

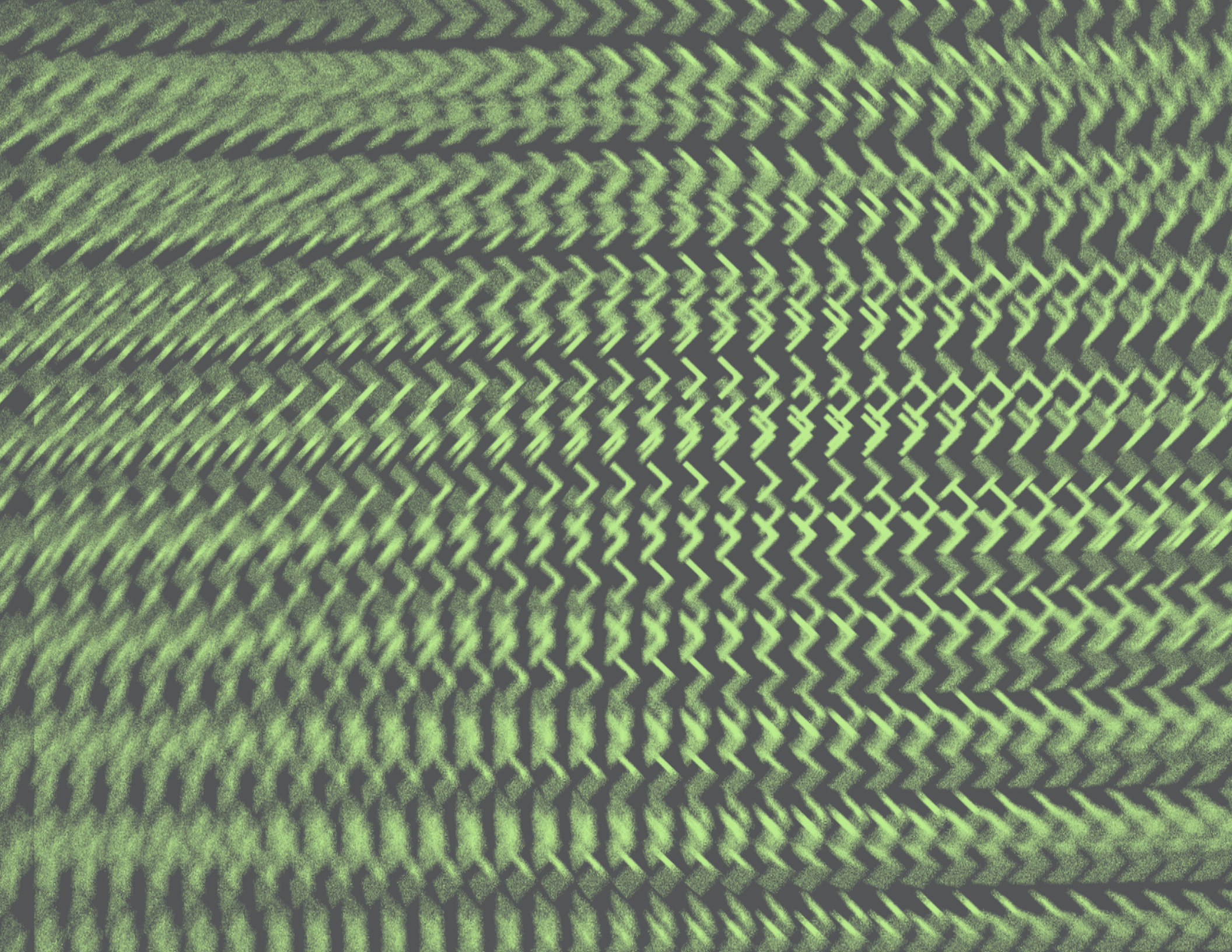
EBOOK

---

# “ The Value of Sysdig's CNAPP

As Told By Customers







**04** Where cloud security began, and where it's headed

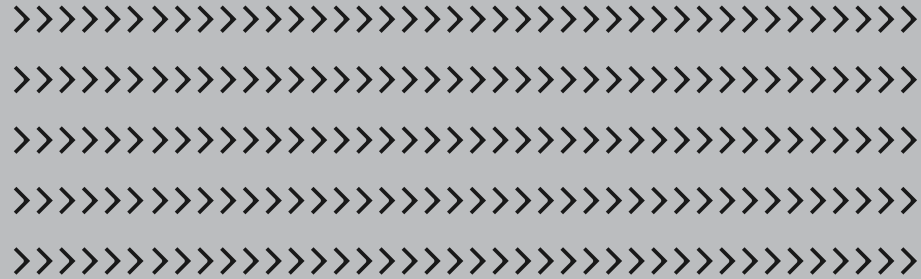
**05** Complete cloud security in a single tool

**06** Cloud security posture management (CSPM)

**09** Cloud detection and response (CDR)

**13** Cloud workload protection platform (CWPP)

**17** Cloud-native application protection platform (CNAPP)



Sysdig's Cloud-Native  
Application Protection Platform

---

## Where cloud security began, and where it's headed

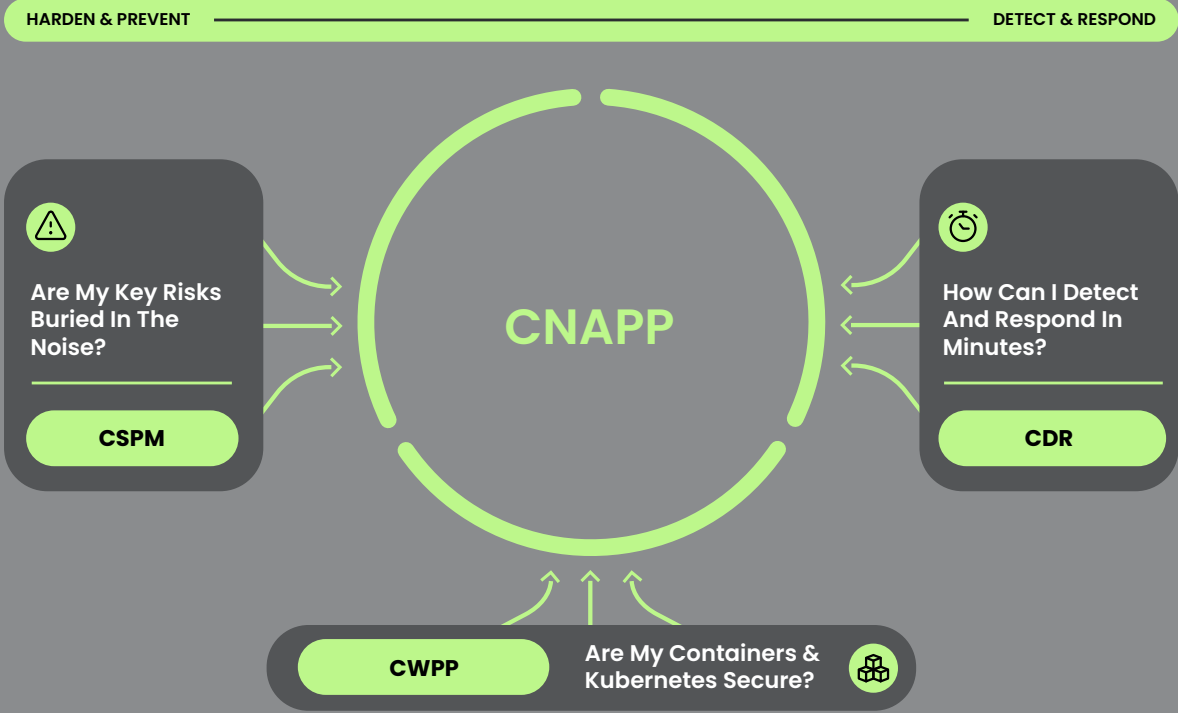
In the early 2000s, most businesses still used on-premises infrastructure, even though the cloud was starting to grow in popularity. Security was likewise designed for on-prem, not the cloud. As a result, organizations reused their traditional security measures (e.g., firewalls, intrusion detection systems, and access control) for cloud environments.

This made visibility into cloud environments a challenge for organizations. Security teams struggled to monitor incidents and vulnerabilities within cloud infrastructure, and relied on the security measures implemented by cloud providers.

Naturally, this somewhat lacking approach became untenable as the cloud grew larger and more complex. Legacy approaches just couldn't keep up with the growth of the cloud attack surface, or the speed and scale of attacks in the cloud.

Today, organizations need to adopt stronger cloud security practices, implement better controls, and have a good plan in place for response. They need tools that go beyond prevention and secure the cloud from end to end. And they need to eliminate silos, blindspots, and tool sprawl. Essentially, the modern cloud requires unified cloud security capabilities.





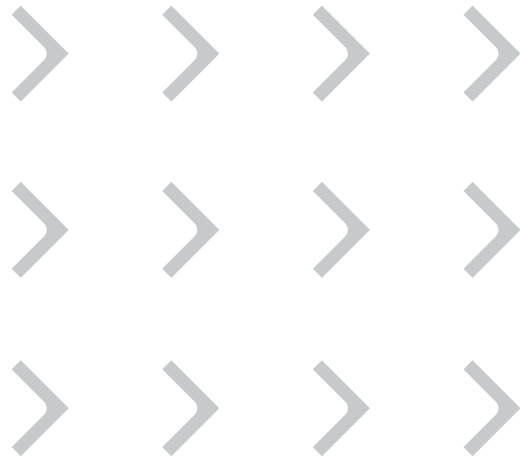
# Complete cloud security in one tool

After years of juggling acronyms, the security industry is converging on CNAPP, or cloud-native application protection platforms. A CNAPP combines the functions of cloud security posture management (CSPM), cloud detection and response (CDR), and cloud workload protection platforms (CWPP).

Bringing all the key use cases of cloud security into one platform makes it easier to secure your cloud environments from end to end. But that also means that to find a complete CNAPP, you need a tool that can handle every piece of the cloud security stack.



Let's hear what our customers have to say about the value they've unlocked with a CNAPP.



## Cloud Security Posture Management (**CSPM**)

---

### What does CSPM do?

CSPM focuses on minimizing risk in cloud infrastructure by strengthening security posture. CSPM tools detect and remediate misconfigurations and posture drift to prevent breaches, and to help ensure compliance.



## CSPM

---



We like that Sysdig uses knowledge of what is in use during production to help us make better-informed posture decisions. It can help filter out 80% or more of the noise. The bottom line is that CSPM is Sysdig's bread and butter, and that inspires confidence.

— *Senior Infrastructure Security Engineer  
at BigCommerce*



### CSPM Case Study

## BigCommerce achieves real-time cloud security

### The Challenge

BigCommerce is a cloud-based e-commerce platform, which makes security and compliance non-negotiable. After struggling with too much alert noise and not enough support, BigCommerce turned to Sysdig.

### The Results

Sysdig enabled BigCommerce to identify and eliminate vulnerabilities, threats, and misconfigurations in real time, while also meeting all their compliance requirements. Leveraging runtime insights has also given BigCommerce an intuitive way to both visualize and analyze threat data.

20%

increase in identifying and prioritizing misconfigurations and vulnerabilities

80%


reduction in vulnerability noise



Watch the BigCommerce case study video

Sysdig

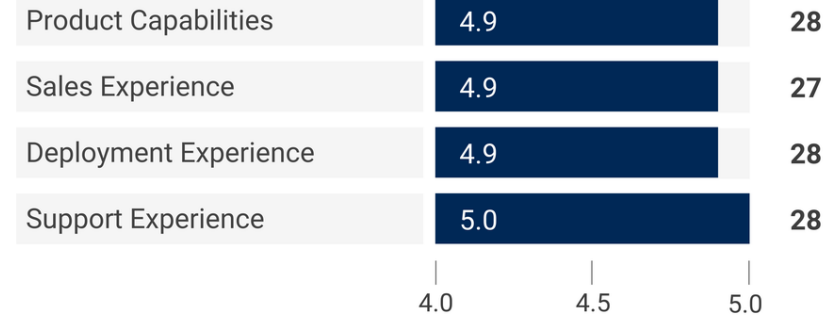
5.0 ★★★★★ (30)

Willingness to Recommend  97%

Rating Histogram



Rating by Category



Number of Responses

Sysdig's results in the Gartner® Voice of the Customer report for CSPM

CSPM

## Sysdig ranks #1

CSPM in the Gartner®

“Voice of the Customer” report

The Gartner® Voice of the Customer reports are a synthesis of reviews and ratings from actual customers. In their Cloud Security Posture Management Tools report, Sysdig was recognized as one of only two Strong Performers, and was the only vendor whose customers gave them an overall rating of 5 out of 5 stars.

# Cloud Detection and Response (**CDR**)

---

## What does CDR do?

Cloud detection and response (CDR) enables security teams to protect their cloud workloads and infrastructure. CDR provides real-time detections of known and unknown threats; deep, cloud-native context into events; and manual and automated response countermeasures to eradicate threats.





CDR

---



For SOC 2 compliance, we need vulnerability scanning, audit logging, and runtime security. Sysdig provides these features out of the box.

— Senior DevOps Engineer at Data  
Notebook Company

CDR Case Study

# Data notebook company shuts down advanced attacks

## The Challenge

This company's cloud-based data notebook blends business intelligence, project management, and AI-driven analytics. After a large spike in users, the company sought out Sysdig to prevent an equal spike in cryptomining attacks.

## The Results

Thanks to Sysdig, the expected flood of attacks never occurred — the organization didn't even need to adjust its policies. Sysdig supports the company's SOC 2 compliance efforts with audit logging, policy management, and vulnerability scanning. Additionally, Sysdig has empowered the company's DevOps team to handle cloud security and compliance with minimal impact on their workload.

99% reduction in time spent addressing malicious activity

60+ cryptomining exploits blocked per day

CDR

**Real-Time Threat Detection Built on Falco**

Did you know that Sysdig's CDR is built directly on Falco — and that Sysdig created and helps to maintain Falco?

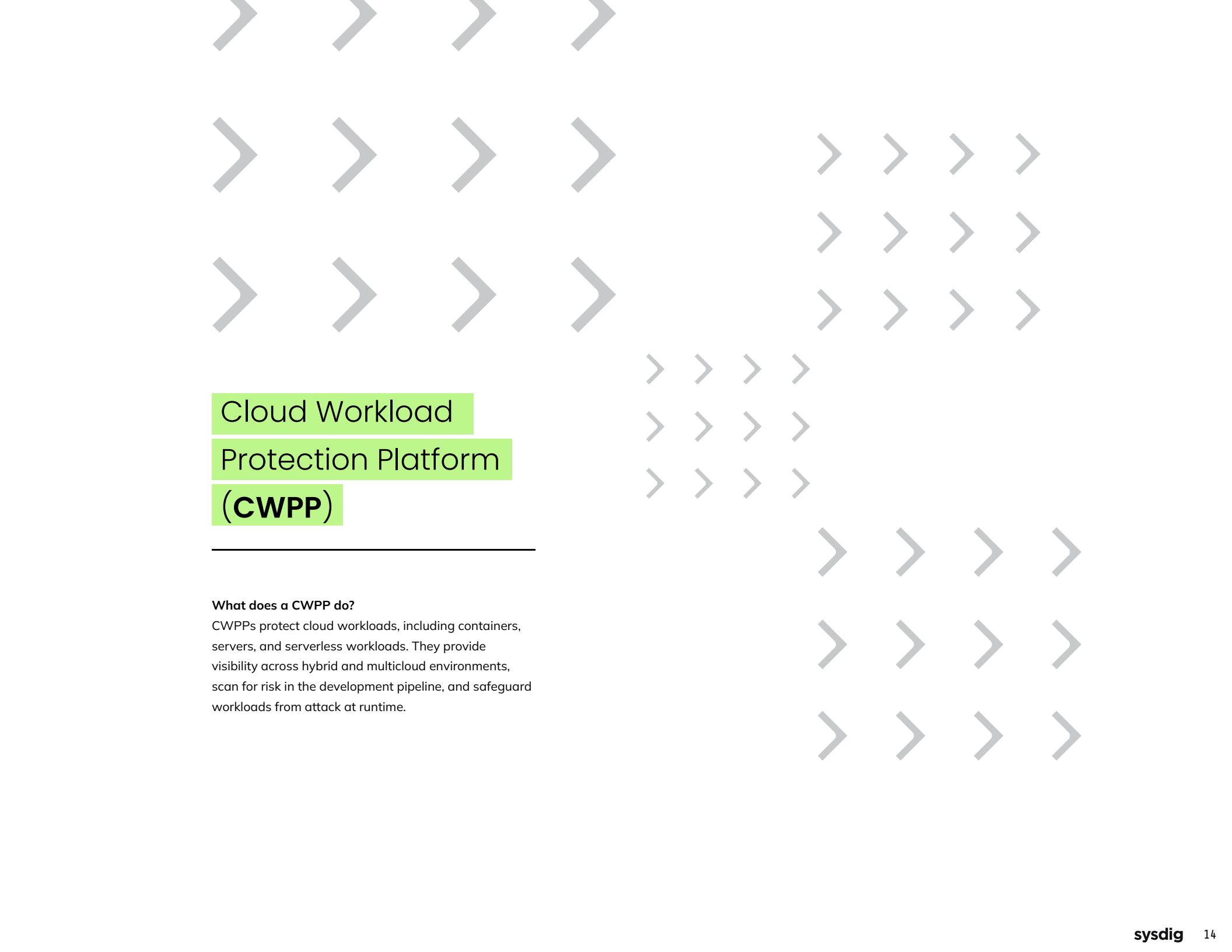
With over 115 million downloads and contributions from companies like IBM, Apple, and Booz Allen Hamilton, Falco is the threat detection engine of choice across the industry, including every cloud provider.



CLOUD NATIVE  
COMPUTING FOUNDATION

**FALCO**  
**GRADUATION**  
2024





## Cloud Workload Protection Platform (CWPP)

---

### What does a CWPP do?

CWPPs protect cloud workloads, including containers, servers, and serverless workloads. They provide visibility across hybrid and multicloud environments, scan for risk in the development pipeline, and safeguard workloads from attack at runtime.

CWPP

---



Immediately out of the box, Sysdig helped us locate vulnerabilities and view our posture and compliance against the clusters we have up and running. That level of visibility is phenomenal, and it's why Sysdig is the only security tool we use for Kubernetes.

— *Senior Manager of Information Security  
at Apree Health*

## CWPP Case Study

# Apree Health gains container visibility and meets compliance

### The Challenge

Apree Health is tearing down the health industry's data silos with a suite of solutions designed to help patients achieve better, more affordable outcomes. They looked to Sysdig to streamline compliance and enhance overall security and incident response.

### The Results

Sysdig provides Apree Health with deep visibility into its Kubernetes deployment through a single, unified view. This, along with its vulnerability and misconfiguration scanning, has been invaluable to the company's compliance efforts. It's also made risk, threat, and vulnerability management significantly easier for Apree Health's security operations team.

>10<sub>hr</sub> per month saved on security and compliance

80% reduction in time to remediation

# GIGAOM

## CWPP

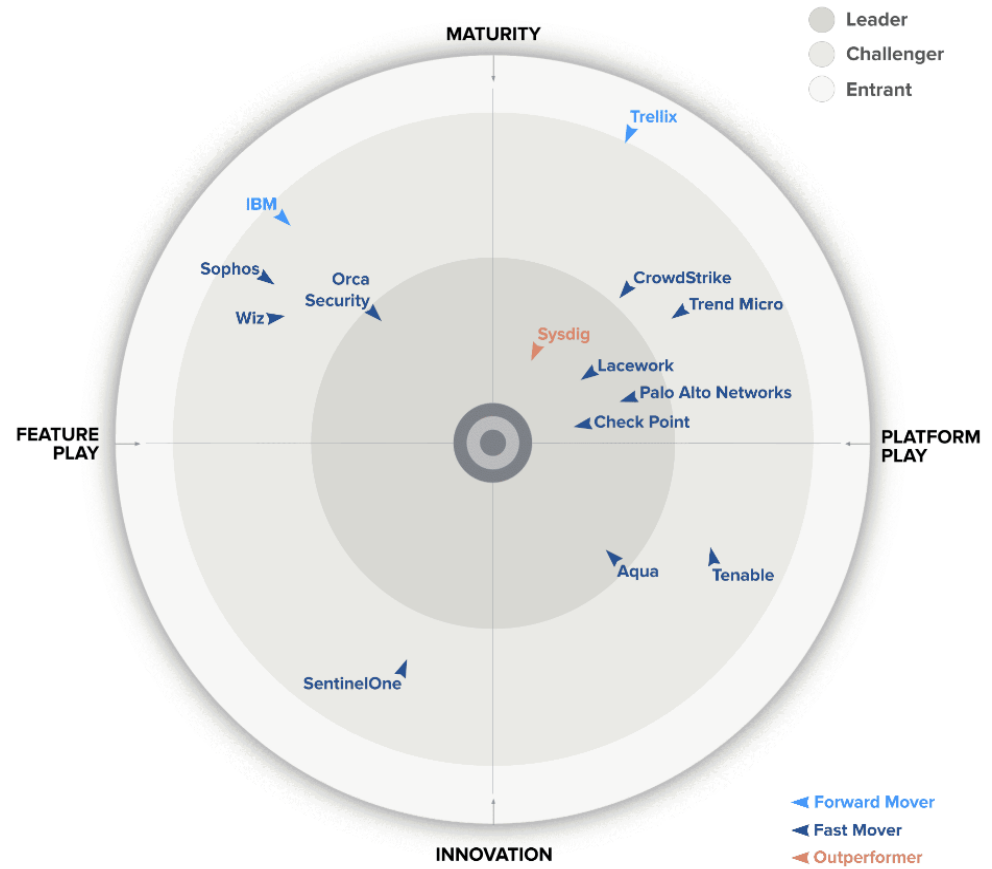
### GigaOm Report Gives Sysdig Highest Rating for Cloud Workload Security

In the GigaOm Radar for Cloud Workload Security, Sysdig placed in the leader's circle, and was the only solution named an Outperformer.



Sysdig is positioned as a Leader and Outperformer in the Maturity/Platform Play quadrant due to its exceptional hybrid environment support and superior workload detection and response capabilities.

— GigaOm Radar for Cloud Workload Security 2024



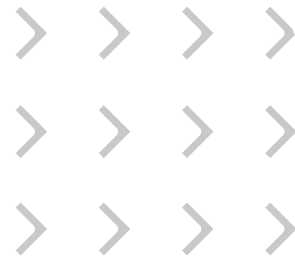


# Cloud-Native Application Protection Platform (**CNAPP**)

---

## The power of consolidation

All of the use cases we've discussed so far are critical for securing the cloud. But by bringing them together in one platform, you get a solution that's more than the sum of its parts.





Leveraging Sysdig’s CNAPP gives you in-depth, multi-layered, agent-based, and agentless coverage across all aspects of your environment – everything from proactive validation of workloads to auditing policies on the public cloud platform you’re running on.

Sysdig’s secret sauce is having the best engine on the market, which gives us real-time runtime insights. Runtime insights leverages knowledge of what’s in use to prioritize risks that matter and provide context to remediate them.

Here’s just a few key benefits of this holistic approach to monitoring for, detecting, and remediating threats:

- End-to-end visibility
- Improved operational efficiency
- Reduced spending
- Stronger overall security posture

CNAPP

---



After comparing our manual solutions with the cost of Sysdig for one year, we chose Sysdig – and are very happy we did. Now, one tool can achieve what previously required six tools, resulting in savings exceeding Sysdig costs.

— Senior Cloud Security and DevOps  
Engineer at health IT organization

### CNAPP Case Study

Healthcare IT  
company achieves  
compliance with  
reduced costs

#### The Challenge

This company's cloud-based platform simplifies health insurance with plan comparisons, a cost estimator, doctor lookup tools, and more. But as they began working with state governments, they needed to meet increasingly strict compliance standards. That's where Sysdig came in.

#### The Results

Sysdig makes compliance easy for the company with out-of-the-box compliance checks that provide an instant snapshot of compliance postures, highlighting each passed and failed control. Sysdig also enables the company to identify threats to health insurance customers and their data in real time, prioritize relevant vulnerabilities, and swiftly address them with contextual information.

98% reduction in  
vulnerability noise

30% reduction in  
computing costs

>10<sub>hr</sub> saved per week  
auditing  
infrastructure



CNAPP

---



We had a visibility gap before Sysdig. With Sysdig, we understand in real time where our risk lies.

— *Cloud Security Lead at data productivity company*

## CNAPP Case Study

# Data productivity company secures SaaS delivery

### The Challenge

This company offers a seamless and unified environment to build, deploy, and scale data pipelines. When they expanded from on-premises to software-as-a-service, they worked with Sysdig to extend security and compliance to containerized environments.

### The Results

With Sysdig, the company was able to bring their security and compliance capabilities into a containerized world. Sysdig allows the company to identify and eliminate vulnerabilities, threats, and misconfigurations in real time while maintaining a high level of transparency. The comprehensive visibility Sysdig provides makes it easy to find and identify threats.

**80%** reduction in  
vulnerability noise

**20%** time savings by  
consolidating  
into a CNAPP

**6<sub>min</sub>** timeframe to  
securely deploy  
code through  
integrated checks

## Runtime Insights

---



Basing everything Sysdig does on runtime insights enables faster threat detection, better vulnerability management, better cost optimization, and ultimately, better security posture.

— *IT Security Manager at fraud detection software company*

