to scan for secrets.

In this old method of development, products were brought to the point of launch and put into production without a close look at security weaknesses. Only after that launch were problems identified and addressed by operations teams struggling to keep the environment stable and the customers happy. The problem with this method is that it took forever to get anything done, and everything was done in a way that wasted time as each issue was addressed one-to-one by the appropriate team.

Looked at more succinctly, the three teams involved in this old working model were as follows:

- **Development:** Focused on making new code and working with code to create new things and produce deliverables for the organization and customers.
- **Operations:** Focused on maintaining integrity of the business operations posture to ensure that changes are known, tracked, and handled if any issues arise.
- **Security:** Focused on making sure that every step of the way all work is checked, audited, scanned, secure, and safe.

Today's modernized workflow introduced small-batch work where changes are put into a continues integration/continuous delivery (or deployment) pipeline, also known by the acronym CI/CD. These pipelines allow for developers to work on the left side of the continuum and produce new code, and when ready, push it into the right side maintained by operations teams who want to keep the environment free from issue. This continuum of the left and right side can be seen in Figure 2-1.

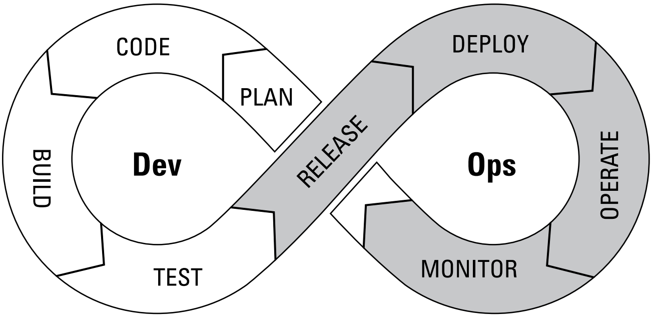


FIGURE 2-1: Viewing the DevOps framework.

Worlds collide! Instead of mass destruction on impact, we have the fusion of these key items that are critical for a new way of efficient work production, and code can be small batch, continuous, and released through safety gates. This integrated team model is called *DevOps*, the fusion of development and operations. A DevOps model allows for the two teams to work closely together so that as updates are released in small batches, there is operational oversight and understanding in place to make sure that production isn't impacted negatively.

Embracing a Culture of Shared Responsibility

In a cloud-based environment, the responsibility for development, production, and security is shared across teams and throughout the development process. Working together within the development pipeline moves the team from a "find and fix" model to one where security issues are identified along the way and remedied before the application is released to the customer.

One of the most interesting trends seen when adopting the framework of DevOps into organizations is how teams respond to alert fatigue. Due to the overwhelming nature of alert storms, the response most seen from team members is to ignore them, which can lead to exploits and security issues.

Not only are the developers and operators seeing more alerts, but they are also challenged with culling false positives, prioritization, and capturing sufficient context. Security teams should help provide a clean and understandable set of risks to developers but also discuss finding ways for all involved to mitigate risk together. Developers, operators, and security teams can all work together to share responsibility.

REMEMBER

Taking this model of collaboration one step further allows for increased security measures. *DevSecOps* integrates security into the DevOps team. This means that security teams are working collaboratively with developers to improve security. DevSecOps allows for the proactive remediation of security issues on the development side.

The cloud is an extremely collaborative space. Many teams across engineering, DevOps, and security interact with the cloud, but cloud ownership really belongs to developers across the entire stack. The trend is only going to shift more in this direction as developers become increasingly responsible for coding more of the computing stack in the cloud. This means that security teams must work with developers to improve security. It means operations teams need to be in the loop (or continuum) with developers and security to ensure production remains stable.

TECHNICAL STUFF

There is a need to ensure that development teams become more of a focus of equation between shift left development and shift right operations. An *SRE* or site reliability engineering team can handle operational issues that come up when handling code pushes in the pipeline. Add a security team into the equation and you have 100 percent coverage of any incident handling event that takes place when deploying code.

Achieving DevOps and DevSecOps

DevOps is achieved by embracing a culture of collaboration. Everything starts with this culture shift. Once you are positioned to have development and operations teams working together, then you can join the two so that processes can be realigned and workflows can be adjusted. This will ensure the continuous pipeline of development work pushed into production remains stable and constant.

TIP

Once culture is addressed and teams are realigned with new process and procedure, you need new toolsets. Later chapters will cover these tools; however, the need to retool is critical to embrace this new workflow.

Lastly, the handling of work through procedure and process must be examined carefully for alignment. For years, developers received lists of findings from security teams in an email with what they needed to fix. Organizations are realizing that this process doesn't work. It takes too much time, is too overwhelming for developer teams, and incurs too much overhead. And most importantly, it doesn't give context to developers on why something needs to be fixed. Once all of these items are in place, DevOps can be achieved. Once security is fused in, DevSecOps can be achieved as well, allowing for security to be a constant throughout the entire workflow and never left out.

TIP

Never make security an afterthought. Cloud native security means you're able to apply security in a cloud environment natively with the tools, processes, services, and functions available to what is made within it. It is baked in and never added after (see Figure 2-2).

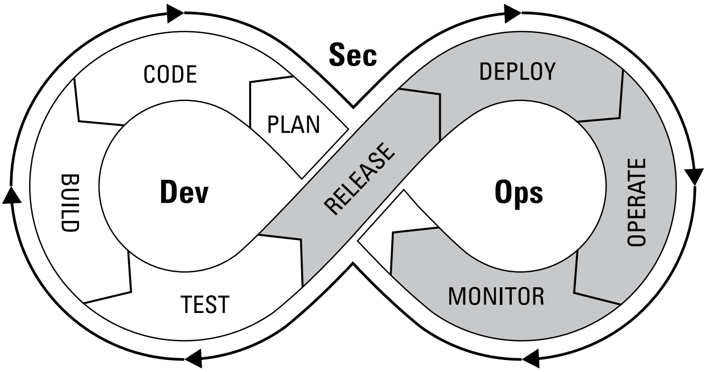


FIGURE 2-2: DevSecOps bakes security right in.

Leaning on Cloud Native Security

Cloud native security helps by putting the focus on security within the cloud and DevOps environments. In the past, work completed in siloes and assessed for security risks after the fact cost time and money. Cloud native security creates an environment in which security is baked into the solution and a constant presence, and one where any security issues are flagged and handled in real time, not as afterthoughts.

These is also the need for tools to snap in to the pipelines and handle security through all phases of the continuum. The industry recognizes the need to move from tools dedicated solely to security to ones that provide value for security and DevOps teams.

REMEMBER

This type of security is critical not only because developers own the remediation and response, but also because it is the only way to scale security up given the common discrepancy in team sizes between security and DevOps.

Security tooling that allows developers to easily understand the state of security for their resources and provides the information they need to proactively remediate issues is necessary and something that CNAPP is well positioned to offer.

IN THIS CHAPTER

- Getting to know cloud-native security solutions
- Removing tools you no longer need
- Deciding which security solution is the best fit
- Unifying various tools and capabilities

Chapter 3 Getting Started with CNAPP

Cloud technology architecture and workflows require a move away from an on-premise security posture and workload. Cloud native security needs to be applied in the right place at the right time. Baking in security throughout the process is a must. It is extremely difficult to simply carbon copy current security tools and workflows to new architectures, making it necessary to turn to something entirely different and new. This is where CNAPP comes in!

Understanding the Concepts of CNAPP

So what is CNAPP? This solution to a very complicated and complex problem has a very simple answer. A CNAPP is nothing more than an end-to-end cloud-native security solution.

TECHNICAL STUFF

CNAPP stands for cloud native application protection platform and is the further breakdown of tools and processes that surround the concepts of the cloud native security model. (For more on the security model, including core capabilities, see Chapter 5.)

CNAPP and its framework include a set of core features:

- **Cloud Security Posture Management (CSPM):** Automates both the identification and management of risks across cloud infrastructures.
- **Cloud Infrastructure Entitlement Management (CIEM):** Manages identities and privileges across cloud infrastructures and services.
- **Cloud Workload Protection Platform (CWPP):** Provides security for the application and for all cloud-associated capabilities.

CNAPP in its original debut focused on these three main features, which are technically at the center of providing security in cloud environments. However, as the cloud evolved and customer needs grew, so did the toolsets that needed to be baked into future iterations of CNAPP. Customers wanted more in an all-in-one tool, and from there, CNAPP started to expand and become more feature dense.

CNAPP provides a central control plane that unifies all security capabilities to protect cloud environments, making your security cloud native. It provides total visibility across silos, ensuring that security, cloud infrastructure, and DevOps teams can deliver full-stack security. CNAPP solutions integrate security and compliance capabilities to secure cloud-native applications throughout the application development life cycle.

REMEMBER

A term coined by Gartner, CNAPP is a new type of cloud security platform that secures cloud-native applications from development to production, while reducing friction and mitigating risks that result from tool silos.

Weeding through the Clutter of Other Solutions

In the cloud, your security operations remain as a priority and must be managed well. Complexity can cause mishaps. If you have too many steps that need to be taken to get something done, it leaves more room for error in those steps. This equals risk.

REMEMBER

To benefit from a CNAPP, first identify the tools you currently use, how they interact, and what they do. This will help you simplify and mitigate risk. To further simplify your security stack and operations, reduce cost and complexity, and ultimately reduce risk, consolidate into CNAPP. This will not only reduce costs but also complexity, helping to create a secure, compliant, cloud-native apps while improving their overall risk posture.

When consolidating, first understand what you do have and what can be further consolidated into CNAPP. These tools may include many current cloud and even on-premise tools currently in use.

TECHNICAL STUFF

CNAPP replaces an array of point-solutions in your cloud security stack with best-of-breed solutions including the following:

- Cloud security posture management (CSPM)
- Cloud Workload Protection tools (CWPP)
- Vulnerability management
- Container and Kubernetes security
- Cloud Infrastructure Entitlement Management (CIEM)
- Infrastructure-as-code (IaC) scanning
- Data Security Posture Management (DSPM)

Security teams and their leadership are almost always on board when it comes to reducing cost, risk, and complexity; closing gaps; and creating a single pane of glass; however, there are times when those who want something specific, and/or rely on a current tool, resist change. Today, enterprises attempt to close these gaps by implementing a variety of tools, each answering a specific risk.

This dispersed tool approach is time consuming, creates friction between security and development, increases overhead, and forces teams to work in silos. Because of this, ensuring buy-in for CNAPP and working together as one team is critical to designing and rolling it out. To get the entire team on board with CNAPP, show how all of these services applied together can help solve the business goals of both moving to new architectures and keeping them as secure as the old ones. CNAPP does this!

Integrating Security and Compliance Capabilities

Today's critical infrastructure and architecture requires seamless integration. As new technologies emerge and others transform, there is one constant — evolution! Integration of security and compliance into the tools at every stage of deployment and development is now as critical as ever not only to ensure safe and secure work but also to save time. CNAPP allows users to stop attack paths targeting cloud data at the source!

REMEMBER

CNAPP natively applies rapid, agentless visibility into critical data by allowing for quick scans of cloud buckets, data volumes, and databases. This allows the toolset to immediately respond to security incidents as they happen in real time. This is always done via a continuous process of detection of critical data exposure and through a single prioritized queue, taking steps toward analysis and response-handling criteria.

But wait, there is more! CNAPP also allows for schema matching so you understand data lineage and flow. When data is moved between environments and regions or stored improperly, you will know.

Choosing the Right Solution

Once on board with simplifying security solutions, it's time to pick the right solution to simplify, reduce, and eliminate costs and blind spots by deploying the CNAPP! Although this is a good recommendation, there will be some challenges in doing this. The first challenge is to make this decision in the first place. The decision usually starts with a proposal to show the benefits (and risks) of going with this solution. This proposal is generally mapped to the current (and future) plans for your organization's technical landscape.

TIP

Going to the cloud or somewhere in the middle? If you're in a hybrid, CNAPP may be the way to go as your work is already in the cloud and more will migrate overtime.

IN THIS CHAPTER

- » Determining if CNAPP is right for you
- » Analyzing exposure to risk
- » Determining risk priorities
- » Remediating existing threats

Chapter 4 The Need for CNAPP

As with many things in life, when it comes to technology solutions there must be a fundamental assessment of needs versus wants. Is CNAPP a security solution that your team really needs?

It's important to start by doing a needs analysis to quickly assess what is necessary and what is not. Identify risk exposures and priorities. What are the risks if you don't make the move to CNAPP? Brand reputation? Sales revenue? Legal ramifications? This chapter takes a closer look at how to determine if CNAPP is the best solution for these concerns and more.

Deciding if CNAPP Is the Right Solution

When determining if CNAPP is the right solution for your team, begin by asking the following questions:

- Is the development setup cloud-based?
- Is development work occurring in a DevOps pipeline?
- Is a real-time layer of security needed?

If the answer to all of these questions is yes, it's time to return to the idea of conducting a needs analysis. Beyond the technical architecture of application development, what are the goals and objectives that CNAPP might meet?

Ask what existing problems need to be solved and identify the potential solutions. Are there currently any gaps that need to be filled? Once you have identified the gaps, document the entire list of requirements for your solution and see if the CNAPP fits in. My guess is it most likely will.

Evaluating Risk Exposures

The most common thing that determines a need is risk exposure. This is where a risk analysis comes in.

Risk, simply defined, is the potential for failure, impact, or issue based on actions taken. Risk analysis is the investigation of risk to conclude what may happen if you do (or don't do) something. This is the simple equation that is applied when considering CNAPP.

TIP

There are many ways applications can be exposed to risk in the cloud, including unintentional public Internet exposure and excessively permissive access rights. There is a need for policy refinement, workflow and process refinement, and overall toolset consolidation. Reducing complexity and creating a single pane of glass reduces risk.

Examples of risk exposure happen to be plentiful when dealing with cloud environments and/or DevOps pipelines. When porting and moving data over to the cloud to interoperate with cloud systems, it is important to secure everything properly. However, the change in architecture creates a problem. The process, workflows, and paths things follow change. The technology evolves.

In order to satisfy the elastic nature of spinning things up the cloud immediately, doing small batch application development work in a continuous fashion, and creating containers of application work on the fly, a security solution is needed that adapts to these new methods of workflow. New problems can't be fixed with old tools. The new problems don't need to be problems at all, just workflows that introduce the possibility of exploit in different ways that potentially introduce risk.

REMEMBER

CNAPP helps close this risk gap by prioritizing and identifying and then implementing solutions around these risks.

Selecting Priorities

To determine risk priorities, you must first know the risks and how they directly impact you. This chapter contains seeds of information that can grow and expand into full-blown architectural design decisions based on the needs analysis.

Let's use a simple example of what may be deemed a priority in a typical organization. Take, for example, a company that makes widgets. Widget-making company ABCD wants to consolidate operations further into the cloud and currently has a large presence of data and application development within a known cloud provider. ABCD is not currently using a CNAPP but is considering it. Company ABCD's biggest threat is information theft, which could make exposure of its design and sales of widgets to other competitors a threat to its survival. The company's biggest risk is data loss.

Now that company ABCD is aware of the priority, what does the current architecture look like? VMD and databases hosting this information? Some in containers using Kubernetes? Shared tenant in the cloud? Possible hopping or traversal issues? Check.

Now, ABCD knows what its security risks are, but what does it currently use to solve this issue? The answer is disparate security systems and native alerts leading to alert fatigue and poor prioritization of priority-one alerts.

In the case of hypothetical company ABCD, CNAPP is the right solution for the selected priorities. Tool consolidation and one pane of glass helps teams address all issues in real time.

REMEMBER

Having too many individual point solutions, typically with a narrow focus, causes a struggle to correlate signals between various parts of a cloud environment. CNAPP solves this.

A CNAPP can monitor and enforce security across an entire cloud application profile, giving organizations — including hypothetical company ABCD — visibility into security issues that have significant business impact.

Identifying and Remediating Threats

With a CNAPP, security teams can identify and remediate the most critical security risks while maintaining an integrated approach to address vulnerabilities in cloud environments. When assessing the needs and then mapping the risks, prioritize them and then identify them. The next step following identification is implementation or remediation.

REMEMBER

To reiterate, the needs boil down to one goal: One platform should secure everything that's built and run in the cloud. When I say everything, I mean everything, all encompassing. One package should protect the entire cloud architecture.

The best way to do this is with a CNAPP. When deploying a solution such as a CNAPP, the goals for this solution are twofold: to identify and help remediate all risks but also to identify which risks are most critical and which should be attended to first as a priority. This is hard to accomplish from current disjointed multiplatform solutions. This is also what leads to alert fatigue or what I like to call it — noise. Pure noise. Things are missed in noise. That leads to risk.

It is well known that siloed security solutions only capture part of the picture. By using a different tool for each cloud security challenge, it is easy to miss out on the most important thing in cloud security: context. In this situation, context is king (or queen). Yes, pun intended!

An effective CNAPP solution should calculate the effective security posture of your cloud and correlate issues to identify the toxic combinations that make your cloud susceptible to attack. Examples of issues could be exposure, lateral movement, and more. A good example is a vulnerability scan alert on a VM that indicates a threat. CNAPP immediately knows that the VM has public access (Internet) and that there are administrative privileges assigned.

This toxic combination of administrative privileges and Internet access is a huge threat and could cause a lot of problems if not mitigated. CNAPP offers this holistic view of the entire security attack surface and helps you handle it like a pro. Now you are positioned to identify and remediate the threat!

IN THIS CHAPTER

- » **Introducing the tools in the CNAPP platform**
- » **Minimizing complexity and cost**
- » **Supporting the security operations teams**

Chapter 5 Core CNAPP Capabilities

What are the core capabilities of a CNAPP? What makes a CNAPP tick? How does it work? What can it do? CNAPP platforms bring together multiple security tools and functions to reduce complexity and overhead, providing for many, many services and functions. But wait, there's more!

CNAPP also has the combined capabilities of cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), cloud workload protection program (CWPP), data security posture management (DSPM), vulnerability management, container and Kubernetes security, and infrastructure-as-code (IaC) scanning tools. It is an expansive platform that allows for the reduction of complexity. It is a single pane of glass solution. It allows for control over your architecture and so much more. It also plays well with others — always good to have in the schoolyard.

Marveling at the Mighty CNAPP Platform

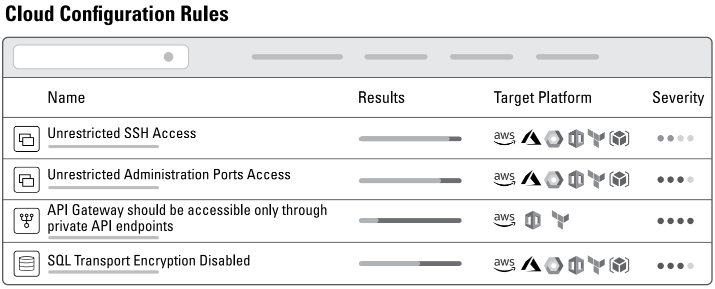
The mighty CNAPP platform, marvel in its presence. Are you astonished? Perplexed? Well, you should be! It is one of the coolest services to come to market and is incredibly helpful. Watch your time combing through operational issues in your security operations centers drop drastically with the increased visibility and clarity provided by this mighty behemoth. What makes it so mighty? CNAPP is an all-inclusive tool unlike all others.

The combined capabilities of CSPM, CIEM, and CWPP tools in the CNAPP make this already awesome platform even more awesome. For a quick overview on the most critical of cloud security services in use today, read on. If you want to know more about the more granular details of these core capabilities and how they fully integrate into CNAPP, turn to Chapter 7.

CSPM

CSPM allows for contextual security posture management across clouds. This type of management allows for continuous detection and remediation of misconfigurations from build time to runtime across hybrid clouds — AWS, GCP, Azure, OCI, Alibaba Cloud, and VMware vSphere.

The CSPM allows you to remediate issues in an established security posture and to do so immediately and automatically. This is done with built-in rulesets, custom rules, and other real-time detection methods. An example of built-in rules ready to go out of the box to provide for immediate baseline security are seen in Figure 5-1.



Cloud Configuration Rules

Name	Results	Target Platform	Severity
Unrestricted SSH Access		aws	●●○○
Unrestricted Administration Ports Access		aws	●●●○
API Gateway should be accessible only through private API endpoints		aws	●●●●
SQL Transport Encryption Disabled		aws	●●●○

FIGURE 5-1: CSPM security rules applying posture management.

Now you can take control of cloud misconfigurations if they happen (and they will), reduce alert fatigue, have a single pane of glass with security policies across your clouds, and even apply it in depth when handling code or IaC. Priceless!

CNAPP connects to a cloud environment and gives complete visibility and actionable context on the most critical misconfigurations so teams can proactively and continuously improve the cloud security posture with a great comprehensive CSPM and over 1400 rules ready to go.

CIEM

CIEM is a toolset that allows you to manage cloud-based identities and privileges so that the entitlements are understood and managed in a secure way. In other words, when using services like identity and access management (IAM) solutions in the cloud (or across clouds), you can mitigate risks associated with too much privilege or entitlement. Analyze cloud entitlements and autogenerate least-privilege policies across your cloud to help teams visualize, detect, prioritize, and remediate identity (IAM) risks. CIEM services are ideal for those who want to reduce the attack surface of access level exploits.

TECHNICAL STUFF

Those new to cloud should understand the complexity of IAM. What it has to offer is actually quite vast compared to well-known on-premise systems. The granularity of assigning rights and privileges, to whom, where, and to do what, is incredibly large in scope. It is exponentially more complicated, and with that complication (or complexity) comes the possibility of errors leading to exploits. A CIEM can help you solve that problem.

TIP

Reducing unnecessary privilege — known as the *least privilege model* — reduces the amount of cloud entitlements held by an identity. The aim is to reduce the privileges to the exact ones needed, therefore reducing the security risk.

The main components of CIEM are entitlement visibility, right-sizing permissions, advanced analytics, and compliance. A CIEM will scan an environment to determine gaps and help resolve them. Because traditional IAM tools found within cloud providers are static, and cloud services require more dynamic (ephemeral) entitlement generation, CIEMs are critical to providing security to reduce threat.

CWPP

CWPP is used to protect workloads in the cloud by providing holistic overarching protection to any and all designated workloads in the cloud environment. Sounds straightforward enough, but only if you know what a workload is!

Cloud environments have changed how work is done, and by working differently, new workflows are created through process, systems, and services. For example, if you're using a platform as a service (PaaS), you will have to spin up specific services that fit in that platform. If you spin up a database, some middleware, and a front end to test a new application, these items need to be part of your current workload. Well, how do you manage the holistic view of applying security to this dynamic workload based on elastic services that will shrink and grow at will? Two databases are now needed in a failover confirmation. Workload (and flow) has changed and so must the security platform keeping an eye on it.

Enter the CWPP! The CWPP applies security to the entire workload, detecting and removing threats as they appear. It does this in workloads such as the previously mentioned PaaS environment but also in many more, including container based, serverless, VM (native or otherwise), physical and virtual mix, hybrid cloud (on premise and public cloud provider), and more! CWPPs have many functions, including vulnerability management, integrity checks, access control, intrusion detection, and prevention. CWPP is the real deal when it comes to workload protection!

TECHNICAL STUFF

Although we have covered core capabilities, there are many other additional capabilities when looking into the depth of CNAPP. These include services such as DSPM, which provides integrated data exposure protection and which is used to continuously monitor for sensitive data like PII, PHI, and PCI across your cloud environment and proactively eliminate attack paths to prevent data breaches. Similarly, the other two tools provide advanced security monitoring to Kubernetes and container-based environments and IaC code-based environments. Together, these tools help CNAPP be all it can be to provide advanced security across the depth and breadth of your organizational assets.

Reducing Complexity and Overhead through Correlation

To understand how CNAPP reduces the complexity and overhead of multiple current systems by combining these great tools into one platform, begin by figuring out what all of them have in common: Cross-tool correlation.

Correlation of vulnerabilities, context, and relationships across the development life cycle, in the cloud and elsewhere, is the key to success when deploying CNAPP.

Once incidents are correlated and understood, action is taken to remediate. Guided and automated remediation to fix vulnerabilities and misconfigurations provides immediate resolution (or mitigation) of possible show-stopping events.

Staying Safe with the Help of Guardrails

Anyone who has been in the driver's seat in the middle of a security exploit mitigation knows you take some wicked turns and get some unexpected high-speed chases! So how do you prevent an imminent crash? Well, guardrails are always helpful. Guardrails are used to prevent unauthorized architecture changes and to give the cloud a guiding path toward success. It keeps the car on the track and provides some stability when you're trying to navigate.

The most important concept to remember about guardrails is that they are meant to help, not hinder, your progress. Not everyone loves to follow a prescribed path, but luckily guardrails are usually in the background and don't really interfere with your efforts. They are designed that way. So, what is a guardrail in the context of a CNAPP?

REMEMBER

As more and more developers have shifted to cloud-based workloads, the security tools of times past have not kept up to date with the new agile high velocity work being done. Because of this, security guardrails (in other words, policies and controls) are put in place so that new DevOps pipeline-based workflows are able to maintain pace, while in the background these guardrails are doing the job of keeping you safe and secure.

Bringing in the SecOps

SecOps (also akin to DevSecOps) is a shortened name for security operations. Security operations teams normally work in security operations centers (SOC) for the purpose of monitoring for security threats and responding to them. Now that you understand the guardrail system and why CNAPP at its core applies security in real time all the time, what happens next? Response is what happens next. That is, if you need a response. Traditional SecOps (security operations teams) monitor for refined alerts from verbose data and conduct incident handling when something is flagged as a priority and requires a response.

CNAPP helps your SecOps teams by applying that shim within the process where a tool-based response may also help automate incident handling and/or allow for teams to respond immediately when an issue arises. As seen in Figure 5-2, you can get immediate alerts that SecOps can monitor and respond to. As well, the CNAPP can also integrate in with your current processes and toolsets to create an even bigger toolset worthy of a true SOC.

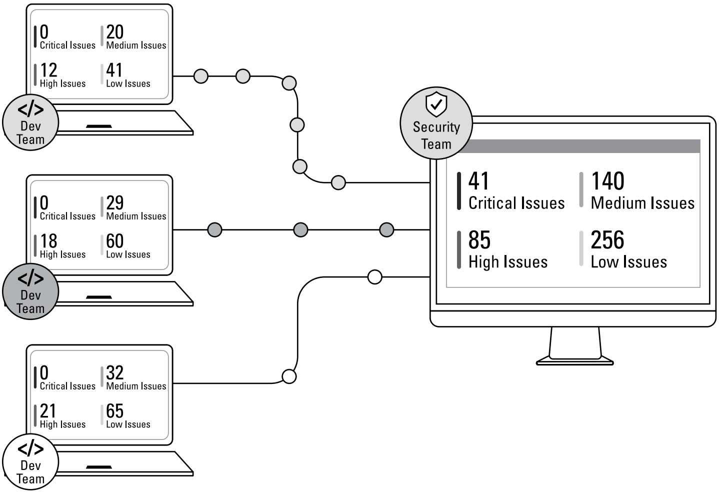


FIGURE 5-2: Monitoring SecOps Alerts with CNAPP.

CNAPP allows for easy integration with SecOps ecosystems to send alerts in near-real time. Now if that doesn't help you stay on top of things, I'm not sure what will. Rest assured, CNAPP core capabilities have you covered from cloud to development, covering new workflows and workloads and providing the safety net needed to satisfy security teams and their need to keep security priority number one!

IN THIS CHAPTER

- » **Exploring the benefits of CNAPP**
- » **Enjoying a simplified solution**
- » **Downsizing current tool management**
- » **Including security in a cloud environment**

Chapter 6
Introducing the Benefits of CNAPP

With still more to learn about the wonder that is CNAPP, it's time to focus on the benefits. When the time comes to add another tool to the toolbox, it can be tough to justify the purchase to the powers-that-be in an organization. And it's also true that some have been burned by buying tools with redundant functions, poor integration, the requirement of additional staff to manage them, and other common headaches associated with integrating new tools.

The great thing about CNAPP is that this particular toolset (or platform) sells itself once you understand why you need it. Read on to find out more.

Benefitting from an Integrated Solution

Everyone loves a friend who always has their back. When it comes to security, CNAPP has yours.

REMEMBER

CNAPP is a one-stop shop that gets rid of those pesky duplications, tough integrations, multiple panes of glass, and headaches associated with managing teams with cross-vendor toolset skills. It is truly a unified security solution that does it all — in a modernized cloud landscape.

As a unified security solution, a CNAPP offers complete security coverage to help you keep up with ephemeral, containerized, and serverless environments, providing you and your organization all of the benefits associated with securing a modernized workload.

Another huge benefit CNAPP brings is integration: Alerting can be streamlined and consolidated. When you have multiple tools sending alerts, a tool that is there to catch them and work through them quickly and efficiently may just become your best friend, especially if that tool helps you mitigate a massive attack and exploit of your trusted systems.

Simplifying to a Single Pane of Glass

REMEMBER

A main benefit of CNAPP is its capability to view and manage data all on one screen. Being able to do this is critical to understanding the landscape of technology today and what it takes to keep pace in today's business world.

Everything, and I mean everything, runs on digital. All aspects of business are moving in the direction of being software-driven. Now more than ever (and even more and more into the future), the development of software is at the core of literally everything we do. Keeping software updated to customer demands has exponentially grown faster and continues to speed up. This means workflows have changed and moved into more agile methods. Loosely translated? You need to do more, faster.

Finally, factor in the technology that is needed to run this software development life cycle (SDLC). Everything has changed. Development now occurs within the cloud because that is the best environment to use elasticity to develop and push new code for applications. These cloud environments host pipelines (DevOps) so that code can be pushed safely and quickly in small batches to make those customers happy and keep them happy — quickly.

With this full understanding of the changed landscape, it's easy to see how overwhelming it would be to lean on multiple security measures with each tool siloed within its own security team. Today's fast-paced environment requires a new toolset that allows you to do this work quickly and efficiently. This is where CNAPP enters the picture.

REMEMBER

The benefits that CNAPP provides with a single pane of glass include:

- Providing a more intuitive look at security events and attacks
- Improving efficiency
- Encouraging collaboration across teams
- Integrating alerts with remediation guidance
- Helping teams make more informed decisions

Minimizing the Necessary Tools

The next major benefit of CNAPP is tool consolidation. CNAPP's one-stop shop allows for the application of security methods in real time for all of the modernized workflows in your cloud provider. Once CNAPP is in use, it is possible to begin to decommission any outdated or redundant tools that will no longer be necessary. Nothing is more annoying than trying to maintain the tools of yesteryear. Why not reduce and eliminate these dinosaurs?

CNAPP provides the capability to reduce the complexity of your current security solutions, which reduces overhead costs. By replacing multiple point products with a single comprehensive tool, it's possible to have a complete picture of risk with one cost and one location to manage.

Staying Secure in the Cloud

During your organization's digital transformation, you may have felt like you'd awoken to a life in the clouds. This can be disorienting!

However, one of the major benefits of CNAPP is, quite frankly, rooted from being in a cloud. Cloud, hybrid, multicloud: No matter where you are in your digital journey, somewhere nestled in every organization today is a small to very large cloud footprint. The benefits of being in the cloud are why everyone is migrating as part of their individual transformations. The easiest way to do development is to do it in a cloud-hosted environment. Because software is the lifeblood of everything these days, it makes total sense that people would be doing some form of software-development work in the elastic cloud. If software is the lifeblood, you can consider data to be the oxygen to enrich it. When considering security, a core component remains to be data. Discovering and protecting sensitive cloud data (for example, PHI, PCI, PII) is absolutely critical!

You want to keep your head in the clouds? Great. But don't forget to consider security! You shouldn't simply migrate to the cloud and hit the ground running. You must take the security team with you. With CNAPP, you can do that easily.

TECHNICAL STUFF

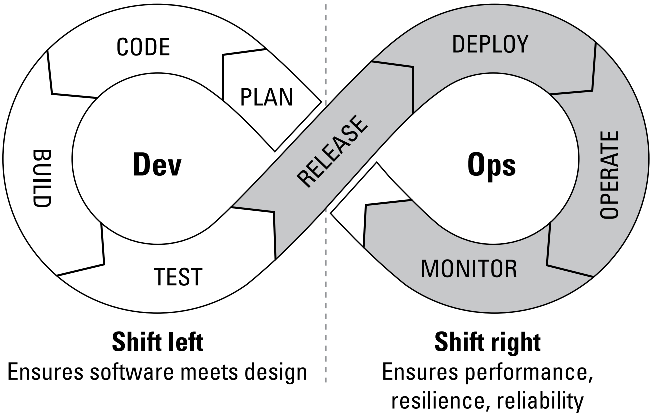
With CNAPP, you get comprehensive cloud and services coverage with visibility and insights across your entire multicloud footprint, including IaaS (infrastructure as a service) and PaaS (platform as a service), extending across VMs (virtual machines), container (Kubernetes), and serverless workloads and into development environments to identify and remediate risks early.

Integrating Security into DevOps

REMEMBER

The best way to embrace the fast-paced cloud environment is to move workload to a DevOps model. DevOps (the fusion of development and operations teams) is what allows you to create a pipeline of continuous integration and continuous deployment (CI/CD) in small-batch work to make customers happy by giving them what they want — but also by not releasing trash that takes down your services. Loosely translated, it's a pipeline that keeps the product coming with no disruption.

When developers work in their integrated development environments (or IDE), they're just working. Work, work work. Go, go, go. Push code into the pipe. Happy pipe, happy life. This is normal workflow and expected at the development left. Focusing on this side of the DevOps continuum is called *shifting left.* On the right side is operations and where we release that cool code into the wild. The entire continuum keeps the code rolling out and makes everyone happy (see Figure 6-1).



CODE
PLAN
BUILD
Dev
TEST
RELEASE
DEPLOY
Ops
OPERATE
MONITOR
Shift left
Ensures software meets design
Shift right
Ensures performance, resilience, reliability

FIGURE 6-1: Shifting left or right.

Traditional (and now outdated) security tools don't monitor this software life cycle pipeline well. CNAPP does. It applies security at the speed of DevOps. It does this because it's integrated into the pipeline and is the great watcher in the sky (get it, we're in the clouds?) and makes sure that security is baked in when moving the team from DevOps to DevSecOps.

Once security is baked into the cloud or DevOps, you can trust that you will be ahead of both known and new emerging threats leveraging new systems in this modernized architecture. When you inject security at every step and further bake it into the DNA of all technology, you don't have to think of security as an afterthought. CNAPP uses guardrails to distribute security responsibility, with native integration included into existing development and DevOps tools.

REMEMBER

Implementing guardrails enables developers to take ownership of security in their work, reducing friction between security and the DevOps team. CNAPP integrates with IDE platforms to identify misconfigurations or compliance issues during development and

CI/CD, as well as with SecOps ecosystems to trigger alerts, tickets, and workflows on violations so teams can act immediately.

TECHNICAL STUFF

IDEs integrate into the DevOps continuum, and if anything is a security issues on the left, it will not make it out to the right because of security gates. Bad code is blocked but also security violating code. CNAPPs allow for a full view of all security issues originating and trying to be released into the wild.

IN THIS CHAPTER

- **Getting to know what makes CNAPP unique**
- **Understanding the CWPP and CSPM aspects of CNAPP**
- **Creating solutions that interact seamlessly**

Chapter 7
What Makes CNAPP Different

CNAPP certainly has a lot going for it! It helps modernize security posture, reduces the workload required to monitor and respond to security attacks, and helps consolidate how you receive and deal with alerts into one platform. But how does it compare to individual solutions that each provide one aspect of CNAPP's capabilities? Is CNAPP simply a stitching together of other individual point solutions?

This chapter takes a closer look at how CNAPP compares to two other security protection solutions: CWPP and CSPM.

Understanding What Sets CNAPP Apart

There are many components that contribute to how CNAPP is able to deliver holistic security coverage in real time including:

- **Cloud native:** CNAPP provides cloud-native security.
- **Proactive security posture:** CNAPP adopts a proactive security posture by being on top of issues as they happen, not reacting after the fact.

- **Context and prioritization:** CNAPP unifies interconnected risk factors into one view so you can respond to a prioritized incident immediately.

REMEMBER

CNAPP technology emerged based on changing trends in the way technology is developed and delivered. With these changes came the need to remain vigilant in new and innovative ways. When security teams have streamlined content with prioritized context, they can immediately respond to real-time events in progress. Specific factors help to create this context so you can be proactive natively in the cloud.

The evolution of risk in the cloud immediately raised the bar on requiring a different way to address security. More risks immediately emerged. The changing compliance measures and practices also changed the need for a more proactive method of identification and mitigation. Shared responsibility required a shared responsibility mindset and response methodology.

The response change required new tools, better tools, and tools that did the job more efficiently. Consolidation of tools into unified platforms required a prebreach handling of issues away from postbreach. All of this was done by using the platform that has all of this functionality within it.

Looking Under the Hood of CNAPP

Lift up the CNAPP platform's hood and you'll see there's a lot going on under there. Various components create the signals going from devices or systems and from functions or services, all ultimately able to be monitored on one central spot. From here, CNAPP shows specific issues or problem areas that need to be addressed. Functionality from a variety of tools make all of this possible. Two of those tools are CWPP and CSPM.

CWPP

TECHNICAL STUFF

Cloud workload protection platform (CWPP) is used to protect workloads in the cloud by providing holistic overarching protection to any and all designated workloads in your cloud environment. Workloads covered include virtual, serverless, container, and more. Workloads include multiple systems that may make up one function or service.

In the cloud, these workloads are very common and work together to provide this needed functionality. For example, if I wanted to provide a database platform for all key data to be stored and then load that data in a bucket for filtering, analysis, or reporting, that entire effort would be considered a workload. Seven containers running an application in Kubernetes is a workload. N-tier architecture serving up a website to customers is a workload. It really is endless how many possibilities you can dream up.

Because cloud environments have changed how we work, we must continue to grow and embrace new technology. We must also find ways to do this work securely. CNAPP provides a security solution that contains CWPP to protect your workloads. With a security graph-based methodology, you can immediately identify problems, for example, in your containers and respond to them. Figure 7-1 shows an example of a CNAPP using a workload to identify where and why there is a problem.

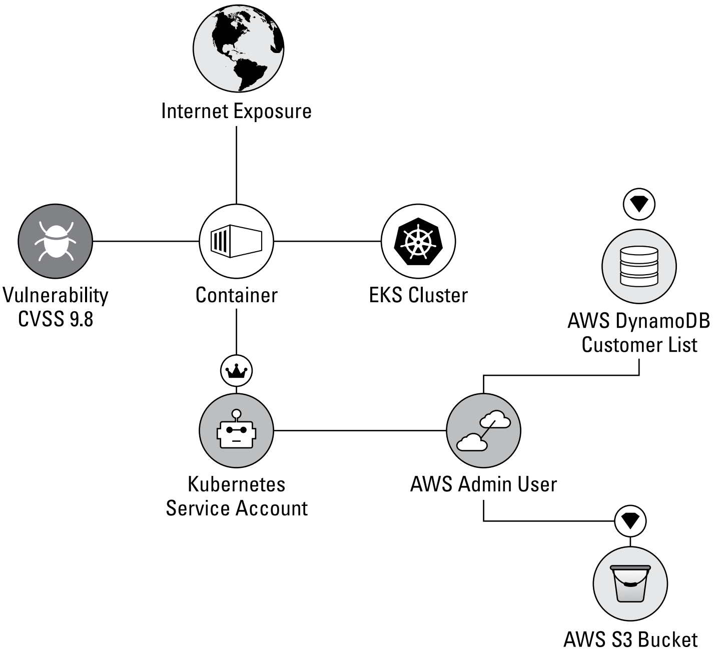


FIGURE 7-1: Correlating a container-based issue with CNAPP.

The CWPP applies security to the entire workload and detects (and removes) threats as they appear. Workloads that are protected include the following:

- Container based
- Serverless
- VM (native or otherwise)
- Physical and virtual mix
- Hybrid cloud (on-premise and public cloud provider)

CWPPs have many functions, including vulnerability management, integrity checks, access control, intrusion detection and prevention, and so much more. CWPP is the real deal when it comes to workload protection!

CSPM

Now let's check out the second heavy hitter in the house: cloud security posture management (CSPM). This technology allows for contextual security posture management across clouds. Why is this so important? It's important because the digital transformation of most companies doesn't just lock them into one cloud provider. In fact, most companies employ many different cloud providers! Three organizations that are the most common cloud providers include Amazon, Google, and Microsoft, but there are certainly others as well. CSPM allows for continuous detection and remediation of misconfigurations from build time to runtime across your hybrid clouds including the following:

- AWS
- GCP
- Azure
- OCI
- Alibaba Cloud
- VMware vSphere

This allows for a holistic view of the forest through the trees as well as the forests which you are adjacent to.

The CSPM allows you to remediate issues in your established secure posture and to do so immediately and automatically. This is done with built-in rulesets, custom rules, and other real-time detection methods. Take control of your cloud misconfigurations if they happen (and they will) to reduce alert fatigue and to have a single pane of glass with your policies across your clouds that you can apply in depth when handling code or IaC. CSPM secures workloads from the outside. It achieves this by evaluating compliant and secure configurations of the cloud platform's control plane. You can use the CSPM to connect to your cloud environments and allow a complete view across clouds.

TECHNICAL STUFF

Cloud management comes in all shapes and sizes. Beyond core capabilities there is a need for CIEM, IaC scanning, DSPM, container and Kubernetes security, and even agentless solutions to help build on CNAPP capabilities. When you look under the hood, it's important to know that beyond the engine there are many other components that are required for the full experience. Much is the same with CNAPP. Consider what makes this solution unique — an agentless solution that provides a customer with a full cloud security management solution that focuses on the engine but also the tires, interior, and other important parts of the vehicle.

Finding Solutions That Work Well Together

If CNAPP includes both CSPM and CWPP technology, what makes CNAPP so special? Simply put, it plays well with others in the schoolyard, which isn't the case with all technology solutions. Unfortunately, many individual point solutions focus on a limited set of security issues and don't integrate well together when it comes to correlating their signals, leading to challenges around prioritizing many low-priority alerts.

Imagine having a CWPP from one vendor and a CSPM from another vendor. If you try to work with them together, you may have your work cut out for you. Will it be seamless, integrated, and work to provide a single pane of glass? When you want many dissimilar vendor systems to work together well, you need to choose wisely.

CNAPP bridges the gap created by individual point solutions, which makes security as simple as mapping and planning out goals, objectives, and current toolsets to give you a path to project deployment.

Once you deploy, you need to consider how you will technically map the CNAPP together. You don't just plug it in and go — or do you? CNAPP must be designed and deployed. It must be configured, tuned, and managed. These steps must be planned out.

REMEMBER

CNAPP is more than a stitching together of all these individual capabilities. By combining user behavior data from the cloud and from workloads, CNAPP provides advanced insights that could improve detection rates and reduce false positives. These insights are priceless and are considered the Holy Grail of CNAPP outputs. When you monitor systems for security, it requires knowledge of security process and practice but also a deep knowledge of risk and compliance.

IN THIS CHAPTER

- **Introducing the five points of security**
- **Understanding the need to shift left**
- **Securing with APIs**
- **Reducing permissions**
- **Embracing a shared security model**

Chapter 8 Effectively Securing Cloud Native Applications

When considering the importance of CNAPP and the role it plays in modernized organizations within the cloud, remember that the need for a cloud-native security solution is what makes CNAPP a critical tool. Cloud-native removes the need to retool, code, or change anything on an application when migrating it. It migrates and works seamlessly because it is native to the systems running in the cloud. No alterations are required to port it over.

The key to effectively securing cloud-native applications is to use a tool like CNAPP that applies a security blanket to the entire cloud environment. It does this by embracing the methods of shift left for development, applying perimeter security at the function and container level, minimizing roles and privileges, securing application dependencies, and managing a shared responsibility security model for your deployment. This is also known as the five points.

Getting to Know CNAPP and the Five Points

CNAPPs provide security, yes, but unpacking the specifics makes it easier to understand just how that's accomplished. It's such a massive umbrella and does so much, but what specifically does CNAPP accomplish to provide this overarching view into the cloud and provide real-time security while also providing a wholistic view into very complex and highly fluid environments?

REMEMBER

CNAPPs do this by embracing DevOps. They do this by focusing on shift-left. CNAPP also does this by looking at security and applying it in very complicated virtual environments where instances are brought up and down constantly over time. It looks at any dependency that maps across workloads for issues and can identify them.

CNAPPs also provide a deeper level of security permission management where credentials, privileges, and entitlements will get you everywhere you want to be. Things need to be locked away ever tighter as time goes by.

This all equals a shared responsibility model for security that crosses all teams, siloes, and boundaries so that when issues arise, the focus and priority is on resolving them.

Shifting Right or Left

For those of you who have lived life in an operations role, you know that stability is your friend. Changes are your enemy. Anytime someone touches something, there is risk that this change may create a large (and sometimes long) impact on a stable production system. This is the same for the security side of things. Change can invite security threats such as misconfigurations that cause exploitable holes, bugs from upgrades, or destruction that requires time to restore or resolve.

This shift right sounds pretty solid, right? Well, the problem is that everyone is being told to shift left! On the DevOps continuum, the right side of the curve is about operations and keeping this stability, and the left curve is focused on the developers and change. And lots of change, too. This is why shifting security left is a major focus for CNAPP.

REMEMBER

By shifting security left, you can provide your security team with tools to prevent untrusted images in your CI/CD pipeline as well as mechanisms to avoid security issues in code before it is deployed to production. By scanning for image vulnerabilities, secrets, and malware early in the development process, developers can participate in enforcing security standards. This leads to cleaner code, less rework, and most importantly, the highest level of quality before being released into production. Shifting security left will allow for toolset-based focus on all aspects of preproduction code in the pipeline. By shifting left, your focus is on application development, which is the lifeblood of organizations looking to advance into the future.

Turning to APIs

Next up on the five points list is applying perimeter security at the function and container level. This can be done with applications programming interfaces (APIs). APIs are used to interface with applications so they can communicate. One important practice to ensure holistic security of an environment is to use API and application security tools built for a cloud-native environment. With direct API connection, your toolsets can interface directly with cloud-native systems for the exact information needed to further manage (and secure) systems in containers, or other unique cloud service like serverless instances.

TECHNICAL STUFF

In containerized environments, it is important to address security at multiple levels — the orchestrator control plane, physical hosts, pods, and containers.

Beyond that, the general approach is to enforce perimeter security at the function level — identifying functions that are triggered by a different source than usual and monitoring for anomalies in event triggers.

CNAPPs allow you to manage systems at the container level and provide more detailed information based on issues with misconfiguration, policy violation, risk, compliance and so much more! Figure 8-1 shows a Kubernetes compliance heatmap used to find violations.

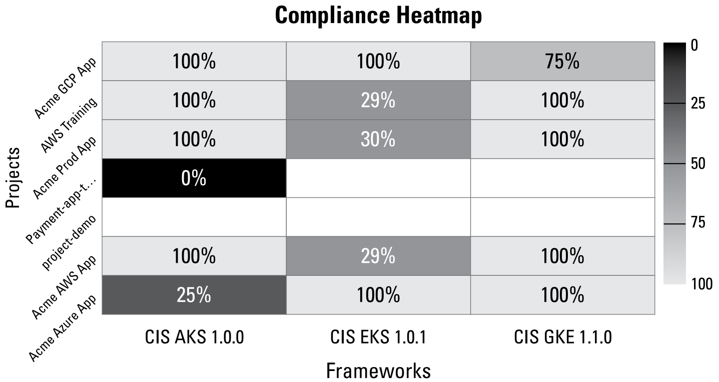


FIGURE 8-1: A look at a Kubernetes compliance heatmap.

Minimizing the Hands in the Pot

CNAPPs let you manage roles and privileges in a very granular, dynamic, and ephemeral environment. There are also many hands in the pot. When you consider a cloud environment, the number of hands in that pot is pretty high! When you think about a DevOps pipeline working in value-streams from womb to the tomb (or the SDLC), *a lot* of people are involved.

The way all of this is managed in the cloud is by identity and access management (IAM). IAM is the way you assign roles to users of the cloud and/or more granular permissions. These can be assigned via function or given out specifically to the privilege itself. So, think of the workload: If you have an application hosted via cloud container function, you may need to create granular permissions for specific areas of it, or if you needed someone to administer the whole thing, you can select a function with the predetermined permissions a person would likely need to do that role. This is how you can use access controls to enforce security.

TIP

Take the time to create a minimal role or set of permissions for each function or container. This ensures that if an element in the cloud-native architecture is compromised, it will cause minimal damage and prevent privilege escalation to other components.

Securing Application Dependencies

Can you secure application dependencies? If so, then yes, you can provide security. Serverless functions and application code often include packages with dependencies that are retrieved from repositories like npm or PyPI. Herein lies the problem. How can you stop security violations when dependencies perform this act?

TIP

To protect your application's dependencies, you need automated tools that include a comprehensive database of open-source components and their vulnerabilities. You also need cloud-native orchestration tools that can trigger application security activities during the development process. By running these tools continuously, you can prevent the inclusion of vulnerable packages in a function or container running in production. When you consider your application dependencies and how to resolve them, only then can you be secure.

Sharing the Responsibility

The truth is, until you share responsibility for security there will always be an avenue of attack left open by those who don't embrace it. You are only as strong as your weakest link. Therefore, you need to embrace a shared responsibility for security as part of a team. Cloud security is team sport, and organizations are demanding a new operating model for how cloud security works. This requires teams to work together.

You must also have shared responsibility levels and a model in technology when considering security. Apply security to all aspects of your technological footprint, big or small. Sharing responsibility is part of everyone's job in security, but when you need to apply security to your cloud solution, code pipeline, or other cloud-model or service, you should consider the CNAPP.

Chapter 9

Ten Strategies for Using CNAPP

There are certainly more than ten strategies for using CNAPP, but this chapter takes a look at the ten most important top-level strategies. These strategies may help you to get this platform approved, implemented, and in use:

- **Embrace the cloud:** Quite frankly, if you are not in the cloud, the CNAPP is not for you. If you have taken steps toward it and are using it, then you are a candidate. Now, if you are a small organization working on a small workload or a mega-corp with millions invested, it all depends on how secure you want to be. Size matters not.
- **Understand the concept of shared responsibility:** If you are in the cloud, great. Next, you need to embrace the DevOps model and mindset, which is agile work with a small batch processing pipeline of continuous work producing continuous product. It does this by focusing on development (the creation of product) and its interaction with operations teams (who keep the environment stable and secure) so that the fusion of both allow for quick resolution of issues that come to light.
- **Consolidate:** If you have too many tools, you need to identify them (asset management), figure out what your

model will look like (multicloud environment), and deploy a tool like CNAPP to seamlessly integrate into the cloud native environment and provide modernized security via one view (one pane of glass).

- **Fix what matters most:** Once you have a toolset that can apply this modernized security need, you can use that holistic view to find and eliminate issues in your environment using cool things like context, prioritization, and signal alert consolidation.
- **Shift left:** Now that you have a grasp on DevOps, let's just jam good ol' security in there and make us some DevSecOps. Now, you have not only shifted left and ensured that code as currency keeps your company growing and earning, but now it can be kept secure every step of the way in the development life cycle.
- **Apply security at the container level:** Different models require different security solutions. With serverless workloads, containers, and other versions of cloud functions outside of the standard VM, you now have to consider that applying to security on them has changed, too. Using APIs to seamlessly connect as an example, you now have new insights into things like containers and other functions. Ultimately, this helps you secure it with ease.
- **Minimize roles and privileges:** Enough said. No seriously, you need to get into identity and access management (IAM) and look at the predefined roles and then the granular privileges you can assign in a cloud environment. Not only is it super-granular but it's intensely difficult to comprehend from all the new lingo and terminology used in cloud and development environments. The goal of security is to minimize them but also to understand them (and the technology) so it's easier to reduce and manage them effectively.
- **Secure application dependencies:** Code reaching out to other code. That's it. Make sure that when this happens you can secure it, because if you can't, trouble will come knocking.
- **Share responsibility:** The key to the future is for everyone to share responsibility for security. A shared responsibility model for teams to follow as well as technology within a CNAPP will lead to a more secure environment.
- **Partner with the experts:** If you need help, you need experience.

Visibility, prioritization, and agility!

Cloud security and development teams need a unified approach to identify and remediate risks and respond to threats in their cloud environments. This book explains how CNAPP can help your business prioritize threats and think about security before anything bad even happens by using a single risk queue that prioritizes what is the most critical next step for your teams to take.

Inside…

- Embrace a shared security model
- Fix what matters most
- Build bridges across teams
- Unify various tools and capabilities
- Analyze exposure to risk

WIZ

Rob Shimonski is a cloud architect and author looking to ensure client success when moving workloads to the cloud. One of Rob's passions is the fusion of security into new technology to make it highly secure but also flexible and usable. Rob's current focus is on CNAPP and how to deploy it to make companies more secure but also highly functional.

ISBN: 978-1-394-20694-0
Not For Resale

9 781394 206940

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT