upwind

CNAPP TL;DR

End-to-End Cloud Infrastructure & App Security in 8 Steps

(Because CNAPP doesn't have to be so complicated)

Table of Contents

01

Stop Using So Many Tools.

Gartner says CNAPP is a unified and tightly integrated set of security and compliance capabilities designed to secure and protect cloud-native applications across development and production.

CNAPPs consolidate a large number of previously siloed capabilities, including container scanning, cloud security posture management, infrastructure as code scanning, cloud infrastructure entitlement management, runtime cloud workload protection and runtime vulnerability/configuration scanning.

THE RISE OF CNAPP
ACCORDING TO GARTNER

2015
Gartner predicts that 95% of cloud security failures will be the customers fault by 2020, launching a rush for customer cloud security tool purchases

2016
CWPP & EDR solutions are named among the most essential cloud security tools

2019
Compliance becomes a major focus for cloud security, launching the growth of CSPM

2022
Enterprises have an average of 10 cloud-native security tools.

2023
45% of breaches are cloud-based, with increasing numbers of organizations reporting cloud security incidents

2024
Security teams see a trend of decreased security budgets, sparking tool consolidation efforts

2025
75% of new CSPM purchases will be part of an integrated CNAPP offering (Gartner)

2026
80% of enterprises will have consolidated security tooling for the life cycle protection of cloud-native applications to 3 or fewer vendors (Gartner)

02

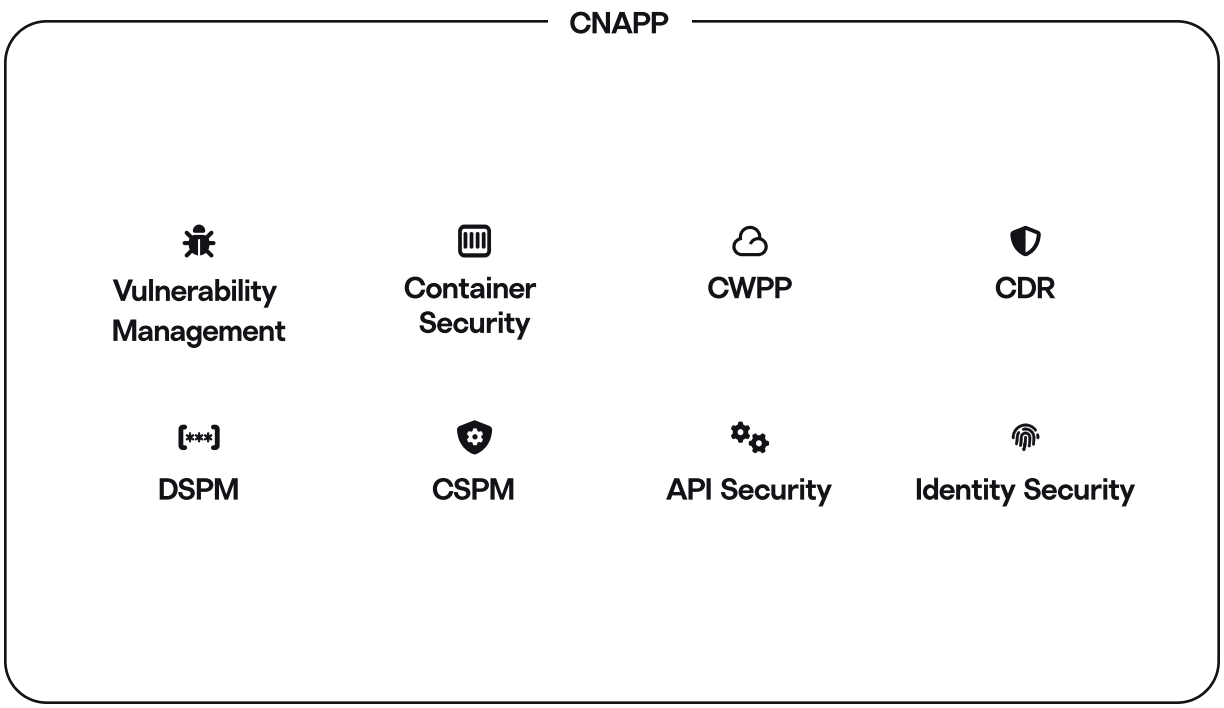
Do More with Less.

Why CNAPP?

Using multiple tools is expensive and creates excessive noise.

Because many security categories overlap, too many tools can create confusion and an overwhelming amount of alerts. It also makes it difficult for organizations to successfully integrate multiple tools, leading to siloed data and a lack of unified context.

In contrast, CNAPP eliminates redundant alert noise and provides unified, contextualized data, eliminating the need for multiple tools.



Cloud security can be broken up into three pillars: posture & vulnerability management, workload protection and application and identity security.

CNAPP combines these pillars into one unified view of your infrastructure and applications across clouds, giving you full visibility of the entire application lifecycle from build time to deployment to runtime.

By leveraging runtime to build time context and layering each of these parts together, you create unified risk visibility across the entire application lifecycle. Cloud security is dynamic, and you need unified, dynamic context to ensure you are secure.

03

Stop Relying on Old Data.

Beyond needing a unified view of your cloud infrastructure and applications, you also need to know what is happening in your environment, when it's happening.

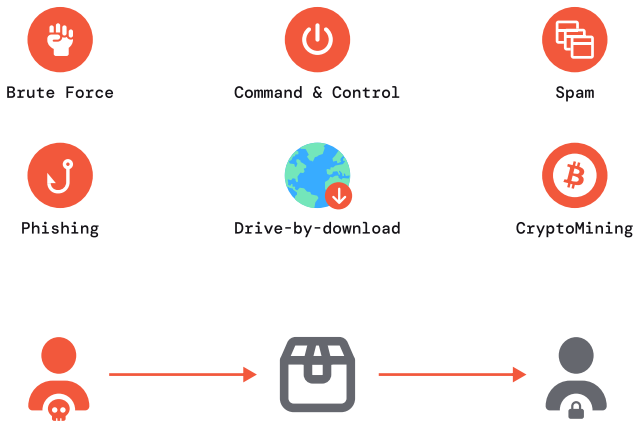
The right approach to CNAPP is to go beyond static analysis and shift-left best practices and combine them with shift right - prioritizing risk and threats by leveraging runtime insights.

Every minute counts when you're experiencing a breach.

277

AVERAGE NUMBER OF DAYS TO IDENTIFY AND CONTAIN A BREACH IN 2023

(SOURCE: IBM.COM/REPORTS/DATA-BREACH)



Cloud attacks are increasing in frequency and organizations need to know about potential risks as they arise and attacks the moment they occur, rather than finding out about them after the damage has been done.

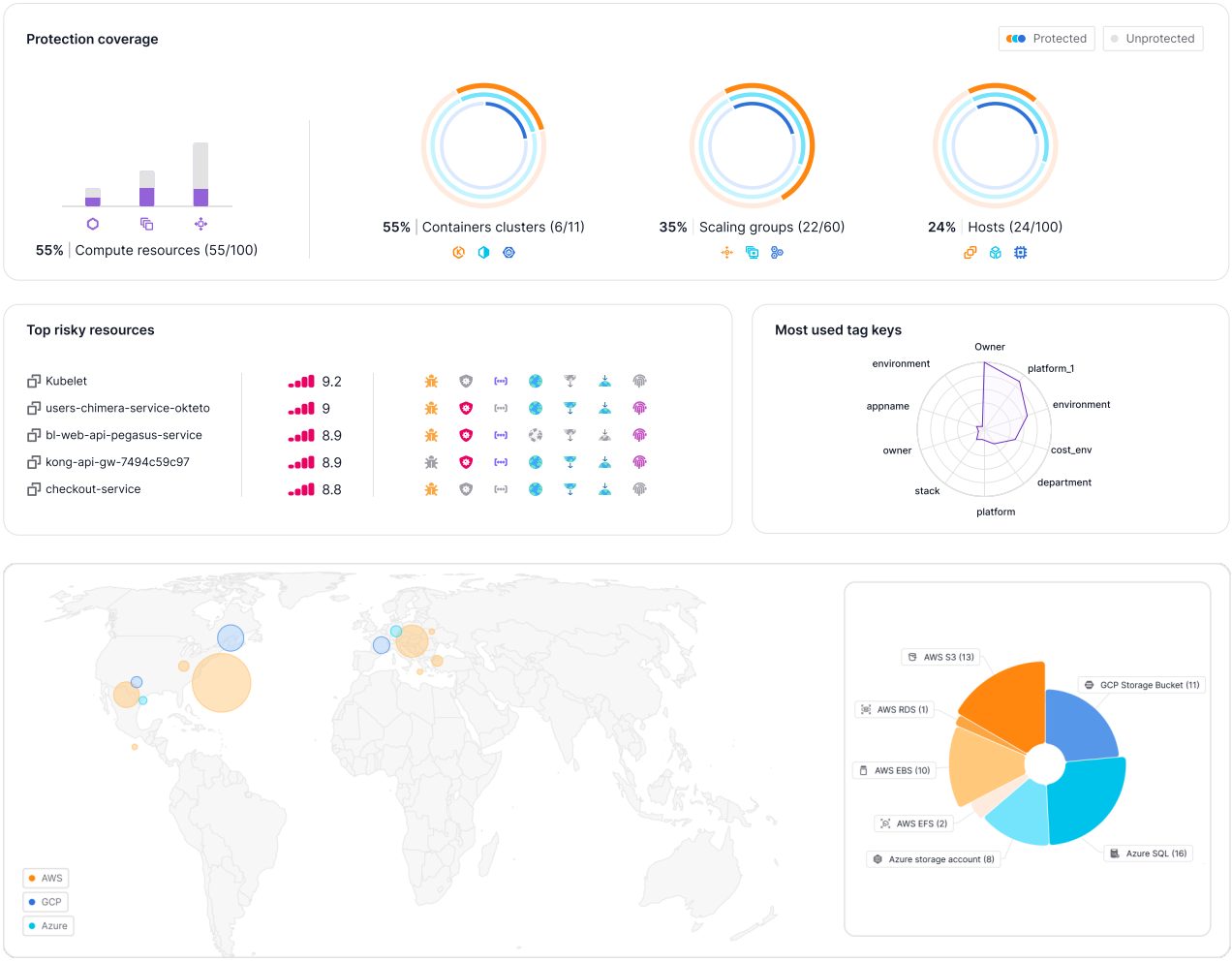
Attackers are becoming increasingly sophisticated, with common attack methods including brute force, command and control, spam, phishing, drive-by downloads and crypto mining becoming commonplace for most enterprises.

04

Know Your Security Reality.

Filtering out noisy alerts and focusing on your most critical risks and threats helps decrease average time to response and time to remediation.

In order to accurately prioritize, you need to understand the state of your cloud and have visibility of your entire cloud inventory, running workloads and applications.



The key to discovering your most critical risks and threats is **understanding what your infrastructure and applications are doing at runtime**. This allows you to prioritize vulnerabilities by answering questions such as:

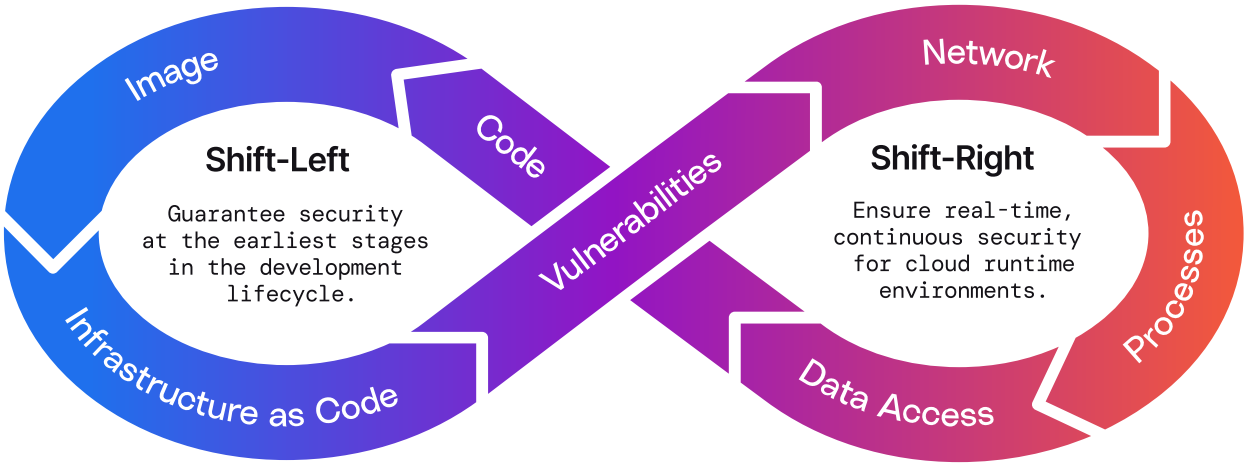
- Is the package loaded into memory or actively in use?
- Is the package exposed to the Internet?
- Is remote execution possible?
- Is there active ingress or egress traffic related to the package?
- Is the package accessing sensitive data?
- Is there an available exploit for the vulnerability?
- Is a vendor-supplied fix available?

05

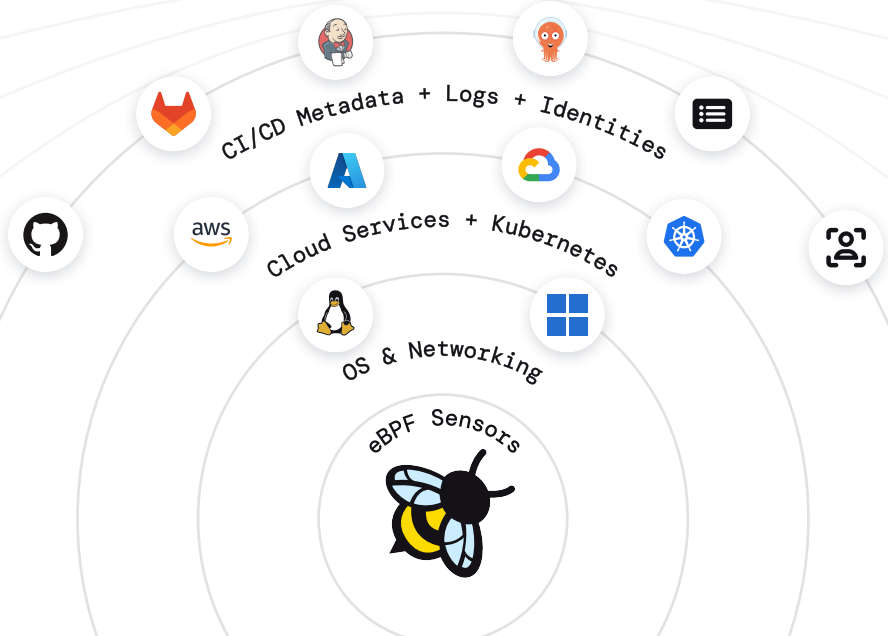
Get On Board with Shift Right.

So how do you leverage runtime insights to prioritize risks & threats?

The answer is shift-right security.



Instead of only using static analysis and agentless scanning that are common in shift-left best practices, shift right focuses on real-time risk and threat insights. eBPF has emerged as the clear industry-leading technology, providing visibility of everything your run at the workload level and allowing you to collect low-level OS data without posing a risk to your production system. eBPF does all of this in real time, including finding and responding to threats as soon as they are detected.

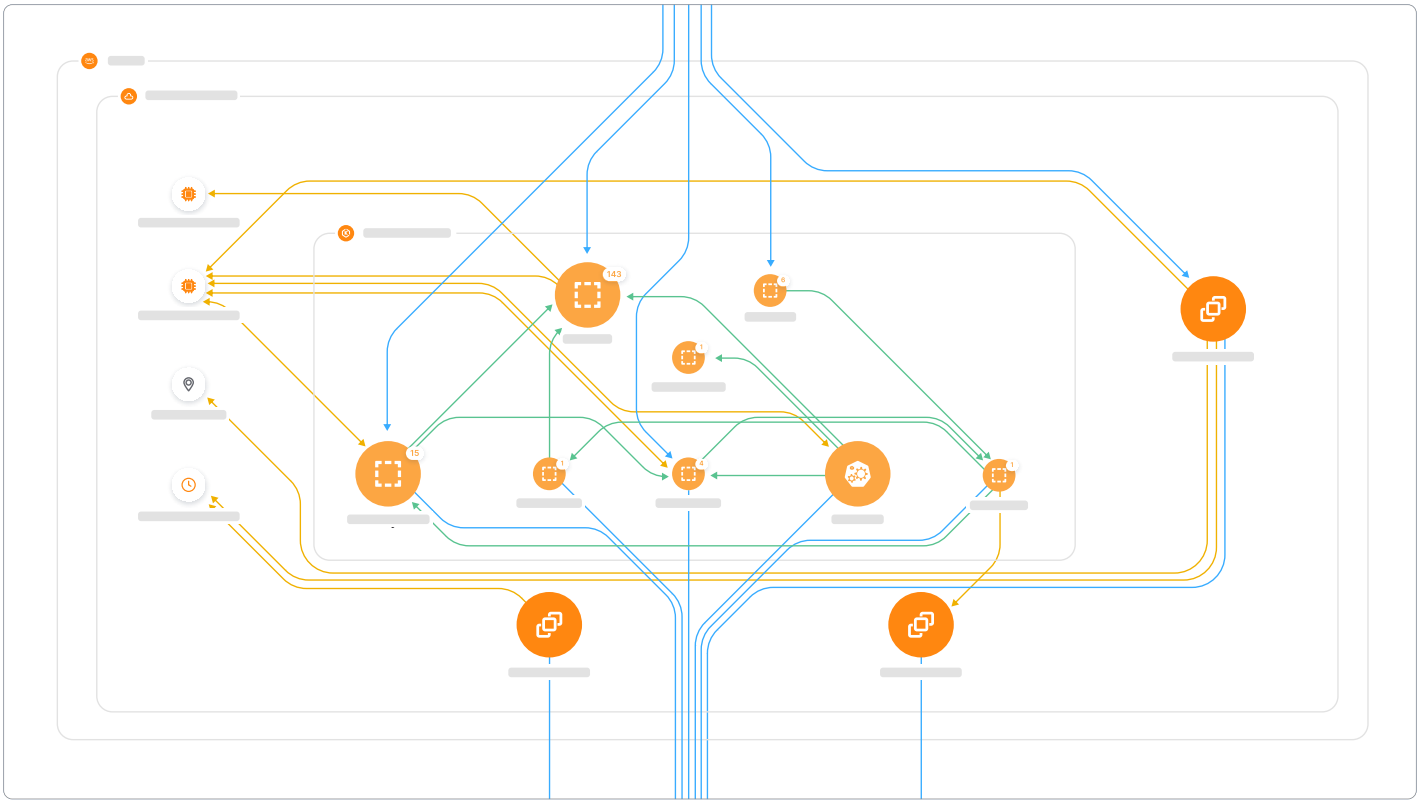


06

The Power of Runtime Data.

Shift right gives you the power of runtime data, including complete visibility of your cloud topology, real-time detection and response, and the ability to understand your environment's security reality.

By understanding your runtime reality, you can turn infrastructure and application operational data into security context, prioritizing your most critical risks and threats.



By leveraging runtime data, you can view real-time network topology and resource communication.

Benefits of real-time insights include:

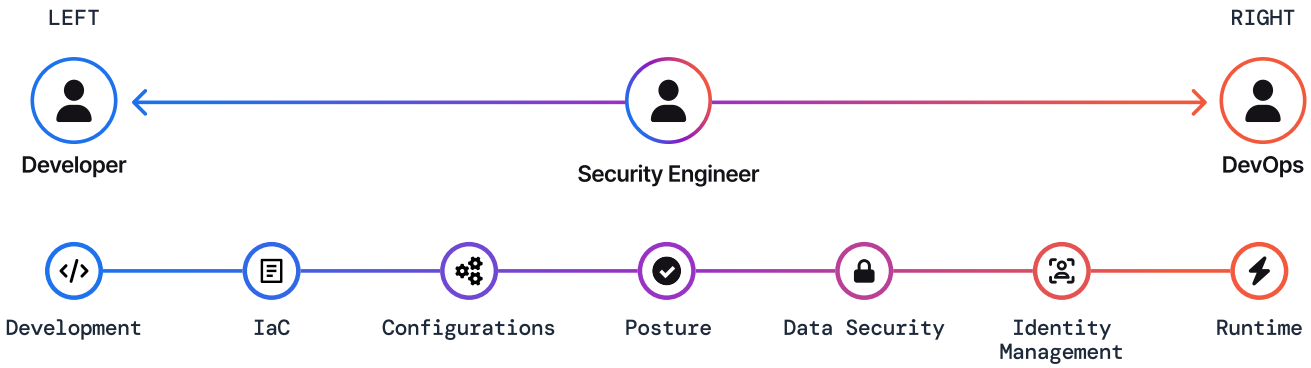
- 360° view of your running services and resource behavior
- Understand who resources are communicating with, including communication within a cluster, within an account and Internet ingress and egress
- Rapidly view changes in resource communication that could signify malicious behavior
- Give your security team DevOps insights, streamlining remediation efforts

07

Become Friends With Your DevOps Team.

With runtime insights, you save your organization time and money by putting DevOps insights into the hands of your security team.

This helps save your security team time in their investigations, and it also lets your DevOps team focus on developing rather than answering security questions.



Runtime gives you context such as:

- Which developer introduced a specific vulnerability into your environment
- A list of all packages within a framework running in your environment, allowing you to quickly roll back or update packages that contain a certain vulnerability (eg log4j)
- Who resources are communicating with, including within a cluster, within an account and with the Internet
- Understand how pull requests impact your running services

08

Make Security Simple.

In other words, cloud security should be simple.

Understand what your infrastructure and applications are doing in real time, prioritize the risks and threats that actually matter and get to the root cause in seconds - all with runtime insights.

About Upwind

In case you haven't guessed already, at Upwind we believe that CNAPP is the answer to cloud security. More specifically, we believe you need runtime insights to dynamically secure your cloud - which is why we are the runtime-powered CNAPP.

Posture & Vulnerability Management

Vulnerability Management	Discover vulnerabilities across your cloud workloads - VMs, Containers, Serverless
CSPM	Detect and remediate misconfigurations from build time to runtime
DSPM	Monitor for sensitive data and secrets exposure and proactively prevent data breaches

Workload Protection

Container Security	Holistically secure containers, Kubernetes across cloud and on-premise data centers
CWPP	Detect and prevent threats across your cloud infrastructure
CDR	Contextualize and streamline cloud security threats and incidents for root cause analysis and automatic response and prevention

Application & Identity Security

API Security	Protect APIs & Layer 7
Identity Security	Discover and analyze human & machine entitlements in the cloud to detect, prioritize and remediate identity (IAM) risks and achieve least privilege

Cloud Security Happens at Runtime.

Realtime Security & App-Layer Identity

API & DNS Awareness with flow correlation

Process level Identity

Active Response

Catch and stop attacks at Runtime

- Malicious Software
- Ransomeware
- Data Exfiltration

Cloud Runtime to Build Time Visibility

See the full map from a running service all the way to your Git

Want to know more about Upwind's CNAPP? Visit www.upwind.io or send us a note at hello@upwind.io to schedule a brief demo and see real-time security in action.