Brought to you by:

LACEWORK

CNAPP

for dummies

A Wiley Brand

Learn more about CNAPP and its history

See how CNAPP offers cloud security at scale

Understand why legacy security isn't enough

Lacework®
Special Edition

Ed Tittel

About Lacework

Lacework offers the data-driven security platform for the cloud and is the leading cloud-native application protection platform (CNAPP) solution. Only Lacework can collect, analyze, and accurately correlate data — without requiring manually written rules — across an organization's AWS, Azure, Google Cloud, and Kubernetes environments, and narrow it down to the handful of security events that matter. Security and DevOps teams around the world trust Lacework to secure cloud-native applications across the full lifecycle from code to cloud. Get started at http://www.lacework.com/.

CNAPP

Lacework® Special Edition

by Ed Tittel

for dummies®
A Wiley Brand

CNAPP For Dummies®, Lacework® 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.

ISBN 978-1-394-17131-6 (pbk); ISBN 978-1-394-17132-3 (ebk)

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.

Publisher's Acknowledgments

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

Development Editor: Rebecca Senninger

Acquisition Editor: Traci Martin

Editorial Manager: Rev Mengle

Business Development Representative: Molly Daugherty

Production Editor: Mohammed Zafar

Table of Contents

Introduction

In 2021, Gartner introduced a term that's taken the cloud security world by storm — cloud-native application protection platform (CNAPP). A CNAPP allows companies to take a more integrated and automated approach to cloud security by combining multiple functions in a single platform. For years, automation has played a critical role in cloud security. In fact, without automation, true cloud security would be a pipe dream. The promise of CNAPP goes a step further — one single platform that can bring value, safety, responsiveness, and productivity to organizations that put it to proper use. Too good to be true? Thereby hangs this book's riveting tale.

About This Book

Modern organizations depend so heavily on cloud computing that cloud security automation can only be described as "essential." Automation helps organizations see and assess cloud events that unfold in a fraction of a second. Plus, automation can correlate data across a customer's entire environment and find patterns — a task that would have previously taken hours or days.

Real automation requires communication across a cloud environment; because the cloud is so dynamic, what happens in one area of the cloud can have reverberating repercussions. But for years, cloud security "automation" has been fragmented, with point solutions only offering automation for specific tasks within the cloud. This patchwork web of point solutions has only made the cloud security landscape more difficult to traverse. Sitting between one point solution and another point solution is a security gap, waiting to be exploited.

Automation that makes the cloud viable, usable, and safe requires a consolidated security platform. As Ulfar Erlingsson, chief architect at Lacework, said, "The rush into the cloud — with its requirements for 24/7 uptime, elastic scalability, and continuous development — requires a new approach that allows security teams to become an enabling partner to DevOps, while continuously validating cloud configurations and activities."

This new approach is called CNAPP.

Foolish Assumptions

In writing this book, I have made certain, perhaps unwise, assumptions about you, gentle reader. First, I assume you know a bit about information technology (IT) practices. Second, I assume you also know something about cybersecurity and associated best practices, processes, and procedures. Third, I assume you understand the basics of cloud computing, to the extent of recognizing these terms: private cloud, public cloud, hybrid cloud, and multi-cloud.

Icons Used in This Book

Occasionally, special icons appear in the left margin. They call attention to important or noteworthy terms and topics. Here's what you find:

REMEMBER

This icon with the proverbial string around the finger points out information worth recalling.

TIP

This icon flags something useful or helpful by way of suggestion, advice, or observation.

WARNING

Warning icons pop up to steer you clear of potholes, money pits, and other dangers.

TECHNICAL STUFF

This icon offers two choices: Technophiles can zero in on upcoming details, while others can skip ahead to avoid them.

Beyond the Book

This book helps you learn more about cloud-native application protection platforms — especially their value and significance. Interested in using a CNAPP? Visit us at `lacework.com`.

IN THIS CHAPTER

- » Reviewing key cloud security challenges
- » Defining CNAPP and why it matters
- » Discussing the benefits of a platform approach

Chapter 1 Hello, CNAPP

Before tackling the ins and outs of a cloud-native application protection platform (CNAPP), it's a good idea to put cloud computing into context. This includes the rise of cloud computing, how the same elements driving its popularity make for a cloud security nightmare, and how CNAPP has come to the rescue.

How the Cloud Changed Everything

In *The Structure of Scientific Revolutions,* philosopher Thomas Kuhn explains a paradigm as a typical example of a pattern for something fundamental and important. According to Kuhn, a paradigm shift occurs when the dominant paradigm under which science operates becomes incompatible with new data, enabling the adoption of a new paradigm. For IT, the cloud is a paradigm shift because it offers an alternative to operating privately owned IT infrastructures in-house.

With the cloud, the IT landscape shifted. Costs grew and shrank with consumption. Buyers no longer needed to buy for peak demand, meaning that unused capacity and resources remained idle at non-peak times. Buyers could trade capital expenditures for operational expenditures. Because they don't require advance approval and budgeting, operational expenditures are typically financed via cashflow. They allow organizations to ramp up consumption during peak times, and then ramp down as peaks subside. The increased flexibility of these characteristics has made cloud computing insanely popular and created widespread demand.

Cloud Challenges: Complexity, Speed, and Scale

In the cloud, things can happen quickly. It takes minutes to spin up entirely new infrastructures or applications. Applications may manifest in a variety of cloud-based forms and can run in containers (such as Docker), on explicit virtual machines (such as Amazon EC2), or in serverless implementations (where the cloud provider allocates computing resources on demand, and takes care of server setup, provisioning, and management on the customer's behalf). It's not unusual for web-scale infrastructures to support thousands of server instances, ready to serve millions of simultaneous users (think Facebook).

Managing security in such a rapidly changing environment is tough. Clouds constantly shrink and expand. Cloud resources are ephemeral — spun up and phased out in the same day. And what happens on one side of the cloud could have far-reaching ramifications.

REMEMBER

Specific security challenges in cloud environments include:

- Integrating applications across multi-cloud or hybrid cloud environments so workloads can migrate freely across multiple clouds and containerized environments.
- Providing insight into actions, traffic, and application activity so organizations can observe and monitor behavior.
- Working with container orchestration, hypervisors, and cloud platform management tools (for serverless applications) to properly manage and secure multi-cloud environments.
- Providing a consolidated view of what's up across all runtime and build-time environments so that resource consumption, compliance, and security monitoring work consistently and coherently.

CNAPP: A history

The automation offered by a CNAPP provides a toolkit to keep things running safely in the cloud, even in the face of incessant change. Before I dive into how a CNAPP solves for these issues, I should take a step back and discuss the factors that led to the conception of this term.

For many businesses, COVID-19 accelerated "digital transformation" initiatives. To help facilitate the shift towards digital business, companies embraced cloud-native application development through microservices-based architectures, containers, DevOps-style pipelines, container orchestration programs such as Kubernetes, and more. The benefits to this approach were obvious: Companies, decentralized from a global pandemic, could now innovate and deploy software at an unprecedented pace and scale. However, providing security over large and ephemeral cloud environments proved extremely challenging.

Companies learned that integrating security into the application development lifecycle was the key to securing the cloud without sacrificing its primary benefit — speed. This gave birth to a new application development philosophy, DevSecOps, which sought to merge security and application development into one seamless process.

In theory, DevSecOps was the silver bullet for securing cloud application development. However, in practice, it often made things more complicated. The vendor landscape became extremely fragmented. Rather than having one single solution that would secure all areas of cloud application development, each tool handled one single function. Companies ended up with ten or more disparate cloud security tools with siloed responsibilities, loosely integrated with one another. This approach was unsustainable and not ideal for dynamic cloud environments that could scale up or down on demand.

Then, in 2021, Gartner coined the term "cloud-native application protection platform," or "CNAPP," and explained how this type of approach was necessary to provide long-lasting cloud security. In its report, Gartner explains how CNAPP aims to bring all these disparate cloud security tools and functions into one single, well-integrated platform.

A CNAPP and its benefits

This new category is the combination of several existing categories such as cloud security posture management (CSPM), cloud workload protection platforms (CWPP), cloud infrastructure entitlement management (CIEM), and "shift left" security capabilities including Infrastructure as Code (IaC) security and code vulnerability scanning. This book explores each of these categories in further detail.

A proper CNAPP protects cloud application development throughout the entirety of the application development lifecycle — from build time through runtime. During build time, a CNAPP offers IaC scanning and vulnerability scanning through integration with continuous integration (CI) and continuous deployment (CD) pipelines. Once an application is deployed, a CNAPP provides runtime security, including continuous threat monitoring and runtime vulnerability scanning. A CNAPP can also scan cloud environments for misconfigurations, manage identities and permissions, automate compliance, and more.

REMEMBER

The advantages and benefits of a CNAPP include at least the following elements:

- **Simplified approach:** A single console covers all clouds, and a single tool handles vulnerabilities, remediation, compliance, and reporting.
- **Continuous visibility (not just snapshots):** Because a CNAPP is cloud-native and cloud-aware, it provides complete and unceasing visibility for events and activities, including within whatever cloud platforms may be involved in an organization's processing environment.
- **Machine learning:** A CNAPP uses ML to identify and label behaviors, establish baselines, recognize new events or activities, and identify anomalies.
- **Fewer, more accurate alerts:** Because it can put activities and events into context, a CNAPP issues alerts only when something genuinely new or recognizably malicious occurs. The organization's IT and security teams can focus their efforts where they can do the most good.

TIP

A low alert noise means your team only needs to look at what's important or noteworthy. Your team no longer has to spend time chasing false positives or noisy alerts, which helps prevent alert fatigue.

- **Tool consolidation:** One consolidated cloud security platform can replace up to 9 point solutions (average number: 5). For consistency, compliance, and peace of mind, it's difficult to overstate the value of a single, comprehensive view of security across all cloud and local IT environments.
- **Power, speed, and scalability of automation:** Automation is the key to a CNAPP's value — automation in how the platform is deployed, how it ingests data across the entire cloud environment, how it analyzes and correlates that data, and how it delivers these insights directly into existing security, developer, and operations workflows.

Future-ready with a Platform Approach

A CNAPP delivers comprehensive cloud security, especially for the hybrid and multi-cloud scenarios typical in modern businesses. But a cloud security platform also addresses macroeconomic trends to which all mature, responsible companies must eventually respond. These include the following indisputable trends across all industries and sectors:

- Accelerated business operations, as businesses look to do more for their employees, clients, customers, and partners increasingly quickly.
- Ever-growing pace of change, as new tools, technologies, and software development approaches reign supreme (DevSecOps, not DevOps).
- A real-time approach to security and compliance, which means that organizations must respond to changing conditions, as well as a complex legal and regulatory landscape, with progressively dangerous and expensive threats and vulnerabilities to fend off. Risk management can't slow things down.

The platform approach considers cloud security from end to end and uses automation to keep up with the pace of change and the scope and scale that come with wholesale cloud adoption and use.

A CNAPP is also inherently flexible, able to accommodate any company's need regardless of cloud maturity level. For companies that are just starting work in the cloud, a CNAPP can provide frictionless visibility via agentless means. However, for those that are more cloud-mature or may be migrating existing workloads to the cloud, companies can adopt a CNAPP starting with agent-based runtime workload monitoring. A CNAPP offers full cloud protection, but how companies get from point A to point B is in their own hands.

Problems with point solutions

A *point solution* is a focused management, monitoring, or reporting tool for cloud applications or platforms that is narrow in scope. It typically deals with only one kind of cloud platform, usually public but sometimes private, or on a focused use case such as compliance or vulnerability management. Given organizations' tendencies to adopt hybrid and multi-cloud strategies, this often means more such tools are in use, rather than fewer such tools.

WARNING

Unfortunately, a plethora of tools brings interesting challenges to the organizations who own them, and the IT and security pros who must put them to work:

- **Ironically, more tools often means more security gaps.** Not all views of security are the same, so an unfortunate side effect of tool proliferation is that more blind spots result from gaps in coverage and from differences in perspective on how security is audited, tracked, managed, reported, and so forth.
- **More tools means more licensing fees, more maintenance and upgrade charges, and a bigger learning curve.** Point solutions aren't cheap, and the price tag for cloud security only gets larger with each additional acquired security tool. Each tool also requires its own user enablement, which adds to cost.

- **Each point solution also imposes drag on its owners from an operational perspective.** Staffers must spend time integrating any tool into their dashboards and desktops. Those tools need regular maintenance, as do all software components. Then there's the effort involved in understanding, writing, and maintaining rules to make such tools work. Each tool also has its own unique user interface and commands, which its operators must know how to use. It all adds up!
- **Point security tools are typically not optimized for cloud platforms.** Many point security tools are founded in legacy approaches that are not built for the cloud. These types of rules-based approaches may be fine for managing access and network traffic, but they don't work well for handling threat detection, remediation, compliance requirements, and other activities that a proper CNAPP handles routinely.

Product portfolios: A cautionary tale

In late 2021, Gartner released a report titled *Predicts 2022: Consolidated Security Platforms Are the Future*, speaking to the trend of tool consolidation across the cybersecurity landscape.

In the research, Gartner calls out a "portfolio approach that should be carefully evaluated." According to Gartner, "vendors are increasingly divided into 'platform' and 'portfolio' camps, with the former integrating tools to make a whole greater than the sum of its parts, and the latter packaging products with little integration." According to Gartner, "differentiating between these approaches is key to the efficiency of the suite, and vendor marketing will *always* say they are a platform."

So, when it comes to CNAPP, carefully evaluate vendors. Make sure they're delivering on the promise of tool consolidation!

IN THIS CHAPTER

- **Establishing full cloud visibility**
- **Exploring benefits of agents and agentless**
- **Gaining visibility from CNAPP**

Chapter 2
Visibility: See More with a CNAPP

Events and activities inside a cloud environment are often hard to see and understand from outside that environment. Nevertheless, companies and organizations operate according to a shared responsibility model for cloud security, placing the onus of data security on their shoulders, as opposed to the cloud service providers themselves. Thus, they must do what they can, and use proper tools, to shine some light on what's happening inside the cloud with their data and applications, particularly from a security perspective.

A key value of CNAPP adoption is gaining end to end visibility into a cloud environment — from application development through application runtime. Read on for more details.

Defining Cloud Visibility

In brief, full cloud visibility means that security information, including logs and monitoring data, is available and transparent, whether it comes from a public or private cloud platform. This could also extend to on-premises systems and services.

For all applications, and all data, full visibility means admins and the security team can inspect identity and access management systems and data, including use of privilege and multi-factor authentication, as well as password requirements. It also means they can check on logging practices to make sure that it's enabled in all circumstances, and that log files are validated, encrypted, and monitored. Finally, it means staff can track critical account activity, use of management console and privileges, and more. They should also be able to monitor unauthorized API calls, and detect and react to vulnerabilities and anomalies.

Full visibility also allows for detailed data analysis of the applications, data, users, traffic, usage, and behavior involved in complex hybrid and multi-cloud systems. That means security tools can employ artificial intelligence (AI) and machine learning (ML; together, AI/ML) to elicit insights and observe patterns, both benign and malignant, based on ongoing behavior within applications, and the ways in which they produce and consume data.

REMEMBER

Knowing and understanding what you see is vital in any or all cloud platforms in use. While visibility is good, it's even more critical to establish context and ensure that security requirements are met.

Four CNAPP Characteristics Essential to Visibility

A CNAPP offers cloud security from end to end. The platform satisfies four characteristics that are essential for any cloud security solution to provide the necessary visibility into what's going on inside operating cloud environments. These characteristics include:

- **Cloud-native and API-driven:** The cloud security solution is written to run in cloud-based environments as part of, or alongside, the organization's own cloud-based applications and services. When a proper security solution runs in the cloud, it uses application programming interfaces (APIs) that work directly and seamlessly within that cloud environment.
- **Hybrid/multi-cloud:** This means a cloud security solution can run across multiple clouds, both private and public (and remember, private clouds can operate inside an organization's own data centers or edge computing sites).

- **Minimal footprint, minimal performance impact:** Cloud-based computing focuses heavily on cost optimization and controls. Thus, security monitoring and management capabilities can neither consume appreciable cloud-based resources nor should they noticeably impact performance of applications and services for which they provide visibility and event responses.
- **Full understanding of cloud context, behavior, and traffic:** Managing security is about detecting threats and averting exploits, but it's also about understanding actors at work, which actions are normal (or not), and where and how traffic flows within and across cloud boundaries. Visibility is key to illuminating cloud context, and distinguishing accepted actors and actions from anomalies.

Why Is Cloud Visibility Important?

Boundaries change or disappear in the cloud as workloads move around and application servers interact with back-end servers for storage, database access, and other things. It's always important to observe and inspect what's flowing across network boundaries (at the data center or the edge, and into and out of one or more clouds, public or private). Full visibility clearly shows which actors are present, what kinds of access they've requested, and which operations are involved. As boundaries shift, it's crucial to look for reconnaissance and signs of impending or active attack.

But full visibility also involves seeing what happens inside any cloud environment, too. Consider answering questions about what's up in the cloud:

- What kinds of application operations are normal or typical?
- How does data move from back-end servers or services into and out of applications?
- Is data that applications use encrypted in storage? In transit? In use in the application itself?
- What sensitive, private, or confidential data do applications use? Does it comply with security policies, regulations, and best practices?

REMEMBER

What goes on with data and applications varies for each different environment in use, particularly when multi-cloud platforms are involved. Some or all of the following considerations may apply:

- **Multi-cloud considerations:** As workloads (applications and their data) move between clouds, answering the preceding questions can help situate the workloads safely. Also, when it comes to workloads in the cloud — particularly those that use proprietary, sensitive, or private data — security should be a top priority.
- **Container considerations:** Container environments can include Docker, package applications, supporting code, and data within unique and distinct runtime environments. Tools and monitoring capabilities may differ; cloud-native details certainly will. Organizations must understand the context in which applications and their data run in containers. And again, they must situate them to comply with applicable policy, regulations, and so forth.
- **Kubernetes considerations:** Kubernetes (K8s) uses a different approach to provisioning, orchestrating, and running applications and their data in the cloud. Organizations must obtain comprehensive, continuous end-to-end security and configuration support for K8s workloads running in all cloud environments.

AGENTLESS VERSUS AGENT-BASED MONITORING

TECHNICAL STUFF

An agent is a small program whose job is to take up residence within or alongside a system or application, and report observations to a third party (usually across a network). Agents usually function as add-ons to existing applications, though they may run as part of the application itself.

Cloud monitoring can be agent-driven or agentless. If the former, it relies on a local agent to collect and send monitoring data to a third party (usually a security management tool). If the latter, it requires that the application itself do the collecting and reporting. A CNAPP accomplishes full end to end cloud visibility by employing both approaches.

Through agentless monitoring, organizations can take snapshots of their environments to uncover misconfigurations and vulnerabilities and monitor activity in cloud accounts for compromise. Agents, however, are built to provide the right information to deal with matters that can be of great import and urgency. When appropriately placed and thoughtfully implemented, agents are the most effective way to generate the context and visibility needed to handle sophisticated cyberattacks, especially during application runtime.

Modern software agents are specifically created for cloud deployment. As opposed to legacy agents, they impose a tiny footprint, and consume only minimal computing, storage, and network resources. They use standard, well-defined but compact ways of representing and communicating security information. They can perform tasks without any source intervention, but they can also interact with other agents as needed. Such agents take data safety and integrity as their most important charge and are careful in handling unauthorized users.

An analogy: CNAPP as home security

When it comes to gaining full cloud visibility, you will inevitably come across a debate as old as time: to use agents or not to use agents. (See the nearby sidebar if you're still debating.) Indeed, many vendors today claim to offer fully agentless solutions that can achieve the promise of CNAPP. However, if full cloud visibility is the goal, companies should have an agentless wide-angle shot of your cloud and an agent-based granular interior view of your cloud — and should be able to correlate the two functions together.

Consider this analogy. There is merit to having a security guard circling your house. The security guard gets an outside-in view of your home's state of affairs. They can see that all doors are closed, that all windows are shut. Or, on the other hand, they could observe that a window has been broken since the last time they circled the house. They could see a door ajar. And they could infer that there is an intruder in the home — or that, if there isn't an intruder yet in the house, an intrusion is impending.

But, for many, that's where the story ends. Agentless cloud security posture management without runtime monitoring — or seeing what's actually happening in your cloud environment — can only provide recurring snapshots of the state of your cloud. Without runtime monitoring, one can't confirm an intruder is actually in the home, what exactly they did in the home, the extent of that intruder's damage, and how to isolate and extract the intruder from the premises.

On the other hand, enacting cloud runtime monitoring is like installing security cameras on the inside of your home. You can see everything that's happening in your cloud environment at any given time. And unlike the security guard taking a wide route around the outside of your home, the cameras inside of your house are continuously running, incessantly capturing every angle of its interior.

That said, the perspective of the security camera isn't the perspective of the security guard. Both have their merits. And for full home security, having both is ideal. The same is true of cloud security.

Benefits of full cloud visibility

Full visibility offers a trove of information and insight. It provides both monitoring capability and the insights necessary to act on observations and detection. Beyond those basic characteristics, full visibility grants organizations other potent benefits, including:

- **Learning from experience:** As organizations work with what they learn from full visibility, they develop a more nuanced and informed understanding of baseline behavior, activity, traffic patterns, and consumption. This presents an opportunity to improve performance and service delivery via tuning and optimization.
- **Paying attention to what's important:** Large, complex systems generate lots of monitoring and logging data. Time, experience, and an understanding of how the overall threat landscape relates to the organization's vulnerabilities and exposures lets IT and security staff members focus on high priority threats and exposures.
- **Putting behaviors into context:** It's hard to understand whether a sudden series of file copies is an attempt at data exfiltration or simply a routine backup. Knowing that the application involved is a scheduled backup job immediately resolves any concerns.

REMEMBER

The ability to see and understand ongoing behavior in context is what gives full visibility its real value — especially on otherwise opaque cloud platforms — and lets staff zero in on genuine causes for alarm or alert.

IN THIS CHAPTER

- » Managing your cloud security posture
- » Securing cloud infrastructure
- » Managing identities and vulnerabilities

Chapter 3 Managing Cloud Risks with a CNAPP

When it comes to security management, it's far too easy to get lost in the weeds. This is especially true when seeking to secure applications in the cloud. Inevitably, the dynamic nature of containerized and cloud environments creates blind spots and security gaps, which too often result in inconsistencies, misconfigurations, and key elements that lack visibility and transparency.

Full threat prevention via risk mitigation is a pipe dream. But that doesn't mean that 100 percent threat prevention shouldn't be the goal. Organizations with modern infrastructures need the ability to identify and fix vulnerabilities in the most cost-effective stage of cloud application development — build time. But organizations can't neglect vulnerability scanning in production, as cloud configuration changes can surface new risks across cloud environments.

Companies also need a well-integrated, consolidated cloud security platform to ensure a strong cloud security posture. An effective security posture in the cloud era requires understanding new threat vectors and the ability to detect unusual activity and account compromise, as well as misconfigurations.

Yet again, a CNAPP is here to save the day.

Managing Cloud Security Posture

Gartner defines cloud security posture management (CSPM) as "a continuous process of cloud security improvement and adaptation to reduce the likelihood of a successful attack." CSPM tools help automate security, uncover risk, and prove compliance in the cloud. To do their jobs, CSPM tools examine and compare cloud environments against a well-defined set of best practices and known security risks.

Cloud-first organizations use CSPM tools to extend security best practices into hybrid cloud and multi-cloud environments. Such tools are good at finding and eliminating configuration mistakes and reducing compliance risks. While CSPM is tied to Infrastructure as a Service (IaaS) cloud environments, it works with Software as a Service (SaaS) and Platform as a Service (PaaS), too.

REMEMBER

Key capabilities found in most CSPM tools include:

- Detecting and, where appropriate, automatically remediating cloud misconfigurations
- Building and managing a collection of best practices for various cloud configurations and services
- Mapping current configuration status to security control framework or regulatory standard
- Scanning and managing SaaS, PaaS, and IaaS platforms in containerized, hybrid, and multi-cloud environments
- Monitoring storage repositories, account permissions (and their use), and encryption for compliance issues and misconfigurations

Implementing CSPM is a challenging task, but given the proper tools, it provides an understanding of a cloud environment that helps organizations monitor their cloud resources, reduce risk, and prove compliance. Likewise, CSPM provides the means and mechanisms to ingest and filter security intelligence feeds, identify potential vulnerabilities and exploits, set priorities, and seek out items in need of response and remediation.

Managing Cloud Infrastructure

A proper CNAPP should include Infrastructure as Code (IaC) scanning. Infrastructure as Code (IaC), or the automated provisioning of cloud infrastructure, is often described as a set of "blueprints" that define your cloud infrastructure. With IaC, developers can automate the provisioning of cloud infrastructure via written code.

IaC enables faster innovation but increases the chance of misconfiguration mistakes. With the scale of IaC, even a single misconfiguration can propagate across hundreds of deployments. This can result in time-intensive and costly remediation in build time.

This is where IaC security comes in. IaC security solutions scan IaC builds for misconfigurations and compliance violations and offer steps for remediation. With this type of solution, security teams can avoid having to spend time on IaC issues outside of their expertise, and development teams can reduce expensive build time remediation costs.

Managing Cloud Identities

The cloud has fundamentally changed the understanding of certain concrete IT and security concepts. The concept of *identity* is a real-world example of this phenomenon.

In short, there's a lot happening in the cloud at any given time. There are many different cloud identities that need access to many different cloud data sets to accomplish their assigned purposes. In the past, these identities would have been human users and groups, but this is no longer the case. Within the cloud, users and groups aren't the only ones that need data to do their jobs; various non-human services and resources also request access to certain cloud data sets on a routine basis.

And thus begins a tangled web of permission and privileges. Who (or what) needs what, where, and when? And it's not enough to simply open the floodgates and allow everyone access to everything. That approach is a major security risk and is, quite frankly, one that many companies have succumbed to out of pure exhaustion.

REMEMBER

The *principle of least privilege* is the tenet of giving a user or resource only the permissions it needs to accomplish a specific task. Without automation, implementing this principle in a complex cloud environment is virtually impossible. Individual cloud providers — AWS, Google Cloud, and Azure — do this relatively well, but their jurisdiction is limited to their specific cloud environments. The challenge is accomplishing this at scale, across multiple clouds and hybrid clouds.

Hence, the advent of cloud infrastructure entitlement management (CIEM). CIEM solutions seek to both identify unusual identity behavior and manage policies around users, groups, and privileges, even in complex multi-cloud and hybrid cloud environments. These solutions expand the idea of identity and access management (IAM) — which has typically been used to refer to humans — to also include non-human resources and services within the cloud. CIEM solutions also ensure that the right people (or resources) have the right permissions at the right time — and that these permission structures stay intact, even as cloud environments grow or shrink.

Managing Vulnerabilities

Traditional security tools do not scale for modern companies that build and deploy application code at a high velocity. A different security strategy is critical for security to be seen as an enabler of innovation, rather than a detractor.

TIP

The key to managing vulnerabilities at the speed of cloud development is to shift security practices "left."

Shift left security

Shift left security is the practice of integrating security checks early and often into the cloud application development lifecycle. By shifting security left, companies realize the benefits of a DevSecOps approach and are able to develop and ship code safely and securely.

A proper CNAPP enables companies to ship security left by offering various build time security features, such as public and private container image registry cloud scanning and inline CI/CD scanning. As a last line of defense, a CNAPP may offer fail-safe deployment protection such as admission controllers that can stop the deployment of code that doesn't meet certain criteria.

TECHNICAL STUFF

Shift left security would also include modern code security tooling and may be included in a CNAPP. This rising category of application security solutions includes application security testing (AST) tools such as static AST (SAST) and dynamic AST (DAST). SAST analyzes an application's source code for vulnerabilities during programming, while DAST examines this same application code by testing it in its running state. DAST also involves simulating attacks against the code itself and observing its response, further testing its vulnerability.

Security composition analysis (SCA) is also considered an integral part of modern code security, as is a software bill of materials (SBOM). While the percentages differ between studies, most research suggests that an overwhelming majority of companies today use open source software. SCA and SBOM are ways of ensuring that application code is fully free of vulnerabilities, including any open-source code or third-party components. Through SCA products, companies can scan for vulnerabilities, check that all application components are properly licensed, and ensure that the entire software supply chain can be trusted.

In many ways, SBOM is the output of SCA. According to Gartner, an SBOM is a collection of "structured, machine-readable metadata that uniquely identifies a software package and the open source or proprietary components used to build it." The goal here is transparency and traceability. If an issue is discovered in an open source code package, it's quickly identified and communicated through more open collaboration.

Attack path analysis

Vulnerability management doesn't end once build time ends. The dynamic nature of the cloud demands continually monitoring for new risks and vulnerabilities that arise once code has been deployed.

TIP

Vulnerability management can be significantly elevated by using runtime data to its advantage. Runtime data provides critical information and insights into what's actually happening in production, which can highlight the vulnerabilities that are most critical to fix in a long list of findings.

A novel approach that some CNAPPs are taking here is something called *attack path analysis*, where the platform pinpoints a number of risks actively present in a cloud environment, then ties these together to understand how an intruder could carry out an attack. The platform then ranks the biggest risks and exposures, based on those connected in the attack path.

For example, an attack path could display an overprivileged user who has access to a resource that is misconfigured, which is connected to a vulnerable host. Security teams could then work to fix one (or all) of the elements of that attack path to prevent a breach from occurring.

At the end of the day, cloud data sits at the core of a CNAPP. And if a CNAPP is ingesting an ample amount of data from across a cloud environment and has the "brain" to make sense of it all, attack path analysis is merely one example of many where that data could be correlated and displayed creatively to promote safety across a cloud environment.

IN THIS CHAPTER

- **Understanding protection platforms and their benefits**
- **Exploring why legacy models are passé**
- **Solving container security woes**

Chapter 4 Pinpointing Cloud Threats with a CNAPP

Vulnerability management and maintaining an airtight cloud security posture are nonnegotiables for modern companies operating in the cloud. However, even the best risk defense can't guarantee 100 percent protection against bad actors. When the breaches happen, another critical facet of CNAPP comes into play — runtime workload protection. This layer of protection is further bolstered by new technologies such as behavioral analytics and anomaly detection, which allow companies to protect against all threats — both known and unknown.

The Cloud Workload Protection Platform (CWPP)

For modern cloud-first or cloud-forward infrastructures, cloud workload protection platforms (CWPPs) offer an important innovation in cloud security and automation. Gartner defines CWPP as a "workload-centric security solution that targets the unique protection requirements" of workloads in cloud-based and other modern enterprise environments. Unlike traditional security tools, cloud workload protection seeks to secure and protect workloads regardless of type, host platform, or location.

A true CWPP should continuously monitor and secure all cloud workloads — cloud hosts, containers, K8s, and PaaS environments. A true CWPP must be Linux-aware and support Linux-based physical and virtual servers, along with vendor-specific enterprise Linux platforms such as Red Hat, SuSE, and so forth. Windows support is becoming increasingly important as well, because organizations that used on-premises Windows environments are now moving to the cloud.

Applications built on public cloud infrastructures are complex and dynamic. Securing cloud workloads at cloud scale and speed can't depend on manual intervention and point solutions. Thus, a CWPP must accommodate cloud workloads at scale, and automate the process of incorporating new cloud services and technologies.

Lastly, a proper CWPP must run natively in the cloud, so it can provide continuous build to runtime threat detection, ongoing behavioral anomaly detection, and misconfiguration and compliance checks.

REMEMBER

This continuous threat monitoring is only possible through a combination of agentless and agent-based approaches (see Chapter 2).

Rules Optional with a CNAPP

A proper CNAPP is fully automated, with limited rules to write or maintain. Using machine learning, such a platform learns what behaviors are normal and expected and what kinds of behaviors could indicate potentially malicious activity. Such an approach takes the threat detection capabilities of a CWPP to new heights.

In the past, security management tools often relied on sets of rules to do their jobs. As with intrusion detection or intrusion prevention systems (IDS and IPS, respectively), incoming packets are subject to a series of rule checks to determine whether request or response traffic should be allowed or denied access to networks and systems under their control. Often, there's considerable time and effort involved in configuring such platforms, and then in writing rules specific to the organization's environment.

Today, thanks to innovations in AI/ML, security tools can use learned or derived understandings of behaviors to look for anomalies. As they appear, such anomalies can be logged and reported, and might even provoke automated responses to fend off or stymie unwanted access or outright attacks.

Here are some examples of anomalous activities:

- A user launches a new binary.
- A process transfers data for the first time.
- An application connects to a suspicious or blacklisted endpoint.

A proper protection platform recognizes these activities as anomalies and causes it to generate a contextual alert. This alert contains sufficient relevant data to permit security or IT staff to investigate and handle such issues within the organization's cloud workload environment.

Behavior beats rules

Rules must be formulated in advance, based on existing understandings of patterns and traffic indicative of reconnaissance or attack. It is by no means a quick process, and requires constant tuning, checking, and adjustment as the threat landscape changes and evolves.

Conversely, anomaly detection is based on observed, actual behavior. Anomaly detection works by establishing and labeling a large collection of normal and benign behaviors, based in part on where they come from, what actions they take, and how frequently they occur. This effort relies on AI/ML, with only modest needs for human interaction and filtering to build and maintain a baseline. And when behaviors fall outside the baseline, they're automatically suspect and are surfaced, along with sufficient contextual information to determine whether they're of concern.

This sort of behavior-based approach can accommodate the kinds of changes that cloud environments typically experience — namely, instantiation of new VMs, containers, applications, and services; entry/exit of user accounts; workload migration; data warehousing and enrichment; and so forth.

Key advantages of a behavior-based approach

TIP

Understanding behavior buys considerable advantages for security management and control. These include:

- **Efficiencies gained:** Security staff can hone in on anomalies of real and direct concern. This saves the time and effort of chasing false positives, and permits rapid response to high-priority, high-risk events and incidents.
- **Cost savings:** Because IT and security staff don't need to write rules — or climb the associated training, learning, testing, and maintenance curves involved in using them — they save on time and effort. Effort can then be directed where it does the most good: responding to and remediating real security concerns.

By focusing on behavior, you can ignore irrelevant physical details. For example, VMs or processes could die or be restarted, or an A-B failover might occur in switching from a primary to a secondary site. None of these things causes real changes in application behavior and usage patterns. A behavior-based understanding of ongoing activity quickly and efficiently separates and flags anomalies, which is exactly what's needed for a full and clear picture of your cloud environment.

Container Security and Compliance

Containers are emerging as the go-to method for streamlining and speeding software development for all kinds of organizations. Thus, container security and compliance strategies must support adoption plans for speedy development that maintains and enforces proper, effective security.

Because containers facilitate rapid development of microservices-based architectures, development teams can modularize and scale applications at will. This speeds every aspect involved in development, such as coding, building and delivering releases, pushing updates, and constant improvement and innovation.

Containers run in agile environments, so applications can execute across a range of infrastructures and runtime environments. Containers are inherently adaptable to changing business needs and technologies, so they're extremely well suited to digitally focused organizations.

REMEMBER

The real key to maintaining speedy development and release cadences is to balance container advantages against their security risks. This means organizations must insist on monitoring integrations, user access, compliance, and relevant threat intelligence. A proper CWPP delivers the foundation for container security and compliance where players follow certain key principles for container security management:

- **Reducing container attack surfaces:** Use continuous, real-time data about container activity to reduce the attack surface and to detect malware, bad code, and security gaps.
- **Ensuring that images come from trusted sources:** Container applications derive from images tied to executable code from a specific kernel instance. Images should only come from trusted sources, and be signed by authorized users.
- **Establishing continuous configuration assessment and analysis:** Because of the change and complexity within container environments, only continuous vulnerability and compliance assessments and remediation can keep up. Misconfigurations are a particular concern.
- **Extending vulnerability detection efforts:** Detection should identify vulnerabilities in the host OS, application language libraries, container images, and in containers themselves, using real-time analytical data across the entire infrastructure. Vulnerability scanning should be integrated across the CI/CD pipeline as well as production environments.
- **Rigorously imposing least privilege:** The principle of least privilege is a cornerstone of effective security regimes. Check and match all access to containers accordingly, and audit and review use of root and superuser access.

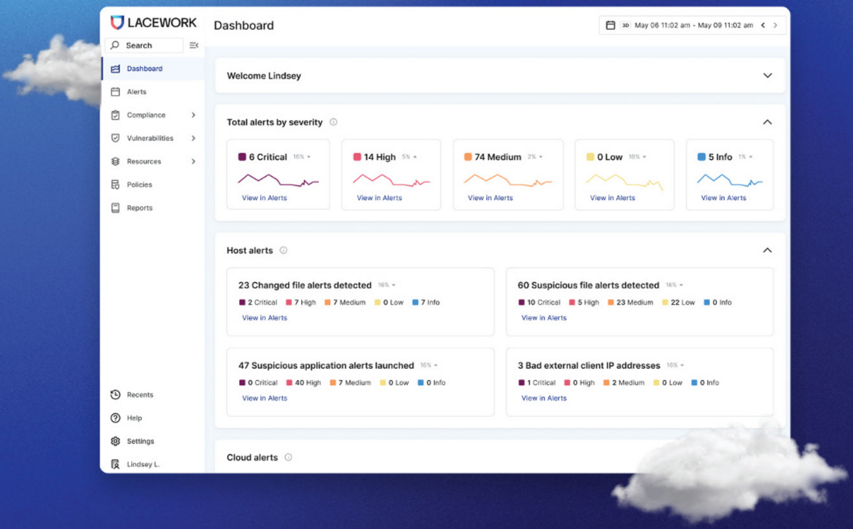
Coupling containerized applications deployed in the cloud with anomaly analysis and security best practices creates the necessary threat detection, protection, and response controls to keep dynamic clouds safe and secure.

Chapter 5
Ten Benefits That Justify a CNAPP Investment

Simply put, without automation there would be no cloud. And, with CNAPP, companies can finally benefit from end to end, automated cloud security in a single platform. A proper CNAPP offers a handful of vital benefits including:

- **Scalability:** A proper CNAPP grows or shrinks with your cloud environment, whether you're working in a single cloud, multi-cloud, or hybrid cloud. Total scalability.
- **Improved visibility:** From outside the cloud, it's often difficult (or impossible) to tell what's really going on in terms of data motion, access, activity, and manipulation. Through a combination of compact, cloud-native software agents and agentless methods, a proper CNAPP provides all the gory details, making them visible and documented.
- **Saved time and money:** A key benefit of a CNAPP is tool consolidation. By meeting the functions of multiple point solutions in one platform, a CNAPP means fewer licenses to renew, fewer trainings to attend, and more time to focus on work that matters.

- **Simplified approach:** Since its baseline uses empirical observation and analysis, a proper CNAPP is easy to use and work with.
- **Context-driven understanding:** Through machine learning, a CNAPP provides information and alerts, along with all the data that staff need to investigate and triage whatever's going on. Furthermore, such a platform also uses machine learning to ingest, label, and identify cloud behaviors and activities, completely informed by context.
- **Accurate alerts:** A CNAPP uses context to establish a baseline for behavior, so it knows precisely what's normal, expected, and routine. Better yet, that means it also knows what's new and different, and possibly malignant. That's how it generates alerts.
- **Better team collaboration:** By tying security insights directly into DevOps workflows, developers can find and fix issues earlier in the development cycle, while security teams can stay ahead of security threats.
- **Security and speed:** Traditional approaches placed security and development speed at odds. By integrating security into the development process, this is no longer the case. With CNAPP, you can have your cake and eat it too.
- **Behavioral anomaly detection:** A CNAPP uses machine learning to ingest, label, and identify cloud behaviors. It knows when behaviors are new and different, and flags them for investigation.
- **Flexible deployment:** A CNAPP is a one-stop shop for all cloud security needs, regardless of cloud maturity. This means that companies can deploy CNAPP functionality at their own pace — whether that means rolling out all features on day one or spreading them out over time.



Dashboard

3D May 06 11:02 am - May 09 11:02 am

Welcome Lindsey

Total alerts by severity

6 Critical 16%	14 High 5%	74 Medium 2%	0 Low 16%	5 Info 1%
View in Alerts	View in Alerts	View in Alerts	View in Alerts	View in Alerts

Host alerts

23 Changed file alerts detected 16%
2 Critical 7 High 7 Medium 0 Low 7 Info
View in Alerts

60 Suspicious file alerts detected 16%
10 Critical 5 High 23 Medium 22 Low 0 Info
View in Alerts

47 Suspicious application alerts launched 16%
0 Critical 40 High 7 Medium 0 Low 0 Info
View in Alerts

3 Bad external client IP addresses 16%
1 Critical 0 High 2 Medium 0 Low 0 Info
View in Alerts

Cloud alerts

Secure from code to cloud

Lacework is the leading data-driven cloud-native application protection platform (CNAPP).

CSPM ✓ IaC ✓ CWPP ✓ K8s ✓ CIEM ✓

Get started at **Lacework.com**

LACEWORK

The future of cloud security is a platform

In late 2021, analysts coined a term that's rocked the cloud security world — cloud-native application protection platform (CNAPP). For years, cloud security was siloed, unscalable, and inefficient. A CNAPP promises something different — an integrated and automated approach by combining multiple functions in a single platform. With *CNAPP For Dummies*, Lacework Special Edition, learn about how the CNAPP came to be, how a CNAPP is the perfect match for the cloud, and why a CNAPP is worth your time and investment.

Inside…

- A brief history of CNAPP
- An overview of CNAPP benefits
- Why platform is right for the cloud
- How CNAPP offers full cloud visibility
- A discussion of CSPM, CWPP, CIEM, and more
- An alternative to rules-based security

LACEWORK

Ed Tittel is a computing writer who's worked as a programmer, a trainer, and a technical evangelist. Ed has contributed to over 100 computing books, and writes regularly for Tom's Hardware and ComputerWorld.

ISBN: 978-1-394-17131-6
Not For Resale

9 781394 171316

for dummies®
A Wiley Brand