

# REPORT. 2023 Global Cloud Threat Report

Archived: 2026-05-03 02:27:21 UTC



[REPORT. 2023 Global Cloud Threat Reportpdf](#)

[AWS Azure Cloud Security Docker](#)



[WEBINAR. DevOps Security, Monitoring and Compliance with OpenShift and Sysdig video](#)

[Cloud Security Openshift Red Hat Sysdig Secure](#)



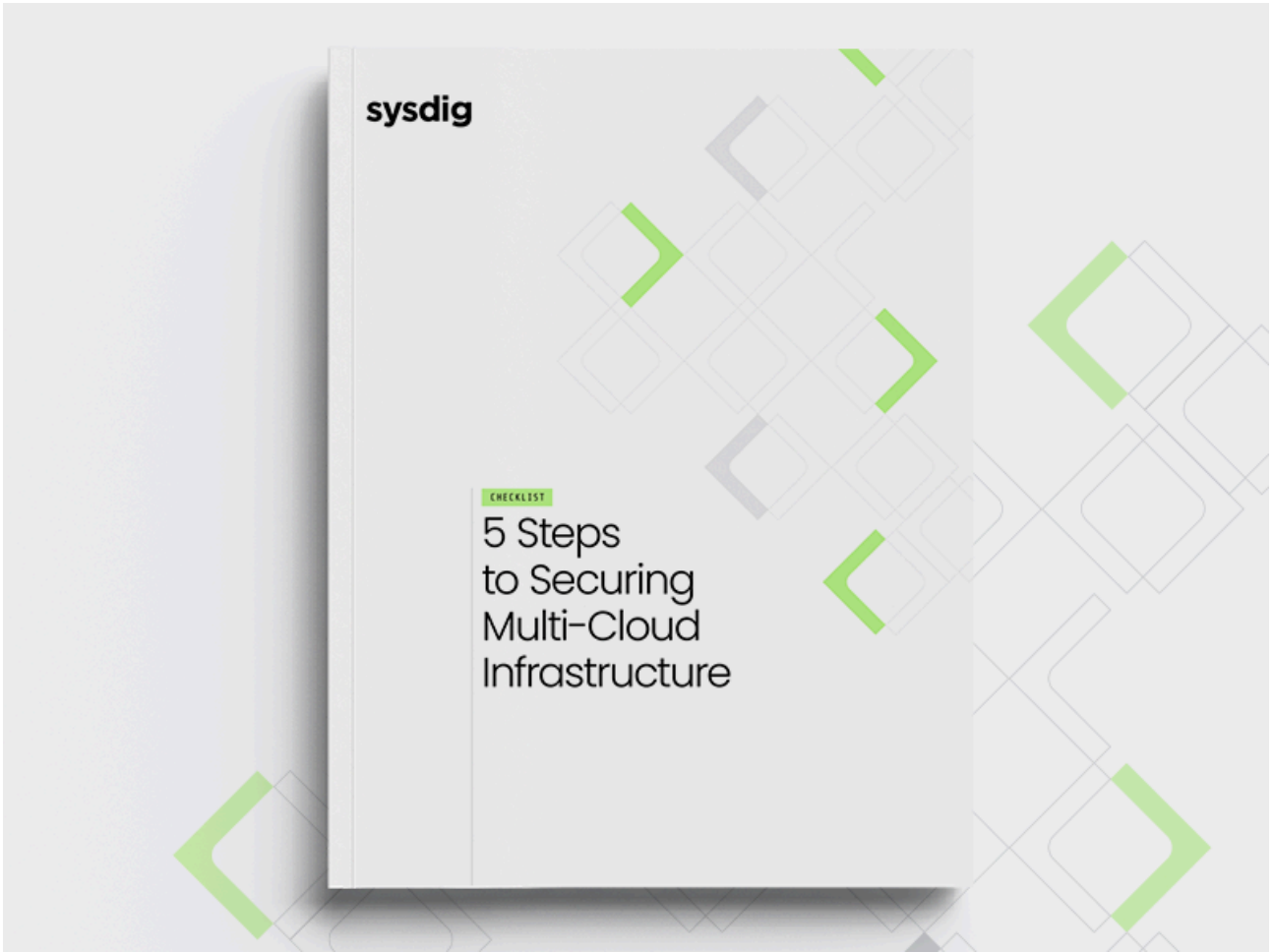
# Continuous Security for AWS Cloud and Containers

---



[GUIDE. Continuous Security for AWS Cloud and Containerspdf](#)

[AWS Cloud Security Sysdig SecureCloud Monitoring](#)



[GUIDE. 5 Steps to Securing Multi-Cloud Infrastructurepdf](#)

[AWSCloud SecuritySysdig Secure](#)



# Close the Security and Visibility Gap for Containers on AWS

**aws** partner network

**Advanced Technology Partner**

---

Containers Competency

---

Public Sector Partner

---

Amazon Outposts

Security is the number one barrier to moving container-based apps to production. Containers live for a few minutes and are essentially black boxes. The containerized environment is dynamic and most organizations have 10's of thousands of microservices to manage. It is hard to manage security risk when your DevOps team cannot see what matters!

With Sysdig Secure DevOps, you can embed security and compliance to create a secure DevOps workflow. Allowing you to:

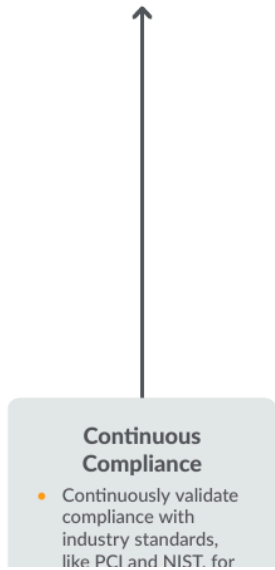
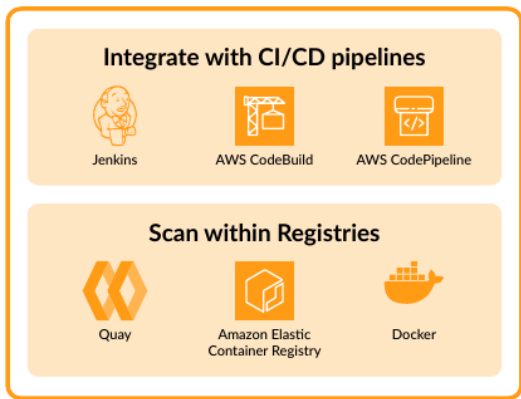
- Secure the build pipeline
- Detect threats at runtime
- Rapidly respond to incidents and conduct forensics investigations
- Continuously validate regulatory compliance

Let's take a look at how the Sysdig Secure DevOps platform plugs into your existing workflow. With Sysdig you can confidently run cloud apps in production on AWS container services like Amazon EKS, Amazon ECS, and AWS Fargate.

## Build

### Image Scanning

- Scan images directly within ECR.
- Integrate directly into your CI/CD pipelines, including AWS CodePipeline and AWS CodeBuild.
- Automate inline image scanning for Fargate, EKS, and ECS containers and ensure your images/registry credentials don't leave



your AWS environment.

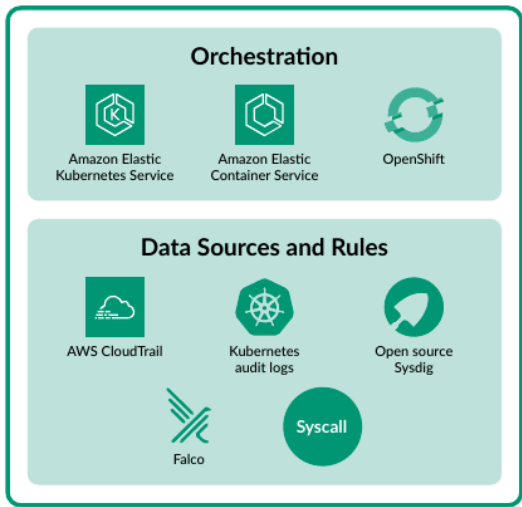


- AWS services during build and runtime.
- Map compliance standards to specific controls using Falco rules to be audit-ready at any time.
  - Audit Kubernetes, container, and cloud activity.
  - Automatically run benchmarks and measure progress against CIS best practices.
  - Enable File Integrity Monitoring (FIM) to detect data tampering.

# Run

## Runtime Security

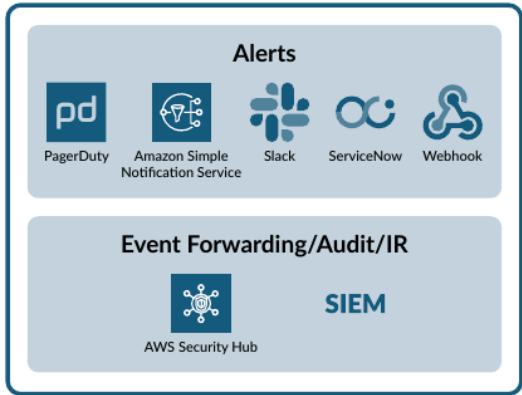
- Secure applications and infrastructure at runtime without impacting performance, with Falco.
- Implement real-time threat detection using syscalls, Kubernetes audit logs and CloudTrail logs.
- Save time with out-of-the-box rules to spot anomalous behavior.



# Respond

## Incident Response and Forensics

- Quickly understand any security breach using granular, system-level capture data, with Kubernetes and cloud context.
- Correlate system, user, and container activity to determine root cause even after containers are gone.
- Accelerate incident response and recover quickly.

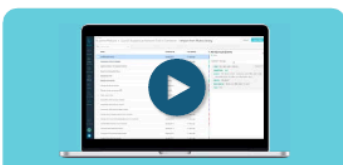


Sysdig is open by design with enterprise-grade scale, and reliability, to support AWS customers. The Sysdig Secure DevOps Platform helps manage security risk, maximize availability, and validate compliance on AWS container services.



Read AWS Security & Monitoring Guide

LEARN MORE



Demo the Sysdig platform today

WATCH A DEMO



Start your Sysdig Secure DevOps FREE trial now

READY TO TRY

All other marks and names mentioned herein may be trademarks of their respective companies.

Copyright © 2020 Sysdig, Inc. All rights reserved. ING-007 Rev. A 9/20

[INFOGRAPHIC. Close the Security and Visibility Gap for Containers on AWSpdf](#)

[AWS Cloud Security Sysdig Secure Cloud Monitoring](#)



# Continuous Security for Microsoft Azure Cloud and Containers



[GUIDE. Security And Monitoring On Azure Container Servicespdf](#)

[AzureCloud Security Sysdig SecureCloud Monitoring](#)



CASE STUDY



## LogDNA Delivers Higher Uptime and Improved Customer Experience

### COMPANY DETAILS:

The LogDNA log management solution enables DevOps teams to aggregate all of their system and application logs into a single platform.

### BUSINESS NEEDS:

- Deliver Kubernetes logging capability to customers
- Transition the entire stack to run as microservices on Kubernetes

### CHALLENGES:

- Managing Prometheus servers was time consuming
- No audit trails for debugging and troubleshooting
- Lack of alerting before an event impacted customer experience

### BUSINESS IMPACT OF SYSDIG:

Improved customer experience by reducing time to resolve performance issues. Improved efficiency for compliance and audit processes.

### SYSDIG PLATFORM BENEFITS:

- Quick insight to address security issues pre-production
- Dashboards help to understand what is going on in the environment
- Audit trails for efficient troubleshooting and compliance reporting
- Fast ramp with dashboard and alert creation across all environments
- Minimal maintenance effort

INFRASTRUCTURE: Amazon Web Services

ORCHESTRATION: Elastic Kubernetes Service (EKS)



### Overview

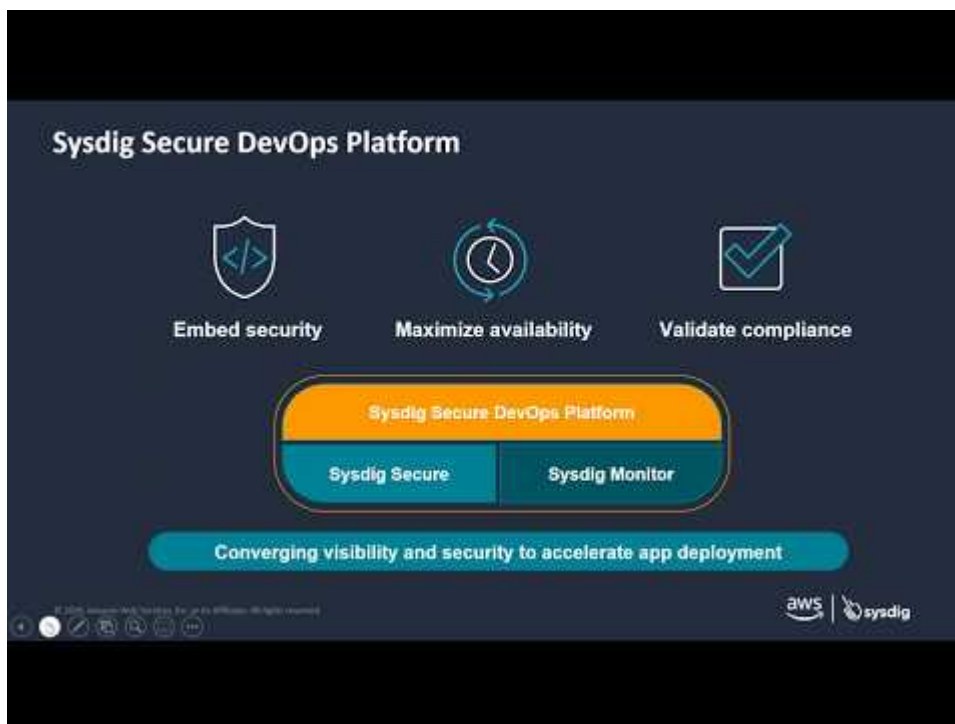
LogDNA is a centralized log management solution that empowers DevOps teams with the tools that they need to develop and debug their applications with ease. They help thousands of companies, from startups to large enterprises, take control of their data and gain valuable insights from their logs.

As Kubernetes has matured over the last few years, LogDNA found that a growing number of customers wanted a Kubernetes logging solution. To meet the market need and to take advantage of consistency, scalability, and repeatability, the company made the decision to transition its entire stack to run as microservices on Kubernetes.

According to Ryan Staatz, Systems Architect at LogDNA, "Microservices make things a lot more interesting. There are a lot of things running at the same time. One of the cloud environments we use is Amazon EKS and we really enjoy the fact that it is a managed service. We don't have to focus on managing the Kubernetes masters and we can just do what we do best, which is running our application stack in Kubernetes."

[CASE STUDY. Mezmo Delivers Higher Uptime and Improved Customer Experiencepdf](#)

[AWSCloud SecuritySysdig\\_SecureCloud Monitoring](#)



[WEBINAR. Best Practices to Secure Containers and Accelerate Software Delivery](#)

[AWS Cloud Security Sysdig Secure](#)



# Streamline Cloud Security Operations with Sysdig and AWS

## Detect, investigate, and respond faster with Sysdig Secure and Amazon Security Lake

As the scale of your cloud-native applications and infrastructure grows, your security teams need effective ways to manage and accelerate security across multicloud and hybrid environments.

The integration of Sysdig Secure with Amazon Security Lake creates an efficient and streamlined approach to security and compliance at scale. It combines Sysdig's powerful runtime security capabilities with Amazon's scalable and cost-effective data lake solution to deliver a more complete view of security data across your entire organization.

With Sysdig and AWS, you can take action on your security data faster and simplify security data management.

### The Future of Security is Open

Sysdig is the creator of Falco, the open source solution for cloud threat detection. Open source drives standardization, speeding innovation with community contributions.



Amazon Security Lake has adopted the Open Cybersecurity Schema Framework (OCSE), an open standard that normalizes and combines security data from AWS and a broad range of enterprise security data sources.

## Combine real-time detection with a purpose-built data lake

Sysdig's Cloud-Native Application Protection Platform (CNAPP), powered by runtime insights, empowers cloud and security teams to detect and respond to threats in real time. Sysdig integrates with Amazon Security Lake, enabling you to store enriched multi-platform cloud security events on AWS where you can use your preferred analytics tools to analyze your security data.

### Why Sysdig Secure?

Sysdig helps AWS customers secure and accelerate innovation in the cloud. Built on open source Falco, Sysdig secures AWS containers, Kubernetes, and cloud services and helps you focus on the threats that matter most.

### Why Amazon Security Lake?

With Amazon Security Lake, teams can utilize a centralized location to analyze security data across your multicloud and hybrid environments to improve the protection of your workloads, applications, and data.

[SOLUTION BRIEF: AWS Security Lakepdf](#)

[AWS Cloud Security Sysdig Secure](#)



# Cloud Security Powered by Runtime Insights

Sysdig provides real-time cloud-native security for Fargate, EKS, and ECS at scale, to help customers migrate or modernize their container and cloud workloads on AWS. Powered by Runtime Insights, Sysdig's Cloud Native Application Protection Platform (CNAPP) stops threats in real time, reduces vulnerabilities by up to 95%, and helps you prioritize and remediate security posture risks.

## Sysdig Use Cases for AWS

Challenges	I need to...	Services	Key Features and Benefits
72% of containers live less than five minutes*	Secure serverless containers	AWS Fargate	Sysdig automates image scanning as an accessible registry for AWS Fargate. It gives deep, real-time visibility to confidently run serverless container workloads on AWS Fargate.
99% of breaches start with cloud misconfigurations**	Detect and respond to cloud threats	AWS Cloudtrail Any AWS services with AWS Cloudtrail logs	Sysdig's Runtime Insights monitors active tasks, in use packages and configurations to detect threats across running containers, hosts, clusters, and cloud services. With open source Falco rules, it can identify suspicious activity across AWS infrastructure.
87% of container images have high or critical vulnerabilities*	Manage container and cloud vulnerabilities	Amazon ECS Amazon EKS Amazon ECR AWS CodeBuild AWS CodePipeline Multiple AWS services	Sysdig profiles running containers to identify in-use vulnerable packages that create a risk in production. It reduces 60-95% of noise by prioritizing vulnerabilities tied to active packages based on this runtime context and risk. Further, it automates image scanning in CI/CD pipelines and Amazon ECR within your AWS environment.
41% cite compliance as top 3 barriers vis-a-vis cloud outcomes***	Manage cloud and container compliance	Across the entire AWS stack	Sysdig's real-time drift detection complements static posture management to minimize visibility gaps. Information about differences in configuration between the in-use resource vs its intended configuration is used to generate suggested fixes and pull requests. Sysdig scans IaC files pre-deployment and maps misconfigs in production back to the source. It automates AWS cloud and container compliance for PCI, NIST, SOC2, FedRAMP, and more.
Over 90% of cloud permissions never get used*	Manage Permissions and Entitlements	Amazon S3 AWS IAM Across the entire AWS stack	With Sysdig, its easy to get visibility into cloud identities, manage permissions, and identify inactive users and identities with excessive permissions. It optimizes access policies to grant just enough privileges and helps restrict permissions to those truly in-use.
59% Containers are instantiated with no CPU limits and 49% with no memory limits*	Maximize performance and reduce costs	Amazon EKS Kubernetes	Sysdig identifies areas in your Kubernetes environments to optimize where there is room to add more pods or move workloads to smaller instances to reduce costs. It helps you predict costs and savings estimates for Kubernetes.

\* Sysdig 2023 Cloud-Native Security and Usage report \*\* Gartner 2021 Hype Cycle for Cloud Security \*\*\* Accenture The race to cloud

[Cloud Security Powered by Runtime Insights.pdf](#)

[AWS Cloud Security Sysdig Secure](#)



[VIDEO. Fargate Scanning In Under 4 Minutes](#)video

[AWS Cloud Security](#)Sysdig Secure



# How to stay PCI Compliant in a container environment



[GUIDE. Red Hat + Sysdig PCI Compliance Guidepdf](#)

[OpenshiftRed HatSysdig SecureRegulatory Compliance](#)



# Secure AWS Fargate Workloads with Sysdig Secure for AWS

## Accelerate secure innovation with serverless compute for containers

Containers continue to grow in popularity, providing an agile and efficient approach for developing and deploying applications for organizations. But scaling containers securely in a serverless environment can present challenges to enterprise organizations. Abstraction layers can obstruct visibility, which can make it harder to spot vulnerabilities and threats, identify misconfigurations, and detect abnormal activity.

For those running AWS Fargate containers, Amazon Web Services (AWS) is responsible for the security OF the cloud. But you are responsible for the security of what's running IN AWS. How can your organization better meet those security needs?

Sysdig, an AWS Security Competency Partner, has deep expertise in container security and can help minimize risk across cloud services and containers running on AWS.

**Up to 15% of enterprise applications will run in a container environment by 2024**



**72% of containers live less than five minutes, complicating security, monitoring, and compliance**



## Secure Your Environment and Optimize Costs with Sysdig

With deep visibility into cloud-native workloads, Sysdig simplifies observability, helping AWS customers monitor performance, rapidly troubleshoot issues, and manage cloud costs.

**Optimize the performance** and availability of AWS Fargate containers with comprehensive monitoring

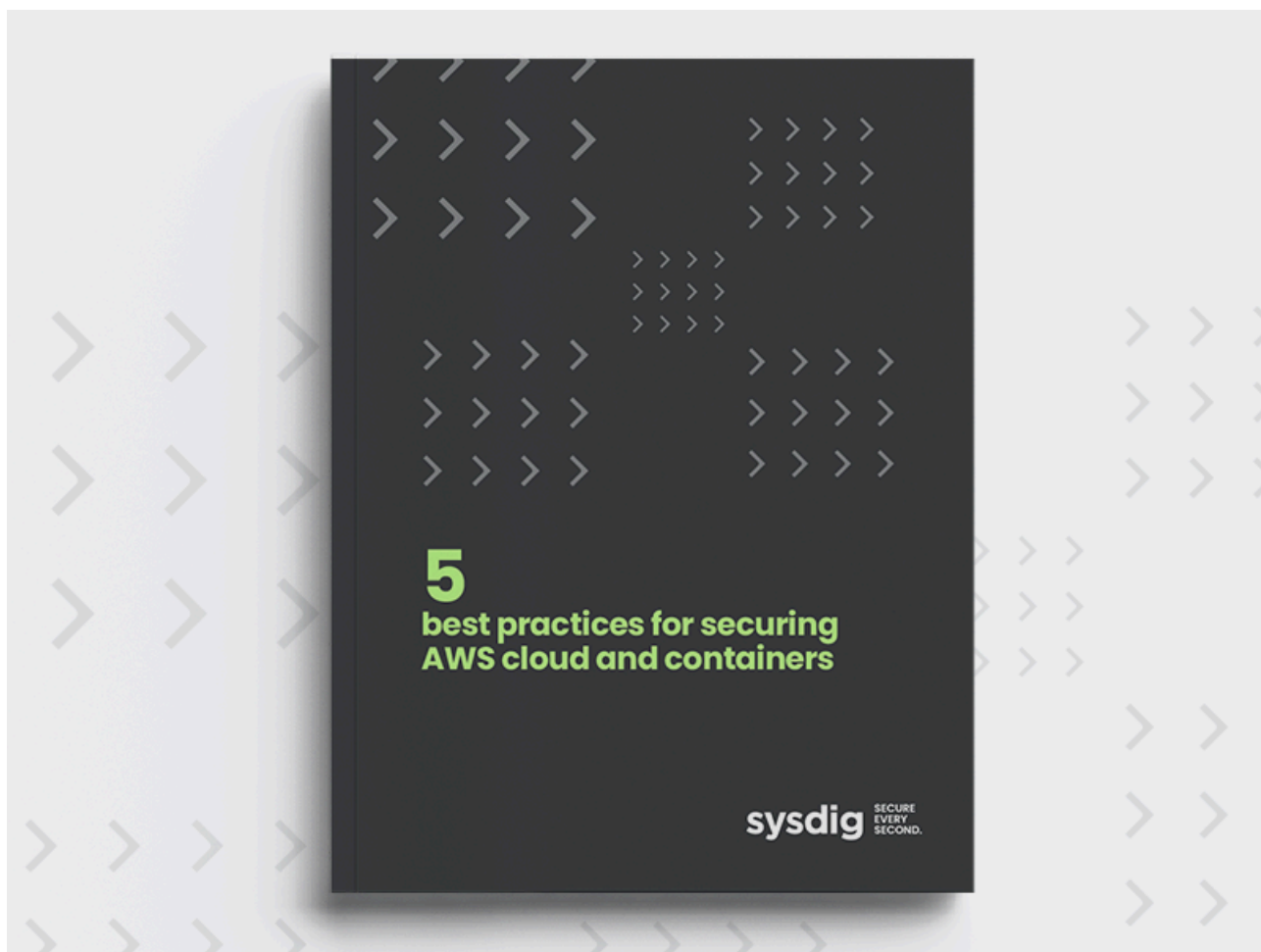
**Quickly identify and resolve issues** with detailed dashboards, alerts, and a prioritized list of remediation recommendations.

**Analyze resource utilization** to improve capacity management planning, optimize cloud usage, and reduce costs.



[SOLUTION BRIEF. Sysdig Secure for AWS Fargatepdf](#)

[AWS Cloud Security Sysdig Secure](#)



[BRIEF. 5 best practices for securing AWS cloud and containerspdf](#)

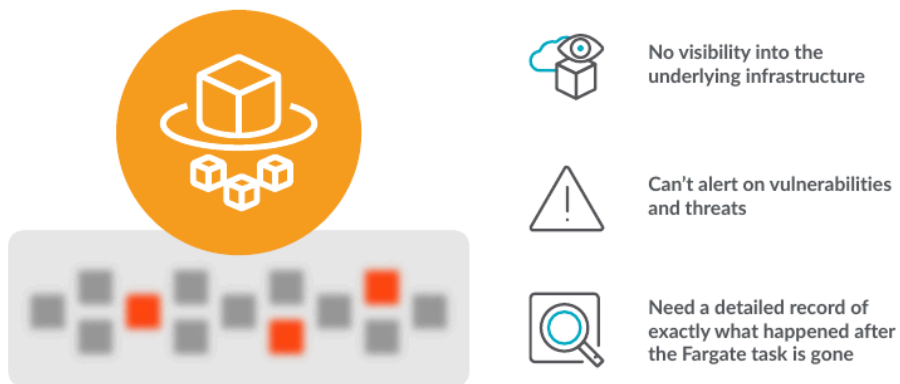
[AWSCloud SecuritySysdig Secure](#)



## Securing Containers on AWS Fargate Checklist

AWS Fargate is a popular serverless compute engine for containers that works with both Amazon ECS and Amazon EKS. Fargate makes it easy for you to focus on building your applications. It removes the need to provision and manage servers, and lets you specify and pay for resources per application.

While serverless environments free you to focus on modern application development there are also some challenges to be addressed. Serverless environments introduce an abstraction layer that hides the underlying infrastructure from the DevOps and security teams. Without access to the host or traditional monitoring tools, your visibility into workload activity can be limited, leaving you blind to threats. Once you identify a security or performance issue, teams need a detailed record of activity to respond to incidents and troubleshoot issues.



The key is to continuously scan for cloud and container vulnerabilities, detect abnormal activity, reduce your risk from cloud misconfigurations and prioritize threats to ensure your containers on Fargate are secure across their entire life cycle. These five key workflows will enable you to address the most critical security and visibility requirements so you can confidently and securely run containers on AWS Fargate.



[GUIDE. AWS Fargate Checklistpdf](#)

[AWSCloud SecuritySysdig\\_Secure](#)



[GUIDE. 5 Steps to Securing AWS Cloud Infrastructurepdf](#)

[AWSCloud SecuritySysdig Secure](#)



[GUIDE. 5 Steps To Securing Microsoft Azure Cloud Infrastructurepdf](#)

[AzureCloud SecuritySysdig Secure](#)



# Securing Modern Cloud Applications & Infrastructure for Financial Services Companies

## Benefits

- Improve resilience, security, efficiency, and time to market
- Enforce compliance and governance via policy as code
- Meet regulatory compliance standards including PCI, NIST ISO, GDPR, and SOC2
- Reduce risk with a secure-by-design platform for containers
- Build a comprehensive DevSecOps solution
- Streamline operations and deliver better customer experiences

Financial services companies have quickly adapted to modern cloud technologies to drive innovation and competitive advantage. Facing a constant risk of security breaches and the demands of stringent compliance standards, DevOps and cloud teams must carefully address security in the new cloud-native world.

Together, Red Hat and Sysdig enable enterprises to confidently run containers, Kubernetes, and cloud. We help FinServ organizations modernize systems, automate processes, and streamline application delivery while improving resilience, security, compliance, and efficiency so you can reduce time to market.

### Red Hat OpenShift Container Platform – Secure by Design

Red Hat® OpenShift® is an enterprise-ready Kubernetes container platform built for an open hybrid cloud strategy. It gives you the ability to choose where you build, deploy, and run applications through a consistent experience across hybrid cloud, multicloud, and edge.

OpenShift delivers a modern, scalable approach to securing your entire application platform stack, from operating system to container to application. As you move to modern application development, OpenShift helps you decrease your operational risk using built-in policy templates to enforce security and configuration best practices.

### Sysdig Secure DevOps Platform – Seeing is Securing

Managing security is a continuous process. Sysdig helps you meet this challenge by embedding security into your DevOps workflows. The Sysdig Secure DevOps Platform provides a container and cloud security stack built on open source innovation. It enables deep visibility across workloads and multi-cloud infrastructure.

With Sysdig, teams secure the build, detect and respond to threats, continuously validate cloud configurations and compliance, and monitor performance across OpenShift and cloud deployments. Pairing Sysdig with OpenShift, you can deliver a comprehensive DevSecOps solution for your financial service applications with a secure platform and security across the entire container lifecycle – from code to cloud.



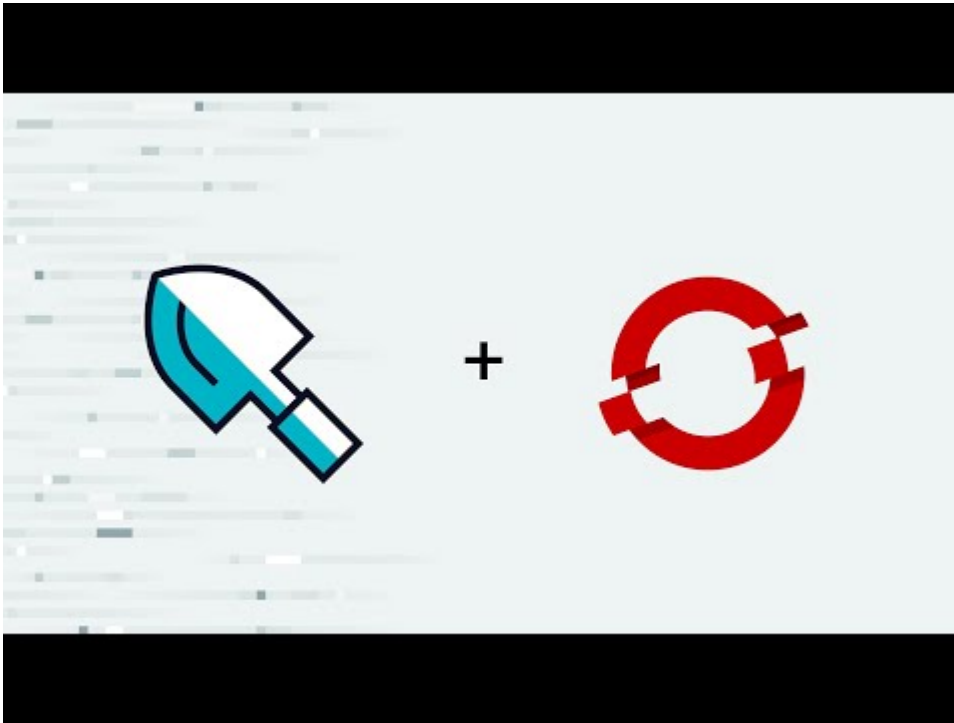
facebook.com/redhatinc  
@redhat  
linkedin.com/company/red-hat

redhat.com

1

[SOLUTION BRIEF: Sysdig & Red Hat Securing Cloud Applications for Financial Services Companiespdf](#)

[Cloud SecurityRed HatSysdig Secure](#)



[VIDEO. Cloud-native security with OpenShift and Sysdig Secure](#)

[OpenShift Red Hat Sysdig Secure](#)



# Detect threats in real time with Falco on AWS

The ultimate line of defense is runtime security

Falco is the open source runtime security solution for threat detection across containers, hosts, Kubernetes and the cloud.

## Container Security

Secure containerized applications, no matter what scale, using the power of eBPF.

## Host Security

Protect your applications in real time wherever they run, whether bare metal or VMs.

## Kubernetes Security

Falco is Kubernetes-compatible, helping you instantly detect suspicious activity across the control plane.

## Cloud Security

Detect intrusions in real time across your cloud, from AWS, GCP or Azure, to Okta, Github and beyond.

## Use Falco to protect your apps at runtime

Falco gives you real-time visibility into unexpected behaviors, config changes, intrusions, and data theft. Falco makes it easy to consume Linux kernel syscalls, and enrich those events with information from Kubernetes and the rest of the cloud native stack. Falco has a rich set of out of the box security rules specifically built for Kubernetes, Linux and the cloud.

- Threat detection for your workloads and cloud infrastructure
- Highly scalable, with containerized architecture and Kubernetes integration
- Performant and low-latency due to a low overhead, streaming event architecture
- Richly connected to a growing ecosystem of plugins and integrations
- Works out-of-the-box, but is highly customizable thanks to a single policy language

[BRIEF. Detect threats in real time with Falco on AWSpdf](#)

[AWS Cloud Security Sysdig Secure Falco](#)



[VIDEO. Securing and Monitoring AWS Container Services](#)

[AWS Cloud Security Sysdig SecureCloud Monitoring](#)



[GUIDE. Cloud Security for AWSpdf](#)

[AWS Cloud Security Sysdig Secure Cloud Monitoring](#)



[VIDEO. ATPCO on deploying Red Hat OpenShift + Sysdig visibility and security platformvideo](#)

[Openshift Red Hat Sysdig Secure Sysdig Monitor](#)

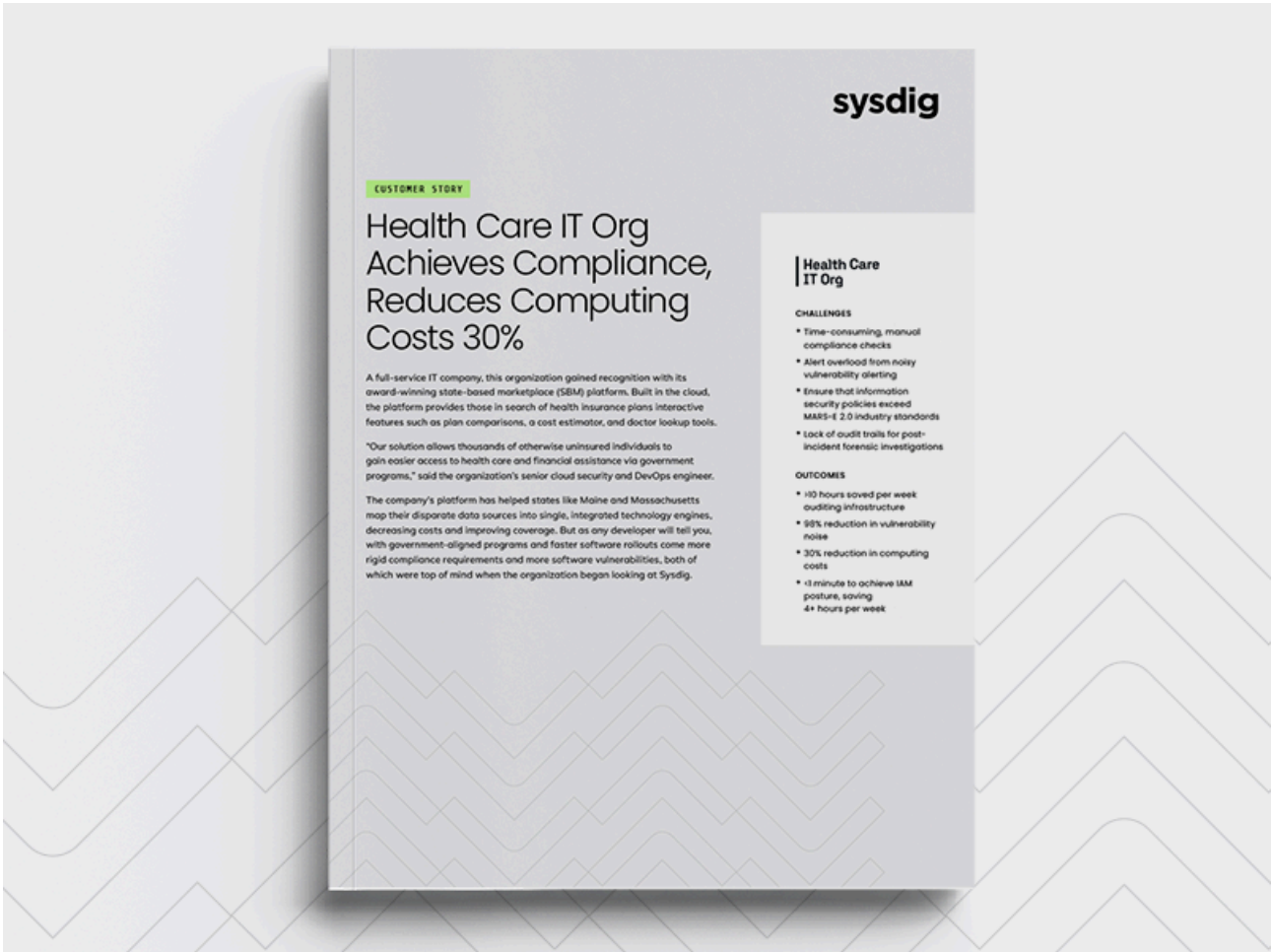


# Innovate at Scale with Runtime Insights and a Security Data Lake

Sysdig Secure and Amazon Security Lake provide a  
modern foundation for securing your cloud estate

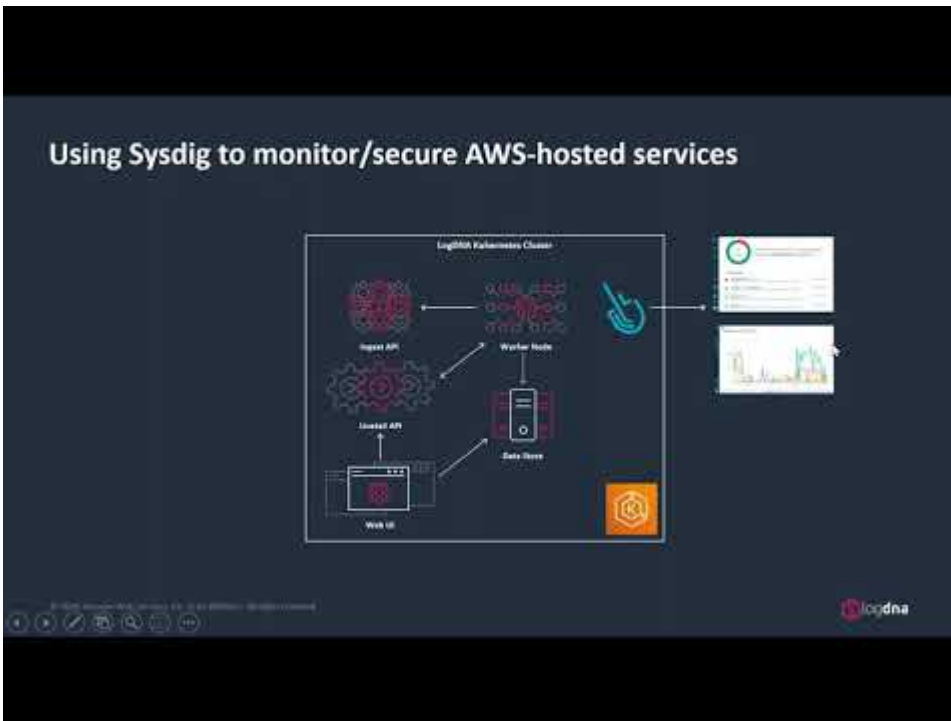
[GUIDE. Sysdig AWS Security Lakepdf](#)

[AWS Cloud Security Sysdig Secure Cloud computing security](#)



[CASE STUDY. Health Care It Orgpdf](#)

[AWS Cloud Security Sysdig Secure Amazon Web Services](#)



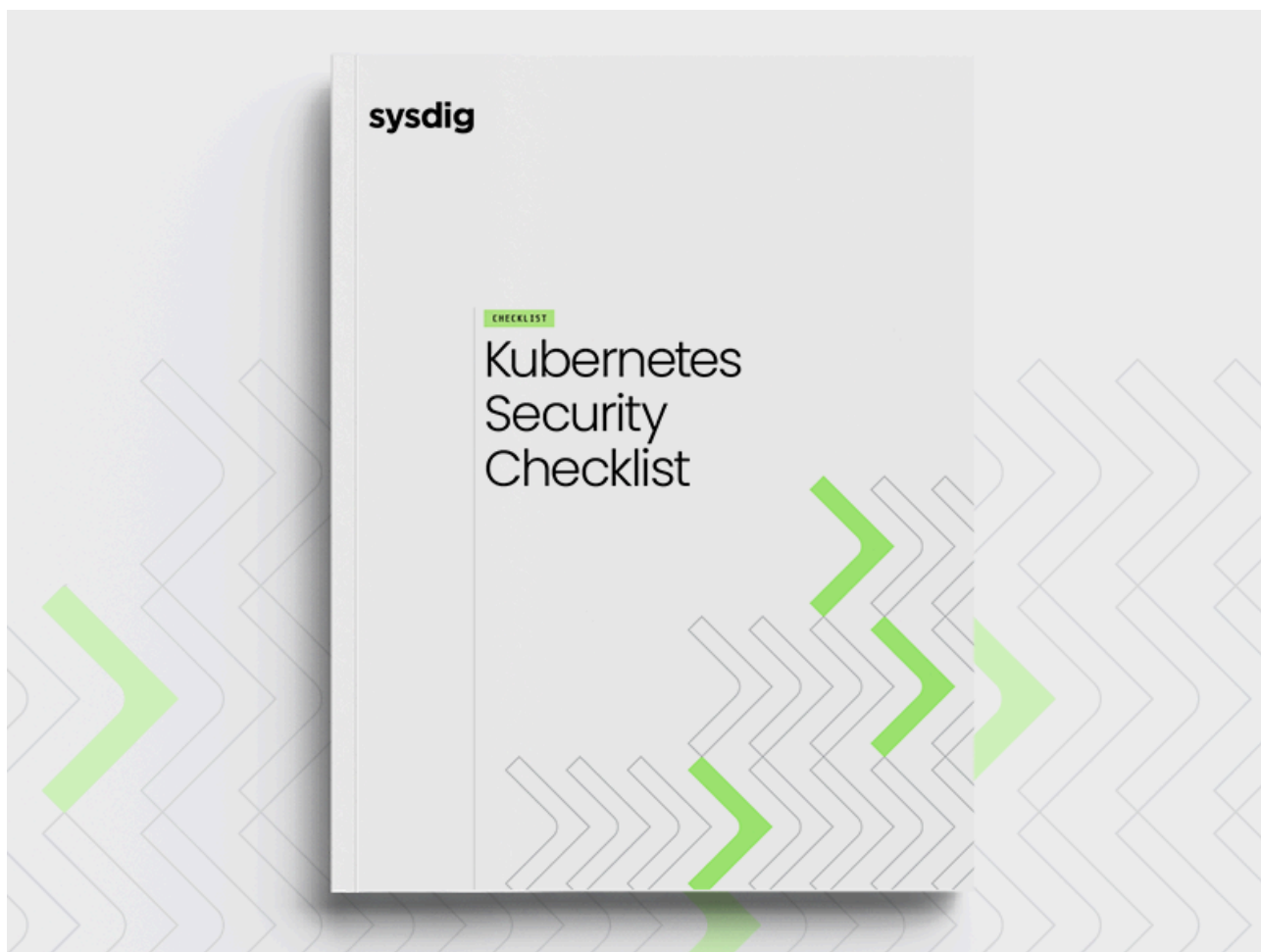
[WEBINAR. LogDNA - Monitoring and Securing Containers on AWS EKS with Sysdigvideo](#)

[AWS Cloud Security Sysdig SecureCloud Monitoring](#)



[WEBINAR. Automating Container Visibility to Accelerate App Deliveryvideo](#)

[Cloud Security Openshift Red Hat Cloud Monitoring](#)



[GUIDE. Kubernetes Security Checklistpdf](#)

[Cloud SecuritySysdig SecureKubernetes](#)



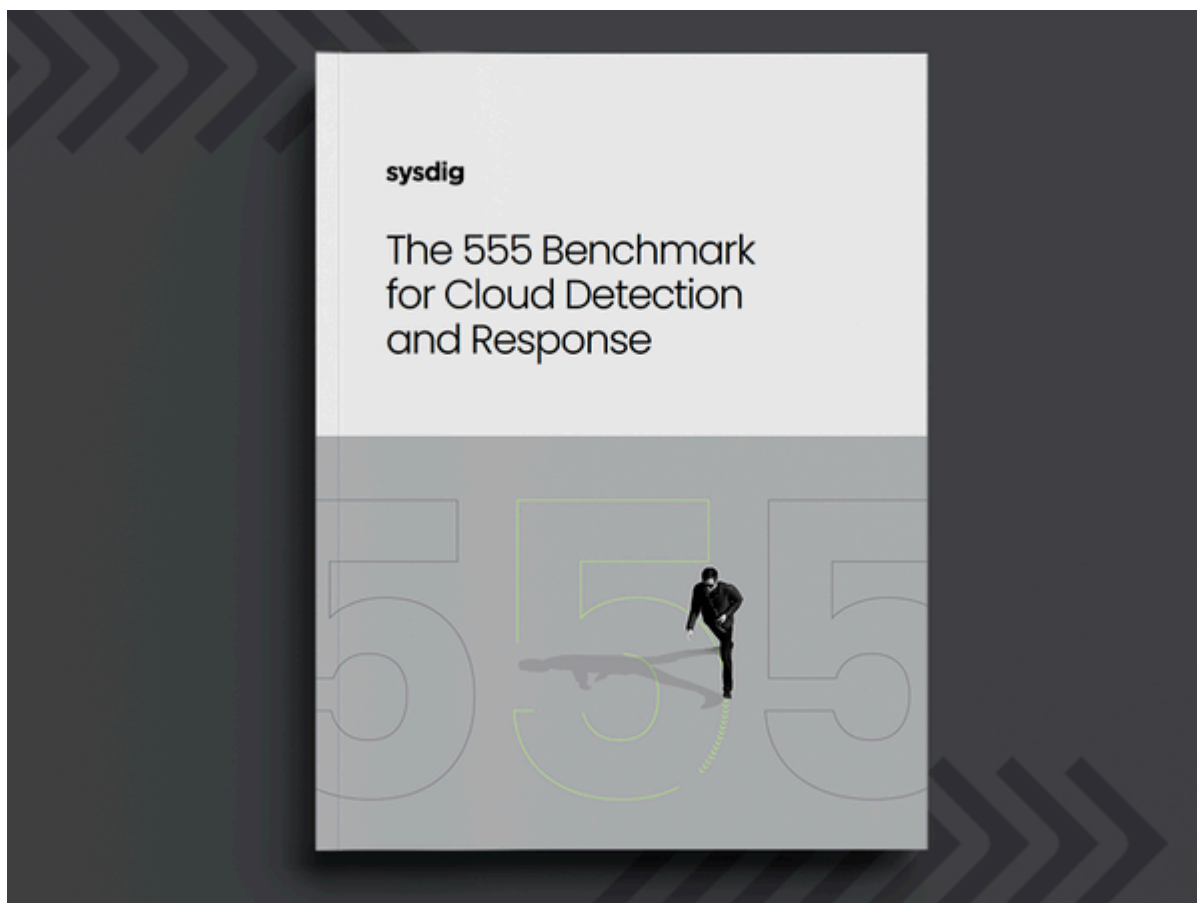
# Sysdig 2021 Container Security and Usage Report

---



[REPORT. 2021 Container Security And Usage Reportpdf](#)

[Cloud SecuritySysdig SecureCloud MonitoringKubernetes](#)



[BRIEF. The 5/5/5 Benchmark for Cloud Detection Responsepdf](#)

[Cloud SecuritySysdig SecureCloud computing security.](#)



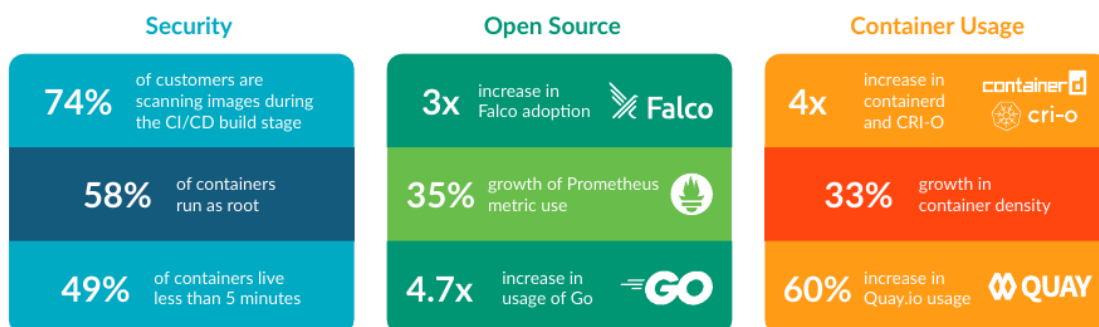
## 2021 Container Security and Usage Snapshot

Shifting left is not enough!  
Doors are still being left open.



In 2020, we saw an acceleration of cloud adoption that led to an increase in container usage. This increase, combined with the fact that half of containers live less than five minutes, reinforces the need to manage container-specific security risks. A majority of our customers scan images during the build stages, but we still see risky configurations. To run container applications with confidence, it's important to address configuration risk, detect runtime threats, and ensure that a detailed recording of container activity is available for incident response and forensics. As we have done the past four years, we are sharing critical annual insights from real-time, real-world usage of nearly 1 billion unique containers that our customers have been running in our environment over the past year. Our goal is to shed light on the current state of container infrastructure, applications, security, and compliance practices.

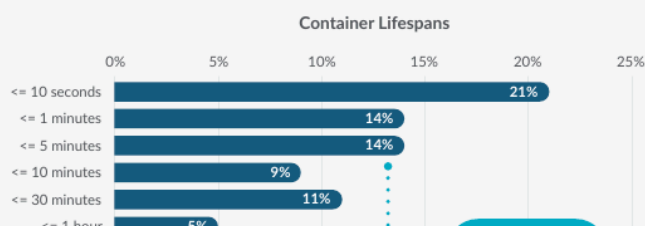
### Key 2021 Trends



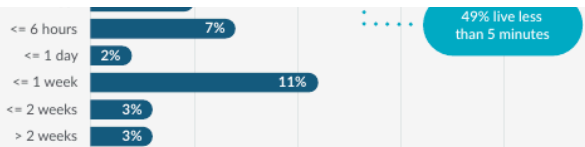
#### Container Security

### Why Shift Left: The Short Life of Containers

Containers have a short-life and need specific security implications. 49% of



containers continue to be alive for less than five minutes. The ephemeral nature of containers remains one of the technology's unique advantages, but presents new issues to consider for security and compliance.

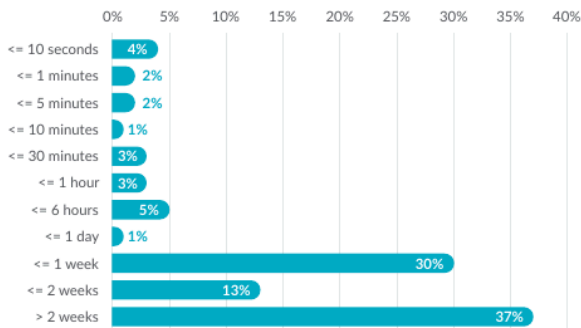


Container Security

### Container Image Churn

Half of the container images are replaced – also known as churn – in a week or less. Automating scanning in CI/CD pipelines and registries can help developers deliver code faster, turning great ideas into reality faster, with more new images, more often, while managing the security risk.

Container Image Lifespans



Images Pulled from Public vs. Private Registries



Container Security

### Public vs. Private Images

With more containers and more churn, new security tools and processes are needed to keep up. We found that 47% of images are pulled from public sources. The risk? Few are checked for security vulnerabilities. Docker Hub, for example, certifies less than 1% of its nearly three million hosted images.

“A manual image scan could take 10 minutes per check-in. With Sysdig, all of that just becomes automatic as part of the pipelines as the team is doing their deployments. Today, we handle thousands of merges per day. If you consider each could take 10 minutes on average and multiply that by thousands a day, we wouldn't be able to operate close to the same speed without Sysdig.”

- SAP Concur

Container Security

### Image Scanning

Preventing vulnerabilities in production requires image scanning. Pass and fail rates for images scanned over a five-day period reveal that over half of images have known vulnerabilities with a severity of high or greater.

Scanning Results  
Median of Containers Scanned



### OS Vulnerabilities by Severity



### Container Security

## OS Vulnerability Snapshot

We noticed that four percent of OS vulnerabilities are high or critical. Although this may seem low, if an OS vulnerability is exploited, it can compromise your entire image and bring down your applications.

### Container Security

## Non-OS Vulnerability Snapshot

Non-OS vulnerability snapshot: Many teams don't check for vulnerabilities in third-party libraries. We found that 53% of non-OS packages have high or critical vulnerabilities. Developers might be unknowingly pulling in vulnerabilities from non-OS open source packages, like Python PIP, Ruby Gem, etc., and introducing security risk.

### Non-OS Vulnerabilities by Severity



### Container Security

## How Common Are Risky Configurations?

While teams understand the need to scan for vulnerabilities, they may not be scanning for common configuration mistakes. What we see is that 58% of images are running as root, leaving an opening for an attacker to execute malicious processes inside the container.

From talking to our customers, in practice, even if risky configurations are detected at build time, teams don't stop containers from moving to production. Instead, they allow a grace period to fix the issue and continuously monitor for suspicious behavior, in order to continue deploying quickly.



### Open Source Software Gains Momentum

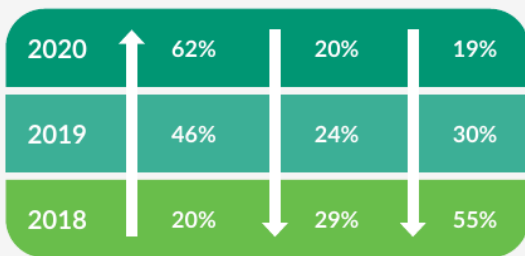
## Falco Adoption Grows Over 3X

Runtime security detects anomalous behavior

### Growth of Falco



in production as a last layer of defense. Falco, the CNCF open-source project contributed by Sysdig, creates runtime policies, detects security violations and generates alerts. Falco is quickly gaining momentum, with adoption increasing by 300 percent over last year.



Metric types in use on average

Open Source Software Gains Momentum

Prometheus Gains Dominance

Custom metric solutions give developers and DevOps teams a way to instrument code to collect unique metrics. Of the three mainstay solutions, JMX, StatsD, and Prometheus, Prometheus metric use increased 35% YoY across our customers – with over 60% of our customers using it.

Open Source Software Gains Momentum

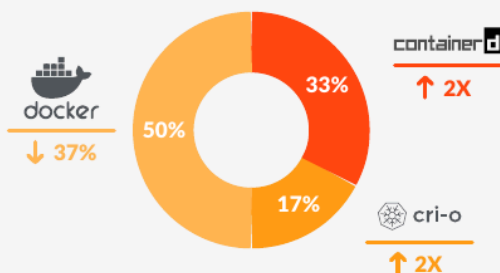
Top 3 Open Source Technologies Deployed by Sysdig Customers

Go is going places!



“ We can tell our developers to emit metrics with Prometheus. You won't have to think about it. They'll just show up in Sysdig .”

- COTA Healthcare



Container Usage

Container Runtimes: Containerd and CRI-O Usage Grows 4x

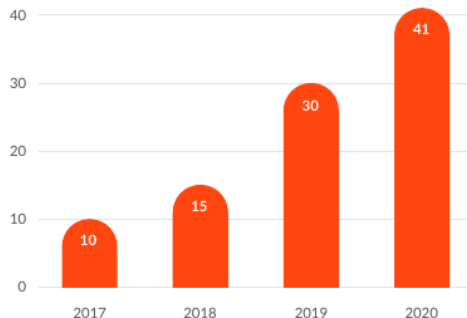
Over the past year, we have seen significant growth for both containerd and Red Hat created CRI-O, both of which were recently adopted by the CNCF in 2019. To be fair, it's important to note that containerd is used by Docker.

Container Usage

## Container Density Per Host Grows 33%

This year, container density grew 33% year-over-year compared with the 100% increase from last year. While the primary goal of containers is to speed development and deployment, many organizations are benefiting from increased utilization of hardware resources due to container efficiencies.

Median Containers per Host



A majority of our customers are scanning images during the build stages, but still see risky configurations. This validates the need to continuously scan images in the registries and at runtime to protect against vulnerabilities. Addressing runtime security, mitigating configuration risks, and capturing container activity for incident response and forensics is essential for securely operating container applications with confidence.

Open source is growing as a core component in Kubernetes environments. The growth of Falco, Prometheus, and Go demonstrate the need for open source solutions to solve the critical problems of securing and monitoring containers.

“With the audit log inside our S3 buckets, we can just go back and see what happened in the event of an attacker coming into the platform. We can also see if they took anything or how they gained access. Having this information saves so much time, because without the audit trails, how do you know what happened? Other solutions do not offer this. Beyond that, Sysdig will help identify who needs to be notified and with lessons learned from the configurations.”

- Worldpay

Learn even more about the dynamics of container usage, security, and compliance in the Sysdig 2021 Container Security and Usage Report.

[GET THE FULL REPORT NOW](#)



Copyright © 2021 Sysdig, Inc. All rights reserved. ING-008 Rev. A 1/21.

[INFOGRAPHIC. 2021 Container Security and Usage Snapshotpdf](#)

[Cloud SecuritySysdig SecureCloud MonitoringKubernetes](#)



## Sysdig 2022 Cloud-Native Security and Usage Report

Everyone is trying to shift left, but the reality is  $\frac{3}{4}$  of running containers have at least one "high" or "critical" vulnerability.

Meanwhile, many companies adopt cloud for operational efficiency, but more than half of containers deployed have no limits, which could waste resources.



[REPORT. 2022 Cloud-Native Security And Usage Reportpdf](#)

[Cloud SecuritySysdig SecureCloud MonitoringKubernetes](#)



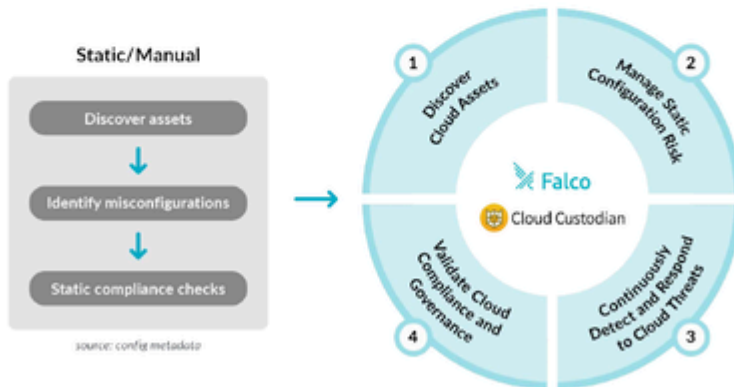
## Continuous Cloud Security Checklist for Google Cloud

As cloud adoption accelerates, there is a growing need to manage security risks within these dynamic environments. With cloud architectures, organizations can be overwhelmed by the sheer number of services they need to secure. A single misconfiguration in a cloud service can lead to a serious data breach. The reality is that human errors are impossible to avoid.

According to Gartner, "Nearly all successful attacks on cloud services are the result of customer misconfiguration and mistakes." Gartner also predicts that through 2023, at least 99 percent of cloud security failures will be the customer's fault.<sup>1</sup>

Imagine a scenario where one of your critical cloud services suddenly stops working. A DevOps engineer investigates and after a few hours of work, discovers unplanned firewall rule changes were made, one of which triggered the service outage. How can you keep track of constant additions and changes to your services on Google Cloud? How can you flag misconfigurations and suspicious activity while focusing on alerts that signal a real threat?

Tackling these unique cloud security risks requires a continuous and automated approach. Our Continuous Cloud Security checklist outlines how you can better manage cloud security risk on Google Cloud.



<sup>1</sup> Gartner: Innovation Insight for Cloud Security Posture Management

[GUIDE. Continuous Cloud Security Checklist For Google Cloudpdf](#)

[Cloud SecuritySysdig\\_Secure](#)

**sysdig**



CHECKLIST

## Sysdig vs. Wiz

### Holistic Visibility With Real-Time Cloud Security Powered By Runtime Insights

Don't be deceived by an attractive user interface. Tools like Wiz lack the ability to fully comprehend what's in use, leading to challenges in proper risk prioritization and actionable remediation with runtime context. Wiz also struggles to identify and respond to cloud and container threats while lacking the necessary runtime context for prioritizing vulnerabilities effectively.

#### Why Customers Choose Sysdig

Sysdig leverages runtime insights to detect threats in real time and surface rich context to respond immediately. This unique runtime visibility enables Sysdig to detect threats in under two seconds and reduce vulnerability noise by 95% with an in-use exposure filter. Solutions like Wiz lack this runtime visibility to prioritize and address the most significant risks.

With Sysdig, you can:

- ✓ Prioritize risks with our real-time detection and runtime insights.
- ✓ Get comprehensive end-to-end security in cloud environments.
- ✓ Leverage a Cloud Attack Graph powered by runtime insights.

[GUIDE. Container and Cloud Security Comparison Checklist: Sysdig vs Wizpdf](#)

[Cloud SecuritySysdig SecureRegulatory Compliance](#)



## Get the SaaS Advantage for Secure DevOps

---

To meet the demands of dynamic cloud-native environments and digital business, visibility and security solutions are increasingly moving to the cloud. From endpoint detection and response (EDR) to network security and monitoring, cloud-based software-as-a-service (SaaS) solutions enable enterprises to break free from hardware dependency and instantiate services wherever required from the data center, to the public cloud, and out to the edge.

The Sysdig Secure DevOps Platform is a SaaS-first solution, purpose-built to deliver cloud-based security and monitoring for containers and Kubernetes. Our solution is more than just a hosted single-tenant instance in the cloud. It is designed to address the unique needs of cloud teams who need to get started quickly with secure DevOps across diverse locations and infrastructures. With Sysdig, you can easily integrate image scanning, runtime security, compliance, monitoring, and forensics while increasing your efficiency and reducing costs so you can focus on delivering great software.

This overview highlights the advantages of SaaS, providing insight into the operational controls and practices of the Sysdig SaaS solution designed to help you securely and efficiently implement cloud-native security and monitoring.



[GUIDE. Get the SaaS Advantagepdf](#)

[Cloud SecuritySysdig\\_SecureCloud MonitoringKubernetes](#)

**sysdig**

TWENTY23

# GLOBAL CLOUD THREAT REPORT

Attacks in the cloud are lighting-fast, with minutes determining the line between detection and severe damage.

**1**

## Cloud Automation Weaponized

Reconnaissance alerts: attack incoming

Cloud attacks happen fast. Recon and discovery are even faster. Automating these techniques allows an attacker to act immediately upon finding a gap in the target system. A recon alert is the first indication that something is awry; a discovery alert means you're too late.

**2**

## 10 Minutes to Pain

Every minute second counts

Cloud attackers are quick and opportunistic, spending only 10 minutes staging the attack. According to [Mandiant](#), the median dwell time on premises is 16 days.

00:00  
FOUND  
CREDENTIAL

00:05  
ALERTS  
FOR RECON

00:10  
ATTACK!

[BRIEF. 2023 Global Cloud Threat Report Exec Summary.pdf](#)

[Cloud SecuritySysdig\\_Secure](#)



[BRIEF. 2024 Cloud Native Security And Usage Report Exec Summary.pdf](#)

[Cloud Security Sysdig SecureCloud computing security](#)



[CASE STUDY. BigCommerce Achieves Real-Time Cloud Securitypdf](#)

[Cloud SecuritySysdig SecureCloud computing security](#)

Forrester Report Prepared For Alexis Bouffard With Forrester

# Now Tech: Cloud Workload Security, Q3 2021

## Forrester's Overview Of 23 Cloud Workload Security Providers

August 2, 2021

By Andras Cser with Merritt Maxim, Alexis Bouffard, Peggy Dostie

FORRESTER

### Summary

You can use cloud workload security (CWS) to govern and protect cloud workloads at all levels, including: 1) cloud service provider (CSP) console; 2) virtualization hypervisor; 3) guest operating system (OS); 4) container and container orchestration layer; and 5) serverless functions. But to realize these benefits, you'll first have to select from a diverse set of vendors that vary by size, functionality, geography, and vertical market focus. Security and risk (S&R) professionals should use this report to understand the value they can expect from a CWS provider and to select one based on size and functionality.

Not Licensed For Distribution.

© 2021 Forrester Research, Inc. All trademarks are property of their respective owners. For more information, see the [Citation Policy](#), contact [citations@forrester.com](mailto:citations@forrester.com), or call +1 866-367-7378.

1

[REPORT. Forrester Now Tech Cloud Workload Security Q3 2021.pdf](#)

[Cloud SecuritySysdig Secure](#)



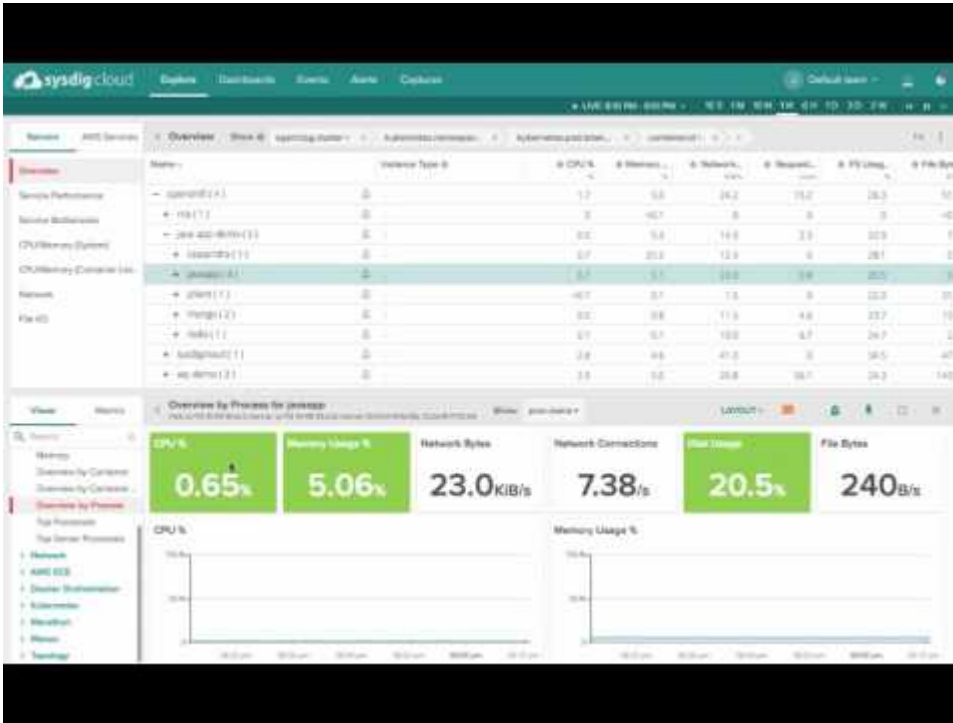
[WEBINAR: Moving Apps to the Cloud? How Top Financials Reduced their Security & Compliance Risk](#)

[Cloud SecurityRed HatCloud Monitoring](#)



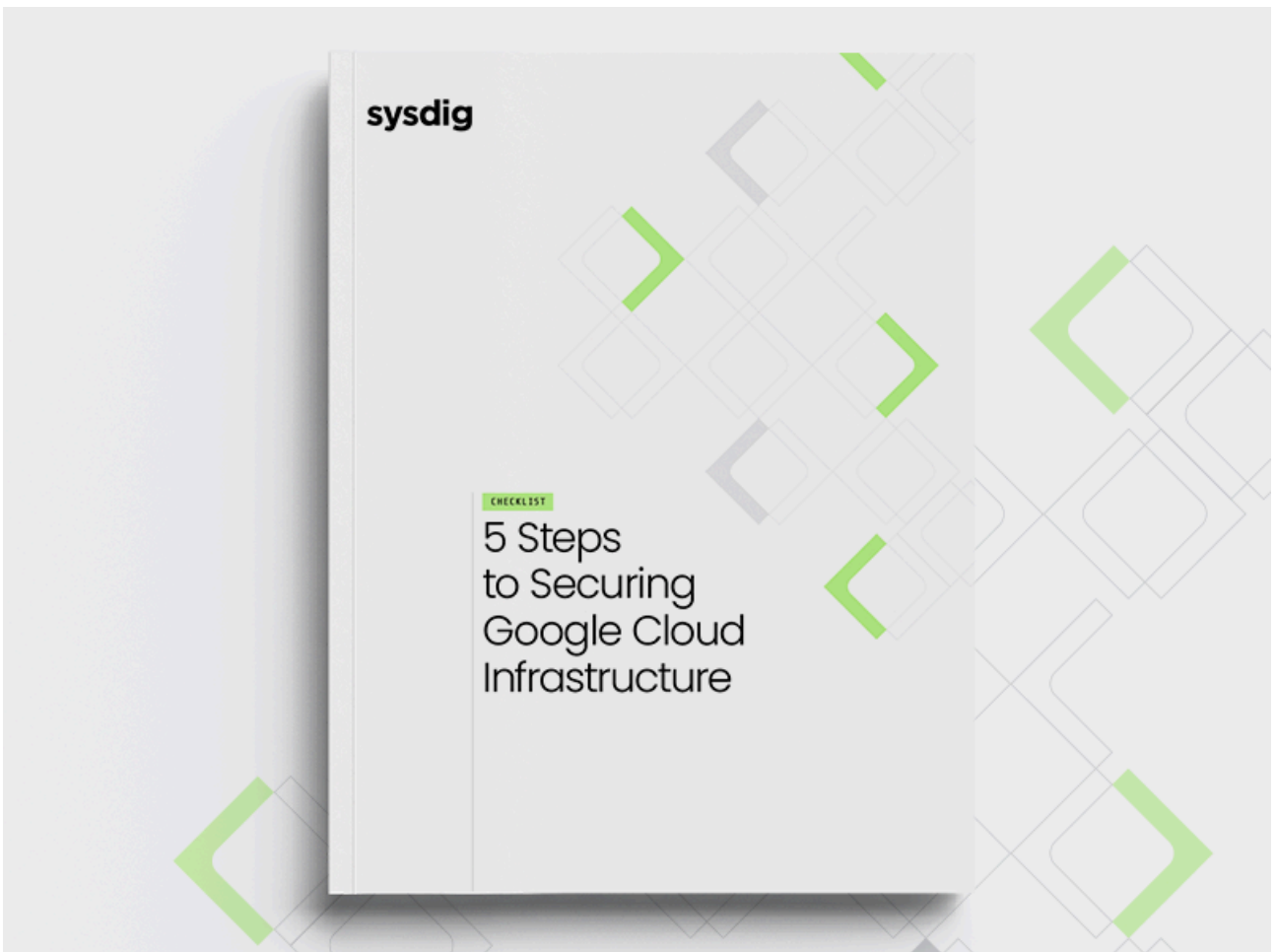
[VIDEO NL. Bereid je voor op de volgende log4j!](#)

[Cloud SecuritySysdig Secure](#)



[VIDEO. Openshift Monitoring with Sysdigvideo](#)

[OpenshiftRed HatSysdig Monitor](#)



[GUIDE. 5 Steps To Securing GCP Cloud Infrastructurepdf](#)

[Cloud SecuritySysdig Secure](#)



## 5 Best Practices for Securing Cloud and Containers in Financial Services

As cloud migration picks up pace in the financial services sector, DevSecOps teams face new challenges. How do you meet stringent security and compliance requirements while working within the complex and nebulous boundaries of cloud and container environments? And how do you balance this with ongoing talent shortages and business pressure to bring products to market fast?

If you're struggling with visibility into your cloud infrastructure, you're not alone. Containers are essentially black boxes. It's hard to see what's going on inside, and the lifespan of a container is very short: in fact, [72% of containers now live less than five minutes](#), according to Sysdig research. Traditional security tools can't see inside containers, handle the dynamic nature of Kubernetes, or scale across multi-cloud deployments. Proprietary security tools can't keep up with the standardization and speed of innovation possible with open-source software.

The solution is tools and security platforms that work together, built on open standards so that they can be customized to the compliance demands of financial services, with vulnerability prioritization to help you spend less time resolving security alerts, and more time on business-critical activities.

Here are five key workflows that will enable you to cover the most critical security and visibility requirements so you can confidently run containers, Kubernetes, and cloud.



[GUIDE. 5 Best Practices for Securing Cloud and Containers in Financial Servicespdf](#)

[Cloud SecuritySysdig Secure](#)

The graphic is a white rectangular brief titled "Sysdig for Amazon Web Services". At the top left, it says "BRIEF". The main title is "Sysdig for Amazon Web Services". Below the title is a sub-headline: "Sysdig's CNAPP protects AWS, hardening security posture and detecting attacks immediately." To the right of this sub-headline is a green button that says "LEARN MORE →".

Below the sub-headline is a paragraph: "10 minutes is all it takes to execute an attack in the cloud after discovering an exploitable target. Outpacing attackers in the cloud requires security teams to meet the 5/5/5 Benchmark. That means five seconds to detect, five minutes to triage, and five minutes to respond to threats. Sysdig's Cloud Native Application Protection Platform (CNAPP) helps AWS customers meet this benchmark's expectations, thus securing and accelerating their cloud innovation."

The central part of the graphic is a diagram. On the left, there are two columns of AWS services. The first column is titled "AWS Services" and lists: Amazon S3, AWS IAM, Amazon CloudWatch, AWS CloudTrail, Amazon CloudFront, and Amazon CloudSearch. The second column is titled "Workloads" and lists: AWS Lambda, Amazon EC2, Amazon ECS, Amazon EKS, Amazon EMR, Amazon Redshift, Amazon SageMaker, Amazon Q, Amazon AppStream, and Amazon WorkSpaces. Arrows from these lists point to a central green box labeled "sysdig CNAPP". Inside this box, there are three sub-sections: "CDR" (Cloud Drift Reporting), "CSPM" (Cloud Security Posture Management) with "CEM, VM etc" below it, and "CWPP" (Cloud Workload Protection) with "CEM, VM etc" below it. To the right of these sub-sections is a screenshot of the Sysdig dashboard showing a line graph and a table.

Below the Sysdig box is a section titled "Events, Alerts and Notifications". It shows icons for various AWS services: Amazon Security Lake, Amazon S3, Amazon S3, Amazon S3, Amazon S3, Webhooks, AWS IAM, and Notification Channels.

At the bottom of the graphic is a section titled "Customer Highlights". It features logos for: worldpay (From FIS), FINRA, Goldman Sachs, bloomreach, IBM, Arkose Labs, COMCAST, AUTOCOMMERCE, Alaska AIRLINES, and Colendy.

[PARTNER BRIEF. Sysdig and Amazon Web Servicespdf](#)

[AWS Cloud Security](#)



[WHITEPAPER: Cybersecurity Regulations Guidancepdf](#)

[Cloud SecuritySysdig SecureCloud computing security.](#)

SANS

Analyst Program 

Whitepaper

---

# A Comprehensive Approach to Cloud Threat Detection and Response

Written by [Jake Williams](#)

June 2022



©2022 SANS™ Institute

[WHITEPAPER. A Comprehensive Approach to Cloud threat Detection and Responsepdf](#)

[Cloud SecuritySysdig\\_Secure](#)



[VIDEO. Sysdig + Red Hat partnership: OpenShift visibility and securityvideo](#)

[OpenshiftRed Hat](#)



[VIDEO. Secure DevOps practices at Yahoo! Japanvideo](#)

[Cloud SecuritySysdig SecureKubernetes](#)



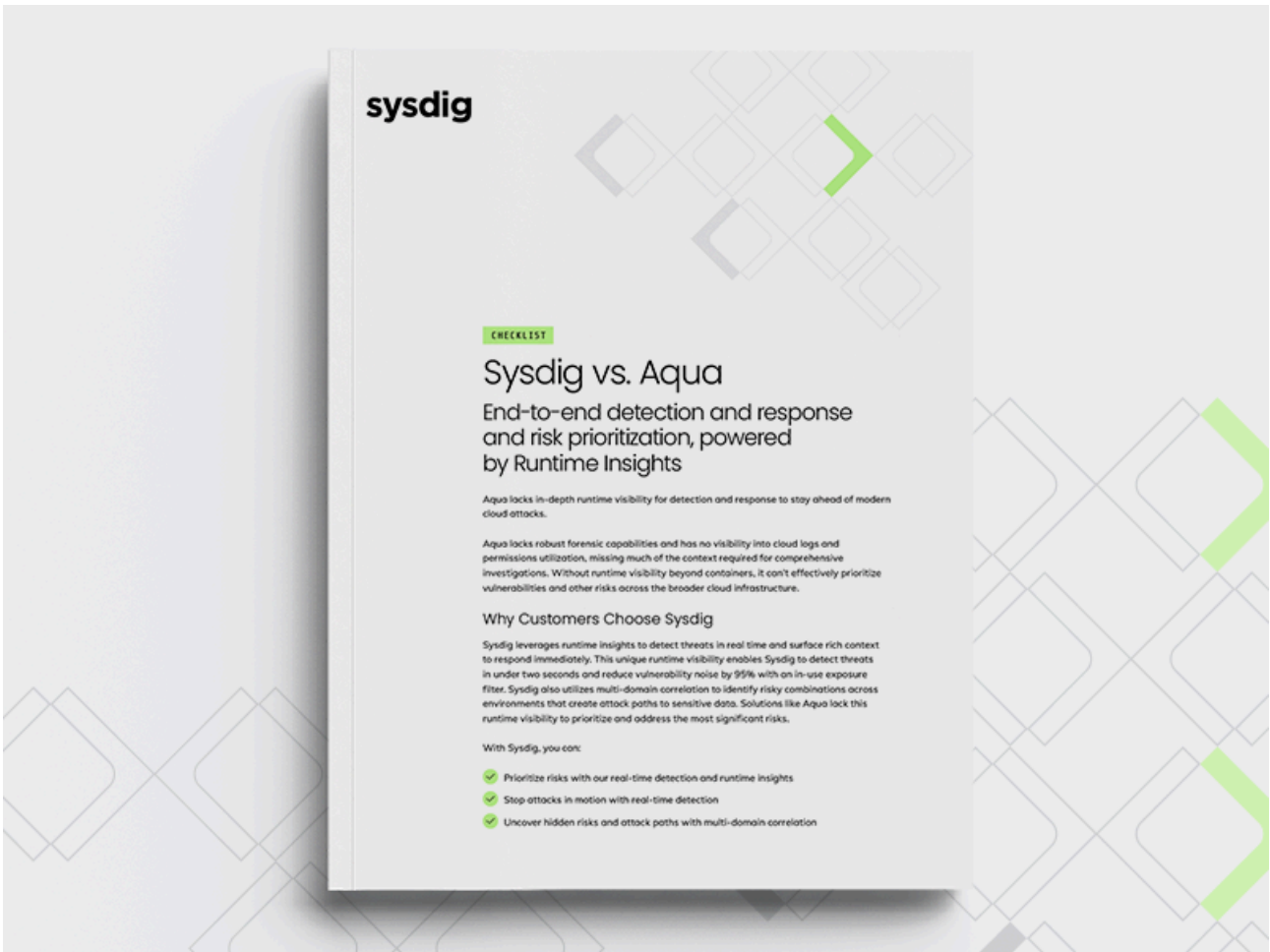
# NIST 800-53 Compliance for Containers and Cloud

---



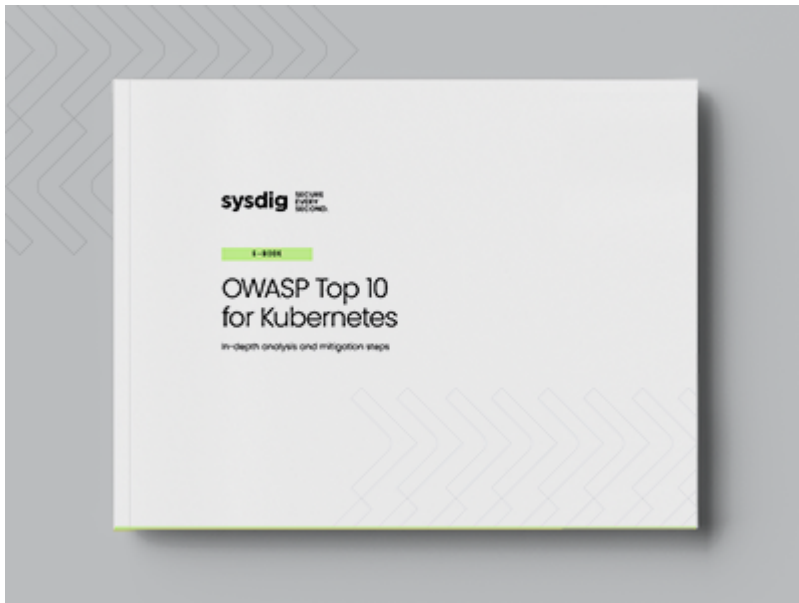
[GUIDE. NIST 800-53 Compliance for Containers and Cloudpdf](#)

[Cloud SecuritySysdig\\_SecureRegulatory\\_Compliance](#)



[GUIDE. Container Security Comparison Checklist: Sysdig vs Aqua Security.pdf](#)

[Cloud Security Sysdig Secure](#)



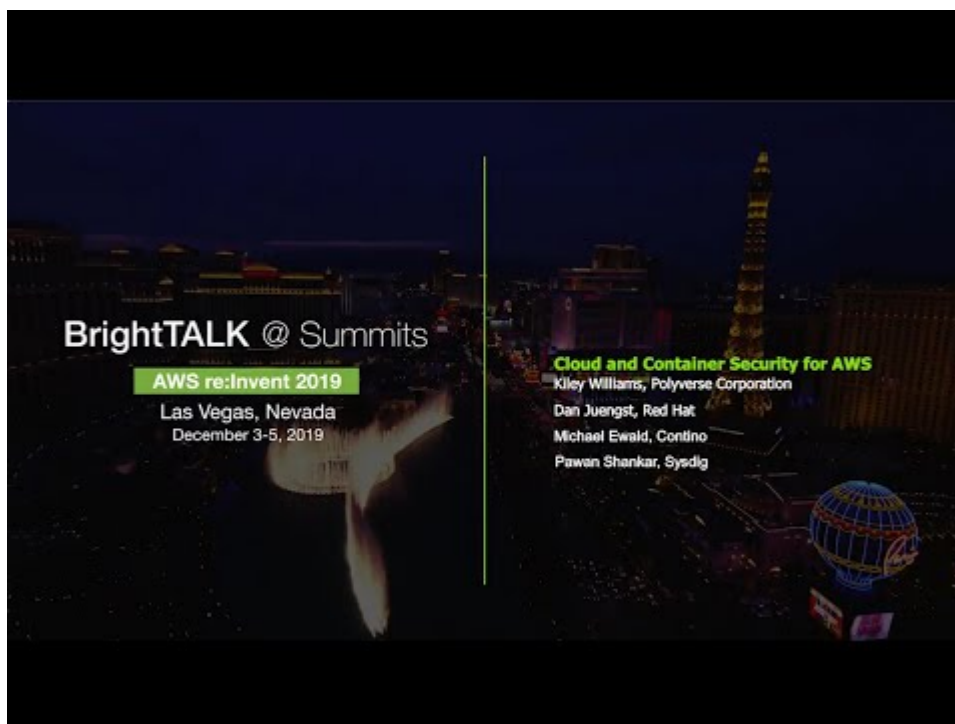
[GUIDE. OWASP Kubernetes Top 10: Mitigating Risks in Cloud-Native Environmentspdf](#)

[Cloud SecuritySysdig SecureKubernetes](#)



[WEBINAR. Automating Security for DevOps Workflowsvideo](#)

[Cloud SecuritySysdig Secure](#)



[WEBINAR. Cloud and Container Security for AWS](#)video

[AWS Cloud Security Kubernetes](#)



## Container and Cloud Security Comparison Checklist: Sysdig vs. CheckPoint CloudGuard

### 55 features compared



Don't rely on a tool that brings a firewall mindset to the cloud. Tools like CheckPoint CloudGuard lack the visibility to accurately detect and respond to vulnerabilities and threats across containers and clouds. Choose a security stack that is:

- Built on open source
- SaaS first
- Instrumented to provide deep visibility with rich context across containers, Kubernetes, and cloud

Run confidently with secure DevOps.

This checklist provides a feature comparison across container and cloud security between Sysdig Secure and CheckPoint CloudGuard.

#### Coverage Areas

- Platform
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection (CWPP)
- Image Scanning
- Runtime Security
- Network Security
- Incident Response and Forensics
- Compliance



[GUIDE. Container & Cloud Security Comparison Checklist: Sysdig vs CheckPoint CloudGuardpdf](#)

[Cloud SecuritySysdig Secure](#)



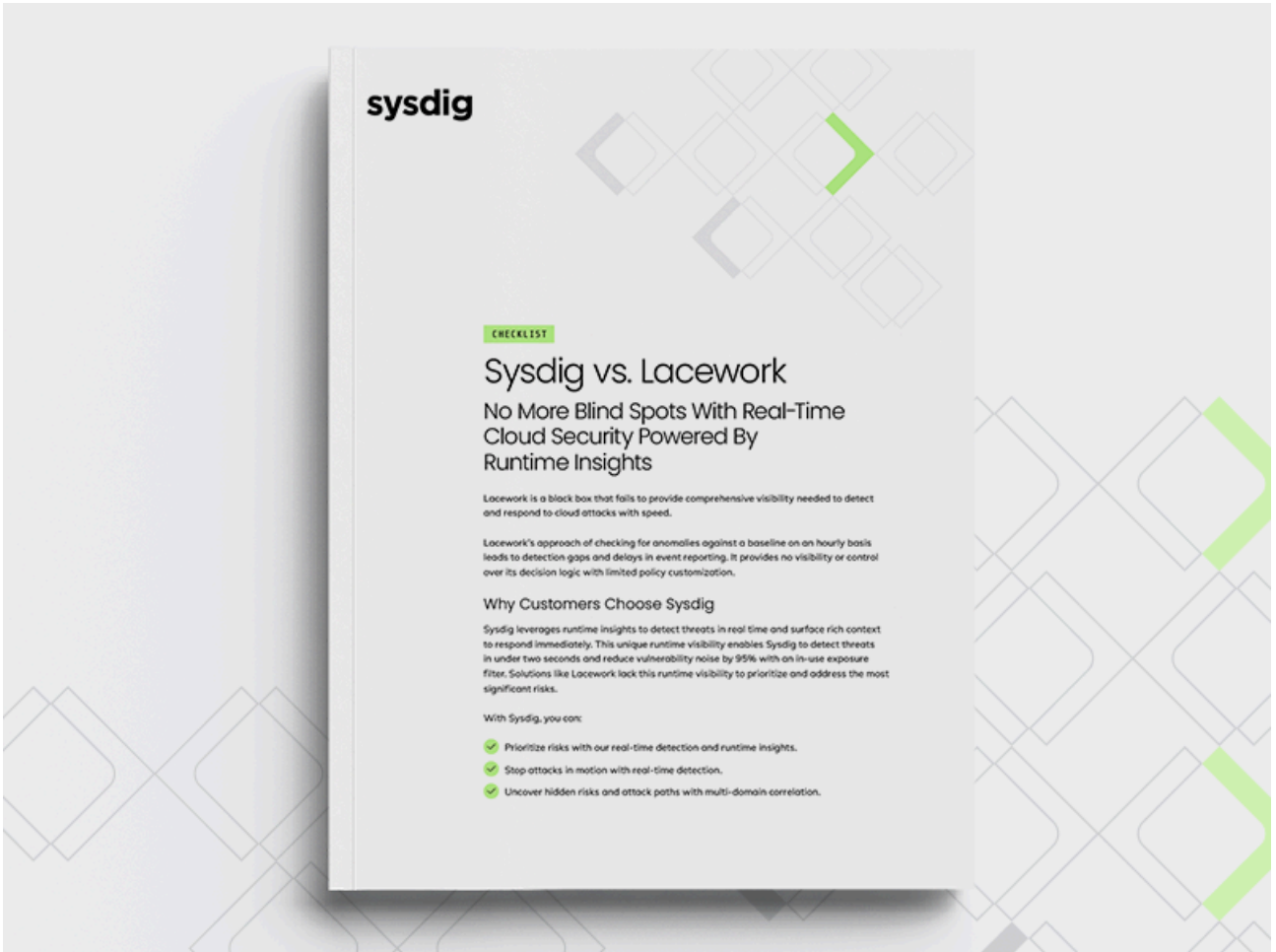
[BRIEF. 2024 Global Threat Executive Summarypdf](#)

[Cloud SecuritySysdig Secure](#)



[Customer Corner: How BigCommerce Achieved Real-Time Cloud Securityvideo](#)

[Cloud SecuritySysdig SecureCloud computing security.](#)



[GUIDE. Container Security Comparison Checklist: Sysdig vs Laceworkpdf](#)

[Cloud SecuritySysdig SecureRegulatory Compliance](#)



[VIDEO. Strengthening Your Security with Agentless Vulnerability Management](#)[video](#)

[Cloud Security](#)[Sysdig Secure](#)[Cloud computing security](#)

**sysdig**

WHITE PAPER

# Securing the Cloud with End-to-End Detection



**READ MORE →**

[WHITEPAPER. Securing the Cloud with End-to-end Detection](#)[pdf](#)

[Cloud Security](#)[Sysdig Secure](#)



[PODCAST. Red Hat X Podcast – May 5, 2020webpage](#)

[OpenshiftRed Hat](#)



[WHITEPAPER. Runtime Insights Are Key To Shift Left Securitypdf](#)

[Cloud SecuritySysdig Secure](#)

# 2018 Docker Usage Report

An inside look at shifting container usage trends.

## Sample size.

Our sample size doubles year-over-year to 90,000 containers.

The data is collected from a segment of containers under management in our [Sysdig Monitor](#) and [Sysdig Secure](#) cloud service. Real users. Real data. Real world.

# 90,000

## Top 12 app components.

The old merges with the new.



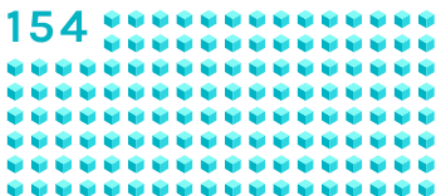
Customers are consistently utilizing open source solutions to construct their microservices and applications. At the top of the list is use of [Java](#) [Virtual Machines](#) (JVM). Increased usage of database solutions like PostgreSQL and MongoDB signal a move to stateful services in containers.

## Container density rising

Density rises 50% year-over-year.

Compared to our [2017 report](#), the median number of containers per host per customer climbed 50%, from 10 to 15. Organizations deliver a larger number of application services from the same hardware, reducing Capex and Opex costs.





### At the other end of the spectrum...

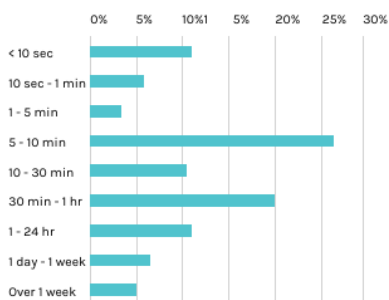
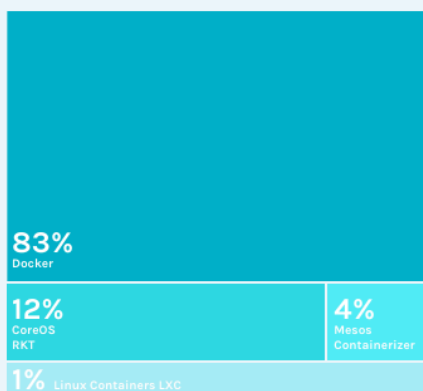
We observed density as high as 154 containers on a single host.

Up from a maximum of 95 in 2017.

### What container runtimes are in use?

Docker reigns, but are we seeing cracks in the dam?

[Docker](#) shows up most in production, but customers appear to have a greater comfort level using non-Docker solutions in production. Use of other platforms, which amounted to less than 2% in 2017, increased significantly. CoreOS rkt grew to 12%, Mesos containerizer to 4%, and LXC grew to 1%.



### What is the lifespan of containers and services?

95% of containers live less than a week.

Eleven percent of containers stay alive for less than 10 seconds. 27% of containers churn between five to 10 minutes. Why so short? Systems scale as needed with demand and live only as long as they add value. Containers are created, do their work, and then go away.

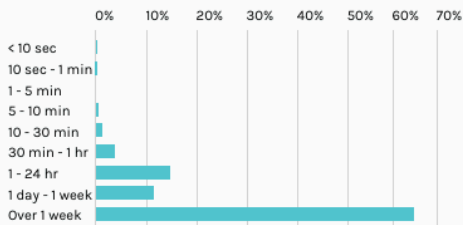
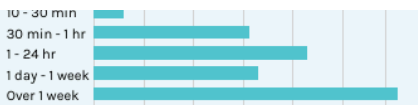
### 69% of container images are updated in one week.

A small percentage of images are updated in less than 10 seconds



- the majority are updated in a week.

By looking at this data, we get an idea of how often customers are doing new deploys of updated containers as a part of their DevOps CI/CD process.



**67% of services stay up beyond a week.**

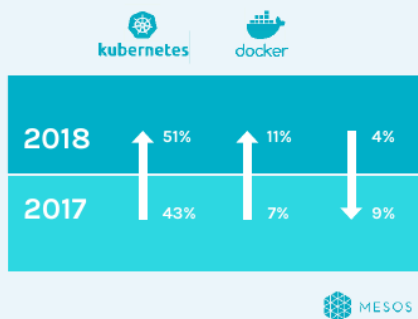
Containers and pods come and go, but services are expected to be available.

For most customers the goal is to keep applications working around the clock. Services allow containers and pods to die and replicate without impacting the application.

### Orchestrators for Docker containers.

First place goes to Kubernetes, followed by Kubernetes and Kubernetes.

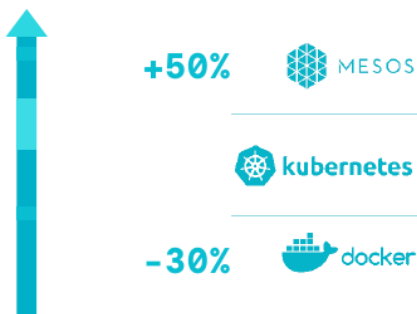
[Kubernetes](#) retained its hold on the lead position for the most frequently used orchestrator. Docker Swarm climbed to number two while Mesos-based orchestration, including [Mesos Marathon](#) and [Mesosphere DC/OS](#), dropped to third.



**Cluster size influences orchestrator choice: Mesos owns the big cluster game.**

Where Mesos is used, the median number of containers deployed is 50% higher than Kubernetes environments.

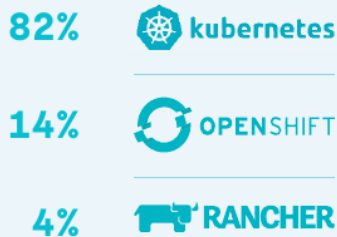
Though fewer in number, Mesos clusters are typically enterprise-scale. [Swarm](#) clusters, conversely, were 30% smaller compared to Kubernetes.



## Top flavors of Kubernetes.

Here come the Kubernetes distributions.

We dissected the use of Kubernetes by brand, to see if the Kubernetes in-use was the upstream open source version, or a package provided by a specific vendor. Open source Kubernetes holds the lion-share, but it appears that [OpenShift](#) is making inroads as is [Rancher](#).



### Response time

Entity up or down?

Pod restart count

CPU, memory, disk use by host

Container count

Event-based

http errors

CPU, memory, disk use by container

## Most popular alert conditions.

It's all about performance + uptime.

What keeps container administrators up at night? Sysdig alerts tell us what matters most. Responsiveness and uptime/downtime top the list. Host and container resource metrics – cpu, memory, and disk usage – are also important. Increasingly, orchestration-focused alerts like, "Pod Restart Count" are used to alert on problems that are likely to impact application performance.

## Popular alert scopes.

Users want to know – How're my pods doing?

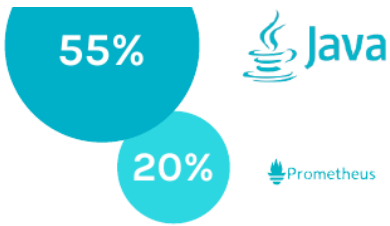
Alerts are "scoped" for a subset of the environment or for the entire infrastructure. The most common [alerts are tied to Kubernetes](#) tags. Scoping by pods is the leading choice followed closely by namespace. Container specific scoping is also popular, evenly split across container name, container image, and container ID.

2017	2018
Deployment name	Pod name
Lower-level orchestrator constructs (e.g pod, replicaSet, etc.)	Namespace
Role of host	Host name
Cloud provider tags	Container name, image or ID
Container name	Cloud provider tags



## Custom metrics.

There's no one format to rule them all.

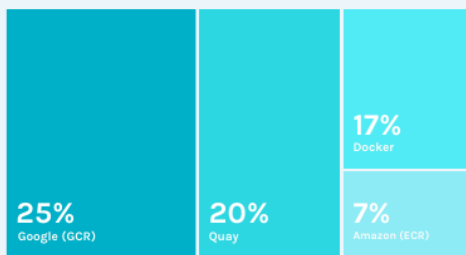


Sysdig automatically collects custom metrics like [JMX](#), [StatsD](#), and [Prometheus](#). JMX metrics associated with Java applications were collected by 55% of users. StatsD comes in at 29% and Prometheus at 20%. With the popularity of Prometheus, we expect its number to grow over time.

### Popular container registries.

It's a split decision - critical but no clear leader.

Registries are fundamental to any container deployment pipeline. Some are public, some private, some as-a-service, and some deployed as on-premises software. Of the top 3, [Google Container Registry](#) (GCR) is the most frequently used by Sysdig customers. [Quay](#) is a close second most used, followed by Docker and Amazon [Elastic Container Registry](#) (ECR).

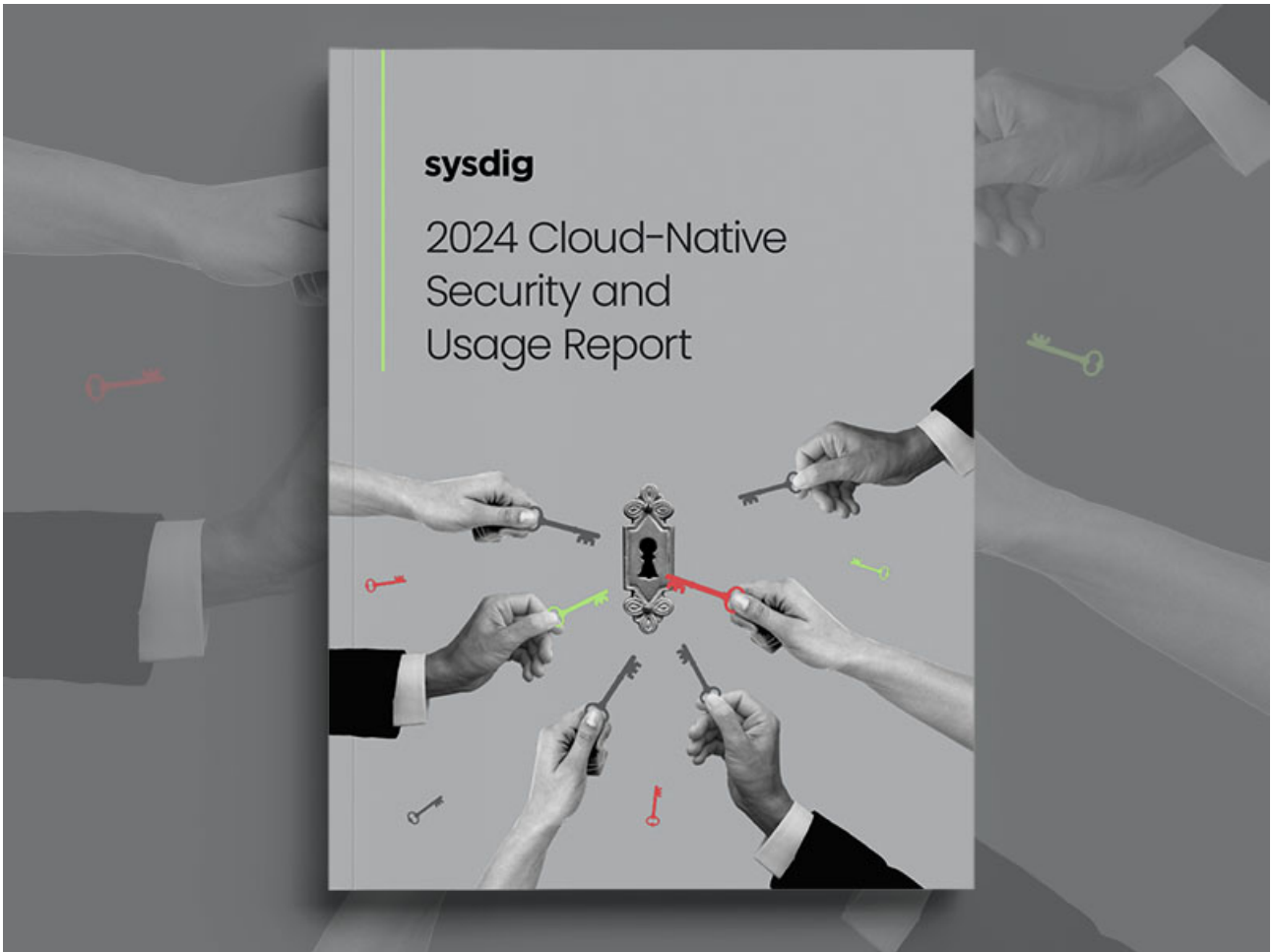


### Want to learn more?

Download the complete [Docker Usage Report](#) to see all the details.

[INFOGRAPHIC. 2018 Docker Usage Reportpdf](#)

[DockerOpenshiftKubernetesPrometheus](#)



[REPORT. 2024 Cloud Native Security And Usage Reportpdf](#)

[Cloud SecuritySysdig SecureCloud computing security.](#)

**TAG CYBER**

# ACHIEVING FULL LIFECYCLE DEVOPS SECURITY USING SYSDIG

EDWARD AMOROSO, TAG CYBER



[REPORT. Achieving Full Lifecycle Devops Security Using Sysdigpdf](#)

[Cloud SecuritySysdig Secure](#)



CHECKLIST

## Sysdig vs. Prisma Cloud

### A Purpose-Built Cloud Security Solution With A Unified CNAPP Platform Powered By Runtime Insights

Do you want a security platform that's built from the ground up for the cloud, or a product that has been stitched together? Prisma Cloud falls short with a product that is assembled from various acquisitions, is hard to use, and misses the whole picture.

#### Why Customers Choose Sysdig

Sysdig Secure is a single, integrated platform solution for CNAPP that uses multi-domain correlation to uncover hidden attack paths in the riskiest combinations of vulnerabilities, configurations, entitlements, and run time, unlike Prisma Cloud which only aggregates data but is unable to uncover new insights or risks.

Sysdig Secure provides real-time detection and runtime insights to help identify and prioritize high risk items like in-use vulnerabilities and permissions to reduce alert fatigue and save time, unlike Prisma Cloud which only provides noisy alerts and risks with limited context and prioritization.

With Sysdig, you can:

- ✓ Get superior user experience with a single, integrated CNAPP solution.
- ✓ Uncover hidden risks and attack paths with multi-domain correlation.
- ✓ Prioritize risks with our real-time detection and runtime insights.

[GUIDE. Container Security Comparison Checklist: Sysdig vs Prisma Cloudpdf](#)

[Cloud SecuritySysdig Secure](#)

BRIEF

# sysdig Google Cloud

Sysdig's Cloud-Native Application Protection Platform (CNAPP) protects Google Cloud, hardening security posture and detecting attacks immediately. [LEARN MORE →](#)

**Joint Customer Highlights**

- SAP Concur
- Goldman Sachs
- BlaBlaCar
- onna
- Calendly
- COMMERCE
- apreehealth

10 minutes is all it takes to execute an attack in the cloud after discovering an exploitable target. Outpacing attackers in the cloud requires security teams to meet the  $5/5/5$  Benchmark.  $5/5/5$  means 5 seconds to detect, 5 minutes to triage, and 5 minutes to respond to threats. Sysdig helps Google Cloud customers get closer to meeting this benchmark's expectations, securing their cloud innovation.

In the cloud, every second counts. Google Cloud users must protect their business without slowing it down. Sysdig secures Google Cloud and container services in real-time with threat detection built on open source Falco. We correlate signals across workloads, identities, and services in Google Cloud to uncover hidden attack paths and prioritize real risk.



**Key Benefits**

- Cloud detection & response**  
Stop attacks in cloud environments faster
- Vulnerability management**  
Reduce vulnerabilities by up to 95%
- Posture management**  
Instantly detect risk changes in cloud
- Permissions and Entitlements**  
Gain visibility into cloud identities

[PARTNER BRIEF. Sysdig and Google Cloud Platformpdf](#)

[Cloud SecuritySysdig Secure](#)



**COMPANY DETAILS:**

French carpooling marketplace with 90 million members in 22 countries.

**BUSINESS NEEDS AND CHALLENGES:**

- Reduce risk by detecting suspicious activity and misconfigurations.
- Automate alerts and streamline incident response.
- Secure containers without adding operations management overhead.
- Flexibility to fine-tune security to their needs.

**BUSINESS IMPACT OF SYSDIG:**

The security team of four has been able to empower the 200 developers to own their applications from development through the container lifespan, including managing the security posture. BlaBlaCar is able to keep its security team and overhead small with an efficient secure DevOps model.

**SYSDIG PLATFORM BENEFITS:**

- Deep visibility to detect suspicious activity and misconfigurations.
- An easy to deploy and maintain SaaS-first solution.
- The power of open source Falco with an enterprise experience.
- Forensics capabilities.

**INFRASTRUCTURE:**

Google Cloud Platform (GCP) and Yandex Managed Service for Kubernetes

**ORCHESTRATION:**

Google Kubernetes Engine (GKE) and Yandex.Cloud



## The BlaBlaCar Security Team of 4 Empowers Developers to Manage Security Risk with Sysdig

### Overview

BlaBlaCar is the world's leading long-distance carpooling platform, with a global community of 90 million drivers and passengers across 22 countries. The platform connects people looking to travel long distances with drivers heading in the same direction so they can travel together, share the cost, and reduce their impact on the environment.

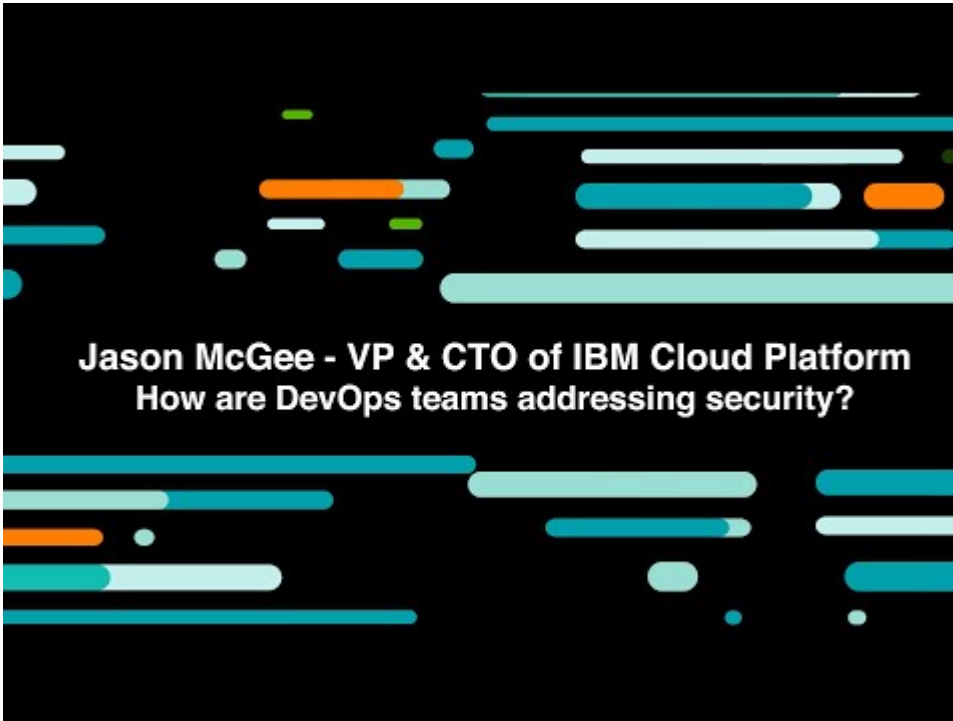
### Challenge

After deciding to add more than 120 nodes to Google Cloud Platform (GCP) and Google Kubernetes Engine (GKE), the BlaBlaCar security team of four people looked for a security solution. Supporting a development team of more than 200, the security team needed a way to empower developers to build and run applications in production, and to ensure security throughout the container lifecycle.



[CASE STUDY. BlaBlaCar Empowers Developers to Manage Security Risk with Sysdigpdf](#)

[Cloud SecuritySysdig\\_SecureKubernetesSysdig\\_Monitor](#)



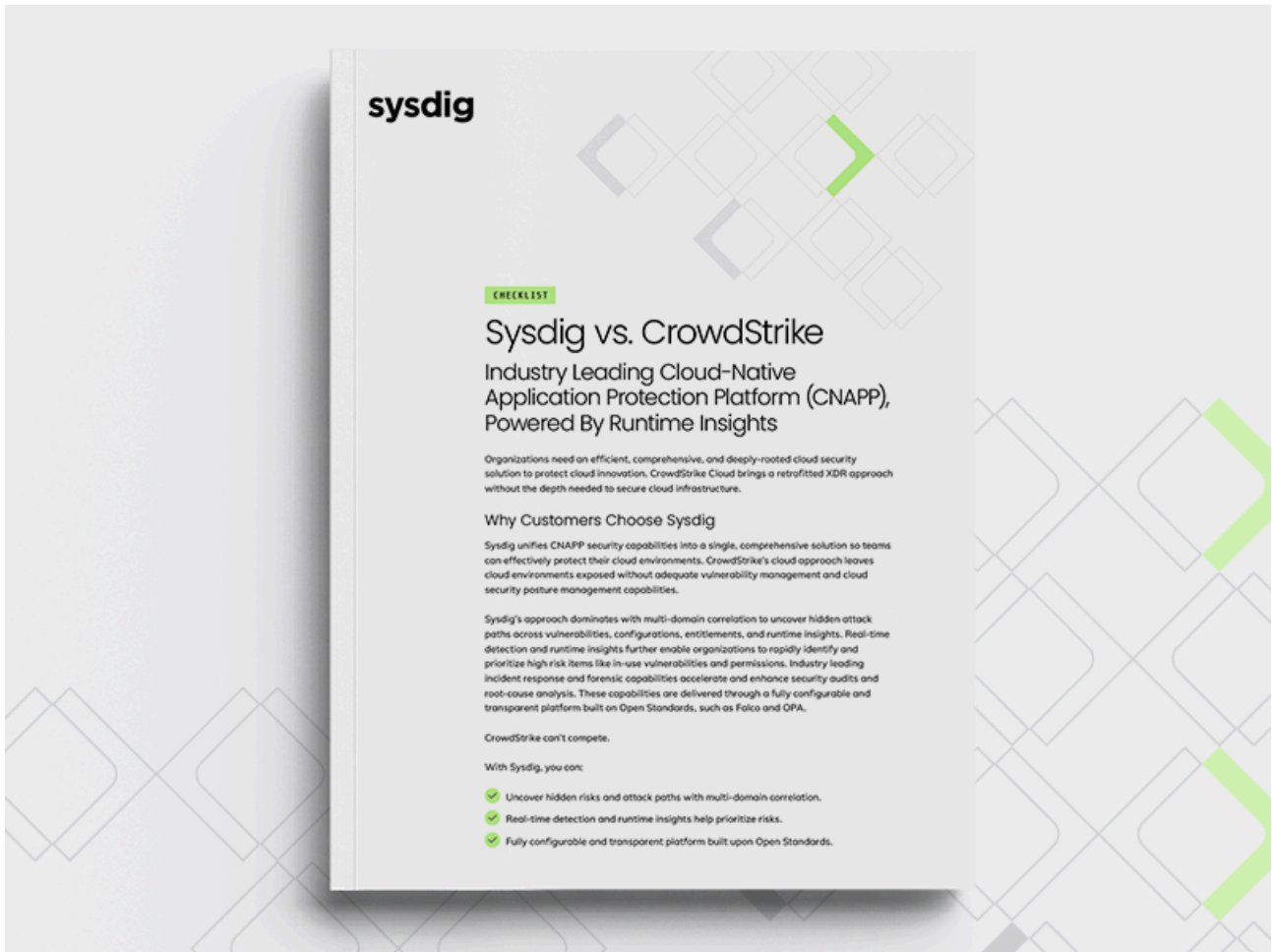
[VIDEO. DevOps Teams Addressing Security: IBMvideo](#)

[Cloud SecuritySysdig SecureCloud MonitoringIBM](#)



[VIDEO. Troubleshooting Processes and Tools: IBMvideo](#)

[Cloud SecuritySysdig SecureCloud MonitoringIBM](#)



[GUIDE. Container Security Comparison Checklist: Sysdig vs CrowdStrikepdf](#)

[Cloud SecuritySysdig Secure](#)



## Container and Cloud Security Comparison Checklist: Sysdig vs Qualys

### 55+ features compared



Don't rely on a tool that is blind to cloud-native workloads. Tools like Qualys lack the visibility you need to accurately detect and respond to container attacks. You will also probably need additional licenses to have a full functionality for the Qualys suite

Your security stack needs to be:

- Built on open source
- Instrumented to provide deep visibility with rich context across containers, hosts, Kubernetes and cloud
- SaaS first

#### Secure Your Cloud from Source to Run.

This checklist provides a feature comparison across container and cloud security between Sysdig Secure and Qualys. This checklist is based on an assessment made by Sysdig and is subject to change over time according to roadmap and releases.

#### Coverage Areas

- Platform
- Cloud Workload Protection (CWPP)
- Vulnerability Management
- Runtime Security
- Incident Response and Forensics
- Kubernetes Security
- Cloud Security Posture Management (CSPM)
- Compliance



[GUIDE. Container Security Comparison: Sysdig vs Qualyspdf](#)

[Cloud SecuritySysdig SecureRegulatory Compliance](#)



[GUIDE. Container and Cloud Security Comparison Checklist: Sysdig vs Orca](#)

[Cloud Security Sysdig Secure Regulatory Compliance](#)



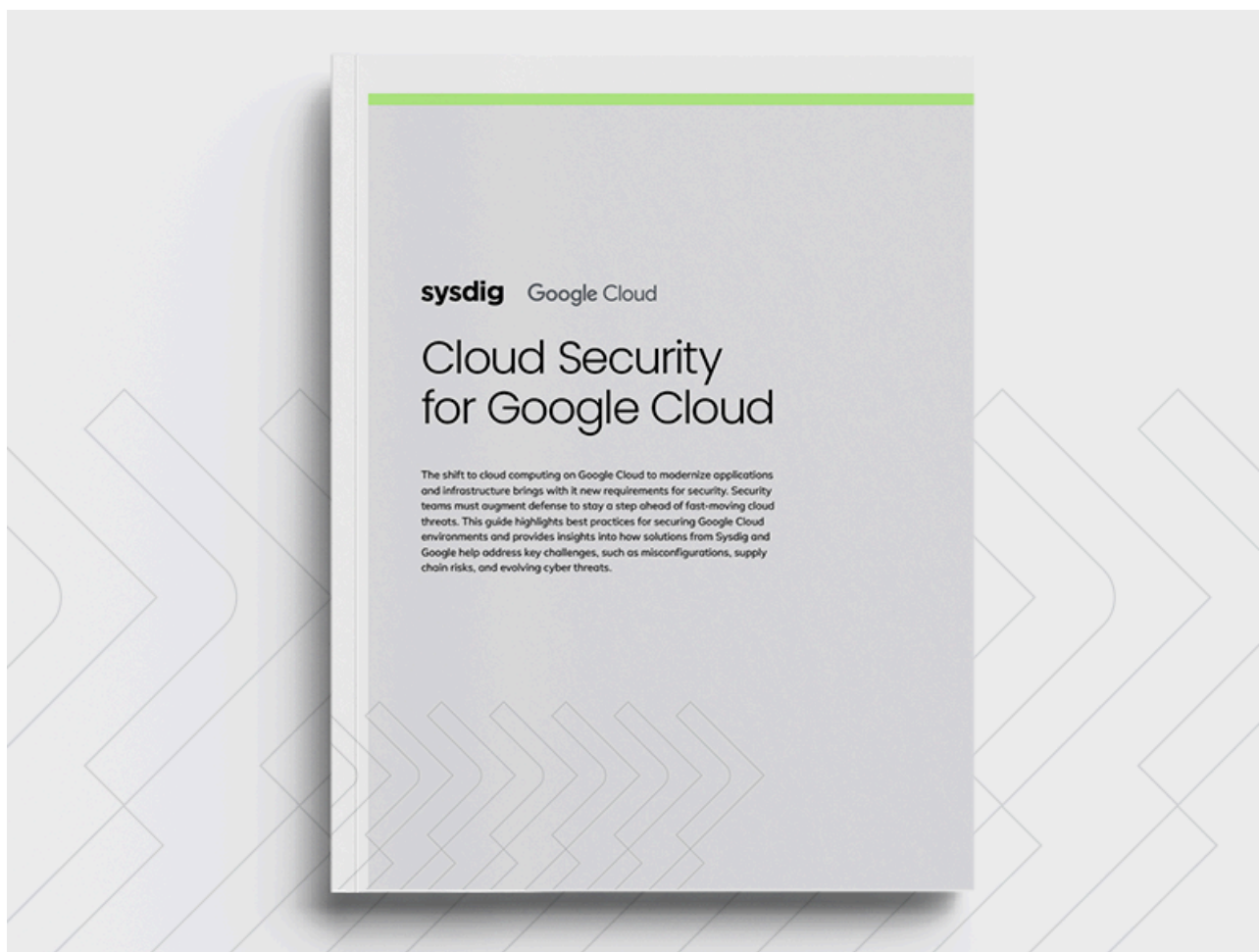
[VIDEO. Journey to Containers: IBMvideo](#)

[Cloud SecuritySysdig SecureCloud MonitoringIBM](#)



[BRIEF. The Business Impact Of Time In Cloud Securitypdf](#)

[Cloud SecuritySysdig SecureCloud computing security.](#)



[GUIDE. Cloud Security for Google Cloudpdf](#)

[Cloud SecuritySysdig Secure](#)



## Container Security Comparison Checklist: Sysdig vs StackRox

55+ features compared



Application development is transforming with the move to CI/CD, containers and open source. Cloud teams need tools that are built to secure containers, Kubernetes and cloud, and integrate into their DevOps workflow.

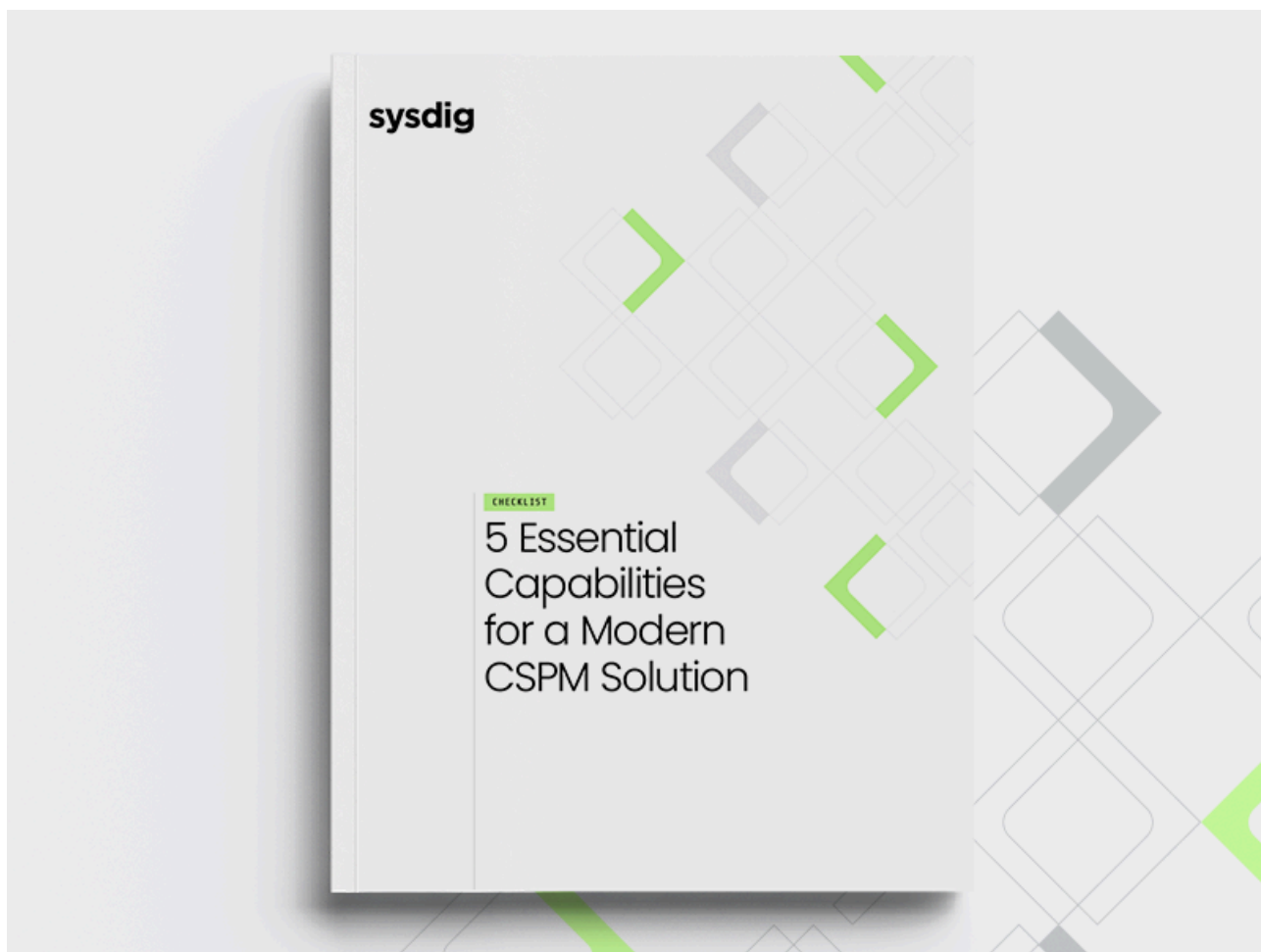
This checklist provides a feature comparison between Sysdig Secure and StackRox.

### Coverage Areas

- Platform
- Instrumentation
- Image Scanning
- Runtime Security
- Network Security
- Incident Response and Forensics
- Compliance

[GUIDE. Container Security Comparison Checklist: Sysdig vs StackRoxpdf](#)

[Cloud SecuritySysdig Secure](#)



[BRIEF. 5 Essential Capabilities for a Modern CSPM Solutionpdf](#)

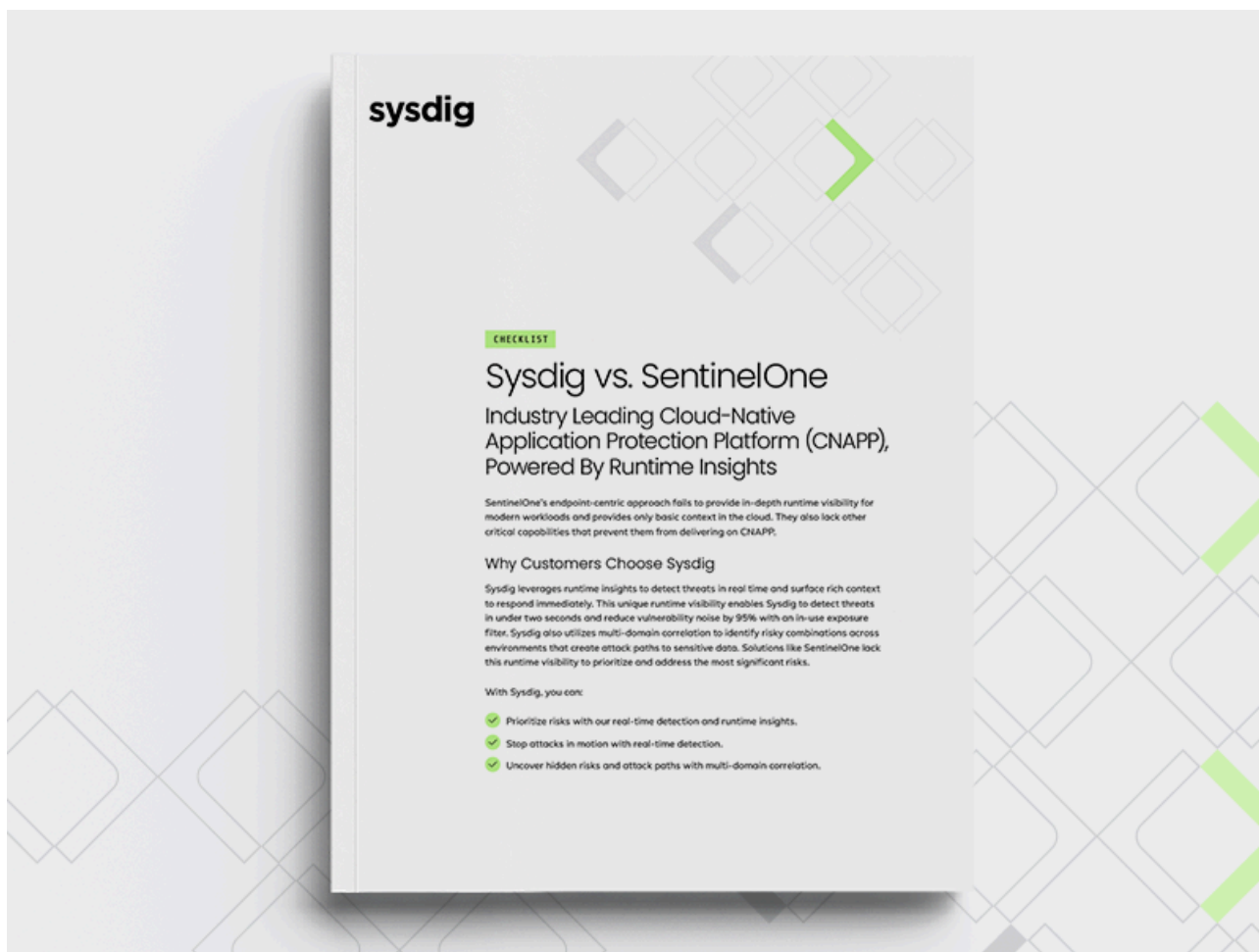
[Cloud SecuritySysdig SecureCloud computing security](#)

# Sysdig 2023 Cloud-Native Security and Usage Report



[REPORT. 2023 Cloud-Native Security & Usage Reportpdf](#)

[Cloud SecuritySysdig\\_SecureCloud MonitoringKubernetes](#)



[GUIDE. Sysdig vs SentinelOne Checklistpdf](#)

[Cloud SecuritySysdig SecureCloud computing security](#)



**BUSINESS VALUE CHECKLIST**

# 5 Critical Business Values Delivered by Sysdig Posture and Permission Management

In today's rapidly evolving business landscape, ensuring the security, compliance, and efficiency of your organization's digital assets is paramount. The deployment and maintenance of a robust security posture has led to a significant increase in the identification of issues and risk findings. Security, operations, and IT teams find themselves grappling with cloud misconfigurations and security weaknesses, which, in turn, expose organizations to potential threats for extended periods. As a response, security leaders are continuously exploring ways to prioritize these risks, reduce friction, and actively contribute to business growth. See how a handful of customers met their goals with the business values delivered by Sysdig:

- Identify and Prioritize Real Risk
- Accelerate Cloud Maturity Based on In-Use Permissions
- Mitigate Compliance Risk with Runtime Insights
- Save Time with In-Use Risk Prioritization
- Reduce Cost by Consolidating Security Tools

[BRIEF. 5 Critical Business Values Delivered By Sysdig Posture And Permission Managementpdf](#)

[Cloud SecuritySysdig\\_SecureCloud computing security](#)



## Snyk & Sysdig Integration: eliminate up to 95 percent of vulnerability noise

### Complete container security from source to production

The only solution that enables true DevOps security from the time the first line of code is written, through the full lifecycle of the Kubernetes workload. Secure applications from the start, protect them at runtime, and eliminate up to 95 percent of container vulnerability noise.

"Sysdig's deep runtime security visibility and Snyk's developer-first tooling enables developer, DevOps, and security teams to achieve better alignment so they can manage risk without delaying software releases," ~ Suresh Vasudevan, Chief Executive Officer, Sysdig

"Together with Sysdig, we're now empowering millions more developers worldwide to innovate securely."

~Peter McKay, Chief Executive Officer, Snyk

### Why Snyk & Sysdig?

Snyk and Sysdig deliver the broadest security coverage for cloud-native application development and delivery while helping teams reduce noise and risk. The industry-first integration of Sysdig Secure and Snyk Container enables security and development teams to prioritize and address security issues based on their exploitability and business impact.



#### Build secure from the start

Begin securing containers as early as the Dockerfile is created by automating the selection of up-to-date, secure base images. Identify issues in code and code dependencies even before they hit your pipelines.



#### Protect against runtime threats

Detect runtime threats and anomalies across containers, Kubernetes, and cloud, automate alerting and response, and capture detailed activity records for forensics.



#### Eliminate container vulnerability noise

Cut out up to 95 percent of container vulnerability noise by identifying packages loaded at runtime. Prioritize vulnerabilities to fix first, eliminating the noise of typical container vulnerability scans.

[SOLUTION BRIEF. Snyk & Sysdig Solution Briefpdf](#)

[Cloud SecuritySysdig Secure](#)

## Market Guide for Cloud Workload Protection Platforms

Published 12 July 2021 - ID G00725997 - 22 min read

By Analyst(s): Neil MacDonald, Tom Croll

Initiatives: [Infrastructure Security](#)

Workload protection must span virtual machines, containers and serverless workloads in public and private clouds. Security and risk management leaders should use this Market Guide to understand the need for protection that spans development and runtime and includes cloud security posture management.

### Overview

#### Key Findings

- Most enterprises are purposefully using more than one public cloud infrastructure as a service (IaaS) platform, but still have on-premises workloads to protect.
- With cloud-native applications, workload security must start proactively during development.
- The cloud workload protection platform (CWPP) market is increasingly overlapping with the cloud security posture management (CSPM) market and "shifting left" into development to address the full life cycle of cloud-native application protection requirements.
- Emerging approaches, such as the use of agentless CWPPs, appeal to buyers because of their ease of deployment.
- Enterprises using endpoint protection platform (EPP) offerings designed to protect end-user devices for server workload protection are putting their data and applications at risk.

#### Recommendations

Security and risk management leaders responsible for infrastructure security should:



Written by **Dave Shackelford**

April 2021

Sponsored by:

**Sysdig**

**Analyst Program** 

©2021 SANS™ Institute

[REPORT. SANS 2021 Cloud Security Survey.pdf](#)

[Cloud SecuritySysdig\\_Secure](#)



[REPORT. 2022 Sysdig Cloud-Native Threat Reportpdf](#)

[Cloud SecuritySysdig Secure](#)



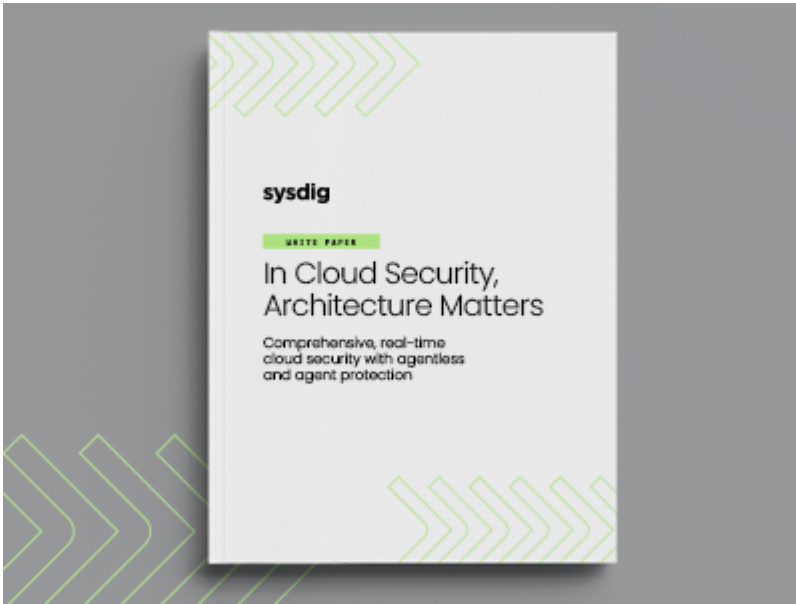
[SOLUTION BRIEF. Combat Active Cloud Risks With Runtime Insightspdf](#)

[Cloud SecuritySysdig SecureCloud computing security](#)



[SOLUTION BRIEF. Stop Advanced Attacks At Cloud Speedpdf](#)

[Cloud SecuritySysdig SecureCloud computing security](#)



[WHITEPAPER. In Cloud Security, Architecture Matterspdf](#)

[Cloud SecuritySysdig Secure](#)



# 2020 Container Security Snapshot

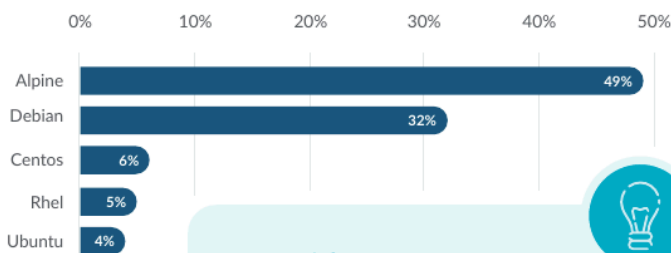
Vulnerabilities and risky configurations inside container images highlight the need for secure DevOps

Containers and Kubernetes are being used heavily by DevOps teams deploying cloud applications. But it's important to know what's inside containers to manage risk effectively.



## What is inside your container?

### What are the top image distros?



#### Key Insight

Alpine is popular, as it is known for images with a minimal footprint. Ironically, the largest image we found was an Alpine based image (10GB!).

Modern software is assembled, not built from scratch. Developers typically use open source base images from various Linux distributions when building their containerized applications.

Alpine is the #1 choice by developers when it comes to building container images.

### How big are images?

#### Key Insight

- Although image size depends on the application, it's not

Average image size observed

**376 MB**



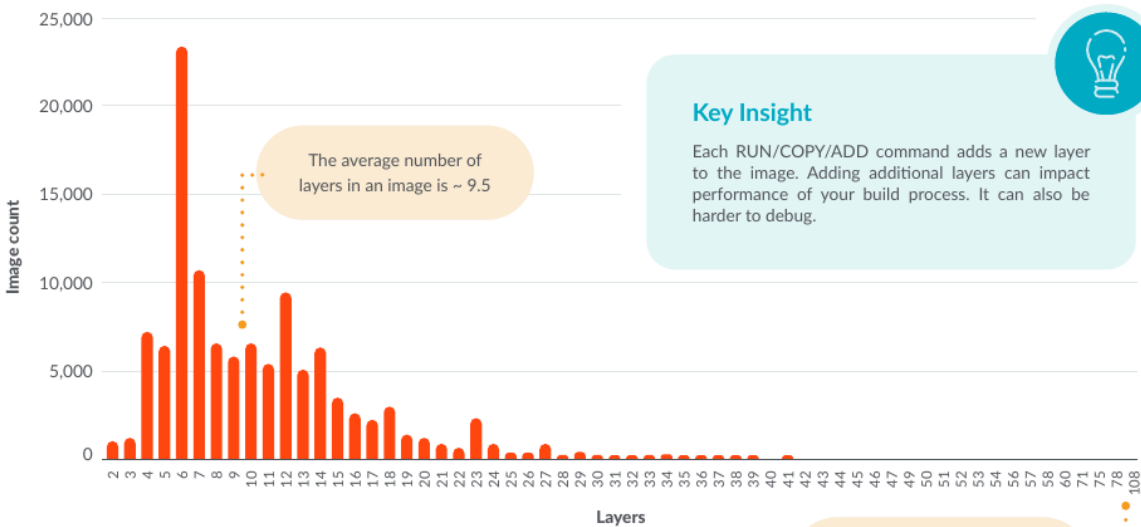
a good practice to have a large image unless absolutely necessary.

- Large images not only take longer to deploy, slowing down release velocity, they expose more opportunities for attack.

largest image size observed  
**10 GB**  
that's 26x larger than the average

### How many layers are part of an image?

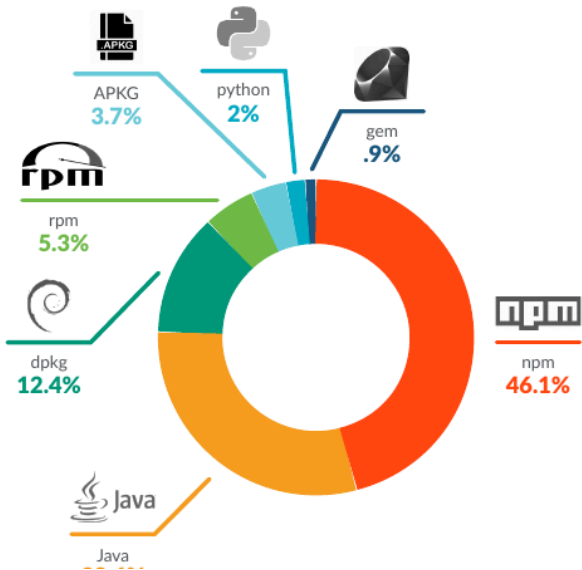
Image Count vs. Layers



**Key Insight**  
Each RUN/COPY/ADD command adds a new layer to the image. Adding additional layers can impact performance of your build process. It can also be harder to debug.

**OUTLIER:**  
The maximum layers observed in the wild was 107!

### What are the top 3rd-party libraries?



Developers also pull in code from open source third-party libraries (non-OS packages) to save time building and deploying applications quickly.

**Key Insight**  
Data shows npm is the most popular open-source non-OS package.

29.6%

### Where are images typically pulled from?

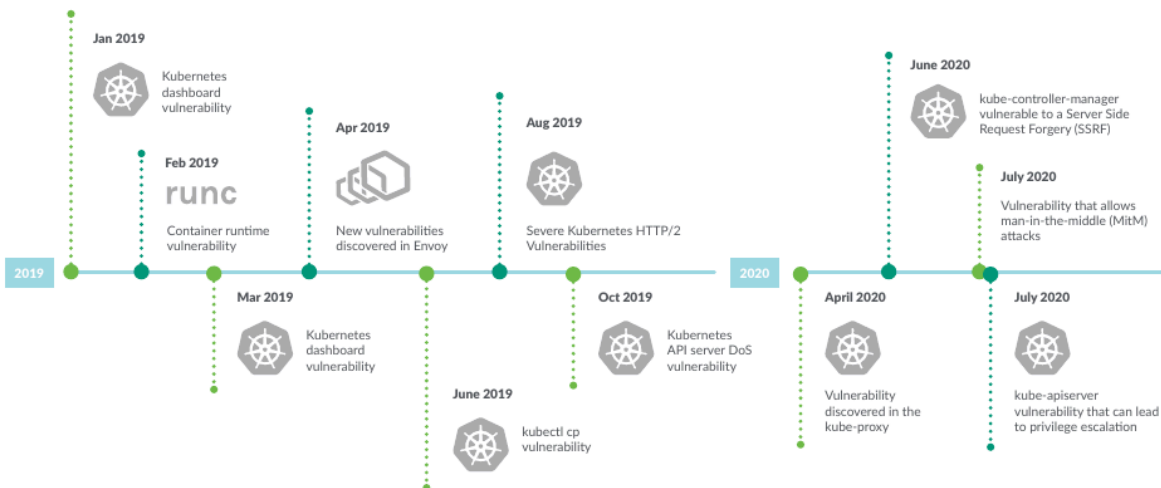
Images from public sources can be risky, as few are checked for security vulnerabilities. Docker Hub, for example, certifies less than 1% of its nearly 3 million hosted images. However, we found that 40% of images are pulled from public sources.

Images Pulled from Public vs. Private Registries



## Where are the vulnerabilities?

### New Kubernetes vulnerabilities continue to be identified



### What type of vulnerabilities matter?

#### Key Insight

- While only 4% of OS vulnerabilities are high or critical, if exploited, these

OS Vulnerabilities by Severity



vulnerabilities can compromise your entire image and bring down your applications.

- What many teams don't check for are vulnerabilities in third-party libraries. Developers might be unknowingly pulling in vulnerabilities from these non-OS open source packages, like Python PIP, Ruby Gem, etc., and introducing security risk.

Non-OS Vulnerabilities by Severity



## Risky configurations are common

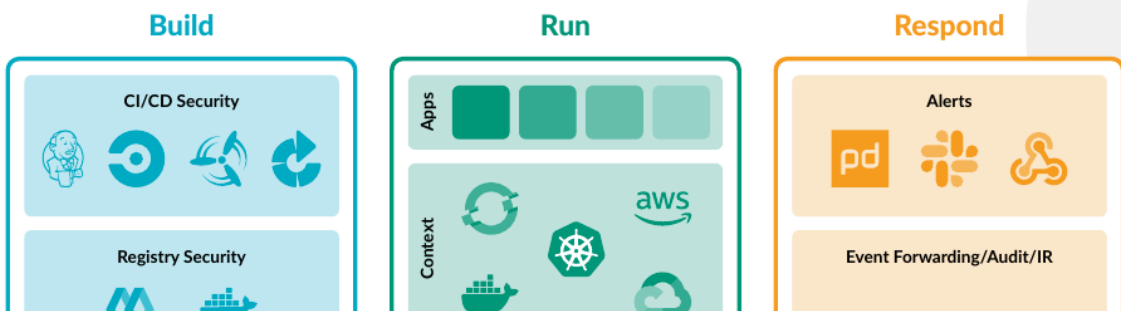
How many images are running as root?

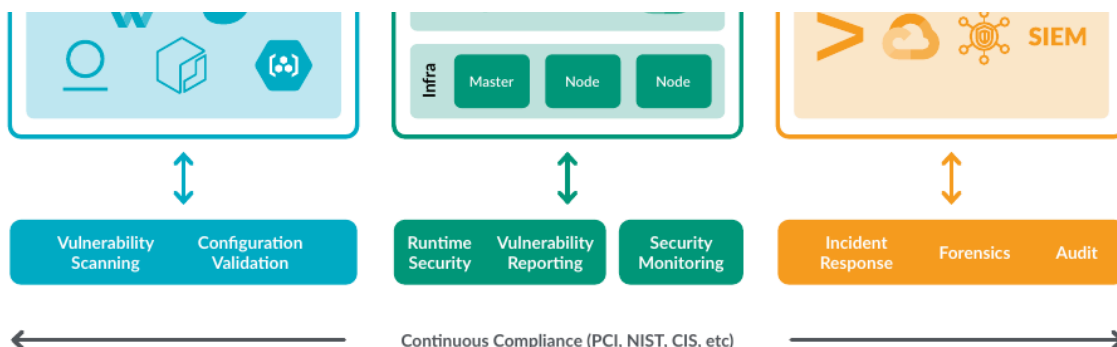


### Key Insight

- While teams understand the need to scan for vulnerabilities, they may not be scanning for common configuration mistakes.
- Even if risky configurations are detected at build time, in practice, teams don't delay deployment to fix the issue. To maintain deployment speed they allow the container to run, and continuously monitor to ensure the fix is implemented within a defined grace period.

## Teams need to adopt a secure DevOps workflow





### Recommendation checklist



- 1 Embed scanning into your CI/CD pipelines and also ensure you have runtime scanning in place to detect newly identified vulnerabilities.
- 2 Scan both OS as well as non-OS packages (over 53% have high/critical CVEs) to manage security risk effectively. [Read more about how to implement Docker scanning with open-source tools.](#)
- 3 Check for configuration parameters, such as image sizes, layers, running images as root, etc., as part of your DevOps security policy. Be aware of outliers if they do exist. [Read more about 12 image scanning best practices here.](#)
- 4 Consider giving a grace period for implementing configuration best practices to allow deployment, but monitor at runtime to ensure the fix is implemented.
- 5 When possible, use multi-stage builds, and only copy the artifacts you need into the final image.
- 6 Ensure you have continuous monitoring, alerting, and enforcement mechanisms to prevent drift (i.e., [Using PodSecurityPolicies in Kubernetes](#)).
- 7 Evaluate open-source runtime security tools like Falco, or commercial products like [Sysdig Secure](#).

You need to manage security risk without slowing down release schedules. By understanding what is inside your containers, you can implement security controls that make sense for your organization.

To learn more about how to secure containers and Kubernetes, download the [Kubernetes Security Checklist](#).

GET IT NOW



Copyright © 2020 Sysdig, Inc. All rights reserved. ING-006 Rev. A 8/20

[INFOGRAPHIC. 2020 Container Security Snapshotpdf](#)

[Cloud SecuritySysdig SecureKubernetes](#)


The image shows the cover of a whitepaper. At the top left is the SANS logo. At the top right is the text 'Analyst Program' with a small bar chart icon. Below the SANS logo is the word 'Whitepaper' in a bold, sans-serif font, with a short orange horizontal line underneath. The main title is '2024 Cloud-Native Application Protection Platform (CNAPP) Buyers Guide' in a large, white, sans-serif font. Below the title, it says 'Written by Dave Shackleford', 'Originally Published March 2023 as "Cloud Native Application Protection Platforms (CNAPPs) Buyers Guide"', and 'Updated September 2023'. At the bottom left is the Sysdig logo, and at the bottom right is the copyright notice '©2023 SANS™ Institute'. The background is a dark blue with abstract, glowing geometric shapes.

**SANS** Analyst Program

Whitepaper

# 2024 Cloud-Native Application Protection Platform (CNAPP) Buyers Guide

Written by Dave Shackleford  
Originally Published March 2023 as "Cloud Native Application Protection Platforms (CNAPPs) Buyers Guide"  
Updated September 2023

 ©2023 SANS™ Institute

[WHITEPAPER. SANS CNAPP Buyers Guidepdf](#)

[Cloud SecuritySysdig Secure](#)



IBM zSystems

IBM LinuxONE



## Unified visibility, security, and compliance with Sysdig Platform for IBM zSystems and IBM LinuxONE

As organizations expand into using containers, microservices, and cloud infrastructure, a new set of issues are emerging. Those challenges include container-based observability, security, and compliance, each of which now requires a different approach to security.

Mission-critical applications across the world rely on IBM zSystems to ensure continuous availability, reliability, and operation in an open hybrid cloud environment. Today, 45 of the top 50 banks, four of the top five airlines, seven of the top 10 global retailers, and 67 of the Fortune 100 rely on IBM zSystems as their core platform<sup>1</sup>.

IBM zSystems and IBM LinuxONE are designed to prevent security threats and protect data across a hybrid cloud environment with certified multitenant workload isolation as well as transparent, pervasive encryption with optimized performance. The Sysdig Platform helps build a security-focused, Kubernetes-based foundation for developing, deploying, and managing applications in containerized and cloud environments.

Together, Sysdig and IBM deliver a cloud-native monitoring and security platform to confidently run containers, Kubernetes, Red Hat OpenShift Container Platform, Linux, and cloud services on IBM zSystems and IBM LinuxONE.

IBM zSystems and IBM LinuxONE provide a strong foundation built for security, resiliency, and availability:

- Integrated **FIPS 140-2 level 4** compliant hardware security module (HSM<sup>2</sup>).
- Leverage **Red Hat OpenShift** Container Platform to modernize applications.
- Multitenancy with full LPAR isolation and virtualization designed for the highest **EAL5+ security certification**<sup>3</sup>.
- **IBM Cloud Hyper Protect Services** to provide data-at-rest and data-in-flight protection.
- Confidential computing through the implementation of **Trusted Execution Environment (TEE)** and **Secure Execution** on Linux on IBM Z and IBM LinuxONE.



1 IBM research and analysis: <https://www.ibm.com/downloads/cas/V24QQ4PW>  
 2 Source: <https://www.ibm.com/security/cryptocards/highlights>  
 3 Source: <https://www.commoncriteriaportal.org/files/epfiles/1160c.pdf>

[SOLUTION BRIEF: Sysdig Platform for IBM zSystems & IBM LinuxONE.pdf](#)

[Cloud SecuritySysdig\\_SecureIBM](#)

## Sysdig Cuts Onboarding to 5 Minutes



[VIDEO. 5 minutes to onboard secure DevOps video](#)

[Cloud Security Sysdig SecureCloud Monitoring Kubernetes](#)

**sysdig + Red Hat**

Secure and accelerate innovation on Red Hat OpenShift.

**Detect, fix, deliver. Foster with runtime insights.**

When Sysdig and Red Hat are deployed on your OpenShift Kubernetes cluster, you get a comprehensive view of your cluster's security and compliance. This view includes all the containers, pods, and services running on your cluster. You can see the configuration of each component and identify any misconfigurations or vulnerabilities. Sysdig also provides real-time alerts and notifications for any security events, so you can respond quickly to any threats.

**BENEFITS**

- **Default, zero-day, and targeted attacks**  
Sysdig Secure Cloud Services, built on Red Hat OpenShift, provides the ability to detect and remediate any security event in real-time, before it can be exploited. This means you can prevent attacks before they start.
- **Business-critical operations and operational readiness**  
Sysdig Secure Cloud Services provides a comprehensive view of your cluster's security and compliance. This view includes all the containers, pods, and services running on your cluster. You can see the configuration of each component and identify any misconfigurations or vulnerabilities. Sysdig also provides real-time alerts and notifications for any security events, so you can respond quickly to any threats.
- **Bring all work of security risks**  
Sysdig Secure Cloud Services provides a comprehensive view of your cluster's security and compliance. This view includes all the containers, pods, and services running on your cluster. You can see the configuration of each component and identify any misconfigurations or vulnerabilities. Sysdig also provides real-time alerts and notifications for any security events, so you can respond quickly to any threats.

Cloud Services

K8s & OpenShift

sysdig secure

CSPM

CIEM

VM

CNSP

[PARTNER BRIEF. Red Hatpdf](#)

[OpenshiftRed Hat](#)



CASE STUDY

COMPANY DETAILS:

Germany-based information extraction company that uses self-learned AI to automate data entry, such as invoices, receipts, travel expenses, and tax documents.

BUSINESS NEEDS:

- Stay ISO 27001 compliant
- Deliver secure applications internationally
- Ensure 'always on' platform availability

CHALLENGES:

- Limited visibility across bare metal and cloud environments
- Lack of data troubleshooting and compliance audits
- Limited activity monitoring and runtime policy enforcement

BUSINESS IMPACT OF SYSDIG:

The Gini operations and developer teams have confidence knowing their environment is secure. They are able to provide stable applications while saving time, allowing developers to focus on revenue-generating activities.

SYSDIG PLATFORM BENEFITS:

- Single tool across hybrid environment saves half a person on a two-person team
- Eases resource needs for proving compliance and audit exercises
- Developers are 20% more efficient
- Better informed capacity planning

INFRASTRUCTURE:

Hybrid: AWS Cloud and bare metal

ORCHESTRATION:

Kubernetes

Improving everyone's life by magically automating unpleasant tasks.

The Gini Way.



Gini Ensures Adherence to Strict EU Compliance Standards, While Reducing Dev and Ops Burdens

Overview

Gini is an information extraction company that automates the process of gathering information from financial documents. Based on self-learning artificial intelligence, Gini makes it easier to automate mundane tasks, such as invoice payments and other once-manual accounting tasks.

With millions of end customers, Gini's engineering team is responsible for maintaining a secure, 'always on' environment. The company operates 25 machines in an environment that spans bare metal and AWS Cloud. To ensure it can secure and monitor its hybrid cloud environment, Gini engineers rely on the Sysdig Secure DevOps Platform.

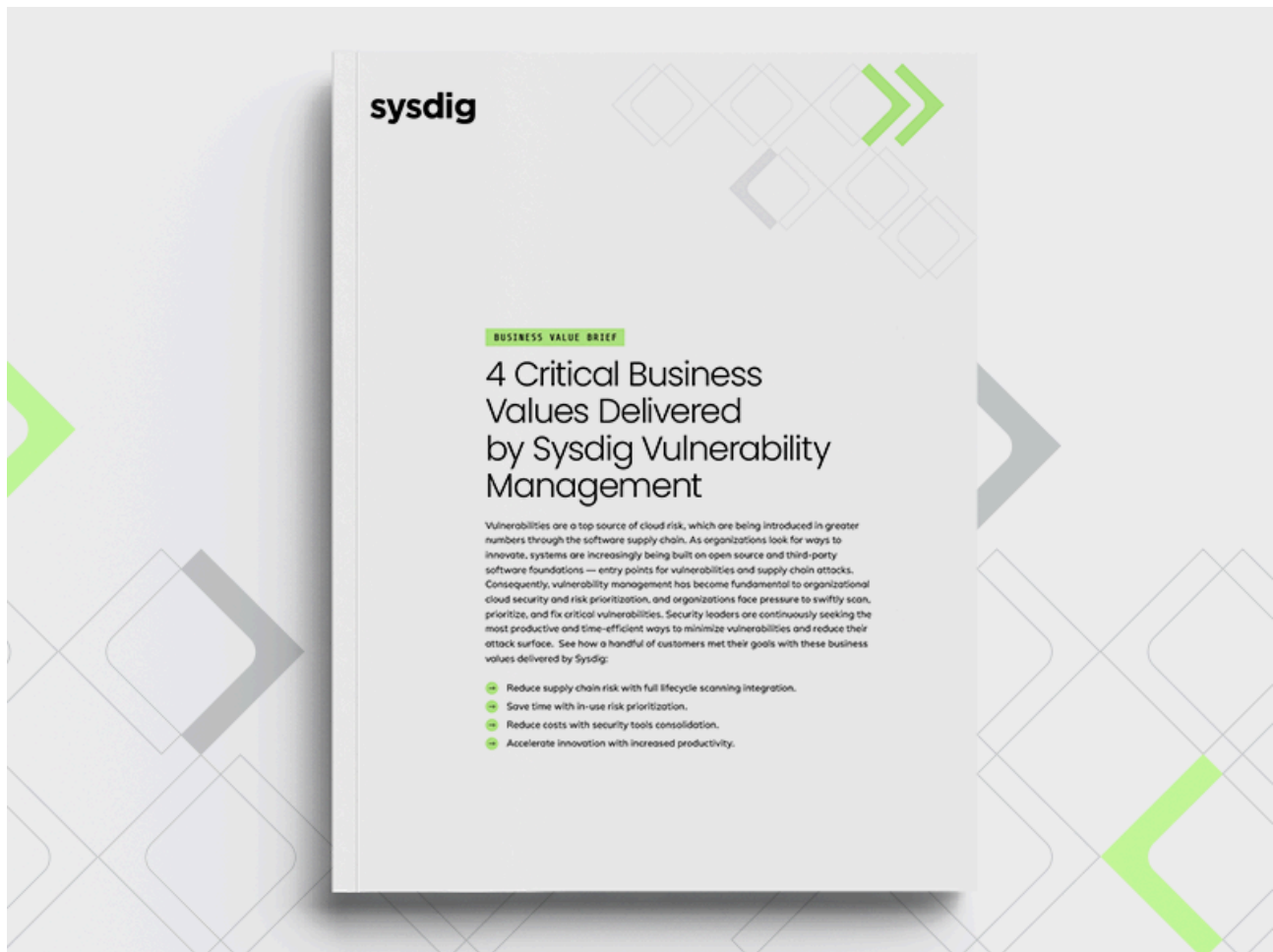
The Challenge

Originally built on bare metal, when Gini decided to transfer its development environment to the cloud, the operations team needed a way to reduce risk and ensure compliance. Gini manages highly sensitive user data, such as contracts and tax documents; therefore, complying with ISO 27001, an international standard for handling data that includes people and processes, is mandatory.



[CASE STUDY. Gini Ensures Adherence to Strict EU Compliance Standards, While Reducing Dev and Ops Burdenspdf](#)

[AWSSysdig SecureKubernetesSysdig Monitor](#)



[BRIEF. 4 Critical Business Values Delivered By Sysdig Vulnerability Managementpdf](#)

[Cloud SecuritySysdig Secure](#)



# Sysdig Guide to SOC 2 Compliance

---



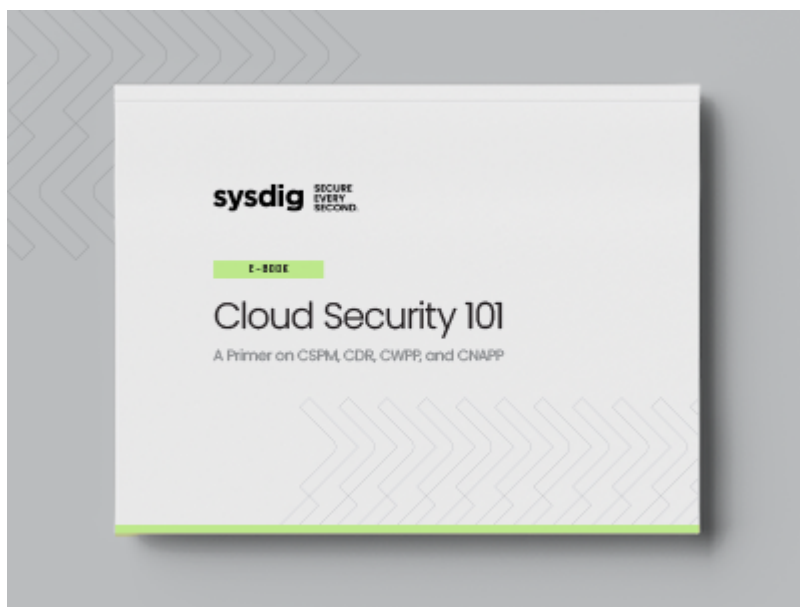
[GUIDE. Sysdig Guide To SOC 2 Compliancepdf](#)

[Cloud SecuritySysdig\\_SecureRegulatory Compliance](#)



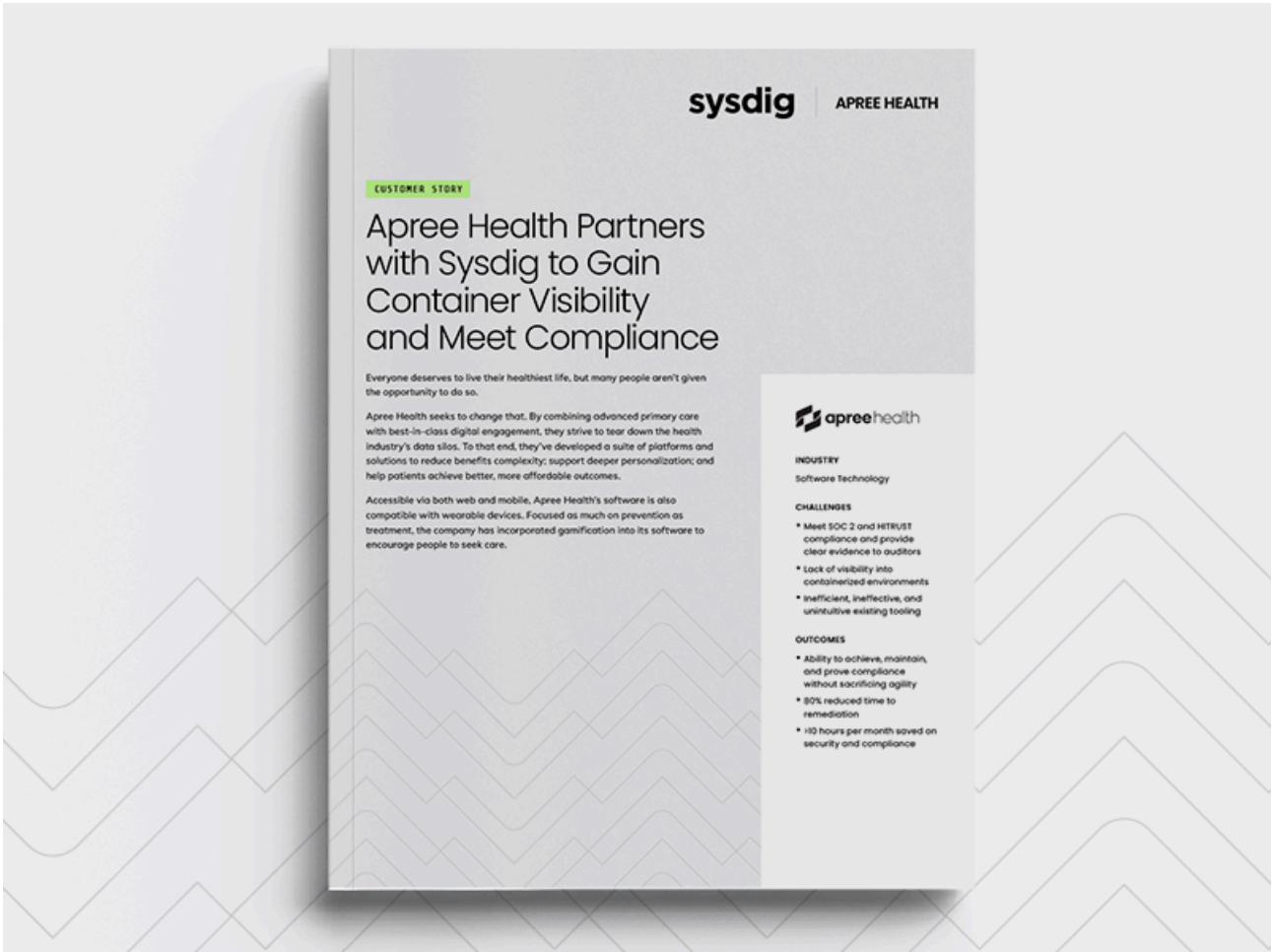
[VIDEO. How to prepare for the next Log4jvideo](#)

[Cloud SecuritySysdig\\_Secure](#)



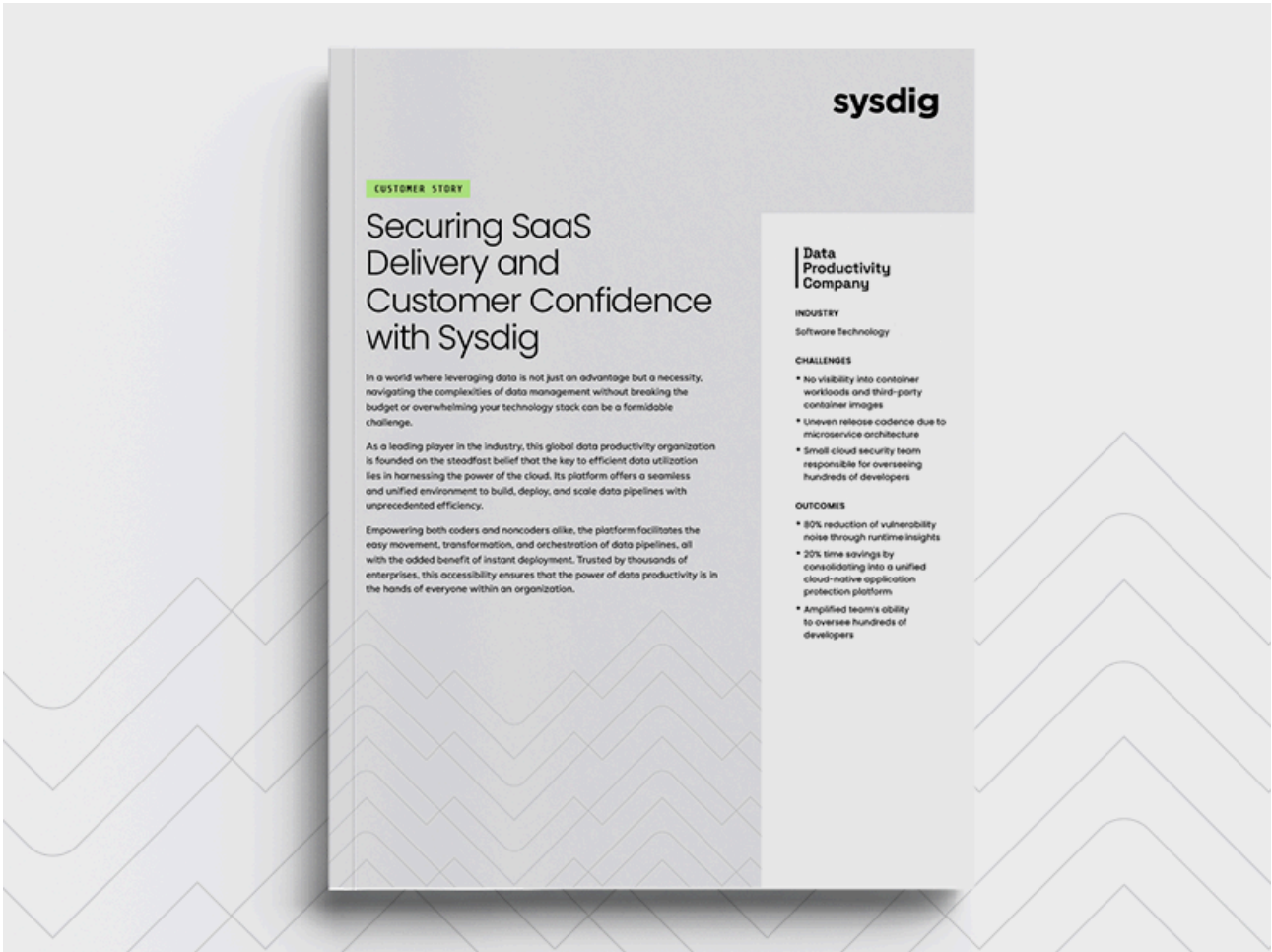
[GUIDE. Cloud Security 101pdf](#)

[Cloud SecuritySysdig\\_Secure](#)



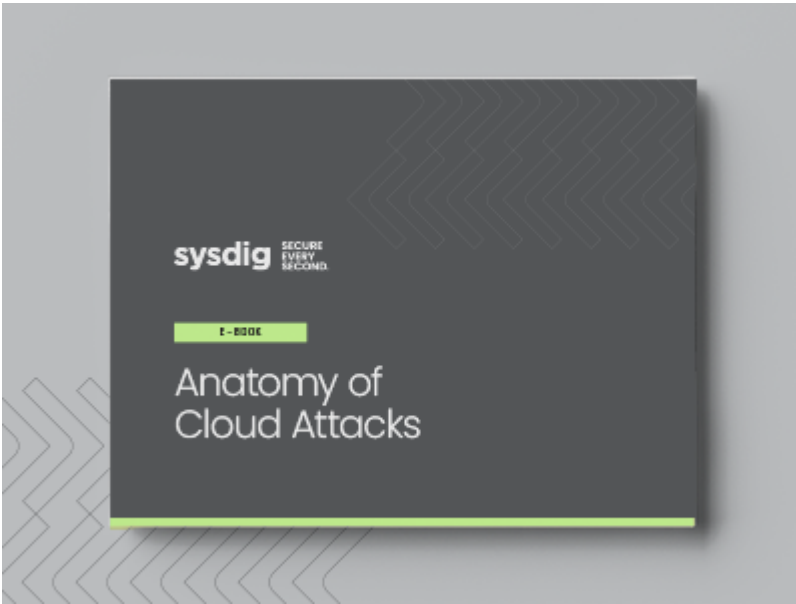
[CASE STUDY. Apree Healthpdf](#)

[Cloud SecuritySysdig SecureCloud computing security](#)



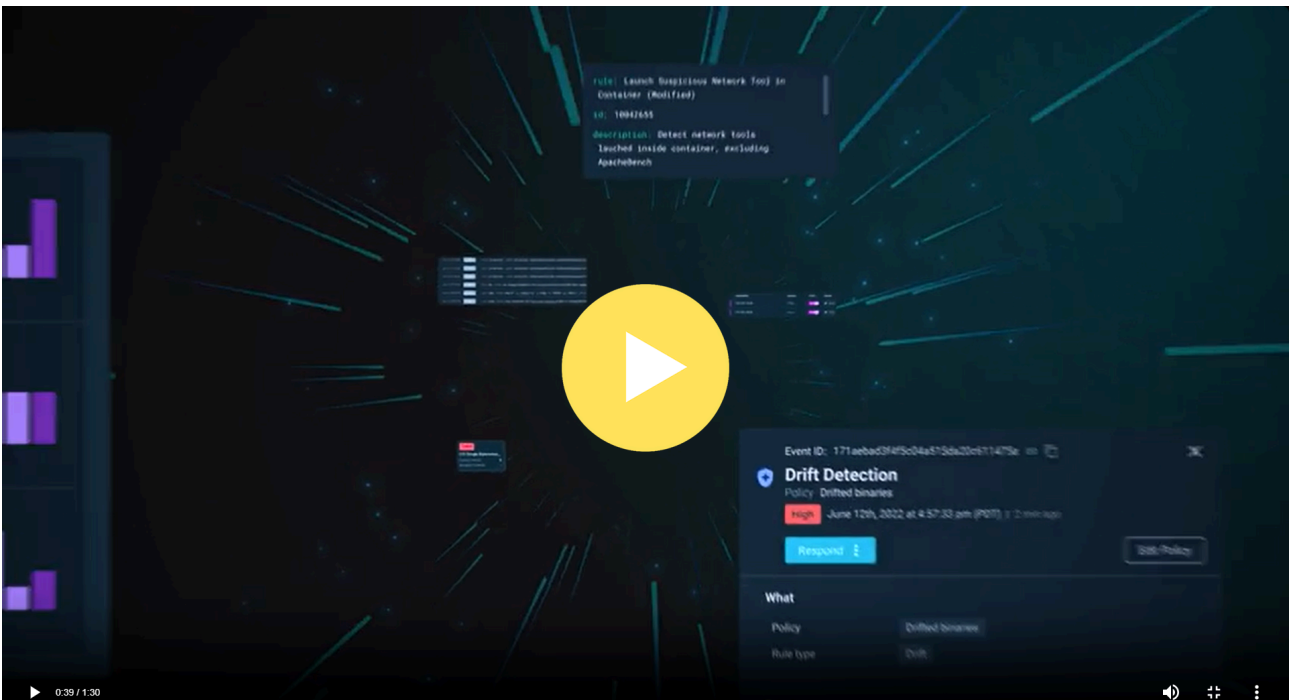
[CASE STUDY. Data Productivity Company.pdf](#)

[Cloud Security Sysdig SecureCloud computing security](#)



[GUIDE. Anatomy Of Cloud Attackspdf](#)

[Cloud SecuritySysdig Secure](#)



[VIDEO. Cloud Security Meets GenAI: Introducing Sysdig Sagevideo](#)

[Cloud SecuritySysdig Secure](#)



CASE STUDY

**COMPANY DETAILS:**

Mercari, Inc. is a Japanese e-commerce company with the mission of "creating a global marketplace that creates new value."

**CHALLENGES:**

- Generally speaking, Kubernetes is not secure by default and must be used with its security risks taken into account.
- With microservices, it is necessary to take security measures for developers and operations.

**SYSDIG PLATFORM BENEFITS:**

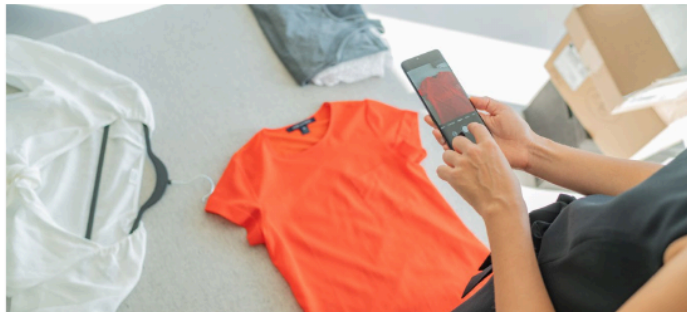
- Suspicious activities, unauthorized intrusion into Kubernetes, and storage of operation logs are monitored.
- All security events and audit activity logs are saved and accessible in the event of anomalous behavior.

**INFRASTRUCTURE:**

Google Cloud Platform (GCP)

**ORCHESTRATION:**

Google Kubernetes Engine (GKE)



## The Sysdig Secure DevOps Platform Provides Robust Security for Kubernetes Clusters Supporting Mercari's Flea Market App

Monitoring of microservices with different security levels living together on the same cluster

Founded in February 2013, the company's mainstay product, "Mercari," is the most widely used flea market app in Japan, with a monthly user count of 17.55 million and an annual gross merchandise volume of over 625.9 billion yen. Since its founding, Mercari, Inc. has continued to diversify its business. In September 2014, for example, the company expanded to the U.S., and in February 2019, it launched the contactless payment service "Merpay."

### Challenge

Monitoring and Logging Kubernetes Clusters to Protect Sensitive Information

Mercari was established in February 2013 with the mission of "creating a global marketplace that creates new value." Since then, the Mercari Flea Market App has grown to become one of the leading products of its kind. In February 2019, the company's subsidiary, Merpay, launched a contactless payment service of



[CASE STUDY. Mercari Uses Sysdig to Secure the Most Widely Used Flea Market App in Japanpdf](#)

[Cloud SecuritySysdig SecureKubernetes](#)

The graphic is a white rectangular panel with a light green geometric pattern in the background. At the top left, it features the Sysdig and AWS logos. Below the logos, the text 'SOLUTION BRIEF' is in a small green box. The main title is 'Sysdig Sage and Amazon Web Services (AWS)' in a large, bold, black font. Underneath the title is the subtitle 'Uncover Hidden Risks and Respond at Cloud Speed with the Power of Generative AI'. A short paragraph follows, explaining that Sysdig Sage extends the power of the Sysdig cloud security platform by using natural language to identify threats and respond faster. Below this paragraph are three bullet points with green checkmarks, each describing a capability: Multistep Reasoning, Multidomain Correlation, and Action Execution. To the right of these bullet points is a 'KEY BENEFITS' section with three green arrows pointing to the text: 'Uncover Hidden Risks and Attack Paths', 'Investigate and Remediate at Cloud Speed', and 'Supercharge Skills with Collective Intuition'. At the bottom left of the panel is a screenshot of the Sysdig Sage interface, showing a list of security events with various status indicators. To the right of the screenshot is a quote from onna, Principal Architect, stating that having an assistant that provides relevant context during an attack or for day-to-day tasks is extremely valuable. The onna logo and title are at the bottom right of the quote.

**sysdig | aws**

**SOLUTION BRIEF**

## Sysdig Sage and Amazon Web Services (AWS)

Uncover Hidden Risks and Respond at Cloud Speed with the Power of Generative AI

In the cloud, every second counts. Sysdig Sage extends the power of the Sysdig cloud security platform, enabling AWS users to use natural language to identify cloud threats and respond faster. It leverages the power of Sysdig runtime insights to reveal hidden connections between risks and security events that would otherwise go undetected. To achieve this, Sysdig's AI architecture is built on the following foundational capabilities:

- ✔ **Multistep Reasoning:** Uses an iterative process to explore multiple investigative steps before providing the most plausible answer.
- ✔ **Multidomain Correlation:** Correlates data from vulnerabilities, compliance, permissions, runtime, and CI/CD to get a complete picture of risks.
- ✔ **Action Execution:** Makes suggestions on further queries, actions, and next steps, and is able to execute these actions directly from chat.

**KEY BENEFITS**

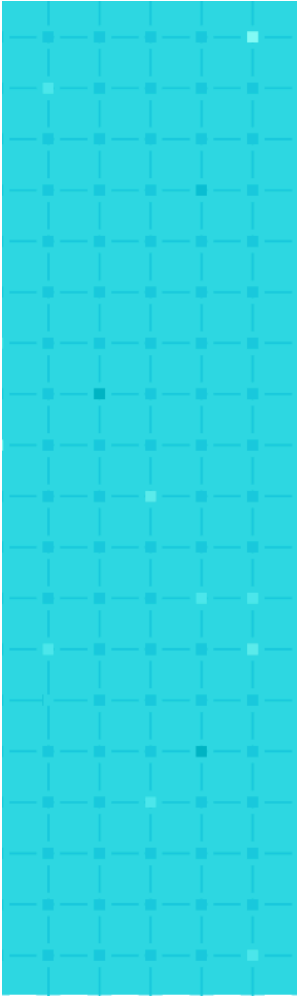
- ➔ Uncover Hidden Risks and Attack Paths
- ➔ Investigate and Remediate at Cloud Speed
- ➔ Supercharge Skills with Collective Intuition

“ Having an assistant that provides relevant context during an attack or for day-to-day tasks is extremely valuable. The architectural approach Sysdig has taken with Sysdig Sage is revolutionary and unlike anything we are seeing from other cloud security vendors”

**onna**  
Principal Architect

[BRIEF. Sysdig Sage AI and AWSpdf](#)

[Cloud SecuritySysdig SecureCloud computing security](#)



# Sysdig

## ATPCO

### Using Sysdig to Monitor and Secure Travel Data Services on Red Hat OpenShift.

As part of their cloud transformation efforts, ATPCO engaged the Sysdig Cloud-Native Visibility and Security Platform, along with the Red Hat OpenShift Container Platform built on Kubernetes. Together, Sysdig and Red Hat help simplify the complicated tasks of securing containers, understanding application behavior, and capturing detailed health, risk, and performance data. We spoke to the ATPCO Team and learned how Sysdig addressed their needs.

---

#### CASE STUDY



[Case Study: ATPCOpdf](#)

[OpenshiftRed Hat](#)

**sysdig** | CUSTOMER STORY **neo4j**

## Empowering Engineering to Reduce Risk at Neo4j

**75%** reduction in false positive alerts

**2 hours** saved per vulnerability

**80%** reduction in vulnerabilities

### Summary

Neo4j, the global leader in graph database technology, needed to maintain customer trust and secure sensitive data across highly regulated environments. Their existing security processes lacked central visibility, overwhelming engineers with false positives and slow remediation cycles. After adopting Sysdig, Neo4j transformed its vulnerability management program with in-use prioritization, automated workflows, and real-time detection. This alignment between security and engineering empowered teams to reduce risk, enable compliance, and accelerate secure innovation.

#### Key Results

- Security and engineering now work as one team with shared visibility and streamlined workflows
- Junior analysts resolve issues faster with contextual risk paths and real-time prioritization
- Neo4j proactively manages risk instead of reacting to noise or compliance deadlines

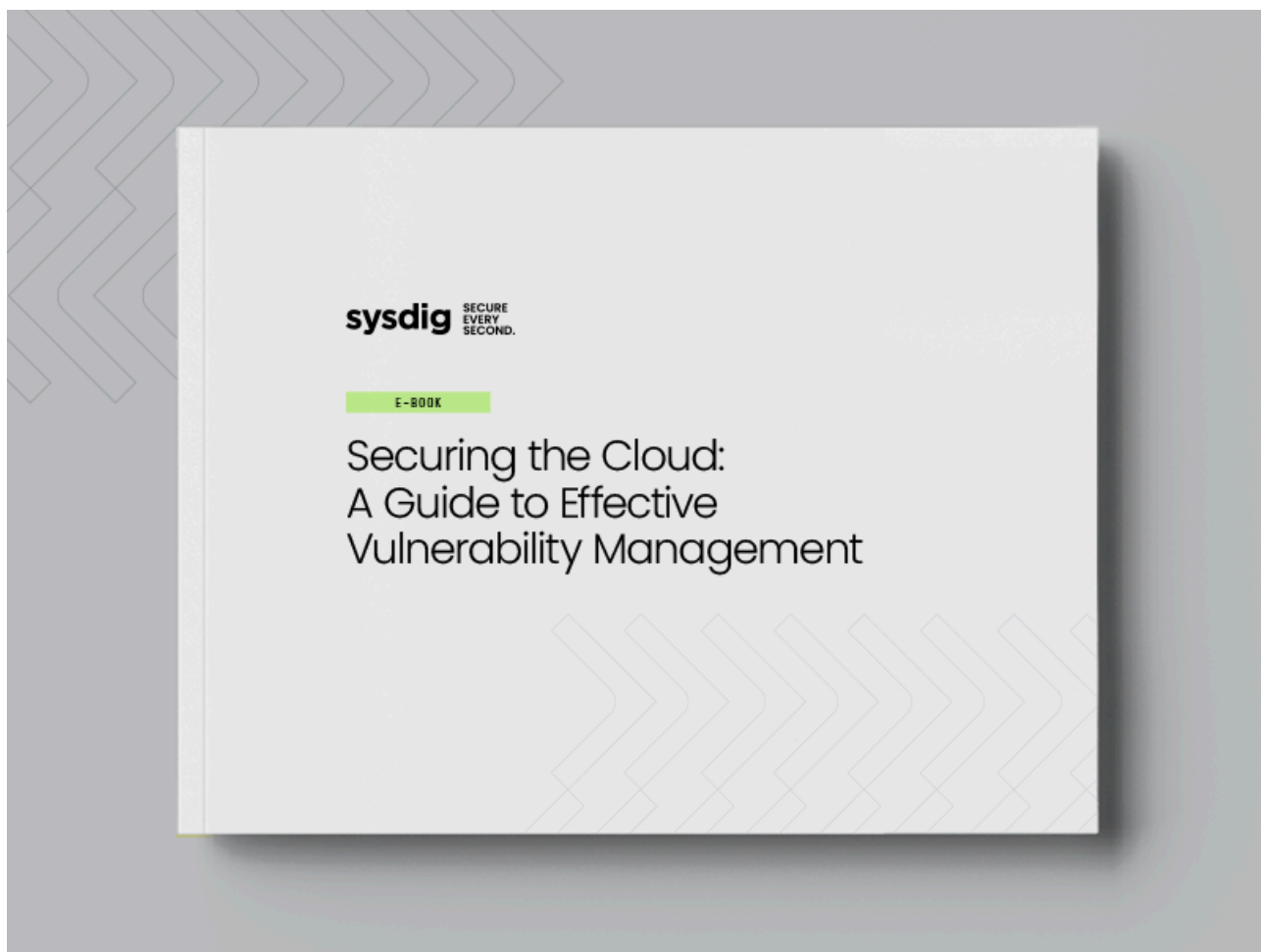
**Neo4j**  
Leader in graph databases and analytics for connected data

**HEADQUARTERS**  
Malmö, Sweden

**INDUSTRY**  
Software Technology

[CASE STUDY. Neo4j Case Study.pdf](#)

[AzureSysdig SecureAmazon Web ServicesKubernetes](#)



[GUIDE. Securing the Cloud A Guide to Effective Vulnerability Managementpdf](#)

[Cloud SecuritySysdig Secure](#)

**TAG CYBER**

**ANALYST REPORT:  
EDR AND CDR  
ARE DIFFERENT.  
HERE'S HOW.**

TAG CYBER ANALYST TEAM  
SUPERVISED BY  
DR. EDWARD AMOROSO



[REPORT. EDR and CDR are different. Here's howpdf](#)

[Cloud SecuritySysdig\\_SecureCloud MonitoringSysdig Monitor](#)



[Container and Kubernetes Securitywebpage](#)

[Cloud SecuritySysdig Secure](#)



[VIDEO. Getting started with secure DevOpsvideo](#)

[Cloud SecuritySysdig SecureKubernetes](#)



[VIDEO. Kubernetes and container topology mapping video](#)

[Docker Sysdig Secure Sysdig Monitor](#)

CUSTOMER STORY

# Santander Group's Ben Visa Vale Protects 800K Cardholders

Founded in 2018, Ben Visa Vale issues prepaid Visa credit cards to over 3,500 companies, with more than 800,000 cardholders between them. Based in Brazil, the company is part of the Santander Group – one of the world's largest multinational financial institutions. Today, Ben Visa Vale facilitates roughly \$36 million in transactions annually.

With 1 million benefits cards in a closed payment loop, Ben Visa Vale currently holds 3.5% of the benefits credit card market in Brazil.



**INDUSTRY**

Finance

**CHALLENGES**

- Forced to choose between delaying software or launching with vulnerabilities
- Lack of visibility into containers and Kubernetes environments
- Expensive, time-consuming compliance testing

**OUTCOMES**

- 70% less time spent on vulnerability management
- 65% fewer resources required for security testing
- 98% fewer vulnerabilities in the production environment

[CASE STUDY. Ben Visa Valepdf](#)

[Cloud SecuritySysdig\\_SecureCloud computing security](#)



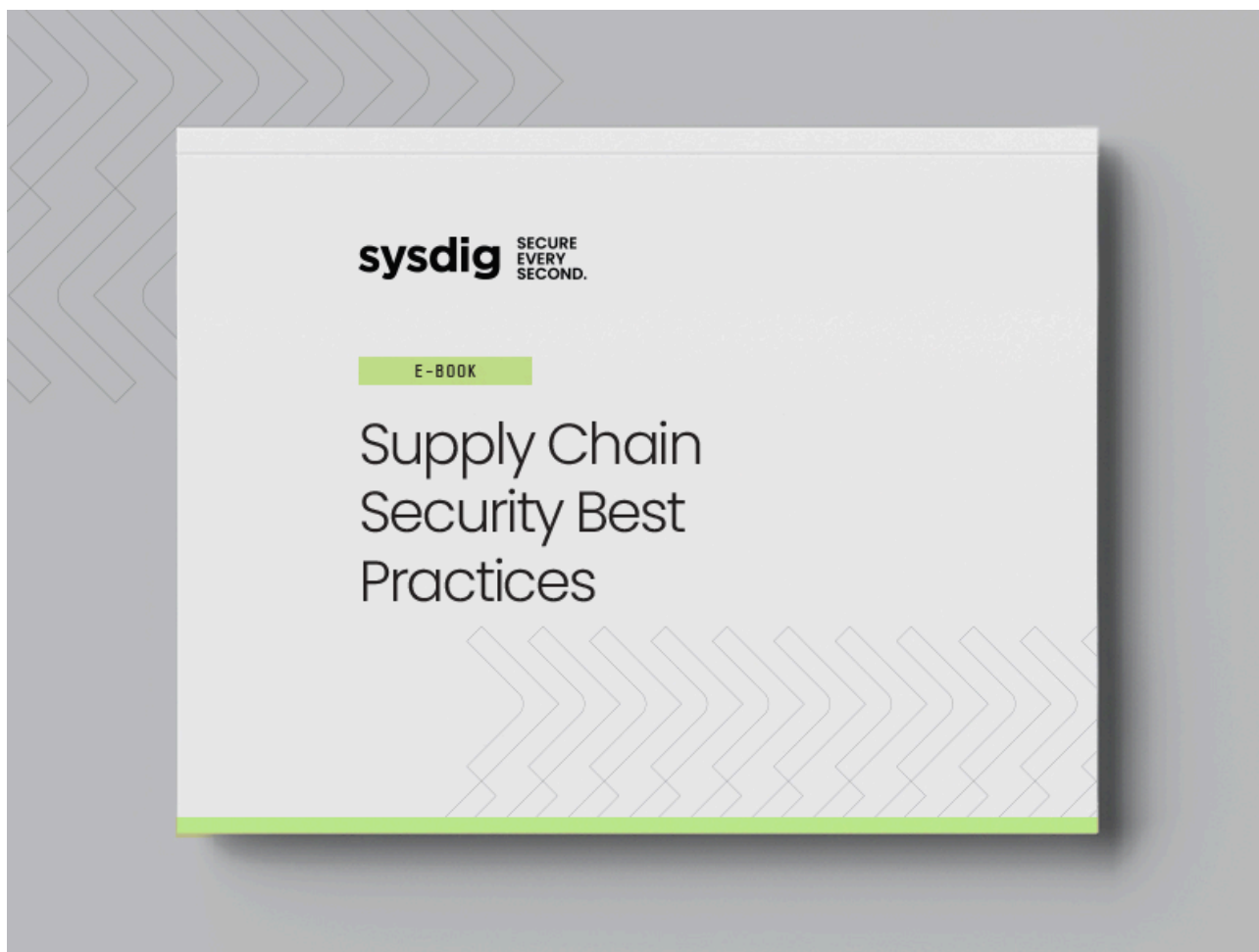
[PODCAST. Screaming in the Cloud: Making Sense of Data](#)[webpage](#)

[Cloud Security](#)[Sysdig Secure](#)



[WEBINAR. Image Scanning Best Practices for Containers and Kubernetes](#)[video](#)

[Cloud Security](#)[Sysdig Secure](#)[Kubernetes](#)



[GUIDE. Supply Chain Security Best Practicespdf](#)

[Cloud SecuritySysdig Secure](#)

FEATURED PARTNER

# sysdig + cybereason

Cloud attackers move fast.  
Sysdig and Cybereason help you move faster. [LEARN MORE →](#)

**10 minutes** — that's all it takes to execute an attack in the cloud after discovering an exploitable target. Outpacing attackers requires security teams to meet the S/S/S Benchmark, which specifies 5 seconds to detect, 5 minutes to triage, and 5 minutes to respond to threats.

**Detect, Investigate, and Respond Faster**

Sysdig and Cybereason help you focus on the most important tasks, such as investigating and resolving critical threats while improving MTTR and MTTD metrics.

Together, our solutions consolidate insights across clouds, endpoints, and broader IT environments to respond quickly to malicious operations.

**BENEFITS**

- **Accelerate threat detection & response**  
Sysdig's CDR alerts are ingested by Cybereason XDR to correlate and provide insights into the end-to-end attack story. Analysts can take rapid action based on recommended responses.
- **Comprehensive attack prevention**  
Get deep visibility into cloud and container activity. Gain a comprehensive view that spans across identities, endpoints, email networks and the cloud for threat correlation and response.

**Sysdig Secure Integration with Cybereason XDR**

```
graph LR; A[Cloud & Kubernetes] --> B[Detected Events  
Sysdig CDR]; B --> C[Consolidated Insights  
Cybereason XDR]; C --> D[MALOP]
```

[PARTNER BRIEF. Sysdig and Cybereasonpdf](#)

[Cloud SecuritySysdig SecureCloud computing securitycybersecurity](#)



# Runtime Insights Are Key To Shift-Left Security In Financial Services

As cloud migration gathers pace in the financial services industry, businesses are leveraging the opportunities for fast and efficient product innovation. But with this new development environment comes new security challenges and unknowns. To keep ahead of threats in an industry that is the [second-most targeted for attack](#), and maintain compliance in the face of increasingly demanding regulatory requirements, organizations require a comprehensive cloud security strategy.

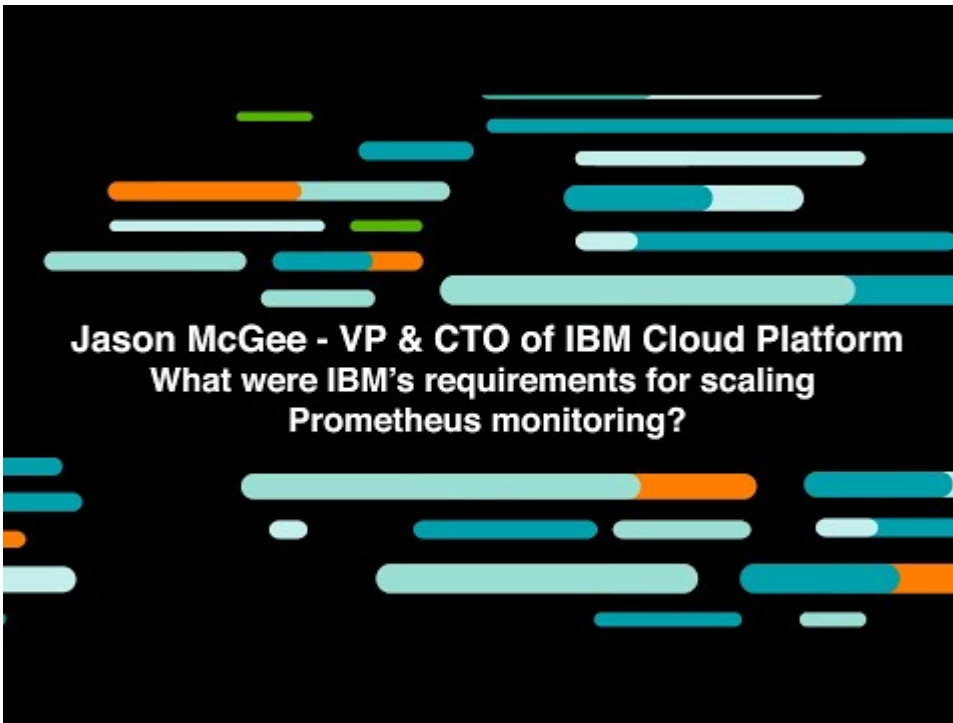
Such programs often emphasize one of two approaches: shift-left or shield-right. Shift-left focuses on processes and tooling that promote secure design and pre-release testing to identify security issues before they become production problems. Shield-right focuses on operational practices, security monitoring, and runtime security mechanisms to prevent security incidents and detect and respond to events as they occur. Both approaches are essential, but in practice, they often run in isolation.

Runtime insights are the glue between these two worlds, enabling organizations to prioritize and mitigate risk, detect and respond to threats, and scale their cybersecurity. This paper explores their importance for shift-left activities or preventative security, helping you avoid attacks on your organization's innovation in the cloud.



[WHITEPAPER. Runtime Insights Are Key To Shift-Left Security In Financial Servicespdf](#)

[Cloud SecuritySysdig Secure](#)



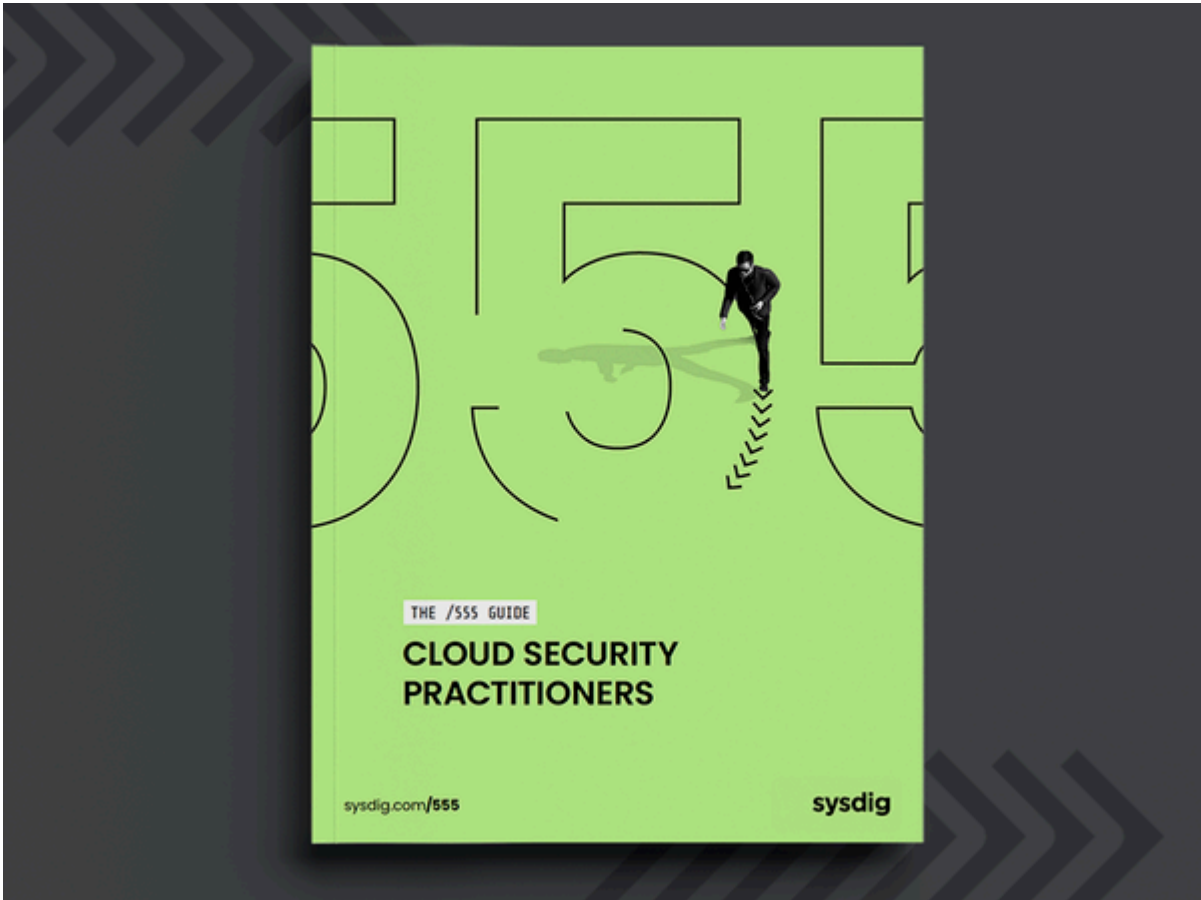
[VIDEO. Requirements for Scaling Prometheus: IBMvideo](#)

[Cloud SecuritySysdig\\_SecureCloud MonitoringIBM](#)



[GUIDE. Using Runtime Insights For Effective Cloud Security with Sysdig and AWSpdf](#)

[Cloud SecuritySysdig\\_SecureCloud computing security.](#)



[WHITEPAPER. The 555 Guide for Cloud Security Practitionerspdf](#)

[Cloud SecuritySysdig Secure](#)



[REPORT. SANS 2022 Cloud Security Surveypdf](#)

[Cloud SecuritySysdig Secure](#)



# 2022 Cloud-Native Threat Report

## EXECUTIVE SUMMARY



### Cloud Adversary Analysis: TeamTNT

Cryptojacking: low risk, high reward for cloud attackers

TeamTNT is a notorious cloud-targeting threat actor that generates the majority of their criminal profits through cryptojacking. Sysdig TRT attributed more than \$8,100 worth of cryptocurrency to TeamTNT, which was mined on stolen cloud infrastructure, costing the victims more than \$430,000. The full impact of TeamTNT and similar entities is unknowable, but at \$1 of profit for every \$53 the victim is billed, the damage to cloud users is extensive.



[BRIEF, 2022 Cloud-Native Threat Report Executive Summary.pdf](#)

[Cloud SecuritySysdig Secure](#)



## Container and Cloud Security Comparison Checklist: Sysdig vs Rapid7

### 55+ features compared



Don't rely on a tool that is blind to container threats. Tools like Rapid7 are composed of multiple products and lack the unified visibility you need to detect and respond to attacks across containers and clouds.

Your security stack needs to be:

- Built on open source.
- SaaS first.
- Instrumented to provide deep visibility with rich context across containers, Kubernetes, and cloud.

Run confidently with secure DevOps.

This checklist provides a feature comparison across container and cloud security between Sysdig Secure and Rapid7.

#### Coverage Areas

- Platform
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection (CWPP)
- Image Scanning
- Runtime Security
- Network Security
- Incident Response and Forensics
- Compliance



[GUIDE. Container & Cloud Security Comparison Checklist: Sysdig vs Rapid7pdf](#)

[Cloud SecuritySysdig Secure](#)



[WHITEPAPER. The 555 Guide for CISOs.pdf](#)

[Cloud SecuritySysdig Secure](#)



[REPORT. 2024 Global Threat Report.pdf](#)

[Cloud SecurityCloud Threats](#)

# A guide to PCI Compliance in Containers and Kubernetes



[GUIDE. A guide to PCI Compliance in Containers and Kubernetespdf](#)

[Sysdig Secure](#)



CASE STUDY

**COMPANY DETAILS:**

Worldpay by FIS is a Fortune 500, global merchant payment processing and services provider.

**BUSINESS NEED:**

- Easy-to-use, self-service security platform
- Security that can scale with FIS
- Reduce operational burden
- Streamline PCI compliance for merchants

**CHALLENGES:**

- Scalable visibility across cloud environments
- Lack of understanding vulnerability severity and remediation steps
- Limited audit trail for troubleshooting and compliance

**BUSINESS IMPACT OF SYSDIG:**

- Improved communication between DevOps and security teams in order to ship PCI-compliant apps faster
- Accelerated identification and remediation of vulnerabilities to avoid customer impact

**SYSDIG PLATFORM BENEFITS:**

- Reduced operational overhead by 50%
- Gained efficiency for troubleshooting and forensics with audit trails
- Achieved results in minutes with fast onboarding
- Reduced maintenance with a SaaS-first solution
- Simplified achieving PCI compliance

**INFRASTRUCTURE:**

Multi Cloud— AWS, Azure and Google

**ORCHESTRATION:**

Red Hat OpenShift



## Worldpay Gains Competitive Edge with Faster Delivery of Innovative PCI-Compliant Payment Solutions Globally

### Overview

Worldpay by FIS is one of the largest global merchant payment processing and services providers. With billions of transactions annually, the Worldpay footprint spans 146 countries and encompasses more than 300 payment types in 126 currencies.

Their goal is to help merchants use technology to solve banking, payment, and investing challenges, as well as deliver superior experiences for their customers. Worldpay does this by building self-service, cloud-based platforms that make it easy for merchants to do business.

### Challenge

As a major player in the ever-evolving payment business, Worldpay must innovate quickly to stay ahead of the competition. For example, when COVID-19 hit in early 2020, contactless payments – voice payments, retina-based payments, and digital payment mediums such as UPI, AePS, etc. – were reprioritized in an instant. To speed application build and delivery to meet changing demand, Worldpay utilizes a Red Hat OpenShift-based environment built on Kubernetes.

As an organization that helps merchants meet PCI compliance, ensuring uptime and security for applications is of critical importance for Worldpay. The company's developers need visibility into their various environments, which requires a security and observability solution that highlights potential issues across clusters and clouds.



[CASE STUDY. Worldpay Gains Competitive Edge with Faster Delivery of Innovative PCI-Compliant Payment Solutions Globallypdf](#)

[Sysdig SecureKubernetesSysdig Monitor](#)



[SERVICE BRIEF: Dedicated CSA Servicepdf](#)

[Sysdig SecureSysdig Monitor](#)



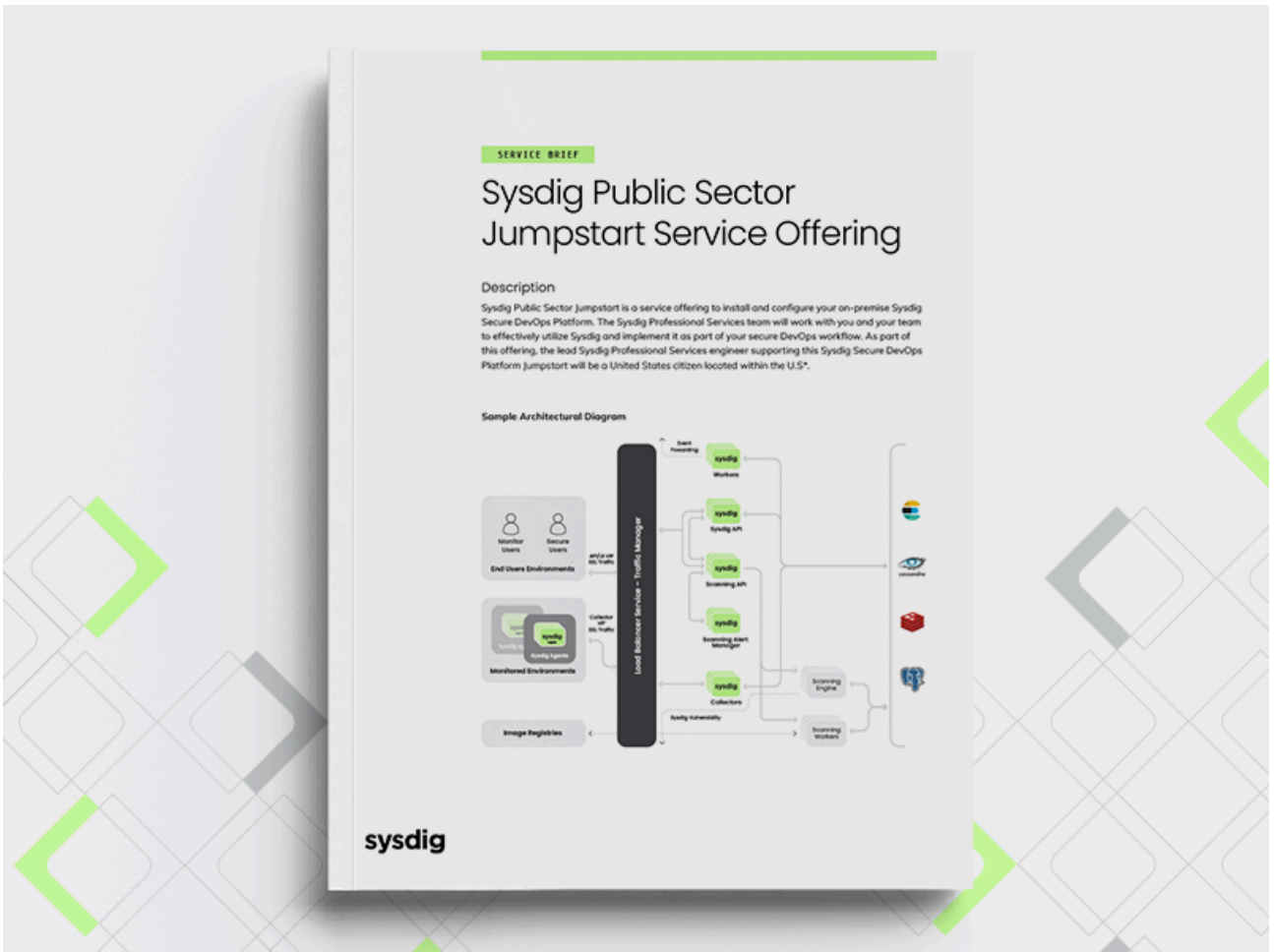
[INFOGRAPHIC. The Evolution of Modern Cloud Securitypdf](#)

[Cloud Security](#)



[VIDEO. Sysdig Company Overview: Reliable and Secure Cloud-Native Applicationsvideo](#)

[Sysdig SecureSysdig Monitor](#)



[BRIEF. Sysdig Public Sector Jumpstartpdf](#)

[Cloud Security](#)

The graphic is a product brief for Sysdig Secure. It features a grey background with a white central panel. The top section has a green highlight on the word 'Security' in the title 'Unify Your Cloud Security'. Below the title is the subtitle 'End-to-end CNAPP Powered by Runtime Insights'. The main body of text describes Sysdig Secure as the industry's only cloud-native application protection platform (CNAPP) that provides comprehensive cloud visibility, preventing attacks before they happen and responding to active threats with cloud speed. It mentions the Cloud Attack Graph, the neural center of Sysdig's CNAPP, and how it correlates assets, activity, and risks across domains. A quote from a Platform Tech Team Lead is included, stating: "In the cloud, everything happens fast. Time is of the essence when stopping attacks. Breaches can be very costly. Sysdig enables us to quickly detect and respond to cloud attacks at cloud speed by knowing what is happening, the exact container or location in the cloud, and what is causing it, versus hours to detect and understand what needs to be done." Below the quote is the signature 'Platform Tech Team Lead' and a small circular icon. The bottom section of the white panel lists three key features: 'Cloud Attack Graph' (correlate and contextualize data), 'Runtime Insights' (leverage knowledge of what's in use), and 'Real-Time Threat Detection' (multilayered detection combining ML, drift control, and Falco rules). The Sysdig logo is at the bottom left of the white panel.

## Unify Your Cloud Security

### End-to-end CNAPP Powered by Runtime Insights

Sysdig Secure is the industry's only cloud-native application protection platform (CNAPP) that delivers the breadth of coverage and depth of insights required to protect your cloud environments. Sysdig consolidates cloud security into a single platform that focuses on the most critical risks across your cloud infrastructure, spanning containers, cloud services, servers, identities, and third-party apps.

With comprehensive cloud visibility, Sysdig Secure prevents attacks before they happen and detects and responds to active threats with cloud speed. Cloud Attack Graph, the neural center of Sysdig's CNAPP, correlates assets, activity, and risks across domains. By leveraging runtime insights, it provides the context needed to instantly prioritize and mitigate the top risks across your cloud environment.

“In the cloud, everything happens fast. Time is of the essence when stopping attacks. Breaches can be very costly. Sysdig enables us to quickly detect and respond to cloud attacks at cloud speed by knowing what is happening, the exact container or location in the cloud, and what is causing it, versus hours to detect and understand what needs to be done.”

Platform Tech Team Lead

- Cloud Attack Graph**  
Correlate and contextualize data from multiple sources to identify and visualize the riskiest combinations and hidden attack paths.
- Runtime Insights**  
Leverage knowledge of what's in use to prioritize which risks to address immediately and unlock time for your security and developer teams.
- Real-Time Threat Detection**  
Multilayered detection combining ML, drift control, and Falco rules curated by Sysdig's Threat Research Team to detect threats in seconds and respond in minutes.

**sysdig** SECURE  
BY  
DESIGN

[PRODUCT BRIEF. Sysdig Securepdf](#)

[Sysdig Secure](#)

As organizations move to containers for next-generation infrastructure and applications, they must balance the need for security without negatively impacting the frequency of software deployments.

## Definitive Guide for Evaluating Container and Kubernetes Security Tools

December 2019

**Written by:** Gary Chen, Research Director, Software Defined Compute, and Frank Dickson, Program Vice President, Cybersecurity Products

### Introduction

Containers are rapidly becoming the foundation for next-generation infrastructure and applications. Enterprises use Kubernetes (K8s), the de facto industry standard for container orchestration, to more rapidly deploy container-based software in order to support their digital transformation initiatives. However, containers and Kubernetes do not cause disruption just because they are new technologies. Kubernetes and containers are disruptive because they are often tied to culture, process, and organizational change. Operations and development teams are learning to work more closely with DevOps, and applications are architected with microservices for greater efficiency, scalability, and economies of parallel development.

Given these changes, IDC data regarding container adopters shows that security is the number 1 challenge. As organizations move to automated software build pipelines with continuous integration and continuous delivery (CI/CD) and agile development methodologies, building security into this new approach without slowing down the speed and frequency of software deployments is one of the security challenges. Another challenge is that containers introduce a new environment with a new packaging format and a different management paradigm with Kubernetes. Without container- and Kubernetes-specific security tools, visibility into the container layer will be nonexistent, creating a security blind spot.

### Considerations for Container and Kubernetes Security

Just like with server virtualization, containers introduce a new layer, and all infrastructure disciplines must build integration with and insight into this layer in order to remain relevant. The network flows, input/output (I/O), and program execution happening at the container layer are invisible to existing virtual machine (VM) or bare metal tools. While containers don't invalidate the need for tools at that level, the use of containers does require the need for container-specific insights. Containers are also intimately tied to many other transformations, such as CI/CD, DevOps, and microservices. Some of the impacts these transformations have on security are as follows:

- » Software is increasingly delivered through complex, automated CI/CD pipelines. While these pipelines simplify the process of software delivery, they can also be leveraged for security by inserting vulnerability scanning and tests into the process earlier rather than doing it all at once at the end. This is often referred to as "shifting left."

### AT A GLANCE

#### WHAT'S IMPORTANT

Organizations are increasingly turning to containers and Kubernetes to improve the efficiency and scalability of software development efforts. Containers introduce new security issues, highlighting the need for container-specific security tools.

[IDC. Definitive Guide for Evaluating Container and Kubernetes Security Tools.pdf](#)

[Sysdig SecureKubernetes](#)



BRIEF

# Sysdig and Microsoft Azure

Secure and monitor containers, Kubernetes, and cloud services on Microsoft Azure.

“ Sysdig reduced our operational burden by 50 percent . ”  
- DevSecOps Cloud Security Architect, FIS

## Why Sysdig

- Single view of risk with no blind spots
- Prioritize what matters with no guesswork
- Fix once at the source with no wasted time



## How It Works



## Key Use Cases

### Container/K8s Security

- Image Scanning
- Kubernetes Security
- Runtime Security
- Compliance
- Network Security
- Incident Response
- Forensics

### Cloud Security

- Infrastructure as Code security
- Cloud Security Posture Management (CSPM)
- Cloud workload protection platform (CWPP)

### Monitoring

- Cloud Monitoring
- Container Monitoring
- Kubernetes Monitoring
- Prometheus Monitoring
- Custom Metrics
- Troubleshooting

## Our Customers



LEARN MORE

[sysdig.com/azure](https://sysdig.com/azure)

Copyright © 2022 Sysdig, Inc. All rights reserved. PB-006 Rev. F 12/22

# Microsoft Partner



[SOLUTION BRIEF. Sysdig and Microsoft Azurepdf](#)

[Azure](#)



[VIDEO. Sysdig Technical Deep Dive: From Wireshark to Sysdigvideo](#)

[Sysdig SecureSysdig Monitor](#)



[SERVICE BRIEF. Admissions Controllerpdf](#)

[Sysdig SecureSysdig Monitor](#)



CASE STUDY

**COMPANY DETAILS:**

The leading global provider of integrated travel, expense, and invoice management solutions for businesses and government agencies.

**BUSINESS NEED:**

- Deliver secure financial applications globally
- Ensure always on platform availability
- Deliver applications quickly and safely to stay competitive

**CHALLENGES:**

- Prometheus was an operational burden
- Manual scanning was labor intensive, slowing them down
- Lack of data for troubleshooting and compliance audits

**BUSINESS IMPACT OF SYSDIG:**

SAP Concur delivers a global, always on platform, that meets security and compliance requirements. New services are brought to market faster.

**SYSDIG PLATFORM BENEFITS:**

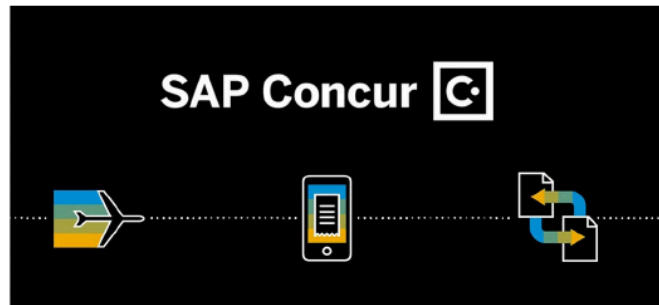
- Automation saves 10,000+ hours
- Secure DevOps approach, single agent is more cost effective
- Forensics, even when containers are gone
- Platform scales with K8s growth- 20x since inception
- Audit trails to ease the burden of audits

**INFRASTRUCTURE:**

Amazon Web Services (AWS) and on-prem

**ORCHESTRATION:**

Kubernetes



## SAP Concur Delivers Secure, Compliant Solutions to More than 50M End Users Globally

### Overview

SAP Concur is a SaaS company that provides travel, expense, and invoice management services to businesses and government agencies. With a global customer reach that includes more than 25,000 SMBs in North America alone, SAP Concur is operating a massive infrastructure at scale. Rolling out new, reliable, and always on services as securely as possible is of the utmost importance to the business.

SAP Concur made the decision to move from a monolithic architecture to microservices for the flexibility in delivering applications faster. Four years after that journey began, SAP Concur now has a team of 20 that is responsible for a container ecosystem that consists of more than 2,000 nodes in production.

### Challenge

Building microservices at SAP Concur started with a small tiger team. As Mike Luedke, Director Engineering at SAP Concur explained, "We started off as a grassroots effort. There were a few of us from different teams that got started originally building a cluster. Eventually, we then opened that up to some early adopters within Concur. After that, it gained traction pretty quickly. We went from an informal group managing this thing, to where it became clear that this was gonna have a definite future at Concur. At that point, we started to build a formalized team around it."



[CASE STUDY. SAP Concur Delivers Secure, Compliant Solutions to More than 50M End Users Globallypdf](#)

[Sysdig SecureCloud MonitoringKubernetesOpen Source](#)



## Goldman Sachs: Accelerating Business With Microservices

### Company Details

The **Goldman Sachs Group** is a leading global financial institution that delivers a broad range of financial services to a large and diversified client base that includes corporations, financial institutions, governments and individuals. Founded in 1869, the firm is headquartered in New York and maintains offices in all major financial centers around the world.

### Industry

Financial Services

### Sysdig Solutions

Sysdig Secure, Sysdig Monitor

### Infrastructure

Amazon Web Services (AWS), Google Cloud Platform (GCP), On-Prem, Private

For Goldman Sachs, speed of software innovation is critical. The ability to be competitive relies on a talented team with software applications that help deliver insights to clients. The engineering division at Goldman Sachs is on the front lines of ensuring the professionals at the firm have the tools necessary to advise customers as the global economy changes.

With this in mind, Goldman Sachs has adopted DevOps principles and microservices to deliver containerized applications at scale across on-premises and cloud environments. As a result of this transformation, Goldman Sachs has accelerated software delivery velocity from one build every two weeks to over a thousand per day.



| Case Study: Goldman Sachs

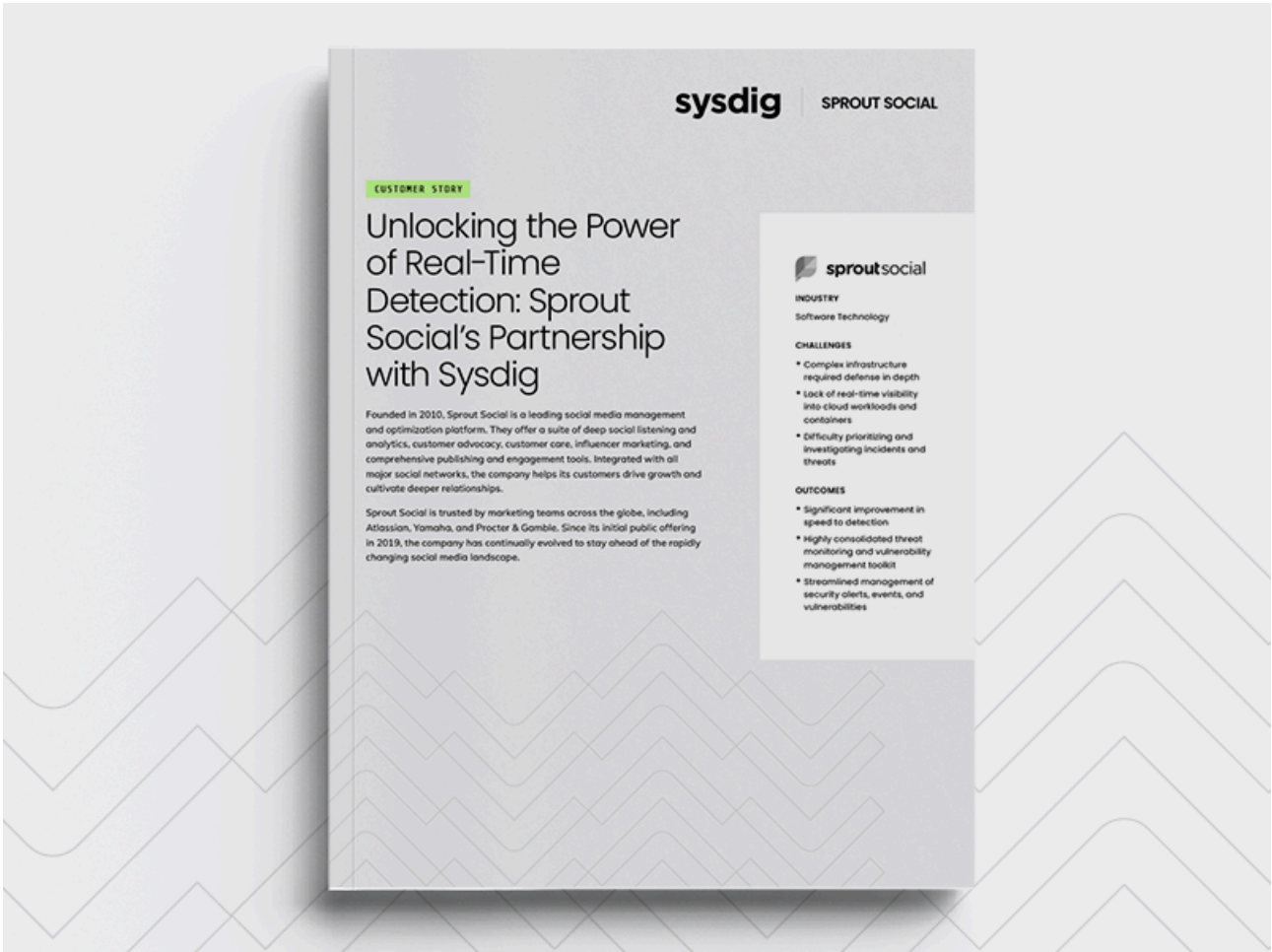
[CASE STUDY. Goldman Sachs Accelerating Business with Microservicespdf](#)

[Sysdig Secure](#)

The image shows a customer story graphic for Sysdig and JumpCloud. At the top left, it says 'sysdig | CUSTOMER STORY' and at the top right is the 'jumpcloud.' logo. The main headline reads 'JumpCloud Outpaces Threats: 80% Fewer Vulnerabilities and 99.8% Less Noise'. Below the headline is a photograph of a man with a beard and glasses, wearing an orange t-shirt, sitting at a desk with two computer monitors. A green banner across the photo contains three statistics: '99.8% reduction in vulnerability noise', '80% reduction in active vulnerabilities', and '3 to 5 fewer engineering hires required'. Below the photo, there is a 'Summary' section with a paragraph of text, a 'Key Results' section with three bullet points, and a box on the right containing 'JumpCloud' description, 'HEADQUARTERS: Colorado, United States', and 'INDUSTRY: Financial Technology'.

[Jump Cloud Sysdig Customer Storypdf](#)

[Sysdig Secure](#)



[CASE STUDY. Unlocking the Power of Real-Time Detection: Sprout Social's Partnership with Sysdigpdf](#)

[Cloud Security](#)



# Cloud and Container Security for Software & Technology Services

## Cloud Apps Need a New Security Stack

Companies are adopting containerized microservices, CI/CD, and on-demand cloud services to speed innovation. This new environment creates security challenges:

- Teams lack visibility to cloud resources, workloads, access and activity to manage risk
- There is an endless list of vulnerabilities and misconfigurations to fix
- Existing EDR tools cannot detect and stop container and cloud breaches

Securing the cloud requires a security stack built on open standards that automates security and closes the loop from source to run.

## Secure Your Containers, Kubernetes and Cloud

Using in use runtime filters, Sysdig provides unique runtime insights to both detect threats in real time and prioritize the highest impact actions so teams can rapidly respond. With Sysdig, teams can also aggregate security findings by root cause to fix at the source.

"Sysdig is a complete CWPP. The Sysdig agent can be installed anywhere a workload is running. It provides deep runtime insights that enable us to immediately find threats and rapidly respond."

**Moustapha Diago**  
Data Security Architect, Talend



"Sysdig was the only solution to provide one comprehensive report on the OpenSSL vulnerability in one place."

**Michal Pazucha**  
Security Architect, Beekeeper



"When the news on Log4j came out, we received calls from our customers asking what the impact was. We were able to scan our containers quickly for vulnerabilities and we knew immediately if there were any issues. Using Sysdig Secure, we were able to find out in less than five minutes what the potential risk would be."

**Sam Brown**  
Director Information Security, Expel



### Vulnerability Management

- Automate container and host scanning
- Prioritize vulnerabilities based on runtime context
- Block vulnerabilities preproduction and monitor for new CVEs at runtime

### Cloud Security Posture Management (CSPM)

- Manage excessive permissions in AWS using an integrated CIEM tool
- Enforce least-privilege policies that grant just enough permissions

### Cloud and Container Compliance

- Meet regulatory compliance standards for containers and cloud
- Save time with out-of-the-box policies that map to specific compliance controls and implement file integrity monitoring (FIM)

### Infrastructure as Code (IaC) Security

- Manage risk when configuring cloud infrastructures and shift security further left with IaC security
- Strengthen cloud and Kubernetes security, as well as compliance, by using policy as code

Try Sysdig for free

START FREE TRIAL

Copyright © 2023 Sysdig, Inc. All rights reserved. PB-019 Rev. A 2/23

[BRIEF: Cloud and Container Security for Software & Technology Servicespdf](#)

[Cloud SecurityCloud Monitoring](#)



# Four Phases of Successful Docker Adoption


**Industry**  
Société Générale, one of Europe's leading financial services groups and a major player in the economy for over 150 years, supports 25 million clients every day with more than 117,000 staff in 66 countries.

**Industry**  
Financial Services

**Sysdig Solution**  
Sysdig Monitor

**Infrastructure**  
Amazon Web Services (AWS)

**Orchestration**  
Docker Swarm; Red Hat Openshift



Société Générale is France's third largest bank by total assets and the sixth largest in Europe. Headquartered in Paris, the multinational financial services firm has divisions supporting global transaction banking, international retail banking, corporate and investment banking, private banking, asset management, and securities services.

Société Générale uses digital strategies to transform banking relationships with its customers, whether they be individuals, institutions, large companies or private banking clients. To keep up with changing digital usage by consumers, Société Générale is increasing its innovation in web and mobile services to ensure its customers enjoy greater autonomy, simplicity, and security.



[CASE STUDY. Societe Generale: Four Phases of Successful Docker Adoptionpdf](#)

[Docker](#)



# Top Business Impacts of Cloud Breaches and How to Mitigate Them

Although you are increasingly seeing cloud breaches in the news, that is still only a fraction of what is actually happening, as cybercrime is vastly underreported. Cyber attacks have become pervasive, so it is not a question of 'if' your organization will experience a cloud breach. It will happen, but you can take steps to block attacks and reduce the frequency and business impact of cyber incidents.



Our team analyzed publicized breaches to understand the tactics threat actors used to gain access and successfully progress the attack to cause serious harm, some with broad and long lasting implications. We identified security posture aspects that facilitated the breach, which you can use to assess your risk exposure. Our suggestions to mitigate risk provide steps your teams can take to prevent or minimize the impact of cyber attacks.

[BRIEF: Top Business Impacts Of Cloud Breaches And How To Mitigate Thempdf](#)

[Cloud SecurityCloud Monitoring](#)



# 7 Cloud Security Requirements for Financial Service Providers

Point solutions aren't protecting your cloud. Here are 7 requirements your security should meet to stay compliant and stop breaches.



1

## Prioritize Risk

Use runtime intelligence to prioritize and focus on the most important risks across workloads, cloud configurations, and permissions.

**95%**  
less vulnerability noise  
with Sysdig runtime insights<sup>1</sup>

**worldpay**  
from FIS

“Showing us what is important and how to fix it is key to reducing our risk. The tool doesn't waste our time.”

**Natnael Teferi**  
Lead DevSecOps Cloud Security Architect

“With Sysdig, we consolidated 6 tools to 1, saving

2

## Consolidate Tools

tools to 1, saving money and time.”

**IT Security Manager**  
Leader in Bot Mitigation

### Consolidate Tools

Simplify your toolkit and eliminate visibility gaps with a single, unified platform to deliver cloud security, monitoring and forensics.

3

### Shift-Left

Design securely and catch security problems early before they move into production.

**742%**

average annual increase in software supply chain attacks over the past 3 years<sup>2</sup>

**3.5x**

increase in web app and API attacks in the financial services sector in 2022<sup>3</sup>

4

### Shield-Right

Defend your production environment. Zero in on the threats and vulnerabilities that appear unexpectedly in runtime.

5

### Manage Cloud Access

Manage excessive permissions and enforce least-privileged access across human and non-human identities.

**90%**

of granted permissions aren't used<sup>4</sup>

**87%**

say open source is valuable to the future of the financial

6

### Use Open Standards

Ensure transparency,

services industry<sup>5</sup>

customizability, and portability with a security platform built on open source standards.

7

## Respond at Cloud Speed

Leverage continuous and real-time streaming detection to respond to events as they occur in ever-changing cloud environments.

## Goldman Sachs

“At our scale, it is important to have a complete record, even if the containers last only a few seconds. We need to be able to capture this data at scale to conduct not only forensics investigations, but also security audits.”

**Wes Williams**  
Global Head of Security  
Incident Response

Sources: 1 [Sysdig](#) 2 [Sonatype State of the Software Supply Chain](#) 3 [Akamai](#) 4 [Sysdig 2022 Cloud-Native Security and Usage Report](#) 5 [Linux Foundation](#)

## Ready to Supercharge Your Cloud Security?

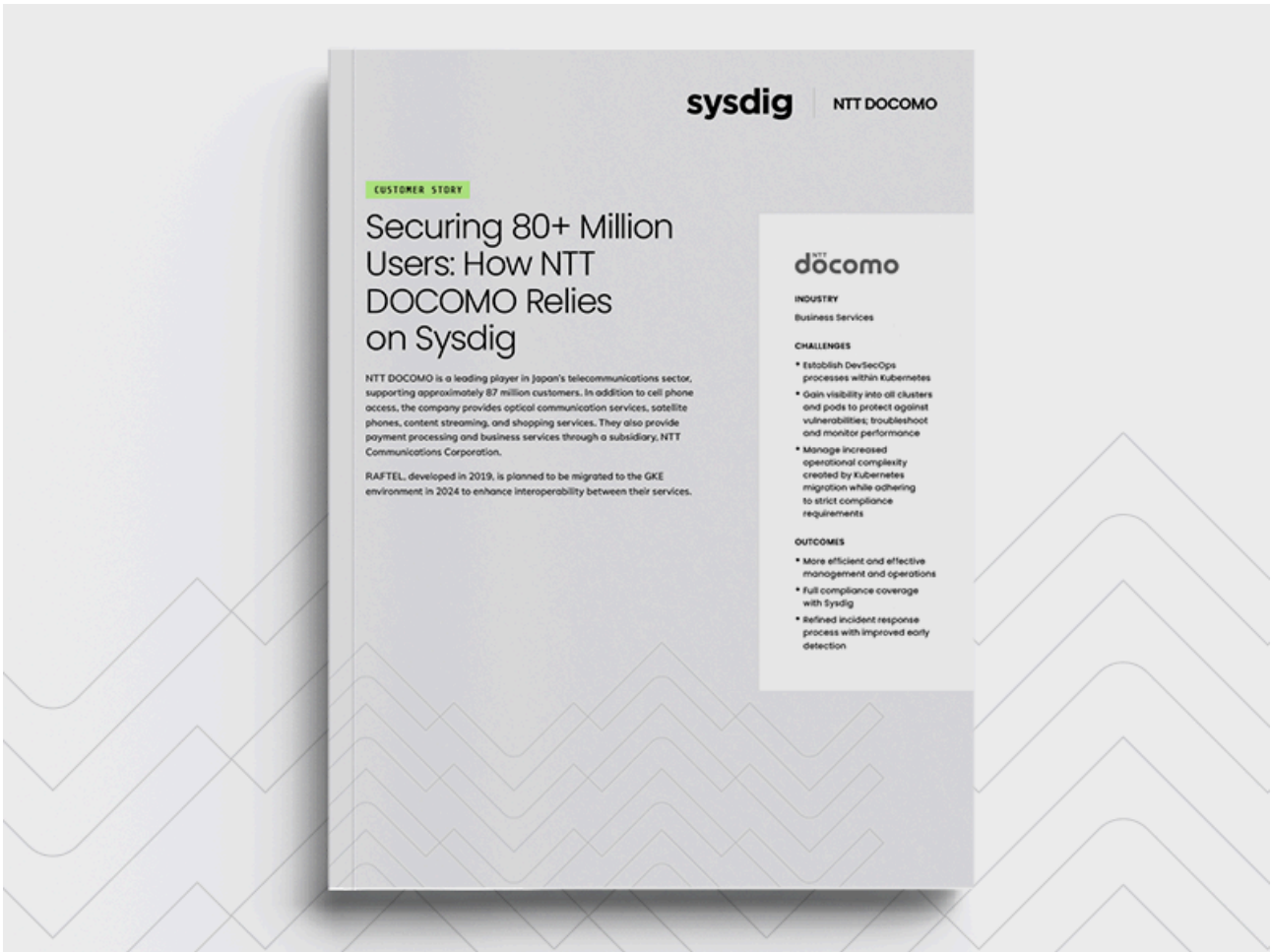
Defend against advanced threats while delivering a standout customer experience. Book your personalized live demo with a Sysdig expert today.

[GET A DEMO](#)

Copyright © 2023 Sysdig, Inc.  
All rights reserved. ING-009 Rev. A 7/23

[INFOGRAPHIC. 7 Cloud Security Requirements for Financial Service Providerspdf](#)

[Cloud Security](#)



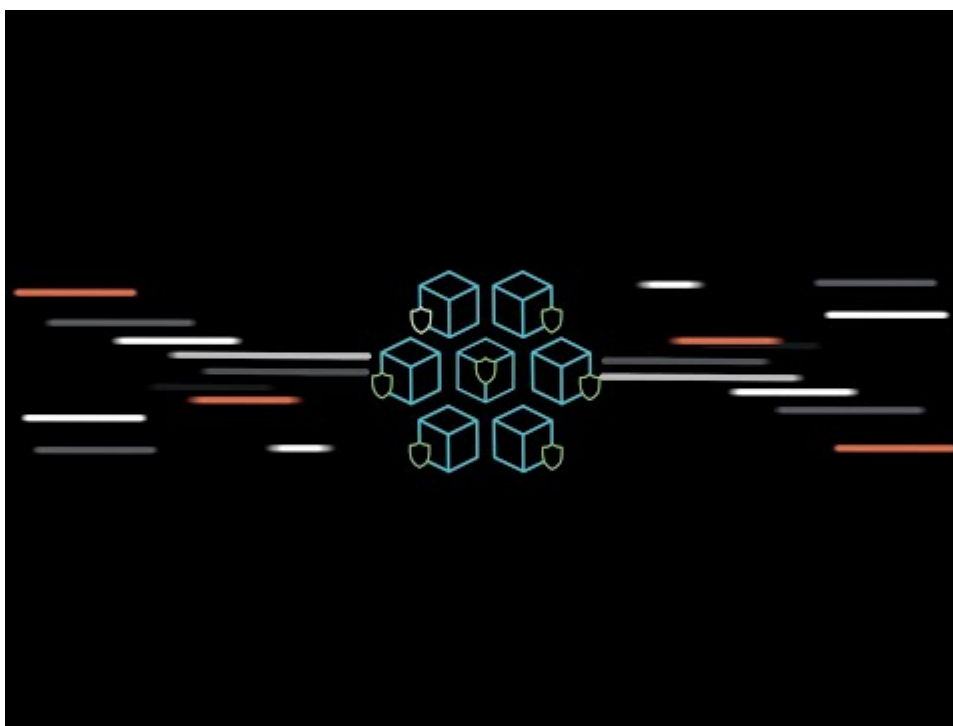
[CASE STUDY. Securing 80+ Million Users: How NTT DOCOMO Relies on Sysdigpdf](#)

[Cloud Security](#)



[WEBINAR. Getting Started with Runtime Security for Containers & Kubernetes](#)[video](#)

[Cloud Security](#)[Kubernetes](#)



[VIDEO. Sysdig Secure Overview](#)[video](#)

[Sysdig Secure](#)



#### CASE STUDY

## Monitoring Java in Docker at CDK

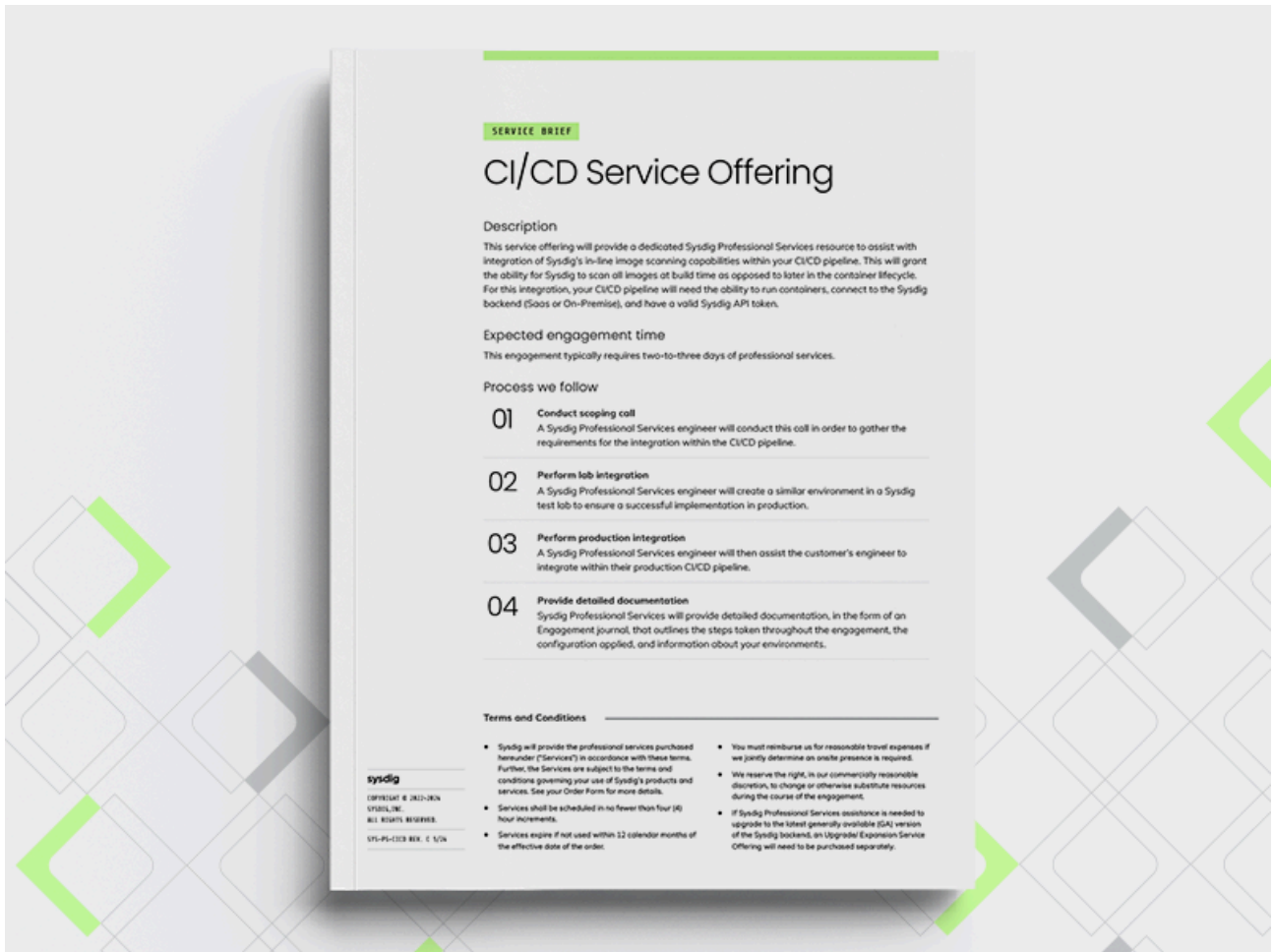
---

The Digital Marketing business unit of CDK global shifted to a containerized approach for their next generation infrastructure. One of the challenges they ran into was how to monitor java applications in containers. Learn about some of their challenges and their use of Sysdig in this context.



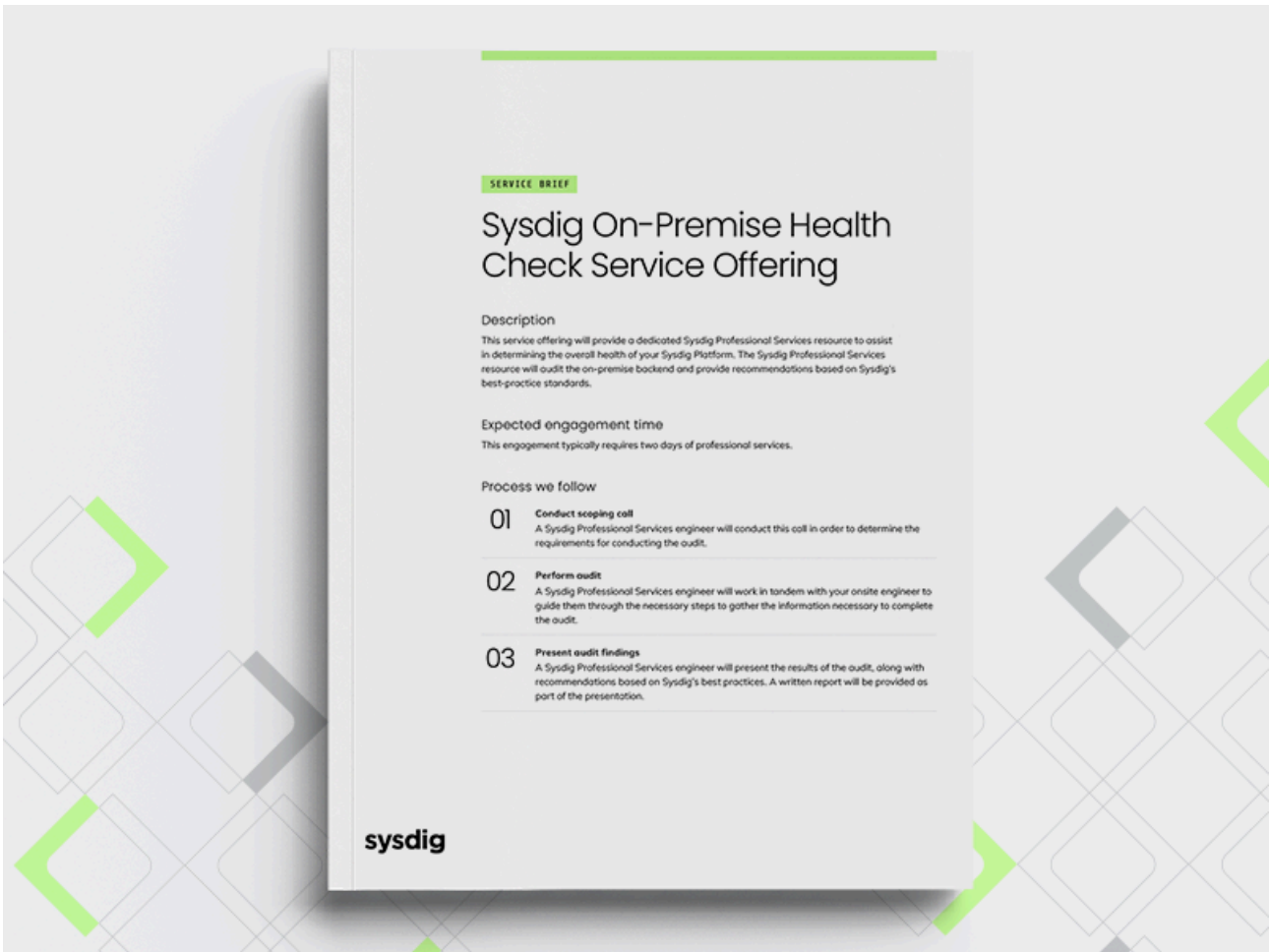
[CASE STUDY. Monitoring Java in Docker at CDKpdf](#)

[DockerSysdig\\_Monitor](#)



[SERVICE BRIEF. CI/CDpdf](#)

[Sysdig SecureSysdig Monitor](#)



[SERVICE BRIEF. On-Premise Health Checkpdf](#)

[Sysdig SecureSysdig Monitor](#)



[VIDEO. Cloud Native visibility and security with Sysdig Platform.video](#)

[Sysdig SecureSysdig Monitor](#)



[BRIEF. Sysdig on AWS: Real-time cloud security for financial servicespdf](#)

[Cloud Security](#)

FROST & SULLIVAN

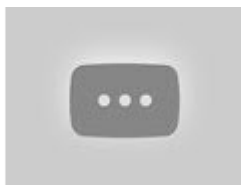
*SysDIG*

# 2022 COMPANY OF THE YEAR

*GLOBAL  
CONTAINER SECURITY INDUSTRY*

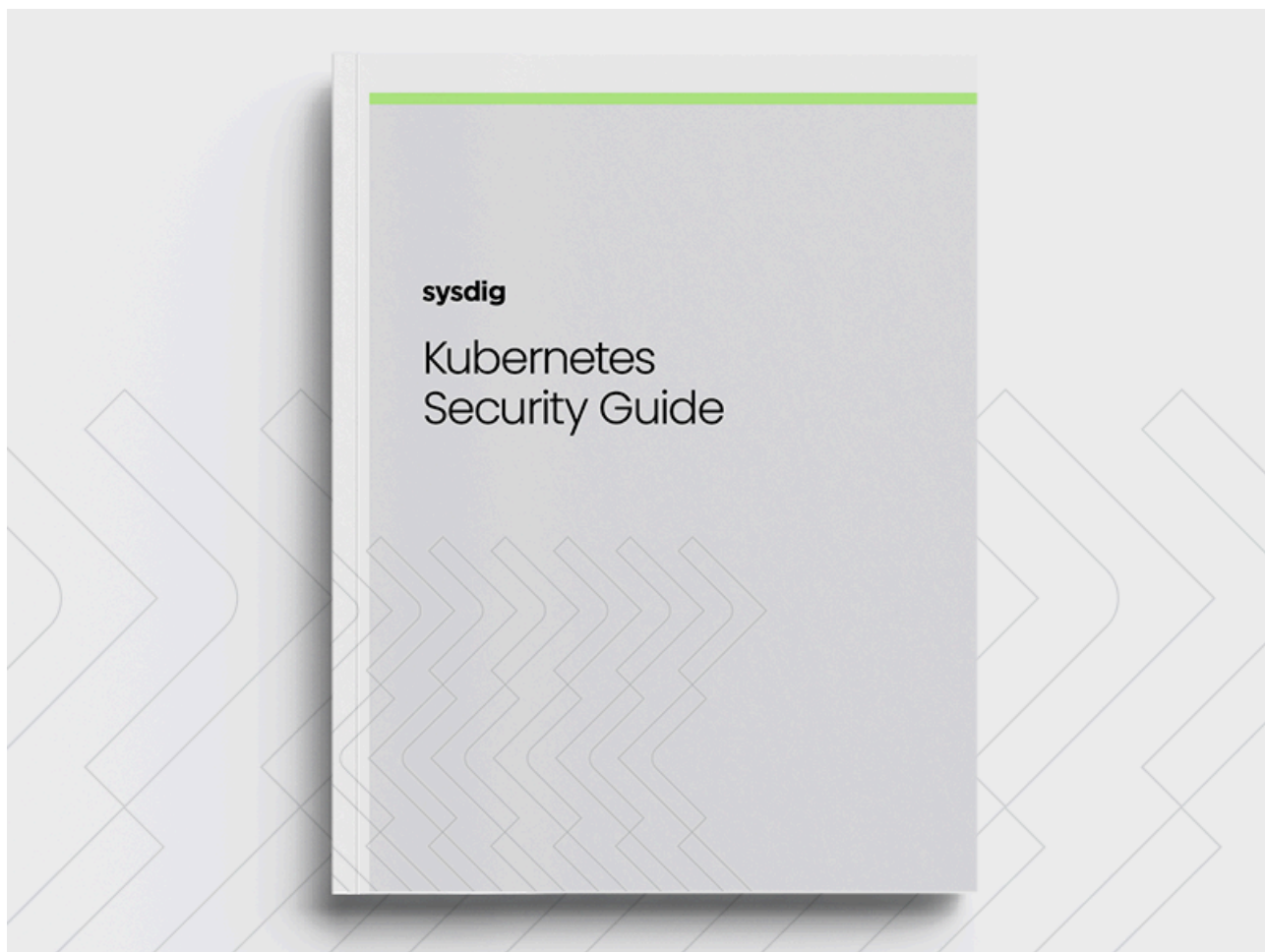
[BRIEF. Frost Sullivan Award 2022.pdf](#)

[Sysdig Secure](#)



[VIDEO. Attack Path & Risk Findingsvideo](#)

[Cloud Security](#)



[GUIDE. Kubernetes Security Guidepdf](#)

[Sysdig SecureKubernetes](#)

**sysdig** | CUSTOMER STORY **CoinDCX**

### India's Largest Crypto Exchange Triples Threat Remediation Speed with Sysdig

**70%** reduction in misconfigurations

**12x** faster vulnerability remediation

**67%** less time spent on reporting tasks

**Summary**

As India's largest cryptocurrency exchange, CoinDCX needed to scale security in an environment defined by rapid growth, evolving compliance demands, and increasingly sophisticated cloud threats. Fragmented tools and manual processes left security teams struggling with visibility gaps, delayed remediation, and regulatory blockers. By adopting Sysdig, CoinDCX modernized its security stack, streamlining detection, automating vulnerability management, and gaining the visibility needed to proactively manage risk and drive continuous improvement across its cloud infrastructure.

**Key Results**

- Customizable detections tailored to company-specific issues
- Automated reporting enables better communication and prioritization
- Comprehensive security including CDR, vulnerability management, and CSPM

**CoinDCX**  
India's crypto giant, 50M+ users strong

**HEADQUARTERS**  
Mumbai, India

**INDUSTRY**  
Financial Technology

[CASE STUDY. CoinDCX.pdf](#)

[AWS Amazon Web Services CSPM Cryptomining](#)

**RADAR REPORT**

**SECURITY & RISK**

**Chris Ray**

**CLOUD WORKLOAD SECURITY (CWS)**

[GigaOm Radar 2024 - Cloud Workload Security \(CWS\)webpage](#)

[Cloud SecurityCloud MonitoringCloud computing security](#)



## TOP 10 USE CASES for Securing Cloud and Containers with Sysdig Secure

When migrating apps to the cloud or developing in modern cloud-native environments, organizations struggle to put together a security plan and get the visibility required to manage security risk, continuously meet and validate compliance, as well as implement real-time protection across cloud and containers.

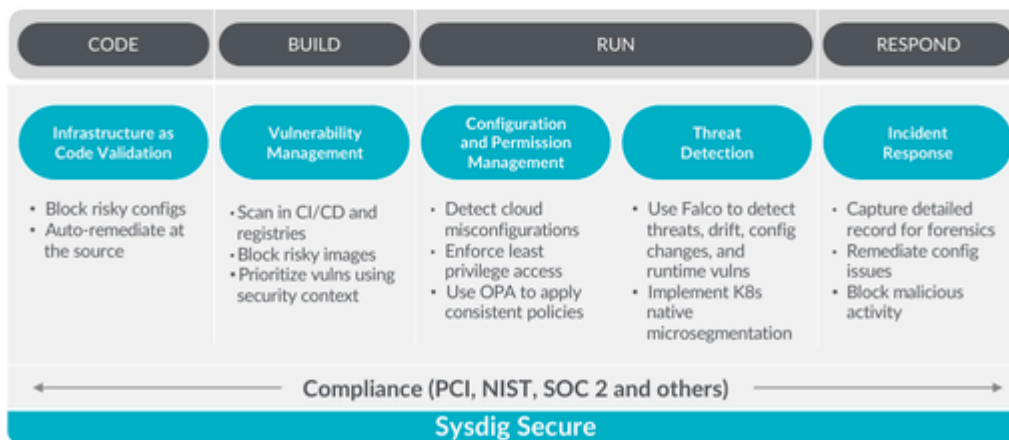
With Sysdig, security, DevOps, and developer teams can find and prioritize software vulnerabilities pre-deployment and in production, detect and respond to

threats, and manage cloud configurations, permissions, and compliance.

From containers and Kubernetes to cloud services, with Sysdig, you get a single view of risk from source to run, with no blind spots, no guesswork, and no black boxes.

Below are the top 10 security use cases supported by Sysdig Secure for organizations to securely run apps in the cloud.

### Secure Containers, Kubernetes and Cloud Services



TOP 10 USE CASES | 1  
for Securing Cloud and Containers with Sysdig Secure

[USE CASE. Top 10 Use Cases for the Sysdig Platformpdf](#)

[Sysdig SecureKubernetesSysdig Monitor](#)



CASE STUDY

COMPANY DETAILS:

Beekeeper is the operating system for frontline businesses. With all communications, systems, and resources in one place, Beekeeper empowers frontline managers and employees to be more agile, productive, and safer in the workplace. The company believes in the potential of every employee and is dedicated to building secure, scalable technology that transforms how frontline teams, managers, and corporate offices work together.

BUSINESS NEED:

- Deliver a secure platform that protects customer data
- Provide remote, frontline workers with reliable applications

TECHNICAL NEED

- Gain insight into anomalous behaviors and potential threats
- Obtain visibility of cloud security posture and increase responsiveness to security and performance incidents

CHALLENGES

- Lack of visibility across security and DevOps workflows
- Targeting faster time-to-resolution
- Manual reviews and reporting was time intensive
- Reached an inflection point with Falco, needed more out-of-the-box functionality

BUSINESS IMPACT OF SYSDIG

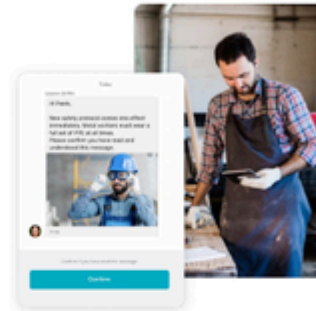
- Provides a single platform for security and DevOps teams to secure and monitor app health
- Gives the team confidence in their app security, enabling them to ship apps faster
- Pinpoints issues and potential threats faster
- Frees up engineering and security resources to focus on core business functions with automation
- Accelerates and streamlines compliance with simpler, more robust reporting

INFRASTRUCTURE

Amazon Web Services; Google Cloud Services Platform

ORCHESTRATION

Amazon Elastic Kubernetes Service (EKS); Google Kubernetes Engine (GKE)



## Beekeeper Serves Up Secure Communications, Data, and Applications Across Cloud Environments

### Overview

Beekeeper was created to help geographically distributed and remote workers stay connected to one another and to customers through its mobile and desktop platform. The company's applications enable secure information sharing between essential frontline workers, as well as deliver key communications and critical tools necessary for clients to succeed at the edge of their businesses.

"Every person that uses our platform demands a high-quality experience," says Michal Pazucha, Security Architect at Beekeeper. "Whether it's an HR manager delivering training across a distributed workforce or if employees in the field are filling out a customer intake form, things have to work flawlessly every time."

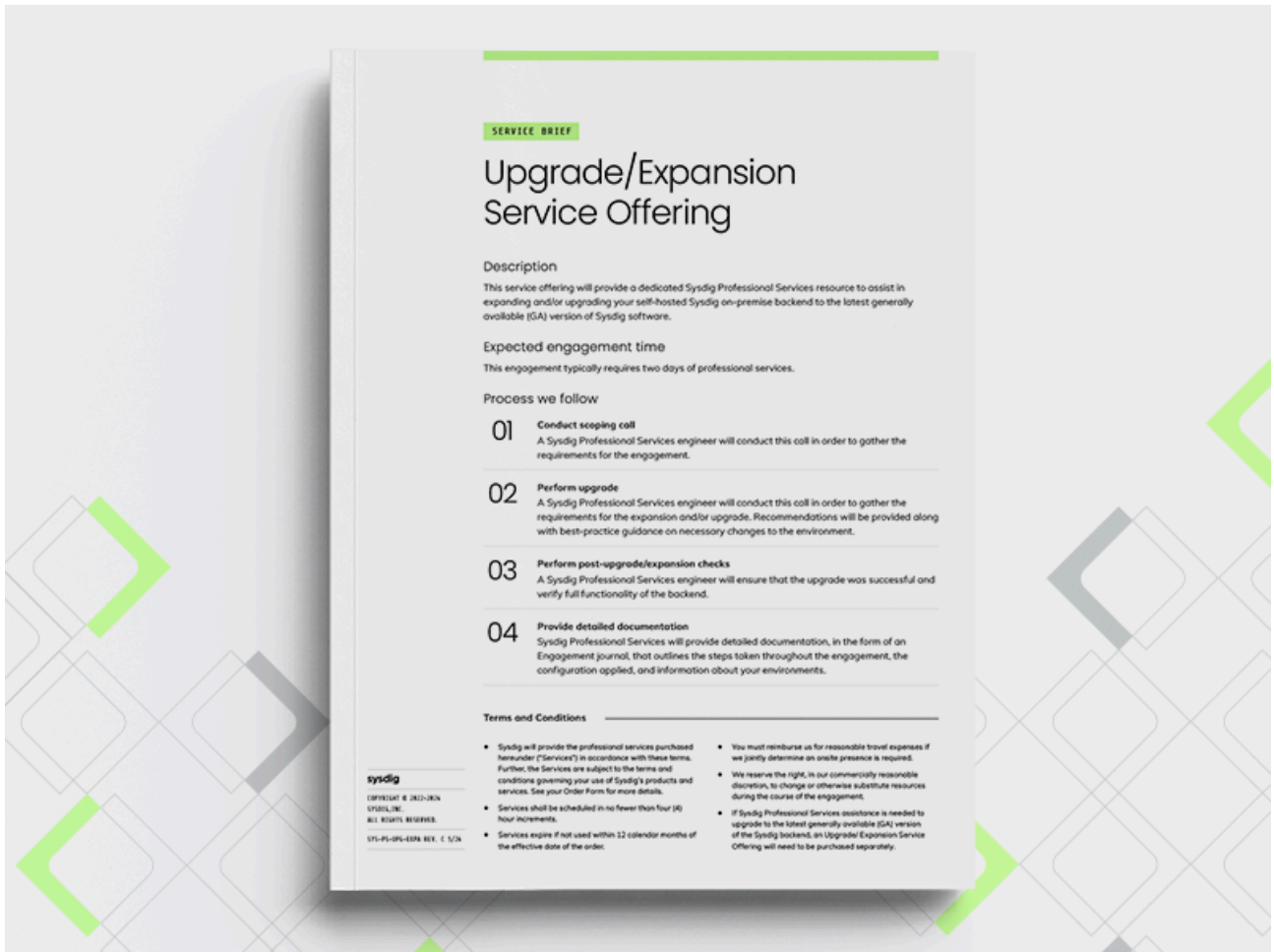
### Security is top priority

Choosing to embrace DevOps practices, Beekeeper wanted to take a disciplined approach with how new



[CASE STUDY. Beekeeper Serves Up Secure Communications, Data, and Applications Across Cloud Environments.pdf](#)

[Sysdig SecureSysdig Monitor](#)



[SERVICE BRIEF. Upgrade And Expansionpdf](#)

[Sysdig SecureSysdig Monitor](#)



[Evolution Of Cloud Security E Bookpdf](#)

[Cloud Security](#)



[BRIEF. 4 Ways Sysdig Enables Value with Cloud and Container Adoptionpdf](#)

[Cloud Security](#)



**sysdig** | CUSTOMER STORY 

## Good-Enough Security Isn't Good Enough When You Serve a Billion People

**>100 million**  
daily authentication requests  
secured with zero latency

**Doubled**  
compliance posture  
in six months

**>1.4 billion**  
biometric identities protected  
with real-time threat detection

### Summary

The Unique Identification Authority of India (UIDAI) runs the world's largest biometric identity system, securing sensitive data for over 1.4 billion people across India. To meet soaring demand and modernize security, UIDAI began migrating from virtual machines to the Kubernetes private cloud environment, which is targeted by attack activity daily.

That's where **Sysdig** came in. With deep **runtime insights**, real-time threat detection, and full support for on-premises architectures, Sysdig helped UIDAI secure hundreds of containerized workloads without compromise, strengthening compliance, improving visibility, and protecting services that millions rely on every day.

#### Key Results

- Enabled instantaneous threat detection and faster response by integrating runtime visibility and streamlining security operations center (SOC) workflows.
- Improved efficiency by filtering out irrelevant vulnerabilities and zeroing in on what's actually running.
- Maintained zero performance impact while securing over 100 million daily authentications.

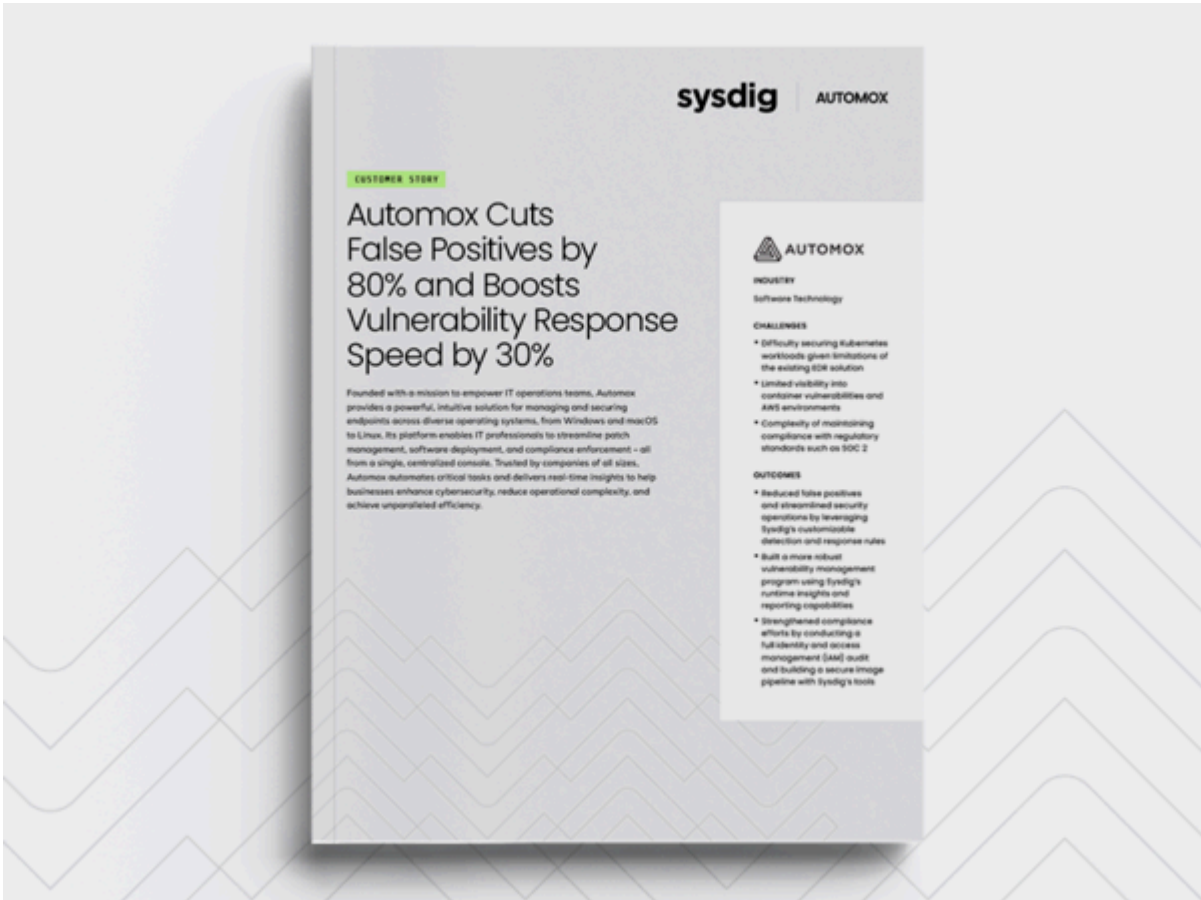
**UIDAI**  
Securing the identities of 1.4 billion people across India.

**HEADQUARTERS**  
Delhi, India

**INDUSTRY**  
Government

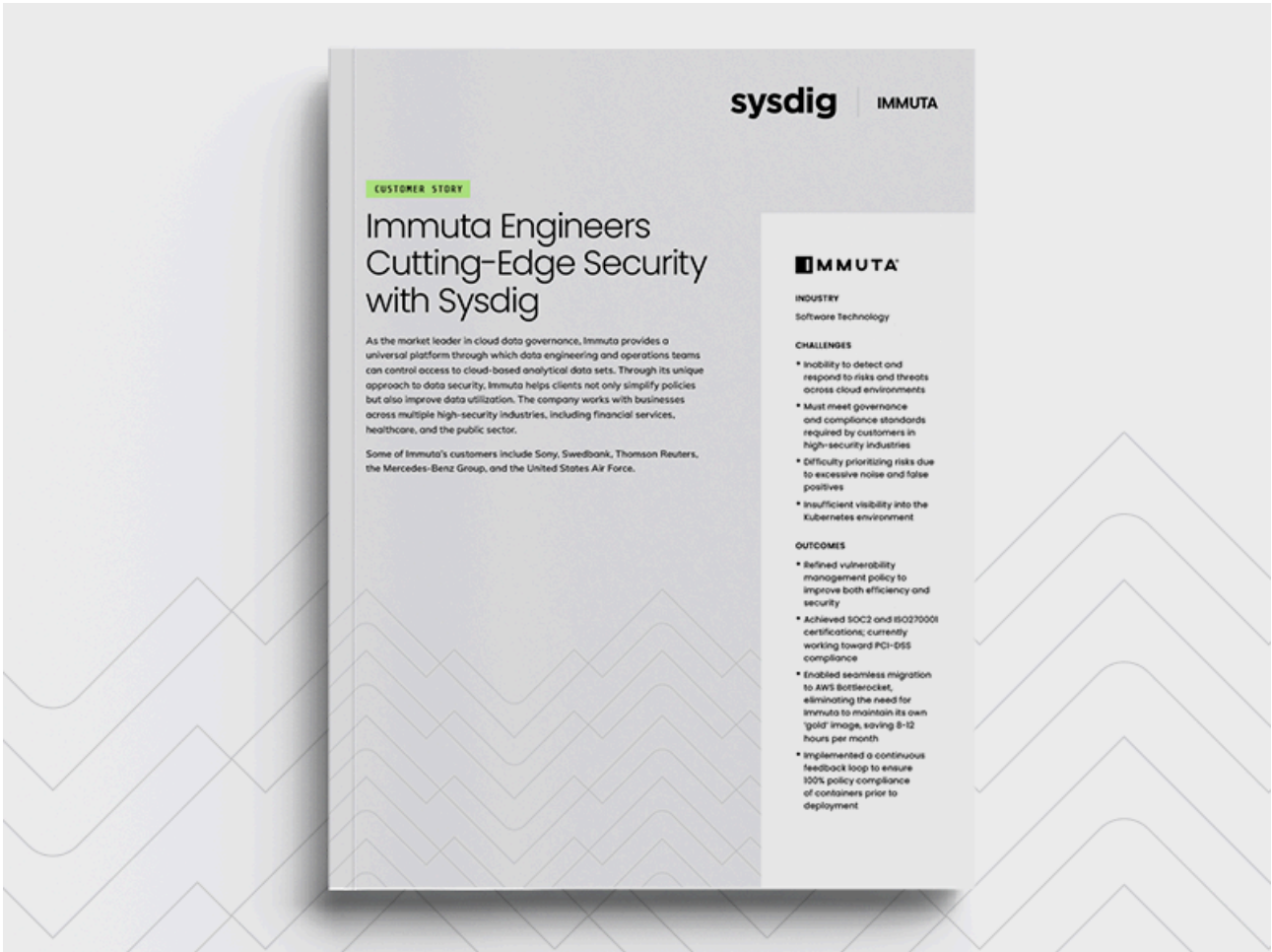
[CASE STUDY. UIDAI.pdf](#)

[Sysdig SecureCloud computing security](#)



[CASE STUDY. Automox Cuts False Positives by 80% and Boosts Vulnerability Response Speed by 30%.pdf](#)

[Sysdig SecureAmazon Web Services](#)



[Immuta Case Study.pdf](#)

[Sysdig Secure](#)



[VIDEO. Rethinking Cloud Security with a CNAPPvideo](#)

[Cloud Security](#)



CASE STUDY

**COMPANY DETAILS:**

ICG Consulting is a cloud-hosted vendor management and back office solution for leading companies, including Duke Energy, US Foods, and Love's Travel Stops. The company provides vendor portals, web invoicing, workflow management software, and dynamic discounting along with other solutions to help businesses communicate, collaborate, and transact.

**BUSINESS NEED:**

- Increase visibility into cloud infrastructure and enhance reporting.
- Gain cost and staffing efficiencies to compete with larger consulting firms.
- Add value to business relationships by improving intelligence and focusing resources on clients' biggest security challenges.

**TECHNICAL NEED**

- Reduce noise and alert fatigue.
- Automate reporting to enable employees to focus on core functions.
- Accelerate time to identify and fix critical vulnerabilities.

**CHALLENGES:**

- Reducing risk without slowing down development.
- Supporting the client's journey to maturity from on-prem environments to the cloud.
- Empowering a small team with more robust security and monitoring capabilities without adding overhead.

**BUSINESS IMPACT OF SYSDIG:**

- Helped generate 15% cost savings by improving the allocation of cloud resources with better capacity planning.
- Eliminated need to hire up to two additional analysts through automation.
- Achieved 30% reduction in alerts without sacrificing security.
- Improved reporting and information sharing with clients, leading to better decision making.
- Increased release pace by 10% per week.

**INFRASTRUCTURE:**

Amazon Web Services (AWS)

**ORCHESTRATION**

Amazon Elastic Kubernetes Service (EKS)



## ICG Consulting leverages Sysdig and AWS to compete with major shops

Since 1990, ICG Consulting has been a trusted expert in back-office applications, such as business process automation, advanced technology, and systems integration. As a result, the company has established a diverse book of clients, which includes major financial services organizations, energy companies, well-known hospitality brands, and diversified shipping and logistics conglomerates. As a software as a service (SaaS) provider, ICG Consulting is acutely aware that cloud-native challenges need cloud-native solutions, that existing tools cannot be applied to secure cloud workloads, and that any cloud-native tools a company adopts should be easy to deploy and scale.

"Everything we do is cloud hosted. Obviously, when we launched more than 30 years ago, everything was on-prem, but now it is all cloud hosted," said Jim O'Rourke, Director of Business Development at ICG Consulting.

With the shift to cloud-based services, ICG Consulting clients can better scale with the accelerated growth that



[CASE STUDY. ICG Consulting leverages Sysdig and AWS to compete with major shopspdf](#)

[Sysdig SecureSysdig Monitor](#)



## Quby.

Monitoring + Securing Mesos Marathon and Java Applications on AWS.

CASE STUDY

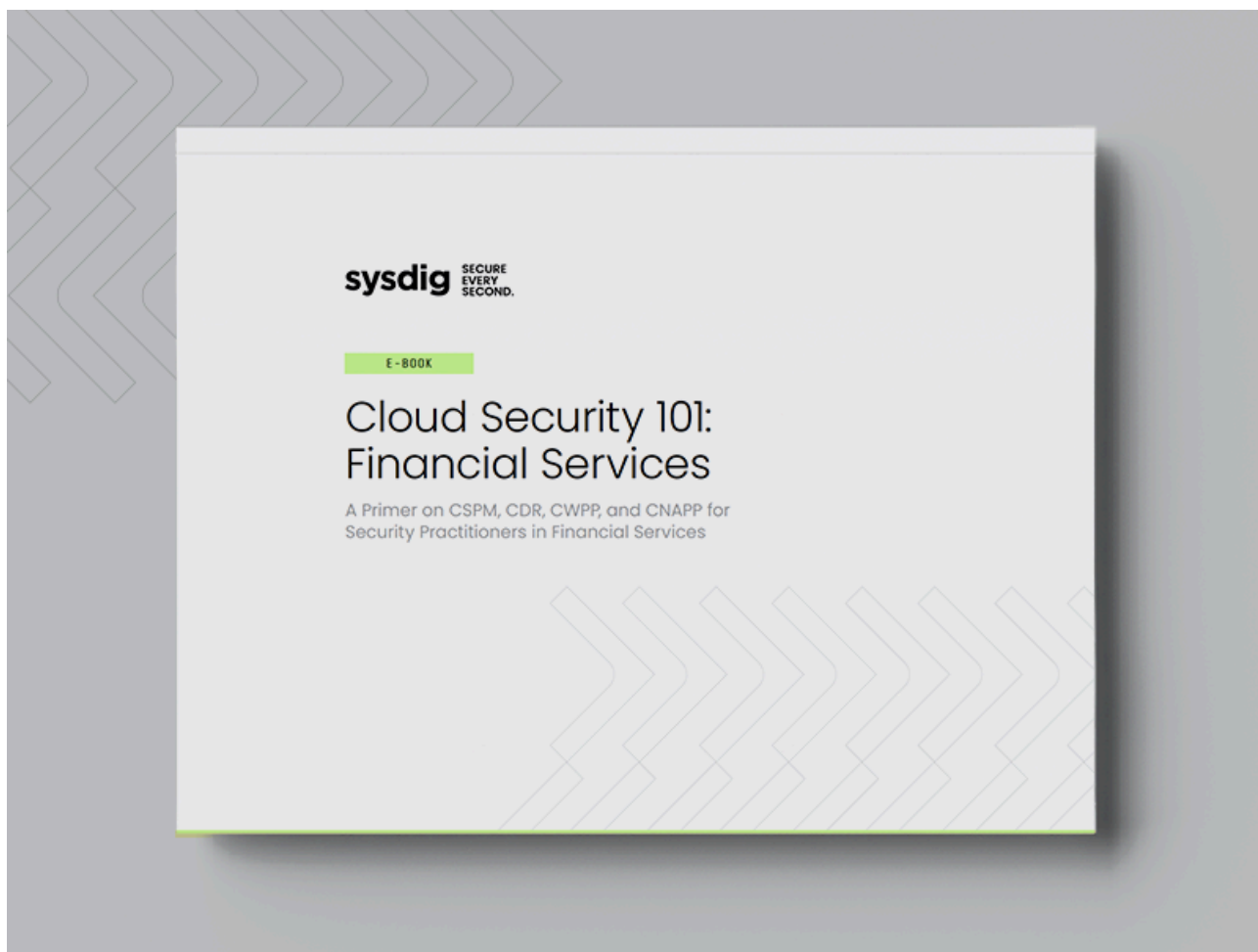
[CASE STUDY. Quby: Monitor + Secure Java Apps on Mesos Marathonpdf](#)

[Sysdig SecureSysdig Monitor](#)



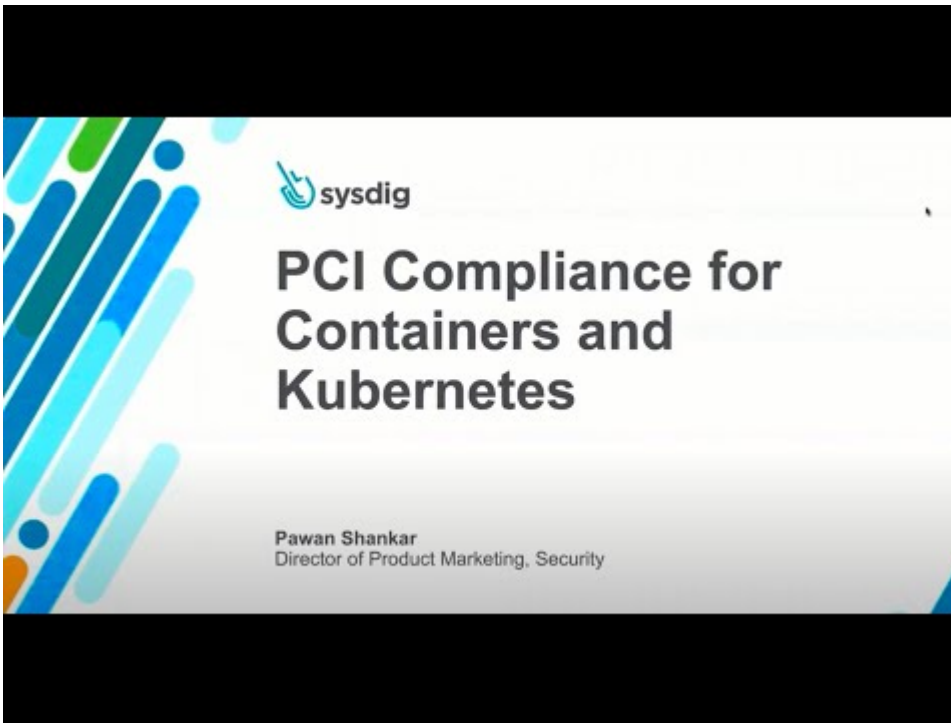
[EBOOK. The Fast Track to Stronger Cloud Security in Financial Servicespdf](#)

[Cloud Security](#)



[GUIDE. Cloud Security 101 for Financial Servicespdf](#)

[Cloud Security](#)



[WEBINAR. PCI Compliance in Containers & Kubernetesvideo](#)

[Cloud Security](#)



[VIDEO. Detecting threats to Kubernetes, containers, and Google Cloudvideo](#)

[Cloud Security](#)



[BRIEF. 6 Tips to Help Strengthen Financial Services Security in the Cloudpdf](#)

[Cloud SecurityCloud MonitoringCloud computing security](#)

CUSTOMER STORY

# Bloomreach Reduces Monitoring Costs by 40% and Achieves 350% ROI with Sysdig

Without visibility and observability, maintaining a reliable cloud platform is functionally impossible.

Bloomreach understands this firsthand. An industry leader in the personalization of the e-commerce experience, they aim to streamline the entire customer journey from top of funnel to post-purchase. From an intuitive dashboard, Bloomreach's customers can seamlessly manage omnichannel marketing, product discovery, and content creation, all while enabling deeper, more effective personalization.



**INDUSTRY**

Software Technology

**COMPANY DETAILS**

Established in 2008, Bloomreach is a leader in the personalization of the e-commerce experience. The company is focused on delivering relevant, contextualized, and consistent digital experiences for search and merchandising. Looking for a "green women's shirt," they are the reason you see only relevant suggestions. Having won multiple awards from both clients and analysts, their roots are grounded in search data and artificial intelligence. They support the entire customer journey, from top of funnel to post-sale.

**CHALLENGES**

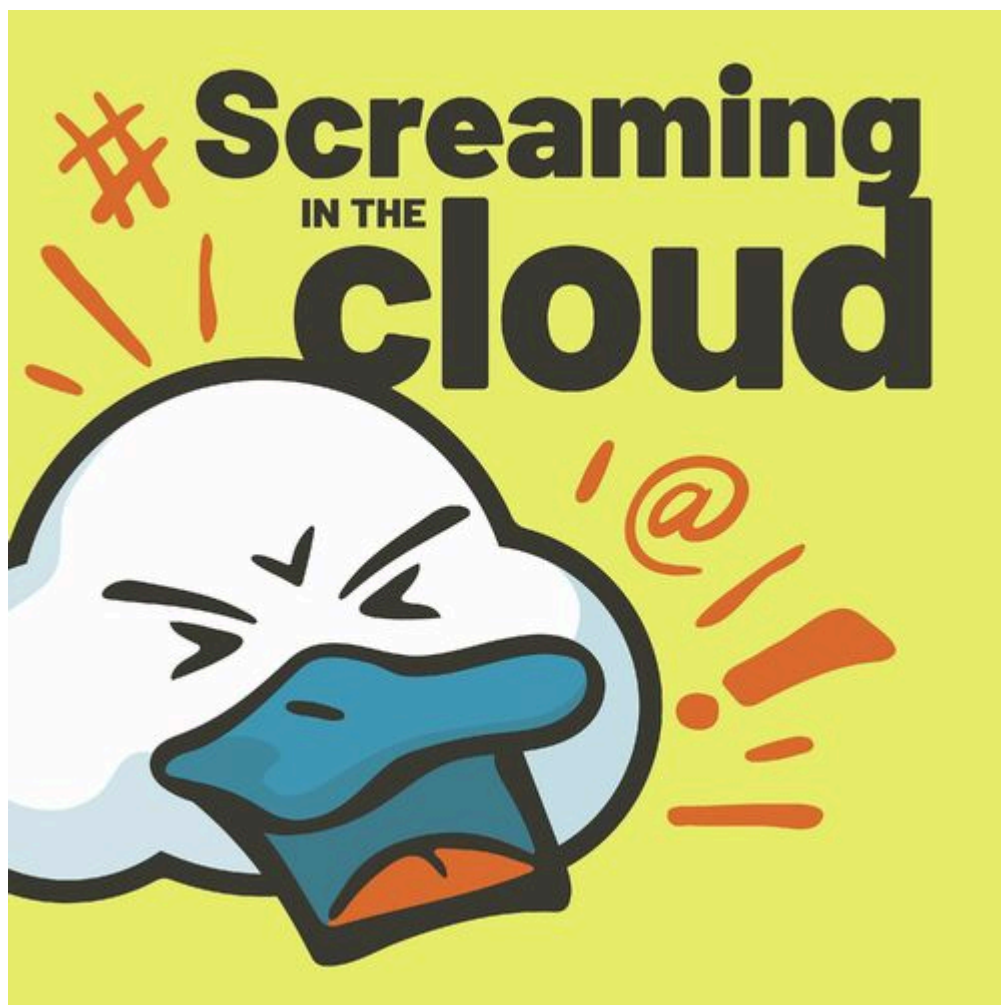
- Unsustainable infrastructure costs
- Monitoring stack is extremely time-consuming for the SRE team to manage
- Information overload and alert fatigue
- Lack of visibility into Kubernetes clusters

**OUTCOMES**

- 40% reduction in infrastructure monitoring costs
- 350% return on investment (ROI) with an optimized operating environment that saves time, money, and manpower
- Reduction in false positives and alert fatigue
- 2,000+ hours saved by increased engineering productivity

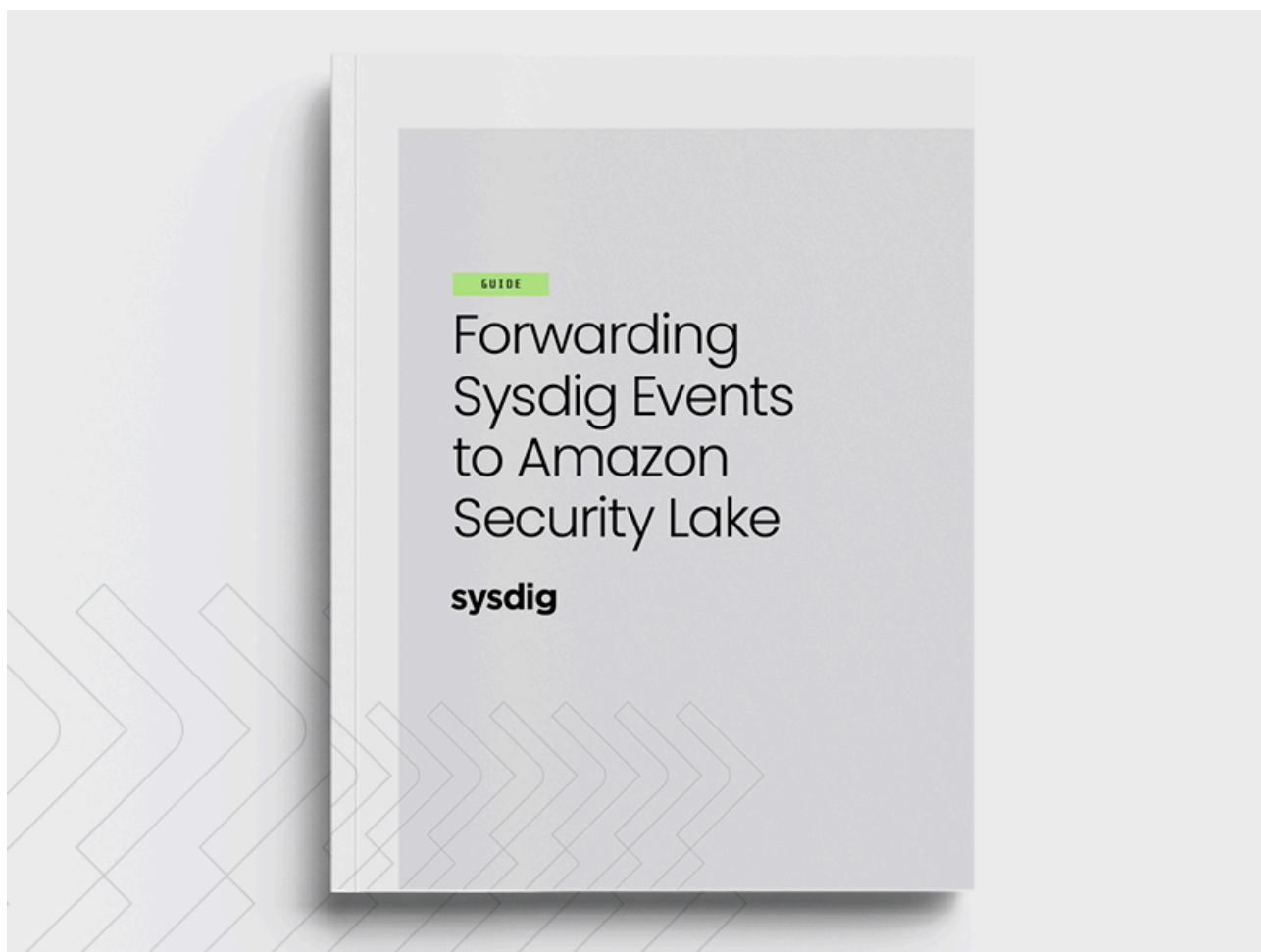
[CASE STUDY. Bloomreachpdf](#)

[AWS](#)



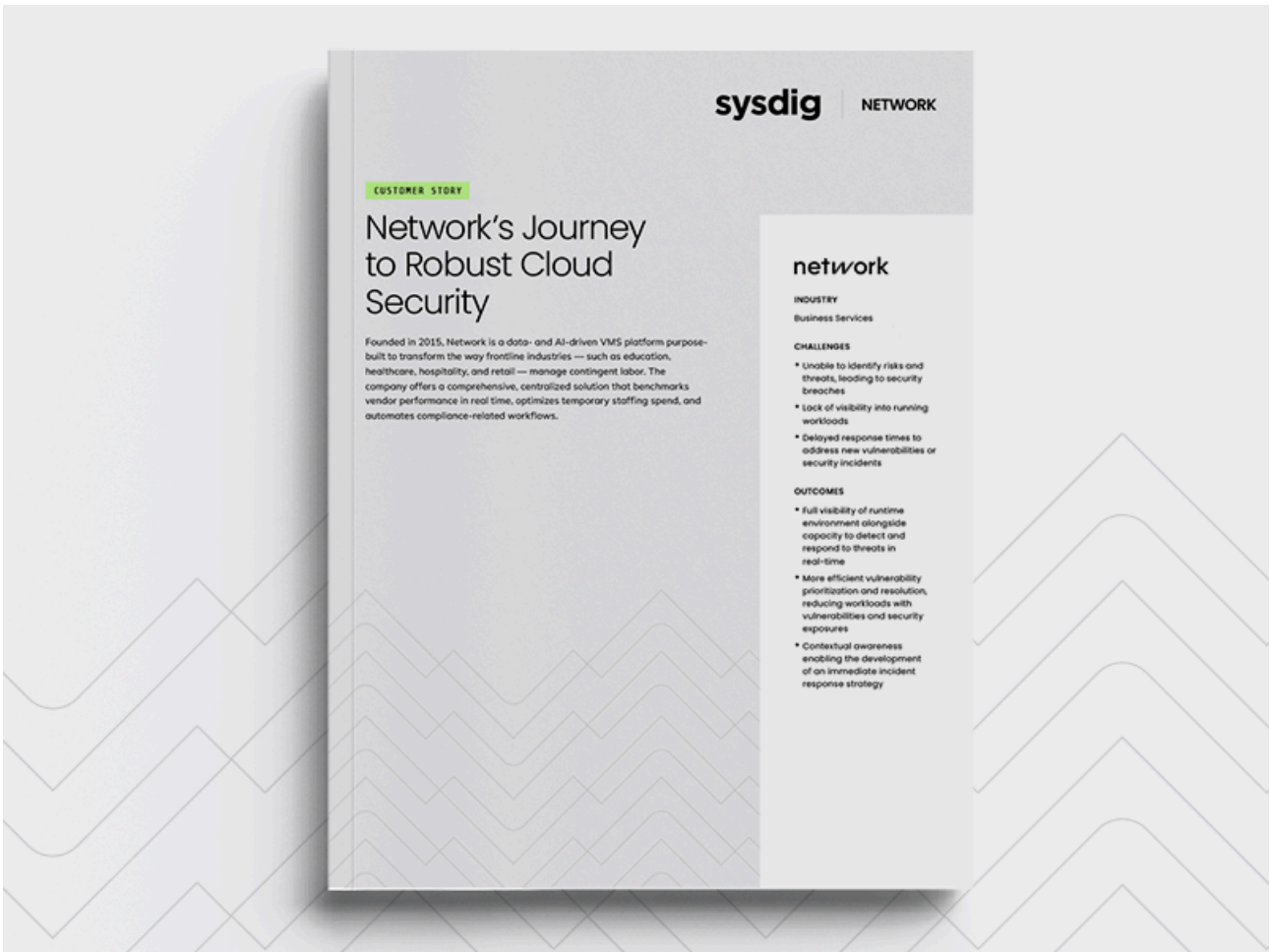
[PODCAST. Screaming in the Cloud: Exposing The Latest Cloud Threats](#) webpage

[Cloud Security](#)



[GUIDE. Forwarding Sysdig Events to Amazon Security Lakepdf](#)

[Cloud Security](#)



[Network Case Study.pdf](#)

[Sysdig Secure](#)



## Get Started with Secure DevOps



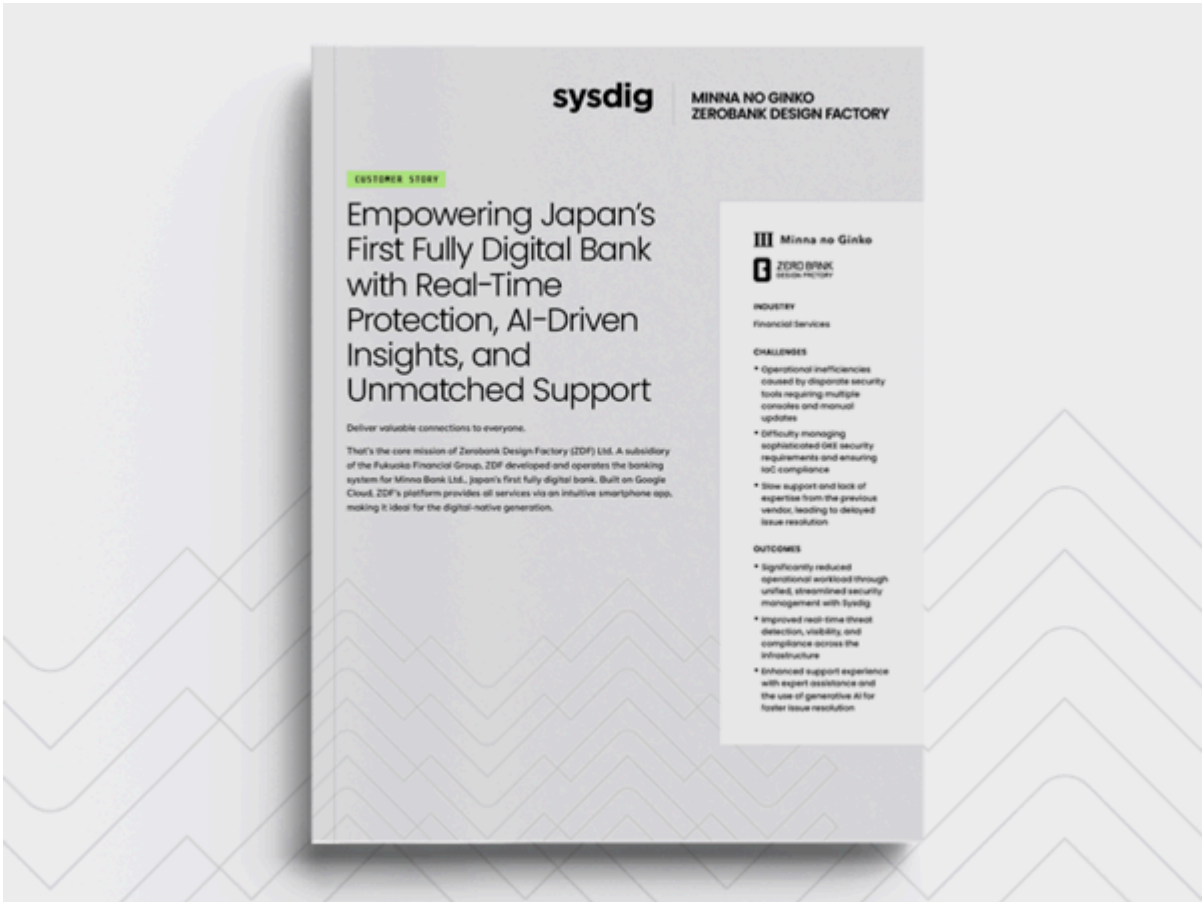
[WEBINAR: Deploy Faster by Automating Container Security, Monitoring and Compliance](#)[video](#)

[Cloud Security](#)[Cloud Monitoring](#)



[VIDEO. Sysdig product demonstration](#)[video](#)

[Sysdig Secure](#)[Sysdig Monitor](#)



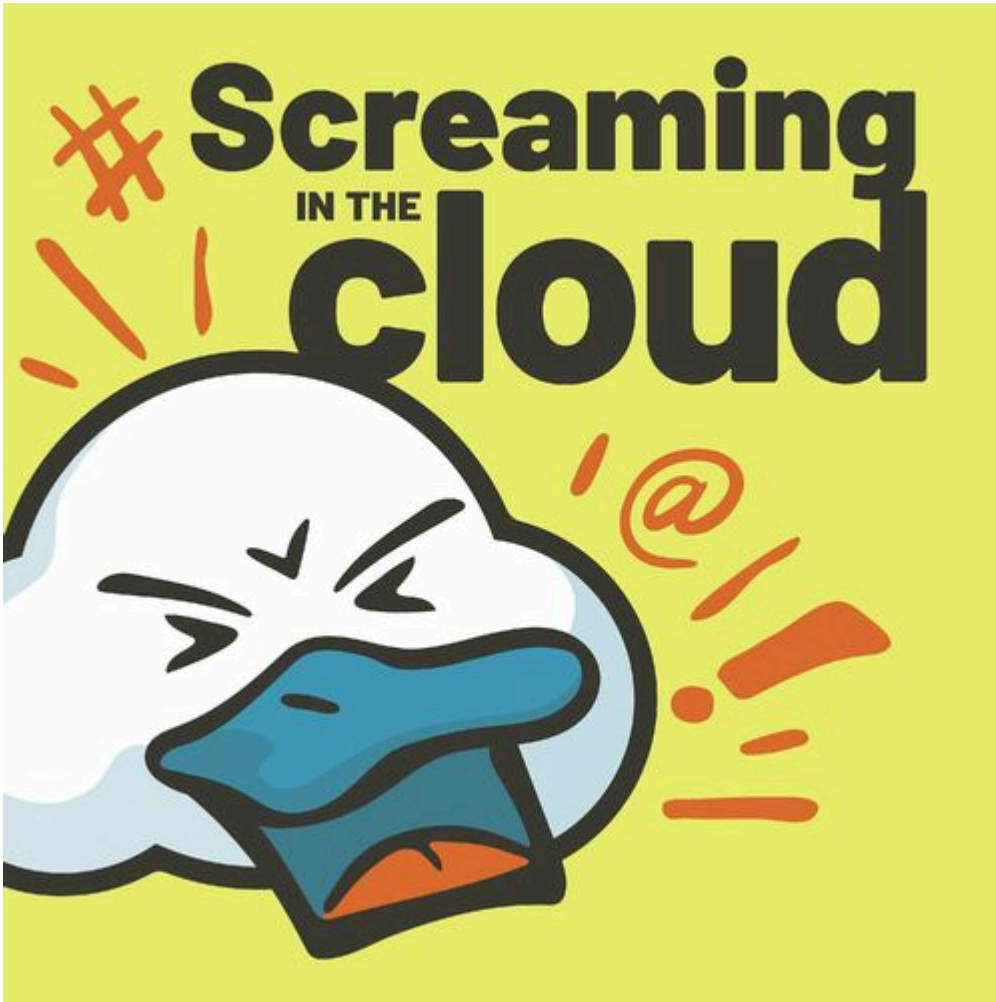
[CASE STUDY. Zerobank Case Study.pdf](#)

[Sysdig Secure](#)



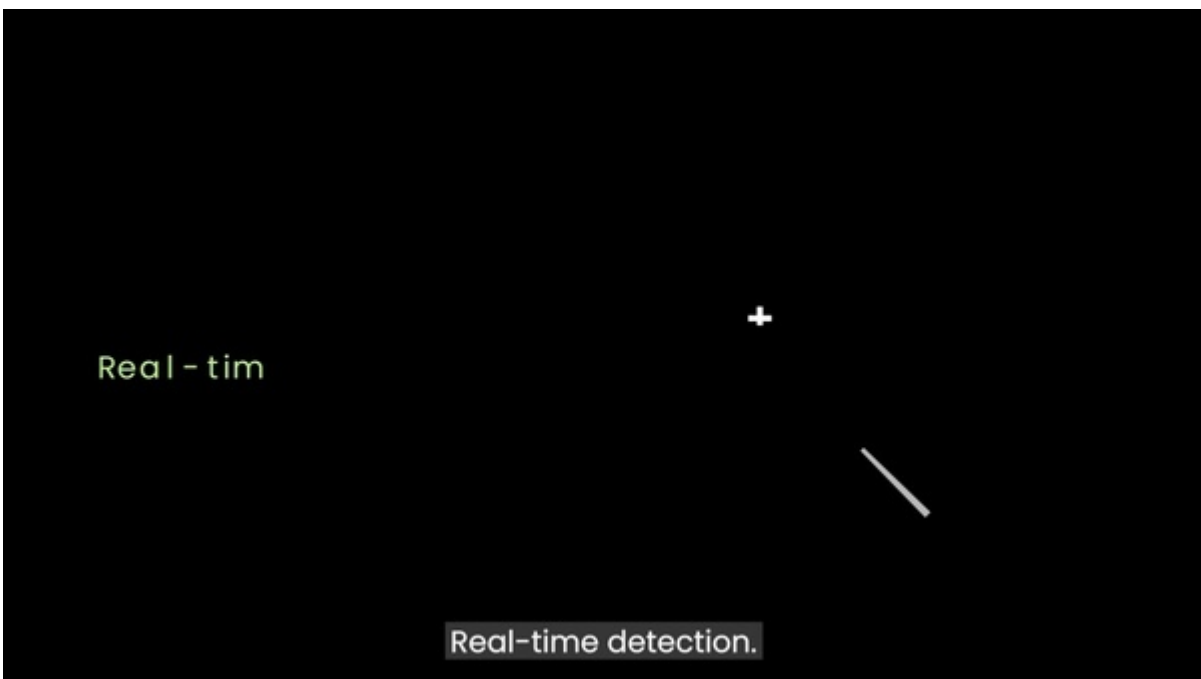
[SERVICE BRIEF: Guided CSE Servicepdf](#)

[Sysdig SecureSysdig Monitor](#)



[PODCAST. Screaming in the Cloud - Cloud-Native Threatswebpage](#)

[Cloud Security](#)



[VIDEO. Real-time cloud security for financial servicesvideo](#)

[Cloud Security](#)



[PODCAST. Screaming in the Cloud: An Open-Source Mindset in Cloud Security with Alex Lawrencewebpage](#)

[Cloud SecurityFalcoOpen Source](#)



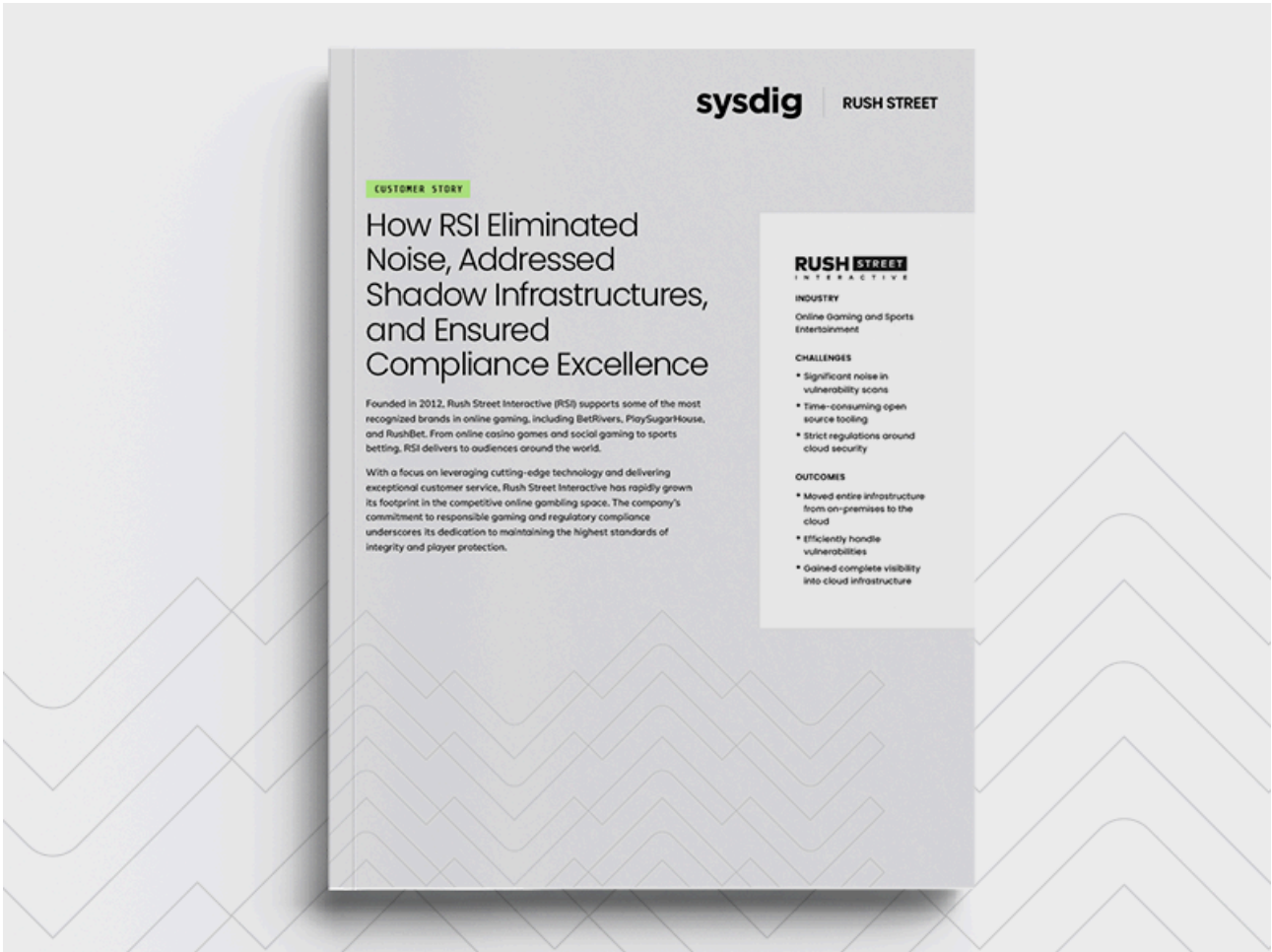
# NIST 800-190 Application Security Guide

---



[GUIDE. NIST 800-190 Application Security Guide Checklistpdf](#)

[Sysdig Secure](#)



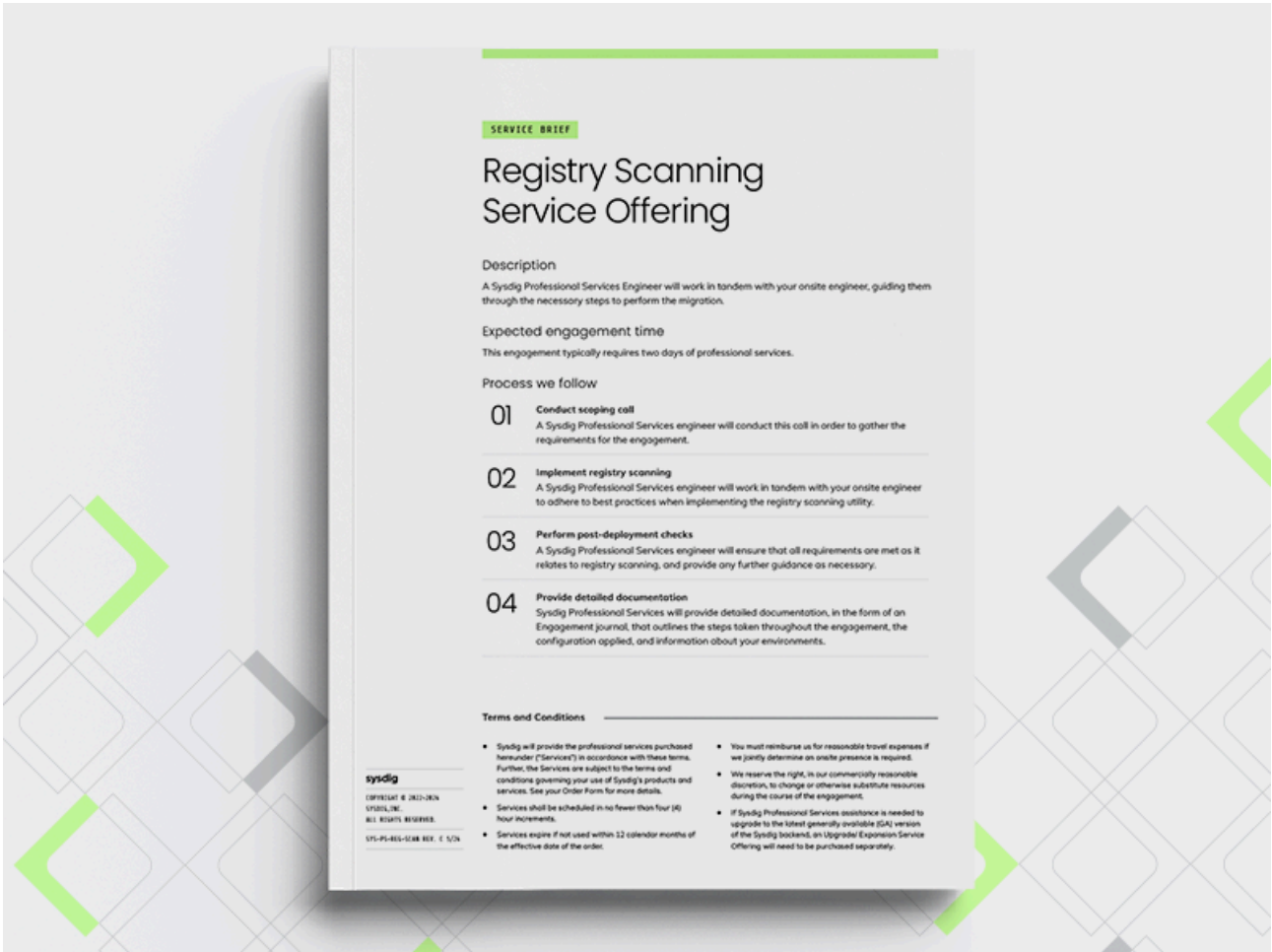
[CASE STUDY. How RSI Eliminated Noise, Addressed Shadow Infrastructures, and Ensured Compliance Excellencepdf](#)

[Cloud Security](#)



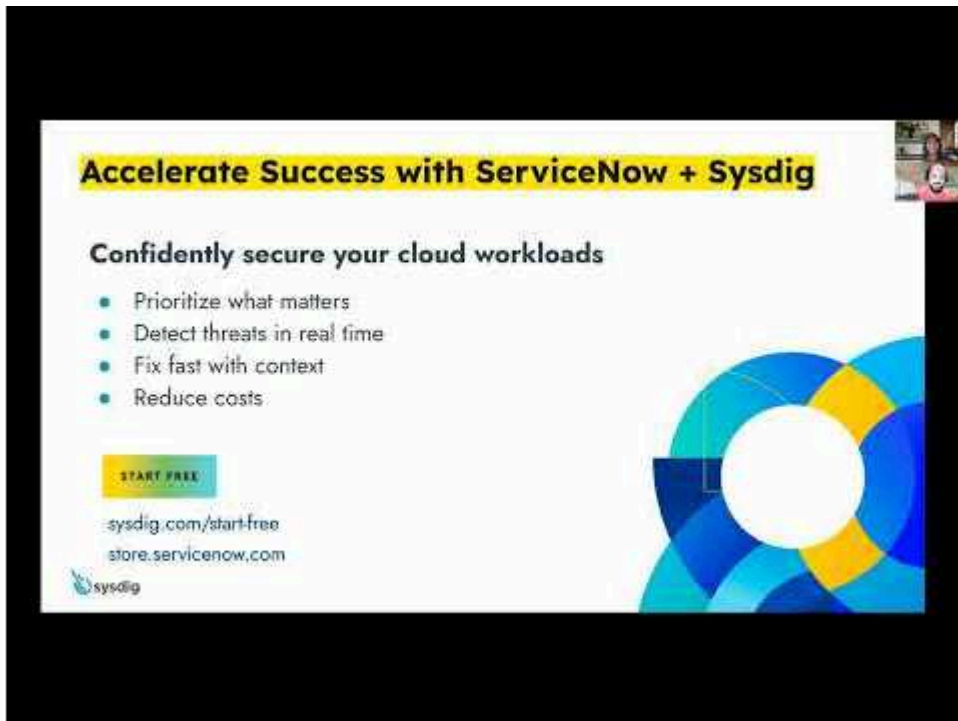
[BRIEF. 5 Best Practices to Securing Cloud and Containerspdf](#)

[Sysdig SecureKubernetes](#)



[SERVICE BRIEF. Registry Scanningpdf](#)

[Sysdig SecureSysdig Monitor](#)



[VIDEO. Accelerate Success with ServiceNow + Sysdigvideo](#)

[Sysdig SecureSysdig Monitor](#)



[WEBINAR. AWS Observability 101: Kubernetes and Prometheus Monitoring with Sysdigvideo](#)

[AWS Cloud Monitoring Prometheus Sysdig Monitor](#)



[SERVICE BRIEF. Sysdig JumpStartpdf](#)

[Sysdig Secure](#)



[BRIEF. 2025 Cloud-Native Security and Usage Reportpdf](#)

[Cloud Security](#)



[CASE STUDY. Loglasspdf](#)

[Sysdig Secure](#)



[INFOGRAPHIC. Unlock The Power Of Nis2pdf](#)

[Cloud Security](#)



[SERVICE BRIEF: Managed CSE Servicepdf](#)

[Sysdig SecureSysdig Monitor](#)

**Introduction**

Principal Analyst Information Security

Originally from 🇧🇷, now based in Toronto 🇨🇦

**Topic areas:** endpoint security, cloud infrastructure security, container/cloud-native security, deception

**Prior experience:** 20+ years across pre-sales and delivery roles in enterprise security.

**Interests:** cloud-native security, security economics

🐦 @fsmontenegro

451 RESEARCH.COM  
©2019 451 Research. All Rights Reserved.

[WEBINAR. 451 Research Webinar: Scaling Cloud-Native to Meet Ops & Security Demands](#)video

[Sysdig Secure](#)[Sysdig Monitor](#)

sysdig

**WHITE PAPER**

**The Business Value of GenAI for Cloud Security**

Accelerate human response with Sysdig Sage™

Cloudwork is no longer a luxury, it's a necessity. As organizations continue to expand their cloud footprint, the complexity of their security posture grows. Sysdig Sage™, powered by GenAI, accelerates human response to security alerts, reducing the time to identify and remediate threats. Sysdig Sage™ is the only security solution that can help you accelerate human response to security alerts, reducing the time to identify and remediate threats.

As cloudwork grows, organizations need a way to help ing solutions increase the effectiveness of security operations. In time, all security operations have pushed back against automation, but now it's time to accelerate human response and understand the value of cloud-native solutions.

Sysdig Sage™, powered by GenAI, provides a security alerting system that can automatically detect the root cause of an alert, and automatically all security alerts to make it easier to investigate and respond to security alerts, reducing the time to identify and remediate threats.

[The Business Value of GenAI for Cloud Security](#)pdf

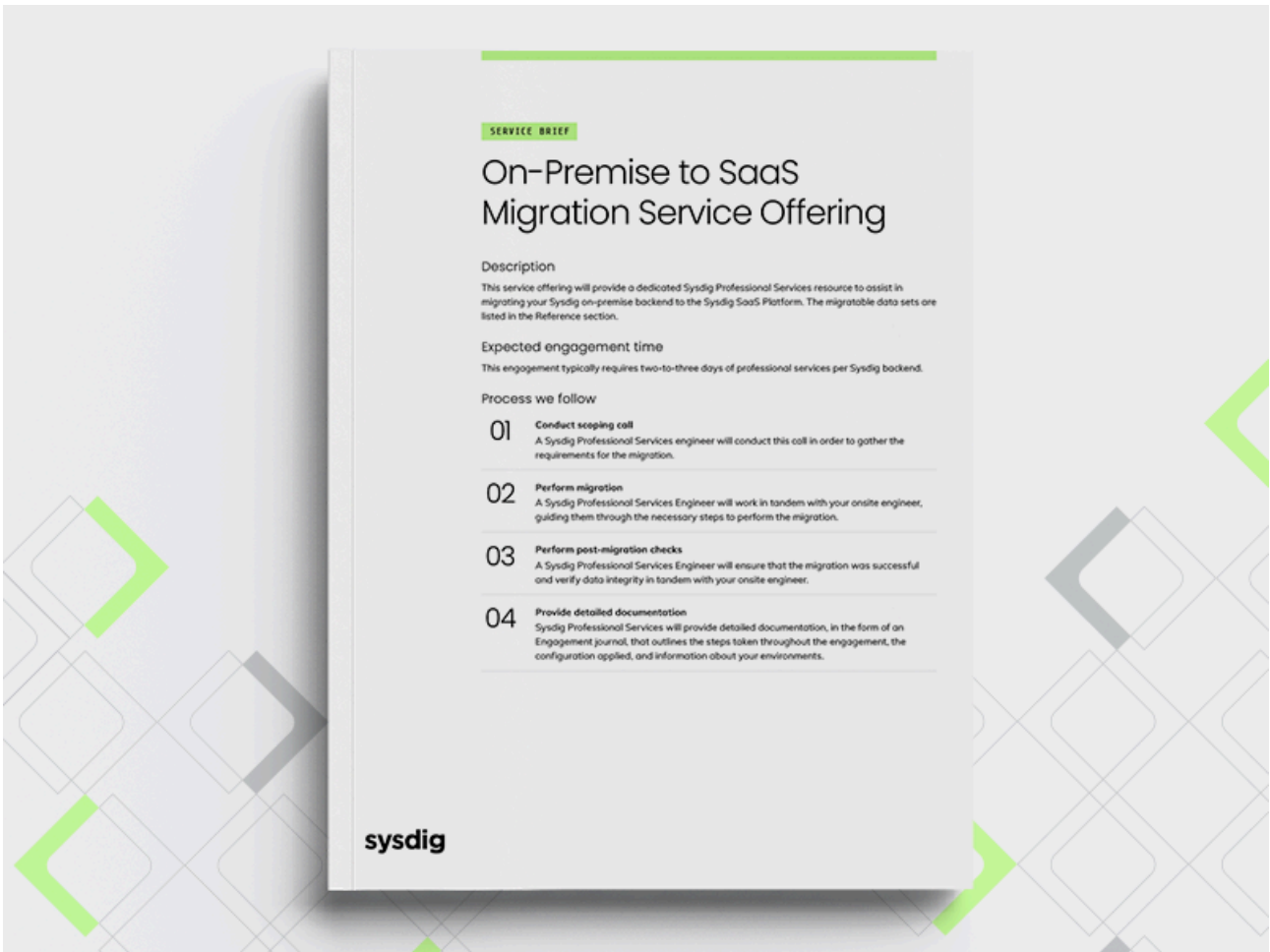
[Cloud Security](#)

# **Sysdig Secure Architecture Guide**



[BRIEF. Sysdig Secure Architecture Guidepdf](#)

[Sysdig Secure](#)




[SERVICE BRIEF. On-Premise To SaaS](#)

[Sysdig SecureSysdig Monitor](#)



[WEBINAR, DevNation Federal: DevSecOps What To Focus On Firstvideo](#)

[Red Hat](#)



# BRIEF

## Secure DevOps for Microsoft Azure

Unified visibility and security to confidently run containers, Kubernetes, and cloud services on Microsoft Azure

### Why Sysdig

- Deep visibility across containers and cloud
- Radically simple to run and scale
- Built on an open-source security stack

Microsoft Partner

Get it from Microsoft Azure Marketplace

### How It Works

Azure services, Data sources, Context

“ Sysdig reduced our operational burden by 50 percent.”  
- DevSecOps Cloud Security Architect at FIS

### Key Use Cases

- Container/K8s Security**
  - Image Scanning
  - Kubernetes Security
  - Runtime Security
  - Compliance
  - Network Security
  - Incident Response
  - Forensics
- Cloud Security**
  - Infrastructure as Code security
  - Cloud Security Posture Management (CSPM)
  - Cloud workload protection
- Monitoring**
  - Container Monitoring
  - Kubernetes Monitoring
  - Prometheus Monitoring
  - Custom Metrics
  - Cloud Monitoring
  - Troubleshooting

Highlighted Customers

Goldman Sachs, worldpay from FIS, logdna, Alaska AIRLINES

Copyright © 2021 Sysdig, Inc. All rights reserved. PB-006 Rev. E 12/21

[Learn More](#) [sysdig.com/partners/microsoft-azure](https://sysdig.com/partners/microsoft-azure)

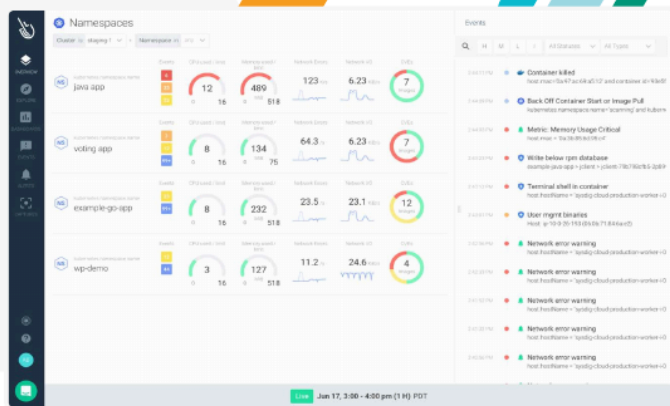
[SOLUTION BRIEF. Sysdig Platform for Microsoft Azure and AKSwebpage](#)

[Azure](#)



# Secure DevOps for Rancher

We partner with Rancher to help enterprises confidently run cloud-native workloads on Kubernetes and containers, in production, across private, hybrid and multi-cloud environments. By automating security, compliance and monitoring for a secure DevOps workflow, developers, service owners and platform teams maximize performance, ensure continuous security and ship cloud applications faster.



## Sysdig Benefits for Rancher Kubernetes-as-a-Service



### Manage Security Risk

- Identify and block vulnerabilities across your CI/CD pipeline.
- Detect and block threats at runtime with Falco-driven policies and Kubernetes native controls.
- Conduct incident response and forensics, even after containers are gone.



### Maximize Performance and Availability

- Scale Prometheus monitoring to millions of metrics with long-term retention.
- Monitor health and performance to prevent issues across private, hybrid and multi-cloud environments.
- Troubleshoot inside clusters, pods and containers.

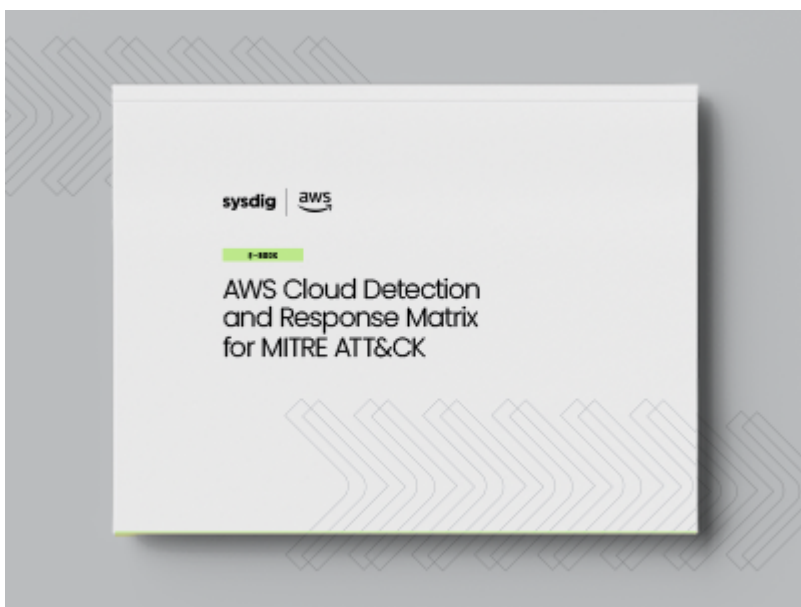


### Validate Cloud Compliance

- Validate compliance using PCI, NIST, and CIS insights.
- Audit clusters, nodes and containers for continuous compliance with detailed activity reports.
- Implement File Integrity Monitoring across the container lifecycle.

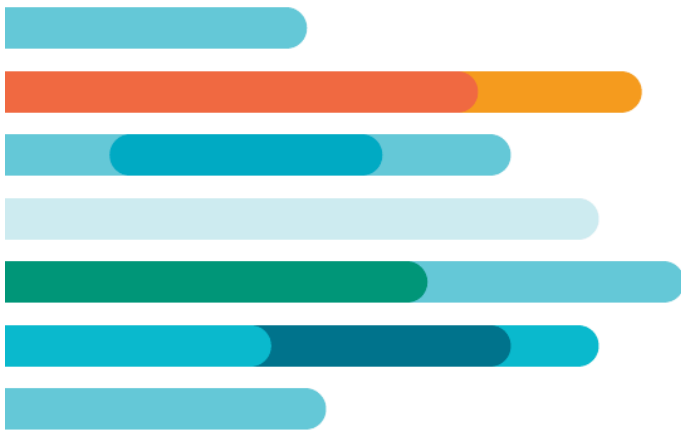
[PARTNER BRIEF. Rancherpdf](#)

[Sysdig Secure Sysdig Monitor](#)



[GUIDE. AWS Cloud Detection and Response Matrix for MITRE ATT&CKpdf](#)

[Cloud Security](#)



# 30-60-90 Day Checklist for a DevOps Engineer



[GUIDE. 30 60 90 Day Checklistpdf](#)

[Cloud SecurityCloud Monitoring](#)

**sysdig** | CUSTOMER STORY **HEALTHCARE IT PROVIDER**

## 99.8% Fewer Alerts, 98% Less Vulnerability Noise: A Security Evolution in Healthcare Tech

**98%** reduction in vulnerability noise | **~125** hours saved per audit | **99.8%** reduction in daily alert volume

### Summary

Tasked with securing sensitive healthcare data across dynamic, cloud-native environments, a leading healthcare IT provider faced mounting challenges: overwhelming alert noise, audit fatigue, and limited runtime visibility. With a small team and no formal security operations center (SOC), they turned to Sysdig to reduce complexity and risk. By embedding real-time detection, continuous compliance, and intelligent automation into daily workflows, they replaced noise with context and manual effort with efficiency. Security friction gave way to developer-friendly collaboration, enabling the team to strengthen their posture without adding staff.

**Healthcare IT Provider**

**HEADQUARTERS**  
United States

**INDUSTRY**  
Healthcare IT / Software Technology

**Key results**

- Accelerated compliance cycles and faster audit readiness
- Deeper collaboration between development and security teams
- Improved threat detection and response with AI-driven insights

[Healthcare It Sysdig Customer Storypdf](#)

[Sysdig SecureSysdig Monitor](#)

**sysdig** INC.

**WHITE PAPER**

## NIS2 Action Plan for the Cloud CISO

[WHITEPAPER. NIS2 Action Plan for the Cloud CISOpdf](#)

[Cloud Security](#)



[SERVICE BRIEF. Runtime Scanningpdf](#)

[Sysdig SecureSysdig\\_Monitor](#)



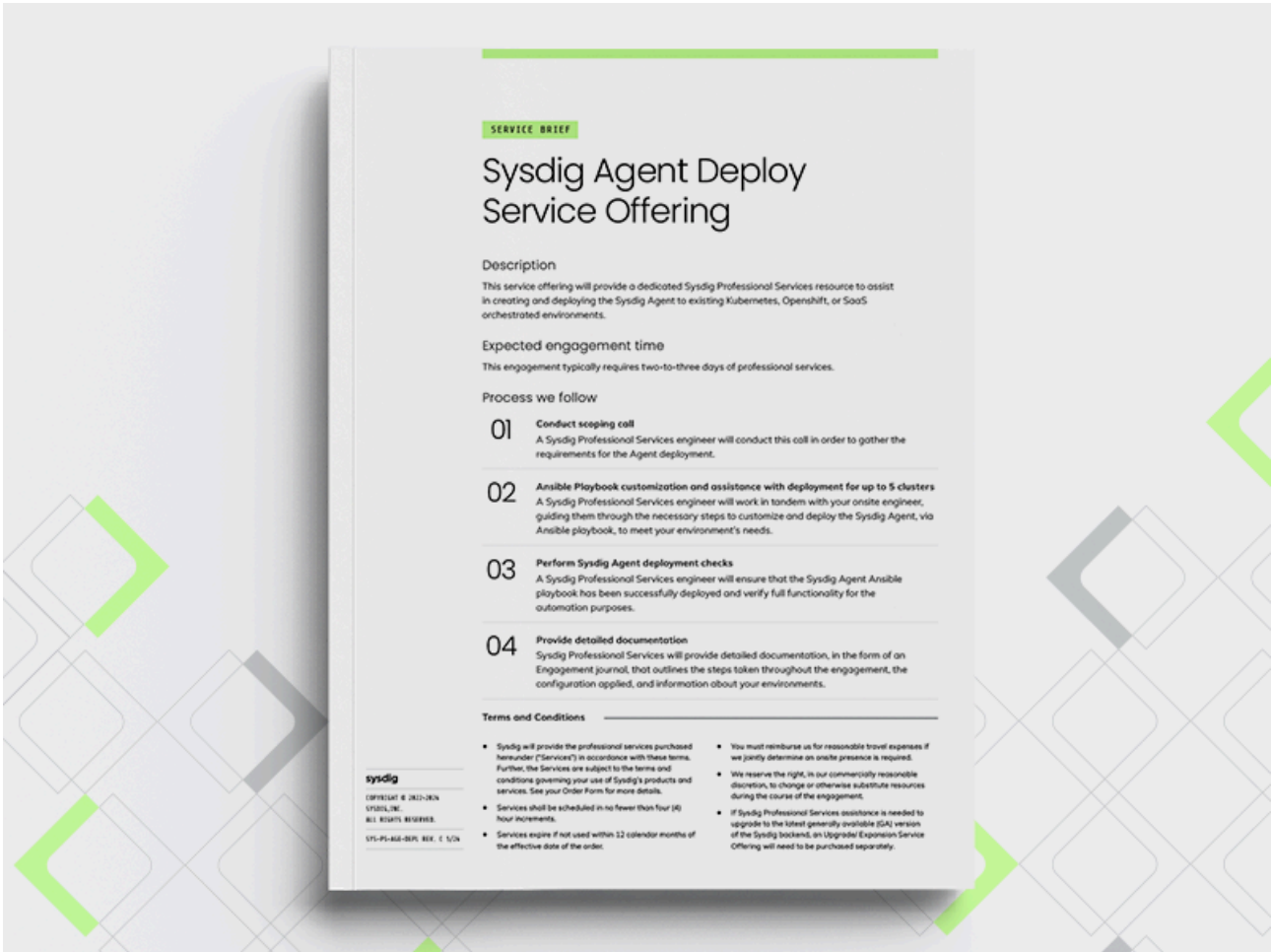
[WHITEPAPER. Your Cloud Security Strategy is Backwardpdf](#)

[Cloud Security](#)



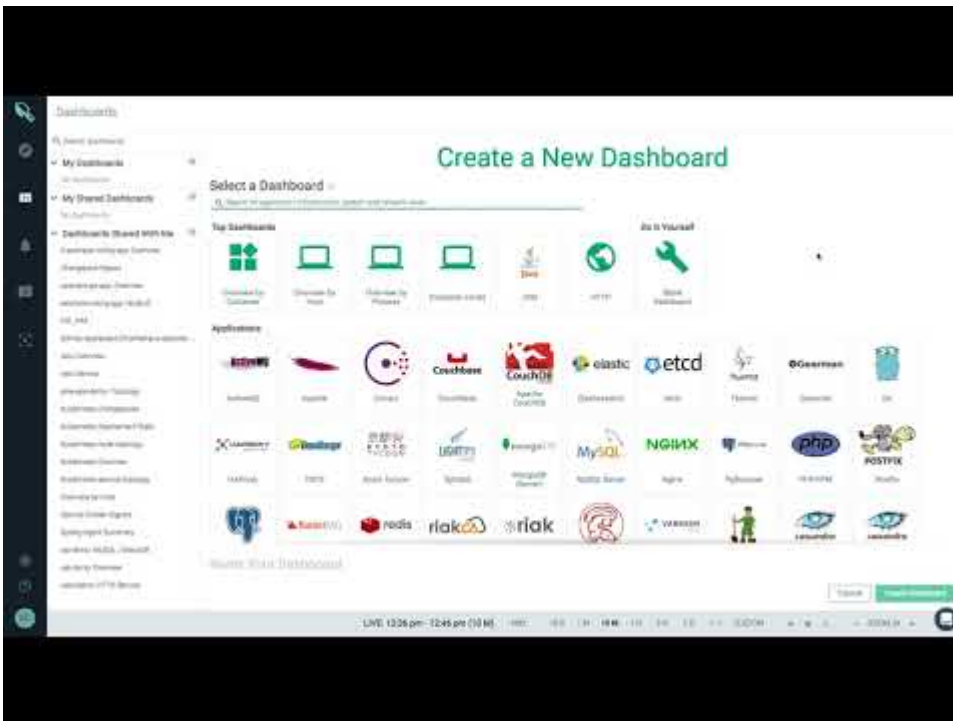
[BRIEF. 2025 Usage Report Executive Takeawayspdf](#)

[Cloud Security](#)



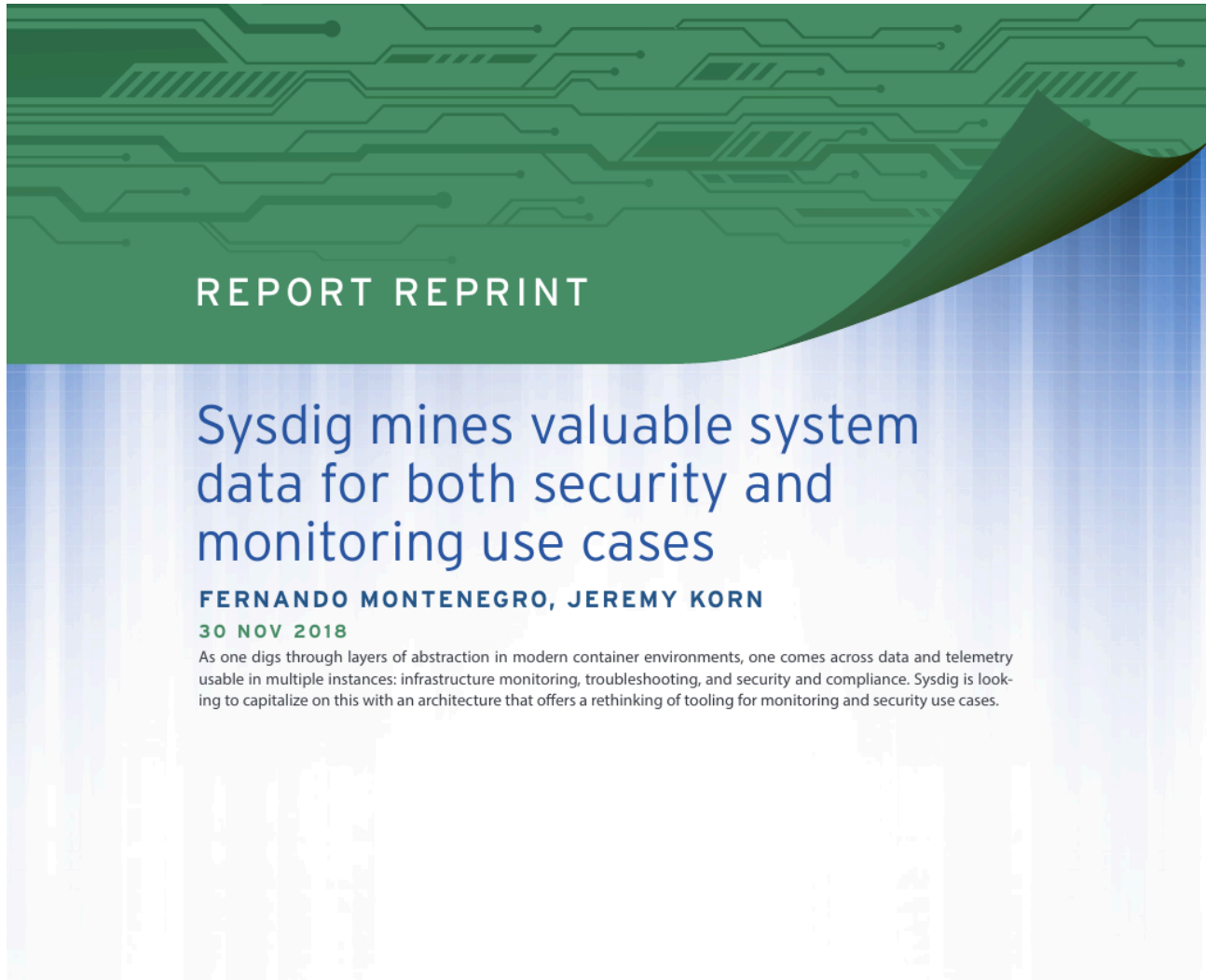
[SERVICE BRIEF. Agent Deploypdf](#)

[Sysdig SecureSysdig\\_Monitor](#)



[VIDEO. Sysdig Monitor - Cloud-native intelligencevideo](#)

[DockerKubernetesSysdig Monitor](#)



## REPORT REPRINT

# Sysdig mines valuable system data for both security and monitoring use cases

**FERNANDO MONTENEGRO, JEREMY KORN**

**30 NOV 2018**

As one digs through layers of abstraction in modern container environments, one comes across data and telemetry usable in multiple instances: infrastructure monitoring, troubleshooting, and security and compliance. Sysdig is looking to capitalize on this with an architecture that offers a rethinking of tooling for monitoring and security use cases.

THIS REPORT, LICENSED TO SYSDIG, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, WAS PUBLISHED AS PART OF OUR SYNDICATED MARKET INSIGHT SUBSCRIPTION SERVICE. IT SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR RE-POSTED, IN WHOLE OR IN PART, BY THE RECIPIENT WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.



©2019 451 Research, LLC | [WWW.451RESEARCH.COM](http://WWW.451RESEARCH.COM)



[REPORT. Sysdig Security And Monitoringpdf](#)



[INFOGRAPHIC. Promql Cheatsheetpdf](#)

[Cloud MonitoringKubernetesPrometheusSysdig Monitor](#)

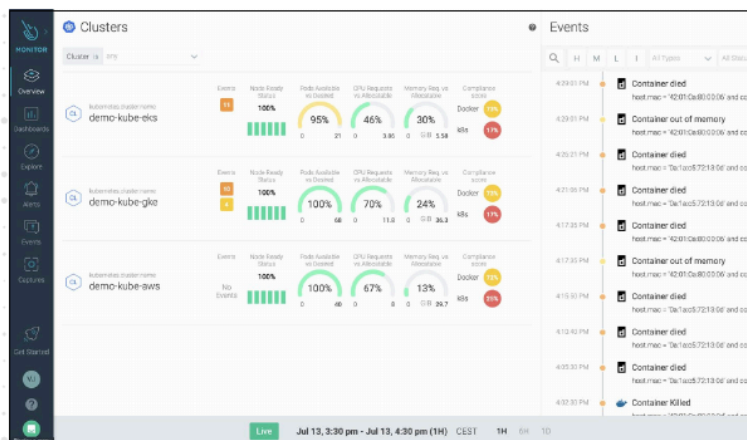


# Kubernetes Monitoring Checklist



Kubernetes has taken the container ecosystem by storm. It acts as the brain for your distributed container deployment and is designed to manage service-oriented applications using containers distributed across clusters of hosts. Kubernetes provides mechanisms for application deployment, service discovery, scheduling, updating, maintenance, and scaling.

You are adopting a DevOps approach, using Kubernetes and containers to accelerate innovation. While this dramatically simplifies deploying applications in containers — and across clouds — it also adds a new set of complexities for managing, securing and troubleshooting applications. Kubernetes and container monitoring is critical to managing application performance, service uptime and troubleshooting.



[GUIDE. Kubernetes Monitoring Checklistpdf](#)



# Security Operations Provider Reduces Vulnerabilities by 95%

## Company Details

Recognized as a leader for managed detection and response (MDR) services, this software-as-a-service (SaaS) company helps customers detect, investigate, hunt, and respond to threats, as well as remediate its clients' digital environments. In short, it does the heavy security lifting so its customers don't have to.

## Industry

Technology

## Sysdig Solution

Sysdig Secure

## Infrastructure

Google Cloud Platform (GCP)

## Orchestration

Google Kubernetes Engine (GKE)

Software  
Technology  
Company

The concept of balancing people, processes, and technology in a security program isn't secret, but finding a mix that is cost-effective and security-effective is elusive for many organizations. It's helped this security operations provider prioritize vulnerabilities and manage compliance so its team can focus on revenue-producing work.

"We see it as our job to help our clients better utilize the security technology that they've already purchased by integrating it with our technology through APIs," said the Director of Information Security. "We deploy the platform into a secure instance within our cloud infrastructure, built using Google Cloud, and provide 24-7 support to our clients."





[VIDEO. How to Get Started with Sysdig Monitorvideo](#)

[Sysdig Monitor](#)



[BRIEF. Data security findingspdf](#)

The graphic is a corporate brief for Sysdig, featuring a green header with the Sysdig logo and tagline. Below the header, there is a section on the left with three key value propositions: Agent AI, Open Innovation, and Runtime Insights. To the right of these is a list of solutions and a grid of logos for integrations, environments, and customers. The background of the graphic has a grey and white geometric pattern.

## sysdig

### Cloud security, the right way.

No guesswork. No black boxes.  
Just cloud defense done right.

Founded by the creators of open source standards — Falco, Stratosphere, and Wazuh — and built on agentic AI, Sysdig delivers real-time cloud defense grounded in the uncompromising truth of runtime.

#### Security and development teams can tailor defenses together — the right way.

**Agent AI**  
Brings clarity and precision to the moments that matter most.

**Open Innovation**  
Creates transparency, customizability, and shared trust across a global community.

**Runtime Insights**  
Reveal what's real, what's risky, what's important right now, and why it matters.

#### SOLUTIONS

- AI workload security
- Cloud detection and response
- Cloud infrastructure entitlement management
- Cloud-native application protection platform
- Cloud security posture management
- Cloud workload protection platform
- Container & Kubernetes security
- Data security findings
- Vulnerability management

#### INTEGRATIONS

Logos for AWS, Azure, GCP, IBM, Oracle, and others.

#### ENVIRONMENTS

Logos for AWS, Azure, GCP, IBM, Oracle, and others.

#### CUSTOMERS

Logos for various companies including IBM, Oracle, and others.

[BRIEF. Sysdig Corporate Brief: Indiapdf](#)



[SOLUTION BRIEF. Securing Containers And Kubernetespdf](#)

[Kubernetes](#)



# Prometheus Monitoring Guide



[GUIDE. Prometheus Monitoringpdf](#)

[KubernetesPrometheusSysdig Monitor](#)

# Kubernetes Monitoring Guide



[GUIDE. Kubernetes Monitoring Guidepdf](#)

[Cloud MonitoringKubernetesSysdig Monitor](#)



# Leading Game Developer Saves Millions While Scaling 10X

**Industry**  
Software Technology

**Sysdig Solution**  
Sysdig Monitor

**Infrastructure**  
Google Cloud Platform (GCP)

**Orchestration**  
Google Kubernetes Engine (GKE)

Game Development Company

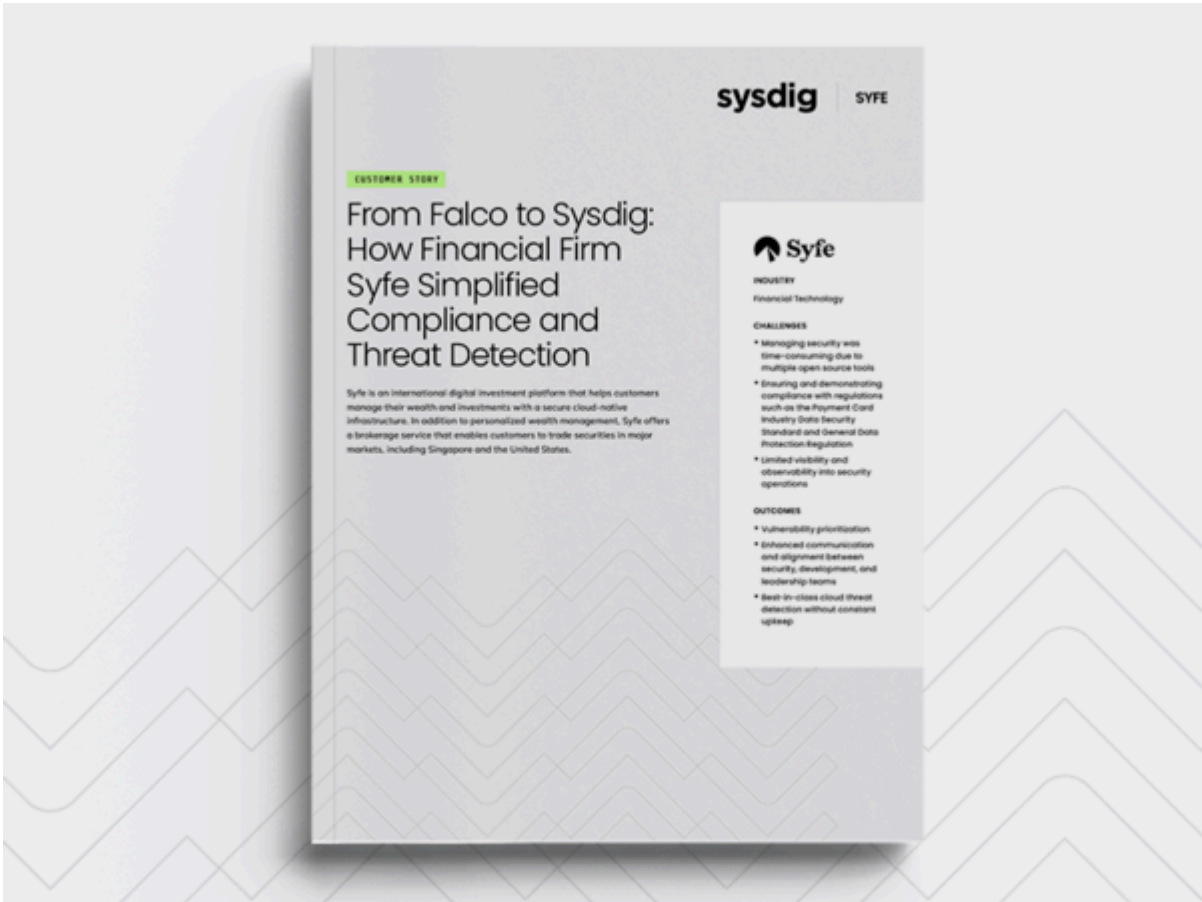
Downloaded billions of times per month, the games built using this technology company's platform are used by gamers worldwide on everything from mobile phones and consoles to desktop computers. A critical revenue stream for the company comes from an auction platform that delivers advertisements to these gamers. Hosted on one of the big three cloud providers, the auction platform allows advertisers to bid on each ad impression.



sysdig | Case Study: Game Development Company

[CASE STUDY. Game Developer Companypdf](#)

[Cloud MonitoringKubernetesSysdig Monitor](#)



[CASE STUDY. From Falco to Sysdig: How Financial Firm Syfe Simplified Compliance and Threat Detectionpdf](#)

**sysdig** | CUSTOMER STORY **BitMEX**

## BitMEX Has Never Lost a Coin

How BitMEX uses runtime visibility to make rapid security decisions

**50%** reduction in mean time to triage

**30 seconds** to begin investigation

**40% to 50%** less time spent investigating inactive vulnerabilities

### Summary

Leading cryptocurrency exchange BitMEX operates in an environment where security failures are irreversible. Under constant attack from highly sophisticated adversaries, even a single compromised custodial private key can result in permanent financial loss, with no recourse or recovery.

To protect the exchange, BitMEX relies on a lean, globally distributed security team. That team needs to understand what is happening across its cloud environment and make decisions quickly, often with incomplete information. Sysdig provides real-time runtime visibility across containers and workloads, changing how the team investigates risk and responds under pressure.

#### Key Results

- Clear visibility into what is actually running across cloud workloads, allowing the security team to assess real exposure instead of theoretical risk.
- Faster investigations with the context needed to determine when issues require immediate action and when they can safely be deprioritized.
- Security teams can focus on high-impact threats and critical systems without slowing development or day-to-day operations.
- Proactive support from Sysdig reduces operational overhead, allowing a leaner security team to scale without adding complexity.

**BitMEX**  
High-performance cryptocurrency derivatives exchange.

**HEADQUARTERS**  
Republic of Seychelles

**REGISTERED**  
Financial Services

[CASE STUDY. BitMEX Has Never Lost a Coinpdf](#)



[CHECKLIST. Agentic AI For Cloud Security Checklistpdf](#)



[Exploring Advanced Cybersecurity with Michael Isbitski – Sysdigwebpage](#)

[cybersecurity](#)

**SECURE EVERY SECOND.**  
Cloud security powered by runtime insights.

For businesses innovating in the cloud, every second counts. Development teams must shorten time to market, while security teams must protect the business without slowing it down.

However, operating in the cloud is different — from the infrastructure to the organizational dependencies to the very anatomy of modern applications. Attackers exploit the complexity and automation of the cloud to move laterally, elevate privileges, and maximize blast radiuses.

To outpace attackers, security teams need to detect, triage, and respond to threats in real time. Disparate point solutions are insufficient and create silos. Operating in the cloud requires a different approach to security — one that tells the whole story of what is happening across interconnected environments.

At Sysdig, we've built a unique cloud security platform that combines *runtime insights*, *real-time detection*, and *AI to secure innovation at cloud speed*. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

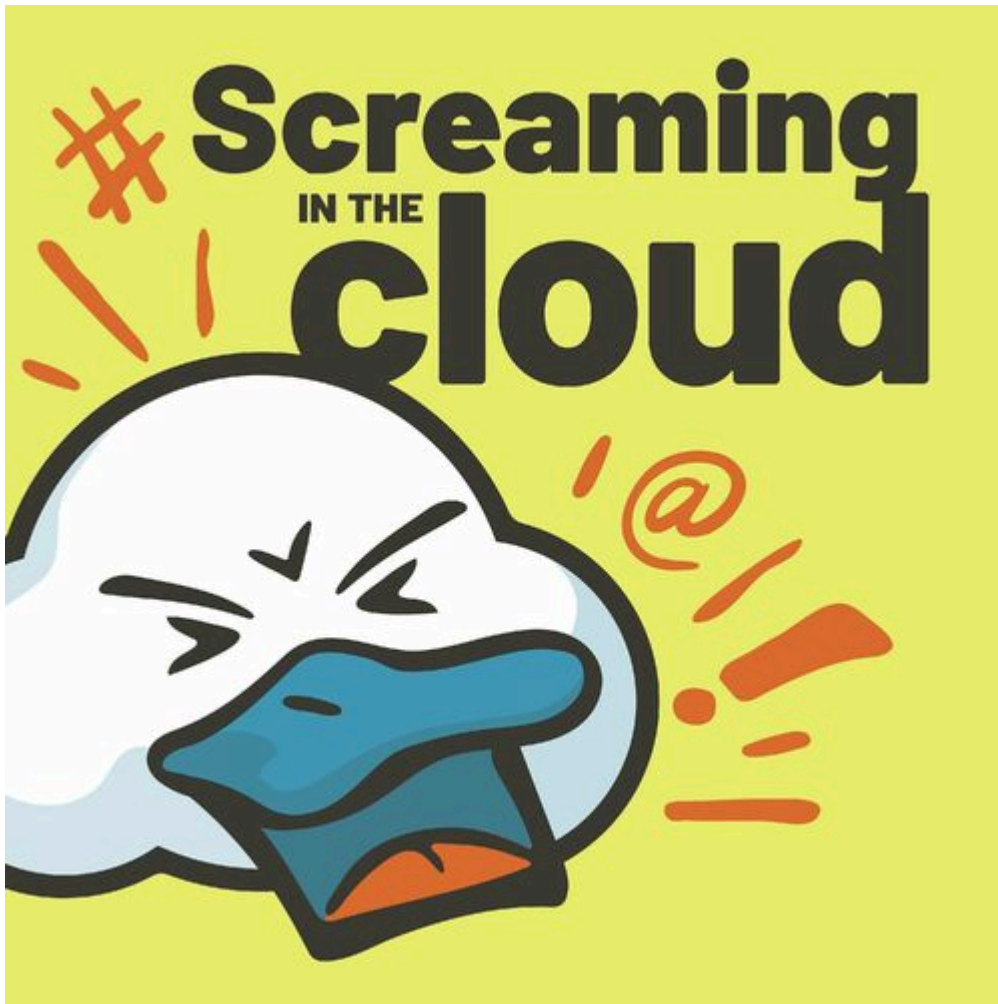
**10 MINUTES is all it takes to execute a cloud attack.**

**Why Sysdig**

- Get Complete Visibility**  
Eliminate visibility gaps created by disparate solutions. Sysdig provides a unified view of risk across your entire cloud estate and the context needed to take action.
- Eliminate 95% of the Noise**  
Identifying your top risks shouldn't require scouring through a mountain of alerts. Sysdig leverages the knowledge of what's in use to prioritize what you need to focus on.
- Detect Threats Within Two Seconds**  
Sysdig accelerates threat detection and response in real time with end-to-end coverage and correlation across workloads, identities, cloud services, and third-party applications.

**sysdig**  
www.sysdig.com

[BRIEF. Sysdig Company Overviewpdf](#)



[PODCAST. Benchmarking Security Attack Response Times in the Age of Automation](#) webpage



# Best Practices for Reducing the Cost of Custom Metrics

When it comes to Kubernetes and cloud monitoring, users must be sure that not only the cloud infrastructure is under control, but that their own applications and other third-party applications exposing metrics themselves are properly observed. Here is when custom metrics come into play.

Talking about Kubernetes and cloud monitoring, custom metrics are a key factor for a huge number of companies. Custom metrics refer to data points that are specific to a particular business or application, and are not typically captured by standard monitoring tools. These metrics provide valuable insight into the performance and usage of a specific application or service, and can help identify areas for improvement or optimization. They must rely on solid observability systems to watch performance, avoid potential availability issues, and measure their own

business KPIs. That's why custom metrics are normalized and widely adopted across almost every organization. But, what about the associated costs of maintaining and storing all these custom time series metrics? As you'd probably guess, this can cause huge overspending.

When talking about metrics costs, metrics cardinality is important. But, what does cardinality mean? The definition of cardinality is "The number of elements in a given mathematical set." Metrics can have multiple labels, at the same time labels can have many different values. The more values for a label, and the more labels in a metric, the more cardinality. In a metrics context, we can say cardinality is the number of combinations of labels and its values for a metric. If you add a new key/value pair to your metric, you will be exponentially increasing cardinality. The more cardinality, the more unique metrics. That means more storage and more infrastructure is needed to support and process data ingestion, storage, and metrics exploration. In summary, this means increased costs.

In this best practices guide, you'll find some tips that will help you with reducing the cost of custom metrics monitoring.

[BRIEF: Best Practices for Reducing the Cost of Custom Metricspdf](#)

[Cloud MonitoringCost OptimizationSysdig Monitor](#)



[VIDEO. Containers in Production: Goldman Sachs video](#)

[Kubernetes](#)

The graphic is a white rectangular card with a dark grey background. At the top left is the 'sysdig' logo. To the right is a decorative pattern of overlapping, light green and grey chevron shapes. Below the logo, the word 'CHECKLIST' is written in a small green box. The main title is 'Secure Your Cloud in Minutes' in a large, bold, black font. Below the title is the subtitle 'Your Checklist for Meeting the 555 Benchmark'. The body of the graphic contains three paragraphs of text: a short introductory paragraph, a paragraph explaining the 555 Benchmark (5 seconds to detect, 5 minutes to correlate, 5 minutes to respond), and a final paragraph stating that the guide helps with speed and efficiency.

**sysdig**

**CHECKLIST**

## Secure Your Cloud in Minutes

### Your Checklist for Meeting the 555 Benchmark

As cloud environments grow, the speed and sophistication of attacks in the cloud have grown just as much. So how can security teams keep up?

Sysdig's 555 Benchmark for Cloud Detection and Response offers a standard to use when measuring how fast your security teams can counter attackers. Specifically, the benchmark finds that to outpace attacks, your security teams need to detect threats within 5 seconds, correlate and triage data within the first 5 minutes, and initiate a tactical response within the next 5 minutes.

This may sound daunting, but it can be done. We've created this guide to help guide your security strategy so you can operate with the speed and efficiency you need. Paired with our 555 Benchmark guides, this resource lays out the steps to tackling modern cybercriminals and improving your threat detection and response readiness in the cloud.

[GUIDE. Secure Your Cloud in Minutespdf](#)

[Cloud computing security](#)



[VIDEO. Running Cloud-Native Workloads In Production with Sysdigvideo](#)

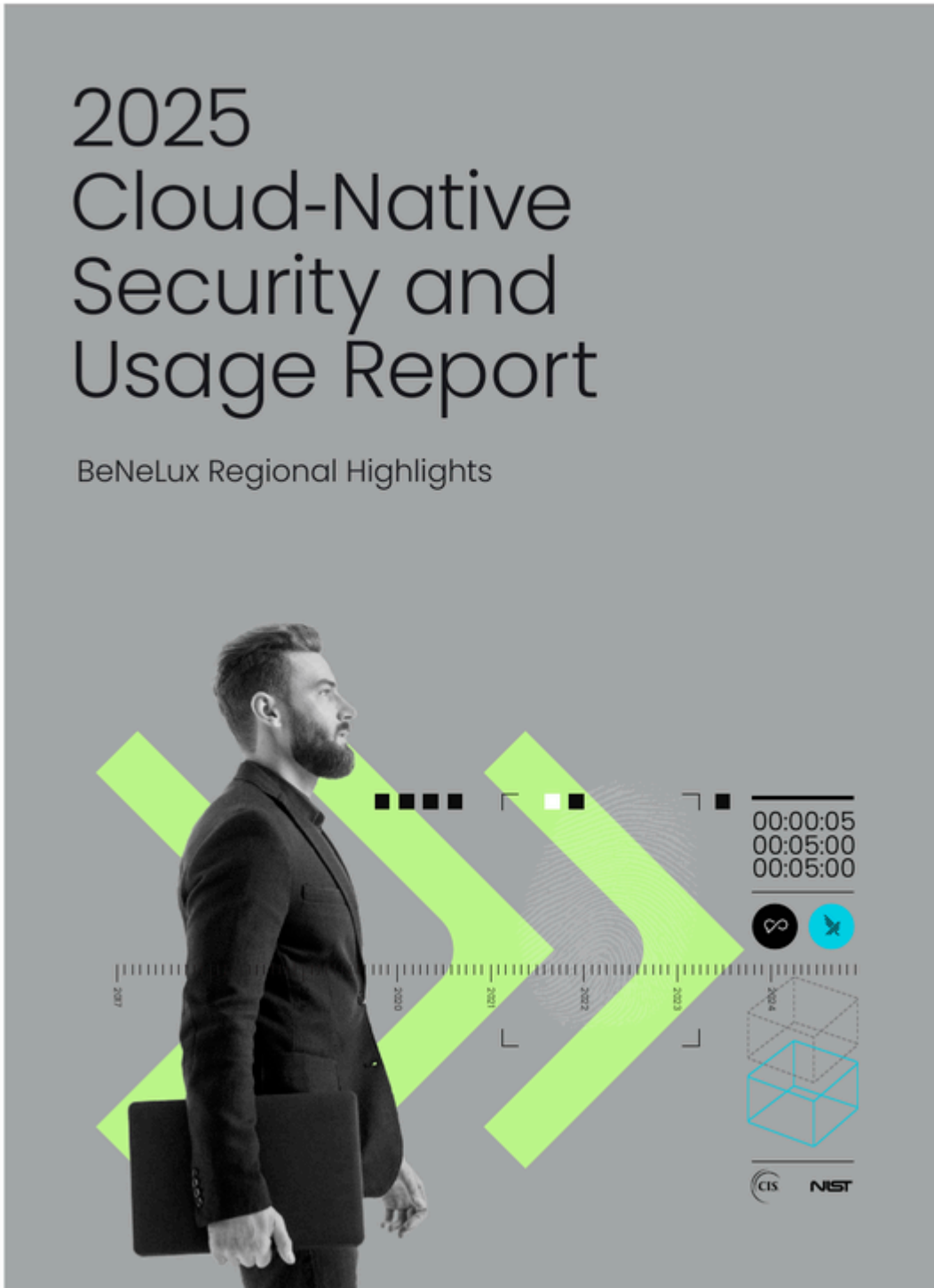


[VIDEO. KubeCon Keynote: Charting a Path to Take Kubernetes to 100,000 Enterprises - Wendy Carteevideo](#)



# 2025 Cloud-Native Security and Usage Report

BeNeLux Regional Highlights



[REPORT. BeNeLux 2025 Cloud Native Security Usage Report - TrueFullstaqpdf](#)



# Six Keys for Scaling Prometheus



Containers are ephemeral and difficult to troubleshoot. They require comprehensive, granular and context-rich data to anticipate and prevent issues that can impact user experience. In order to effectively manage the cloud native applications, DevOps teams require a toolset designed specifically to analyze, predict and prevent issues in containers, Kubernetes services, and Cloud-native infrastructure.

Prometheus has become the de-facto standard for DevOps / SRE teams to monitor Kubernetes workloads. It offers a number of advantages - it's easy to set up, implement and maintain on a single server. Prometheus is also well suited for highly dynamic Kubernetes-based environments.

As the scope of Kubernetes development and production deployment increases in enterprises, DevOps / SRE teams quickly find the need to scale Prometheus-based monitoring capability. Several open source tools are available for scaling Prometheus.

Figure 1: Do-It-Yourself Scaled Prometheus Technology Reference Architecture



A technology reference architecture is outlined above for reference. Here are the six keys for scaling Prometheus:

[WHITEPAPER. Six Keys for Scaling Prometheuspdf](#)

[PrometheusSysdig Monitor](#)



# Kubernetes and Cloud Monitoring for Financial Services

## Modern Cloud Applications Need Modern Monitoring

Organizations are using Kubernetes, Prometheus, and DevOps workflows to build modern cloud-native applications. However, the dynamic nature of these complex environments can lead to gaps in visibility and difficulty in resolving issues when they arise. Meeting user expectations for availability, performance, and cost requires complete visibility into infrastructure, services, and applications across hybrid and multicloud environments. Traditional tools were not built for containers and Kubernetes and can't deliver the granular data and troubleshooting context to rapidly address issues. SREs and developers need easy-to-use monitoring solutions that integrate into DevOps workflows without breaking open source standards.

## Sysdig Monitor Radically Simplifies Cloud and Kubernetes Monitoring

With deep visibility into cloud-native workloads, [Sysdig Monitor](#) helps organizations troubleshoot faster and lower costs. You get immediate, granular details and troubleshooting tools for rapidly changing container environments.

"Installing Sysdig is quick and easy. You don't have to implement a GUI or open firewalls, which with that type of implementation is costly. Getting Sysdig SaaS up and running basically took 30 minutes until the first cluster provided metrics. Compared to other tools we used previously, it took us a month to get to the same point. Sysdig comes with great out-of-the-box dashboards and alerts which saves us loads of time."

**Natnael Teferi**, Lead DevSecOps Cloud Security Architect, Worldpay by FIS



"Sysdig's investment in Prometheus and other open source technologies has enabled us to adapt and pivot when we needed to."

**John Elm**, Software Engineer Lead, Experian Data Labs



"Our charter is to optimize and secure the services running in our environment. We need, for instance, to understand communication patterns and cluster usage, to identify bad behavior and security events, and to know if an application is under- or over-utilized. To achieve these goals, we not only need detailed telemetry, but we need application context. This is a hard problem to solve."

**Chetan Mehendiratta**, Vice President of Engineering, Goldman Sachs



### Kubernetes Monitoring and Troubleshooting

- Troubleshoot Kubernetes errors 10x faster
- Debug cluster, workload, pod, and control plane-level issues quickly
- See a prioritized list of issues with remediation steps, live logs, and YAML files

### Managed Service for Prometheus

- Leverage an enterprise-class managed Prometheus service to dramatically lower the maintenance burden
- Find insights faster with intuitive dashboards and automatic service discovery
- Reduce PromQL complexity using our simple form UI

### Optimizing Cloud-Native Application Costs

- Standardize on a multicloud monitoring solution
- Lower the cost of custom metrics and cut Kubernetes costs by an average of 40%
- Monitor serverless, self-managed, and managed cloud services with a single tool

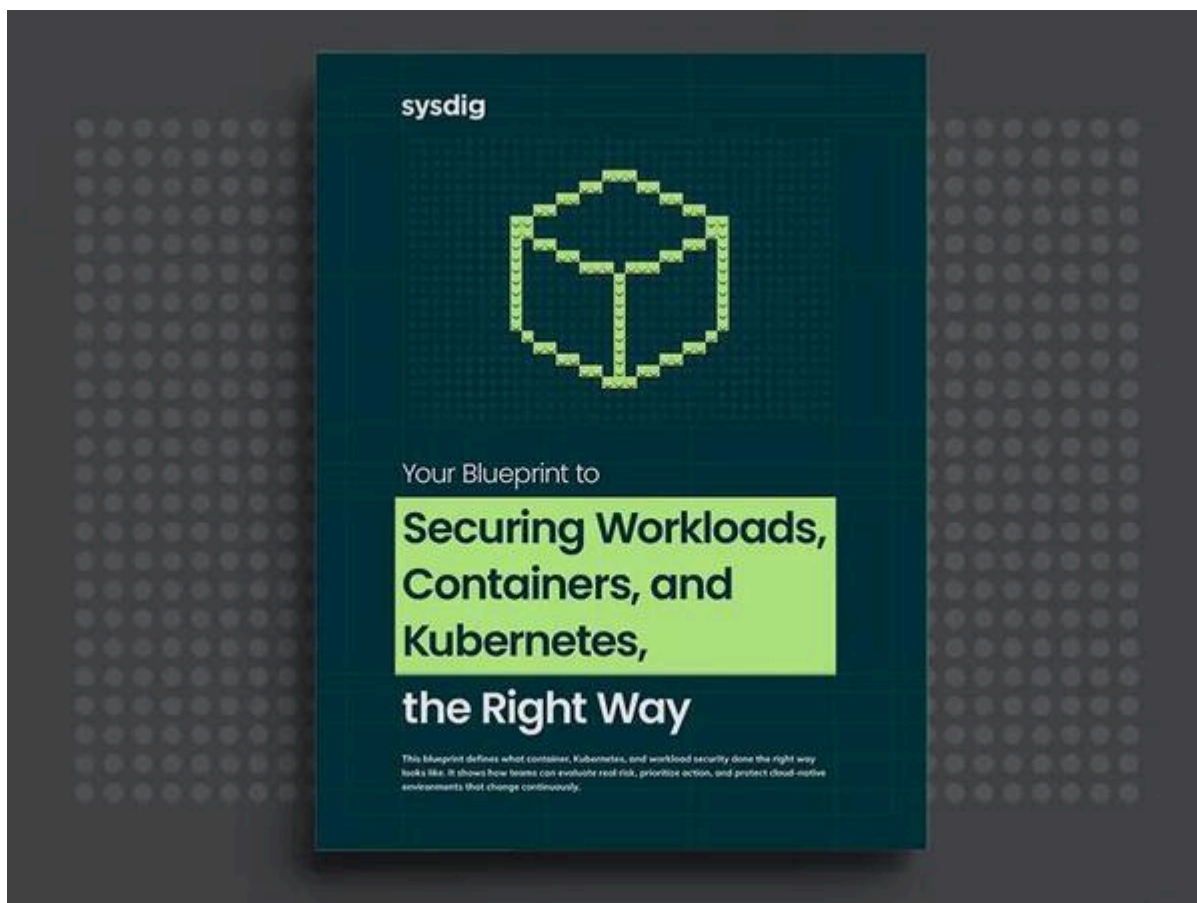
Try Sysdig for free

START FREE TRIAL

Copyright © 2022 Sysdig, Inc. All rights reserved. PB-017 Rev. A 12/22

[BRIEF: Kubernetes and Cloud Monitoring for Financial Servicespdf](#)

[Cloud MonitoringKubernetes](#)

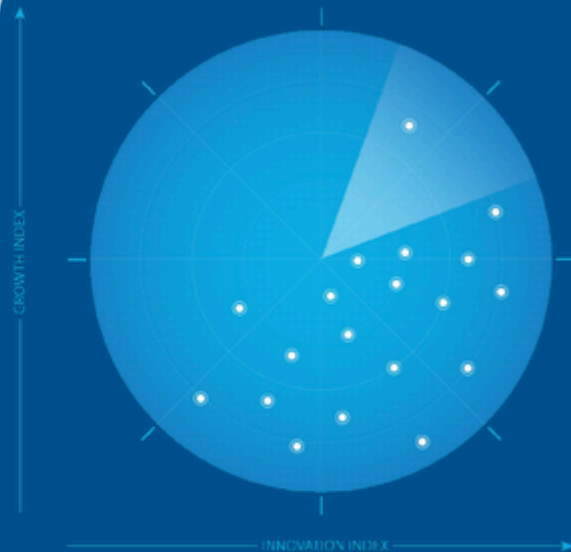


[BLUEPRINT. Your Blueprint to Securing Workloads, Containers, and Kubernetes, the Right Waypdf](#)

FROST & SULLIVAN

# Frost Radar™: Cloud-native Application Protection Platforms, 2022

A Benchmarking System  
to Spark Companies to  
Action - Innovation That  
Fuels New Deal Flow and  
Growth Pipelines



Author: Anh Tien Vu  
Industry Principal, Global Cybersecurity

PD8C-74  
November 2022

[REPORT. Frost Radar Cloud Native Application Protection Platforms 2022.pdf](#)



[CASE STUDY. Data Notebookpdf](#)

[Cloud MonitoringSysdig Monitor](#)

**sysdig** | CUSTOMER STORY **PARTIOR**

## Unlocking the Power of AI: How Partior Saves One Week Each Month with Sysdig Sage™

**1 week** saved per month with Sysdig Sage

**10%** fewer cases to investigate

**57%** reduction in alert noise

### Summary

For blockchain-based Partior, security meant going beyond compliance checkboxes to build real defenses. Used by leading global banks, the company built its platform with a security-first philosophy, recognizing that compliance certifications alone would not protect against sophisticated attackers. To safeguard global transactions, Partior pursued a defense-in-depth strategy in collaboration with Sysdig to deliver the system-level visibility and runtime insights needed to expose the truth in the cloud. Through defense-in-depth and artificial intelligence (AI)-powered prioritization, the Partior team cut through noise, strengthened collaboration, and gained the confidence to secure every transaction without compromise.

#### Key Results

- Deep system call visibility delivers a source of truth that attackers can't evade
- Leaner container images reduced noise and false positives
- Stronger assurance for banks with transparent vulnerability reporting
- Fewer false positives and faster triaging with Sysdig Sage

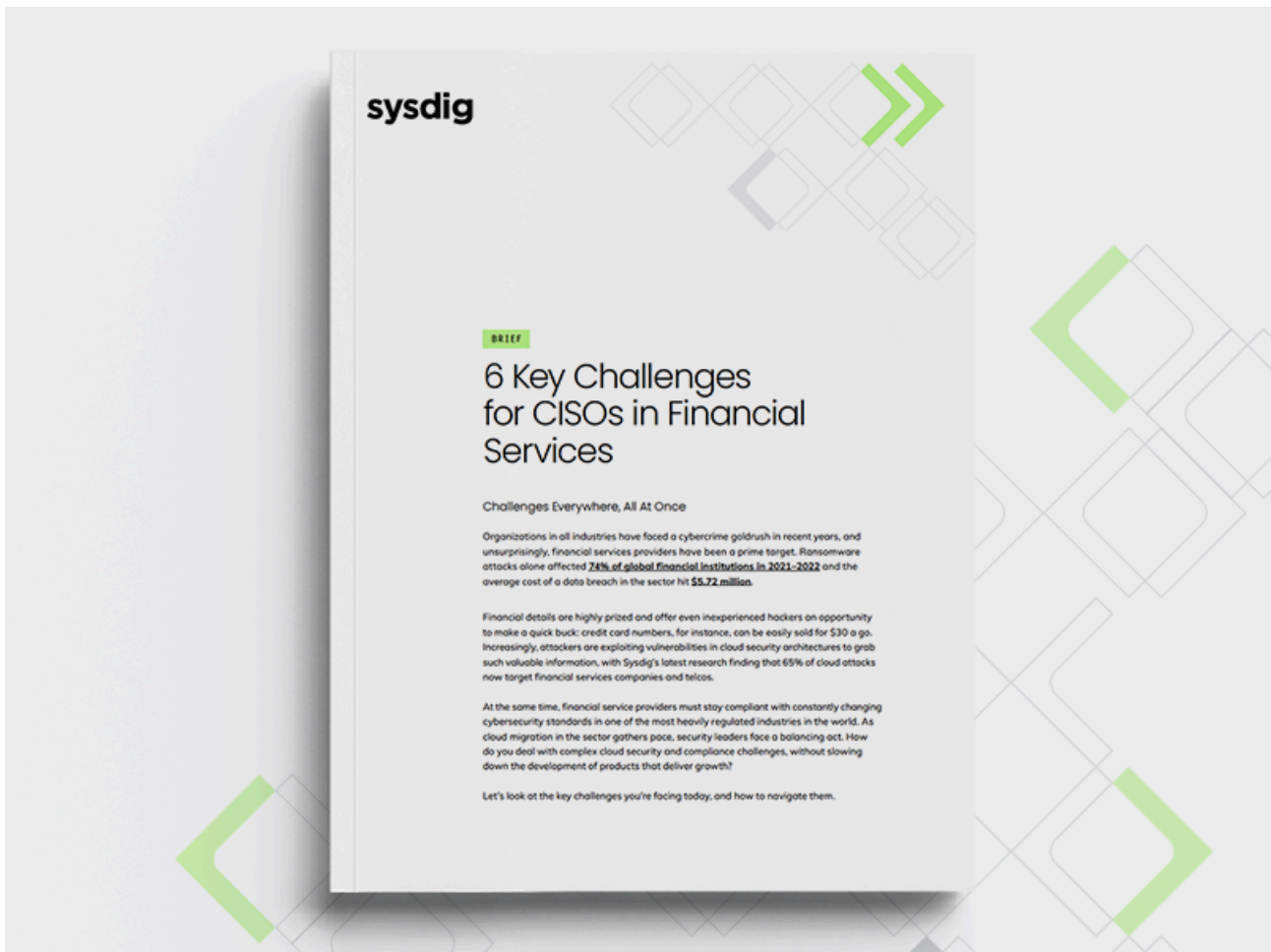
#### Partior

Blockchain network enabling real-time clearing and settlement for global banks.

HEADQUARTERS  
**Singapore**

INDUSTRY  
**Financial Services**

[CASE STUDY: Partiorpdf](#)



[BRIEF. 6 Key Challenges for CISOs in Financial Servicespdf](#)



[WHITEPAPER JP. AIBOM: The infrastructure, risks, and how to secure AI modelspdf](#)



[Endpoint Instrumentation Architecture for Cloud Security Detection and Responsepdf](#)



[VIDEO. The Sysdig vision.video](#)



[REPORT. ESG Survey Report: Cloud Detection And Responsepdf](#)



# Kubernetes and Cloud Monitoring for SaaS Companies

## Modern Cloud Applications Need Modern Monitoring

Organizations are using Kubernetes, Prometheus, and DevOps workflows to build modern cloud-native applications. However, the dynamic nature of these complex environments can lead to gaps in visibility and difficulty in resolving issues when they arise. Meeting user expectations for availability, performance, and cost requires complete visibility into infrastructure, services, and applications across hybrid and multicloud environments. Traditional tools were not built for containers and Kubernetes and can't deliver the granular data and troubleshooting context to rapidly address issues. SREs and developers need easy-to-use monitoring solutions that integrate into DevOps workflows without breaking open source standards.

## Sysdig Monitor Radically Simplifies Cloud and Kubernetes Monitoring

With deep visibility into cloud-native workloads, [Sysdig Monitor](#) helps organizations troubleshoot faster and lower costs. You get immediate, granular details and troubleshooting tools for rapidly changing container environments.

"We were so busy expanding and trying to meet the demand for our internal applications teams that we didn't really have a lot of spare cycles to figure out a scaling solution for Prometheus, so we started taking a look at commercial options. Since Sysdig Monitor's managed Prometheus service is based on open standards we didn't have to worry about re-tooling our monitoring environment."

**Tiziano Tarolla**, Senior Development Manager, SAP Concur

"It's too tedious to go through logs and alerts manually to meet the standards we've established. It would require a full-time person and is not a good use of time. Sysdig enables us to automate the entire process and reach a more accurate level of insight faster."

**Michal Pazucha**, Security Architect at BeekeeperLead, Experian Data Labs

"With Sysdig, we're able to resolve incidents faster. We're able to get insights faster. We're able to tell when there are performance problems faster. And so as a result, we're able to deliver a consistent and better customer experience that we otherwise would not be able to without Sysdig."

**Ryan Staatz**, Systems Architect, Mezmo, Inc.

### Kubernetes Monitoring and Troubleshooting

- Troubleshoot Kubernetes errors 10x faster
- Debug cluster, workload, pod, and control plane-level issues quickly
- See a prioritized list of issues with remediation steps, live logs, and YAML files

### Managed Service for Prometheus

- Leverage an enterprise-class managed Prometheus service to dramatically lower the maintenance burden
- Find insights faster with intuitive dashboards and automatic service discovery
- Reduce PromQL complexity using our simple form UI

### Optimizing Cloud-Native Application Costs

- Standardize on a multicloud monitoring solution
- Lower the cost of custom metrics and cut Kubernetes costs by an average of 40%
- Monitor serverless, self-managed, and managed cloud services with a single tool

Try Sysdig for free

START FREE TRIAL

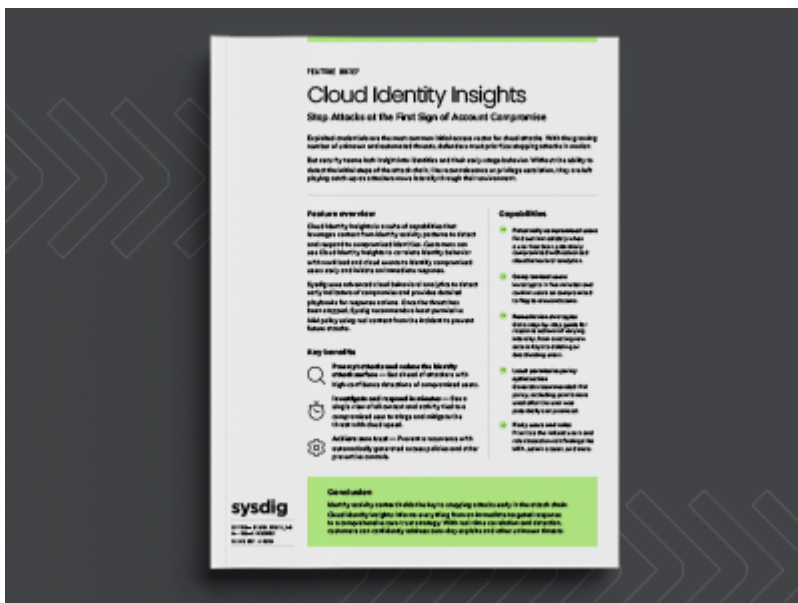
Copyright © 2022 Sysdig, Inc. All rights reserved. PB-018 Rev. A 12/22

[BRIEF: Kubernetes and Cloud Monitoring for SaaS Companiespdf](#)

[Kubernetes](#)



[WHITEPAPER. AIBOM: The Infrastructure Risks And How To Secure AI Modelspdf](#)



[Cloud Identity Insightspdf](#)

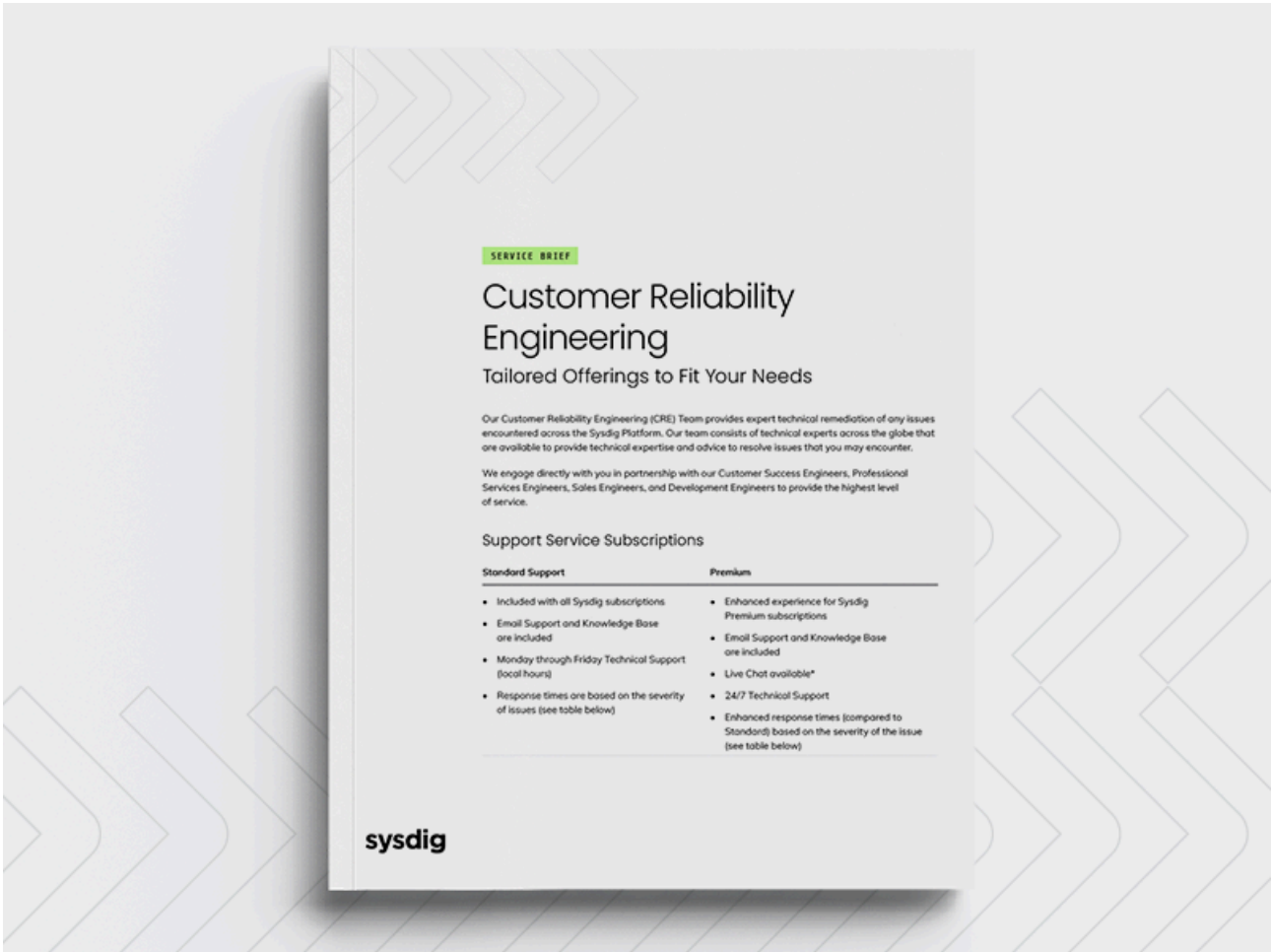


[BRIEF. Cloud Threat Detection Built On Open Sourcepdf](#)

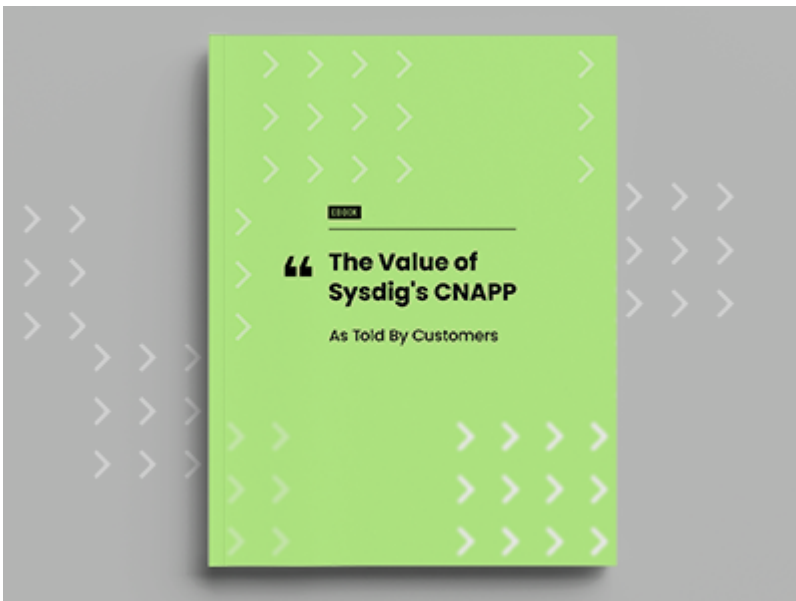
[FalcoOpen Source](#)



[GUIDE. A Guide to Building a Future-Proof Vulnerability Management Programpdf](#)

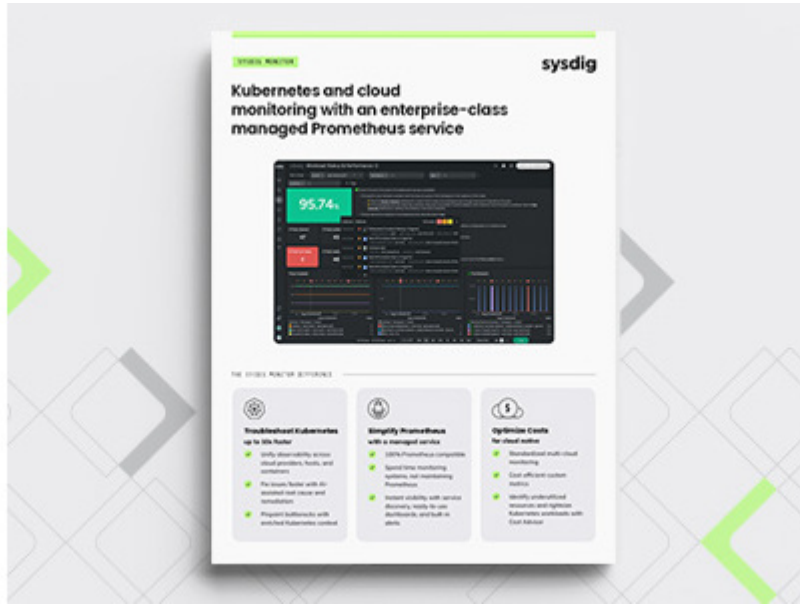


[SERVICE BRIEF. Customer Reliability Engineeringpdf](#)



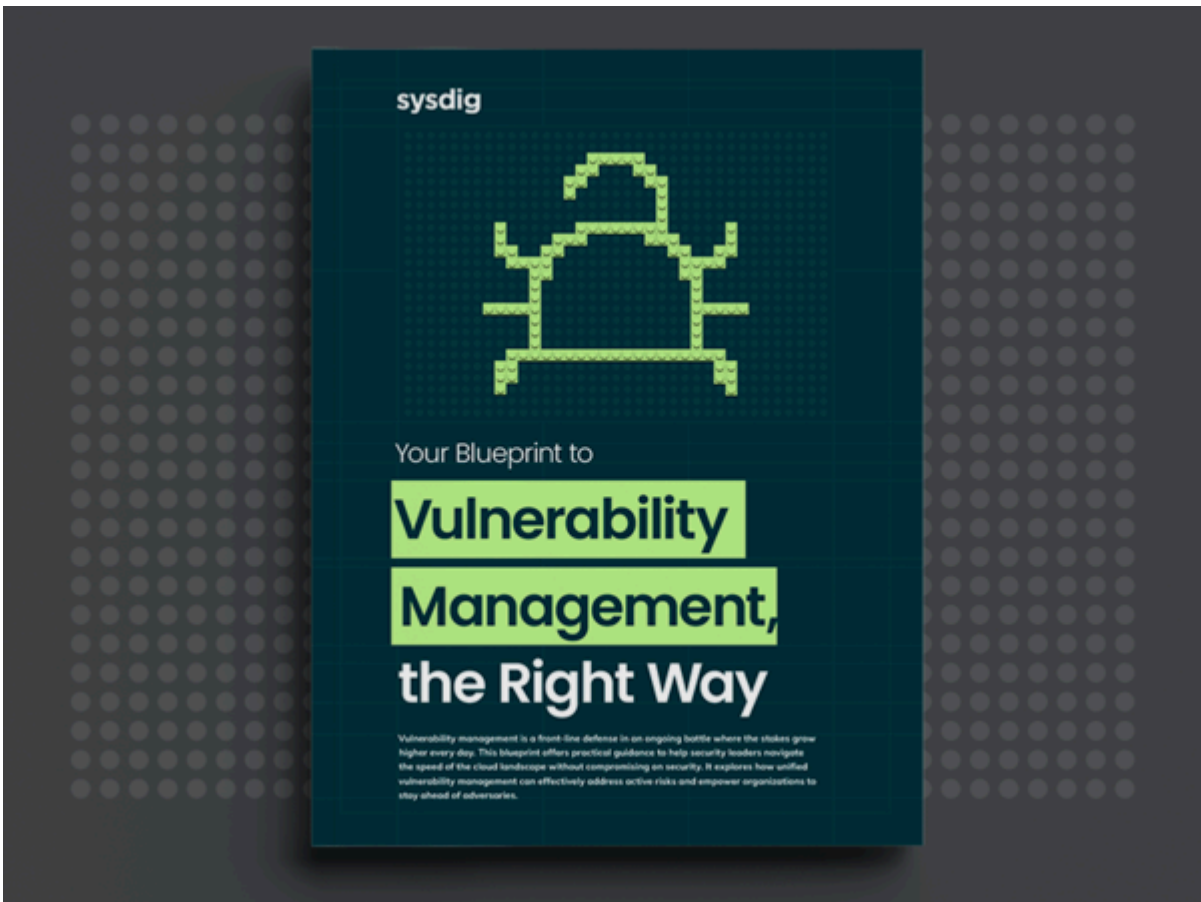
[The Value of Sysdig's CNAPPpdf](#)

[CSPM](#)



[PRODUCT BRIEF. Sysdig Monitor.pdf](#)

[Sysdig Monitor](#)



[Blueprint. Vulnerability Management, the Right Way.pdf](#)

# Kubernetes Rightsizing Guide



[GUIDE. Kubernetes Rightsizing Guidepdf](#)

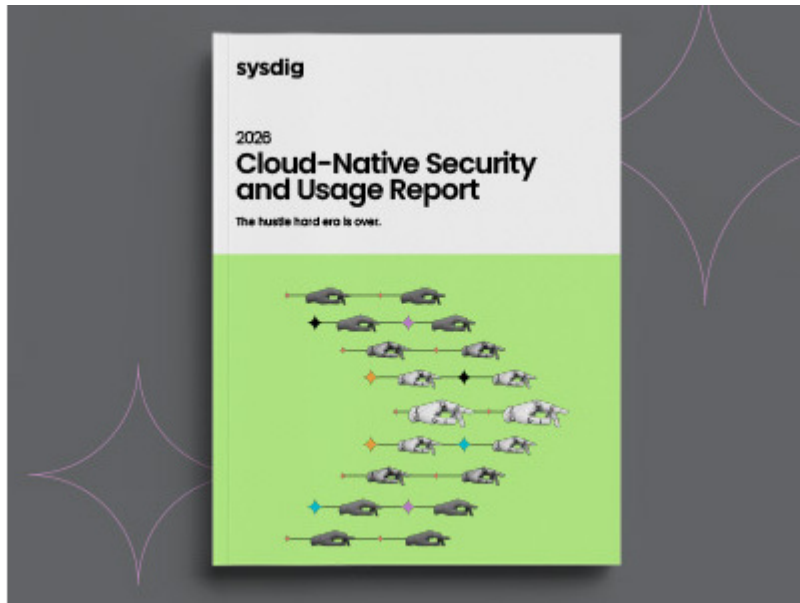
[Kubernetes](#)



[BRIEF. Stop Watching, Start Defending for Practitionerspdf](#)



[Frost Sullivan Company Of The Year Container Kubernetes Securitypdf](#)



[REPORT. 2026 Cloud-Native Security and Usage Reportpdf](#)



[CHECKLIST. The runtime readiness checklistpdf](#)



[VIDEO. Sysdig Monitor: Overview of Alerts](#)[video](#)

[Cloud Monitoring](#)[Kubernetes](#)[Prometheus](#)[Sysdig Monitor](#)



## 6 Considerations for Kubernetes Capacity Planning

Capacity management has always been an issue for companies, but it becomes especially challenging when operating workloads in a cloud-native environment. Cloud-native deployments have to take into account, and declare, specific resources required to operate effectively. Yet, achieving the right balance of availability and reliability requires DevOps, Security, and other IT teams to identify their needs as they establish the relationship between the application architecture and the underlying cloud infrastructure.

There are a variety of factors to consider, and different teams sometimes function with competing needs, so it can be challenging to create a comprehensive and universally-adopted capacity management strategy. Performance and cost will always be factors, and so will the myriad of conditions that regularly change as workload needs shift.

Modern organizations that have adopted a Kubernetes-based approach to application development and workload management will want to prioritize capacity planning. This guide offers a framework that will help enterprises make their environments more efficient and be prepared to support the needs of their Kubernetes clusters through effective use and planning of resources.

### Planning for the reality of Kubernetes limitations

Kubernetes delivers so many advantages, but the reality about its inherent resource constraints is that having too little resources can result in CPU activity being throttled and pods receiving an out-of-memory (OOM) error. Conversely, if pods are requesting too much, then the Kubernetes engine won't have enough space to allocate new workloads and resources will be wasted. The right balance is determined by what a team's most pressing needs are, and those may change over time.



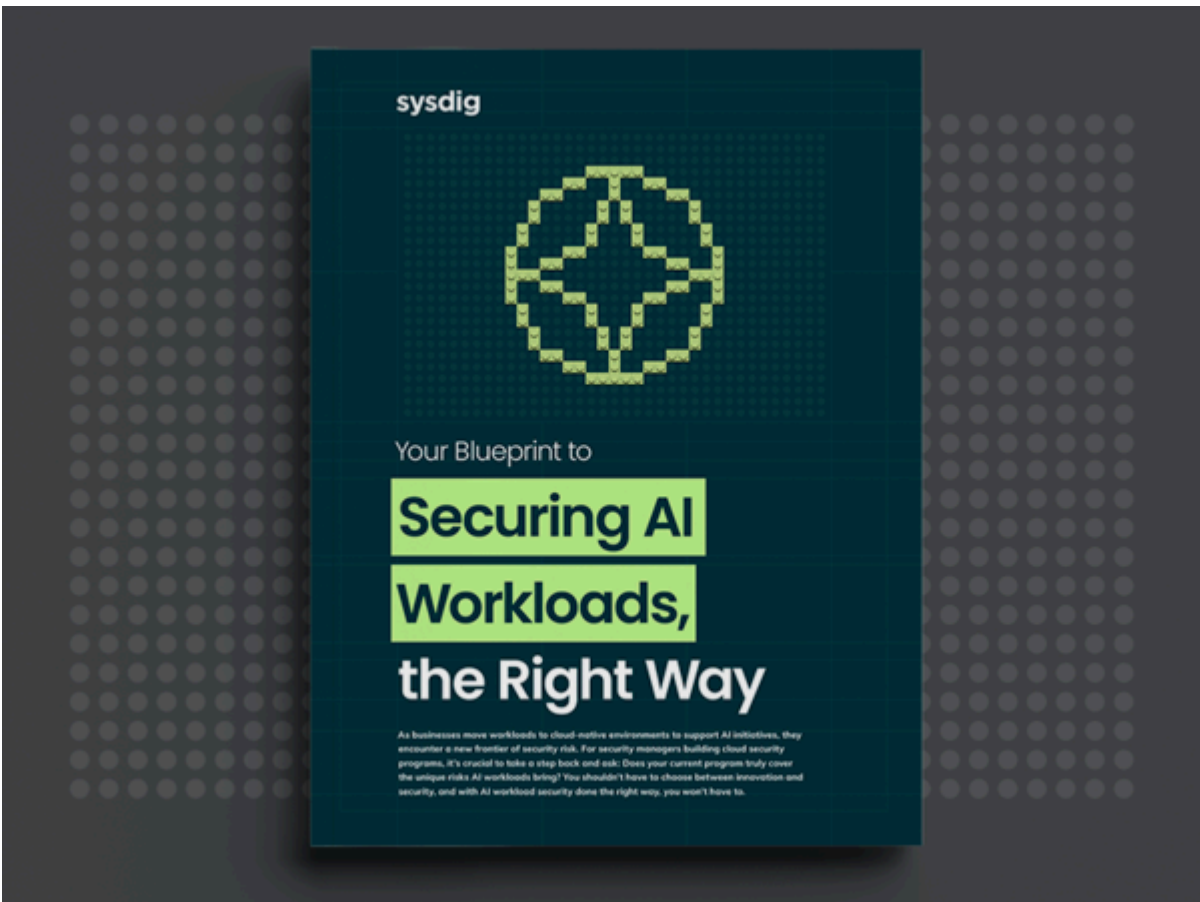
[BRIEF: 6 Considerations For Kubernetes Capacity Planningpdf](#)

[Cloud MonitoringKubernetesSysdig Monitor](#)



[Sysdig Sage Solution Briefpdf](#)

[Cloud computing security](#)



[BLUEPRINT. Your Blueprint to Securing AI Workloads, the Right Waypdf](#)



[BRIEF. The Business Value of Agentic AI For Cloud Securitypdf](#)

[Sysdig Sage](#)

# Top 10 metrics in PostgreSQL monitoring with Prometheus

Learn the top 10 metrics in PostgreSQL monitoring, with alert examples, both for PostgreSQL instances in Kubernetes and AWS RDS! Read the full guide in <https://sysdig.com/blog/postgresql-monitoring/>

1



## AVAILABILITY Server is up

Checking that your instance is up and running should be the first step in PostgreSQL monitoring. The exporter will monitor the connection and availability of the PostgreSQL instance.

```
pg_up == 0
```

3

### REPLICATION

## Replication lag



A high replication lag rate can lead to coherence problems if the master goes down.

```
pg_replication_lag > 10
```

### AVAILABILITY

## Postmaster Service Uptime

The minimum postmaster service uptime should reflect the last known controlled server restart. Otherwise, a server may have been restarted for unknown reasons.

```
time() - pg_postmaster_start_time_seconds < 3600
```



2

4

### STORAGE

## Database size

Running out of disk is a common problem in all databases. Let's figure out what is the storage usage of each of the PostgreSQL databases in our instance.

```
pg_database_size_bytes
```



6

### NET WORKING

## Number of available connections

A common problem in databases is running out of network connections.

```
((sum(pg_settings_max_connections) by (server) - sum(pg_settings_superuser_reserved_connections) by (server)) - sum(pg_stat_activity_count) by (server)) / sum(pg_settings_max_connections) by (server) * 100 < 10
```



5



## Available storage

Check also the available disk in your instance.

### KUBERNETES

```
predict_linear(node_filesystem_free_bytes[1w], 3600 * 24) / (1024 * 1024 * 1024) < 1
```

### AWS RDS POSTGRESQL

```
predict_linear(aws_rds_free_storage_space_average[48h], 48 * 3600) < 0
```

7

### PERFORMANCE

## Latency

Latency is a key indicator of your database performance. You can measure how long it takes to get the result of the slowest active transaction.

```
pg_stat_activity_max_tx_duration(state='active') > 2
```



8

### PERFORMANCE

## Cache hit rate

High latency can be a consequence of problems with cache in memory, which increases disk usage, so everything is slower.

```
100 * (rate(pg_stat_database_blks_hit[$_interval]) / ((rate(pg_stat_database_blks_hit[$_interval]) + rate(pg_stat_database_blks_read[$_interval])) > 0)) < 80
```



9

### PERFORMANCE

## Memory available

The solution for a low hit rate is increasing the memory usage of your instance. Check if there's enough memory available.

### KUBERNETES

```
sum by(namespace, pod, container) (kube_pod_container_resource_limits(resource='memory')) - sum by(namespace, pod, container) (container_memory_usage_bytes(container!='POD', container!=''))
```

### AWS RDS POSTGRESQL

```
aws_rds_freeable_memory_average
```



10

### PERFORMANCE

## Requested buffer checkpoints

PostgreSQL uses the buffer checkpoints to write the dirty buffers on the disk. A high number of requested checkpoints compared to the number of scheduled checkpoints can directly impact performance.

```
rate(pg_stat_bgwriter_checkpoints_req[5m]) / (rate(pg_stat_bgwriter_checkpoints_req[5m]) + rate(pg_stat_bgwriter_checkpoints_timed[5m])) * 100
```



[INFOGRAPHIC. Top 10 Metrics In Postgresql monitoring with Prometheuspdf](#)

[Cloud MonitoringOpen SourcePrometheusSysdig Monitor](#)



# 5 Keys to Optimizing Costs of Running Cloud-Native Apps

## Cloud and Kubernetes costs, the challenge

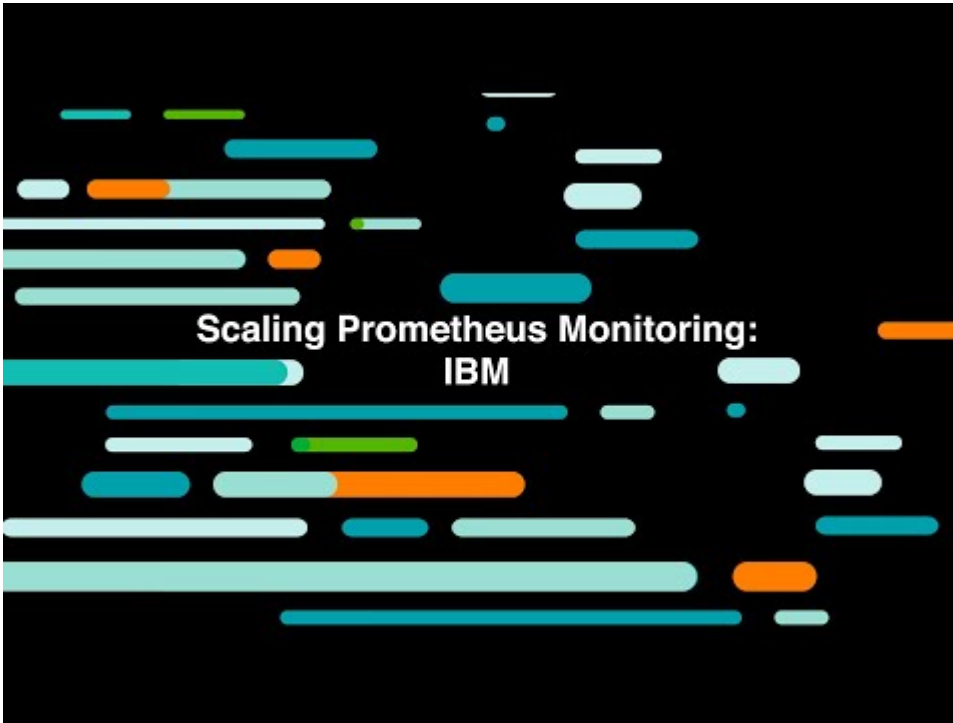
Cloud and Kubernetes costs is certainly a broad and complex topic. If you are early in your cloud-native journey, you'll soon realize that cost management is something that needs to be tackled, the sooner the better. Companies that don't take care of their Kubernetes and cloud costs are most likely to waste tons of money on their Kubernetes and cloud bills at the end of the month. This can sound pretty obvious, but many businesses don't realize how tough and necessary this task can be until they spend thousands of dollars.

So why is managing Kubernetes costs so challenging? Many factors contribute to this problem, but the nature of microservices is a key contributor. These new microservices architectures enable users, departments, and organizations to deploy and maintain applications easier and faster. In this new era, you have to pay attention to the associated costs of deploying and maintaining services in the cloud. Poor architectures and application designs, as well as deploying or scaling up applications easily are some of the factors that contribute to runaway costs. That's why you may end up overspending resources and money, making your Kubernetes and cloud bills grow significantly.



[BRIEF: 5 Keys to Optimizing Costs of Running Cloud-Native Appspdf](#)

[Cloud MonitoringCost OptimizationSysdig Monitor](#)



[VIDEO. Scaling Prometheus Monitoring: IBMvideo](#)

[Cloud MonitoringIBMPrometheusSysdig Monitor](#)

**sysdig**

**BRIEF**

## Stop watching. Start defending.

Act the moment risk becomes real  
— before it becomes a breach.

Exploitation timelines have collapsed — from months to hours. As cloud environments scale and change constantly, the window to detect and respond has nearly disappeared. Small exposures can quickly become major incidents.

Security at cloud speed means acting where risk is real — at runtime. Early signals — a misused credential, an unexpected process, a workload behaving differently — reveal what actually matters, giving teams the clarity to act before issues escalate.

Organizations have more visibility than ever, but still struggle to act. Dashboards overflow with alerts. Posture scans highlight what might be exposed. Logs capture activity across systems. But most systems surface potential risk — not what's actually happening.

That's the gap your teams don't just need visibility. They need to understand what presents real risk right now — and what action to take before it impacts the business.

**FORRESTER**  
**WAVE LEADER 2024**  
Cloud Native Application Protection Solutions

Sysdig named a Leader in the Forrester Wave™, Cloud Native Application Protection Solutions, Q1 2024

**“ Sysdig doesn't waste time on what doesn't matter. It helps us stay focused on the vulnerabilities and events that are actually a priority — so we can secure the organization quickly and efficiently. ”**

**jumpcloud.**  
— Robert Phan, CISO at JumpCloud

[BRIEF. Stop Watching, Start Defending for Leaderspdf](#)



DECEMBER 2024

## The Power of Native Cloud Detection and Response Services

Dave Gruber, Principal Analyst

**Abstract:** The pace of cloud infrastructure development and innovation has left many security professionals caught without the level of knowledge, visibility, and mechanisms they need to understand and investigate threats in the cloud. While advancements in detection and response solutions—including extended detection and response (XDR), security event and incident management, and evolving cloud-native application protection platforms—have come along, few can achieve their cloud security objectives. New strategies are needed.

### Overview

Modern operating environments are diverse, comprised of infrastructure, services, and applications deployed in the cloud and on premises. Security strategies require defense in depth, including proactive security hygiene and posture management, preventative controls, and detection and response mechanisms that align with and respond to individual attack vectors within the operating environment.

As the threat landscape continues to evolve and enable attackers to find ways to evade security control, the role of detection and response has elevated, spawning further investment in tools that can provide the level of visibility and threat signal needed to detect novel and known threats in all environments.

#### The Struggle Continues With Cloud Detection and Response

The pace of cloud infrastructure development and innovation has left many security professionals caught without the level of knowledge they need to understand and investigate threats in the cloud.

Across the many vectors that comprise an organization's attack surface, research from TechTarget's Enterprise Strategy Group showed cloud detection and response as a notable gap for many, as organizations struggle to capture, correlate, and analyze signals required to understand and investigate attacks.<sup>1</sup>

Highlighting this issue, Enterprise Strategy Group's research showed that the top two use cases for XDR investments are the need to investigate advanced threats,

followed by the need to support threat detection and response for cloud resources.<sup>2</sup>

But when it comes to cloud security operations, many organizations are still ramping up, often depending on cloud-specific knowledgeable resources for support. This is evident in the fact that only 30% of organizations reported their security operations center completely owns all aspects of cloud security; in other words, 70% of organizations depend on separate cloud SecOps teams to secure cloud infrastructure.<sup>3</sup> As organizational models evolve to meet the security needs of this fast-moving area, overlapping security tools create additional challenges, as traditional detection and response tools often lack the data, context, and analytics required. New strategies are needed.

<sup>1</sup> Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.

<sup>2</sup> Ibid.

<sup>3</sup> Ibid.

This Enterprise Strategy Group Showcase was commissioned by Amazon Web Services and is distributed under license from TechTarget, Inc.

© 2024 TechTarget, Inc. All Rights Reserved

1

[WHITE PAPER. The Power of Native Cloud Detection and Response Servicespdf](#)

# Cloud Security Powered by **Runtime Insights**



In the cloud, every second counts. Malicious actors are weaponizing the flexibility and programmability of the cloud to stay undetected and move fast. 10 minutes — that's all it takes to execute a cloud attack.

Sysdig is the only cloud-native application protection platform (CNAPP) powered by runtime insights that provides the visibility, coverage, and context required by security teams to outpace attackers. From prevention to defense, Sysdig helps your business focus on what matters: innovation.



"I want to immediately know when someone's in my environment — not 15 minutes or several hours later. With Sysdig, we can identify and address potential threats in real time."

Senior Infrastructure Security Engineer



## Get Complete Visibility

Eliminate visibility gaps created by disparate solutions. Sysdig provides a unified view of risk across your entire cloud estate and the context needed to take action.



## Eliminate 95% of the Noise

Identifying your top risks shouldn't require scouring through a mountain of alerts. Sysdig leverages the knowledge of what's in use to prioritize what you need to focus on.



## Detect and Respond to Threats Fast

Cloud attacks are fast, but you can be faster. Sysdig accelerates threat detection and response in real time with end-to-end coverage and correlation across workloads, identities, cloud services, and third-party applications.



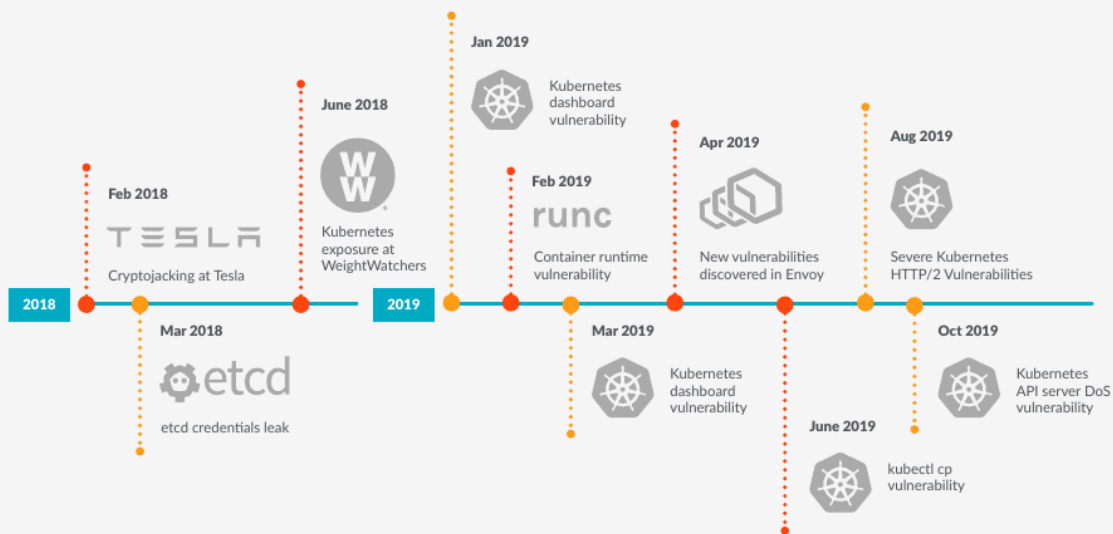
[BRIEF. Company Overviewpdf](#)



# Securing Kubernetes in Production

## Are you ready?

As Kubernetes scales up, security is the #1 challenge facing DevOps\*



\* IDC TechBrief: Containers

**Vulnerabilities or misconfigurations were not addressed before deployment**

52% container images fall scans with high severity\* that leaves applications exposed to attacks\*

**Best practices for runtime prevention and detection were not in place**

On average, 21 containers per node are running as root, opening the door for container breakouts\*

**Most container breaches are often undetected until it is too late**

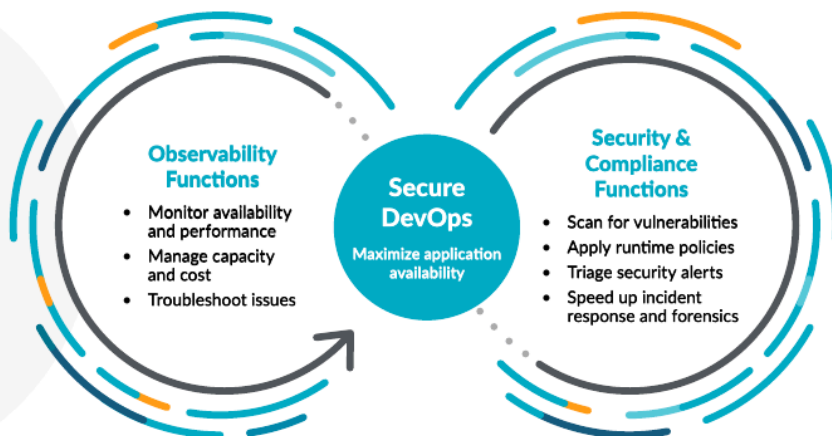
5 min container lifespan requires purpose-built tools for audit and incident response\*

**Security is often addressed after deployment**

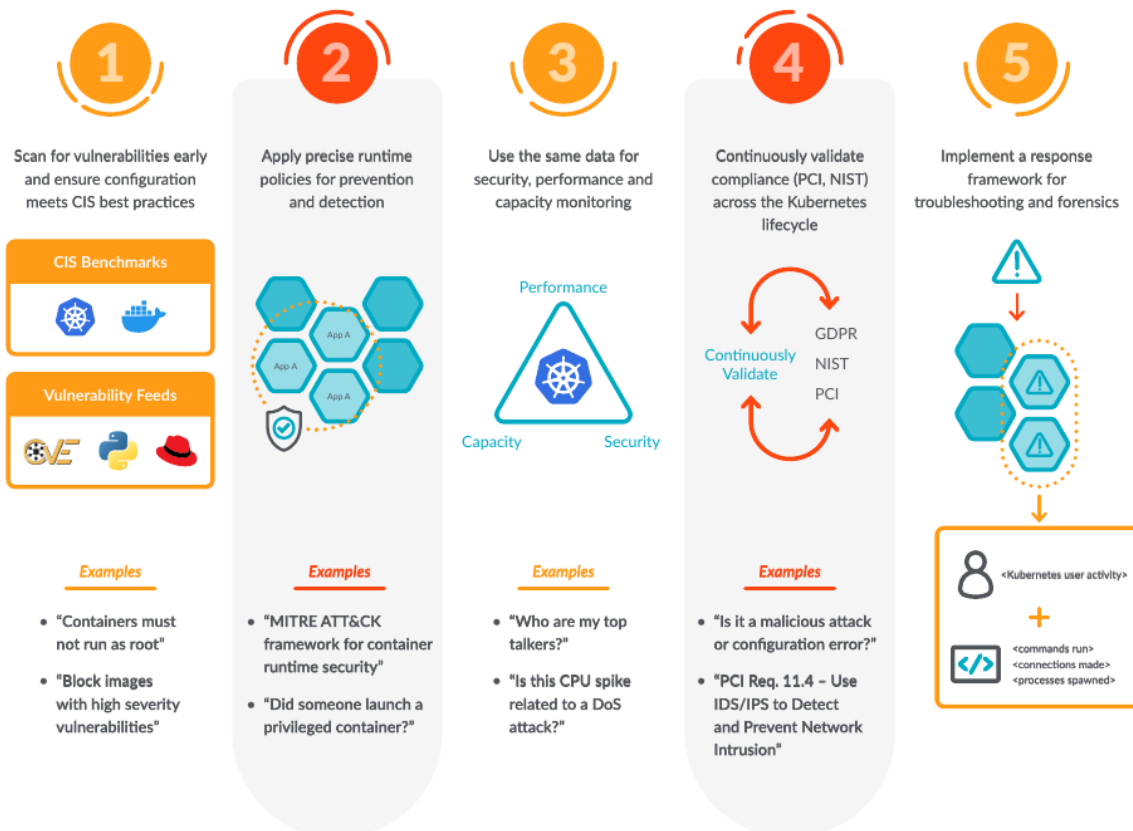
\* Sysdig 2019 container usage report

[Read the Report](#)

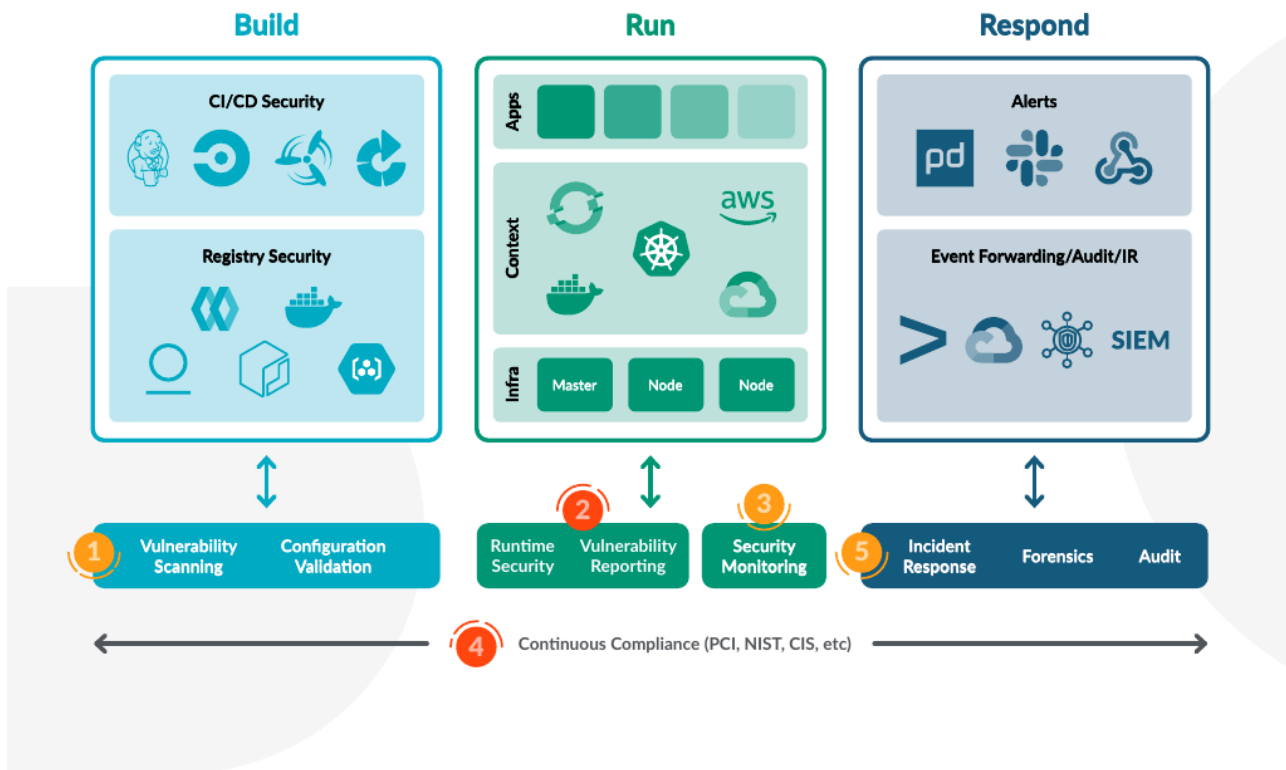
DevOps adds security and compliance into their workflow



### Adopt a 5 step checklist for a secure DevOps workflow



Embed your secure DevOps workflow into your existing cloud-native ecosystem



Tools must support a secure DevOps workflow to run Kubernetes and containers in production.



To learn more about how security is converging with DevOps, read the 5 Keys to a Secure DevOps Workflow.

GET IT NOW



[INFOGRAPHIC. Securing Kubernetes in Production. Are You Ready?pdf](#)

[Kubernetes](#)



## Checklist: Container Security from Code to Runtime

Modern software development has shifted towards microservices built on containers, Kubernetes, and cloud, and at the same time, adoption of DevOps culture is driving continuous software deployment to rapidly meet business needs. Security in these fast-moving cloud-native environments requires a radically different approach.

Software vulnerabilities, misconfigurations, and suspicious activity at runtime are all areas of concern for developers, operations, and security teams. As containers and DevOps practices blur the boundary between code development and the production environment, security solutions that satisfy the needs of development teams or operations teams in isolation can leave gaps and result in inefficient security practices.

Adopting a cohesive and automated approach to security from development through production helps teams stay vigilant against cyberattacks, reduce noise, and tackle the unique risks of containers, Kubernetes, and cloud. The right practices from source to run are critical for securing your cloud-native environment, but will also enable greater efficiency to help you ship applications faster.

The following checklist outlines key security strategies and best practices to follow from source to run. These key aspects of container security center around three major themes:

### Build Secure from the Start

Introducing security practices as early as possible in the development phase of your software development lifecycle (SDLC) helps you guard against issues that can expose risk, delay, and cost in later stages. This "Shift Left" approach encourages development teams to implement the required practices and tools to ensure they build secure applications from the start.

### Protect against runtime threats

While code, container, and IaC security best practices provide protection from known issues and misconfigurations, these practices alone are not enough. A host of security threats, by their very nature, only manifest during runtime. Detecting and responding to malicious activity such as privilege escalation attempts in containers requires new vantage points and cloud-native controls.

### Prioritize security alerts that matter

Containers are often bloated with contents and packages, overwhelming developers with vulnerabilities. Attempting to wade through an unmanageable number of issues takes precious time away from coding and leaves organizations open to risk. Techniques such as using runtime intelligence will help developers prioritize vulnerabilities for packages that are actually used when a container runs, reducing the burden by as much as 95%.

[GUIDE. Checklist Container Security From Code To Runtimepdf](#)

[Snyk](#)



## Vulnerability Management for the Cloud

Prioritize and Fix the Vulnerabilities that Matter

Cloud-native environments move fast, and vulnerabilities are easy targets for attacks. But legacy vulnerability tools haven't kept up. They flood teams with noise and lack the cloud context needed to focus efforts where they matter most. Sysdig delivers vulnerability management built for the realities of modern application development.

Sysdig combines runtime insights, cloud context, and AI-powered remediation to help you cut through the noise and fix what matters faster. With visibility across the full application lifecycle, from source to runtime, and intelligent prioritization, Sysdig reduces alert fatigue and accelerates time to remediate. Wherever your workloads run in the cloud, Sysdig helps you take control of vulnerabilities at scale.



Throwing a thousand tickets at engineers isn't a strategy. Sysdig breaks remediation into clear, achievable tasks — with results we can see.

CISO



### Runtime-powered prioritization

Filter out up to 95% of alert noise by prioritizing in-use vulnerabilities, enriched with risk context like exploitability, exposure, and criticality.



### AI-guided remediation

Sysdig Sage™, our AI cloud security analyst, delivers expert-level recommendations to fix high-impact vulnerabilities fast.



### Expansive coverage

Get unified visibility into vulnerabilities across cloud and on-prem, spanning containers, Kubernetes, traditional hosts, and the full application lifecycle, from development to production.



### Streamlined collaboration

Bridge the gap between security and developers by automatically routing fixes to the right teams, with full-context alerts delivered through ticketing integrations.



[SOLUTION BRIEF, Vulnerability Management for the Cloudpdf](#)



[BRIEF. CXO Takeaways from the Sysdig 2026 Cloud-Native Security & Usage Reportpdf](#)



# Need to Extend Prometheus Monitoring?

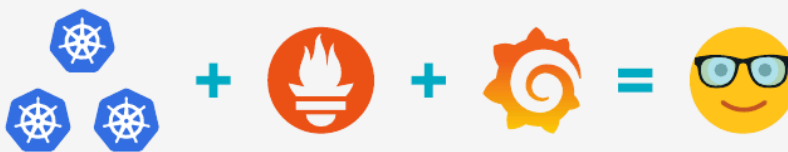
Dynamic, container-based environments can be a challenge for monitoring cloud-native applications. While Prometheus is gaining rapid developer adoption as the open-source monitoring standard, scaling beyond a few clusters can be challenging.

## Typical Prometheus Journey

### Typical Prometheus Journey

#### Start

You most likely have developers using the Prometheus open source project within your organization. Usually, Prometheus is adopted to monitor a small project or application. That's because Prometheus is fairly easy to use in a small environment with a few exporters and Grafana dashboards.



### Typical Prometheus Journey

#### Expand

When additional clusters are added for new services, there is a need to switch between different Prometheus servers to see metrics across the clusters. While this is workable, gaps around metric retention, metric scalability, ability to query across clusters and integration in the DevOps workflow begin to emerge.





### Typical Prometheus Journey

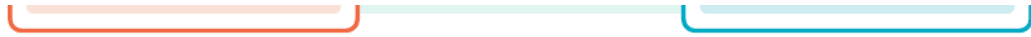
## Scale

As your environment expands, complexity in maintaining global visibility increases. You may need to grow the volume of metrics, retain metrics and analyze and query them, as well as implement access controls. Many organizations invest significant resources and time to address these scale challenges in-house with very limited success.



## Options for Extending Prometheus

Build it Yourself	Core Considerations	The Sysdig Solution
<p>Build and manage Prometheus. Customize monitoring capabilities to fit your teams, applications, and cloud-native rollout.</p>	<p><b>Configuration and Maintenance</b></p>	<p>Free up valuable resources with a completely vendor-supported On-Prem or SaaS solution that offers full Prometheus compatibility.</p>
<p>Identify exporters to monitor applications and services from the open source community.</p>	<p><b>Integrations</b></p>	<p>Access managed integrations for applications via PromCat, paired with the right dashboards and alerts.</p>
<p>Gain visibility with metrics ingested every 10 seconds and limited retention for each Prometheus server.</p>	<p><b>Scale</b></p>	<p>Centralize on a scalable platform that offers millions of time series data with 10-second resolution and 13 months of retention.</p>
<p>Trial and error to understand what is important to monitor in a cloud-native context.</p>	<p><b>Troubleshooting</b></p>	<p>Get access to deep container visibility with the ability to troubleshoot faster and proactively with service and container level context.</p>
<p>Secure Prometheus data connection and control access to the metrics on a server by server basis.</p>	<p><b>Access</b></p>	<p>Use enterprise access controls like RBAC, SSO, LDAP or Sysdig Teams.</p>



Learn more about turnkey Prometheus scaling solution, **Sysdig Monitor**

[LEARN MORE](#)



ING-005 Rev. A 4/20



[INFOGRAPHIC. Need to Extend Prometheus Monitoring?pdf](#)

[Open Source Prometheus Sysdig Monitor](#)



[VIDEO. KubeCon Intro: Falco - Loris Degioanni, Sysdigvideo](#)

A Sysdig case study infographic titled "How One Company Reduced SOC 2 Audit Work by 80%". The infographic is set against a grey background with large white arrows pointing right. It features a central image of a person working at a computer. The infographic lists key results: 1/4 lower total cost of ownership, 80% faster audit evidence collection, and SOC 2 compliance achieved and maintained. It also includes a summary of the company's challenges and how Sysdig provided a solution, along with key results and company information.

**sysdig** | ESTABLISHED 2007 Global Digital Infrastructure Provider

## How One Company Reduced SOC 2 Audit Work by 80%

**1/4** lower total cost of ownership

**80%** faster audit evidence collection

**SOC 2** compliance achieved and maintained

### Summary

A global digital infrastructure provider needed a more reliable way to meet System and Organization Controls (SOC) 2 requirements across a large fleet of Kubernetes clusters. Engineers were spending too many hours combing through logs, and their tools often made it hard to see what was actually happening in production. As the audit deadline approached, the team needed a clearer and more dependable path to validating controls and resolving issues early.

Growth added another layer of complexity. As more teams deployed services independently, the operational picture became increasingly fragmented. Tooling varied from group to group, and understanding how applications behaved across environments required time that the teams no longer had. The organization needed a shared, trustworthy view of activity in production that could support both compliance work and day-to-day decision-making at scale.

sysdig brought that clarity. With real-time runtime insight and automated reporting, the team could replace manual, last-minute reviews with a continuous understanding of their posture and a more confident path through each audit cycle.

#### Key Results

- Eliminated the manual work that previously slowed compliance and audit readiness.
- Improved risk prioritization with accurate runtime insights instead of noisy alerts.
- Consolidated fragmented tools into one platform built to scale with global infrastructures.

**Global Digital Infrastructure Provider**  
Global operator of distributed digital infrastructure platforms.

**HEADQUARTERS**  
United States

**INDUSTRY**  
Infrastructure Software & Services

[CASE STUDY. Global Digital Infrastructure Provider.pdf](#)



[BLUEPRINT. Agentic Cloud Security, the Right Way.pdf](#)

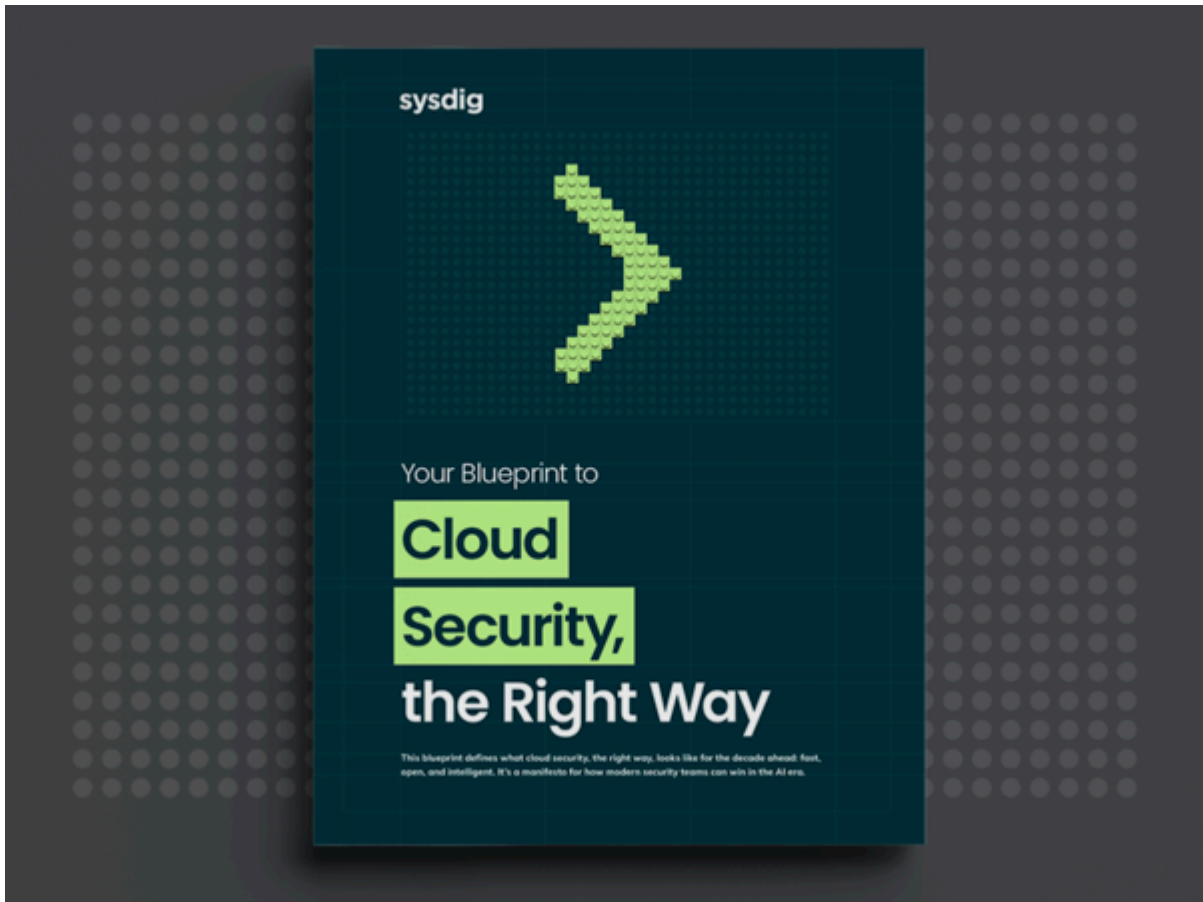


[BRIEF: 4 Critical Business Values Delivered By Sysdig Cloud Detection And Response.pdf](#)



[EBOOK. Securing the Cloud: The Benefits of Falco with an Enterprise Experiencepdf](#)

[Falco](#)



[BLUEPRINT. Cloud Security, the Right Way.pdf](#)



[VIDEO. You're Monitoring Kubernetes Wrong](#)video

[KubernetesSysdig Monitor](#)



[VIDEO. Extending security with Sysdig and IBM Cloud Pak for Multicloud Management \(MCM\)](#)video

# Sysdig Sage™

## The first conversational AI cloud security analyst

Accelerate human response to cloud threats



Cloud risk is constantly evolving. Attacks are becoming faster and more sophisticated. To stop threats, defenders need help investigating and understanding the full picture in real time.

Sysdig Sage brings generative AI insights to the Sysdig cloud-native application protection platform (CNAPP). Powered by an autonomous AI agent architecture, Sysdig Sage uses multi-step reasoning and contextual awareness to thoroughly analyze cloud security threats, incidents, and posture, accelerating the resolution of cloud risk and security incidents.



This is what AI should have been doing for us all along. It's about making the human's response capability better and faster.

Chief Information Security Officer



### Accelerate response with a conversation

When you have only minutes to respond, Sysdig Sage turns lengthy investigations into fast, meaningful conversations that help you focus on what matters most.



### Augment defense with a team of AI experts

Sysdig Sage uses an autonomous agents approach, employing specialized domain-specific AI agents that work together like a team of experts to help address cloud security challenges.



### Manage cloud security at any skill level

Sysdig Sage empowers everyone to make the most of Sysdig's real-time cloud security platform.



[Solution Brief: Sysdig Sage.pdf](#)

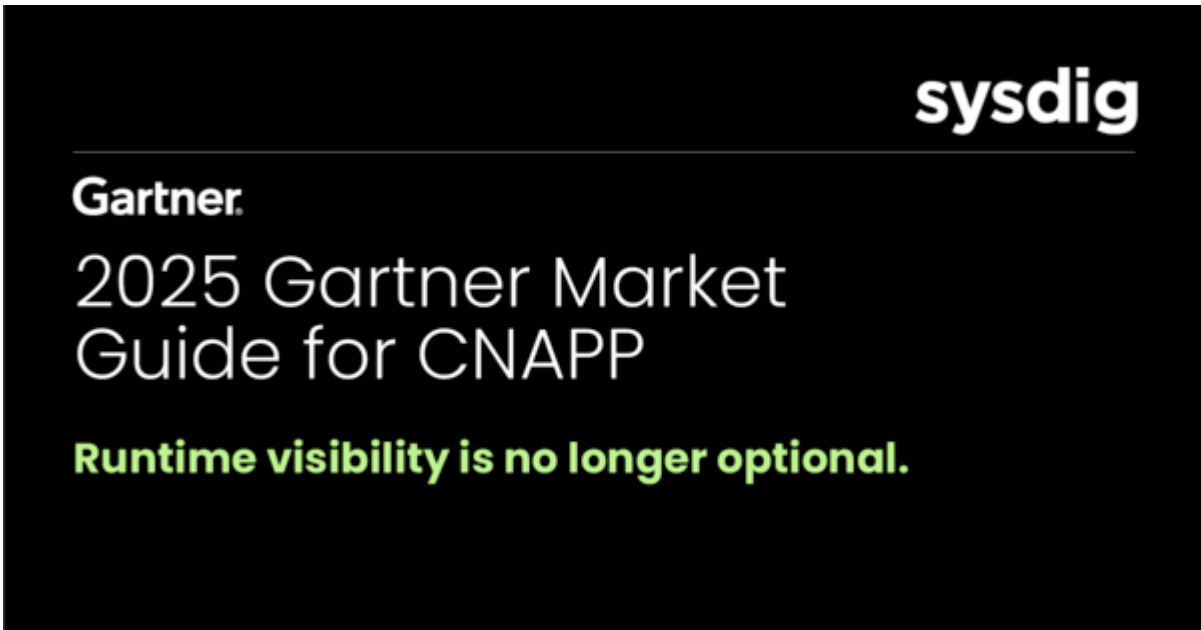
[Sysdig Sage](#)



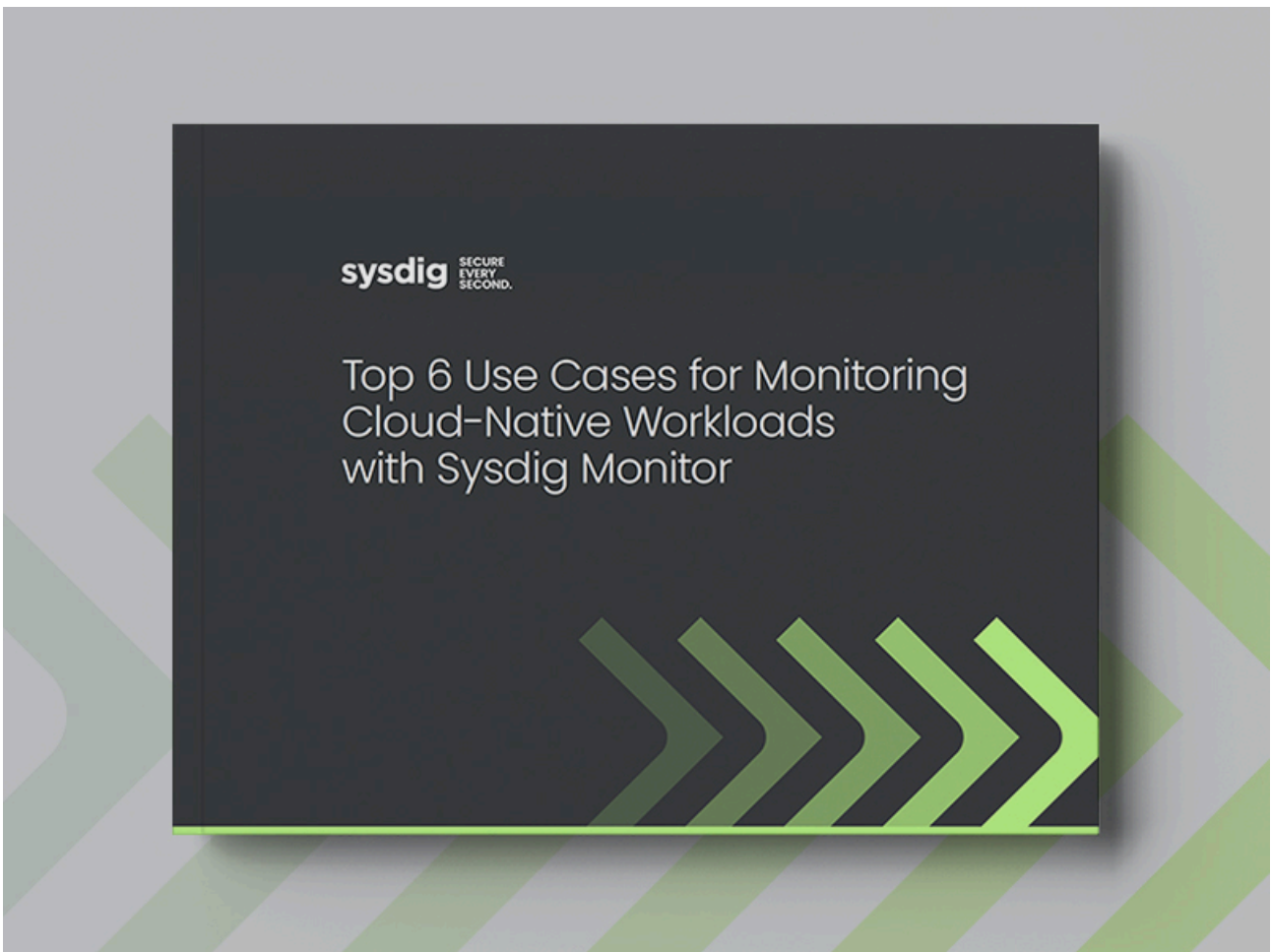
[TOOLKIT. The Practitioner's Toolkit for Securing Workloads, Containers, and Kubernetespdf](#)



[Why it's time to rethink vulnerability management | Sysdigwebpage](#)

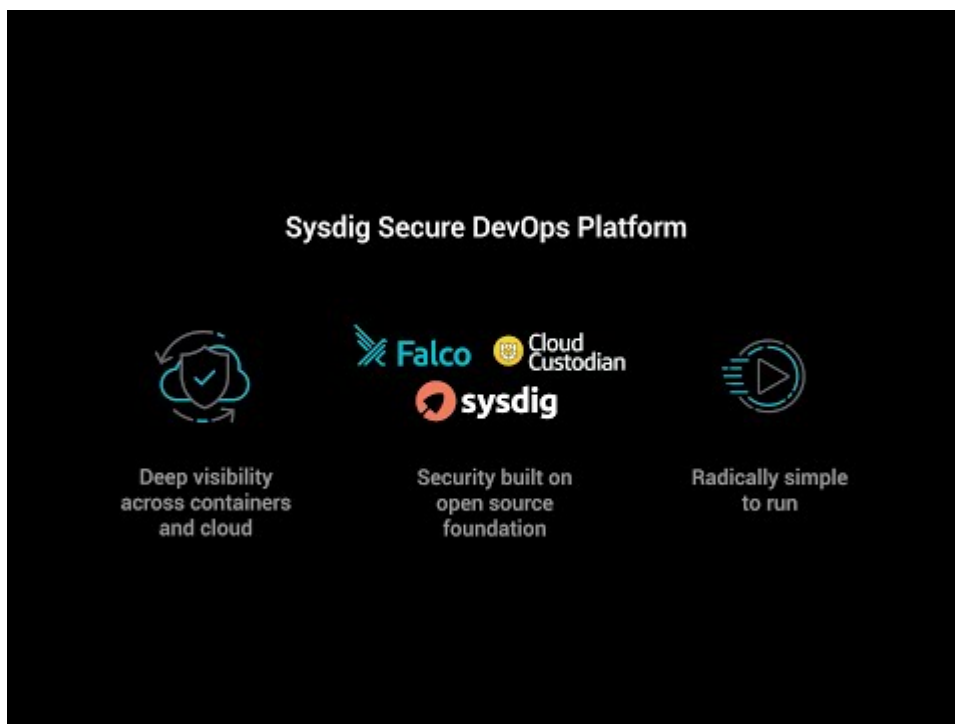


[2025 Gartner® CNAPP Market Guide: Runtime visibility is no longer optional | Sysdig webpage](#)



[EBOOK. Top 6 Use Cases Monitoring Cloud Native Workloads With Sysdig Monitorpdf](#)

[KubernetesSysdig Monitor](#)



[VIDEO. Unified threat detection across containers and cloud with Sysdigvideo](#)

**sysdig** | CUSTOMER STORY Cryptotrading Platform

## Caught in Runtime: How Sysdig Detected Credential Exposure in a Crypto Platform Before It Became a Breach

“Sysdig gave us the real-time visibility we were missing with point-in-time scans. By leaning on runtime security, we caught a risky credential exposure early before it could reach production.”

**Head of Security**  
Cryptotrading Platform

### Summary

After identifying a credential exposure caused by an internal automation job, a major crypto platform saw firsthand the limitations of point-in-time defenses. The incident occurred in a staging environment, where a scheduled privileged access management (PAM) process inadvertently exposed a database password in a shell script. When the update tool was deployed to production, Sysdig's out-of-the-box runtime policies surfaced the behavior in real-time, allowing the team to trace it back to a trusted internal process. Within minutes, they rotated credentials and removed sensitive event data.

The experience reshaped their security strategy. The organization began leaning more heavily on runtime insights, accelerating its response workflow, and deepening collaboration between security and engineering teams. Runtime visibility is now a cornerstone of their defense-in-depth strategy.

### Key Results

- Rapid detection of exposed credentials via runtime alert
- Credential rotation and remediation completed within 30 hours
- No data loss, no customer impact, and improved policy enforcement

**Cryptotrading Platform**  
Cloud-based platform for secure, high-speed cryptocurrency trading.

**HEADQUARTERS**  
Global

**INDUSTRY**  
Financial Technology

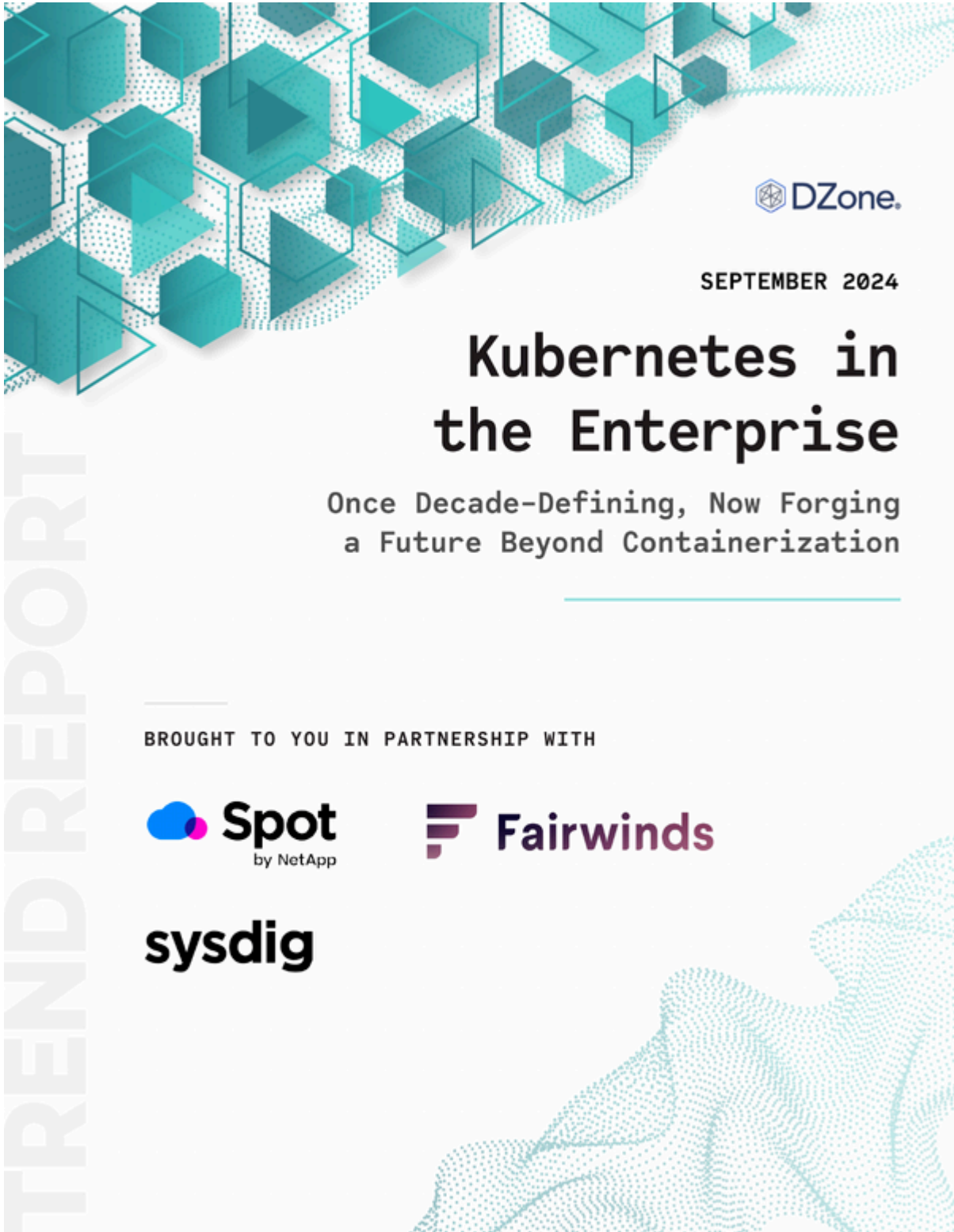
[CASE STUDY. Cryptotrading Platformpdf](#)

[Regulatory Compliance](#)

[The vision comes to life: Agentic cloud security with Sysdig Sage™ | Sysdigwebpage](#)



[BRIEF. On-premises and private cloud securitypdf](#)



 DZone.

SEPTEMBER 2024

# Kubernetes in the Enterprise

Once Decade-Defining, Now Forging  
a Future Beyond Containerization

BROUGHT TO YOU IN PARTNERSHIP WITH



[REPORT. DZone Kubernetes in the Enterprise Trend Report 2024pdf](#)

[KubernetesSoftware development](#)

**sysdig** | **Retail Tech Company**

### Holiday Season Breach Attempt. No Impact. No Downtime.

**3x** Faster Detection  
**Zero** Downtime  
**880%** Faster Onboarding

**Summary**

During the high-pressure season of the holiday season, a security breach attempt hit a retail tech company. The retail tech company's security team was alerted to the breach attempt by Sysdig's AI-powered security engine. The security team was able to identify the breach attempt and investigate the root cause of the breach attempt. The security team was able to identify the breach attempt and investigate the root cause of the breach attempt. The security team was able to identify the breach attempt and investigate the root cause of the breach attempt.

**Key Results**

- Conducted a security audit and implemented security measures
- Implemented a security patch across the company
- Implemented a security patch across the company

**Retail Tech Company**  
Leading security management platform for retail tech companies and retail brands.

—A.L.  
C-Information

[CASE STUDY. Retail Tech Company.pdf](#)

**sysdig**

## The Grand Atlas of Software Security

What you need at every stage of the pipeline

This infographic illustrates the various security tools and services needed at every stage of the pipeline, from development to production. The pipeline is divided into three main stages: Development, Staging, and Production. Each stage has its own set of security tools and services. The infographic also includes a list of key results and a summary of the overall security strategy.

**Development**

- Static Application Security Testing (SAST)
- Software Composition Analysis (SCA)
- Container Security
- Infrastructure as Code (IaC) Security

**Staging**

- Dynamic Application Security Testing (DAST)
- Penetration Testing
- Vulnerability Assessment

**Production**

- Intrusion Detection and Prevention (IDP)
- Security Information and Event Management (SIEM)
- Cloud Security
- Incident Response

**Key Results**

- Reduced security incidents by 50%
- Improved security posture across the organization
- Increased security awareness among developers

**Summary**

Security is a continuous process that requires a multi-layered approach. By implementing the right security tools and services at every stage of the pipeline, organizations can reduce the risk of security incidents and improve their overall security posture.

[INFOGRAPHIC. The Grand Atlas of Software Security.pdf](#)



## 2019 Container Usage Snapshot

Five-minute container life highlights the need for specific security controls

Enterprises are adapting to cloud-native architectures. As a result, usage patterns, processes, and organizational structures are changing.

We've collected insights from real-time, real-world usage of over 2 million running containers to shed light on the current state of infrastructure, applications, security, and compliance practices.

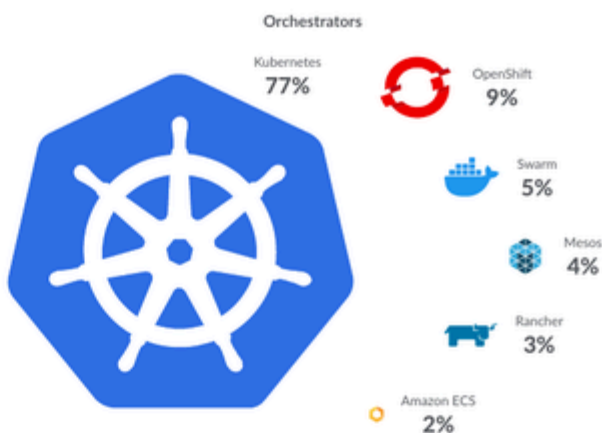


### Orchestration

#### Kubernetes Dominates

Kubernetes takes a whopping 77% share of orchestrators in-use. That number expands to 89% when you add in Red Hat OpenShift and Rancher - both built with Kubernetes.

The results change significantly when looking at on-prem deployments. [Read the full report to see how.](#)

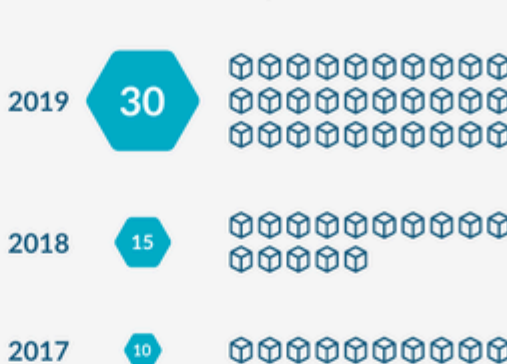


### Container Density

#### Containers-Per-Host Density Increases 100%

The median number of containers per host doubled to 30 in the past year. More apps and more compute power = more containers.

#### Median Containers per Host



### Lifespan

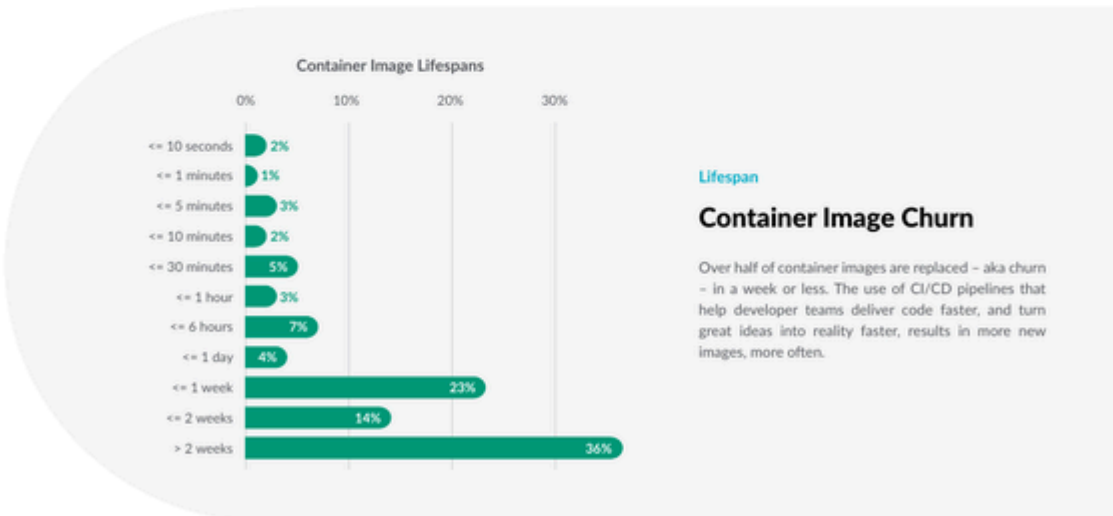
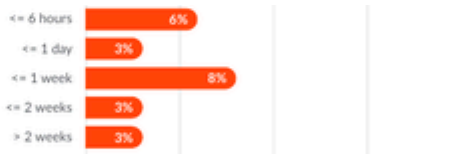
#### The Short Life of Containers

Yes, containers are ephemeral. Surprisingly, over half of containers are alive for less than five minutes. The number of containers alive for 10 seconds or less has

#### Container Lifespans



doubled since 2018 to 22%. The growth of batch processing and serverless frameworks on Kubernetes is likely responsible for the shift.



**Security**

### Public vs. Private Images

With more containers and more churn, new security tools and processes are needed to keep up. We found that 40% of images are pulled from public sources. The risk? Few are checked for security vulnerabilities. Docker Hub, for example, certifies less than 1% of its nearly 3 million hosted images.

Images Pulled from Public vs. Private Registries



Scanning Results  
Median of Containers Scanned



**Security**

### Image Scanning

To prevent vulnerabilities in production requires image scanning. Pass and fail rates for images scanned over a five-day period reveal that over half of images have known vulnerabilities with a severity of high or greater.

“We need to check configurations and validate that our images are free of vulnerabilities before pushing to production.”  
- Global Travel Company



## Top Runtime Threats

Runtime security detects anomalous behavior in production as a last layer of defense. Falco, the CNCF open source project contributed by Sysdig, enables runtime policies that detect security violations and generate alerts. Using Sysdig Secure, which automates runtime security with Falco policies, we found that the top security risks encountered include containers that:



Start with too many permissions or attempt to escalate privileges



Spawn a shell or exhibit command activity from an attached terminal

“With security events, the frontline is our developer team. They know what their applications should and should not be doing.”

- Director of Engineering at a Global Travel Company

“Troubleshooting, forensics, and audit can be handled at scale when you have a single source of truth across the teams.”

- VP of Engineering at a Top 5 Investment Bank

21

containers that run as root



4

containers that run in privileged mode



### Compliance

## Container Compliance Issues

To reduce risk and meet compliance standards including PCI-DSS, HIPAA, and GDPR, organizations should regularly check hosts and containers against a set of best practices. Audits performed using the CIS benchmark for Docker reveal room for improvement. For example, we found that on the median, container hosts have 21 containers that run as root and 4 containers that run in privileged mode.

### Services

## Top 10 Open Source Containers

Open source powers innovation across infrastructure and applications. Here are the top 10 open source technologies deployed.



Prometheus JMX StatsD



### Custom metrics

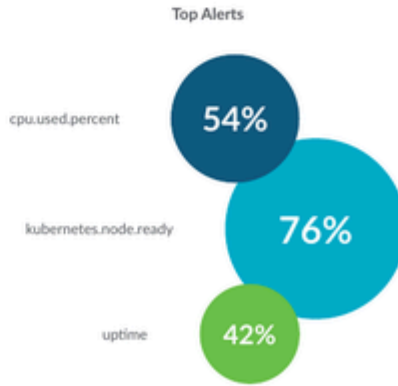
## Prometheus Rises

Custom metrics solutions are a popular way to monitor applications in production clouds. Prometheus metric use increased 130% y/y – up from 20%. Alternatives like JMX metrics (for Java apps) and StatsD are diminishing, down 45% and 17% respectively.

### Alerts

## Top Alert Conditions

Alerts showcase what users see as most disruptive. The most commonly used alert conditions have shifted in favor of Kubernetes infrastructure while continuing to focus on resource utilization and uptime. Of more than 800 unique alert conditions used across Sysdig customers, here are the top 3:



Learn even more about the dynamics of container usage, security, and compliance in the Sysdig 2019 Container Usage Report.

[GET IT NOW](#)



[2019 Container Usage Snapshotpdf](#)

[Kubernetes](#)



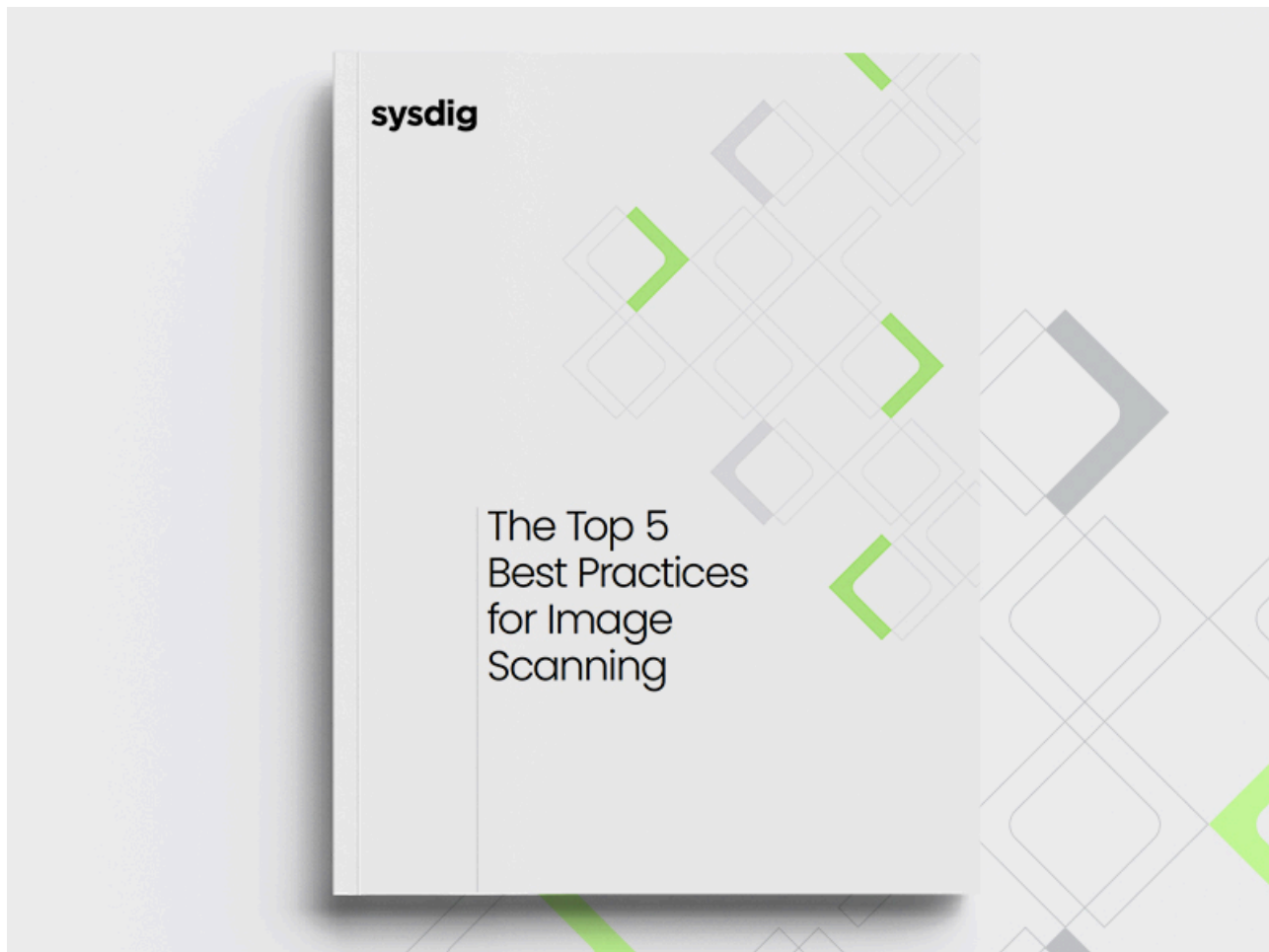
[EBOOK JP. Top 5 Use Cases for Securing Cloud and Containers with Sysdig Securepdf](#)



## **Cybersecurity Strategy Must Include Both Shift-Left and Shield-Right Approaches**

[WHITEPAPER. Cybersecurity Strategy Must Include Both Shift-Left and Shield-Right Approachespdf](#)

[Snyk](#)



[BRIEF. Top 5 Best Practices For Image Scanningpdf](#)



[BRIEF. End-to-End Cloud Security for Amazon Web Servicespdf](#)

[Amazon Web Services](#)

---

Source: [https://sysdig.com/content/c/pf-2023-global-cloud-threat-report?x=u\\_WFRi&xs=524303#page=1](https://sysdig.com/content/c/pf-2023-global-cloud-threat-report?x=u_WFRi&xs=524303#page=1)