# REPORT. 2023 Global Cloud Threat Report

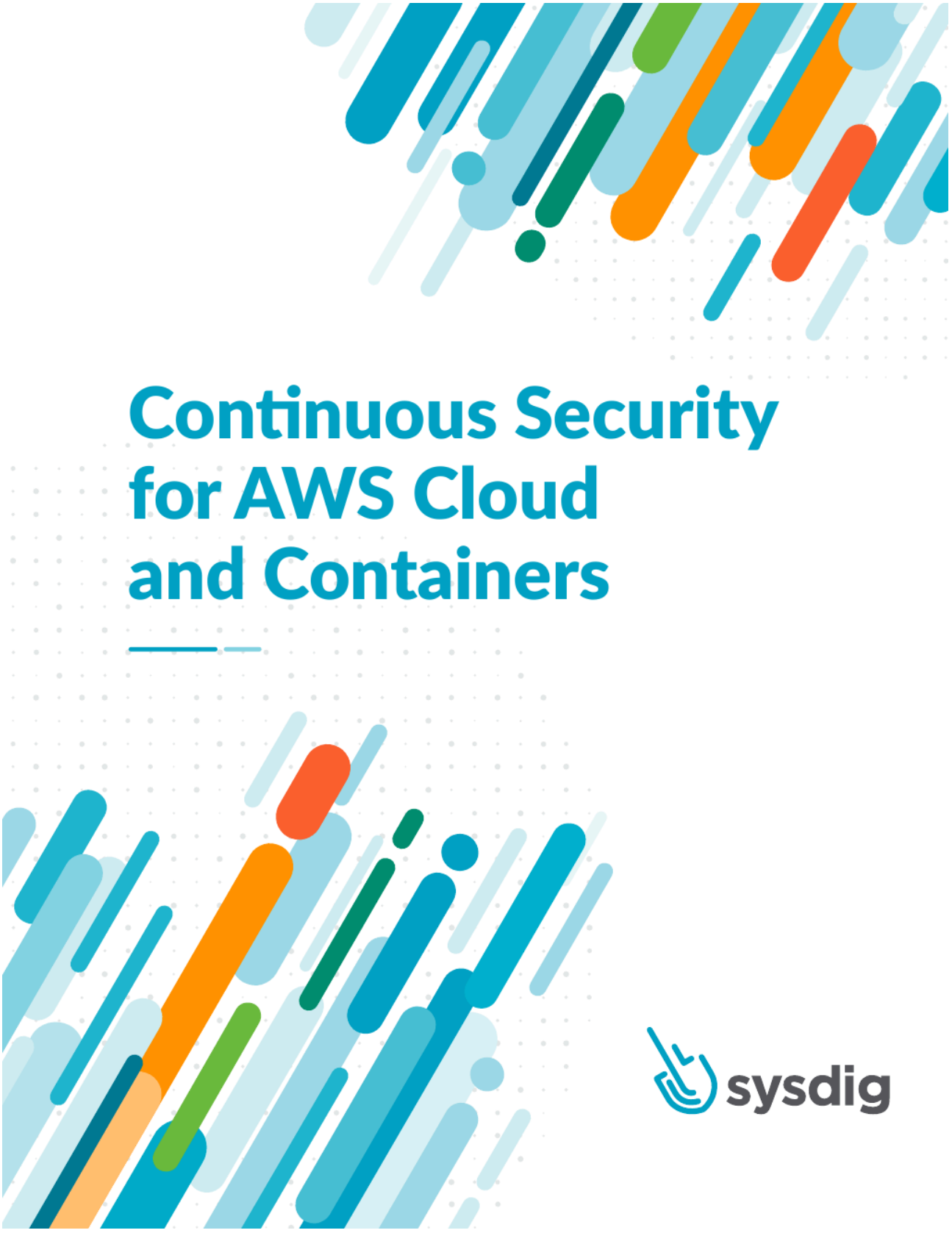
Archived: 2026-05-03 02:27:21 UTC


REPORT. 2023 Global Cloud Threat Reportpdf

AWSAzureCloud SecurityDocker

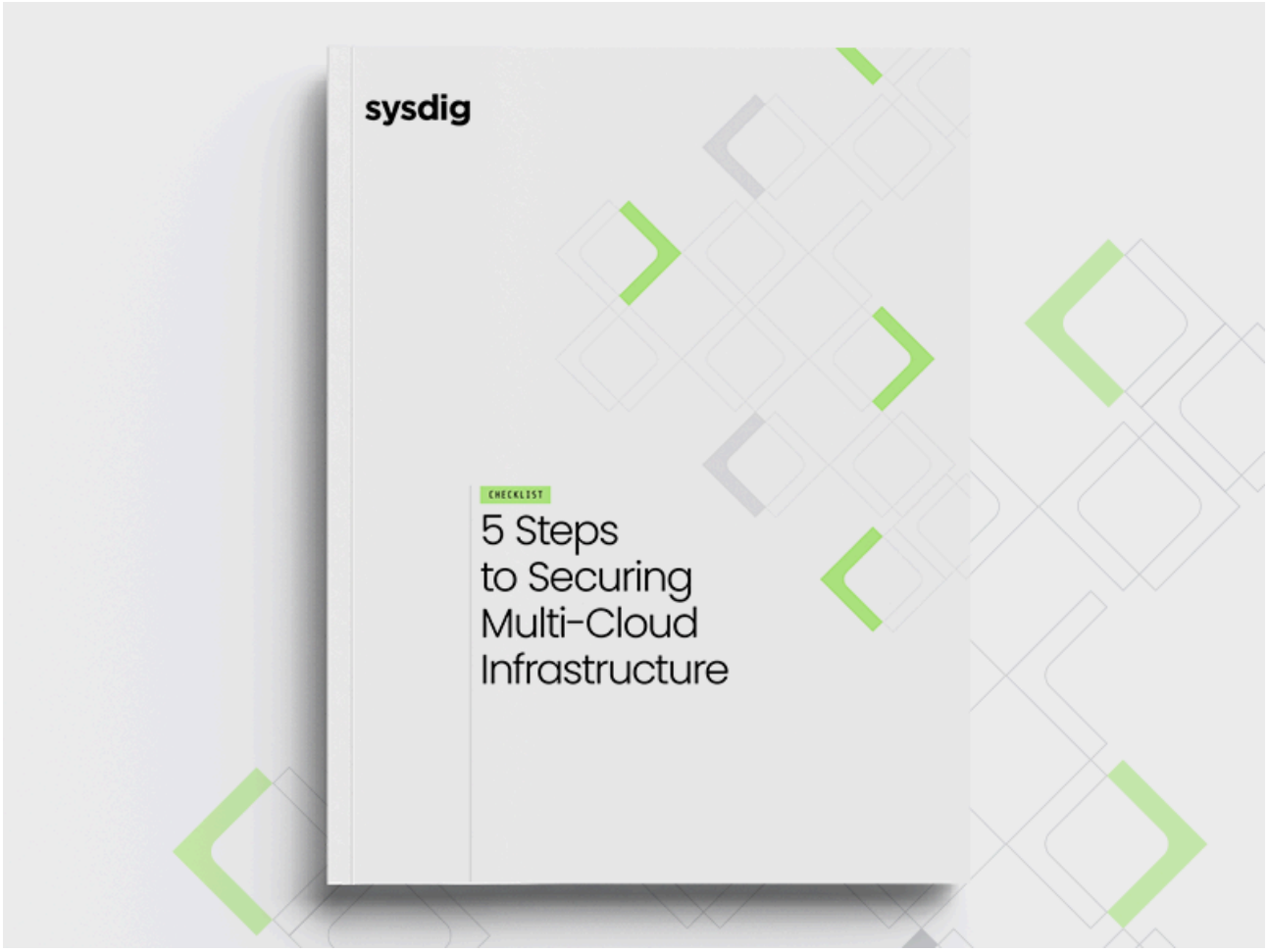

WEBINAR. DevOps Security, Monitoring and Compliance with OpenShift and Sysdigvideo

Cloud SecurityOpenshiftRed HatSysdig Secure




GUIDE. Continuous Security for AWS Cloud and Containerspdf

AWSCloud SecuritySysdig SecureCloud Monitoring




GUIDE. 5 Steps to Securing Multi-Cloud Infrastructurepdf

AWSCloud SecuritySysdig Secure

sysdig

# 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:

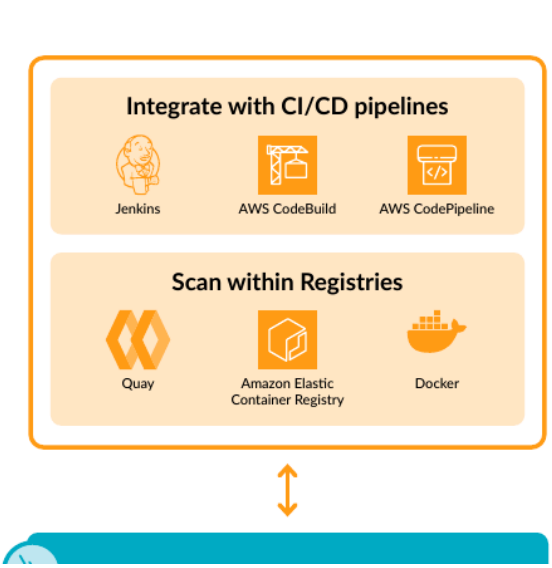
- Secure the build pipeline
- Detect threats at runtime
- Rapidly respond to incidents and conduct forensics investigations
- Continuously validate regulatory compliance

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




**Continuous Compliance**

- Continuously validate compliance with industry standards, like PCI and NIST, for

your AWS environment.

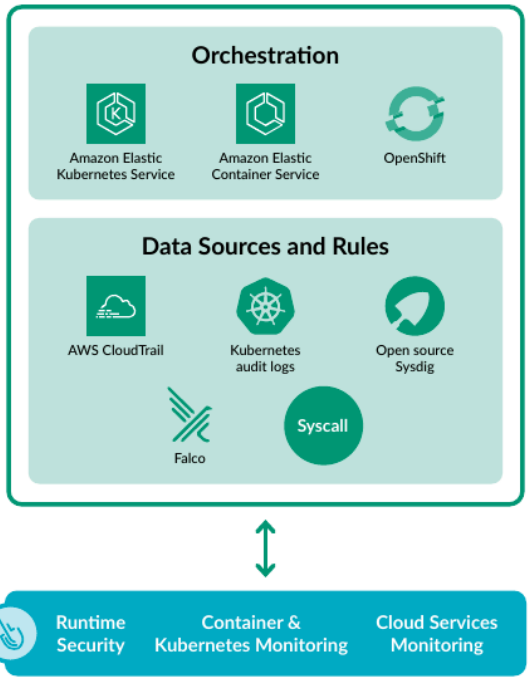

AWS services during build and runtime.

- 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.



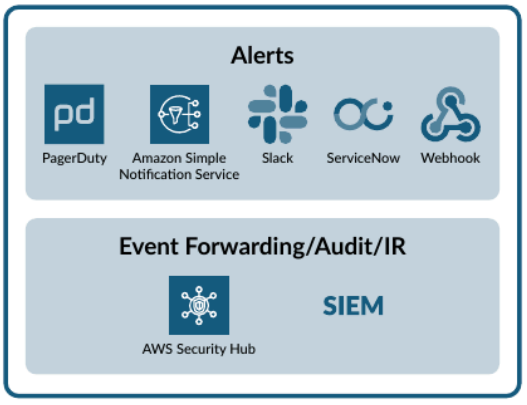




# Respond

## Incident Response and Forensics

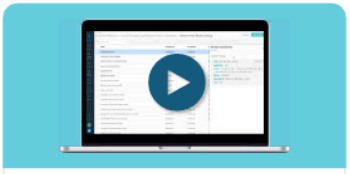
- Quickly understand any security breach using granular, system-level capture data, with Kubernetes and cloud context.
- Correlate system, user, and container activity to determine root cause even after containers are gone.
- Accelerate incident response and recover quickly.




**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

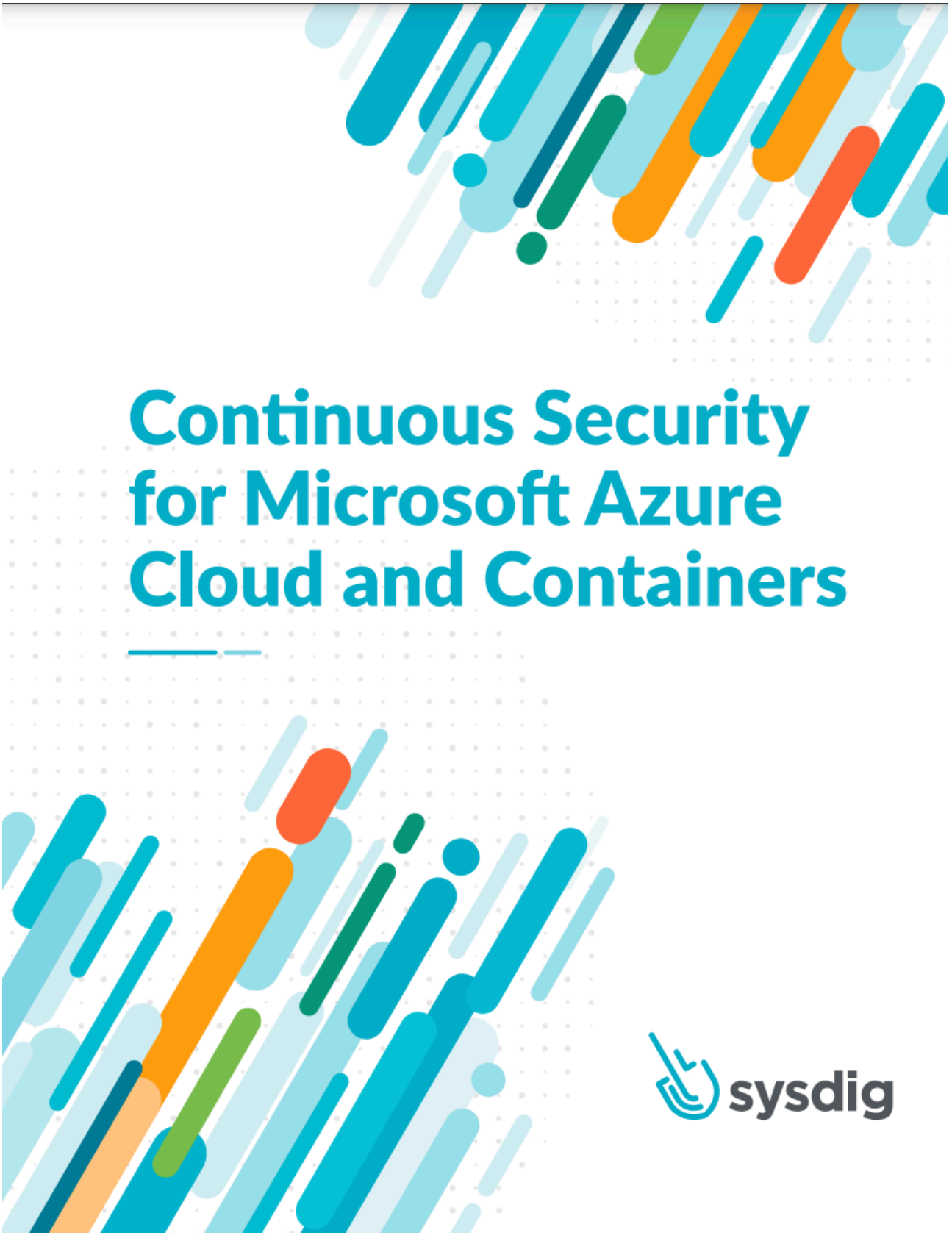
READY TO TRY

ll 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

AWSCloud SecuritySysdig SecureCloud Monitoring




GUIDE. Security And Monitoring On Azure Container Servicespdf

AzureCloud SecuritySysdig SecureCloud Monitoring

sysdig

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)

logdna

## Overview

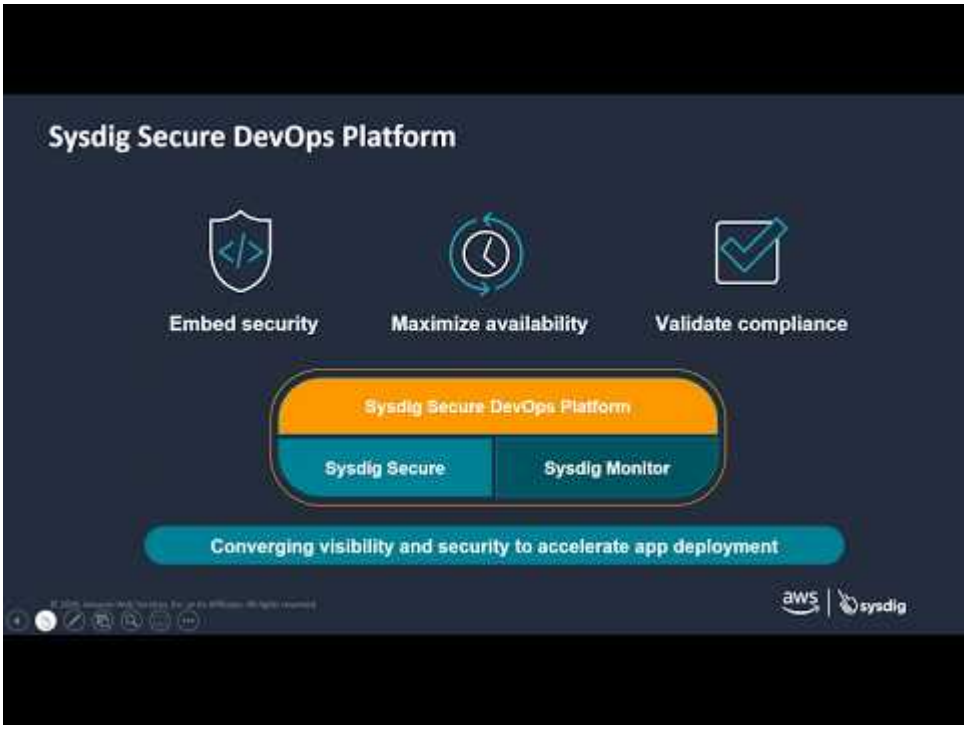
LogDNA is a centralized log management solution that empowers DevOps teams with the tools that they need to develop and debug their applications with ease. They help thousands of companies, from startups to large enterprises, take control of their data and gain valuable insights from their logs.

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 Deliveryvideo

AWSCloud SecuritySysdig Secure


SOLUTION BRIEF. AWS Security Lakepdf

AWSCloud SecuritySysdig Secure


[Cloud Security Powered by Runtime Insightspdf]

[AWSCloud SecuritySysdig Secure]

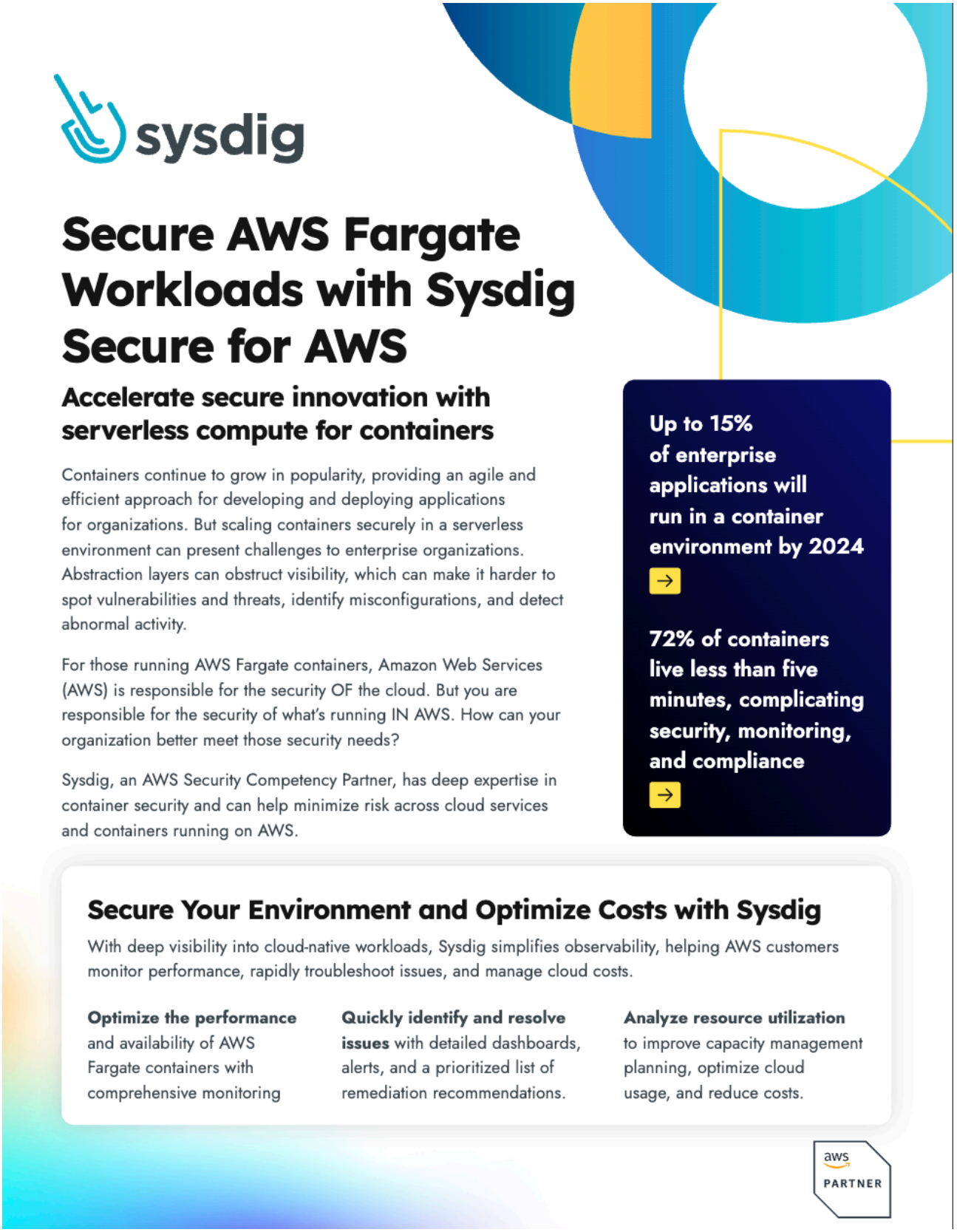
VIDEO. Fargate Scanning In Under 4 Minutesvideo

AWSCloud SecuritySysdig Secure

# How to stay PCI Compliant in a container environment

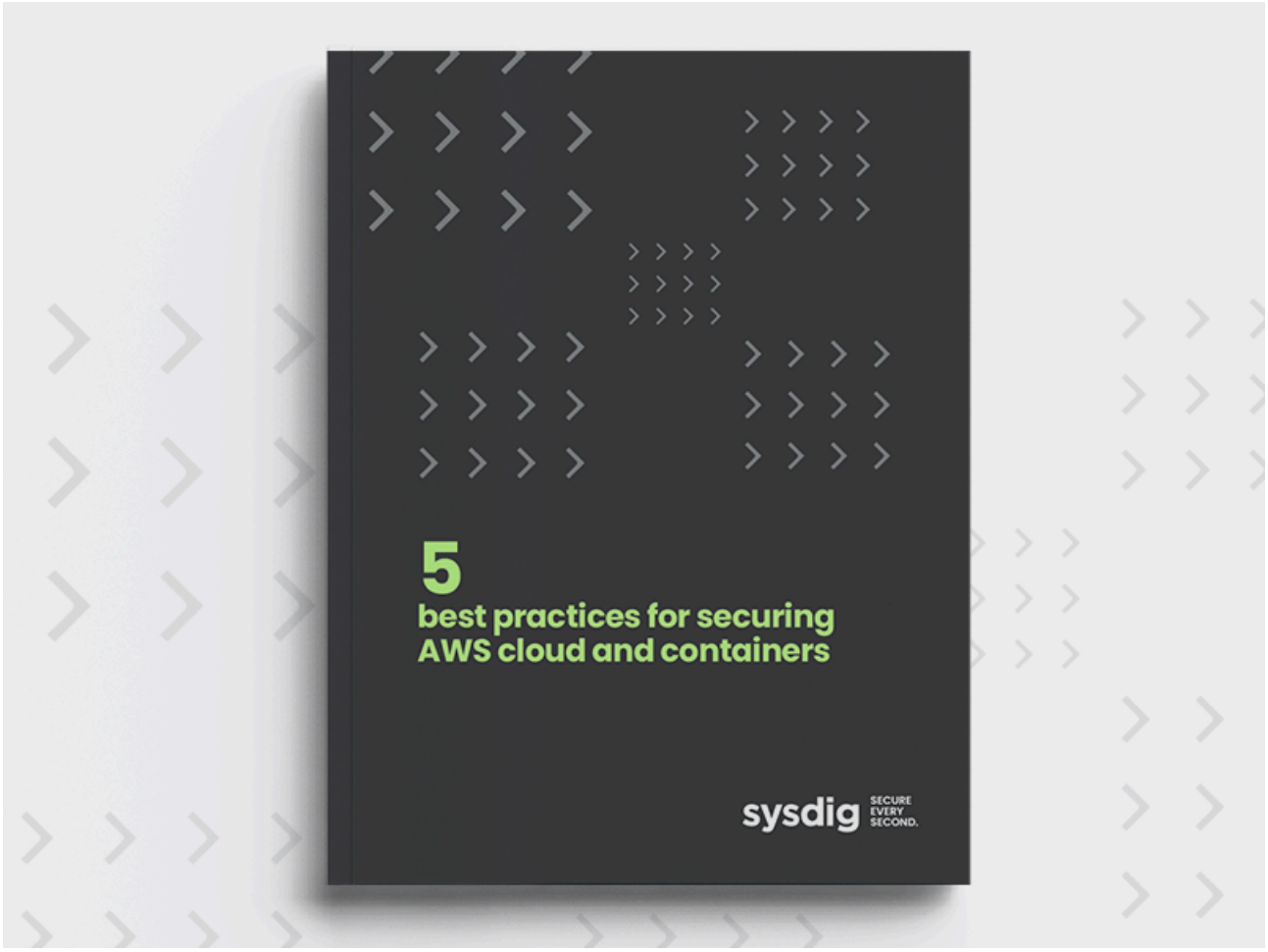
GUIDE. Red Hat + Sysdig PCI Compliance Guidepdf

OpenshiftRed HatSysdig SecureRegulatory Compliance




SOLUTION BRIEF. Sysdig Secure for AWS Fargatepdf

AWSCloud SecuritySysdig 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.

No visibility into the underlying infrastructure

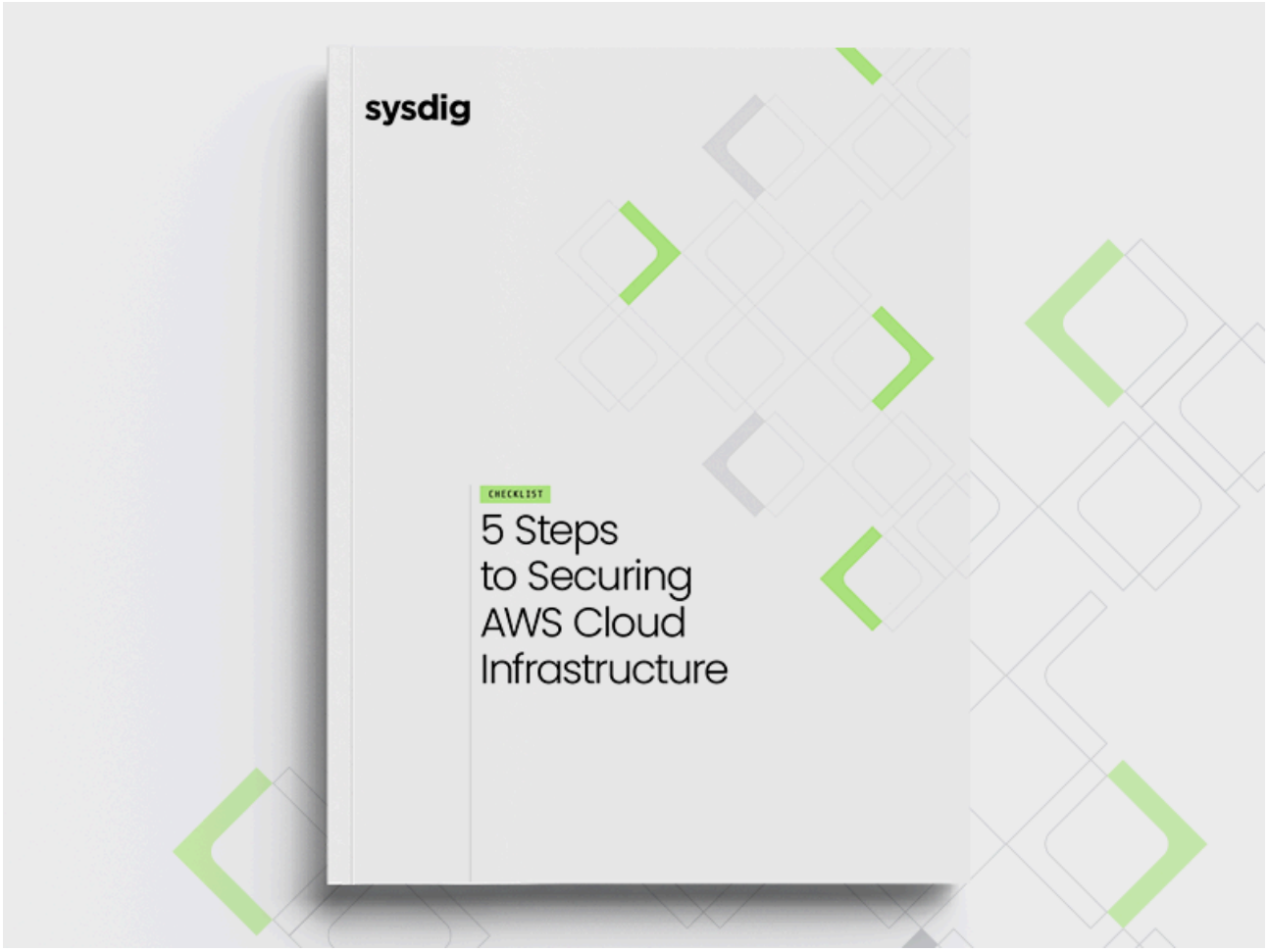
Can't alert on vulnerabilities and threats

Need a detailed record of exactly what happened after the Fargate task is gone

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.

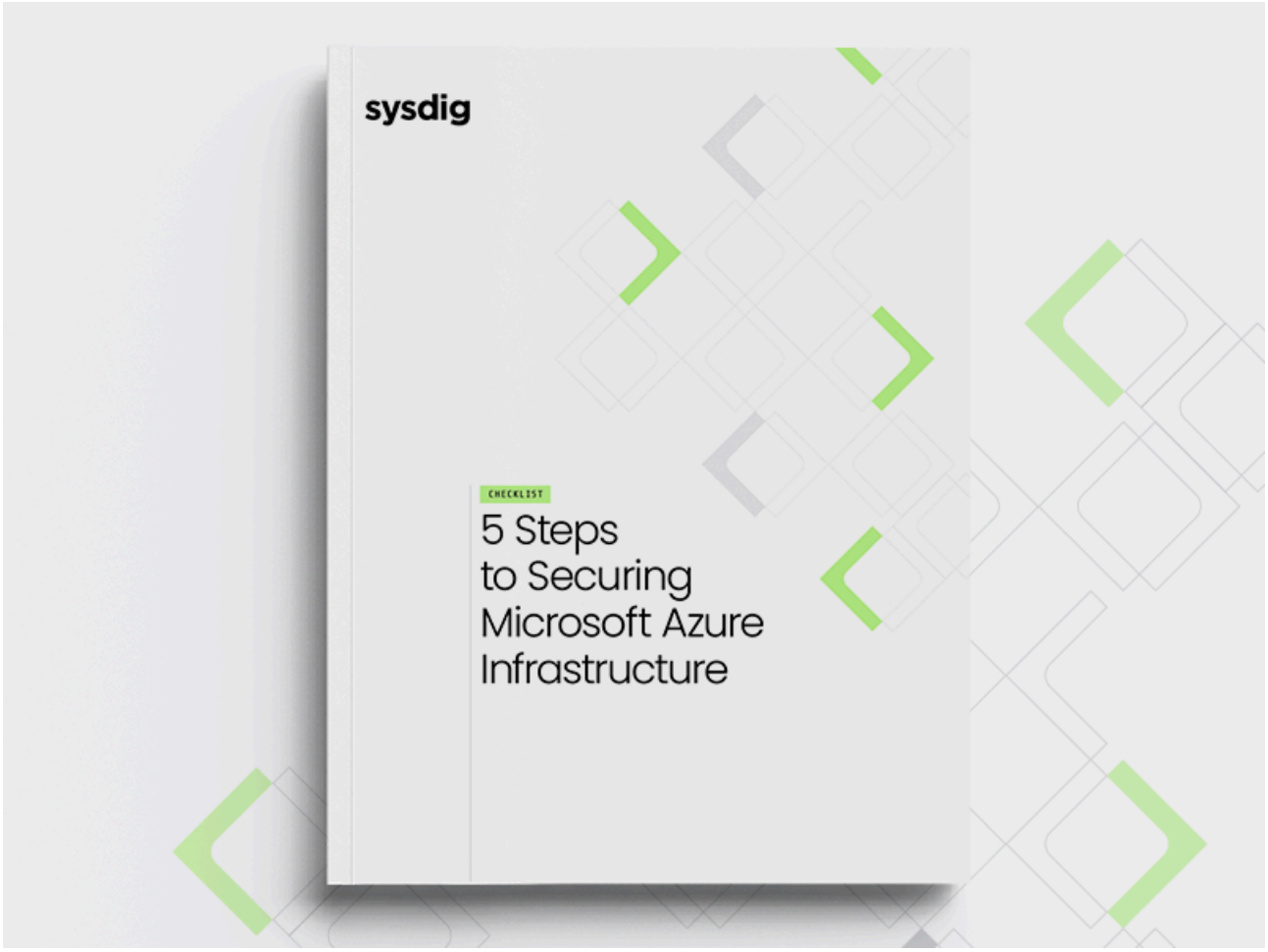
GUIDE. AWS Fargate Checklistpdf

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

Red Hat | sysdig

FinServ Fact Sheet

# 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.

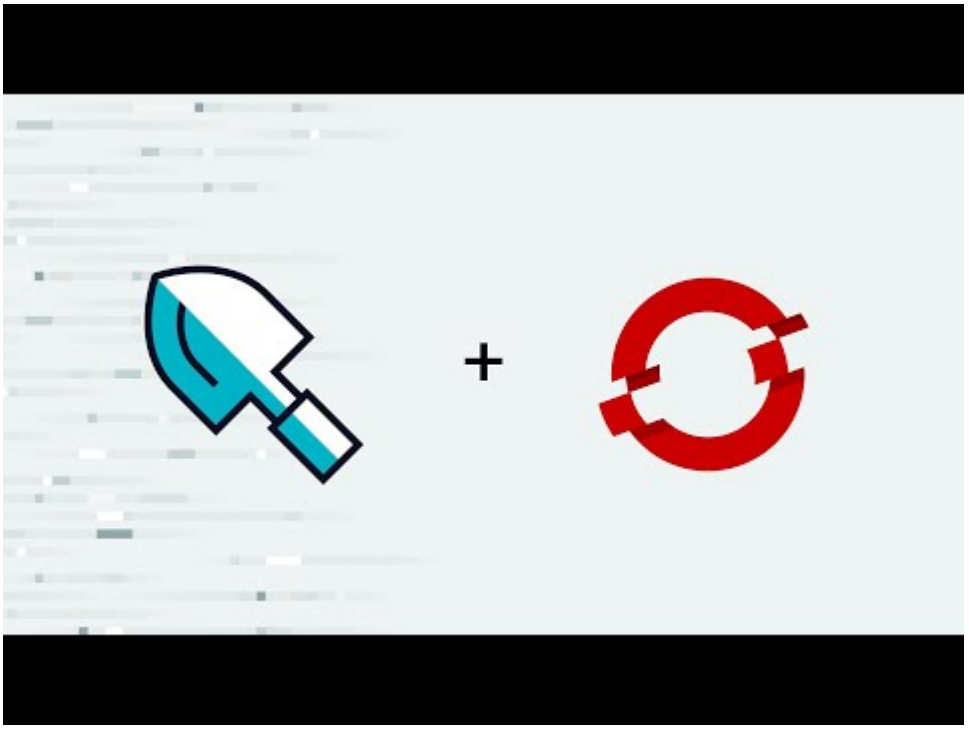
facebook.com/redhatinc
@redhat
linkedin.com/company/red-hat

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 Securevideo

OpenshiftRed HatSysdig Secure


BRIEF. Detect threats in real time with Falco on AWSpdf

AWSCloud SecuritySysdig SecureFalco


VIDEO. Securing and Monitoring AWS Container Servicesvideo

AWSCloud SecuritySysdig SecureCloud Monitoring

GUIDE. Cloud Security for AWSpdf

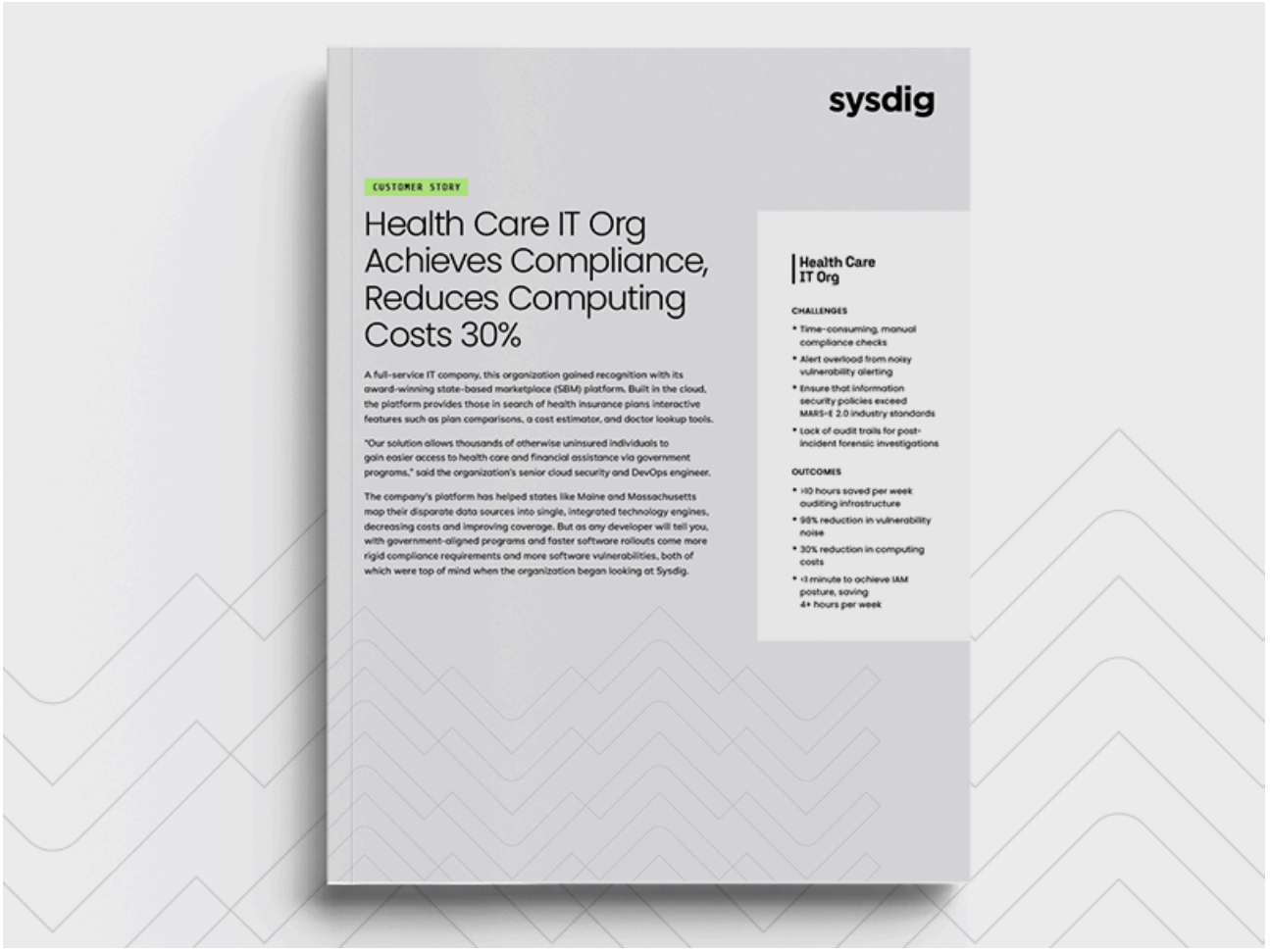
AWSCloud SecuritySysdig SecureCloud Monitoring


VIDEO. ATPCO on deploying Red Hat OpenShift + Sysdig visibility and security platformvideo

OpenshiftRed HatSysdig SecureSysdig Monitor

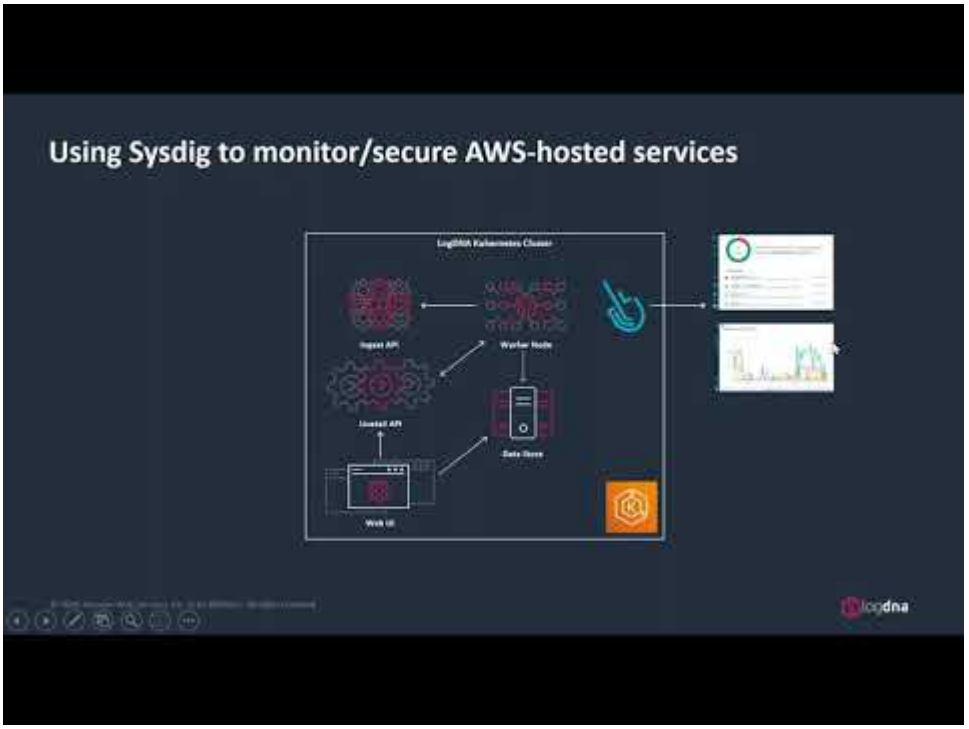

GUIDE. Sysdig AWS Security Lakepdf

AWSCloud SecuritySysdig SecureCloud computing security




[CASE STUDY. Health Care It Orgpdf]

[AWSCloud SecuritySysdig SecureAmazon Web Services]

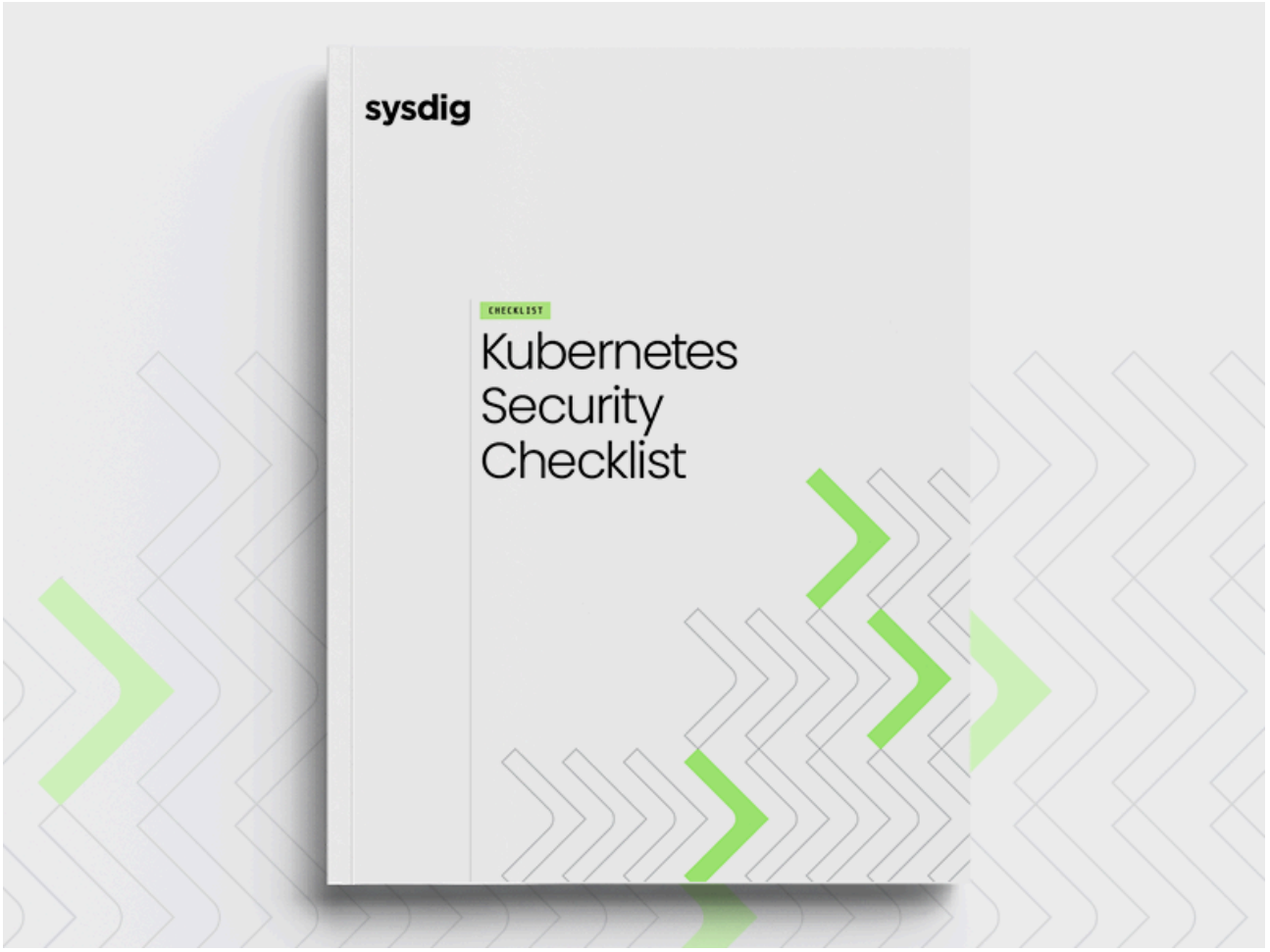


WEBINAR. LogDNA - Monitoring and Securing Containers on AWS EKS with Sysdigvideo

AWSCloud SecuritySysdig SecureCloud Monitoring


WEBINAR. Automating Container Visibility to Accelerate App Deliveryvideo

Cloud SecurityOpenshiftRed HatCloud Monitoring

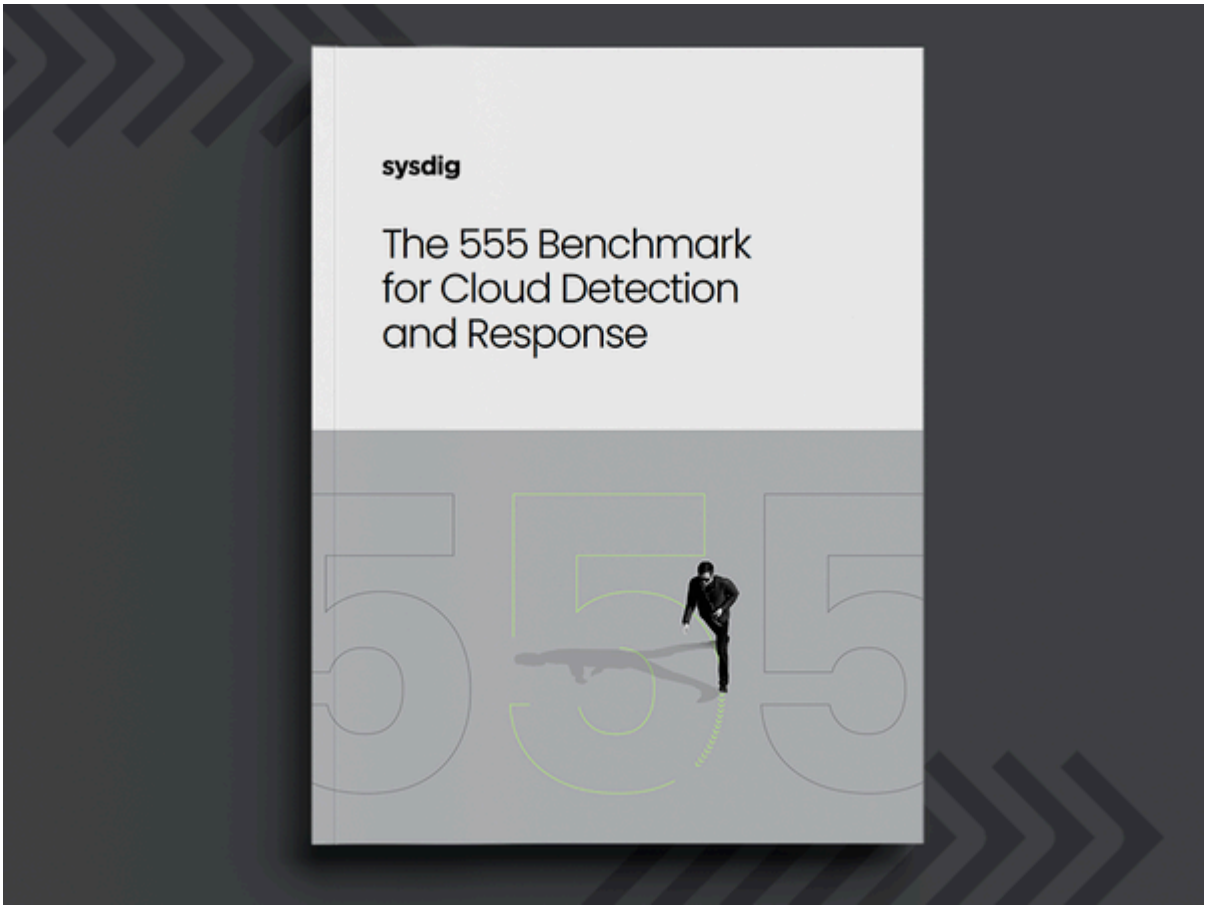



GUIDE. Kubernetes Security Checklistpdf

Cloud SecuritySysdig SecureKubernetes


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

sysdig

# 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

### Security

- **74%** of customers are scanning images during the CI/CD build stage
- **58%** of containers run as root
- **49%** of containers live less than 5 minutes

### Open Source

- **3x** increase in Falco adoption
- **35%** growth of Prometheus metric use
- **4.7x** increase in usage of Go

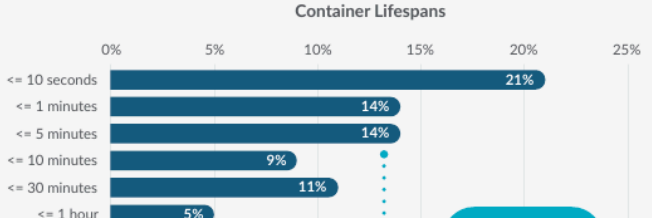
### Container Usage

- **4x** increase in containerd and CRI-O
- **33%** growth in container density
- **60%** increase in Quay.io usage

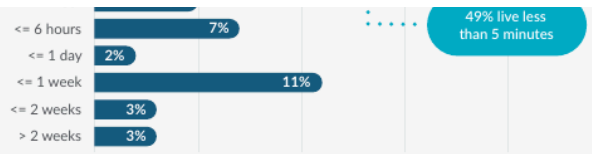
Container Security

## Why Shift Left: The Short Life of Containers

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



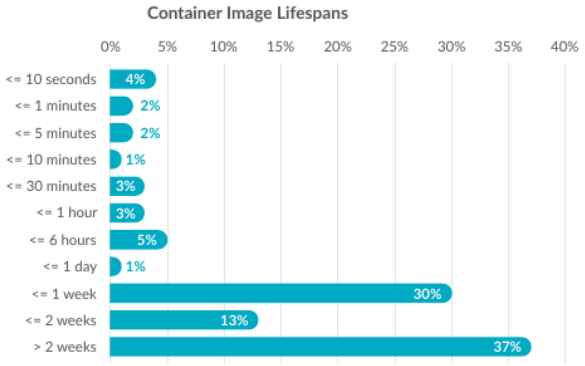
containers continue to be alive for less than five minutes. The ephemeral nature of containers remains one of the technology's unique advantages, but presents new issues to consider for security and compliance.

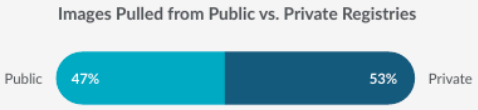



Container Security

## 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 Security

## Public vs. Private Images

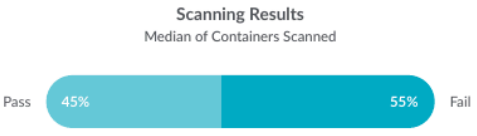
With more containers and more churn, new security tools and processes are needed to keep up. We found that 47% of images are pulled from public sources. The risk? Few are checked for security vulnerabilities. Docker Hub, for example, certifies less than 1% of its nearly three million hosted images.

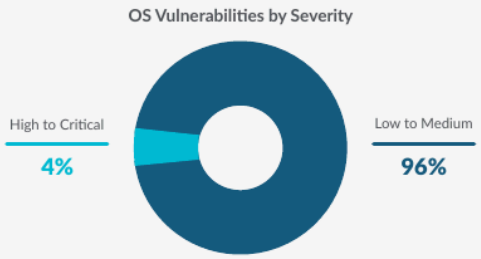
> "A manual image scan could take 10 minutes per check-in. With Sysdig, all of that just becomes automatic as part of the pipelines as the team is doing their deployments. Today, we handle thousands of merges per day. If you consider each could take 10 minutes on average and multiply that by thousands 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.






Container Security

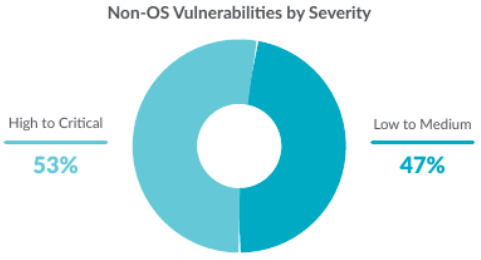
## OS Vulnerability Snapshot

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.





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.

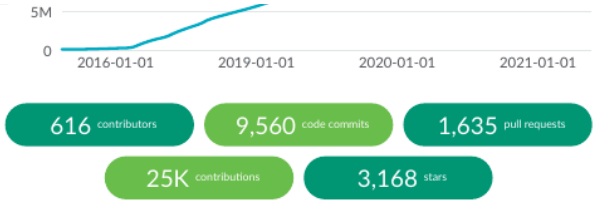
From talking to our customers, in practice, even if risky configurations are detected at build time, teams don't stop containers from moving to production. Instead, they allow a grace period to fix the issue and continuously monitor for suspicious behavior, in order to continue deploying quickly.

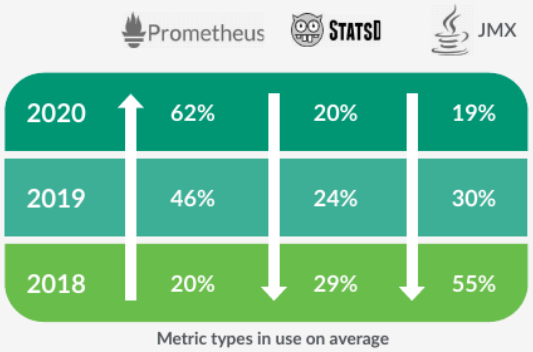
Open Source Software Gains Momentum

## Falco Adoption Grows Over 3X

Runtime security detects anomalous behavior

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

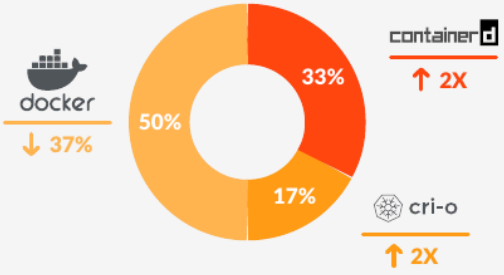
Custom metric solutions give developers and DevOps teams a way to instrument code to collect unique metrics. Of the three mainstay solutions, JMX, StatsD, and Prometheus, Prometheus metric use increased 35% YoY across our customers — with over 60% of our customers using it.

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

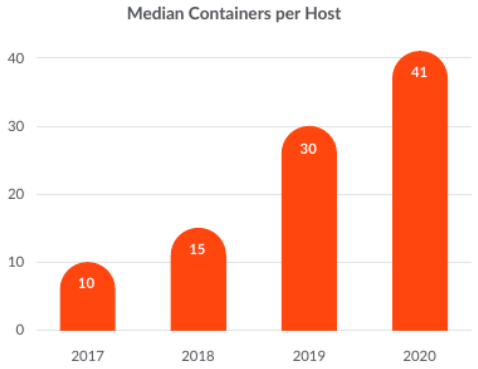
## Container Runtimes: Containerd and CRI-O Usage Grows 4x

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.




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

sysdig

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

INFOGRAPHIC. 2021 Container Security and Usage Snapshotpdf

Cloud SecuritySysdig SecureCloud MonitoringKubernetes


REPORT. 2022 Cloud-Native Security And Usage Reportpdf

Cloud SecuritySysdig SecureCloud MonitoringKubernetes

sysdig

# 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.[1]

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.


[1] 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.

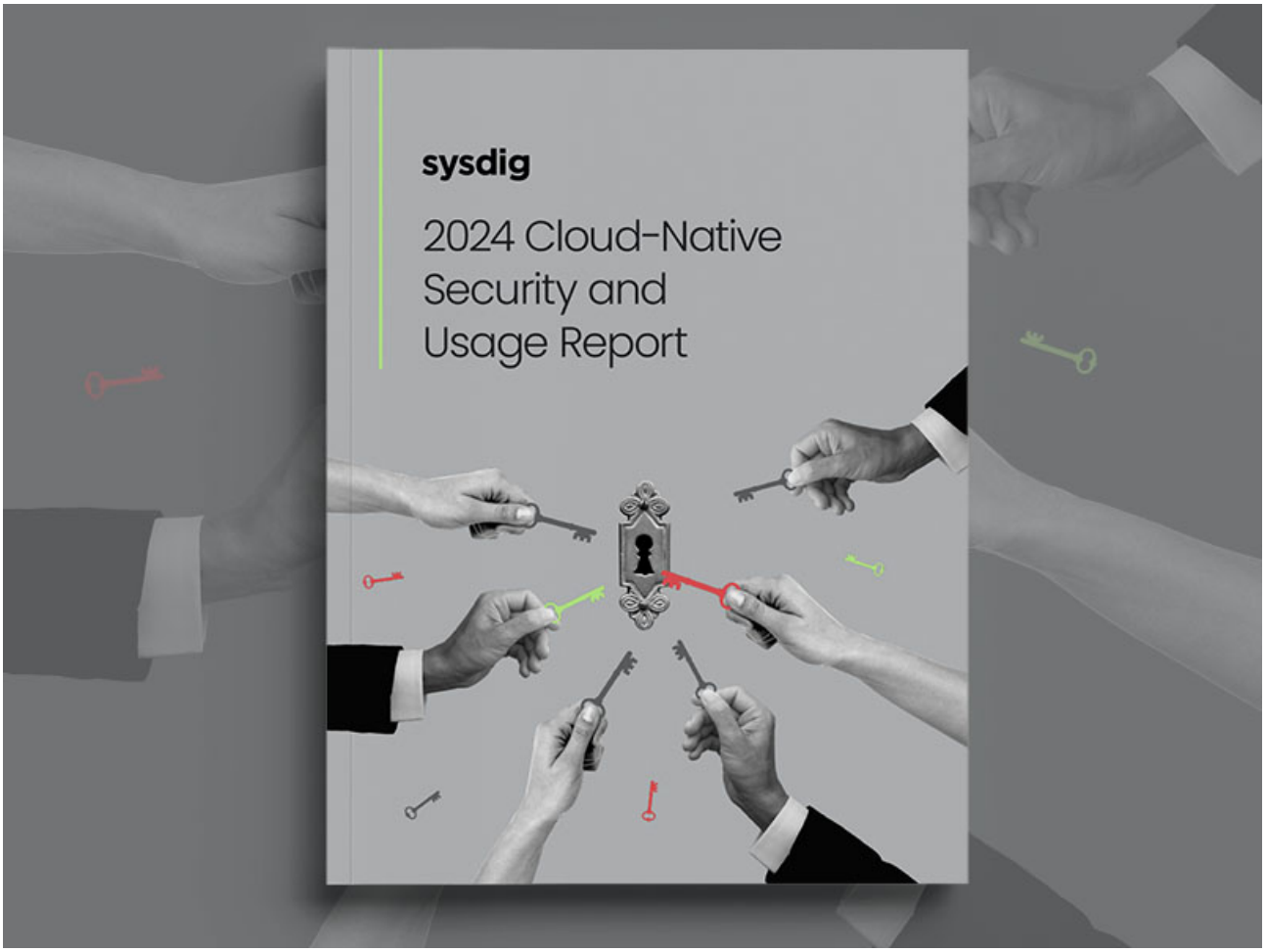
This overview highlights the advantages of SaaS, providing insight into the operational controls and practices of the Sysdig SaaS solution designed to help you securely and efficiently implement cloud-native security and monitoring.

GUIDE. Get the SaaS Advantagepdf

Cloud SecuritySysdig SecureCloud MonitoringKubernetes


BRIEF. 2023 Global Cloud Threat Report Exec Summarypdf

Cloud SecuritySysdig Secure




BRIEF. 2024 Cloud Native Security And Usage Report Exec Summarypdf

Cloud SecuritySysdig 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, or call +1 866-367-7378.



REPORT. Forrester Now Tech Cloud Workload Security Q3 2021pdf

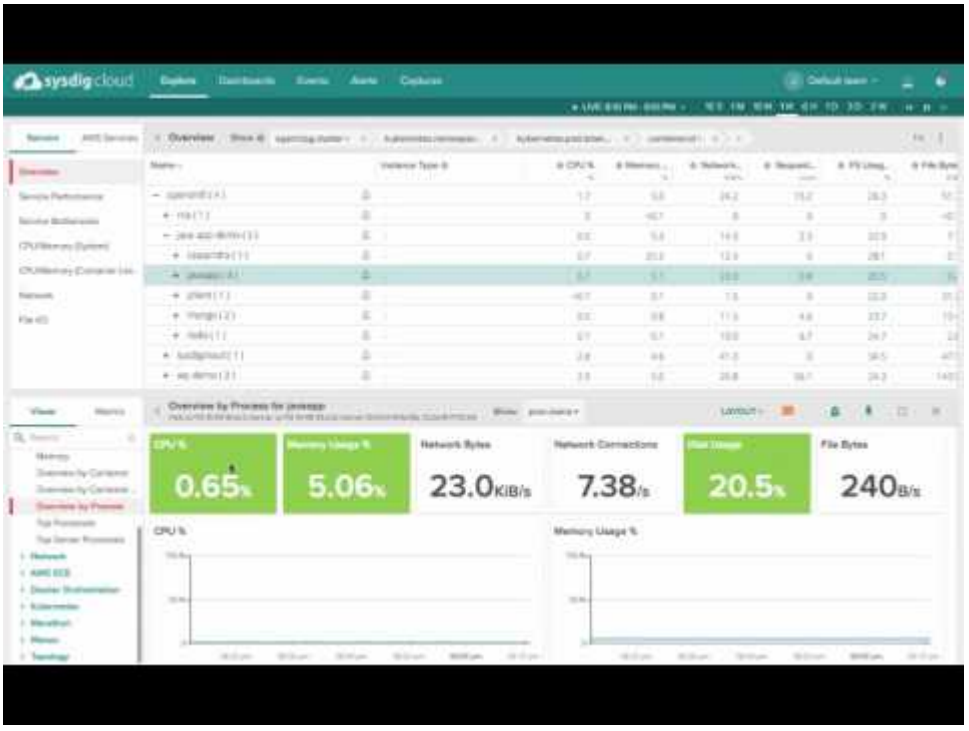
Cloud SecuritySysdig Secure


WEBINAR: Moving Apps to the Cloud? How Top Financials Reduced their Security & Compliance Riskvideo

Cloud SecurityRed HatCloud Monitoring

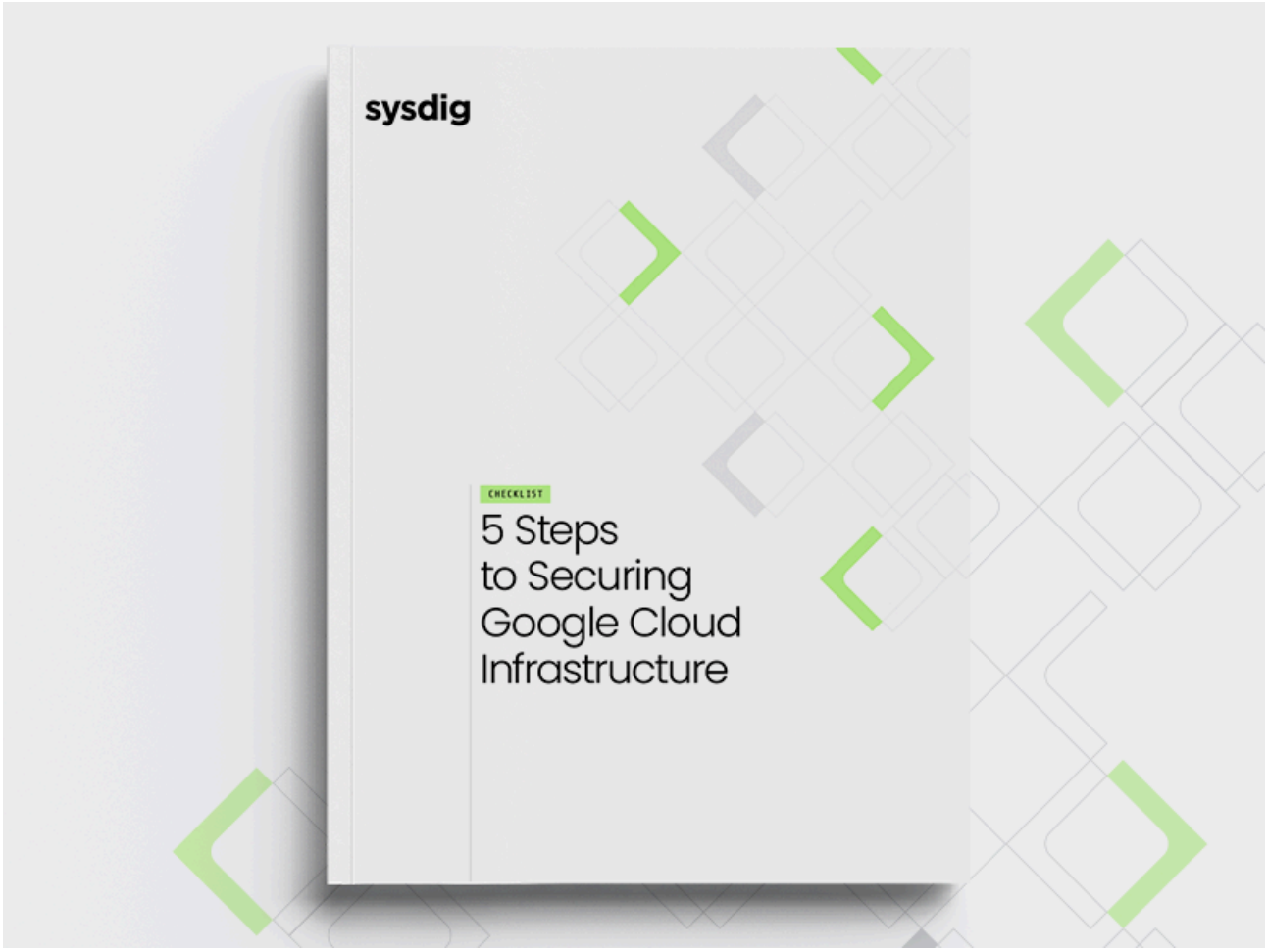

VIDEO NL. Bereid je voor op de volgende log4j!video

Cloud SecuritySysdig Secure




[VIDEO. Openshift Monitoring with Sysdigvideo]

[OpenshiftRed HatSysdig Monitor]

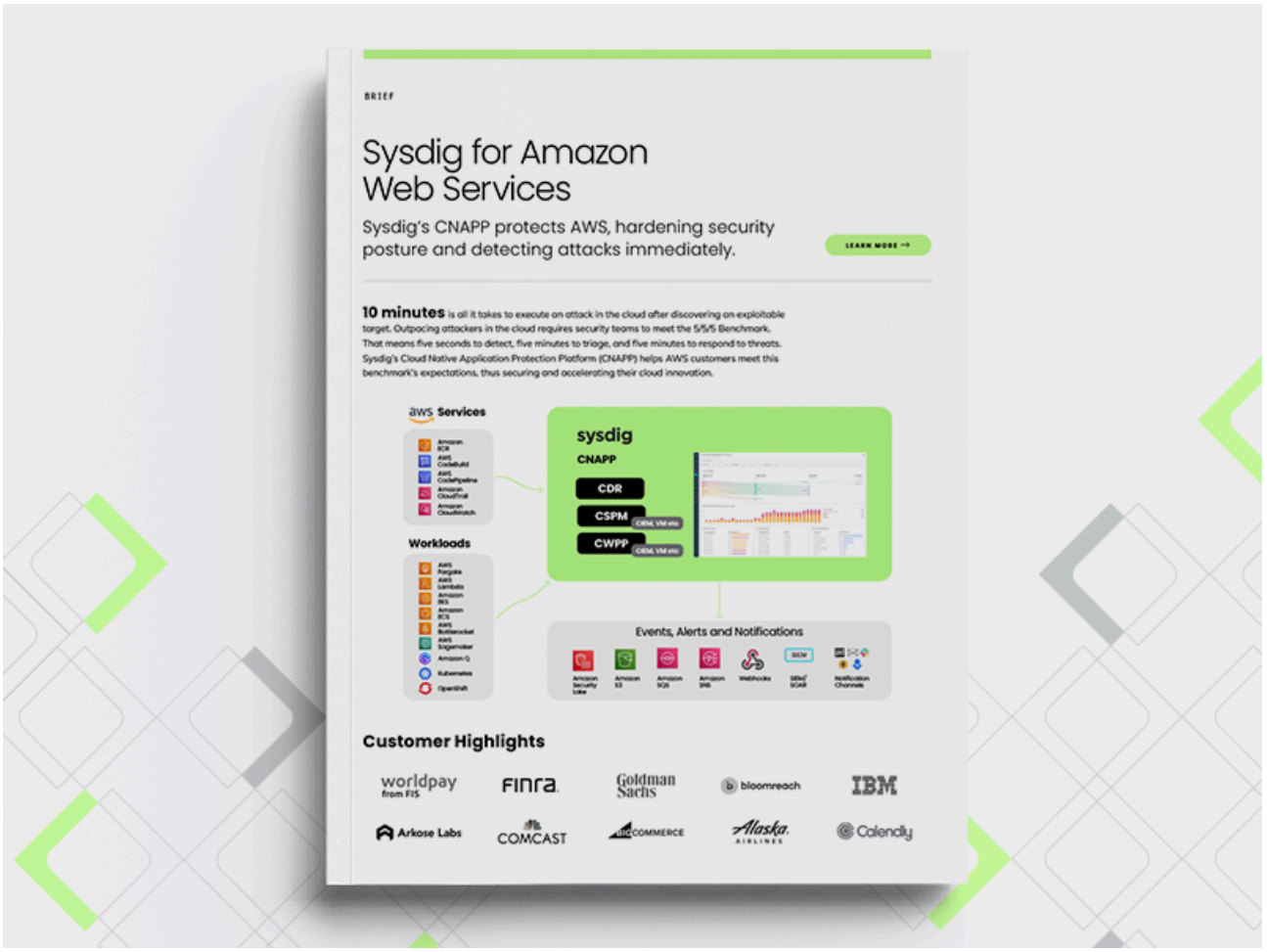


GUIDE. 5 Steps To Securing GCP Cloud Infrastructurepdf

Cloud SecuritySysdig Secure


GUIDE. 5 Best Practices for Securing Cloud and Containers in Financial Servicespdf

Cloud SecuritySysdig Secure

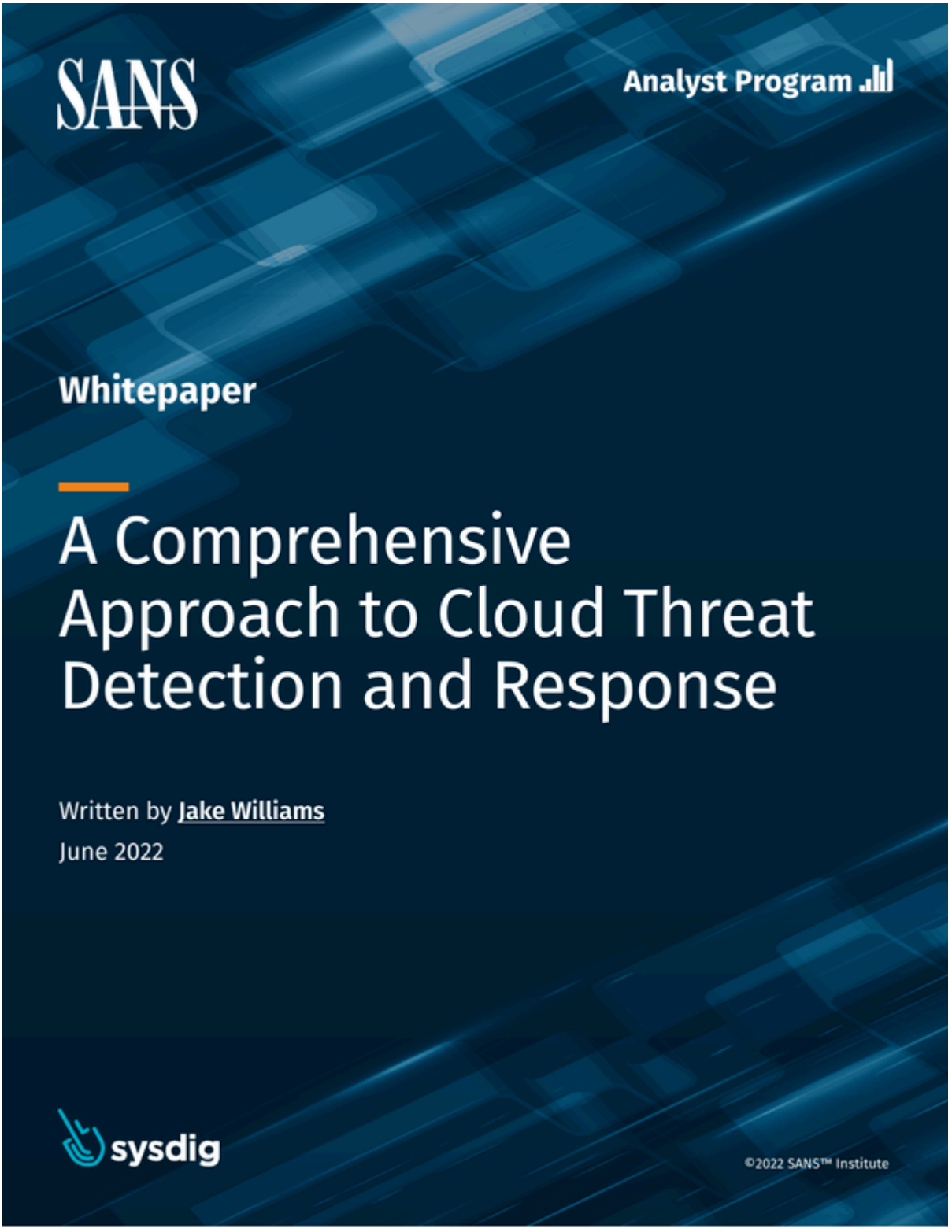



PARTNER BRIEF. Sysdig and Amazon Web Servicespdf

AWSCloud Security


WHITEPAPER: Cybersecurity Regulations Guidancepdf

Cloud SecuritySysdig SecureCloud computing security




WHITEPAPER. A Comprehensive Approach to Cloud threat Detection and Responsepdf

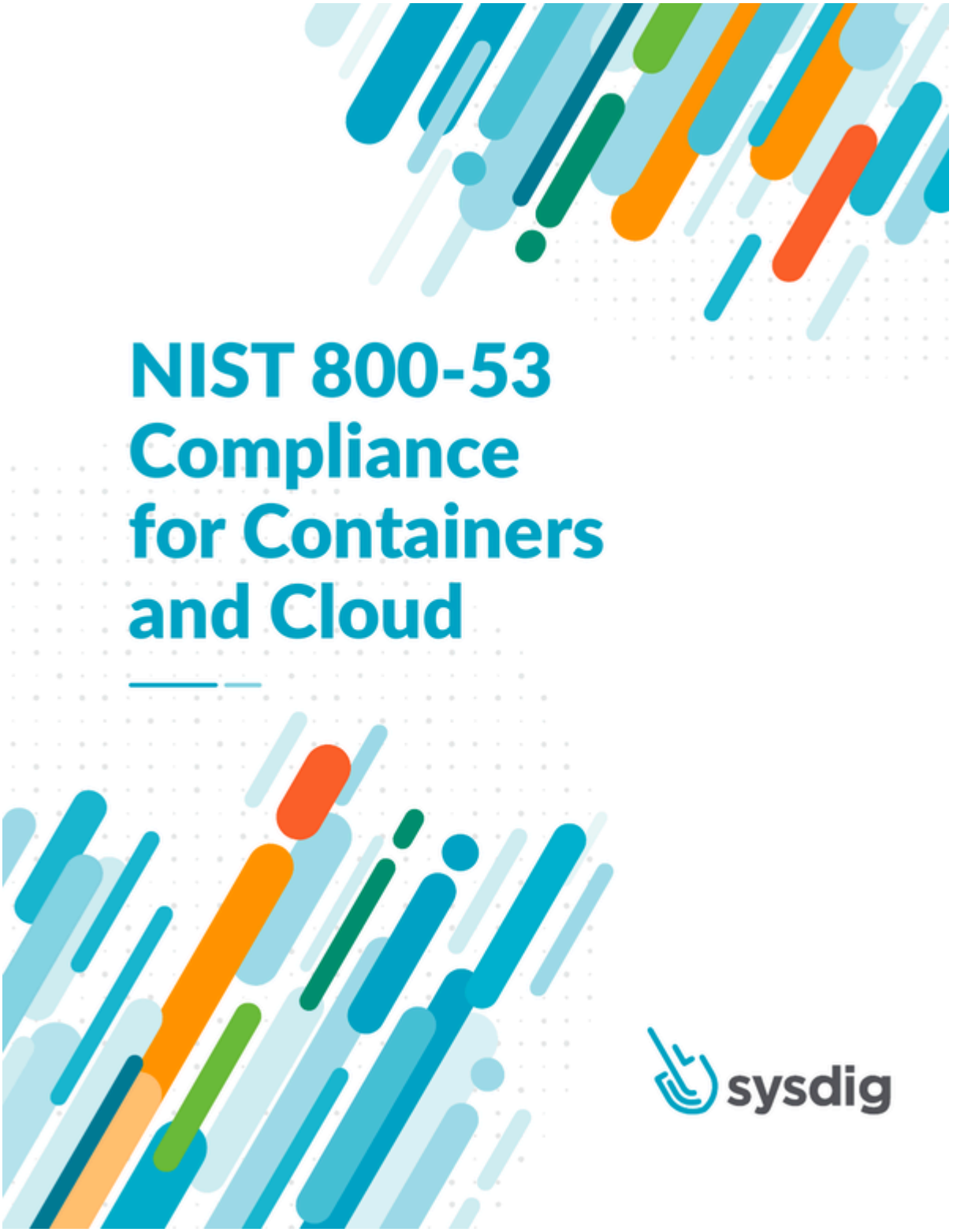
Cloud SecuritySysdig Secure

VIDEO. Sysdig + Red Hat partnership: OpenShift visibility and securityvideo

OpenshiftRed Hat

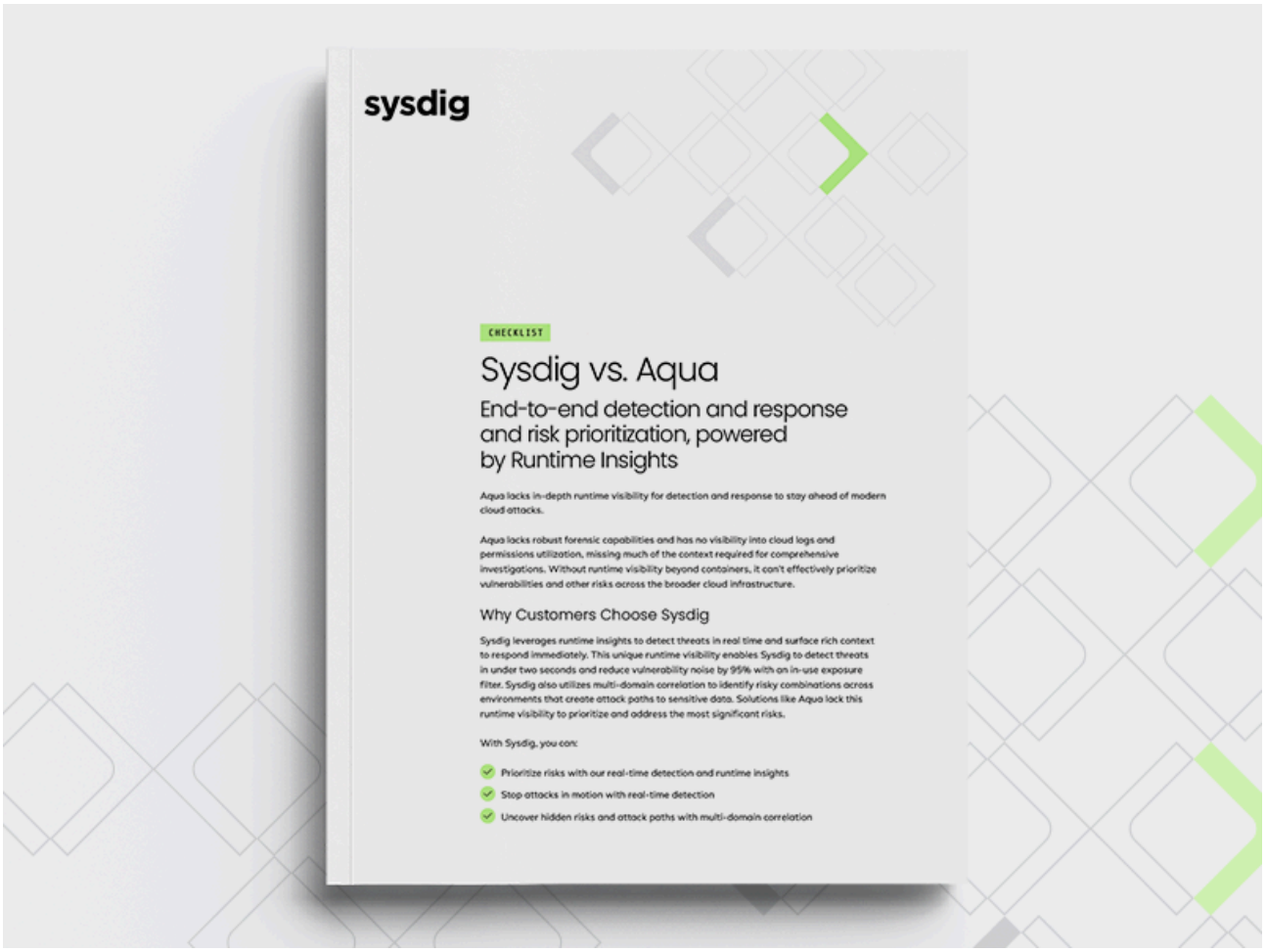

VIDEO. Secure DevOps practices at Yahoo! Japanvideo

Cloud SecuritySysdig SecureKubernetes



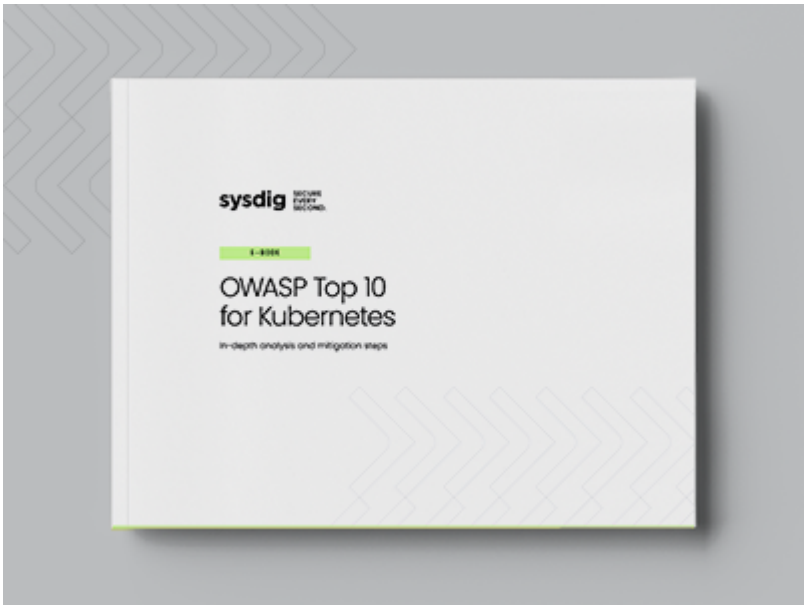

GUIDE. NIST 800-53 Compliance for Containers and Cloudpdf

Cloud SecuritySysdig SecureRegulatory Compliance




GUIDE. Container Security Comparison Checklist: Sysdig vs Aqua Securitypdf

Cloud SecuritySysdig Secure

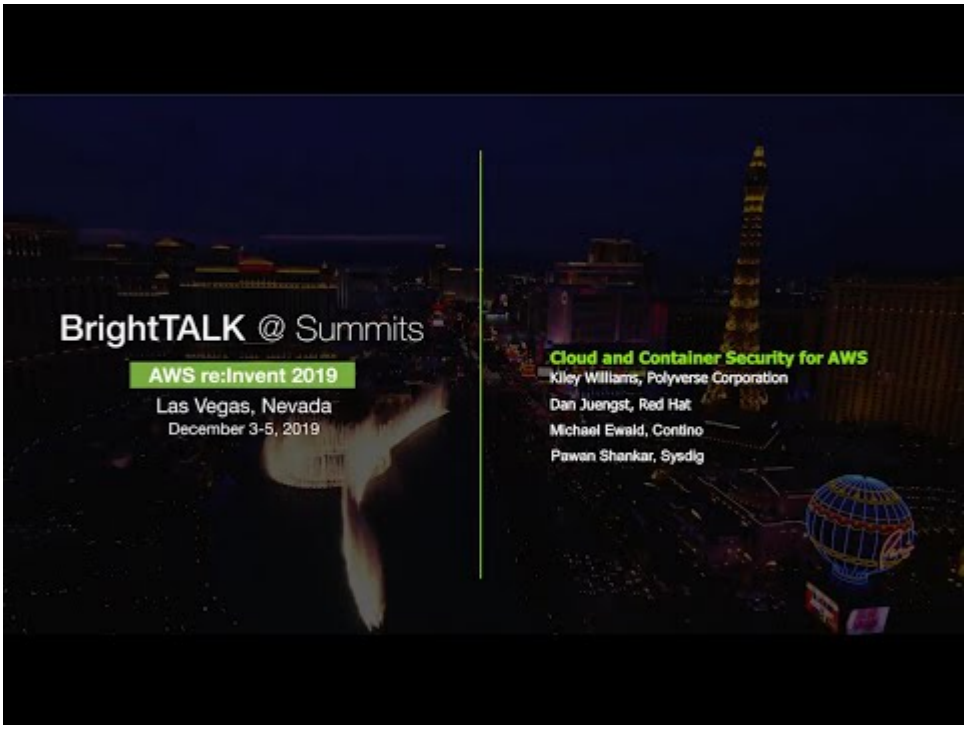



GUIDE. OWASP Kubernetes Top 10: Mitigating Risks in Cloud-Native Environmentspdf

Cloud SecuritySysdig SecureKubernetes


WEBINAR. Automating Security for DevOps Workflowsvideo

Cloud SecuritySysdig Secure




WEBINAR. Cloud and Container Security for AWSvideo

AWSCloud SecurityKubernetes


GUIDE. Container & Cloud Security Comparison Checklist: Sysdig vs CheckPoint CloudGuardpdf

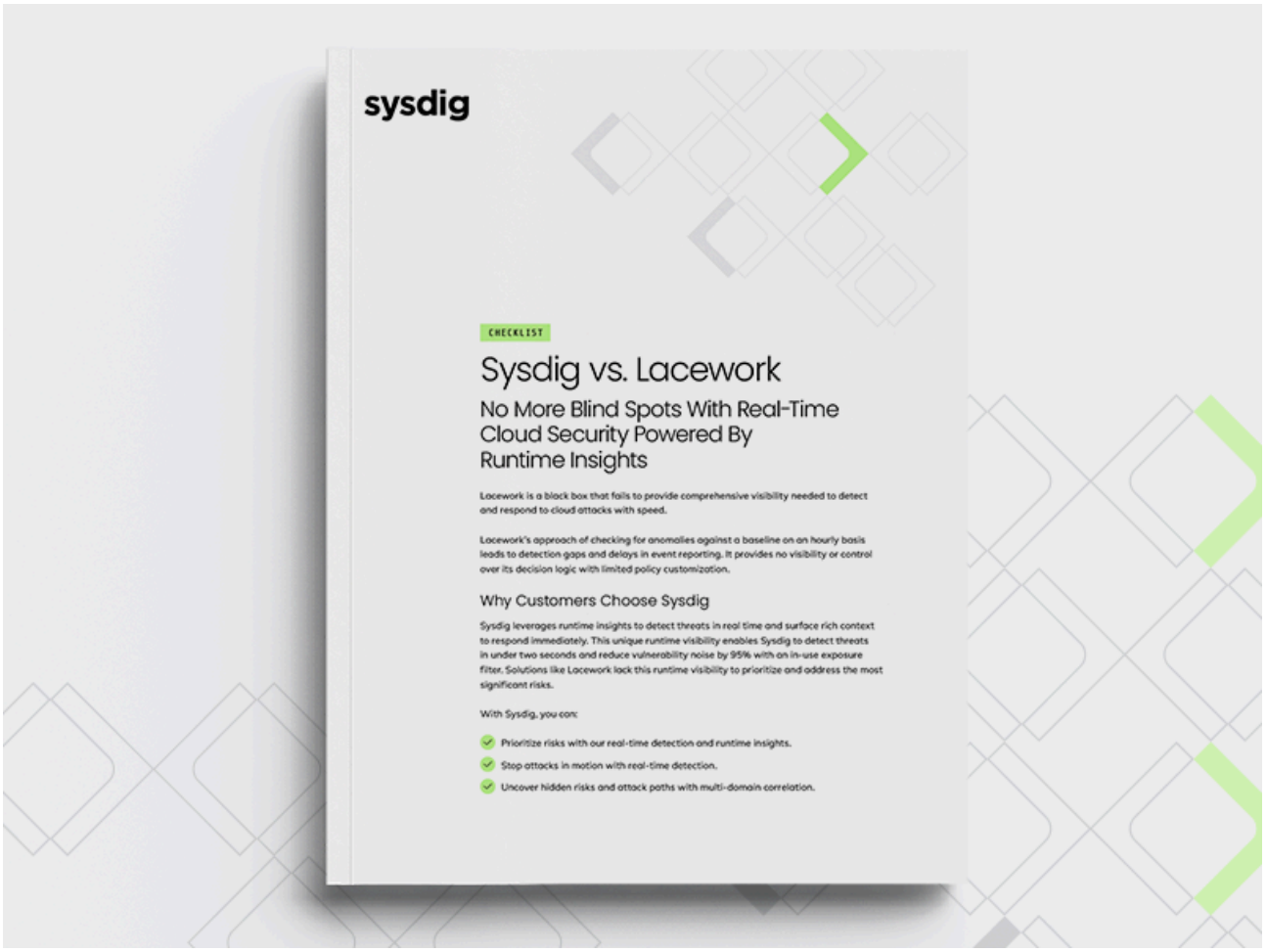
Cloud SecuritySysdig Secure


[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 Managementvideo

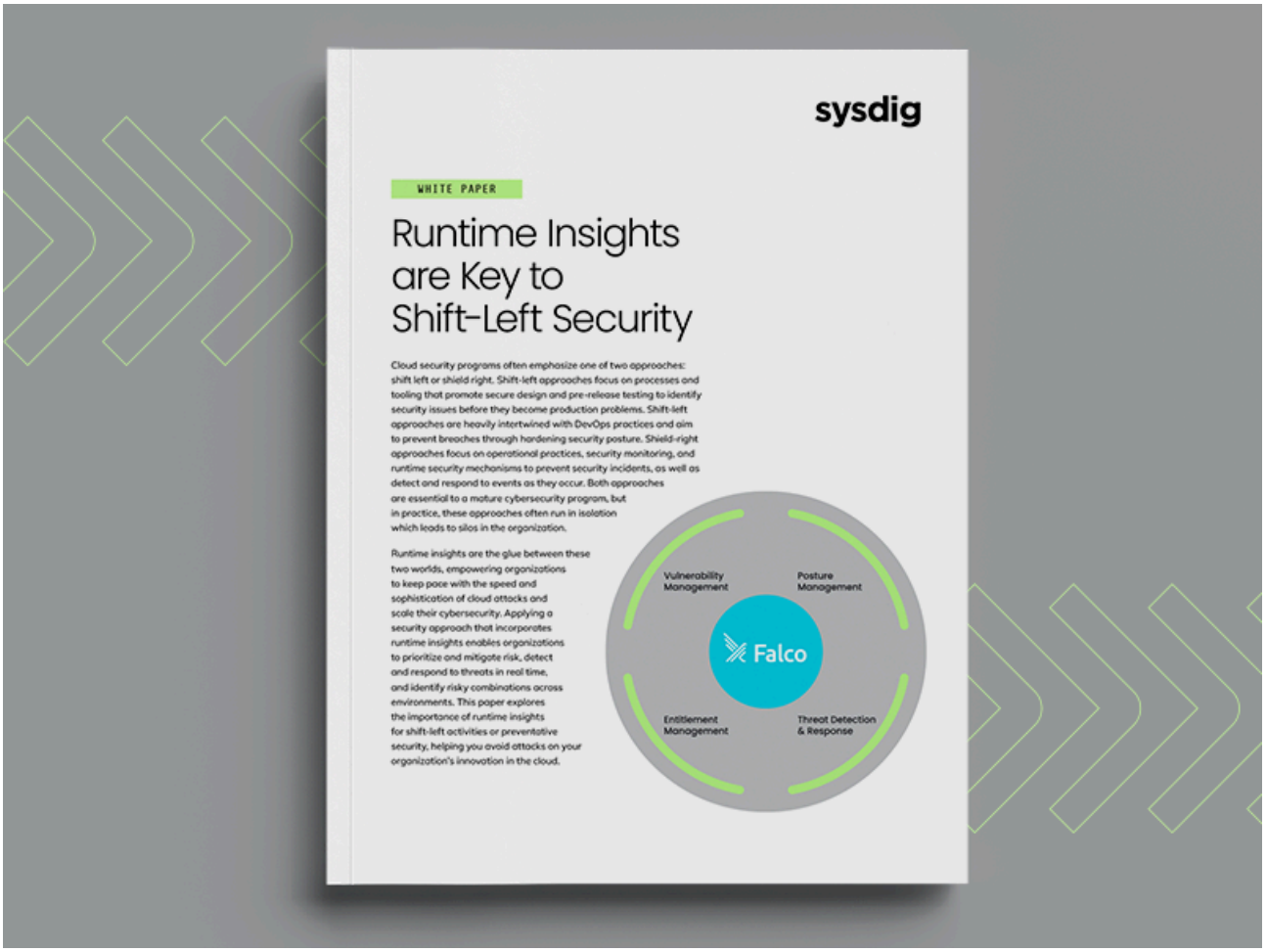
Cloud SecuritySysdig SecureCloud computing security


WHITEPAPER. Securing the Cloud with End-to-end Detectionpdf

Cloud SecuritySysdig 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.

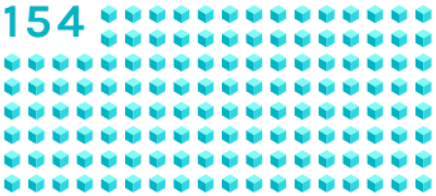
### The old merges with the new.

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...

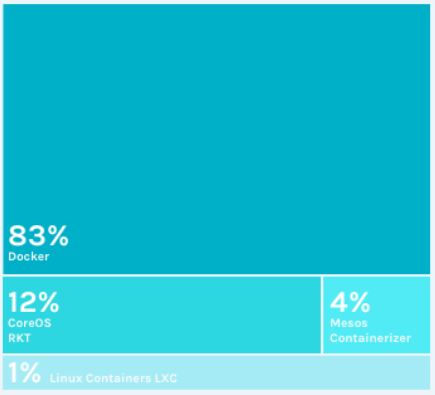
We observed density as high as 154 containers on a single host.

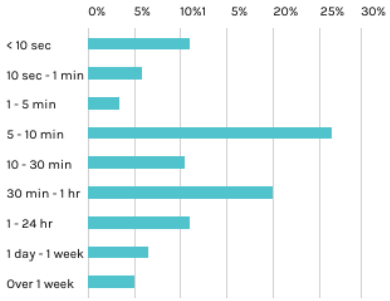
Up from a maximum of 95 in 2017.

## 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%.



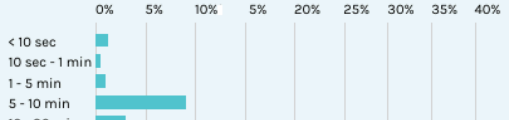

## What is the lifespan of containers and services?

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.

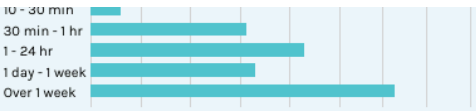
## 69% of container images are updated in one week.

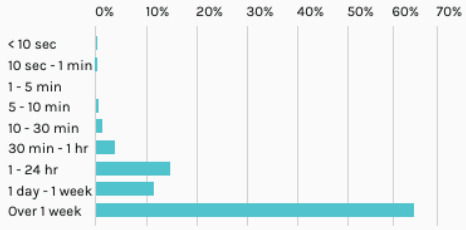
A small percentage of images are updated in less than 10 seconds



– 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.

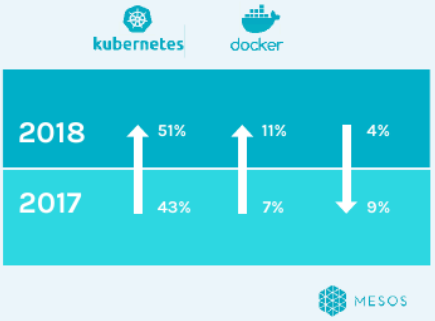
Containers and pods come and go, but services are expected to be available.

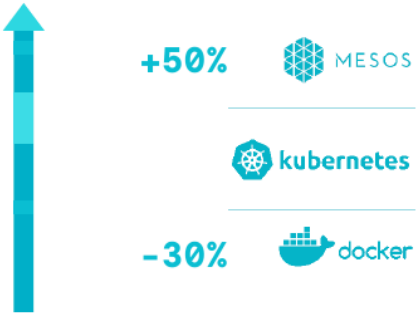
For most customers the goal is to keep applications working around the clock. Services allow containers and pods to die and replicate without impacting the application.

## 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.

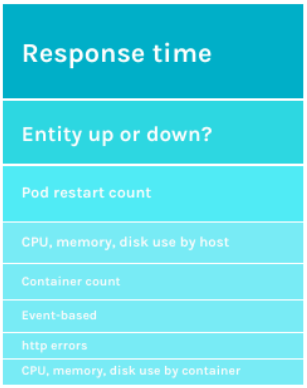
### Here come the Kubernetes distributions.

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.

82% kubernetes

14% OPENSHIFT

4% RANCHER




## Most popular alert conditions.

### It's all about performance + uptime.

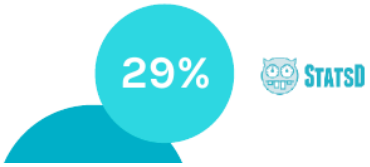
What keeps container administrators up at night? Sysdig alerts tell us what matters most. Responsiveness and uptime/downtime top the list. Host and container resource metrics - cpu, memory, and disk usage - are also important. Increasingly, orchestration-focused alerts like, "Pod Restart Count" are used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

## Popular alert scopes.

### Users want to know - How're my pods doing?

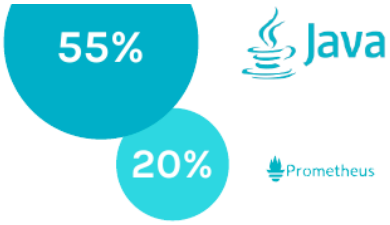
Alerts are "scoped" for a subset of the environment or for the entire infrastructure. The most common alerts are tied to Kubernetes tags. Scoping by pods is the leading choice followed closely by namespace. Container specific scoping is also popular, evenly split across container name, container image,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

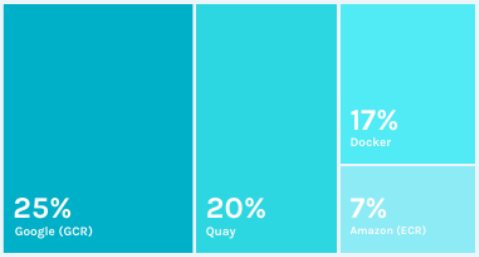



Sysdig automatically collects custom metrics like JMX, StatsD, and Prometheus. JMX metrics associated with Java applications were collected by 55% of users. StatsD comes in at 29% and Prometheus at 20%. With the popularity of Prometheus, we expect its number to grow over time.

## 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).



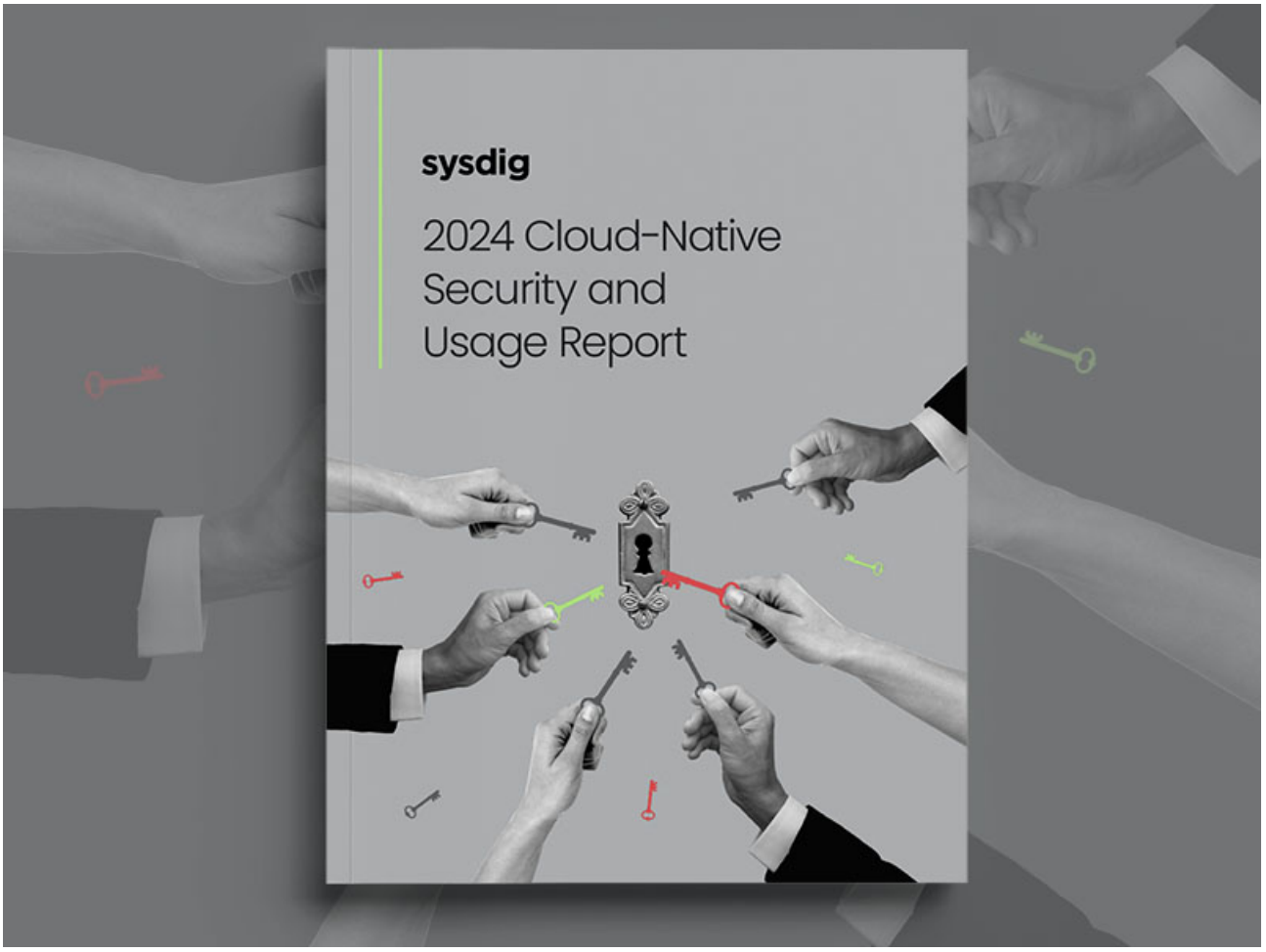


## Want to learn more?

Download the complete Docker Usage Report to see all the details.

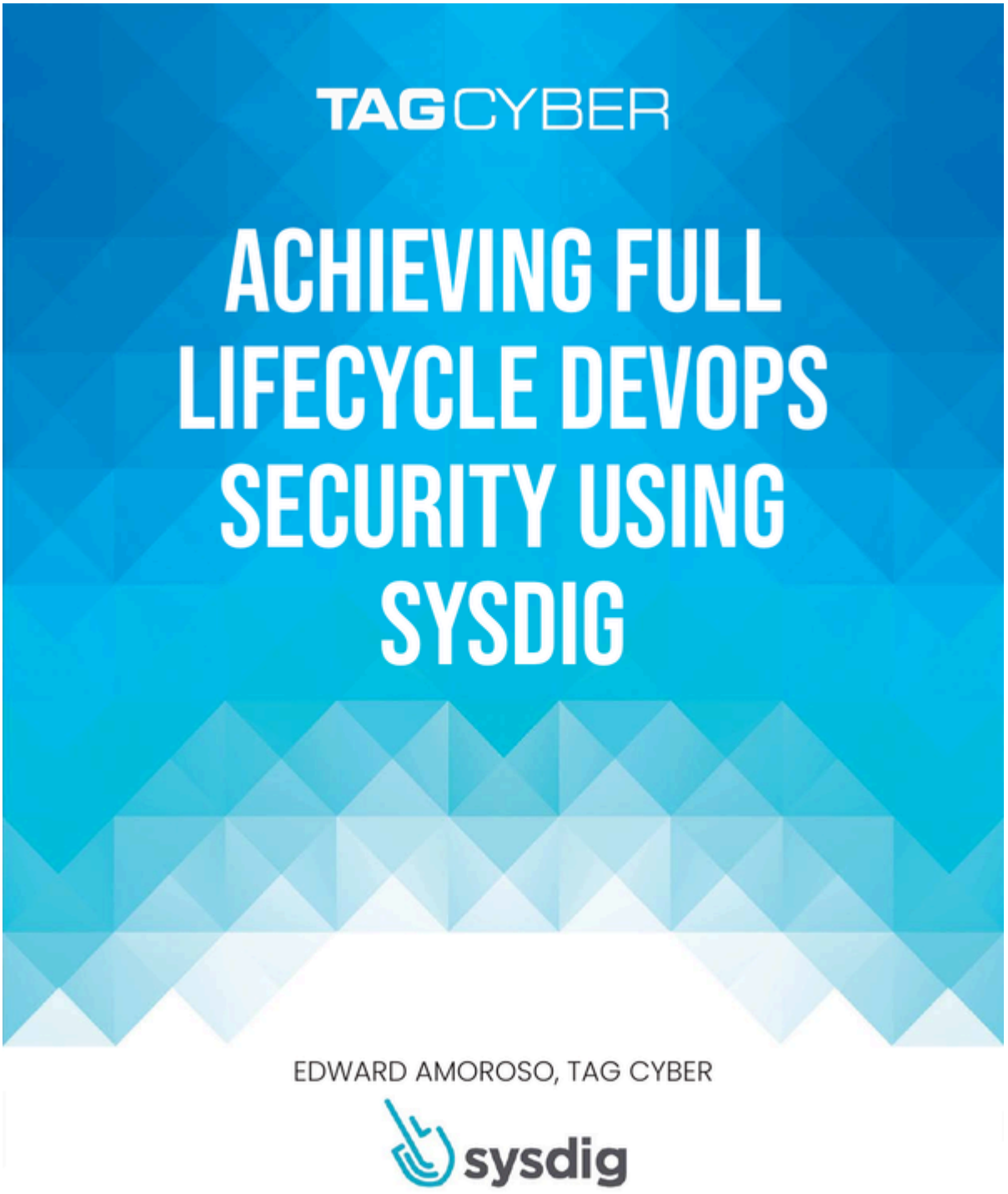
INFOGRAPHIC. 2018 Docker Usage Reportpdf

DockerOpenshiftKubernetesPrometheus




REPORT. 2024 Cloud Native Security And Usage Reportpdf

Cloud SecuritySysdig SecureCloud computing security




REPORT. Achieving Full Lifecycle Devops Security Using Sysdigpdf

Cloud SecuritySysdig Secure

sysdig



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


PARTNER BRIEF. Sysdig and Google Cloud Platformpdf

Cloud SecuritySysdig Secure

sysdig

CASE STUDY

**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

BlaBlaCar

# 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

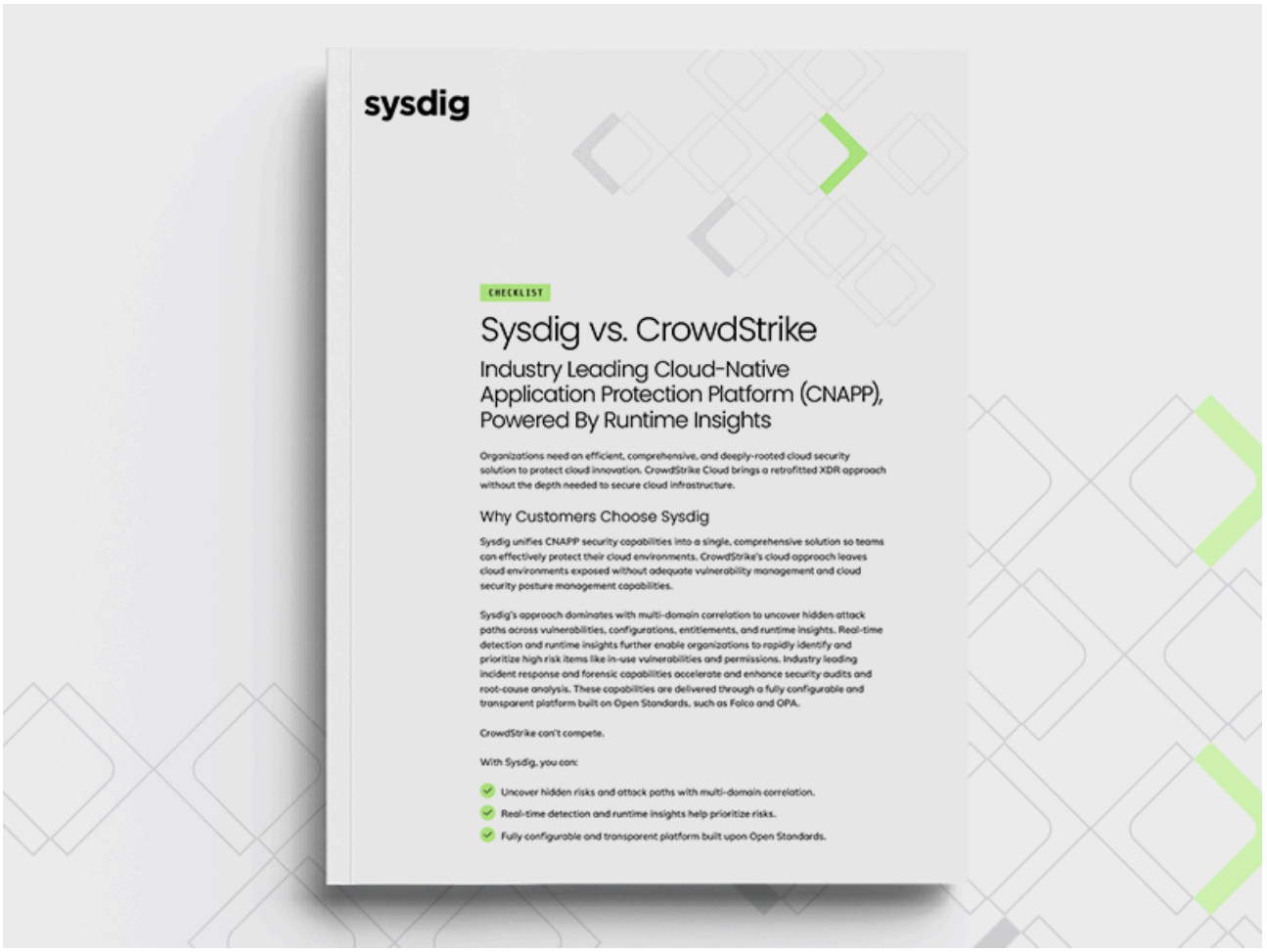
Cloud SecuritySysdig SecureKubernetesSysdig Monitor


VIDEO. DevOps Teams Addressing Security: IBMvideo

Cloud SecuritySysdig SecureCloud MonitoringIBM

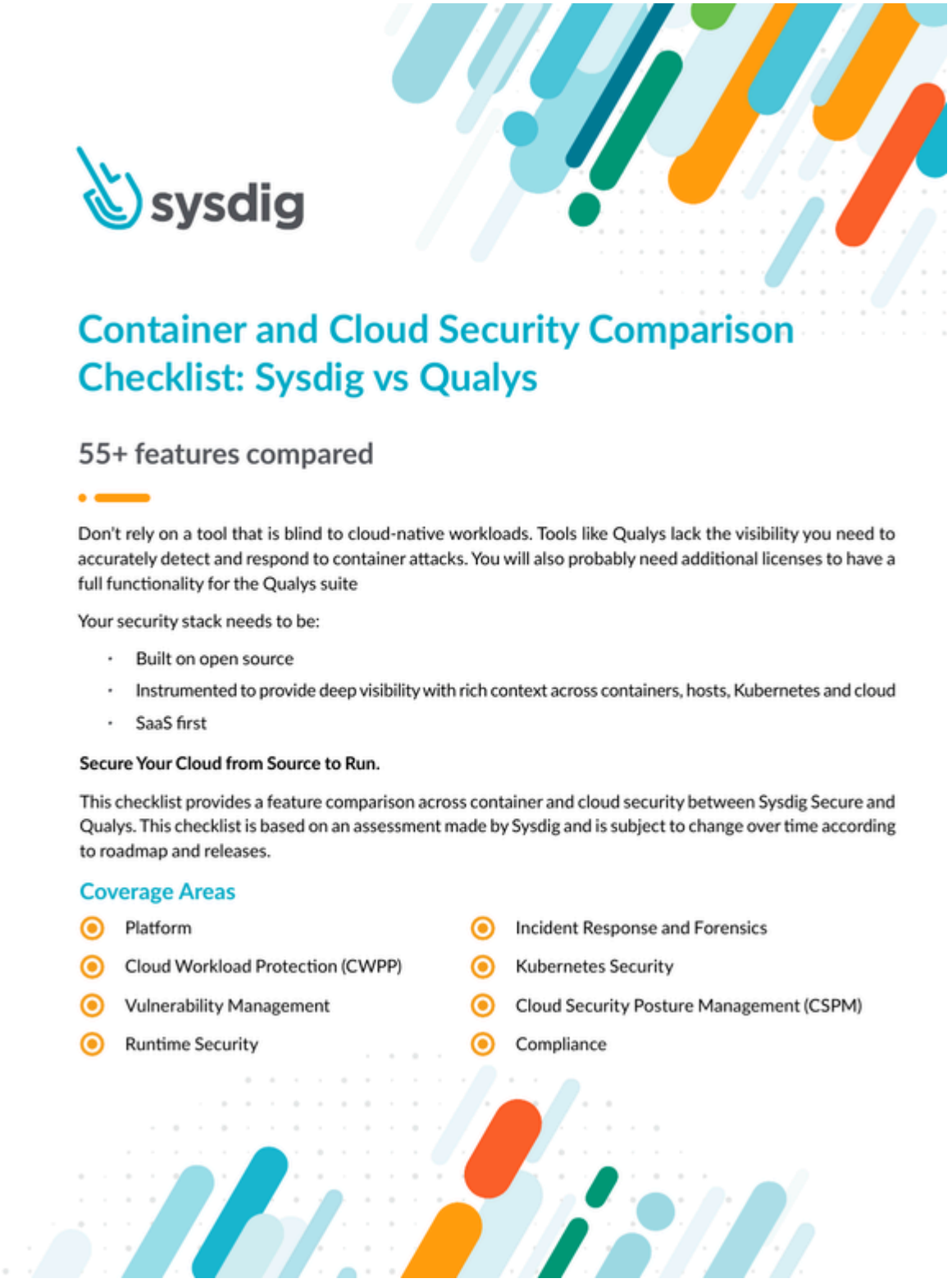

VIDEO. Troubleshooting Processes and Tools: IBMvideo

Cloud SecuritySysdig SecureCloud MonitoringIBM




GUIDE. Container Security Comparison Checklist: Sysdig vs CrowdStrikepdf

Cloud SecuritySysdig Secure




GUIDE. Container Security Comparison: Sysdig vs Qualyspdf

Cloud SecuritySysdig SecureRegulatory Compliance


GUIDE. Container and Cloud Security Comparison Checklist: Sysdig vs Orcapdf

Cloud SecuritySysdig SecureRegulatory Compliance

VIDEO. Journey to Containers: IBMvideo

Cloud SecuritySysdig SecureCloud MonitoringIBM


BRIEF. The Business Impact Of Time In Cloud Securitypdf

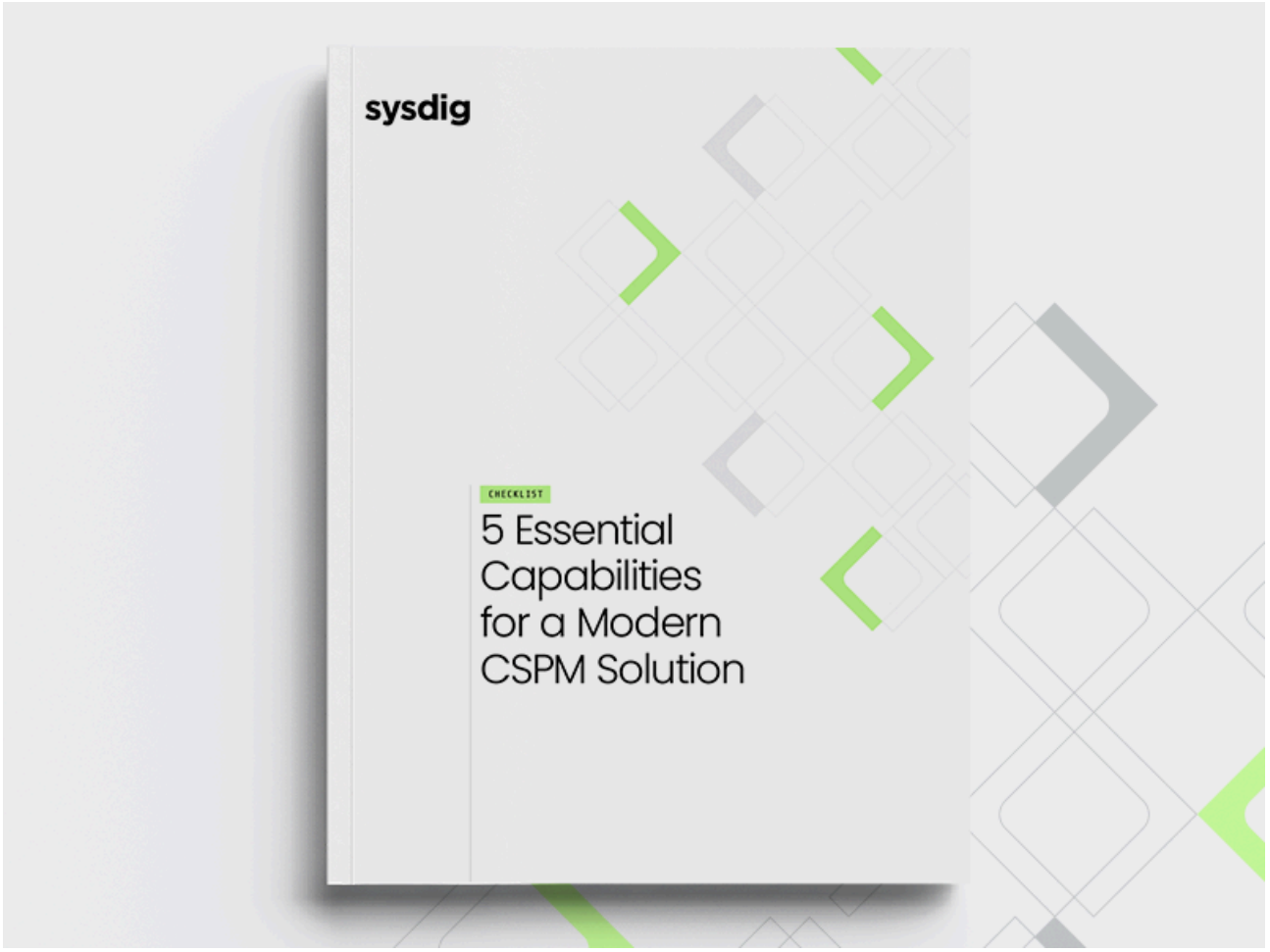
Cloud SecuritySysdig SecureCloud computing security


GUIDE. Cloud Security for Google Cloudpdf

Cloud SecuritySysdig Secure


GUIDE. Container Security Comparison Checklist: Sysdig vs StackRoxpdf

Cloud SecuritySysdig Secure

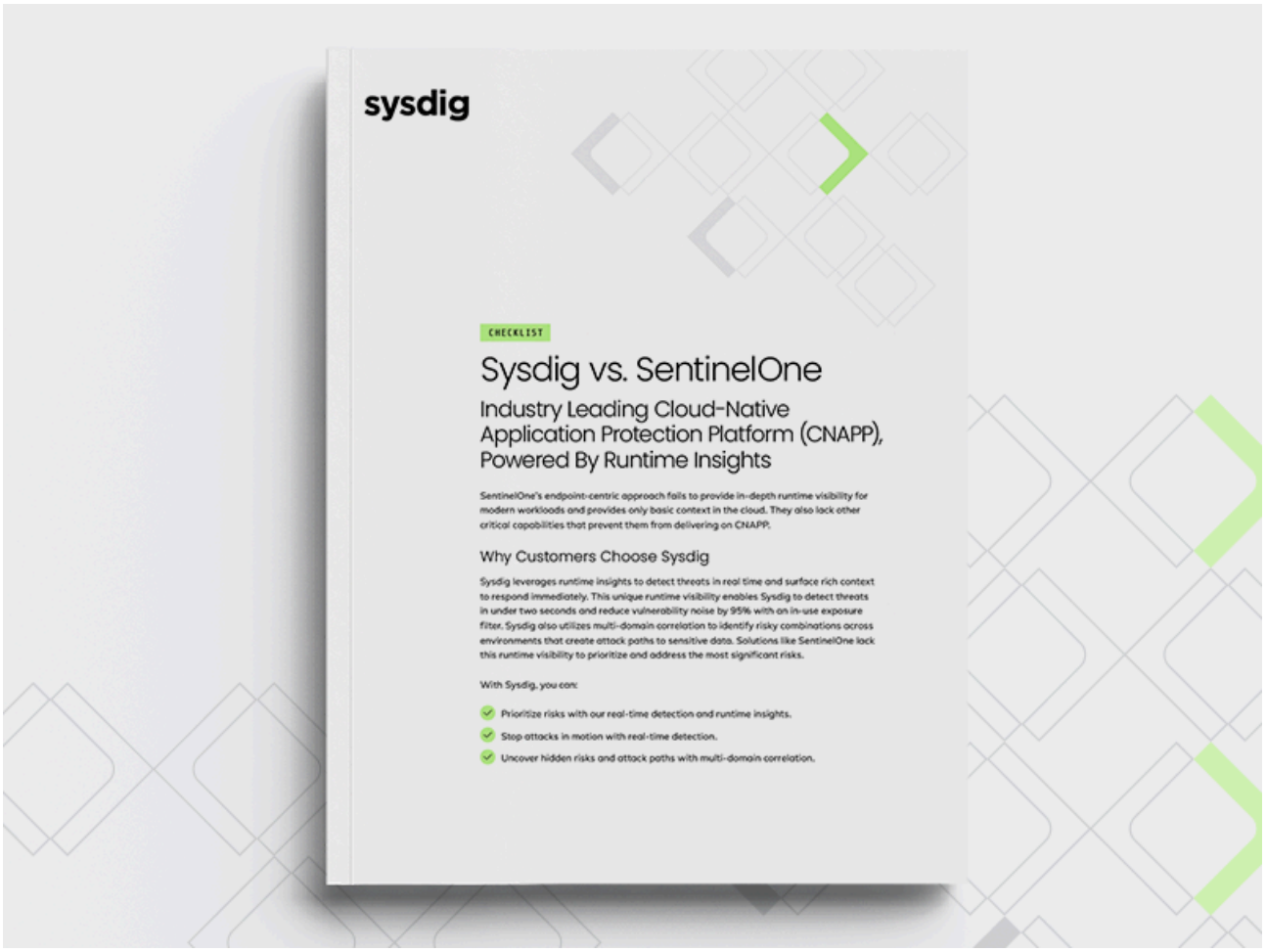



BRIEF. 5 Essential Capabilities for a Modern CSPM Solutionpdf

Cloud SecuritySysdig SecureCloud computing security


REPORT. 2023 Cloud-Native Security & Usage Reportpdf

Cloud SecuritySysdig SecureCloud MonitoringKubernetes




GUIDE. Sysdig vs SentinelOne Checklistpdf

Cloud SecuritySysdig SecureCloud computing security

sysdig

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:

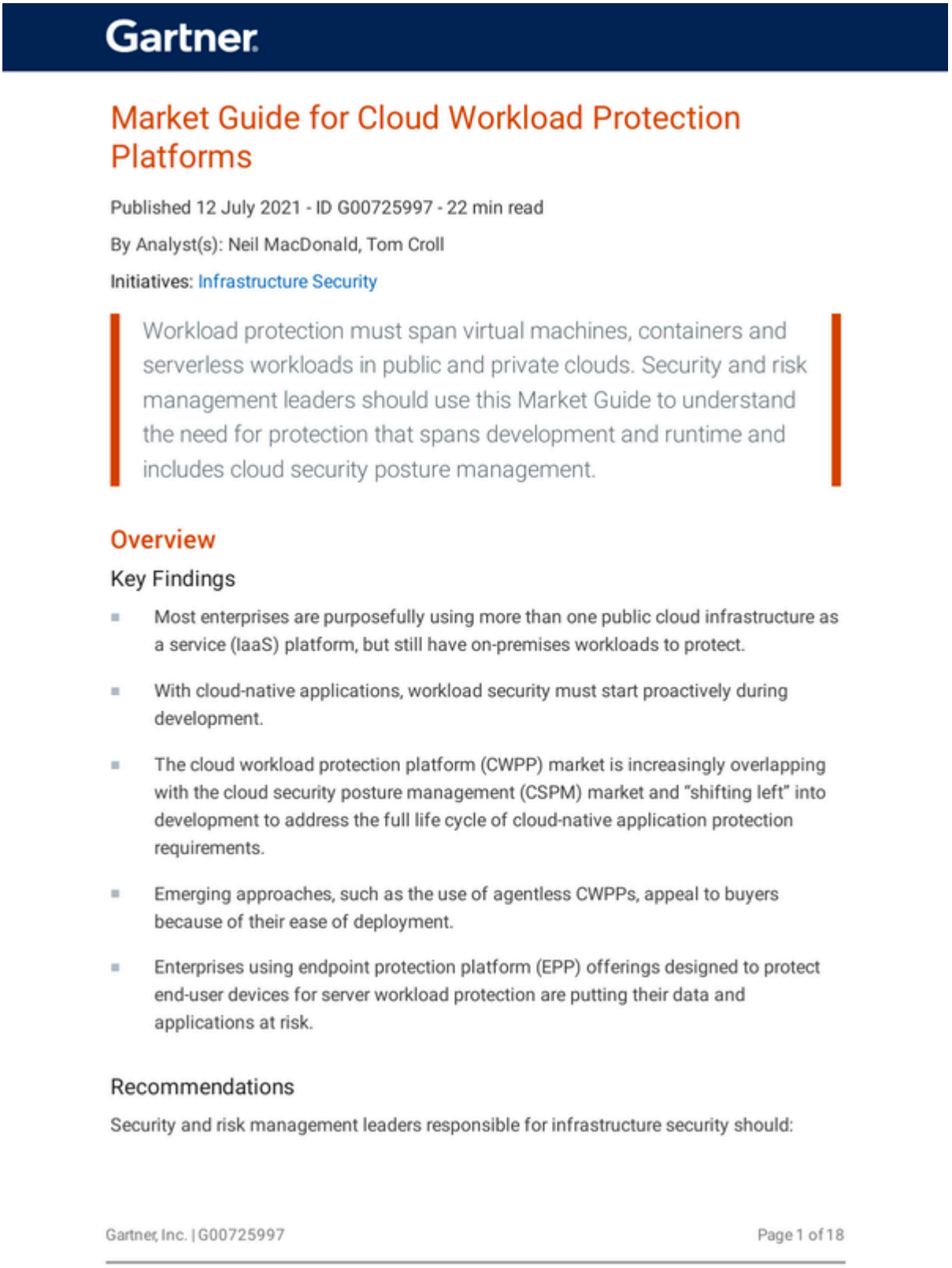
- Identify and Prioritize Real Risk
- Accelerate Cloud Maturity Based on In-Use Permissions
- Mitigate Compliance Risk with Runtime Insights
- Save Time with In-Use Risk Prioritization
- Reduce Cost by Consolidating Security Tools

BRIEF. 5 Critical Business Values Delivered By Sysdig Posture And Permission Managementpdf

Cloud SecuritySysdig SecureCloud computing security


SOLUTION BRIEF. Snyk & Sysdig Solution Briefpdf

Cloud SecuritySysdig Secure



Gartner

# 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:



[REPORT. 2021 Gartner Market Guide for Cloud Workload Protection Platforms (CWPP)pdf]

[Cloud SecuritySysdig Secure]


Written by **Dave Shackleford**

April 2021

*Sponsored by:*
**Sysdig**

Analyst Program

©2021 SANS™ Institute

REPORT. SANS 2021 Cloud Security Surveypdf

Cloud SecuritySysdig Secure


REPORT. 2022 Sysdig Cloud-Native Threat Reportpdf

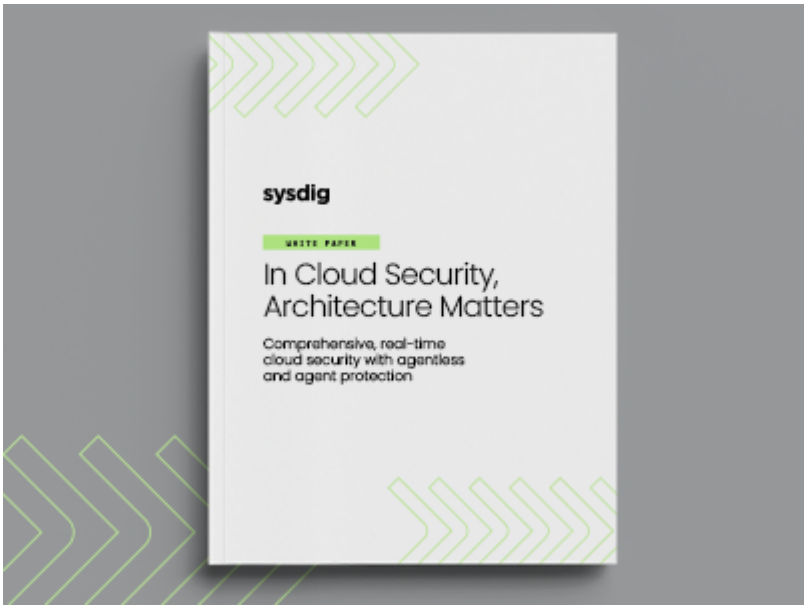
Cloud SecuritySysdig Secure


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

sysdig

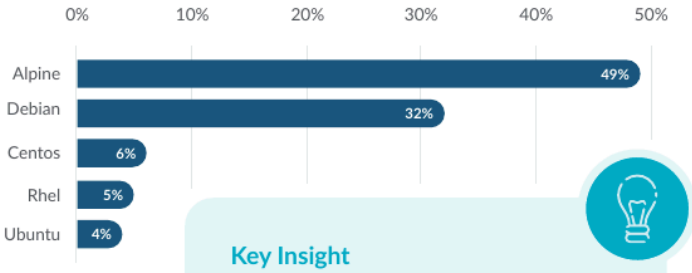
# 2020 Container Security Snapshot

**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.

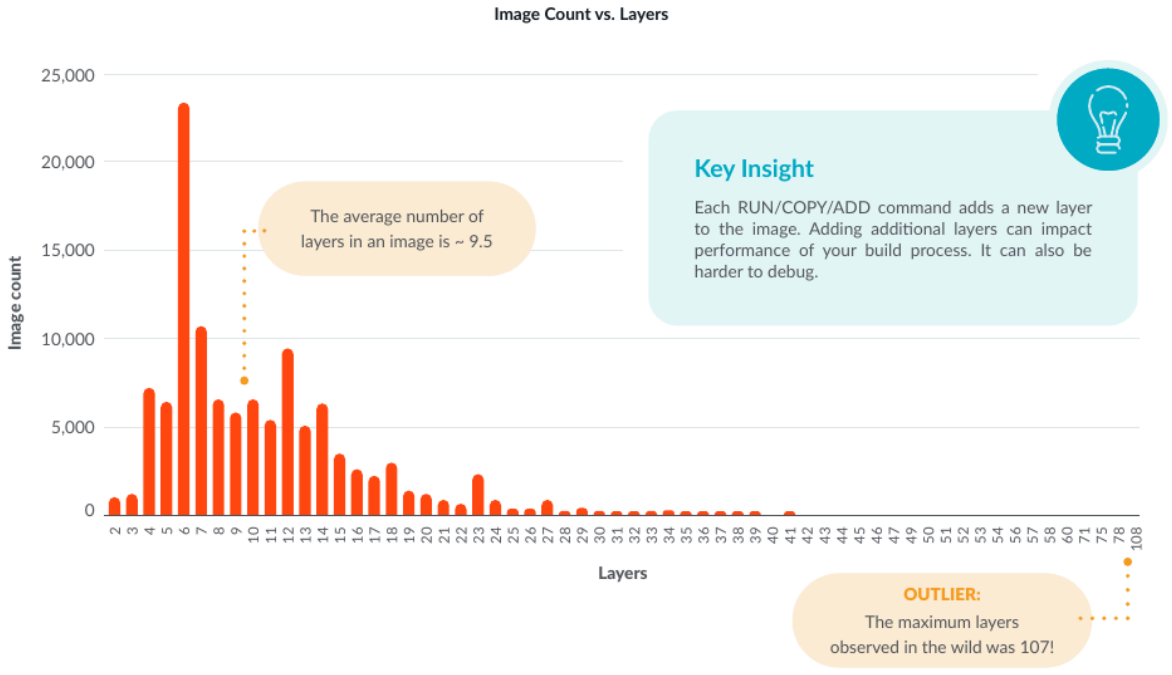
- Large images not only take longer to deploy, slowing down release velocity, they expose more opportunities for attack.

largest image size observed

**10 GB**

that's 26x larger than the average

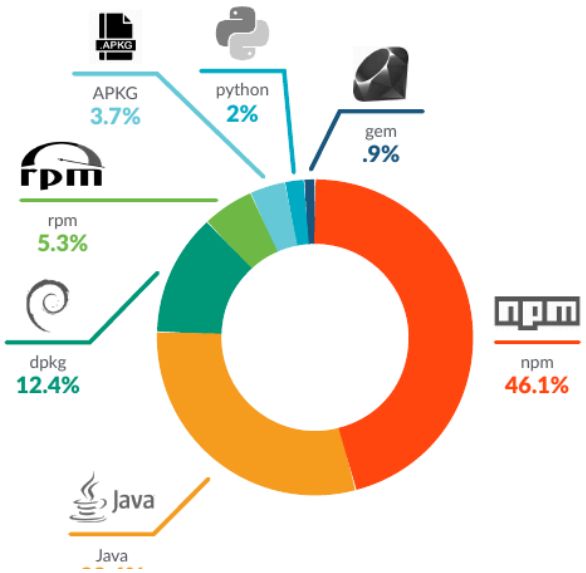
## How many layers are part of an image?




### 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.

## 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%

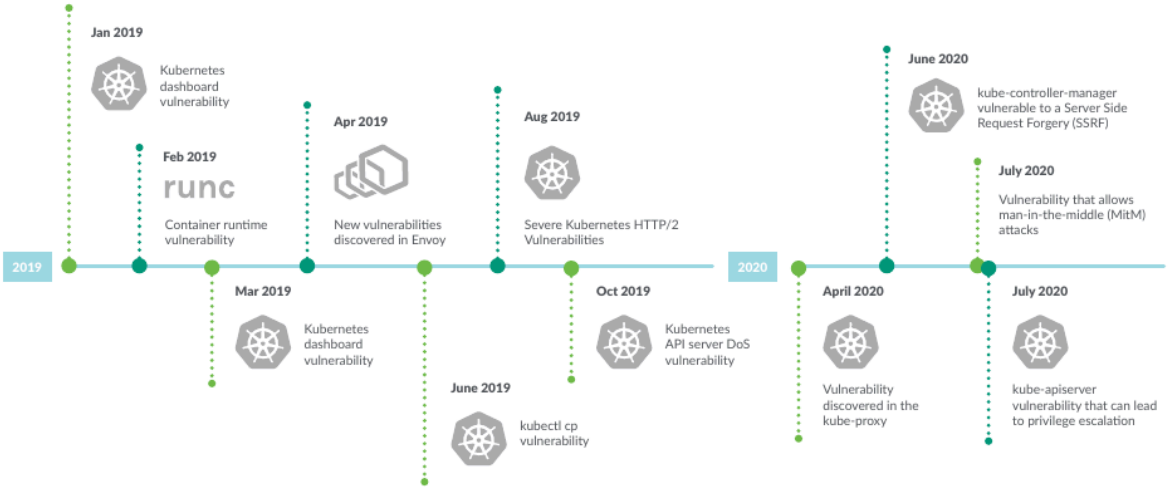
## Where are images typically pulled from?

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?

**OS Vulnerabilities by Severity**


### Key Insight

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

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.

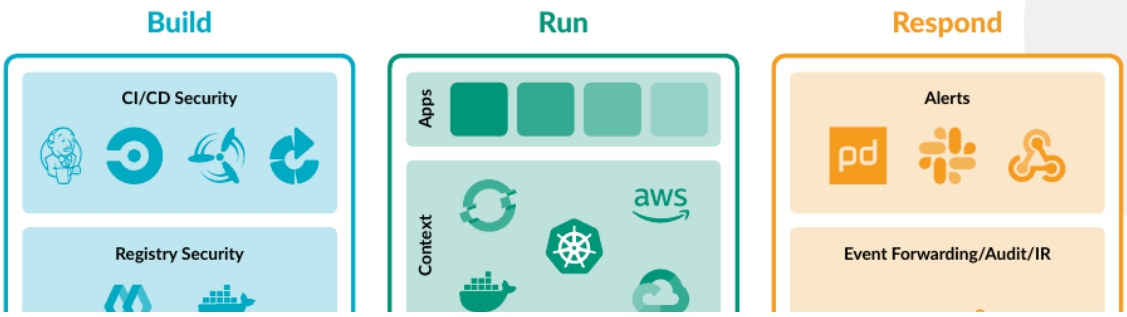

# Risky configurations are common

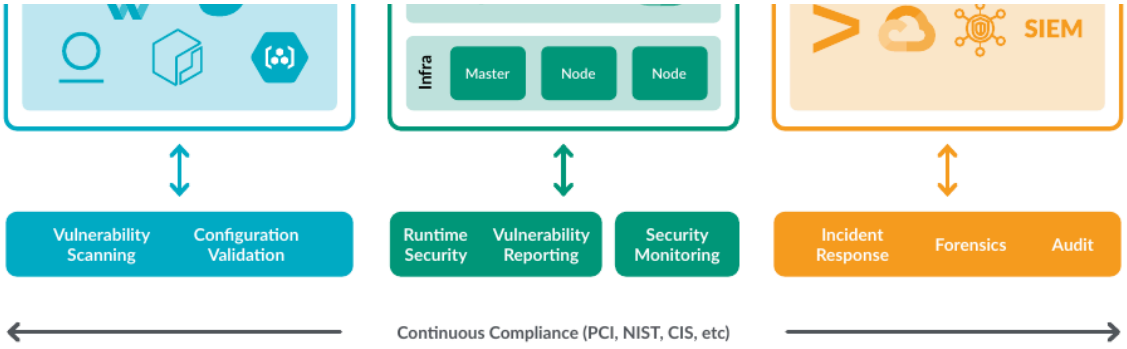
How many images are running as root?


## 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

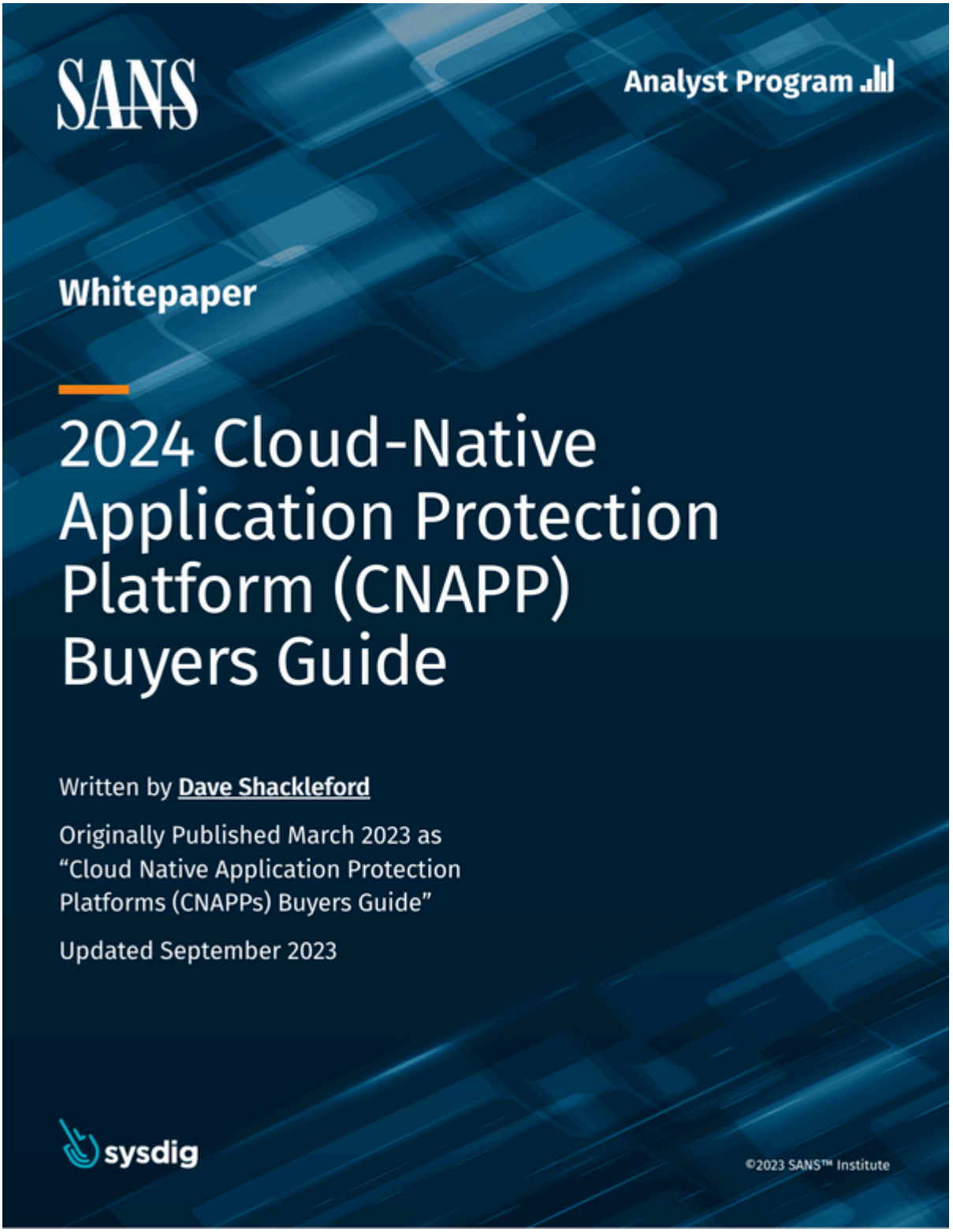
1. Embed scanning into your CI/CD pipelines and also ensure you have runtime scanning in place to detect newly identified vulnerabilities.
2. Scan both OS as well as non-OS packages (over 53% have high/critical CVEs) to manage security risk effectively. Read more about how to implement Docker scanning 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
sysdig
Copyright © 2020 Sysdig, Inc. All rights reserved. ING-006 Rev. A 8/20

INFOGRAPHIC. 2020 Container Security Snapshotpdf

Cloud SecuritySysdig SecureKubernetes




WHITEPAPER. SANS CNAPP Buyers Guidepdf

Cloud SecuritySysdig Secure

sysdig 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[1].

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.

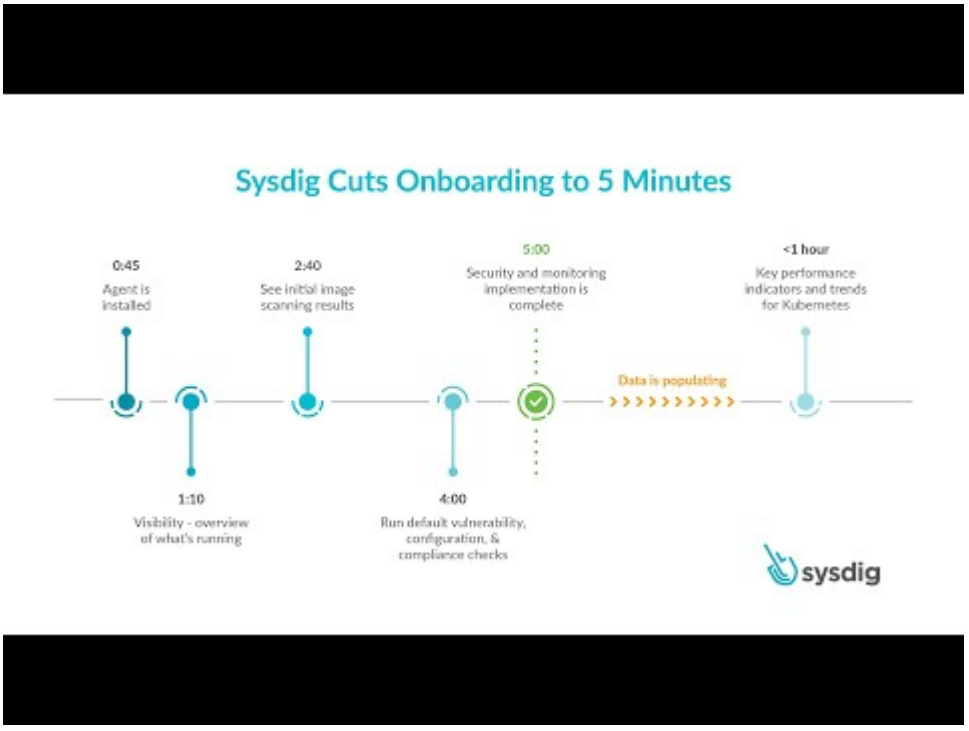
IBM zSystems and IBM LinuxONE provide a strong foundation built for security, resiliency, and availability:

- Integrated **FIPS 140-2 level 4** compliant hardware security module (HSM[2]).
- Leverage **Red Hat OpenShift** Container Platform to modernize applications.
- Multitenancy with full LPAR isolation and virtualization designed for the highest **EAL5+ security certification**[3].
- **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 LinuxONEpdf]

[Cloud SecuritySysdig SecureIBM]




VIDEO. 5 minutes to onboard secure DevOpsvideo

Cloud SecuritySysdig SecureCloud MonitoringKubernetes


PARTNER BRIEF. Red Hatpdf

OpenshiftRed Hat

sysdig

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

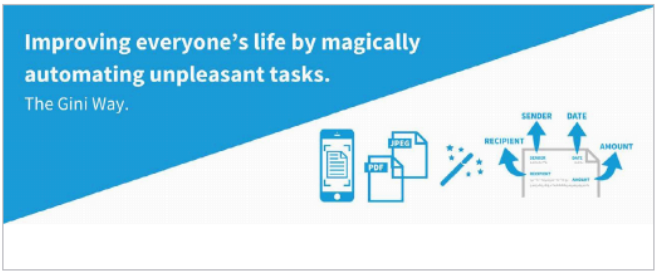
**BUSINESS IMPACT OF SYSDIG:**
The Gini operations and developer teams have confidence knowing their environment is secure. They are able to provide stable applications while saving time, allowing developers to focus on revenue-generating activities.

**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

gini




# 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.

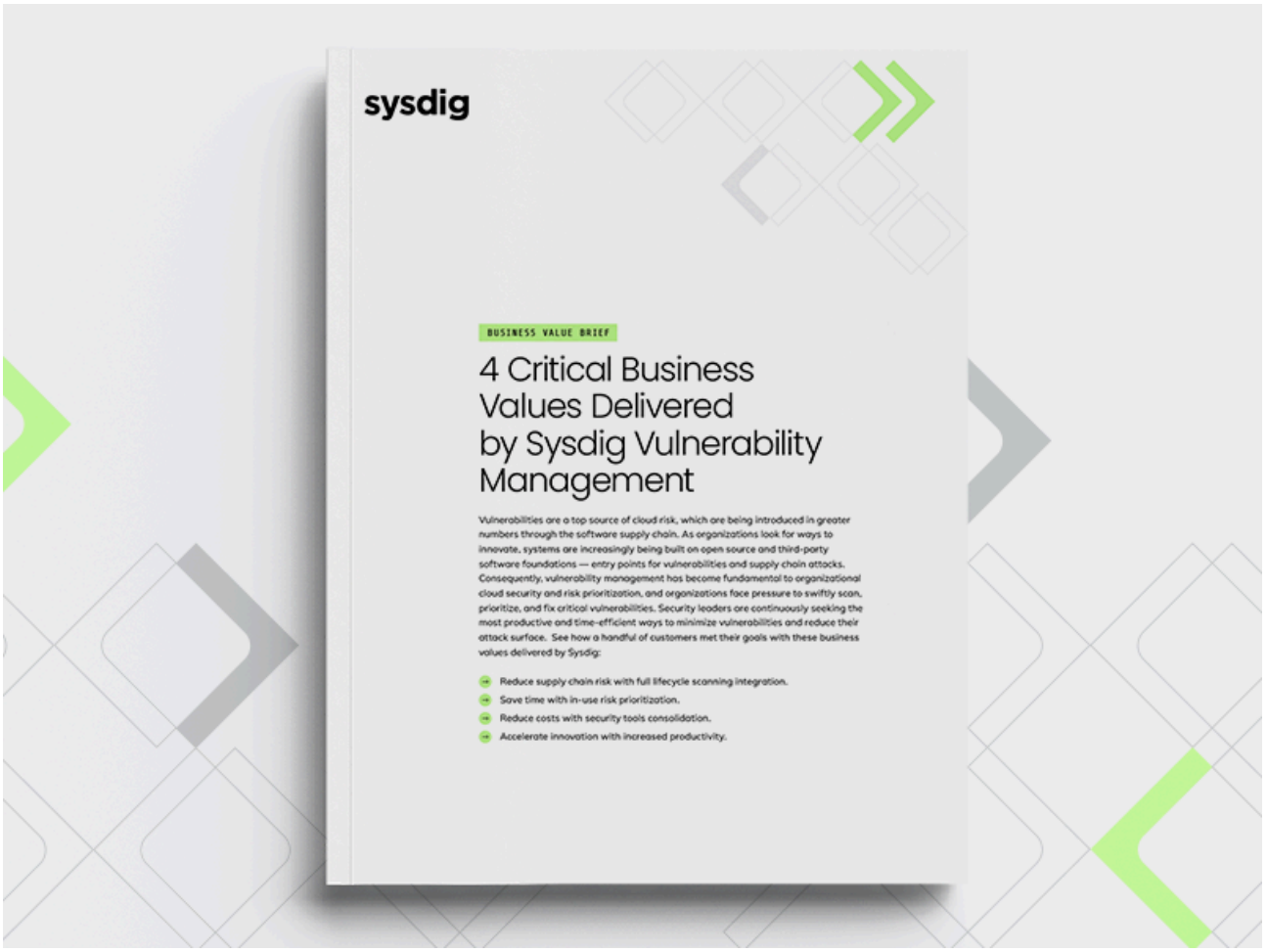
With millions of end customers, Gini's engineering team is responsible for maintaining a secure, 'always on' environment. The company operates 25 machines in an environment that spans bare metal and AWS Cloud. To ensure it can secure and monitor its hybrid cloud environment, Gini engineers rely on the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

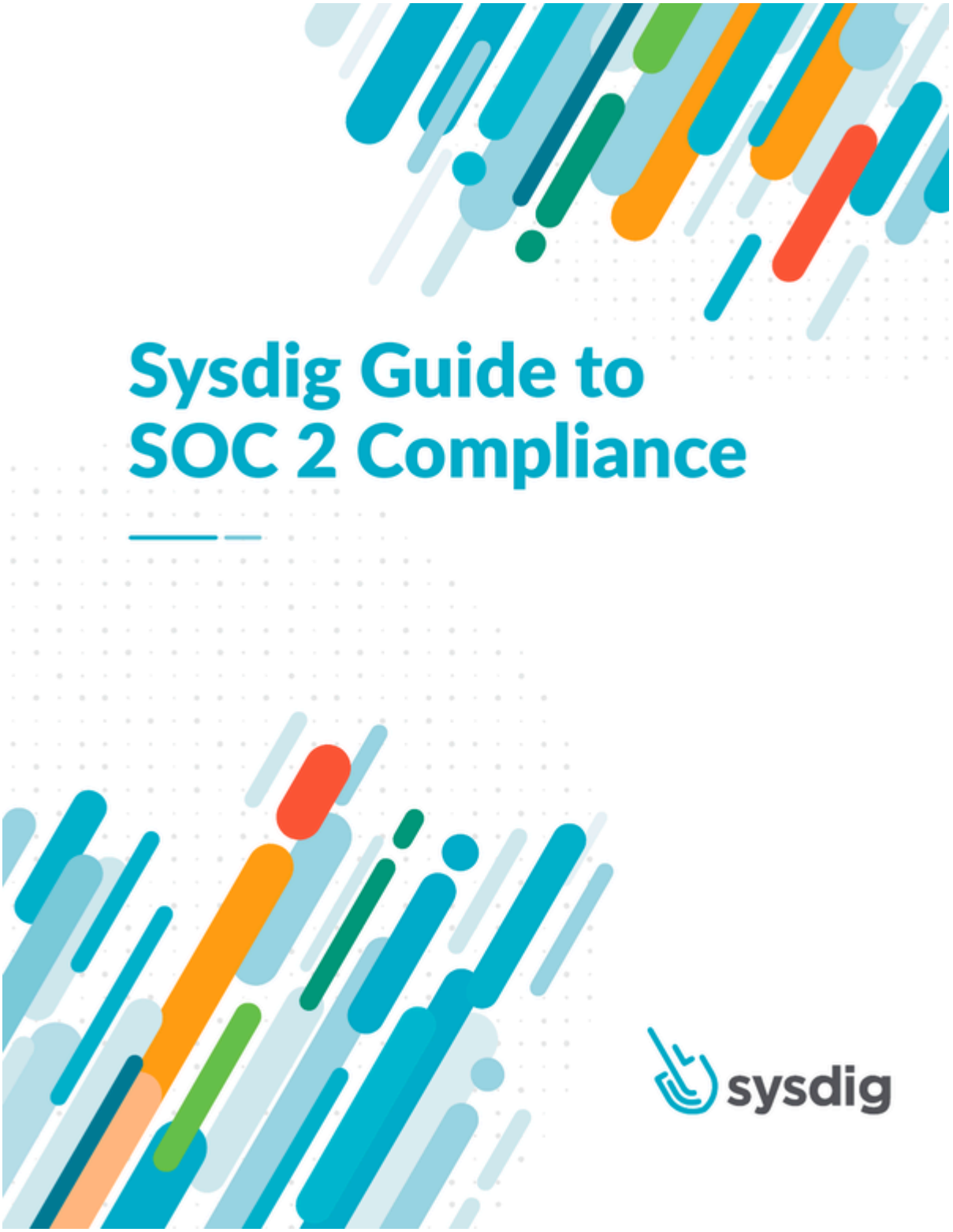
CASE STUDY. Gini Ensures Adherence to Strict EU Compliance Standards, While Reducing Dev and Ops Burdenspdf

AWSSysdig SecureKubernetesSysdig Monitor




BRIEF. 4 Critical Business Values Delivered By Sysdig Vulnerability Managementpdf

Cloud SecuritySysdig Secure

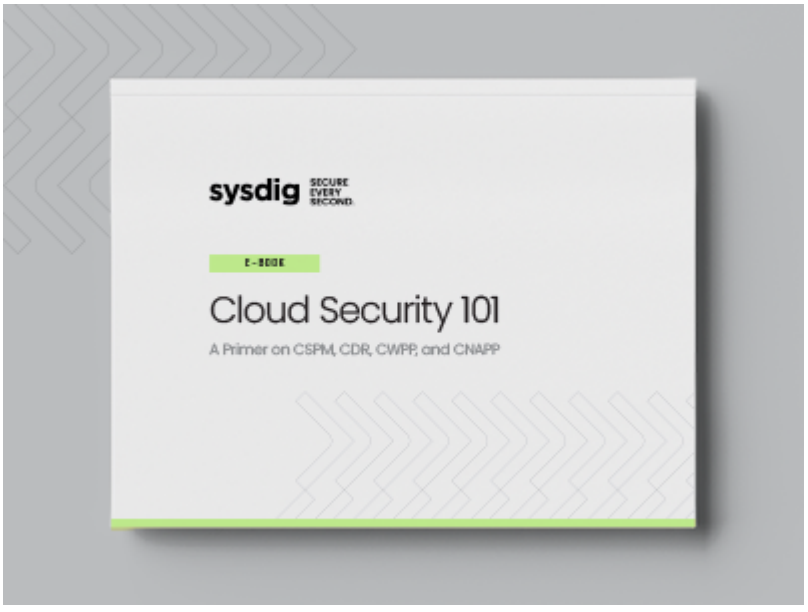



GUIDE. Sysdig Guide To SOC 2 Compliancepdf

Cloud SecuritySysdig SecureRegulatory Compliance

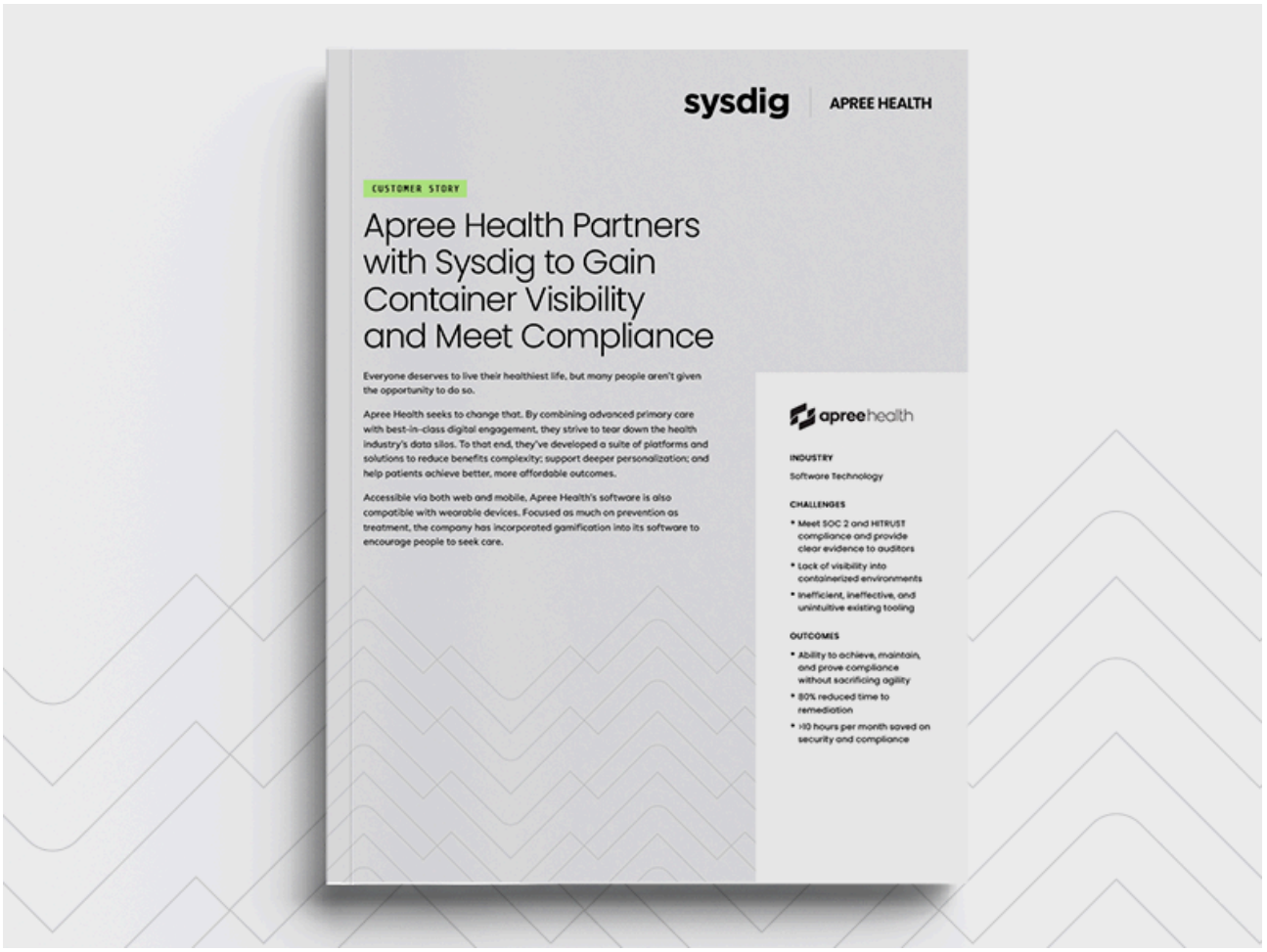

VIDEO. How to prepare for the next Log4jvideo

Cloud SecuritySysdig Secure



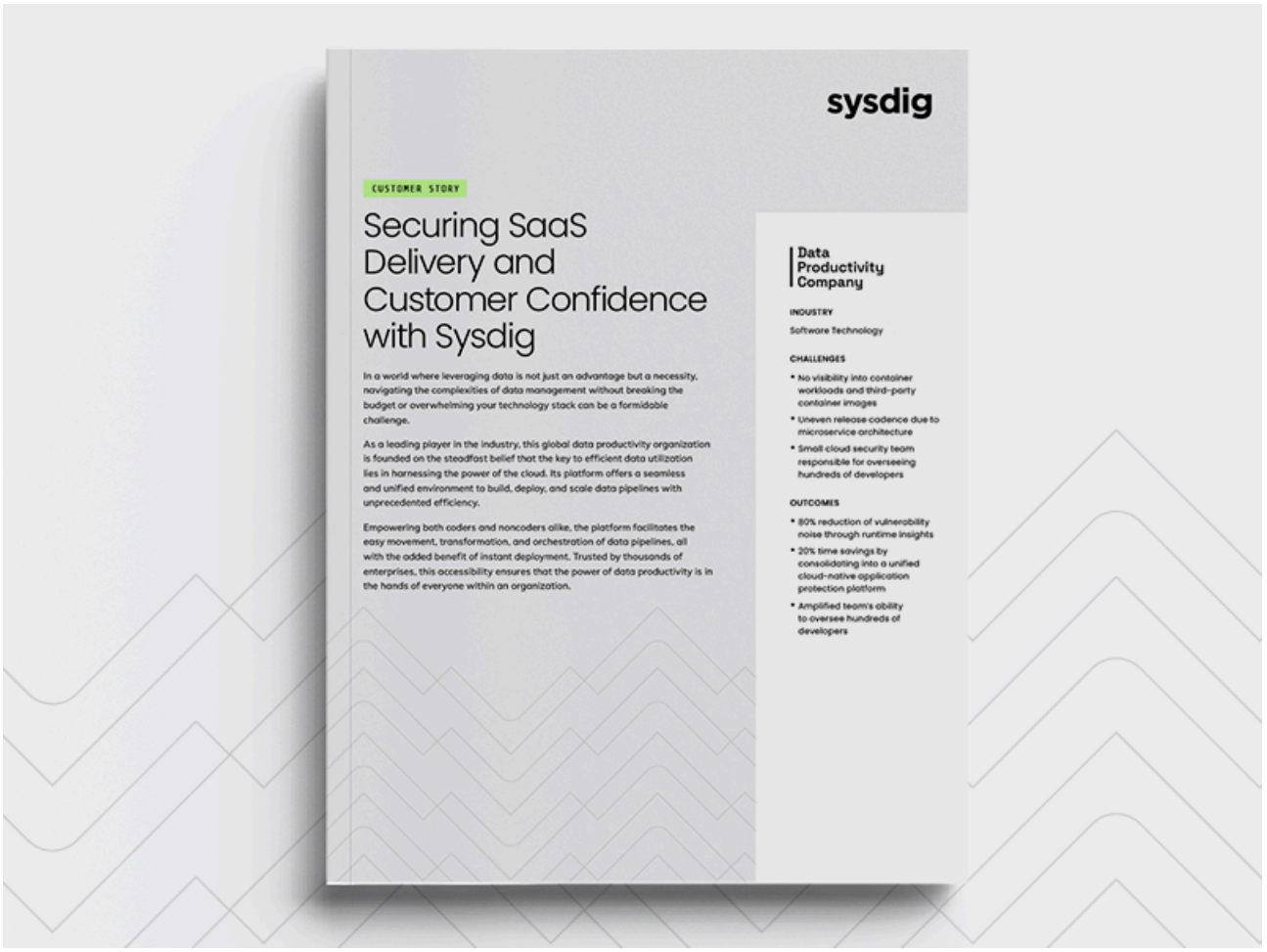

GUIDE. Cloud Security 101pdf

Cloud SecuritySysdig Secure



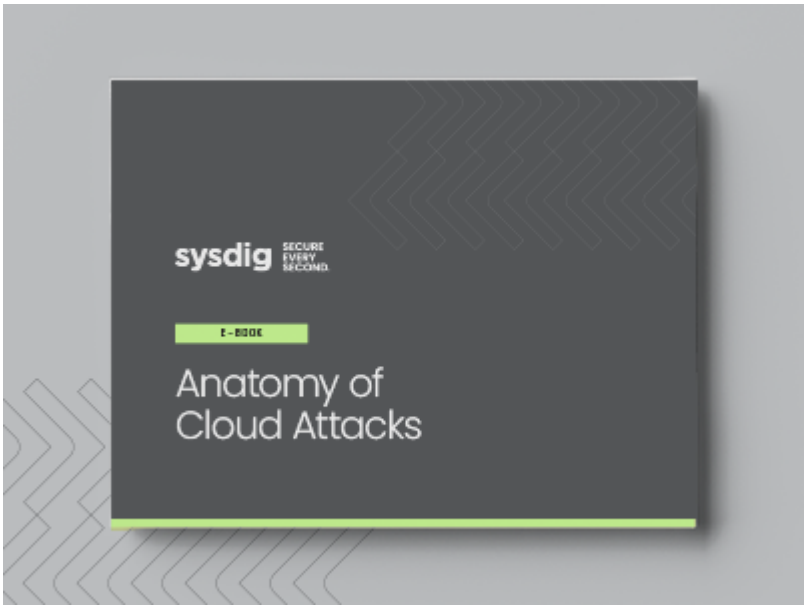

CASE STUDY. Apree Healthpdf

Cloud SecuritySysdig SecureCloud computing security



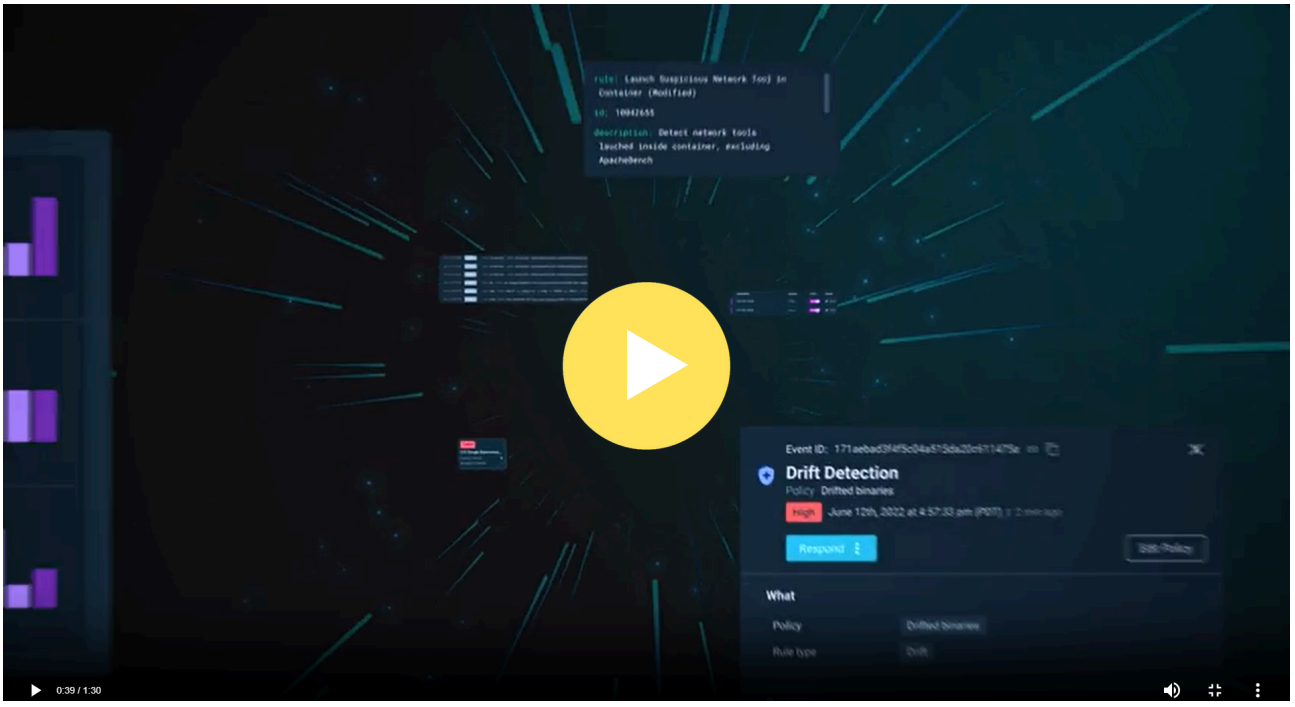

CASE STUDY. Data Productivity Companypdf

Cloud SecuritySysdig SecureCloud computing security




GUIDE. Anatomy Of Cloud Attackspdf

Cloud SecuritySysdig Secure




VIDEO. Cloud Security Meets GenAI: Introducing Sysdig Sagevideo

Cloud SecuritySysdig Secure

sysdig

CASE STUDY

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

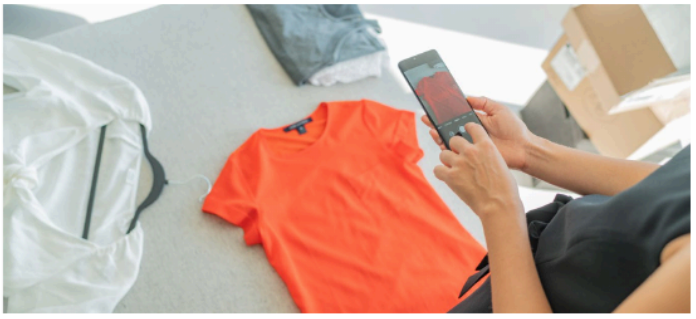
**CHALLENGES:**
- Generally speaking, Kubernetes is not secure by default and must be used with its security risks taken into account.
- With microservices, it is necessary to take security measures for developers and operations.

**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)

MERCARI



# 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

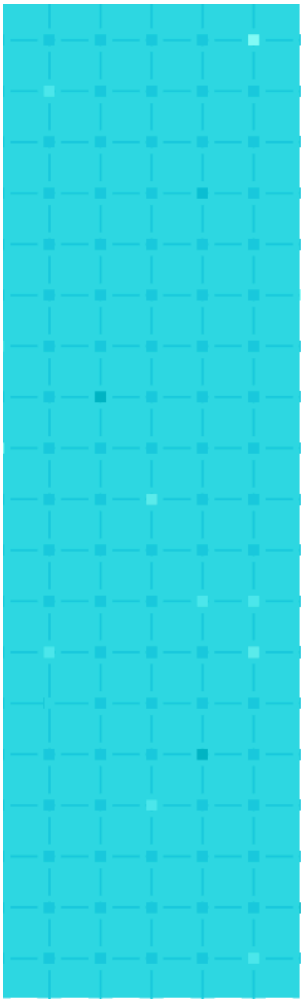
Mercari was established in February 2013 with the mission of "creating a global marketplace that creates new value." Since then, the Mercari Flea Market App has grown to become one of the leading products of its kind. In February 2019, the company's subsidiary, Merpay, launched a contactless payment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

CASE STUDY. Mercari Uses Sysdig to Secure the Most Widely Used Flea Market App in Japanpdf

Cloud SecuritySysdig SecureKubernetes


[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.

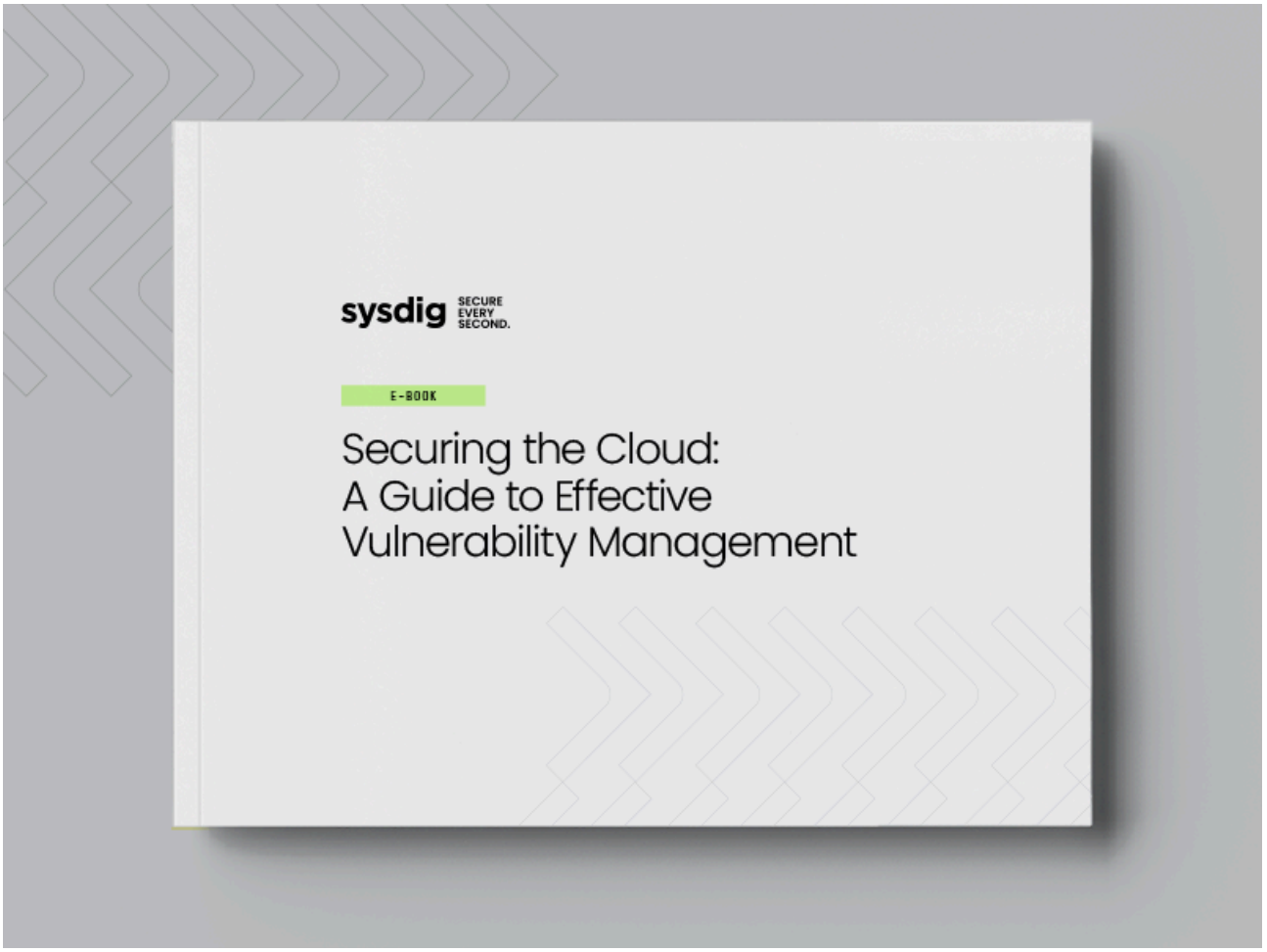
CASE STUDY

Case Study: ATPCOpdf

OpenshiftRed Hat

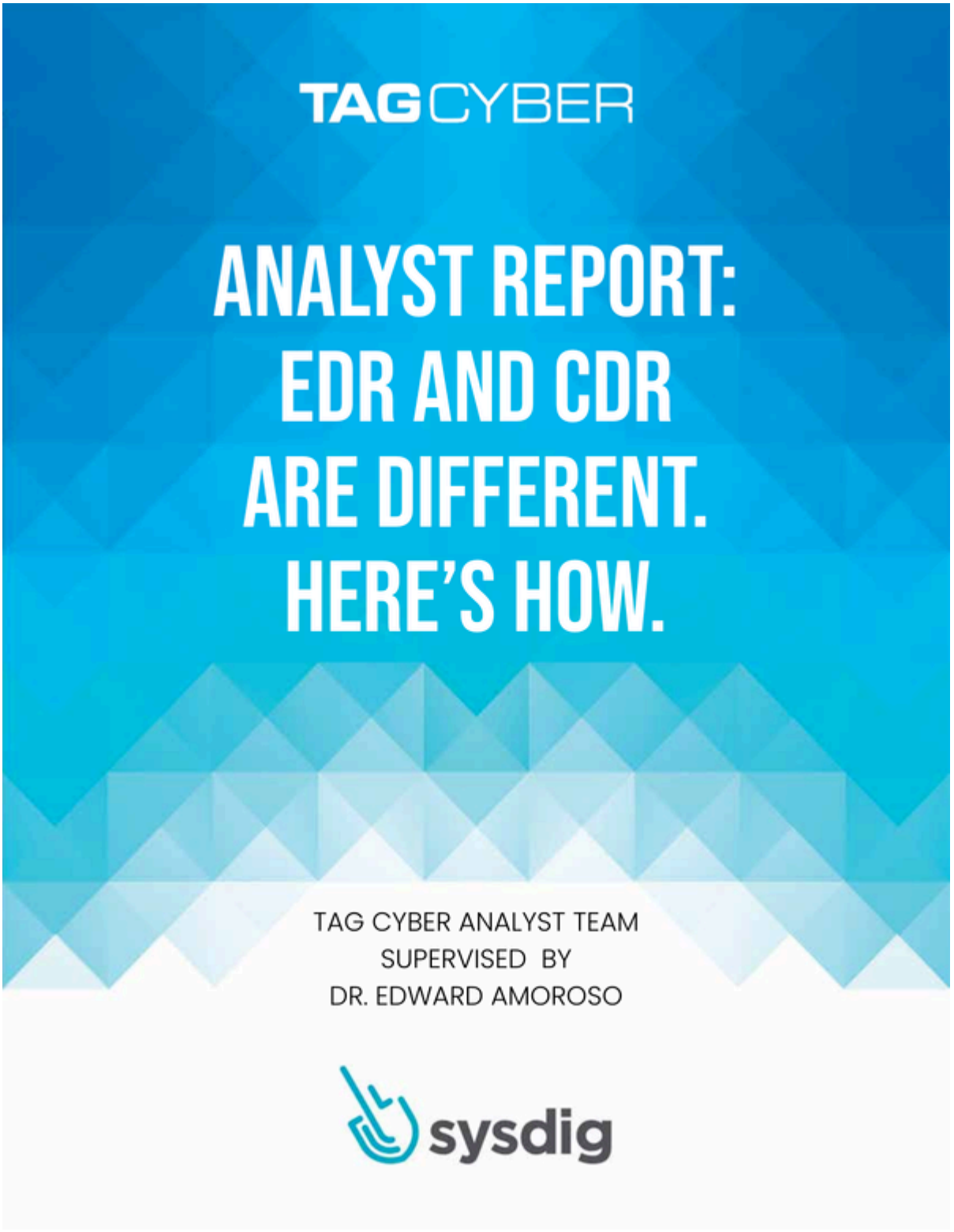

CASE STUDY. Neo4j Case Studypdf

AzureSysdig SecureAmazon Web ServicesKubernetes




GUIDE. Securing the Cloud A Guide to Effective Vulnerability Managementpdf

Cloud SecuritySysdig Secure




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 mappingvideo

DockerSysdig SecureSysdig Monitor


CASE STUDY. Ben Visa Valepdf

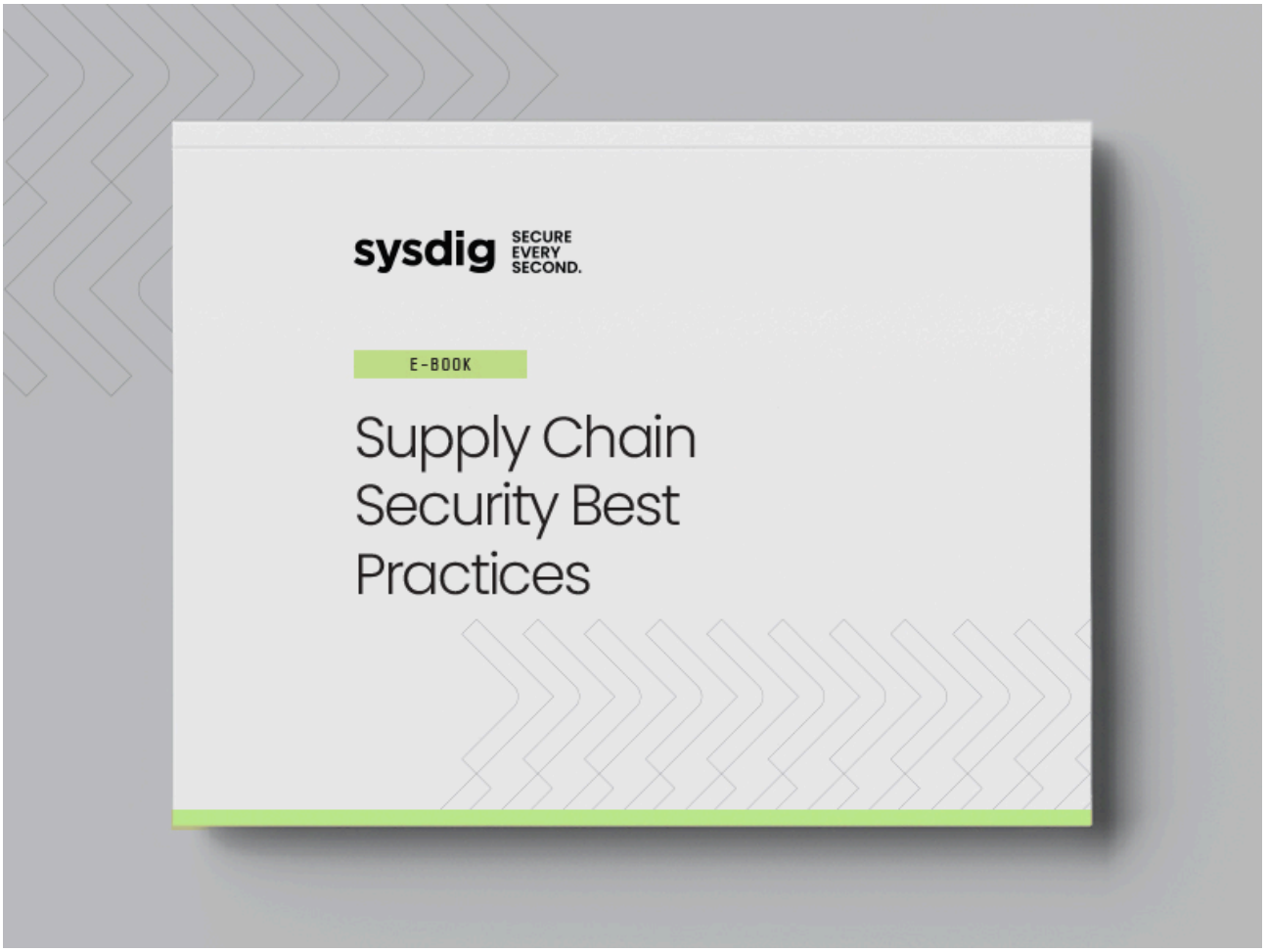
Cloud SecuritySysdig SecureCloud computing security

PODCAST. Screaming in the Cloud: Making Sense of Datawebpage

Cloud SecuritySysdig Secure


WEBINAR. Image Scanning Best Practices for Containers and Kubernetesvideo

Cloud SecuritySysdig SecureKubernetes




GUIDE. Supply Chain Security Best Practicespdf

Cloud SecuritySysdig Secure


PARTNER BRIEF. Sysdig and Cybereasonpdf

Cloud SecuritySysdig SecureCloud computing securitycybersecurity

sysdig

# 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

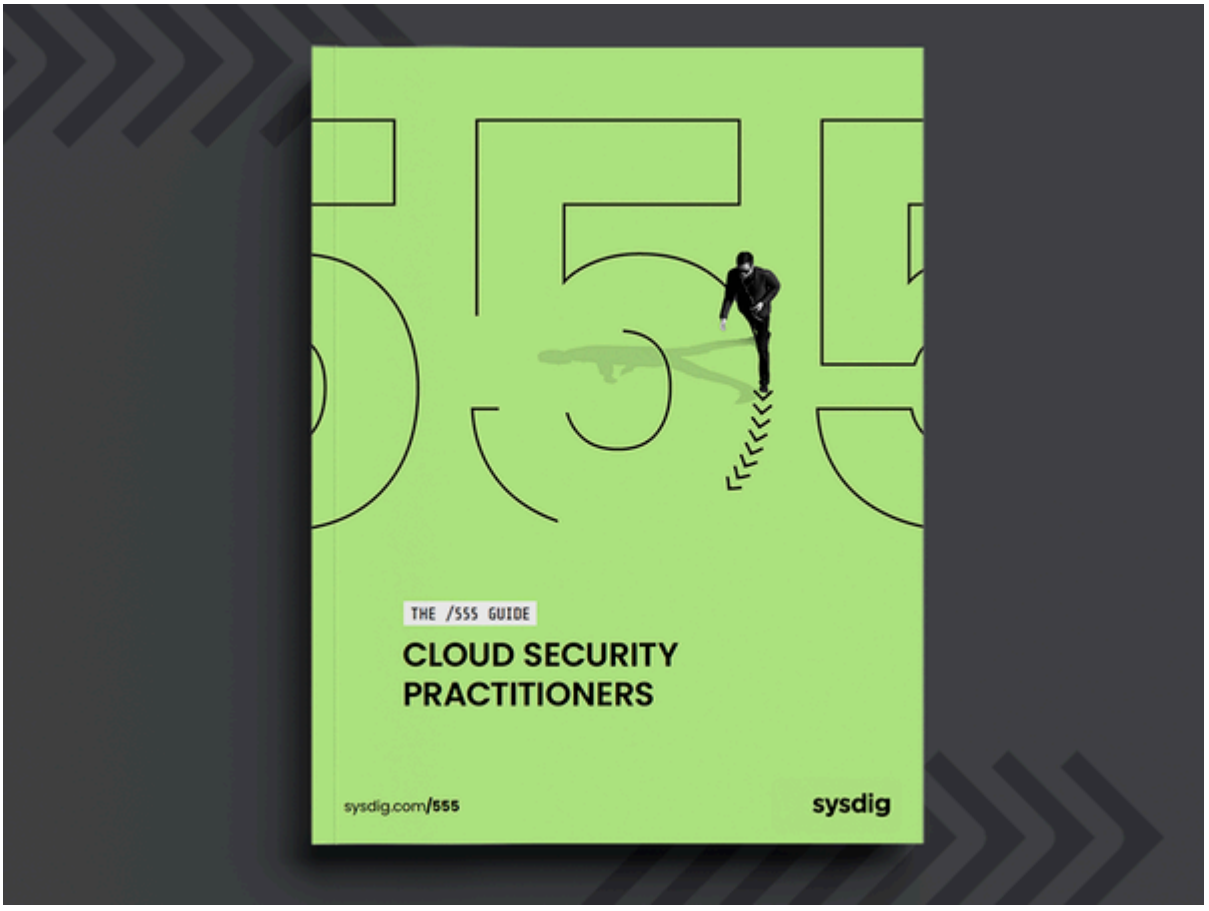
Cloud SecuritySysdig Secure


VIDEO. Requirements for Scaling Prometheus: IBMvideo

Cloud SecuritySysdig SecureCloud MonitoringIBM

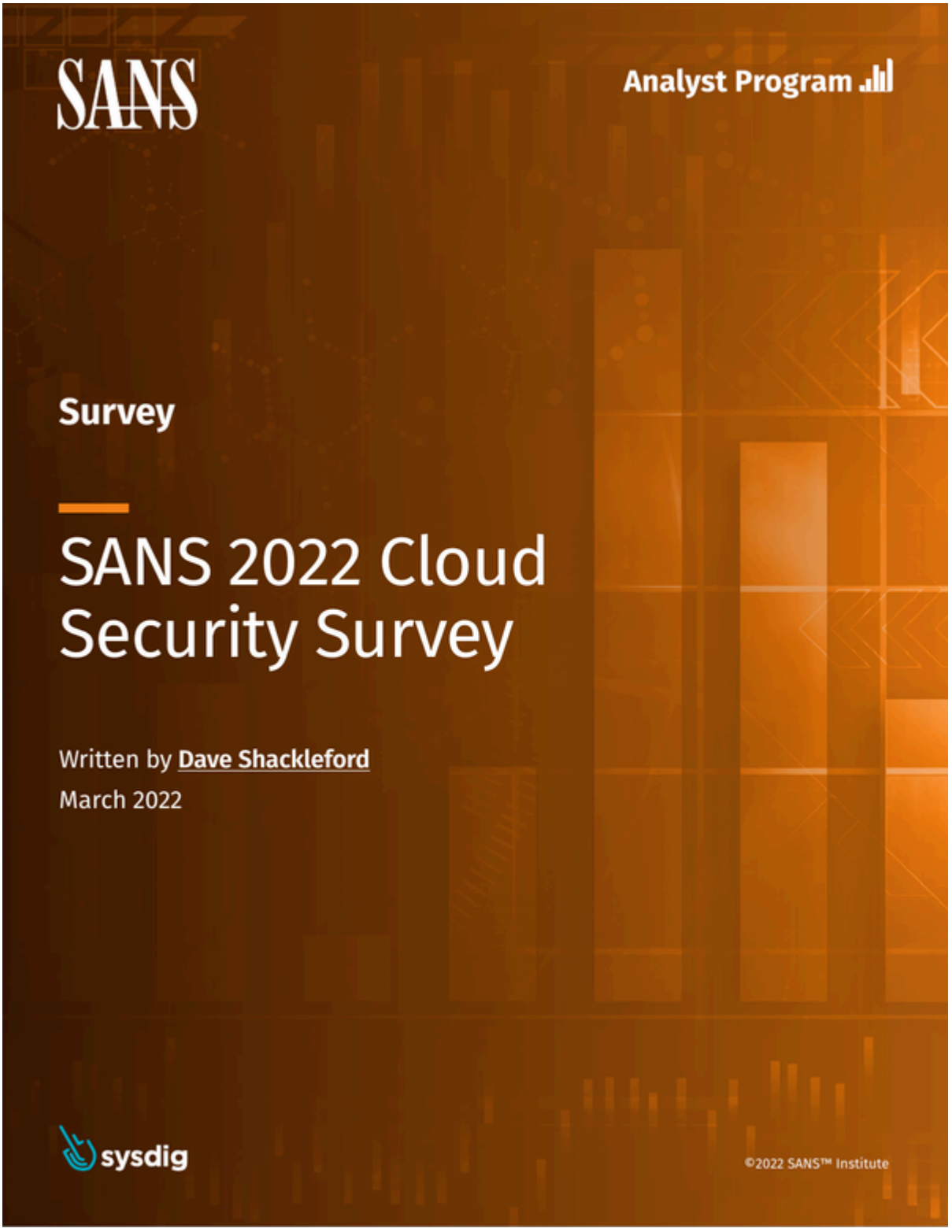

GUIDE. Using Runtime Insights For Effective Cloud Security with Sysdig and AWSpdf

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

sysdig

# 2022 Cloud-Native Threat Report

## EXECUTIVE SUMMARY

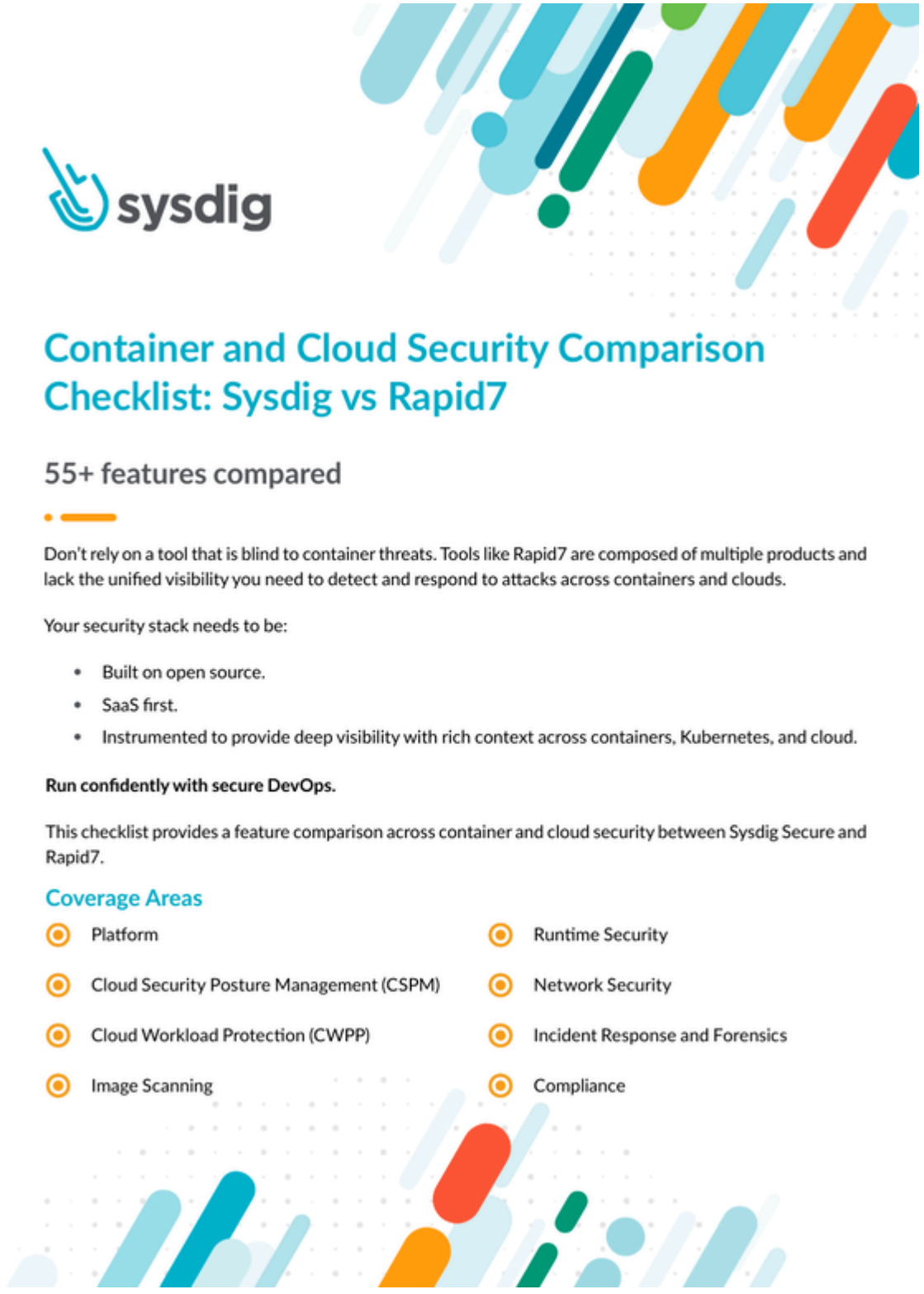
### Cloud Adversary Analysis: TeamTNT

**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 Summarypdf

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 CISOspdf

Cloud SecuritySysdig Secure


REPORT. 2024 Global Threat Reportpdf

Cloud SecurityCloud Threats

# A guide to PCI Compliance in Containers and Kubernetes


GUIDE. A guide to PCI Compliance in Containers and Kubernetespdf

Sysdig Secure

sysdig

CASE STUDY


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

**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 trial 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
from FIS

## 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

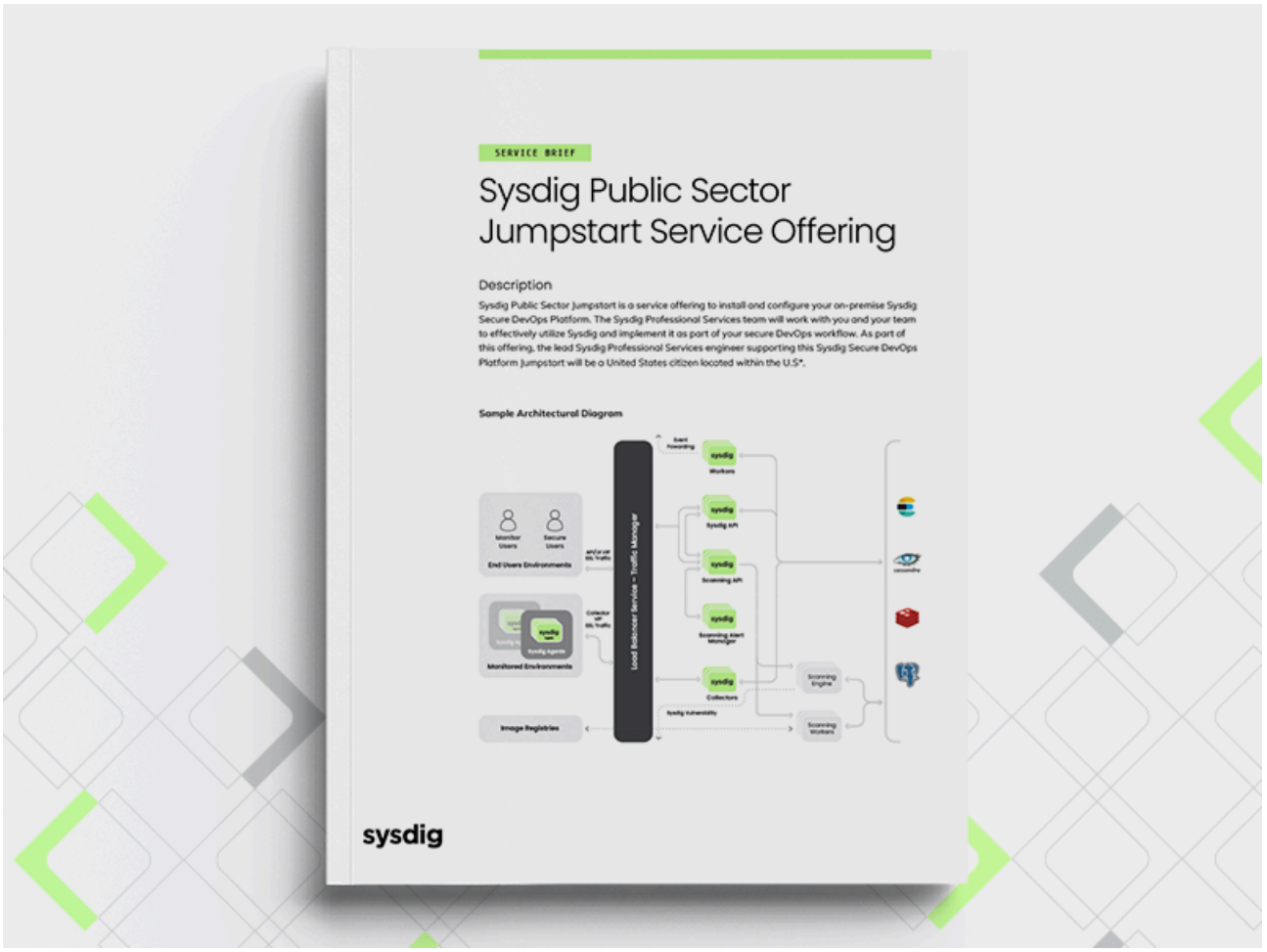
Sysdig SecureSysdig Monitor


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]


PRODUCT BRIEF. Sysdig Securepdf

Sysdig Secure

IDC ANALYZE THE FUTURE

**IDC WORKBOOK**

*Sponsored by: Sysdig*

**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

**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.

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."

IDC. Definitive Guide for Evaluating Container and Kubernetes Security Toolspdf

Sysdig SecureKubernetes


SOLUTION BRIEF. Sysdig and Microsoft Azurepdf

Azure

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

[Sysdig SecureSysdig Monitor]

SERVICE BRIEF

Admissions Controller Service Offering

Description

This service offering will provide a dedicated Sysdig Professional Services resource to assist in implementing the Sysdig Admissions Controller in the customer's Kubernetes/Openshift environment.

Expected engagement time

This engagement typically requires two-to-three days of professional services.

Process we follow

01 **Conduct scoping call**
A Sysdig Professional Services engineer will conduct this call in order to gather the requirements for the engagement.

02 **Perform deployment**
A Sysdig Professional Services engineer will work in tandem with your on-site engineer to guide them through the necessary steps to deploy the Admissions Controller.

03 **Perform post-deployment checks**
A Sysdig Professional Services engineer will ensure that the deployment was successful and verify full functionality.

04 **Provide detailed documentation**
Sysdig Professional Services will provide detailed documentation, in the form of an Engagement journal, that outlines the steps taken throughout the engagement, the configuration applied, and information about your environments.

Terms and Conditions

- Sysdig will provide the professional services purchased hereunder ("Services") in accordance with these terms. Further, the Services are subject to the terms and conditions governing your use of Sysdig's products and services. See your Order Form for more details.
- Services shall be scheduled in no fewer than four (4) hour increments.
- Services expire if not used within 12 calendar months of the effective date of the order.
- You must reimburse us for reasonable travel expenses if we jointly determine an onsite presence is required.
- We reserve the right, in our commercially reasonable discretion, to change or otherwise substitute resources during the course of the engagement.
- If Sysdig Professional Services assistance is needed to upgrade to the latest generally available (GA) version of the Sysdig backend, an Upgrade/Expansion Service Offering will need to be purchased separately.

sysdig

COPYRIGHT © 2022-2024
SYSDIG, INC.
ALL RIGHTS RESERVED.

SYS-PS-ADM-CONT REV. C 5/24

SERVICE BRIEF. Admissions Controllerpdf

Sysdig SecureSysdig Monitor

sysdig

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


# 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

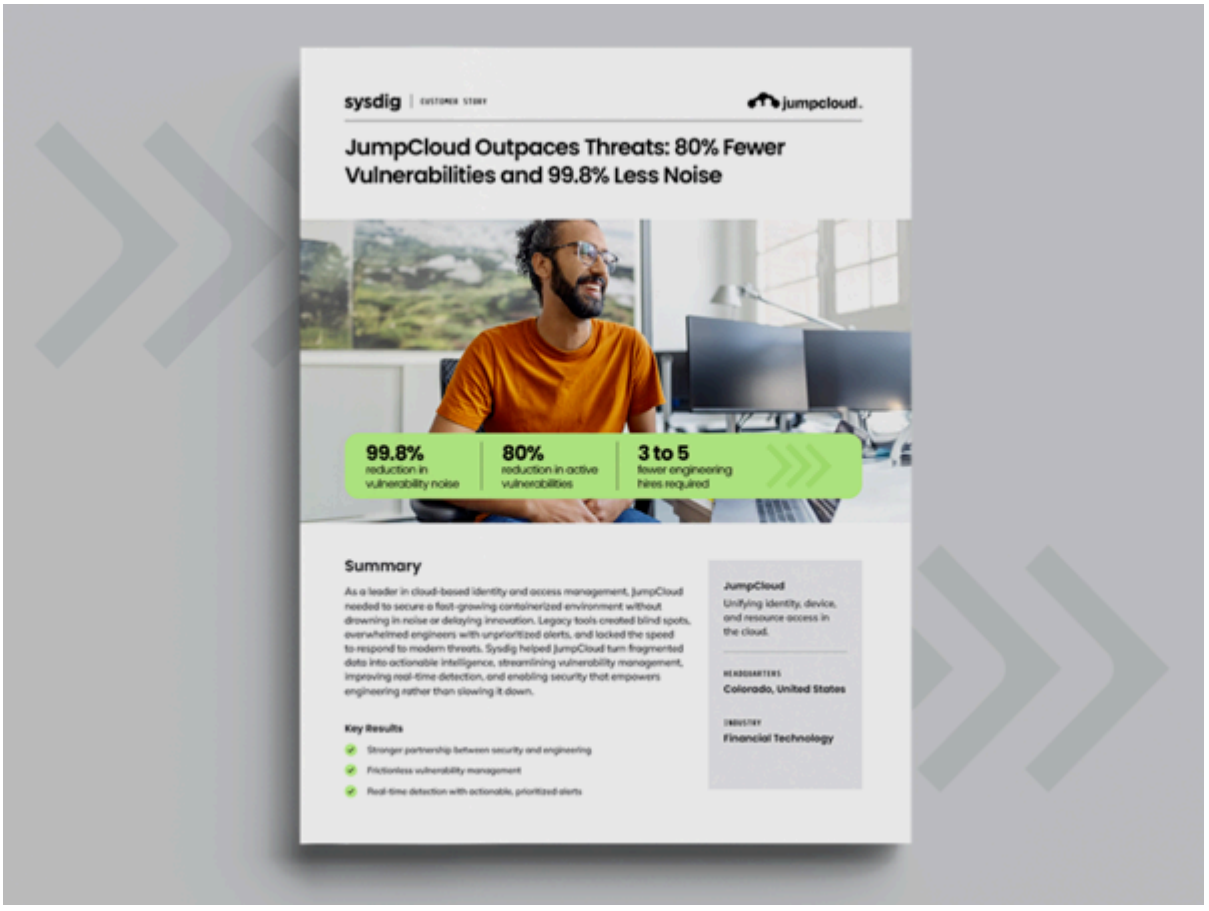
Building microservices at SAP Concur started with a small tiger team. As Mike Luedke, Director Engineering at SAP Concur explained, “We started off as a grassroots effort. There were a few of us from different teams that got started originally building a cluster. Eventually, we then opened that up to 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

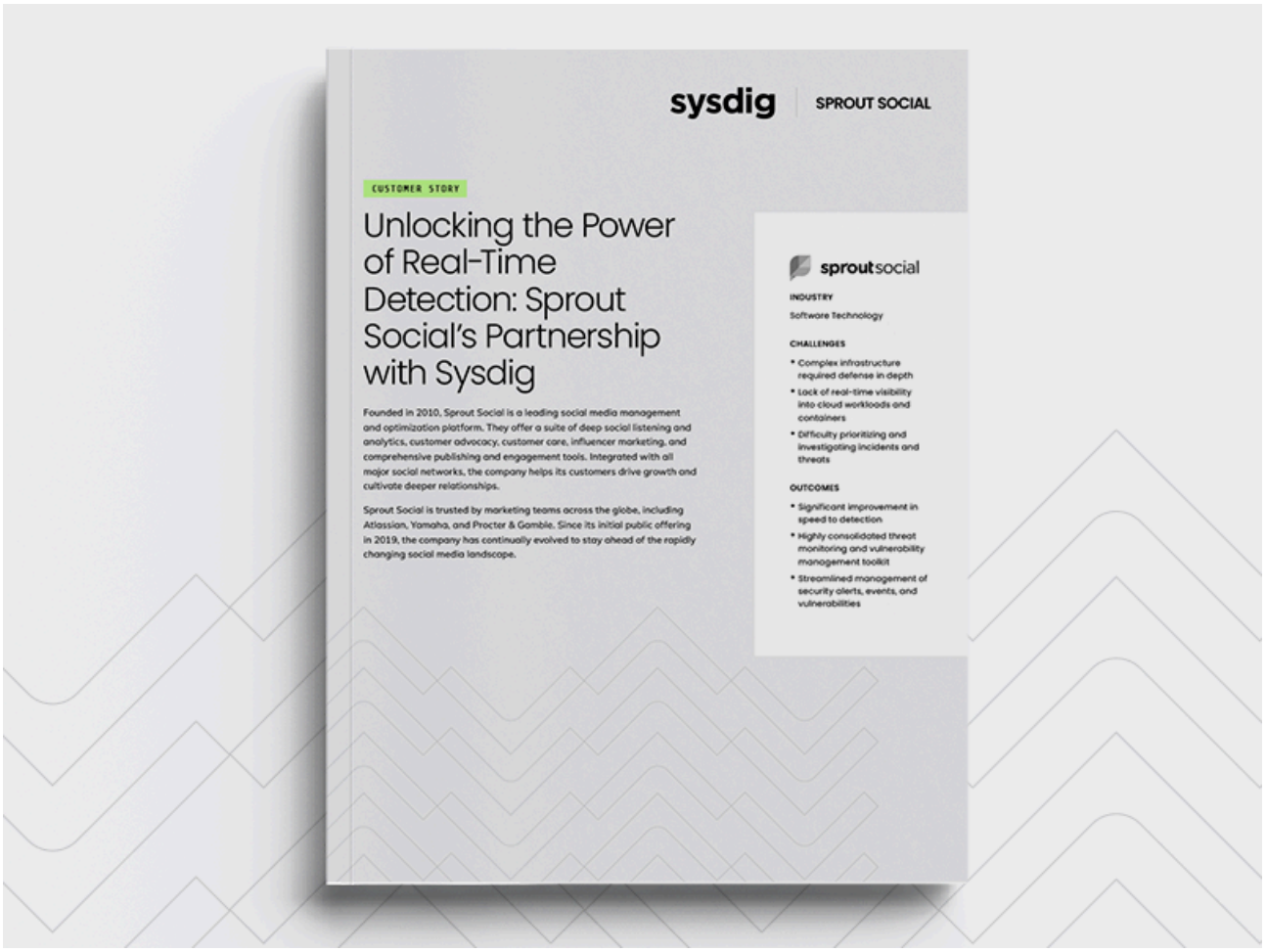

CASE STUDY. Goldman Sachs Accelerating Business with Microservicespdf

Sysdig Secure




Jump Cloud Sysdig Customer Storypdf

Sysdig Secure




CASE STUDY. Unlocking the Power of Real-Time Detection: Sprout Social's Partnership with Sysdigpdf

Cloud Security


BRIEF: Cloud and Container Security for Software & Technology Servicespdf

Cloud SecurityCloud Monitoring


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

[Docker]


BRIEF: Top Business Impacts Of Cloud Breaches And How To Mitigate Thempdf

Cloud SecurityCloud Monitoring

sysdig

# 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[1]

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


money and time."
IT Security Manager
Leader in Bot Mitigation
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[2]
3.5x
increase in web app and API attacks in the financial services sector in 2022[3]
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[4]
87%
say open source is valuable to the future
6
Use Open Standards
Ensure transparency,

services industry[5]

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?

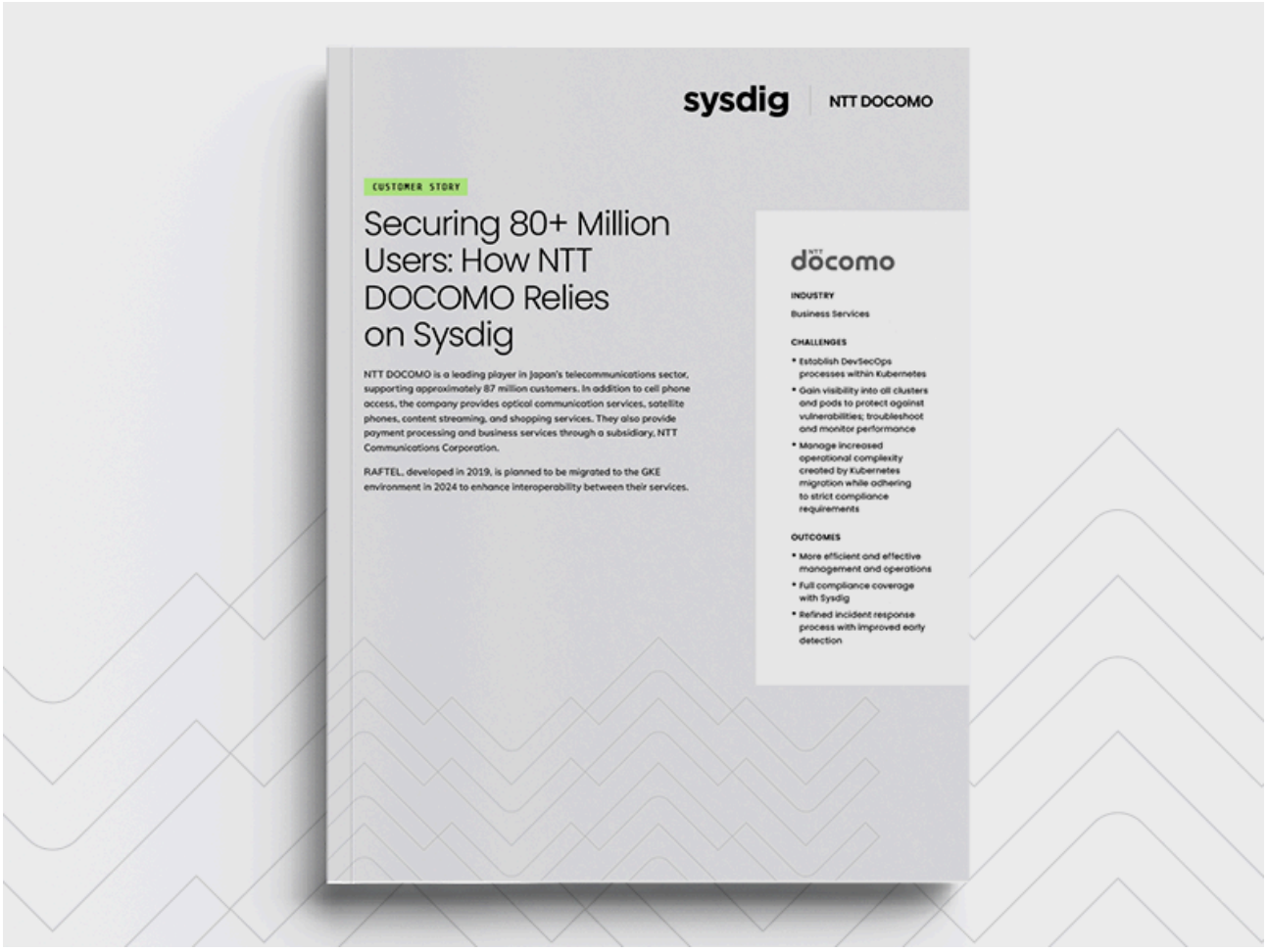
Defend against advanced threats while delivering a standout customer experience. Book your personalized live demo with a Sysdig expert today.

GET A DEMO

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

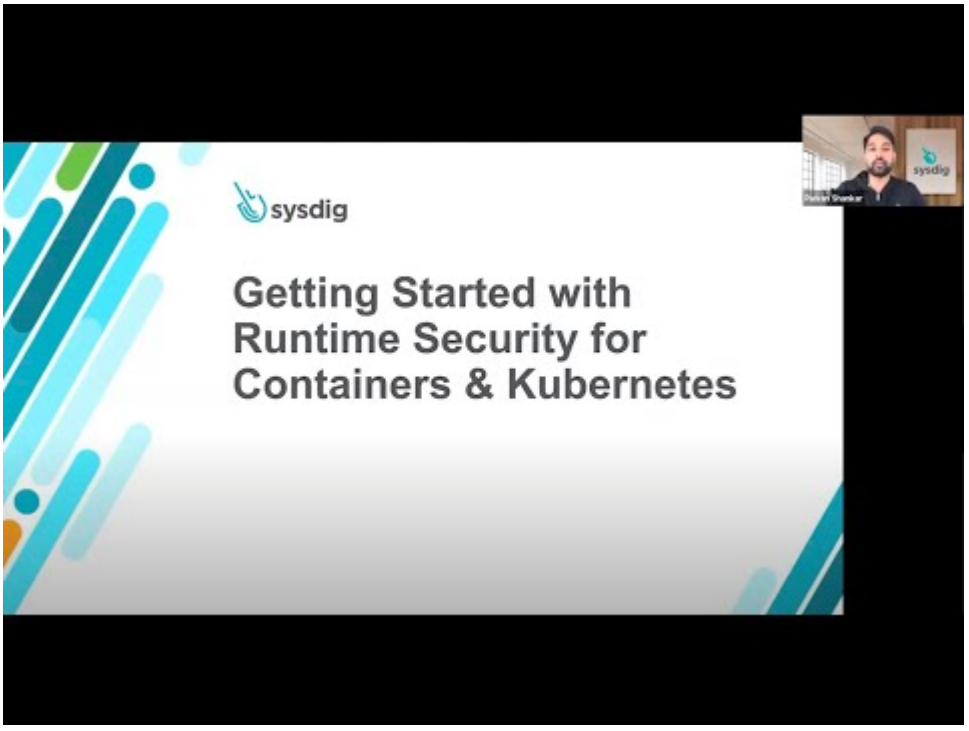
INFOGRAPHIC. 7 Cloud Security Requirements for Financial Service Providerspdf

Cloud Security



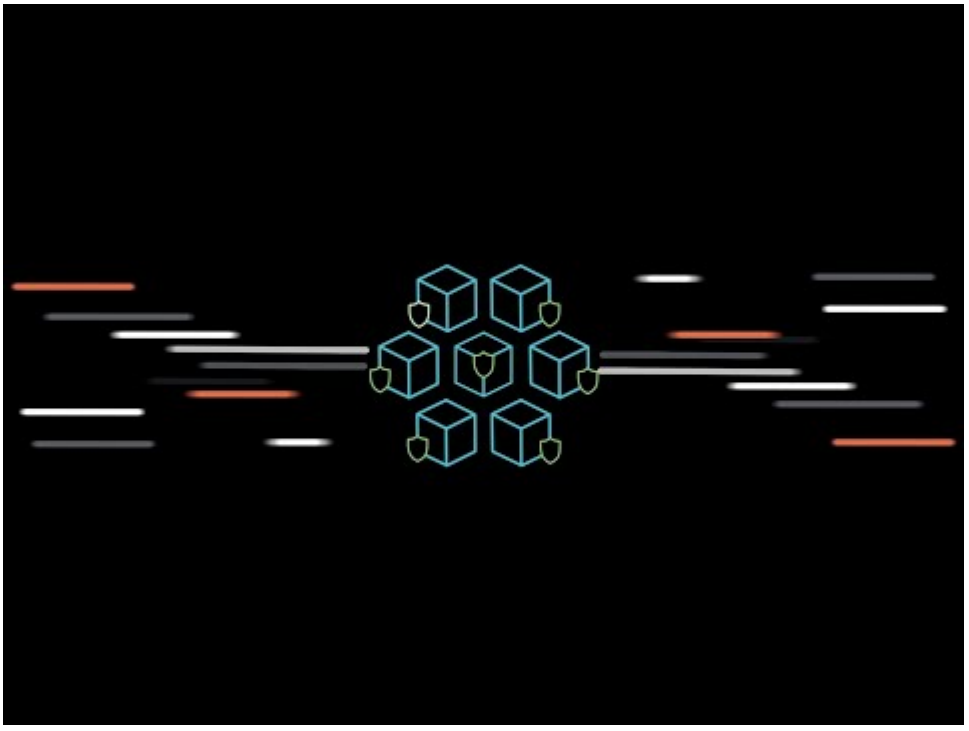

CASE STUDY. Securing 80+ Million Users: How NTT DOCOMO Relies on Sysdigpdf

Cloud Security




WEBINAR. Getting Started with Runtime Security for Containers & Kubernetesvideo

Cloud SecurityKubernetes



VIDEO. Sysdig Secure Overviewvideo

Sysdig Secure

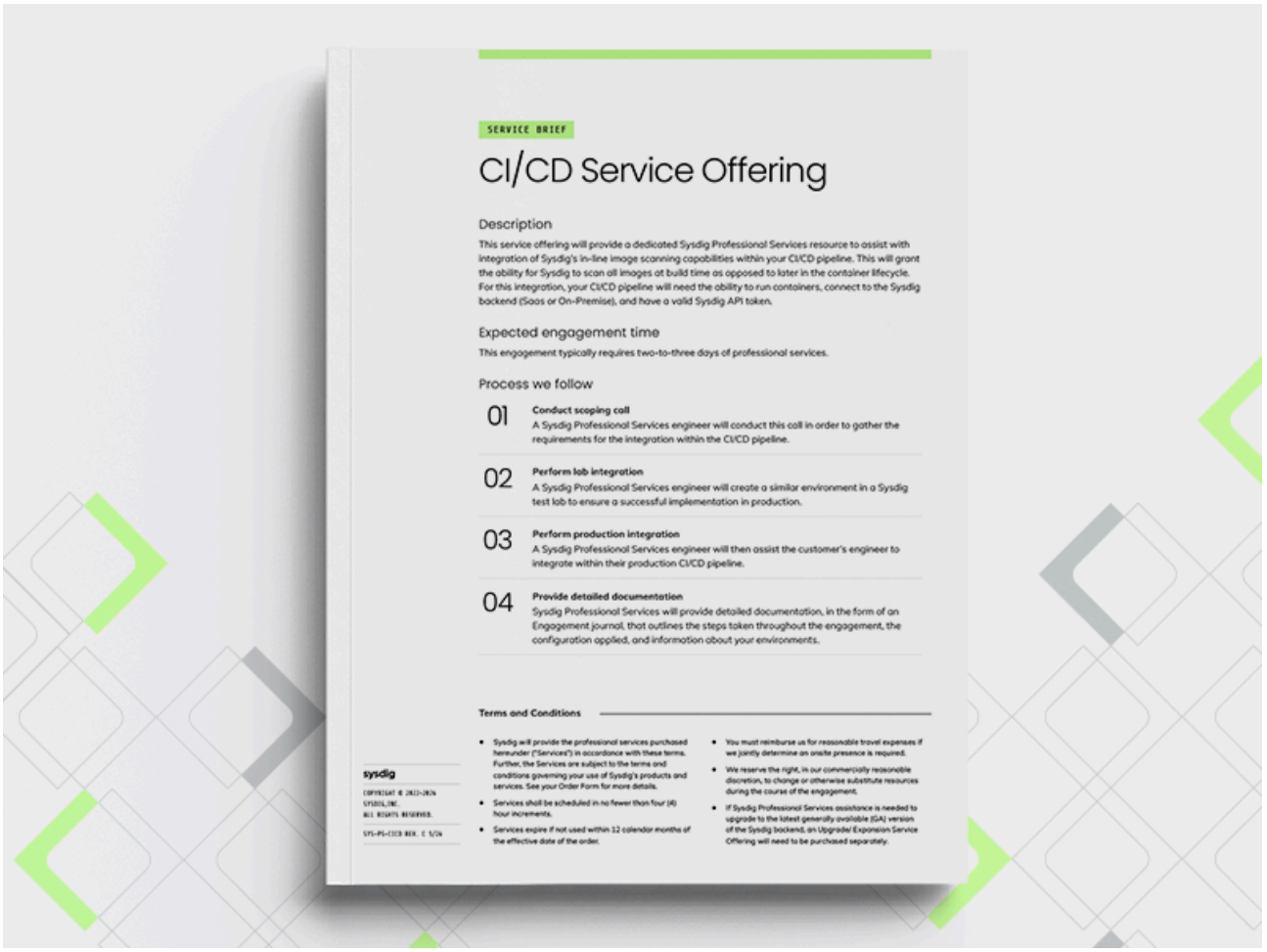
CASE STUDY

# 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/CD Service Offering

## Description

This service offering will provide a dedicated Sysdig Professional Services resource to assist with integration of Sysdig's in-line image scanning capabilities within your CI/CD pipeline. This will grant the ability for Sysdig to scan all images at build time as opposed to later in the container lifecycle. For this integration, your CI/CD pipeline will need the ability to run containers, connect to the Sysdig backend (Saas or On-Premise), and have a valid Sysdig API token.

## Expected engagement time

This engagement typically requires two-to-three days of professional services.

## Process we follow

01 **Conduct scoping call**
A Sysdig Professional Services engineer will conduct this call in order to gather the requirements for the integration within the CI/CD pipeline.

02 **Perform lab integration**
A Sysdig Professional Services engineer will create a similar environment in a Sysdig test lab to ensure a successful implementation in production.

03 **Perform production integration**
A Sysdig Professional Services engineer will then assist the customer's engineer to integrate within their production CI/CD pipeline.

04 **Provide detailed documentation**
Sysdig Professional Services will provide detailed documentation, in the form of an Engagement journal, that outlines the steps taken throughout the engagement, the configuration applied, and information about your environments.

## Terms and Conditions

- Sysdig will provide the professional services purchased hereunder ("Services") in accordance with these terms. Further, the Services are subject to the terms and conditions governing your use of Sysdig's products and services. See your Order Form for more details.
- Services shall be scheduled in no fewer than four (4) hour increments.
- Services expire if not used within 12 calendar months of the effective date of the order.
- You must reimburse us for reasonable travel expenses if we jointly determine an onsite presence is required.
- We reserve the right, in our commercially reasonable discretion, to change or otherwise substitute resources during the course of the engagement.
- If Sysdig Professional Services assistance is needed to upgrade to the latest generally available (GA) version of the Sysdig backend, an Upgrade/ Expansion Service Offering will need to be purchased separately.

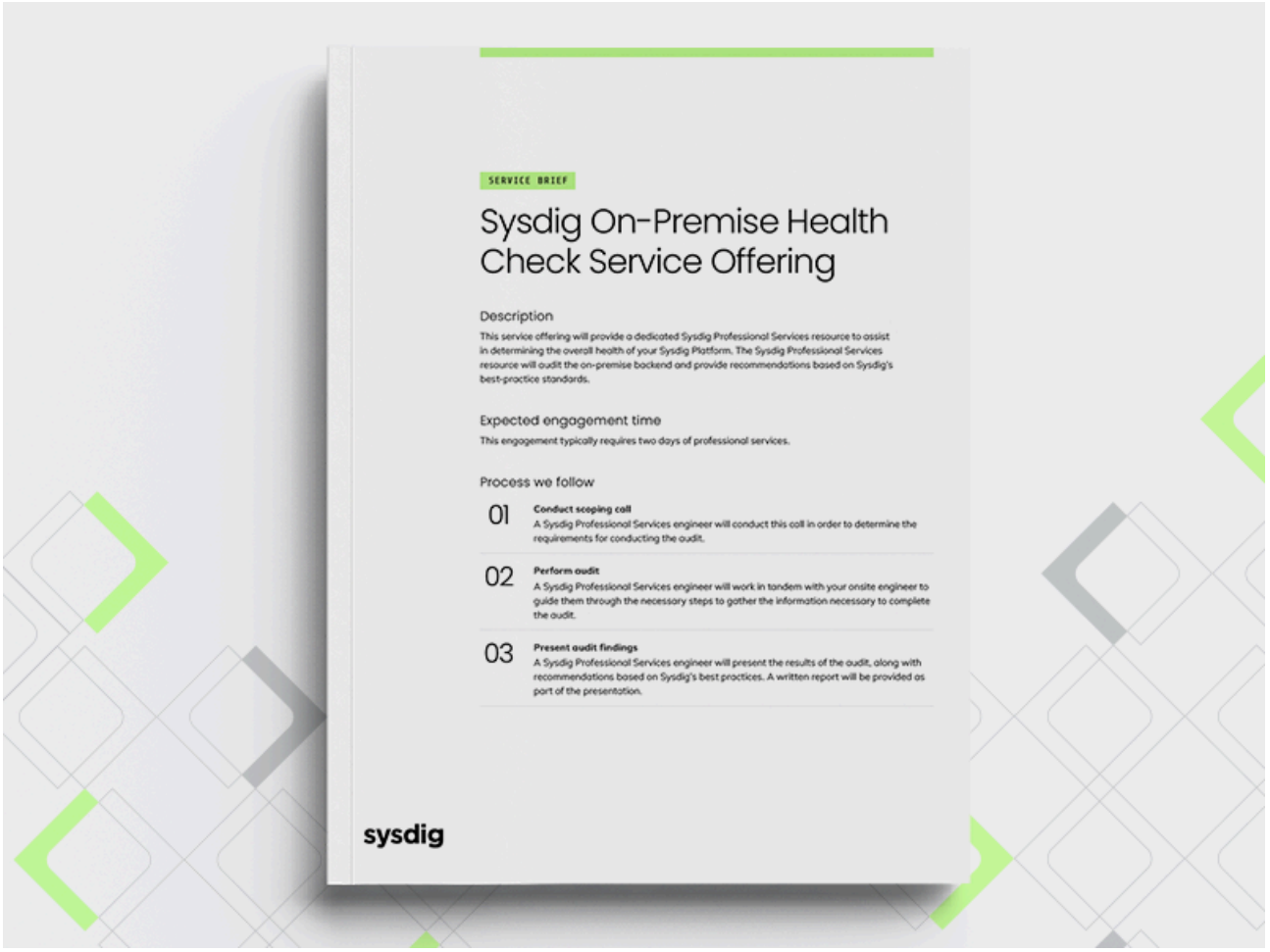
sysdig

COPYRIGHT © 2021-2024
SYSDIG, INC.
ALL RIGHTS RESERVED.

SYS-PS-CICD REV. C 5/24

[SERVICE BRIEF. CI/CDpdf]

[Sysdig SecureSysdig Monitor]

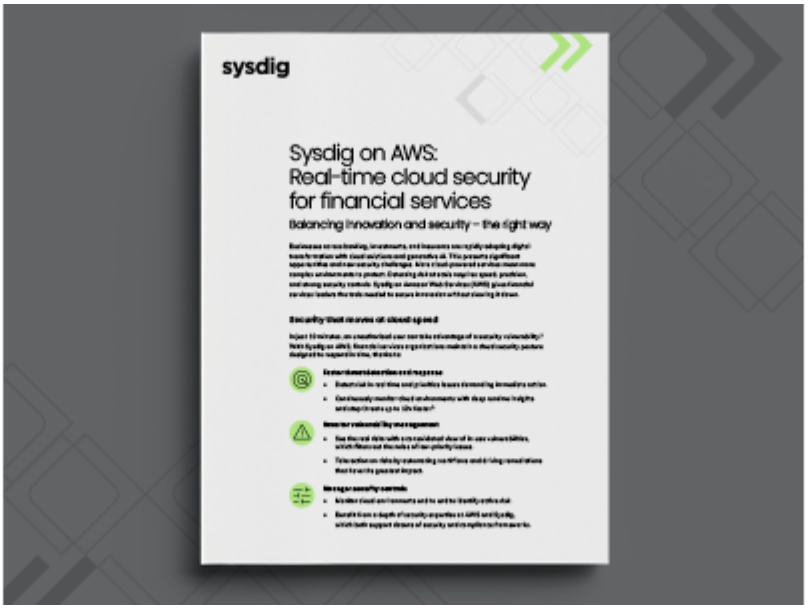



SERVICE BRIEF. On-Premise Health Checkpdf

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

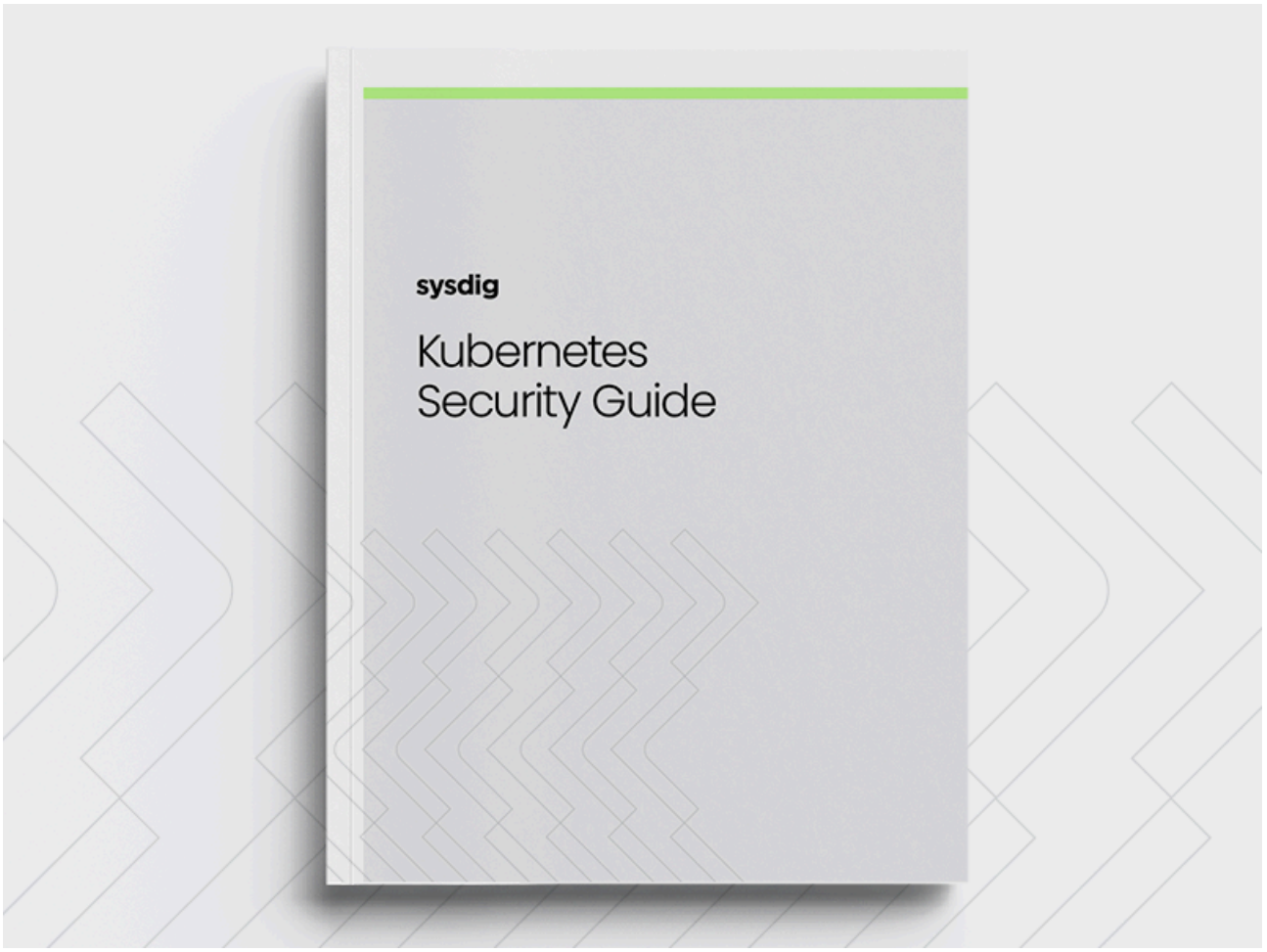
Cloud Security


BRIEF. Frost Sullivan Award 2022pdf

Sysdig Secure

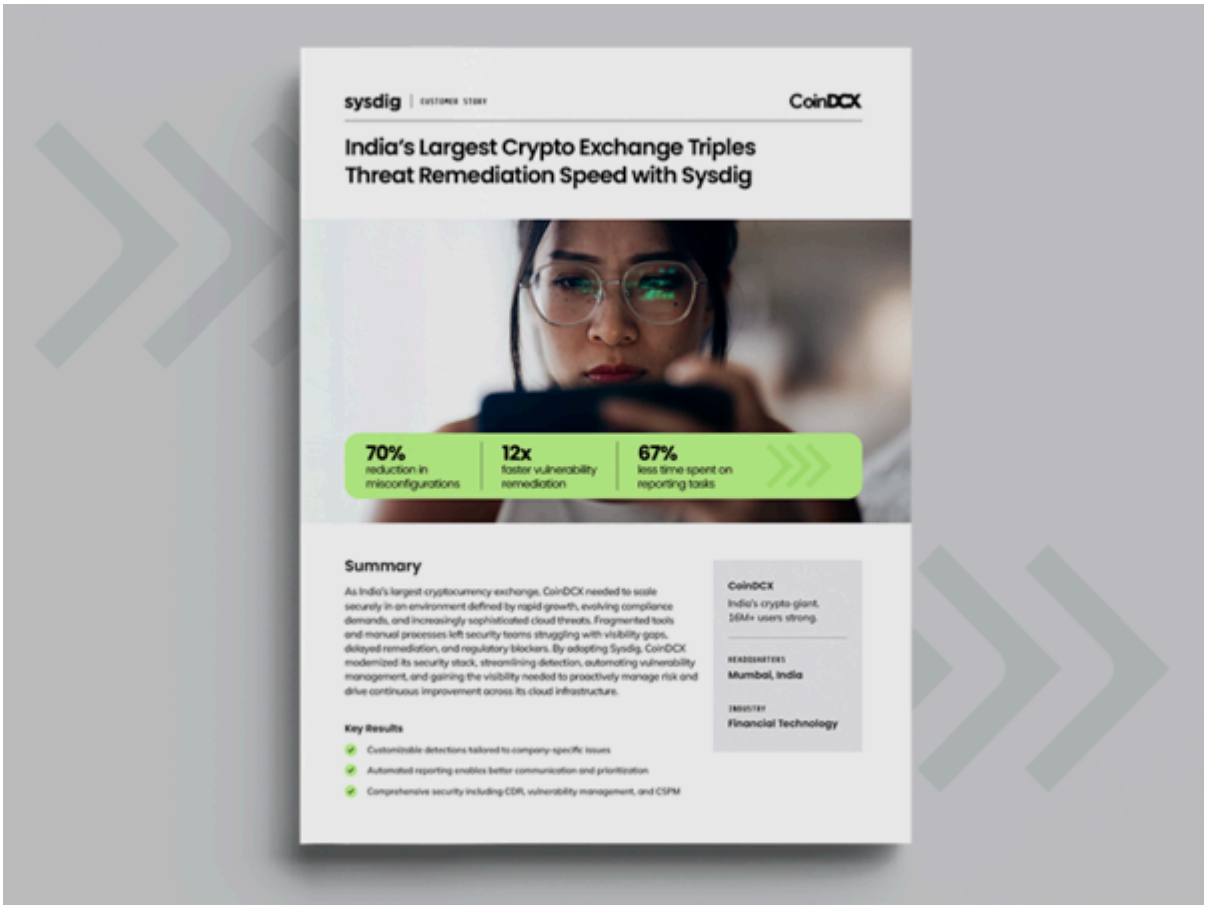
VIDEO. Attack Path & Risk Findingsvideo

Cloud Security




GUIDE. Kubernetes Security Guidepdf

Sysdig SecureKubernetes




CASE STUDY. CoinDCXpdf

AWSAmazon Web ServicesCSPMCryptomining

GigaOm Radar 2024 - Cloud Workload Security (CWS)webpage

Cloud SecurityCloud MonitoringCloud computing security

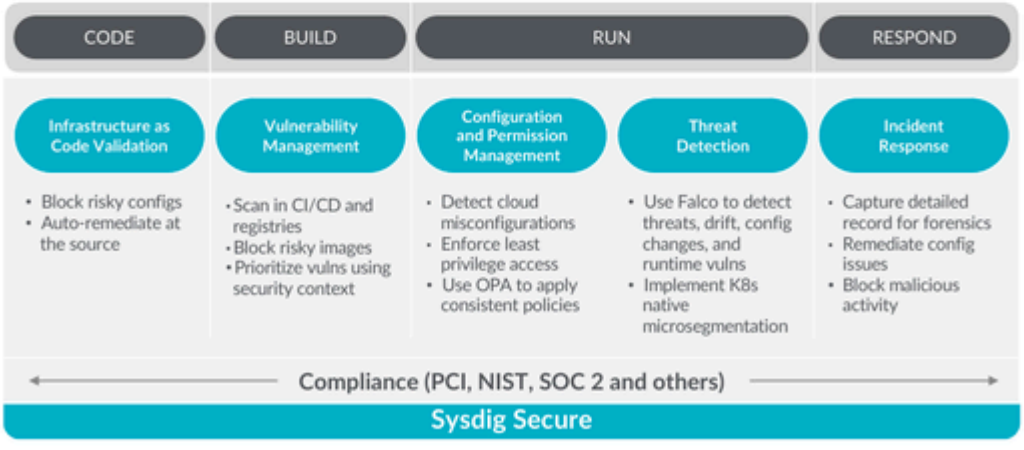

When migrating apps to the cloud or developing in modern cloud-native environments, organizations struggle to put together a security plan and get the visibility required to manage security risk, continuously meet and validate compliance, as well as implement real-time protection across cloud and containers.

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






USE CASE. Top 10 Use Cases for the Sysdig Platformpdf

Sysdig SecureKubernetesSysdig Monitor

sysdig

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."

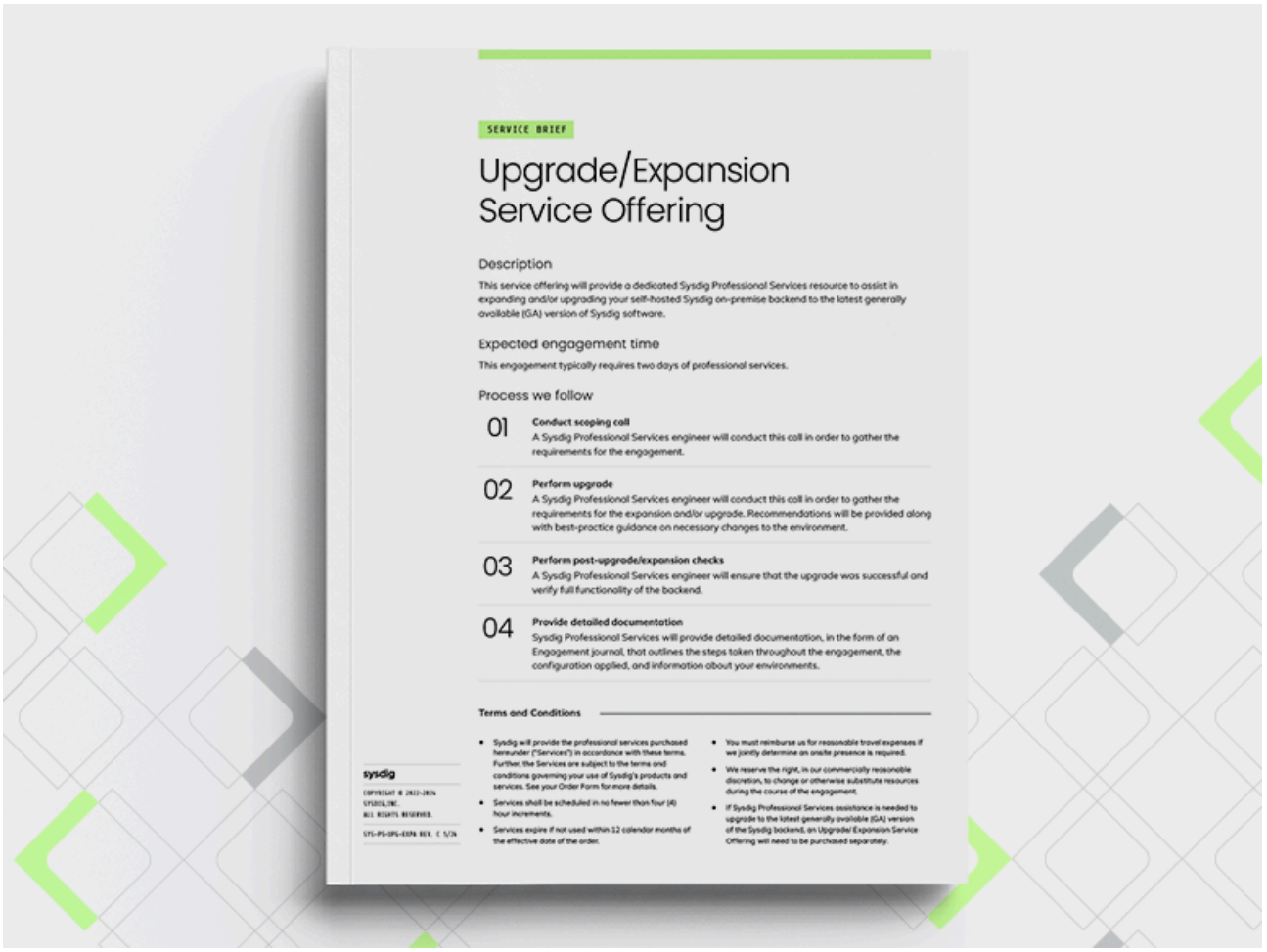
## Security is top priority

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

BEEKEEPER

[CASE STUDY. Beekeeper Serves Up Secure Communications, Data, and Applications Across Cloud Environmentspdf]

[Sysdig SecureSysdig Monitor]



SERVICE BRIEF

# Upgrade/Expansion Service Offering

## Description

This service offering will provide a dedicated Sysdig Professional Services resource to assist in expanding and/or upgrading your self-hosted Sysdig on-premise backend to the latest generally available (GA) version of Sysdig software.

## Expected engagement time

This engagement typically requires two days of professional services.

## Process we follow

01 **Conduct scoping call**
A Sysdig Professional Services engineer will conduct this call in order to gather the requirements for the engagement.

02 **Perform upgrade**
A Sysdig Professional Services engineer will conduct this call in order to gather the requirements for the expansion and/or upgrade. Recommendations will be provided along with best-practice guidance on necessary changes to the environment.

03 **Perform post-upgrade/expansion checks**
A Sysdig Professional Services engineer will ensure that the upgrade was successful and verify full functionality of the backend.

04 **Provide detailed documentation**
Sysdig Professional Services will provide detailed documentation, in the form of an Engagement journal, that outlines the steps taken throughout the engagement, the configuration applied, and information about your environments.

## Terms and Conditions

- Sysdig will provide the professional services purchased hereunder ("Services") in accordance with these terms. Further, the Services are subject to the terms and conditions governing your use of Sysdig's products and services. See your Order Form for more details.
- Services shall be scheduled in no fewer than four (4) hour increments.
- Services expire if not used within 12 calendar months of the effective date of the order.
- You must reimburse us for reasonable travel expenses if we jointly determine an onsite presence is required.
- We reserve the right, in our commercially reasonable discretion, to change or otherwise substitute resources during the course of the engagement.
- If Sysdig Professional Services assistance is needed to upgrade to the latest generally available (GA) version of the Sysdig backend, an Upgrade/ Expansion Service Offering will need to be purchased separately.

sysdig

COPYRIGHT © 2021-2024
SYSDIG, INC.
ALL RIGHTS RESERVED.

SYS-PS-SPS-EXPA REV. C 5/24

[SERVICE BRIEF. Upgrade And Expansionpdf]

[Sysdig SecureSysdig Monitor]


Evolution Of Cloud Security E Bookpdf

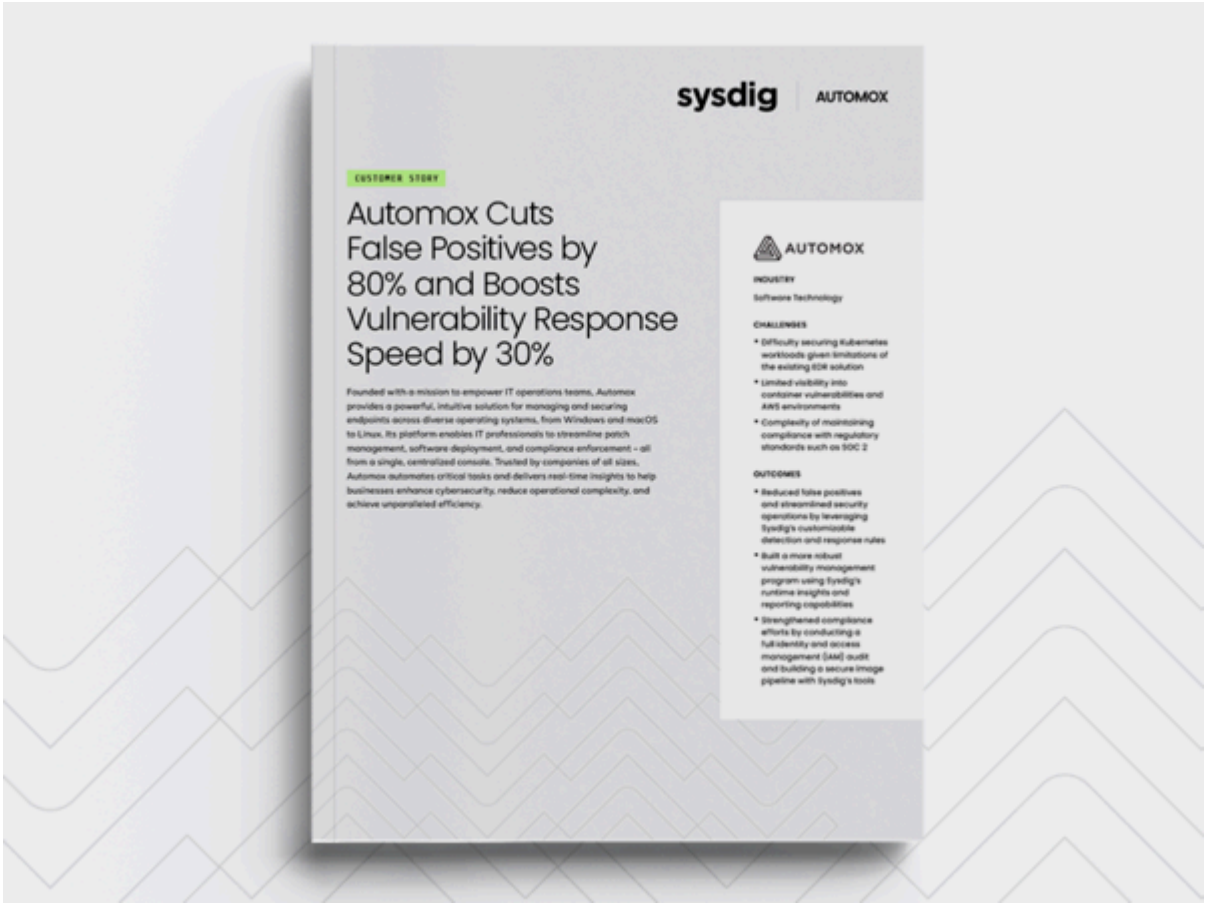
Cloud Security


BRIEF. 4 Ways Sysdig Enables Value with Cloud and Container Adoptionpdf

Cloud Security

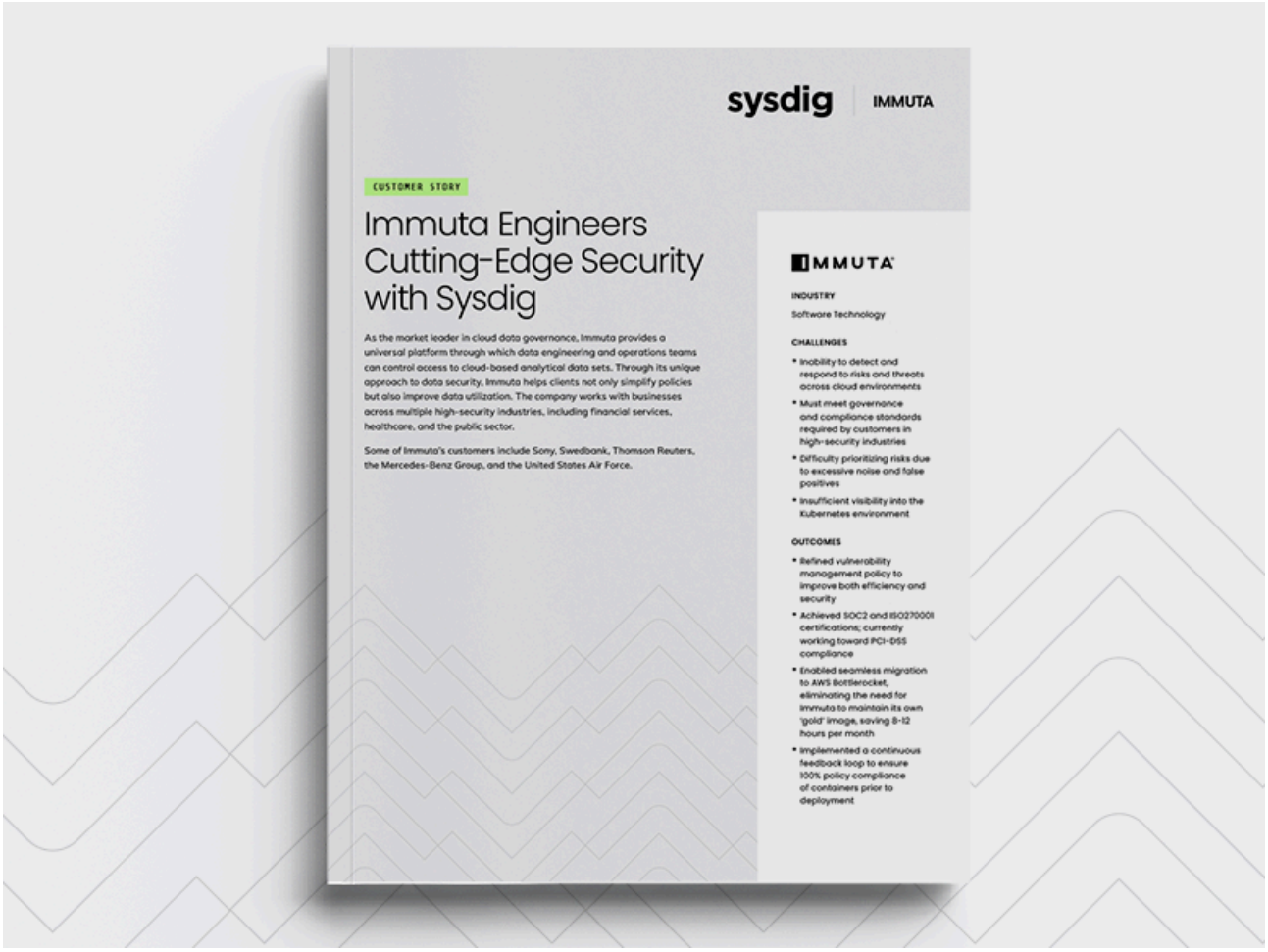

[CASE STUDY. UIDIApdf]

[Sysdig SecureCloud computing security]



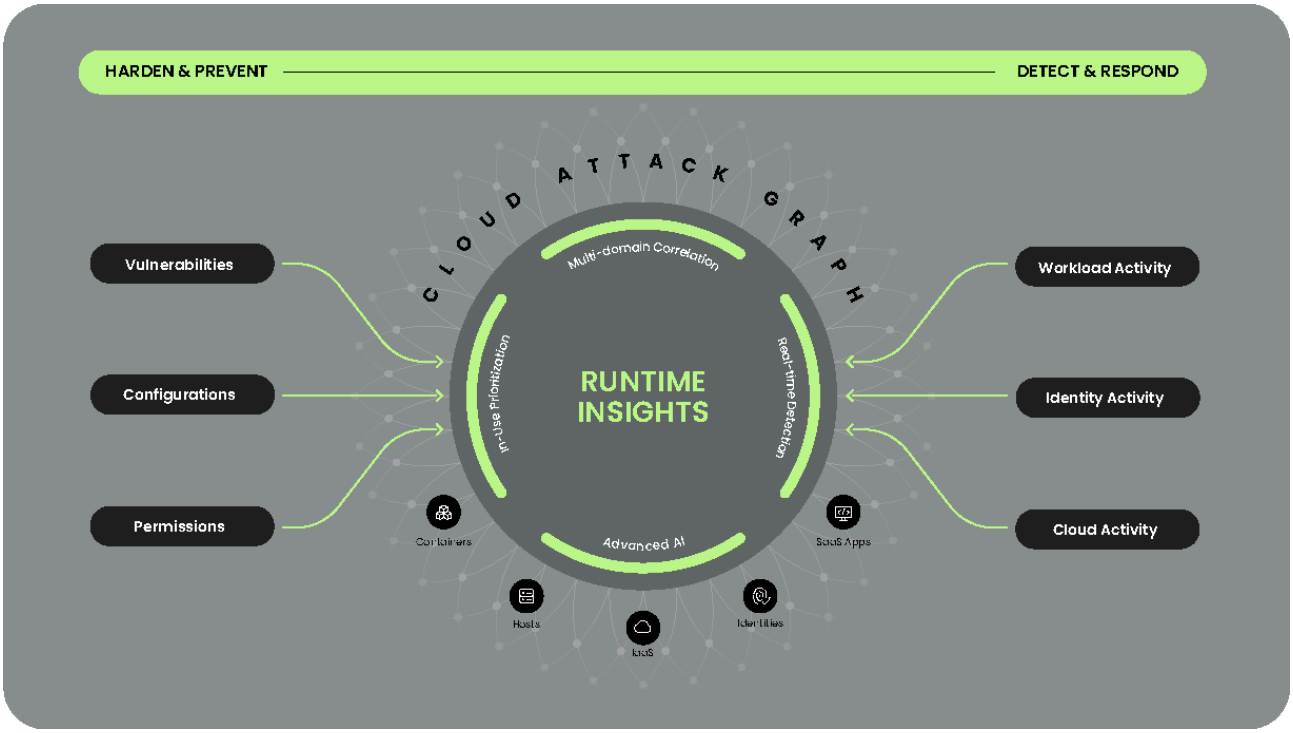

CASE STUDY. Automox Cuts False Positives by 80% and Boosts Vulnerability Response Speed by 30%pdf

Sysdig SecureAmazon Web Services




[Immuta Case Studypdf]

[Sysdig Secure]



VIDEO. Rethinking Cloud Security with a CNAPPvideo

Cloud Security

sysdig

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
BUSINESS PROCESS SOLUTIONS



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

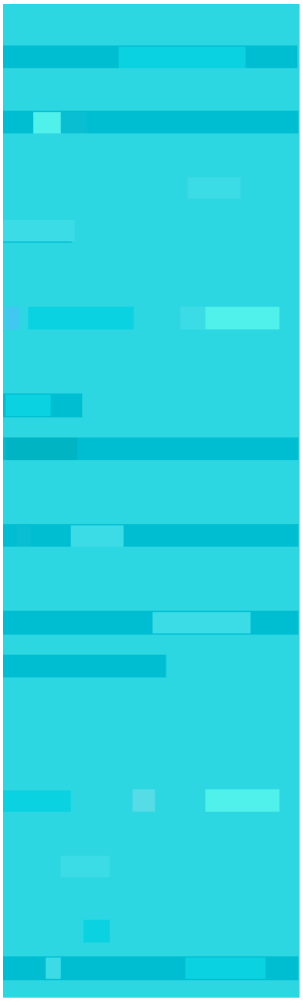
Since 1990, ICG Consulting has been a trusted expert in back-office applications, such as business process automation, advanced technology, and systems integration. As a result, the company has established a diverse book of clients, which includes major financial services organizations, energy companies, 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

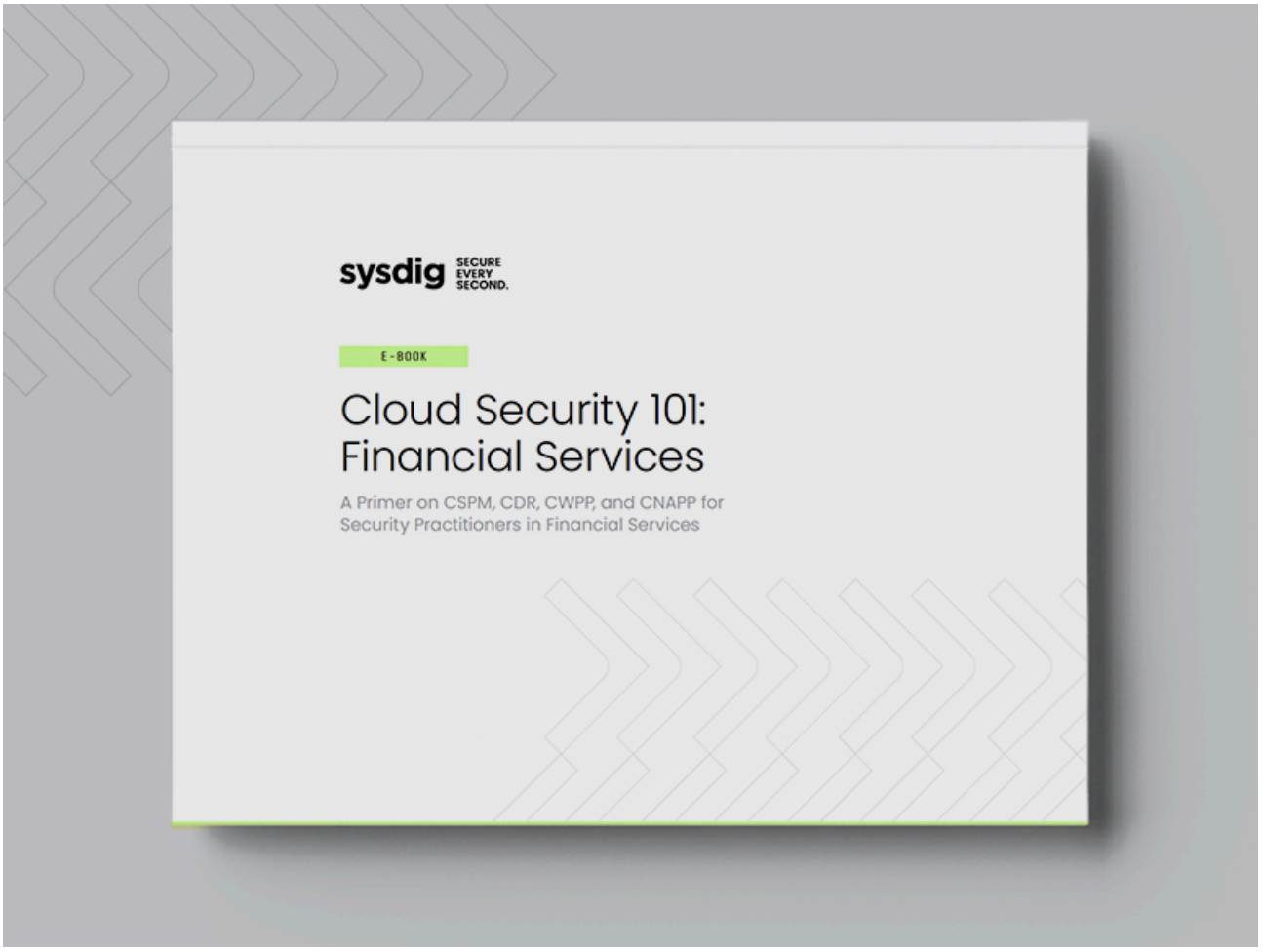



CASE STUDY. Quby: Monitor + Secure Java Apps on Mesos Marathonpdf

Sysdig SecureSysdig Monitor

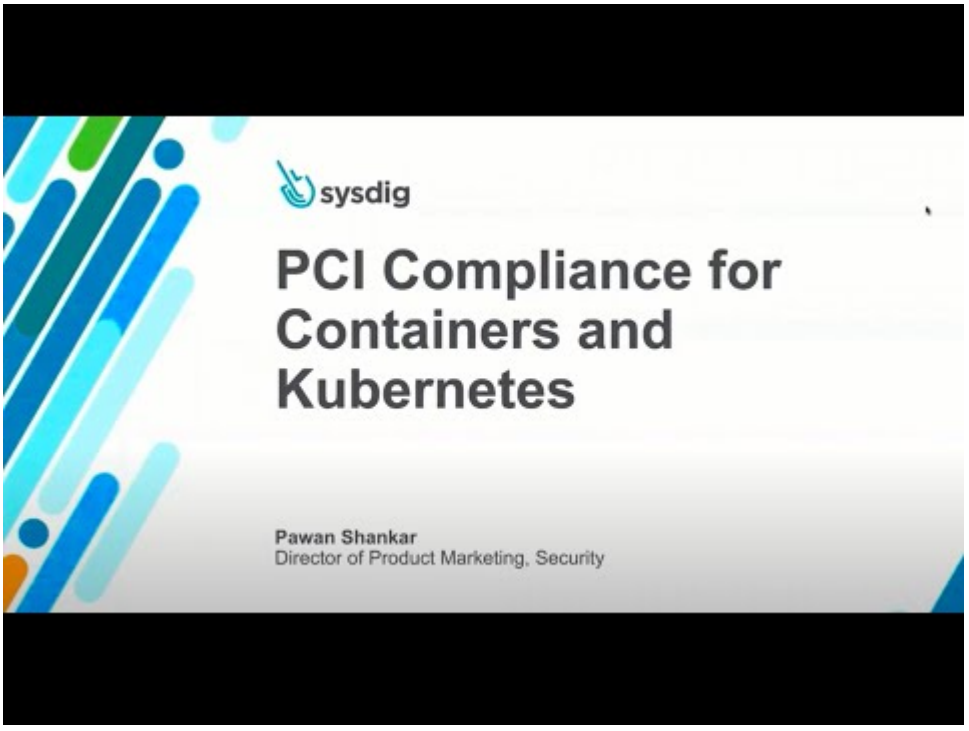

EBOOK. The Fast Track to Stronger Cloud Security in Financial Servicespdf

Cloud Security




GUIDE. Cloud Security 101 for Financial Servicespdf

Cloud Security




[WEBINAR. PCI Compliance in Containers & Kubernetesvideo]

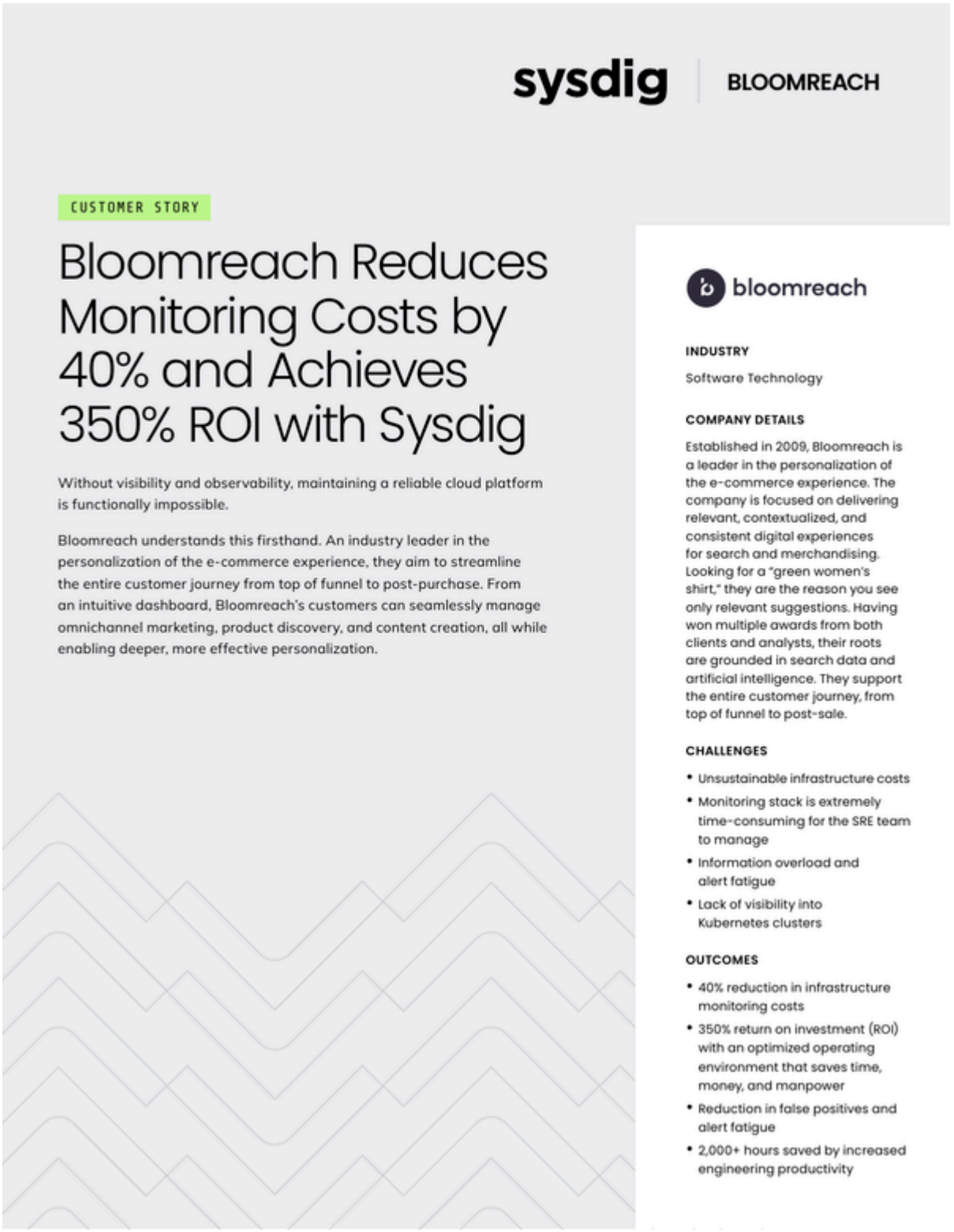
[Cloud Security]


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

[Cloud Security]

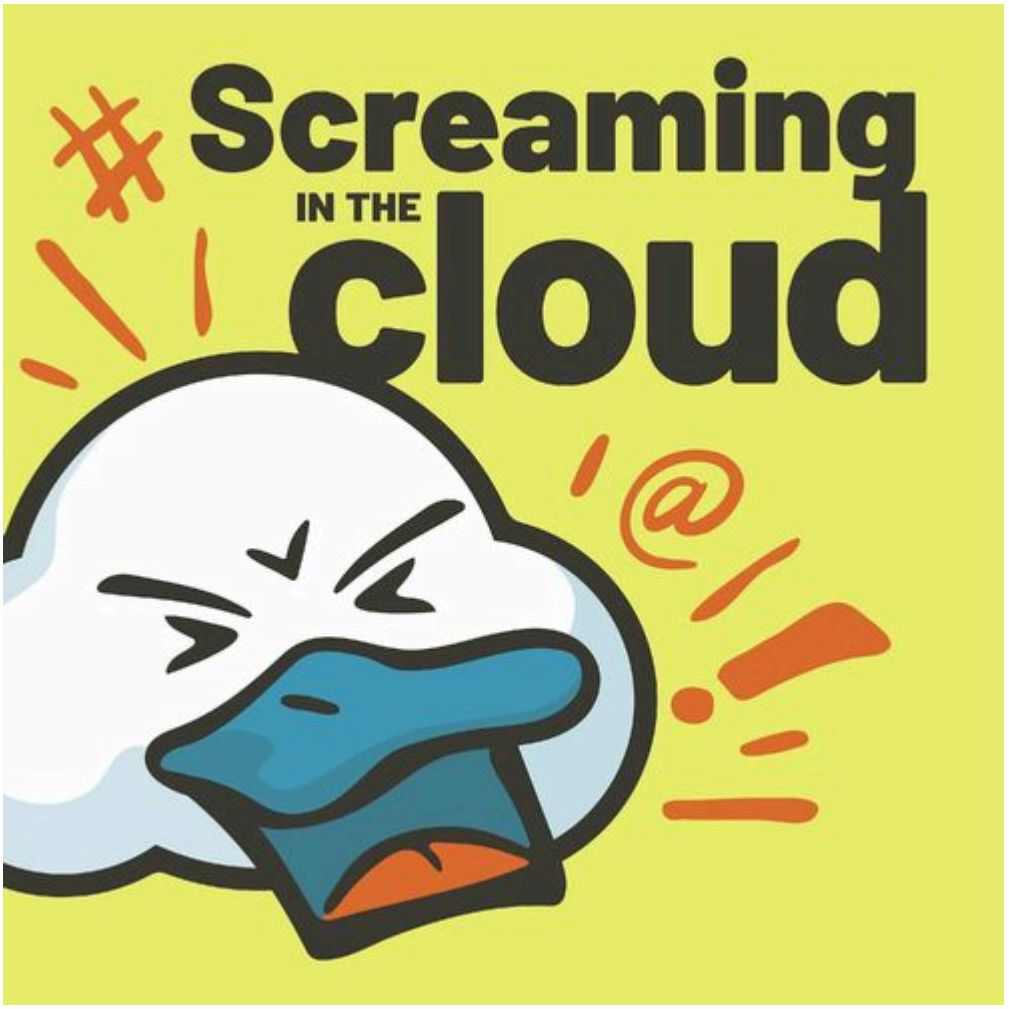

BRIEF. 6 Tips to Help Strengthen Financial Services Security in the Cloudpdf

Cloud SecurityCloud MonitoringCloud computing security



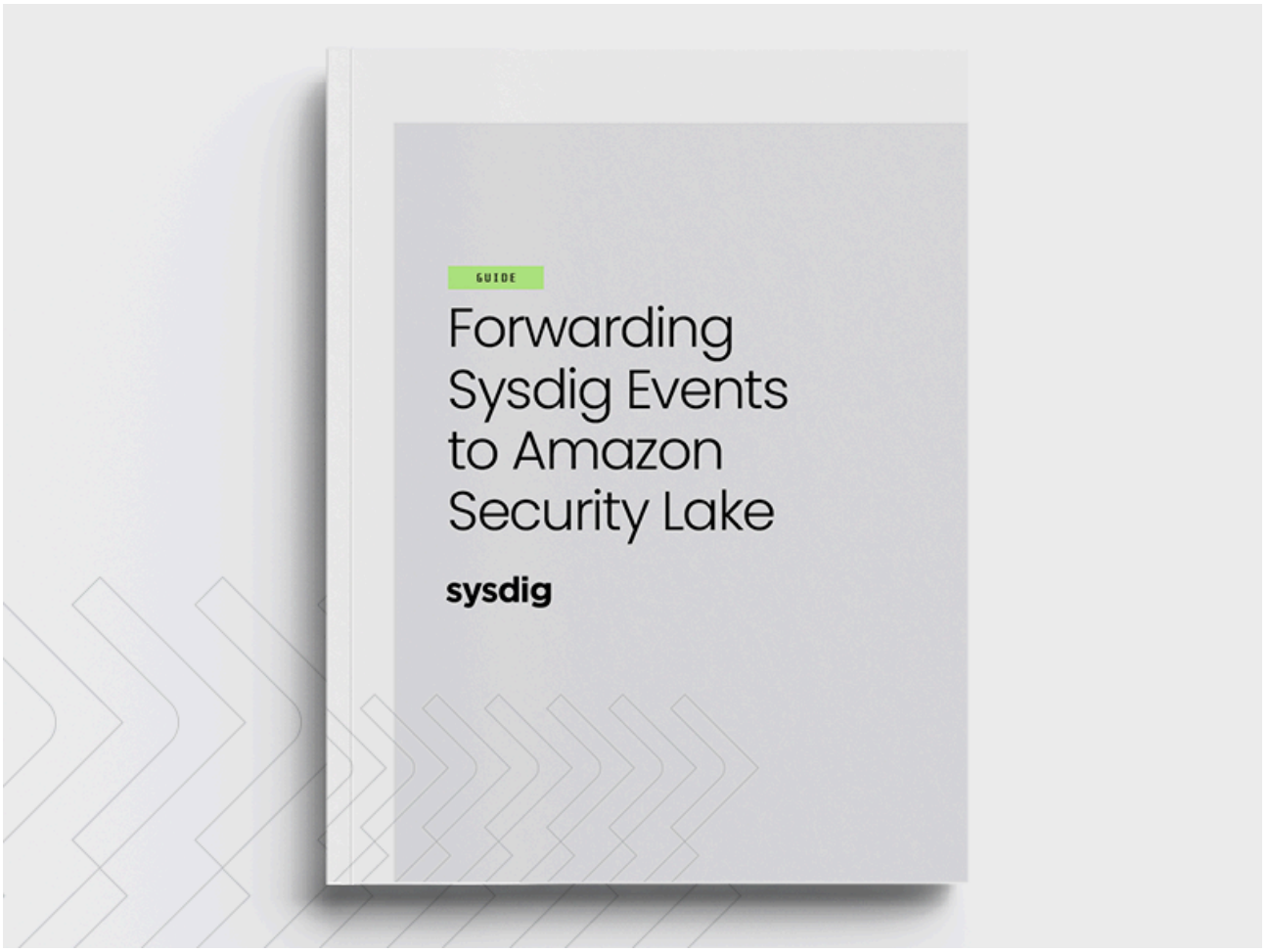

CASE STUDY. Bloomreachpdf

AWS



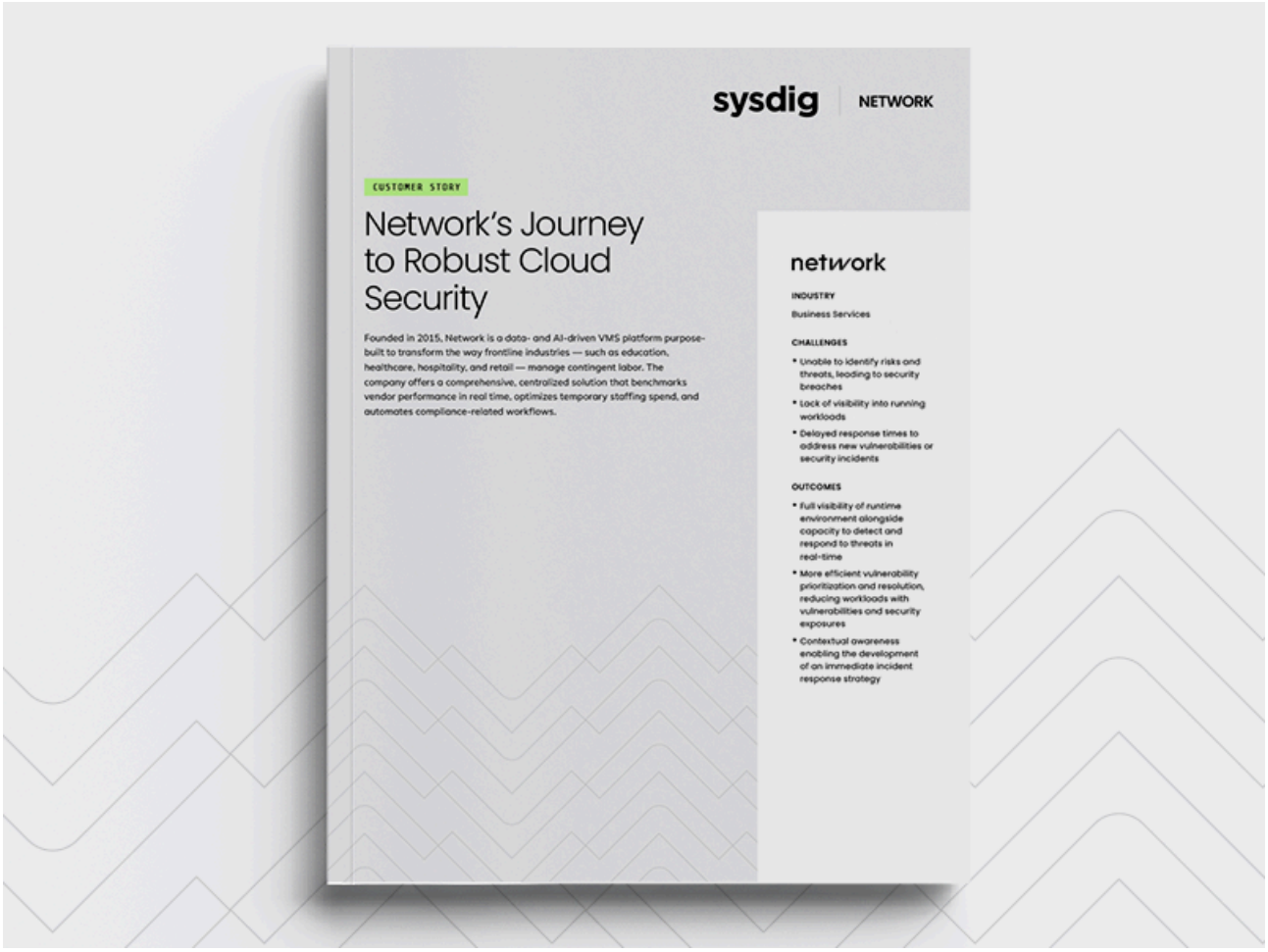

PODCAST. Screaming in the Cloud: Exposing The Latest Cloud Threatswebpage

Cloud Security



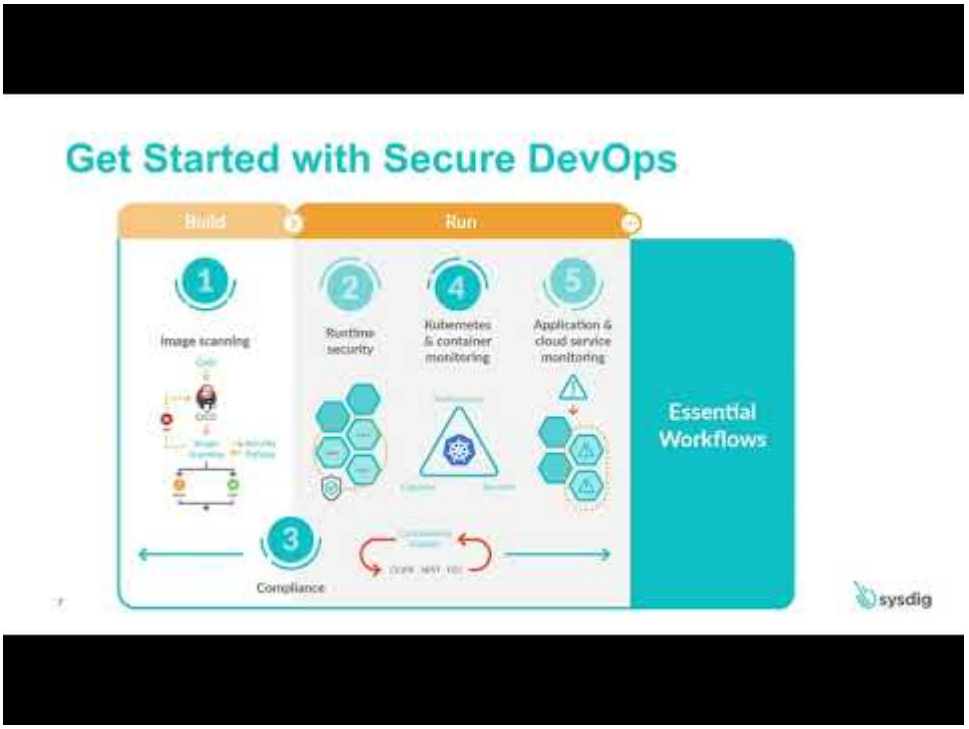

GUIDE. Forwarding Sysdig Events to Amazon Security Lakepdf

Cloud Security




[Network Case Studypdf]

[Sysdig Secure]

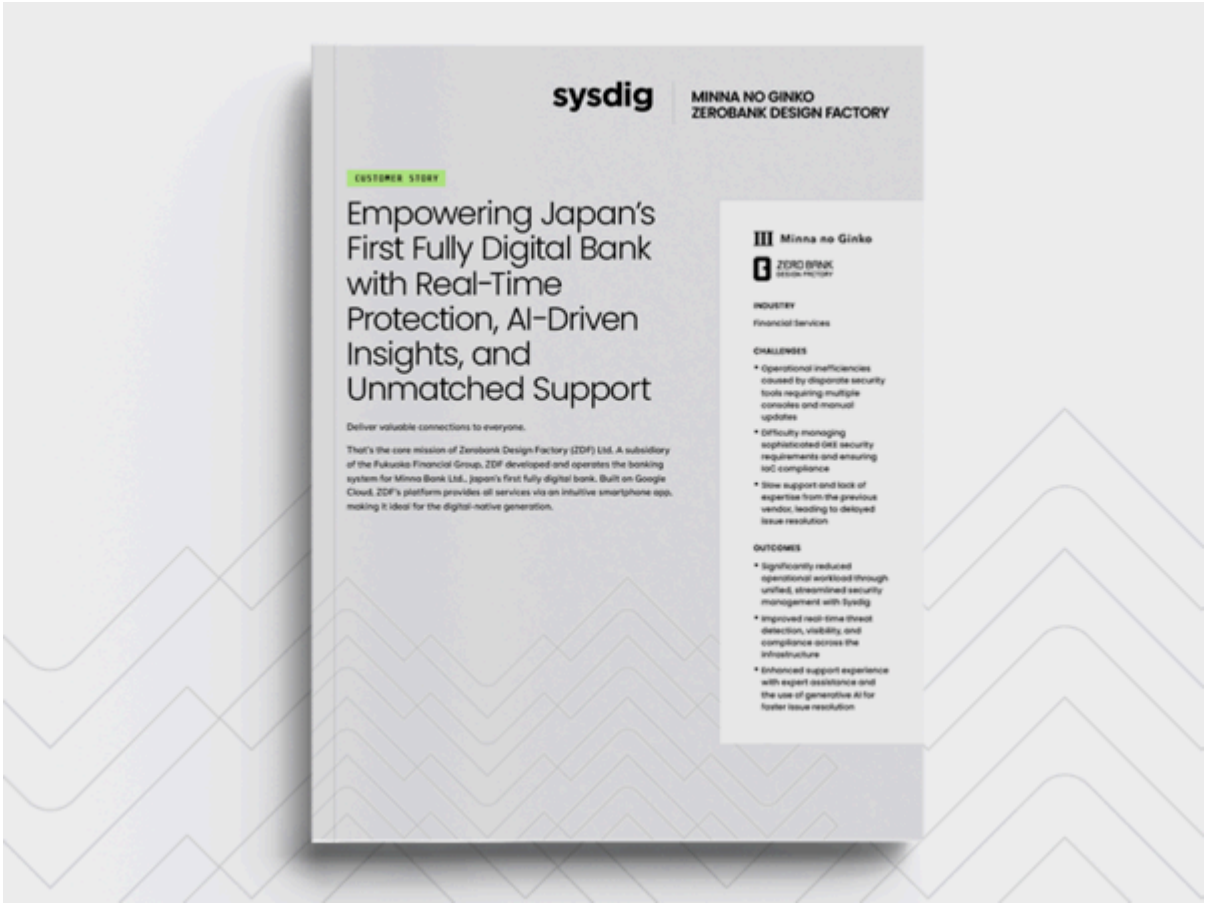


WEBINAR: Deploy Faster by Automating Container Security, Monitoring and Compliancevideo

Cloud SecurityCloud Monitoring

VIDEO. Sysdig product demonstration.video

Sysdig SecureSysdig Monitor

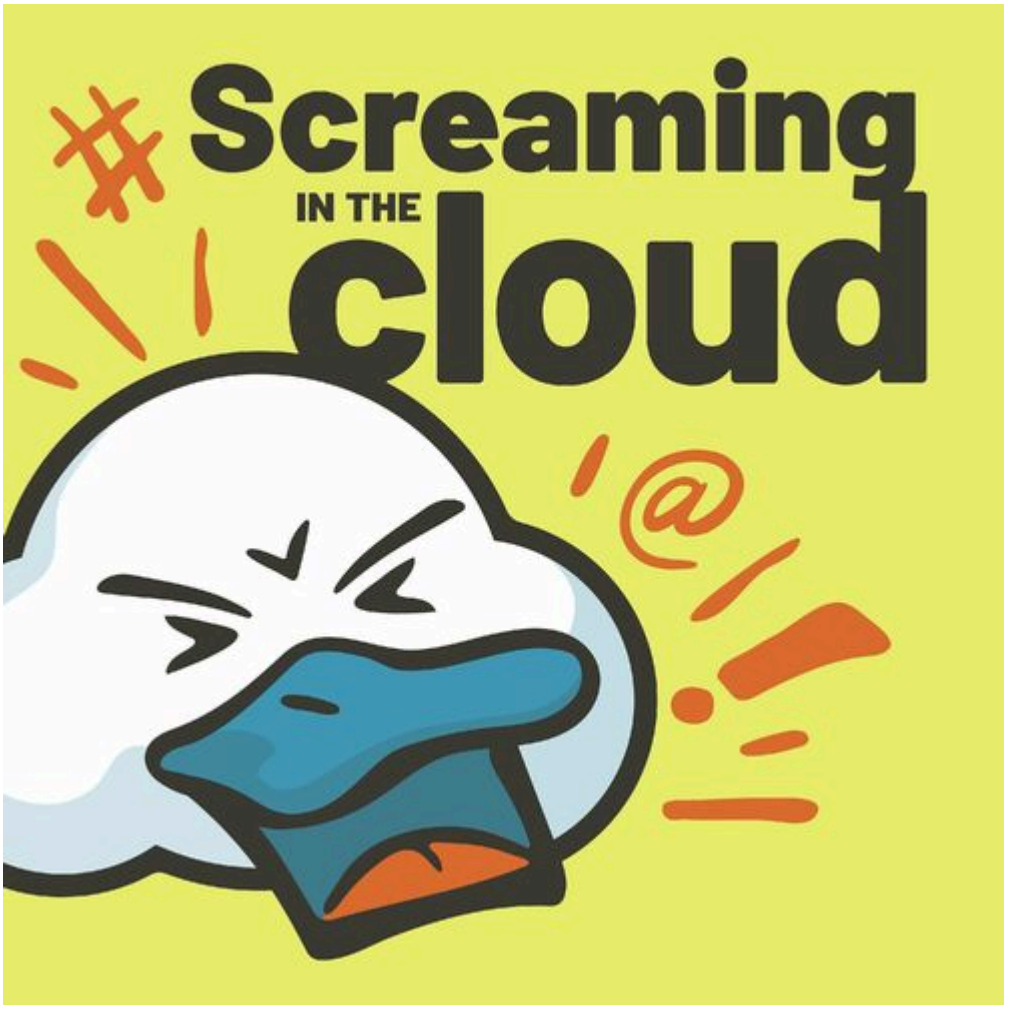



CASE STUDY. Zerobank Case Studypdf

Sysdig Secure

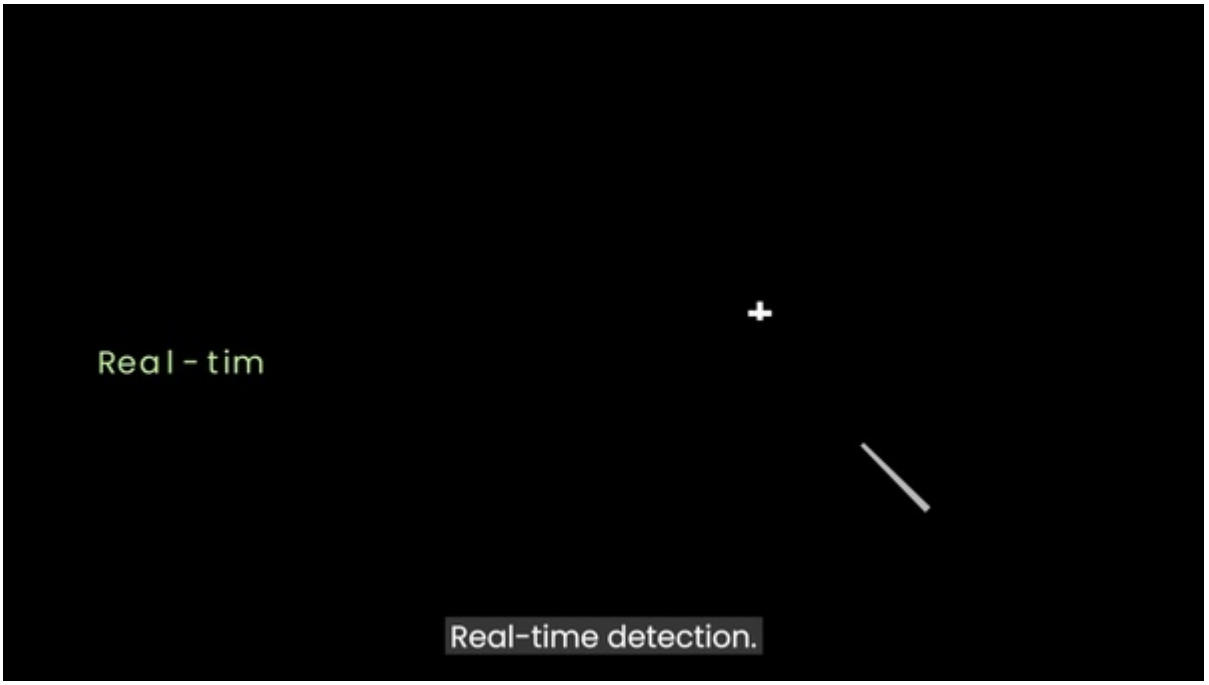

SERVICE BRIEF: Guided CSE Servicepdf

Sysdig SecureSysdig Monitor




PODCAST. Screaming in the Cloud - Cloud-Native Threatswebpage

Cloud Security

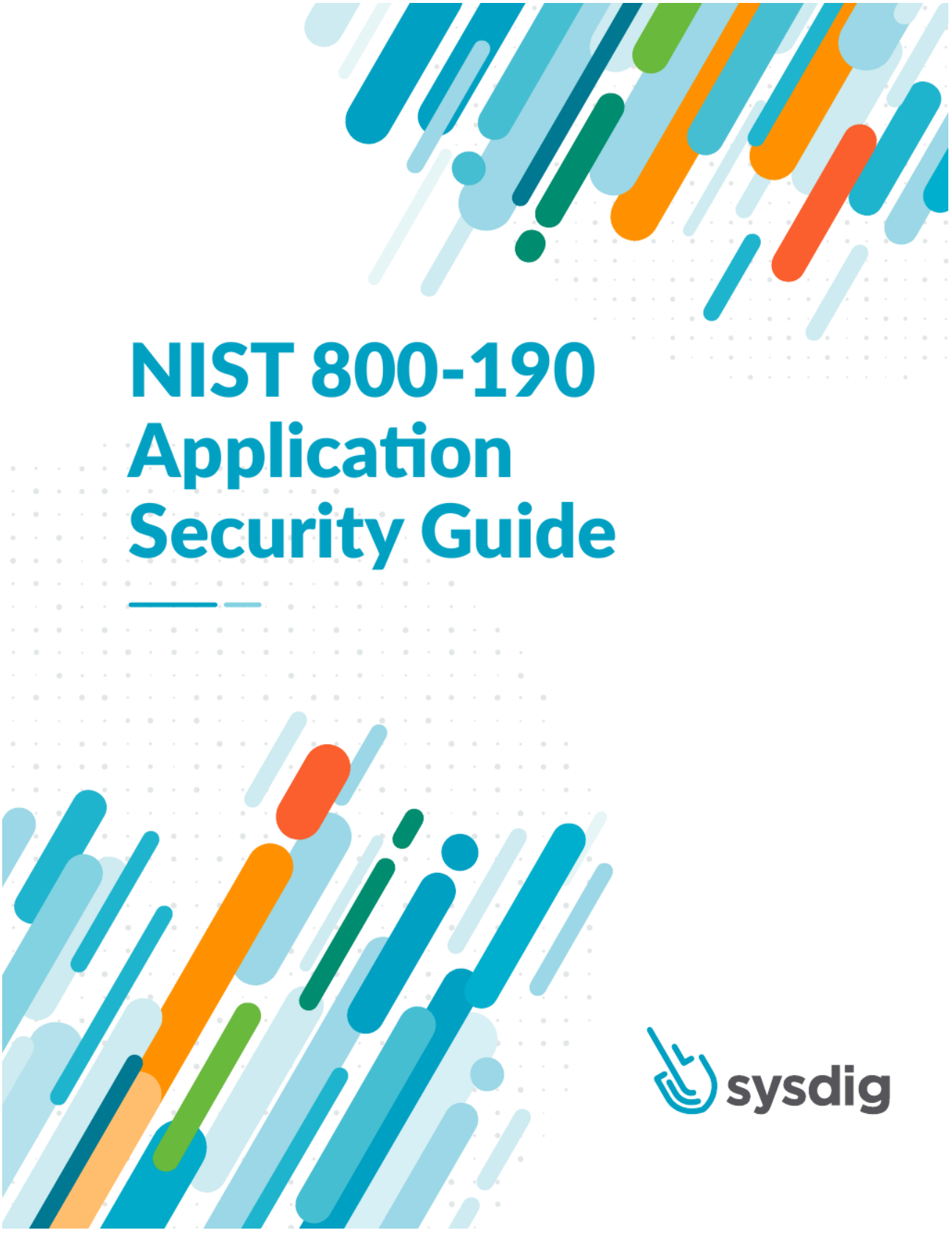


VIDEO. Real-time cloud security for financial servicesvideo

Cloud Security

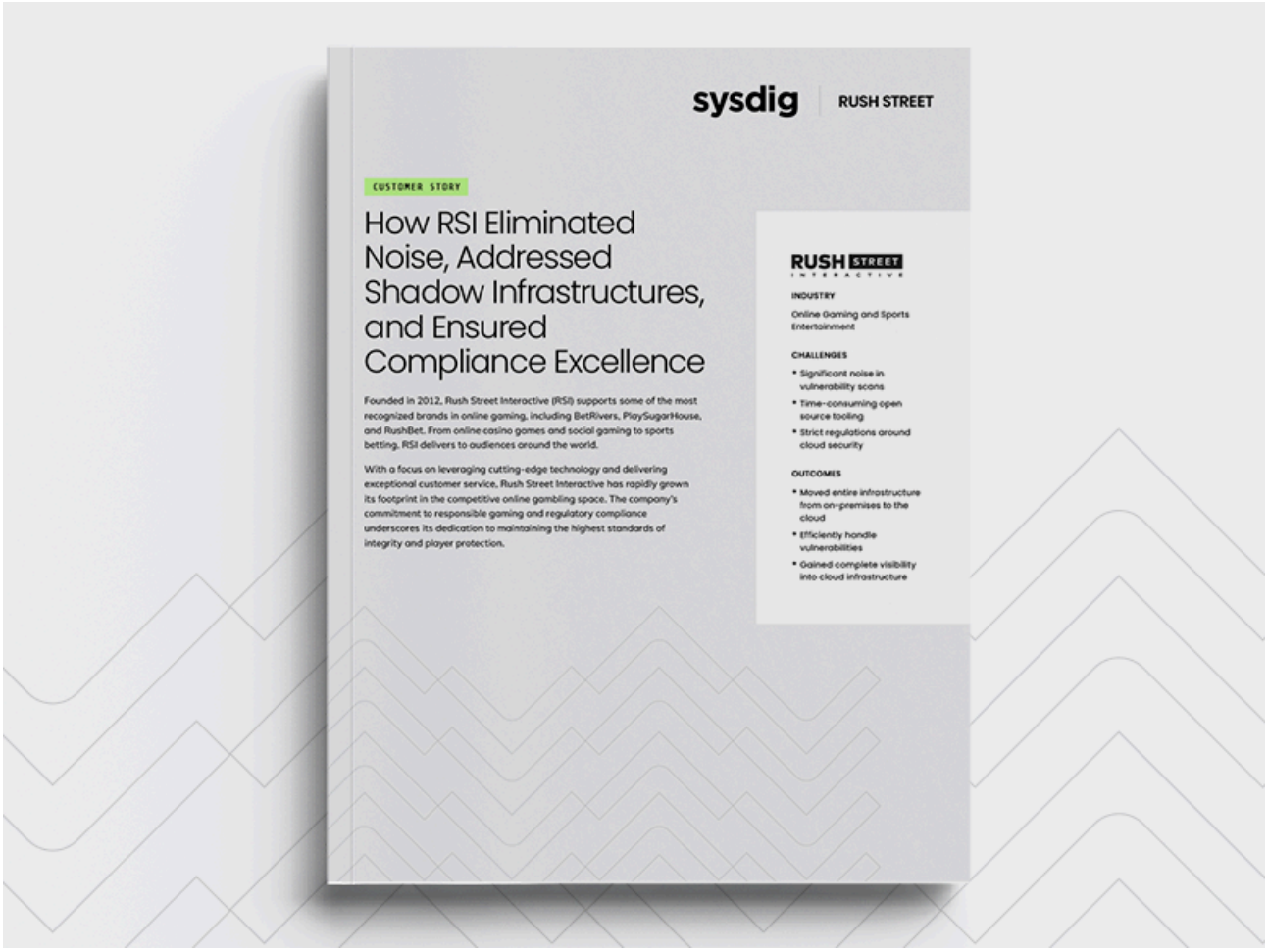

PODCAST. Screaming in the Cloud: An Open-Source Mindset in Cloud Security with Alex Lawrencewebpage

Cloud SecurityFalcoOpen Source




GUIDE. NIST 800-190 Application Security Guide Checklistpdf

Sysdig Secure

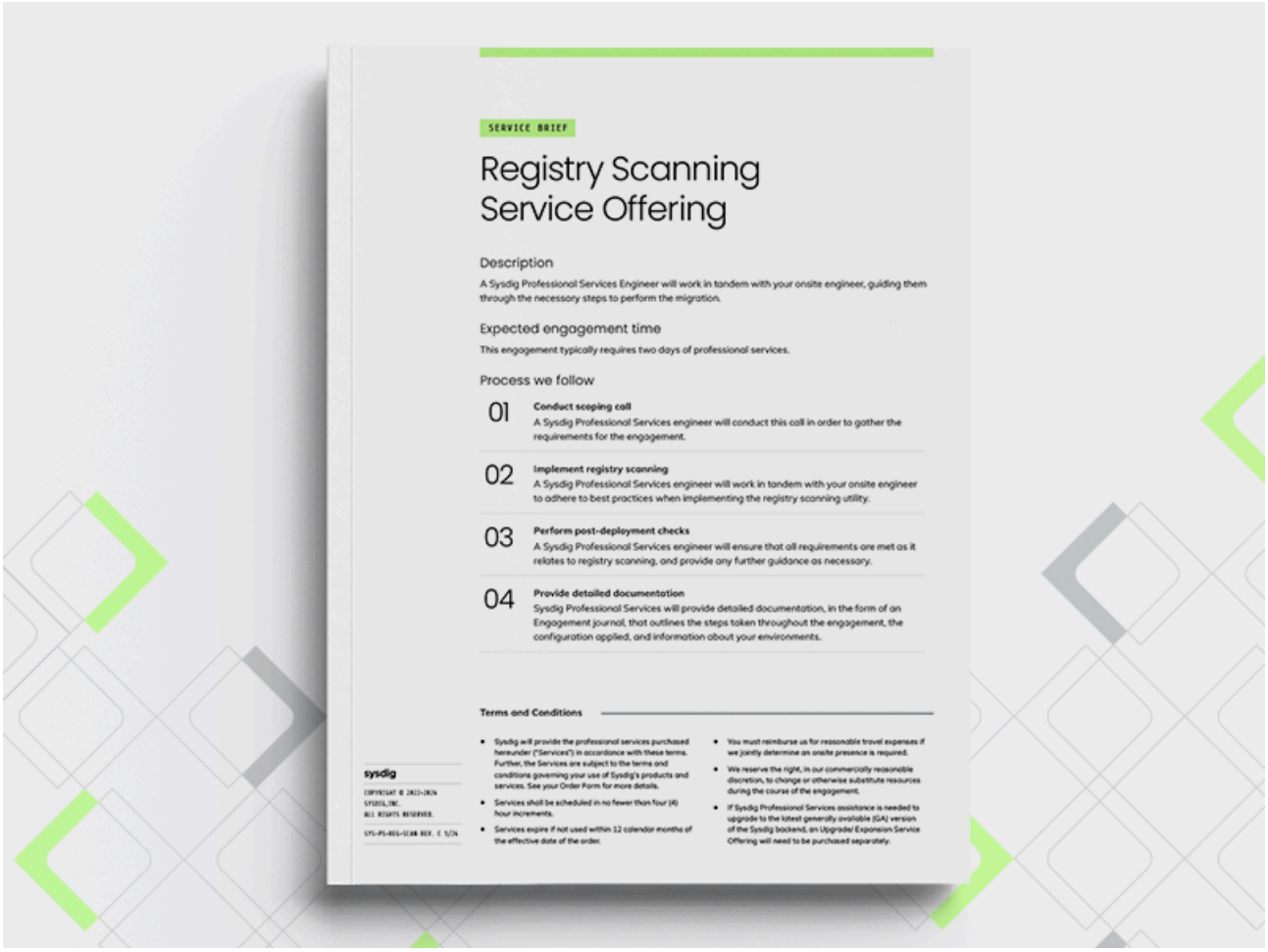



CASE STUDY. How RSI Eliminated Noise, Addressed Shadow Infrastructures, and Ensured Compliance Excellencepdf

Cloud Security


BRIEF. 5 Best Practices to Securing Cloud and Containerspdf

Sysdig SecureKubernetes



SERVICE BRIEF

Registry Scanning Service Offering

Description

A Sysdig Professional Services Engineer will work in tandem with your onsite engineer, guiding them through the necessary steps to perform the migration.

Expected engagement time

This engagement typically requires two days of professional services.

Process we follow

01 **Conduct scoping call**
A Sysdig Professional Services engineer will conduct this call in order to gather the requirements for the engagement.

02 **Implement registry scanning**
A Sysdig Professional Services engineer will work in tandem with your onsite engineer to adhere to best practices when implementing the registry scanning utility.

03 **Perform post-deployment checks**
A Sysdig Professional Services engineer will ensure that all requirements are met as it relates to registry scanning, and provide any further guidance as necessary.

04 **Provide detailed documentation**
Sysdig Professional Services will provide detailed documentation, in the form of an Engagement journal, that outlines the steps taken throughout the engagement, the configuration applied, and information about your environments.

Terms and Conditions

- Sysdig will provide the professional services purchased hereunder ("Services") in accordance with these terms. Further, the Services are subject to the terms and conditions governing your use of Sysdig's products and services. See your Order Form for more details.
- Services shall be scheduled in no fewer than four (4) hour increments.
- Services expire if not used within 12 calendar months of the effective date of the order.
- You must reimburse us for reasonable travel expenses if we jointly determine an onsite presence is required.
- We reserve the right, in our commercially reasonable discretion, to change or otherwise substitute resources during the course of the engagement.
- If Sysdig Professional Services assistance is needed to upgrade to the latest generally available (GA) version of the Sysdig backend, an Upgrade/ Expansion Service Offering will need to be purchased separately.

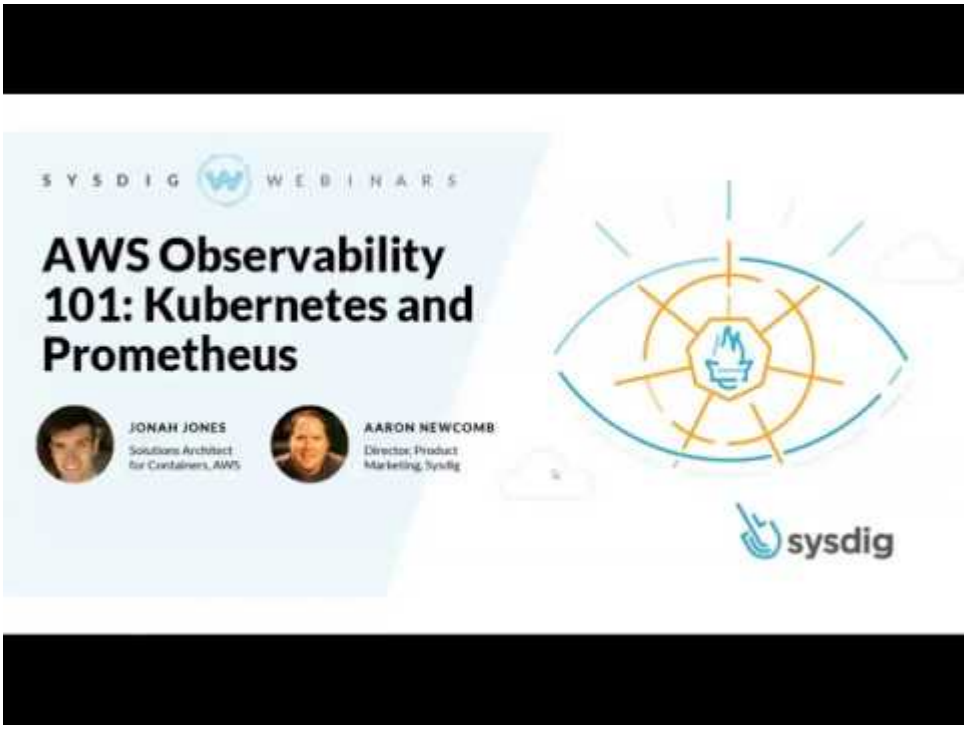
sysdig

[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

AWSCloud MonitoringPrometheusSysdig Monitor


SERVICE BRIEF. Sysdig JumpStartpdf

Sysdig Secure


BRIEF. 2025 Cloud-Native Security and Usage Reportpdf

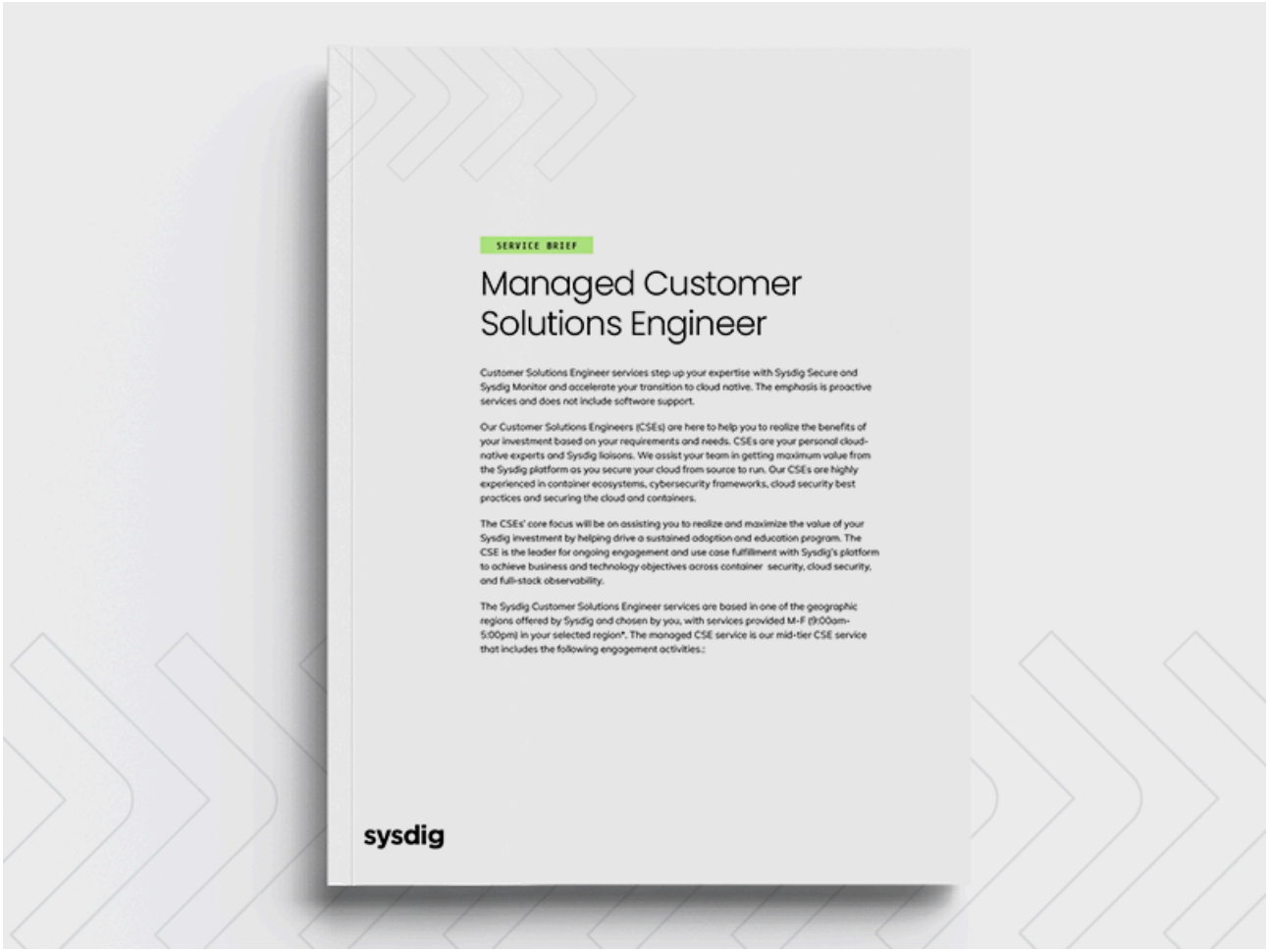
Cloud Security


CASE STUDY. Loglasspdf

Sysdig Secure


INFOGRAPHIC. Unlock The Power Of Nis2pdf

Cloud Security




SERVICE BRIEF: Managed CSE Servicepdf

Sysdig SecureSysdig Monitor


[WEBINAR. 451 Research Webinar: Scaling Cloud-Native to Meet Ops & Security Demandsvideo]

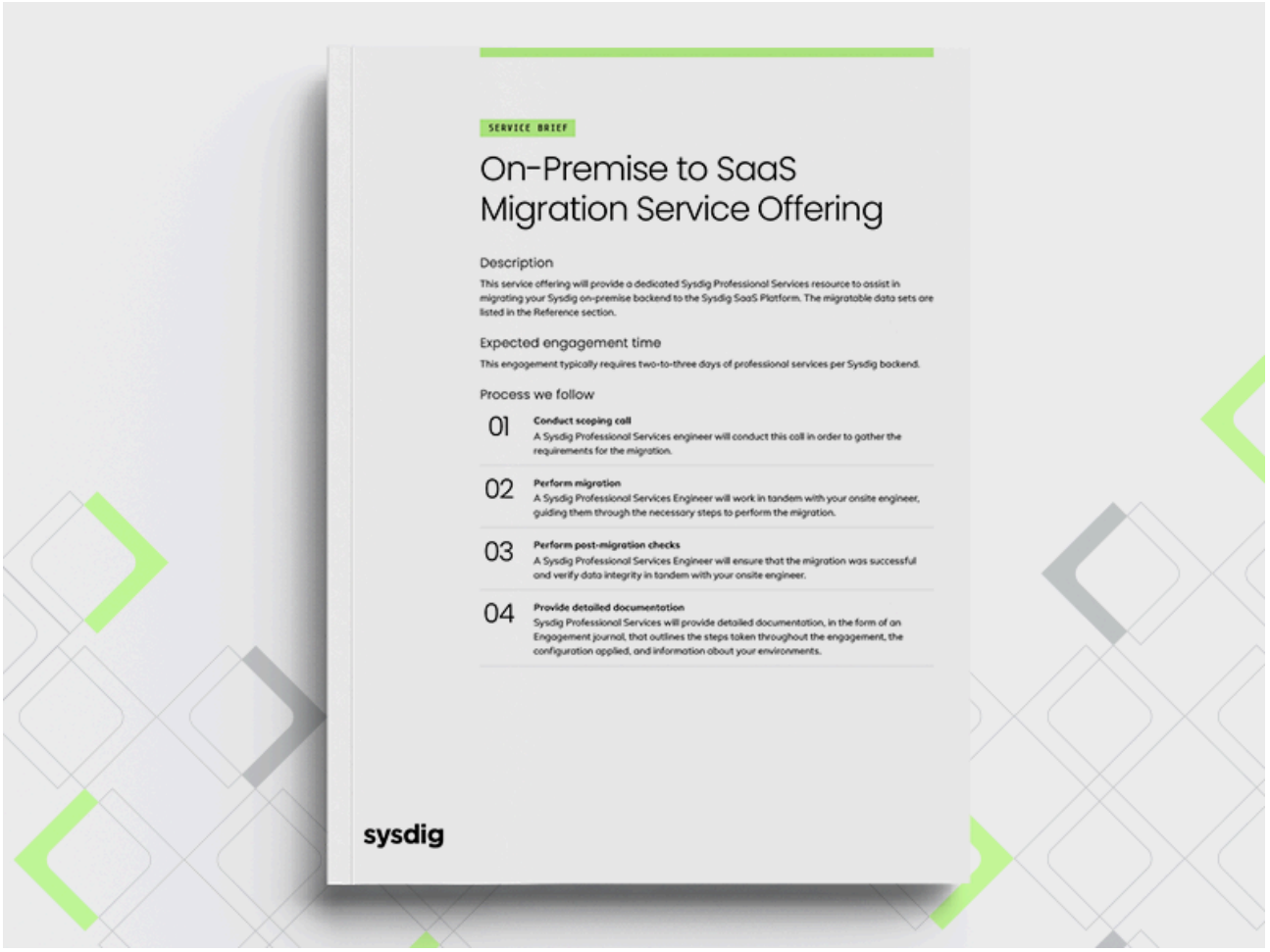
[Sysdig SecureSysdig Monitor]


[The Business Value of GenAI for Cloud Securitypdf]

[Cloud Security]


BRIEF. Sysdig Secure Architecture Guidepdf

Sysdig Secure

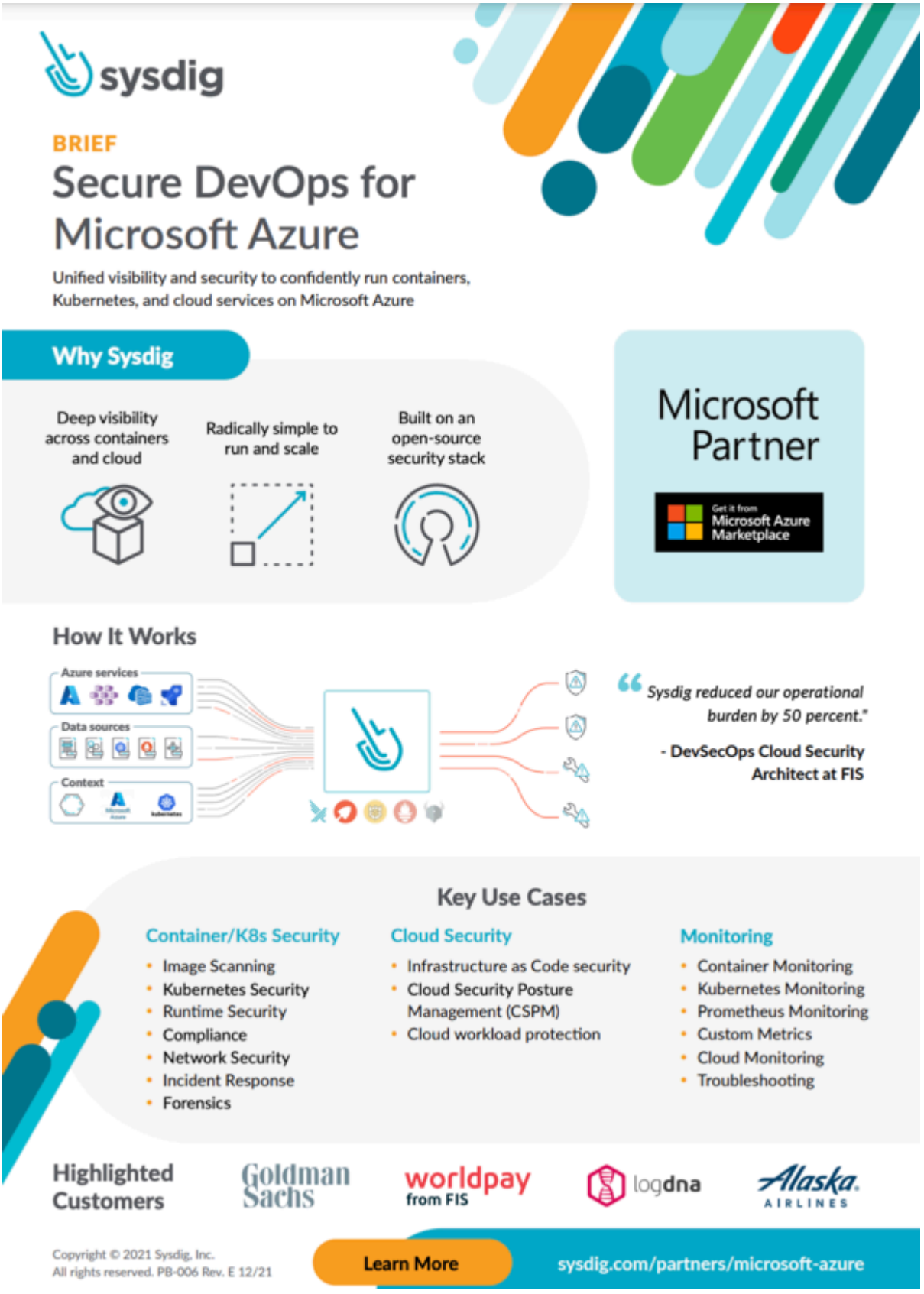



SERVICE BRIEF. On-Premise To SaaSpdf

Sysdig SecureSysdig Monitor

[WEBINAR. DevNation Federal: DevSecOps What To Focus On Firstvideo]

[Red Hat]



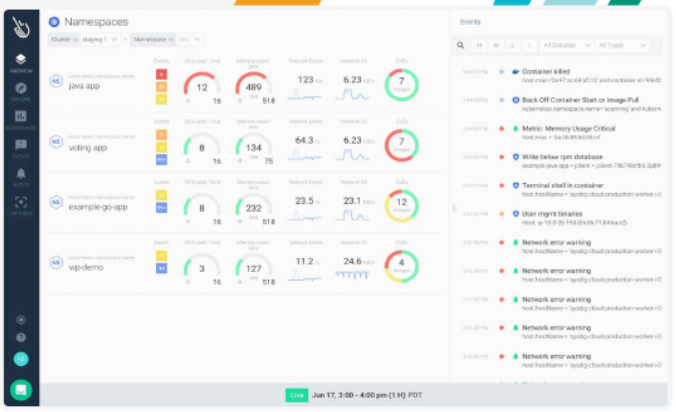
[SOLUTION BRIEF. Sysdig Platform for Microsoft Azure and AKSwebpage]

[Azure]

sysdig

# 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

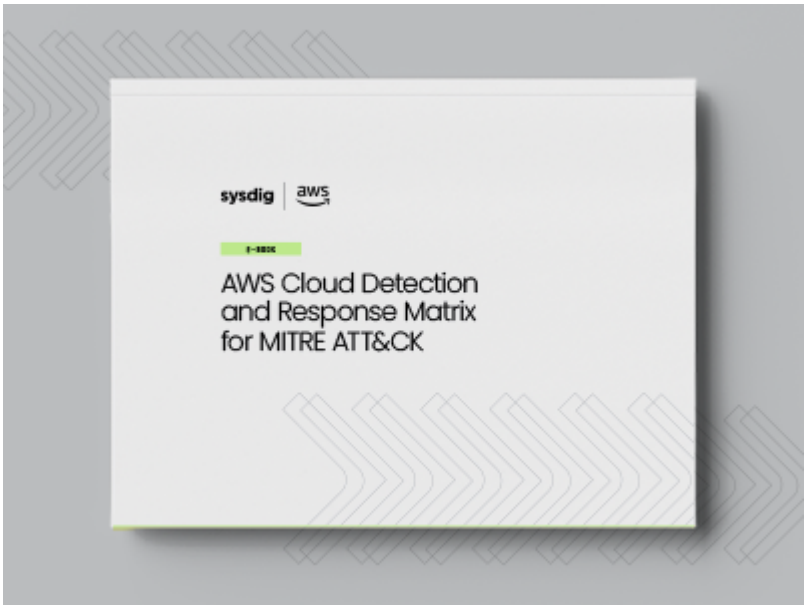
- Scale Prometheus monitoring to millions of metrics with long-term retention.
- Monitor health and performance to prevent issues across private, hybrid and multi-cloud environments.
- Troubleshoot inside clusters, pods and containers.

### 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.

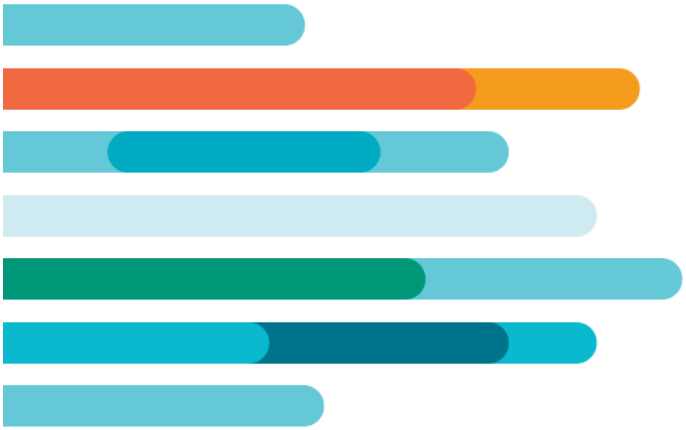
[PARTNER BRIEF. Rancherpdf]

Sysdig SecureSysdig Monitor




GUIDE. AWS Cloud Detection and Response Matrix for MITRE ATT&CKpdf

Cloud Security

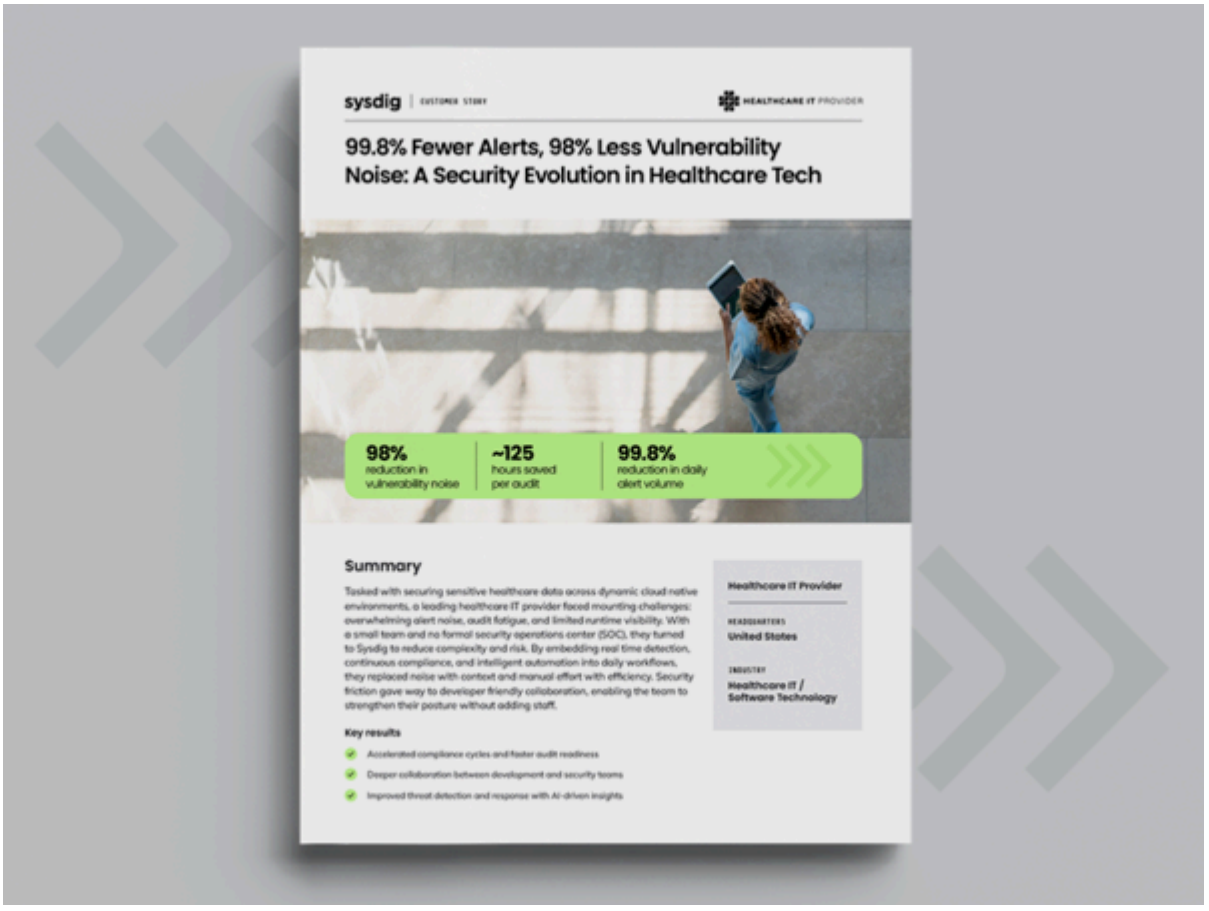


sysdig

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

GUIDE. 30 60 90 Day Checklistpdf

Cloud SecurityCloud Monitoring




Healthcare It Sysdig Customer Storypdf

Sysdig SecureSysdig Monitor


WHITEPAPER. NIS2 Action Plan for the Cloud CISOpdf

Cloud Security

SERVICE BRIEF

# Runtime Scanning Service Offering

## Description

This service offering will provide a dedicated Sysdig Professional Services resource to assist with enabling and configuring the ability to evaluate running images within an existing environment. This functionality is achieved using Falco rules and by assigning them to policies. In this Service Offering, a Professional Services Engineer (PSE) will assist with tuning, modifying, and creating custom policies and Falco rules to address up to five specific use cases.

## Expected engagement time

This engagement typically requires five days of professional services.

## Process we follow

01 **Conduct scoping call**
A Sysdig Professional Services engineer will conduct this call in order to gather the requirements for the requested policies and rules.

02 **Tune existing rules**
A Sysdig Professional Services engineer will work in tandem with your onsite engineer to run the Falco policy tuner.

03 **Implement additional rules and policies**
A Sysdig Professional Services engineer will assist with creation and implementation of additional policies and rules based on the use cases presented in the scoping call.

04 **Provide detailed documentation**
Sysdig Professional Services will provide detailed documentation, in the form of an Engagement journal, that outlines the steps taken throughout the engagement, the configuration applied, and information about your environments.

## Terms and Conditions

- Sysdig will provide the professional services purchased hereunder ("Services") in accordance with these terms. Further, the Services are subject to the terms and conditions governing your use of Sysdig's products and services. See your Order Form for more details.
- Services shall be scheduled in no fewer than four (4) hour increments.
- Services expire if not used within 12 calendar months of the effective date of the order.
- You must reimburse us for reasonable travel expenses if we jointly determine an onsite presence is required.
- We reserve the right, in our commercially reasonable discretion, to change or otherwise substitute resources during the course of the engagement.
- If Sysdig Professional Services assistance is needed to upgrade to the latest generally available (GA) version of the Sysdig backend, an Upgrade/ Expansion Service Offering will need to be purchased separately.

sysdig

COPYRIGHT © 2021-2024
SYSDIG, INC.
ALL RIGHTS RESERVED.

SYS-PS-BUN-SCAN REV. B 5/24

[SERVICE BRIEF. Runtime Scanningpdf]

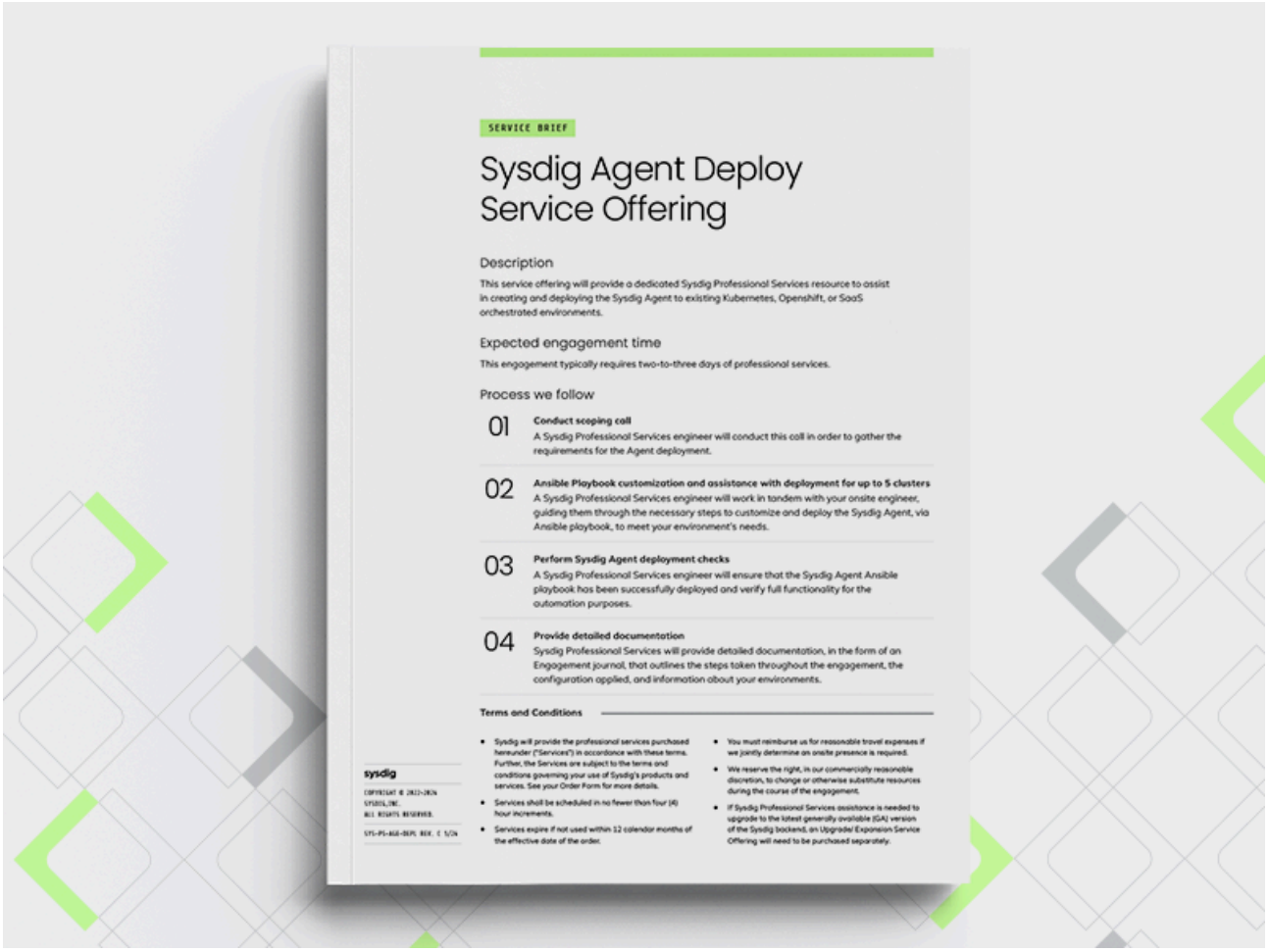
[Sysdig SecureSysdig Monitor]


WHITEPAPER. Your Cloud Security Strategy is Backwardpdf

Cloud Security


BRIEF. 2025 Usage Report Executive Takeawayspdf

Cloud Security



SERVICE BRIEF

# Sysdig Agent Deploy Service Offering

## Description

This service offering will provide a dedicated Sysdig Professional Services resource to assist in creating and deploying the Sysdig Agent to existing Kubernetes, Openshift, or SaaS orchestrated environments.

## Expected engagement time

This engagement typically requires two-to-three days of professional services.

## Process we follow

01 **Conduct scoping call**
A Sysdig Professional Services engineer will conduct this call in order to gather the requirements for the Agent deployment.

02 **Ansible Playbook customization and assistance with deployment for up to 5 clusters**
A Sysdig Professional Services engineer will work in tandem with your onsite engineer, guiding them through the necessary steps to customize and deploy the Sysdig Agent, via Ansible playbook, to meet your environment's needs.

03 **Perform Sysdig Agent deployment checks**
A Sysdig Professional Services engineer will ensure that the Sysdig Agent Ansible playbook has been successfully deployed and verify full functionality for the automation purposes.

04 **Provide detailed documentation**
Sysdig Professional Services will provide detailed documentation, in the form of an Engagement journal, that outlines the steps taken throughout the engagement, the configuration applied, and information about your environments.

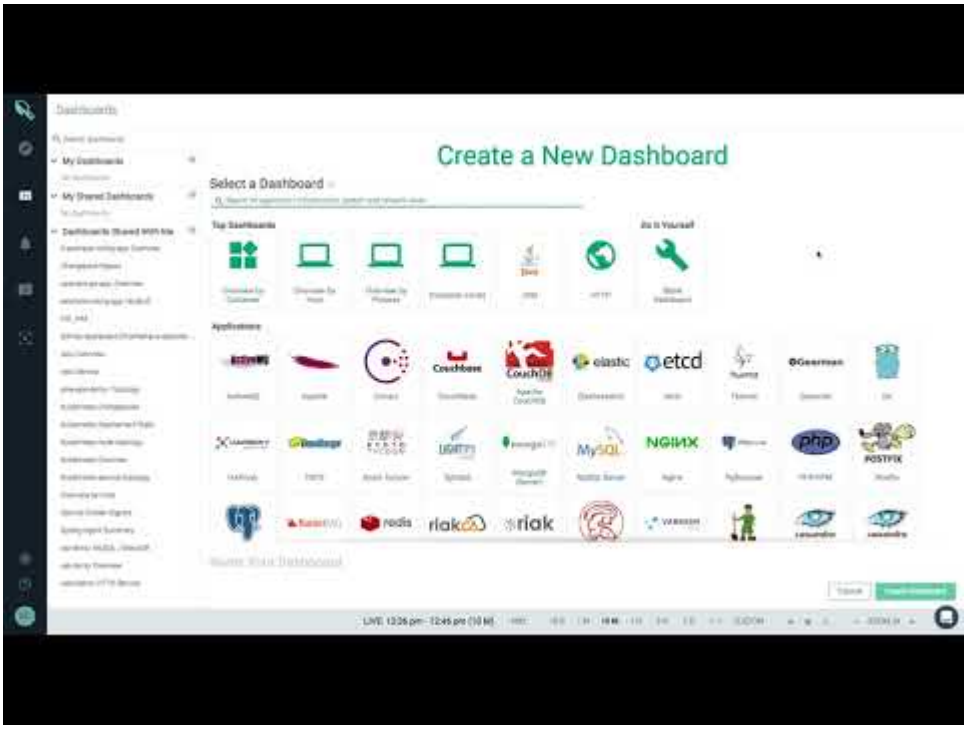
## Terms and Conditions

- Sysdig will provide the professional services purchased hereunder ("Services") in accordance with these terms. Further, the Services are subject to the terms and conditions governing your use of Sysdig's products and services. See your Order Form for more details.
- Services shall be scheduled in no fewer than four (4) hour increments.
- Services expire if not used within 12 calendar months of the effective date of the order.
- You must reimburse us for reasonable travel expenses if we jointly determine an onsite presence is required.
- We reserve the right, in our commercially reasonable discretion, to change or otherwise substitute resources during the course of the engagement.
- If Sysdig Professional Services assistance is needed to upgrade to the latest generally available (GA) version of the Sysdig backend, an Upgrade/ Expansion Service Offering will need to be purchased separately.

sysdig

[SERVICE BRIEF. Agent Deploypdf]

[Sysdig SecureSysdig Monitor]



VIDEO. Sysdig Monitor - Cloud-native intelligencevideo

DockerKubernetesSysdig Monitor


REPORT. Sysdig Security And Monitoringpdf

[Sysdig SecureSysdig Monitor]


[VIDEO. Sysdig x Neo4j: Transform the relationship between Security & Devvideo]

[Cloud Security]

[INFOGRAPHIC. Promql Cheatsheetpdf]

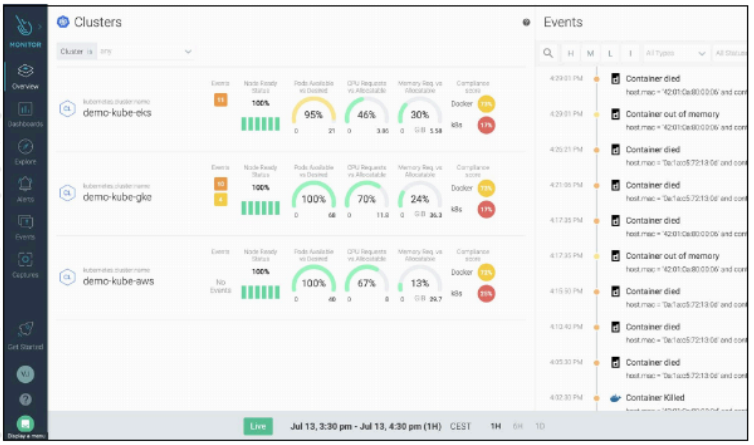
[Cloud MonitoringKubernetesPrometheusSysdig Monitor]

sysdig

# Kubernetes Monitoring Checklist

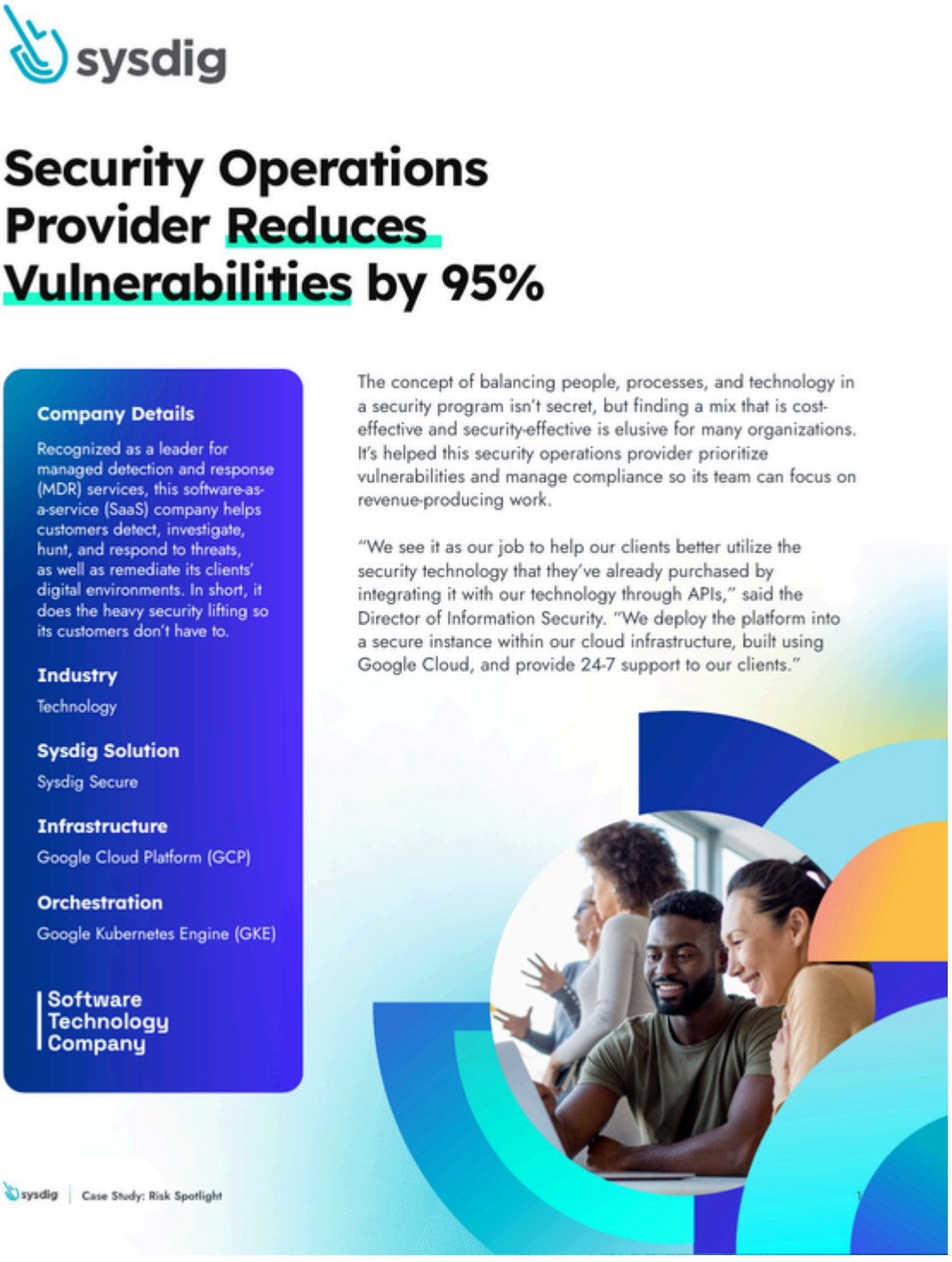
Kubernetes has taken the container ecosystem by storm. It acts as the brain for your distributed container deployment and is designed to manage service-oriented applications using containers distributed across clusters of hosts. Kubernetes provides mechanisms for application deployment, service discovery,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

Cloud MonitoringKubernetesSysdig Monitor




CASE STUDY. Security Operations Provider Reduces Vulnerabilities by 95%pdf

Vulnerability (computing)

VIDEO. How to Get Started with Sysdig Monitorvideo

Sysdig Monitor

sysdig

Data Security Findings

Cloud-native data security posture management (DSPM)

Sensitive data such as personally identifiable information (PII), protected health information (PHI), and financial data are valuable targets for attackers. Protecting this data is made more challenging because different clouds, storage, and databases impact visibility and control.

Sysdig Secure treats sensitive data as a first-class security signal — alongside vulnerabilities, misconfigurations, identities, and runtime threats — to help you reduce risk and prioritize what matters most.

**The challenge: Managing data risk without runtime context**

Organizations face three persistent challenges in securing data in the cloud:

- **Data visibility gaps**
  Blind spots for where sensitive data lives or what type of data it is.
- **Poor prioritization**
  Lack of context for threats and vulnerabilities impacting assets with PII, PHI, or financial data.
- **Slow response**
  Lack of prioritization slows mean time to remediate and mean time to respond.

Failure to connect sensitive data with runtime insights makes it hard to take the right action.

**The Sysdig solution: DSPM integrated into CNAPP**

Sysdig combines data security findings with runtime context to provide:

- **Runtime activity**
  Correlate data findings with behaviors like suspicious process activity or lateral movement.
- **Unified risk prioritization**
  Data context added to vulnerability management and threat detection.
- **Threat contextualization**
  Visualize data in attack paths to understand blast radius and criticality.

Sysdig reveals data exposure to help focus remediation and contextualize threats for faster, more confident response.

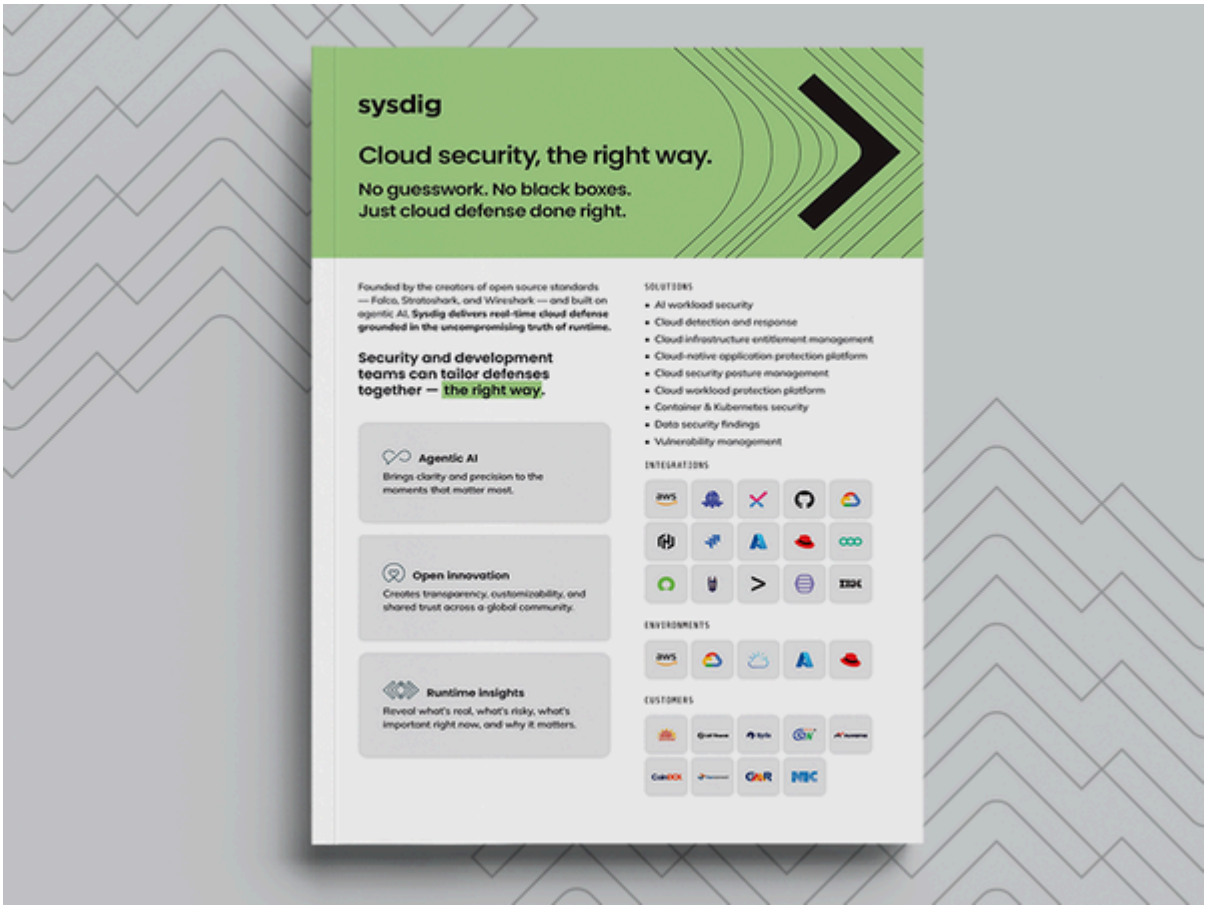
**Unified data security across clouds**

Data security findings integrate seamlessly into the Sysdig Secure user experience:

- Sensitive data context appears directly in resource views
- Findings are correlated with posture, identity, vulnerabilities, and runtime detections
- Data risks can be queried and automated using Sysdig Query Language (SysQL)

This unified experience — available in a single pane of glass — reduces tool sprawl and accelerates triage, investigations, remediation, and response.

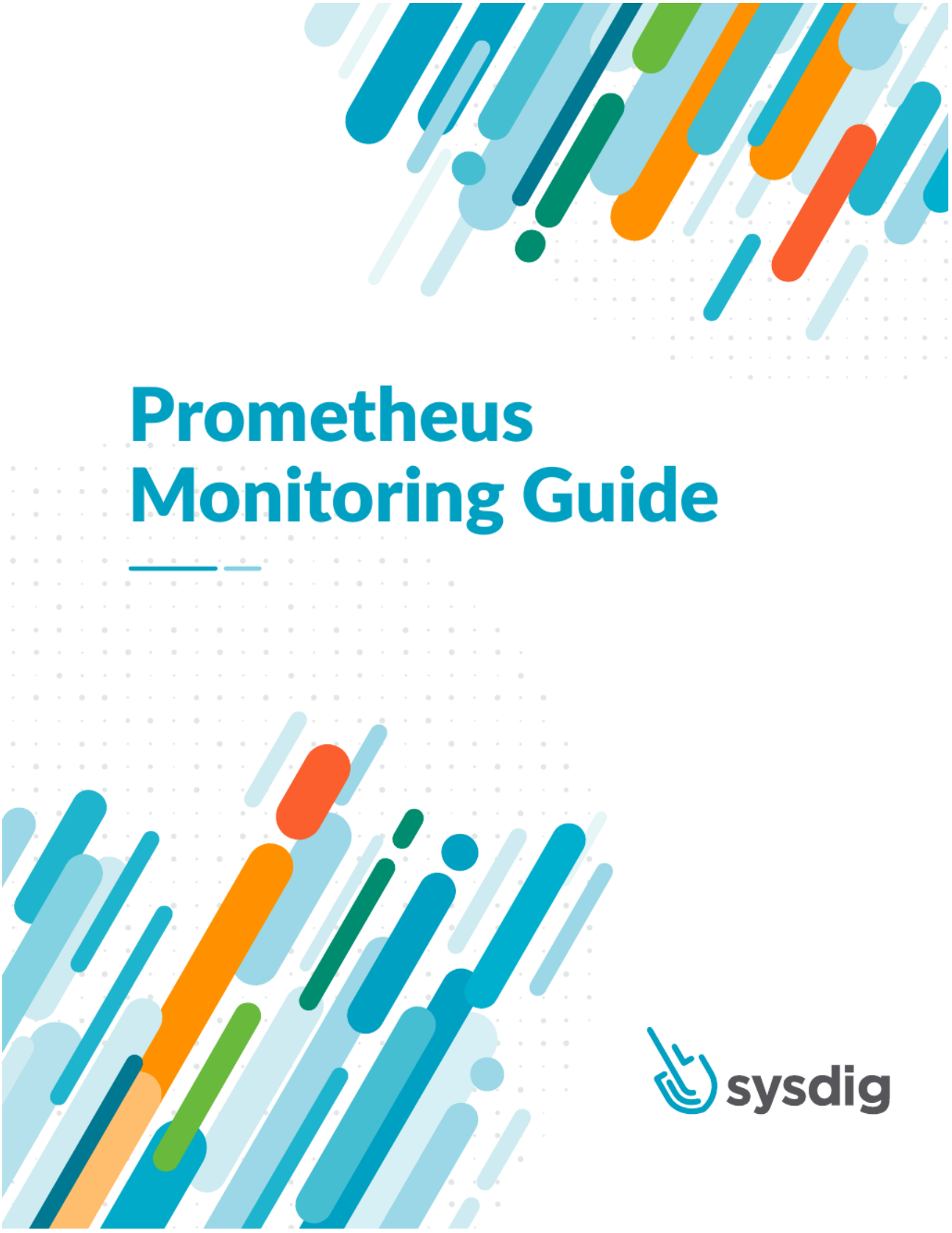
BRIEF. Data security findingspdf




BRIEF. Sysdig Corporate Brief: Indiapdf


SOLUTION BRIEF. Securing Containers And Kubernetespdf

Kubernetes




GUIDE. Prometheus Monitoringpdf

KubernetesPrometheusSysdig Monitor


GUIDE. Kubernetes Monitoring Guidepdf

Cloud MonitoringKubernetesSysdig Monitor


CASE STUDY. Game Developer Companypdf

Cloud MonitoringKubernetesSysdig Monitor


CASE STUDY. From Falco to Sysdig: How Financial Firm Syfe Simplified Compliance and Threat Detectionpdf

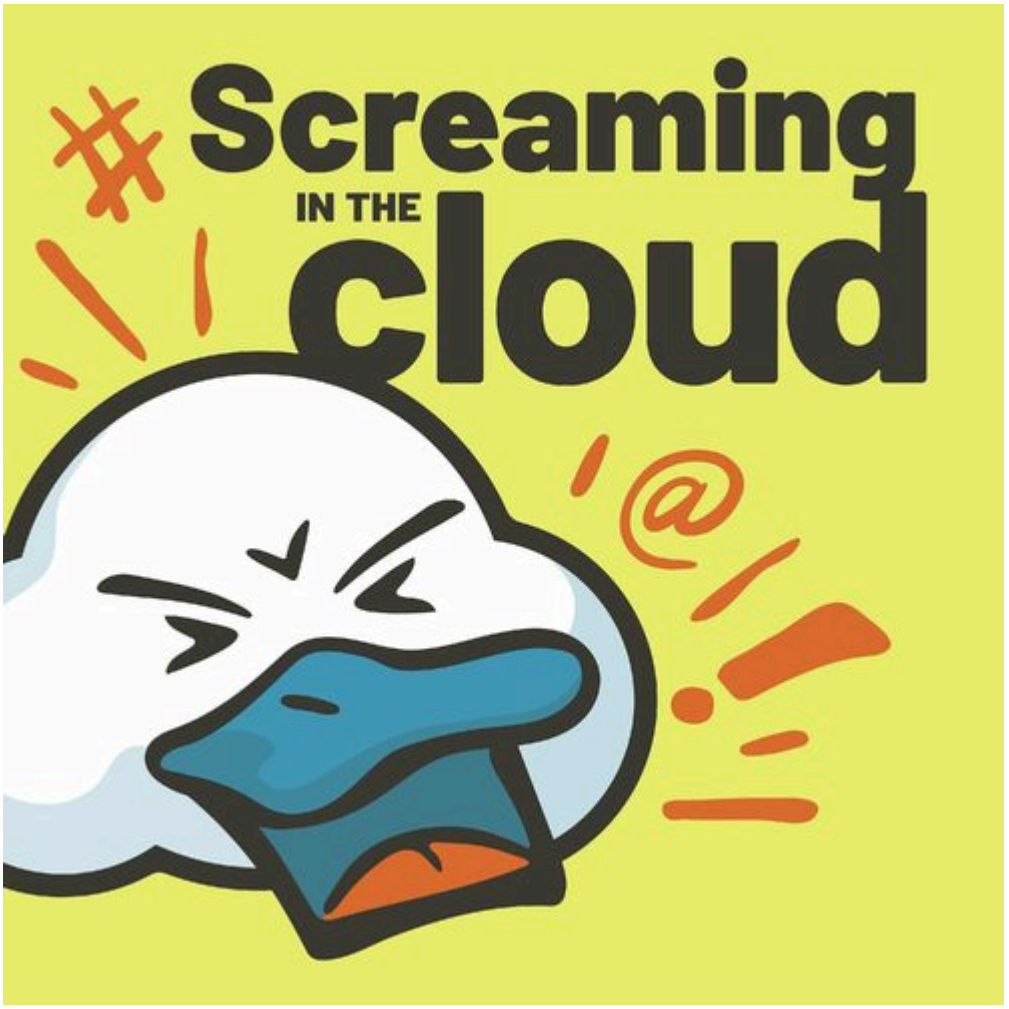

CASE STUDY. BitMEX Has Never Lost a Coinpdf


CHECKLIST. Agentic AI For Cloud Security Checklistpdf


Exploring Advanced Cybersecurity with Michael Isbitski – Sysdigwebpage

cybersecurity


[BRIEF. Sysdig Company Overviewpdf]




PODCAST. Benchmarking Security Attack Response Times in the Age of Automationwebpage

sysdig

# 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.

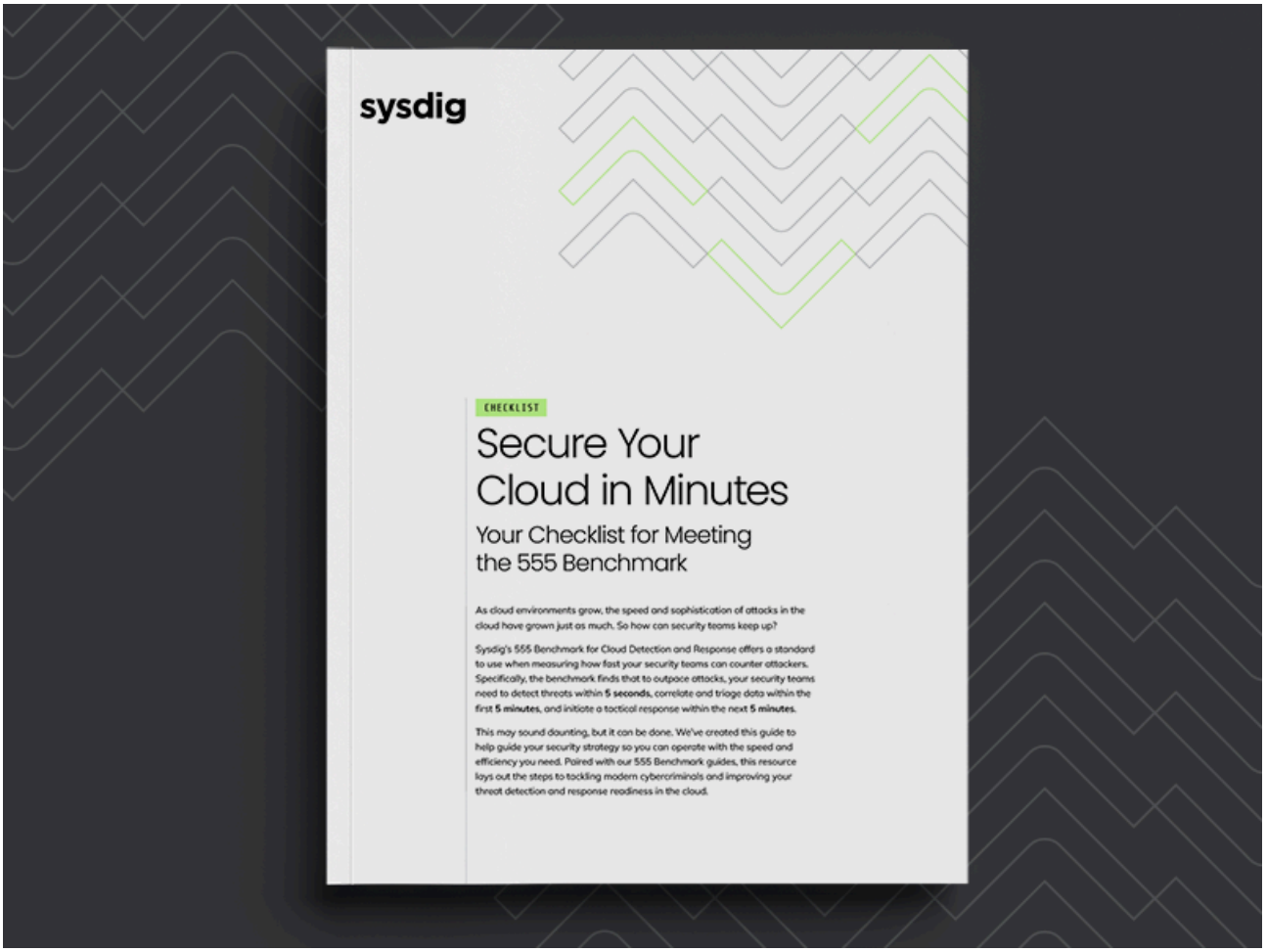
In this best practices guide, you'll find some tips that will help you with reducing the cost of custom metrics monitoring.

BRIEF: Best Practices for Reducing the Cost of Custom Metricspdf

Cloud MonitoringCost OptimizationSysdig Monitor

VIDEO. Containers in Production: Goldman Sachsvideo

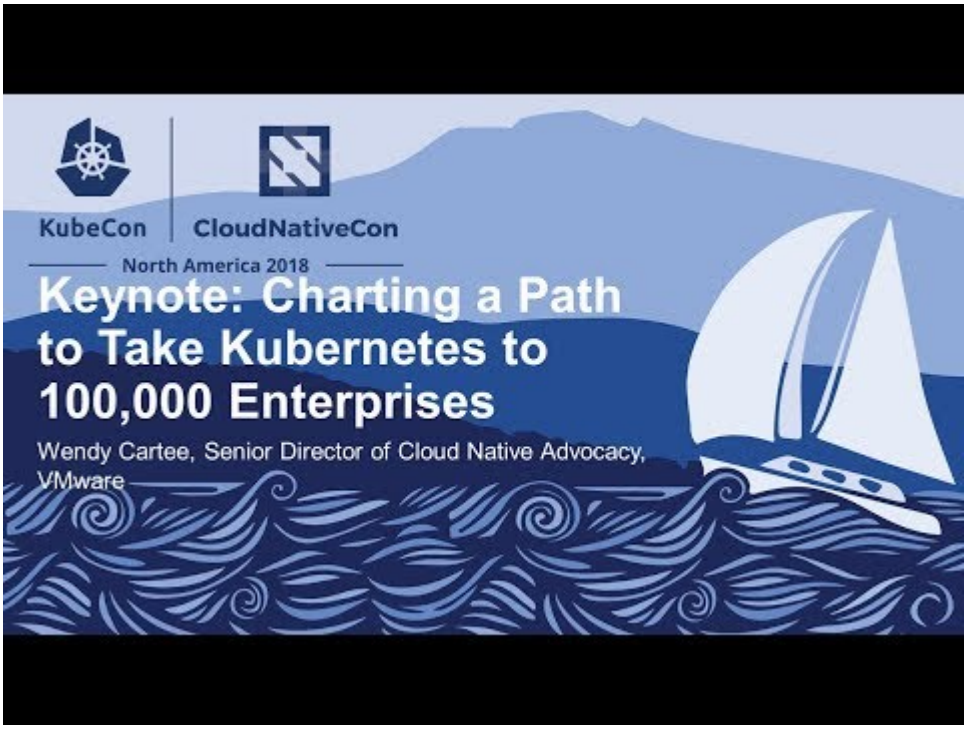
Kubernetes



GUIDE. Secure Your Cloud in Minutespdf

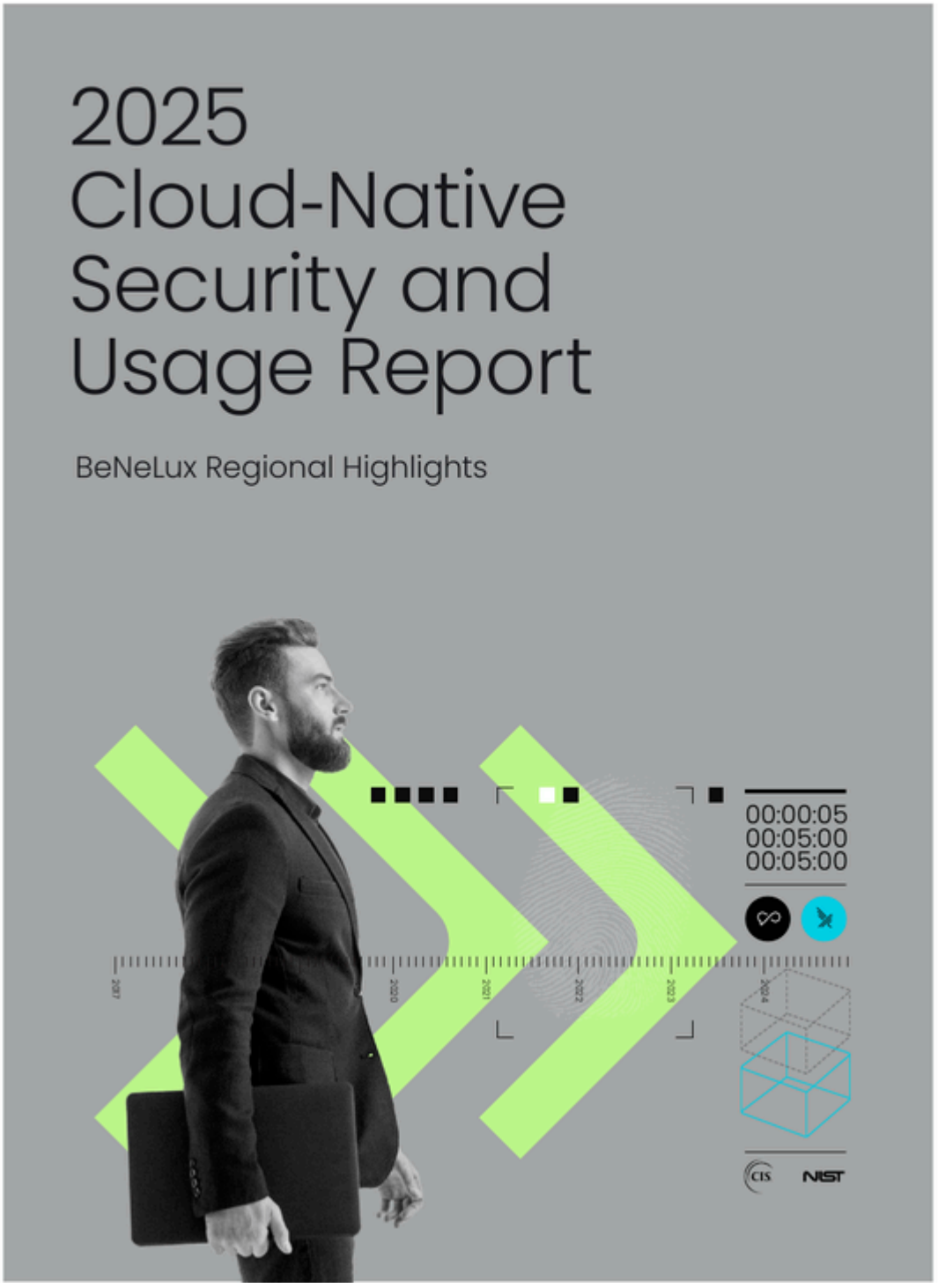
Cloud computing security


VIDEO. Running Cloud-Native Workloads In Production with Sysdigvideo




VIDEO. KubeCon Keynote: Charting a Path to Take Kubernetes to 100,000 Enterprises - Wendy Carteevideo

sysdig TrueFullstaq




REPORT. BeNeLux 2025 Cloud Native Security Usage Report - TrueFullstaqpdf

sysdig

# 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

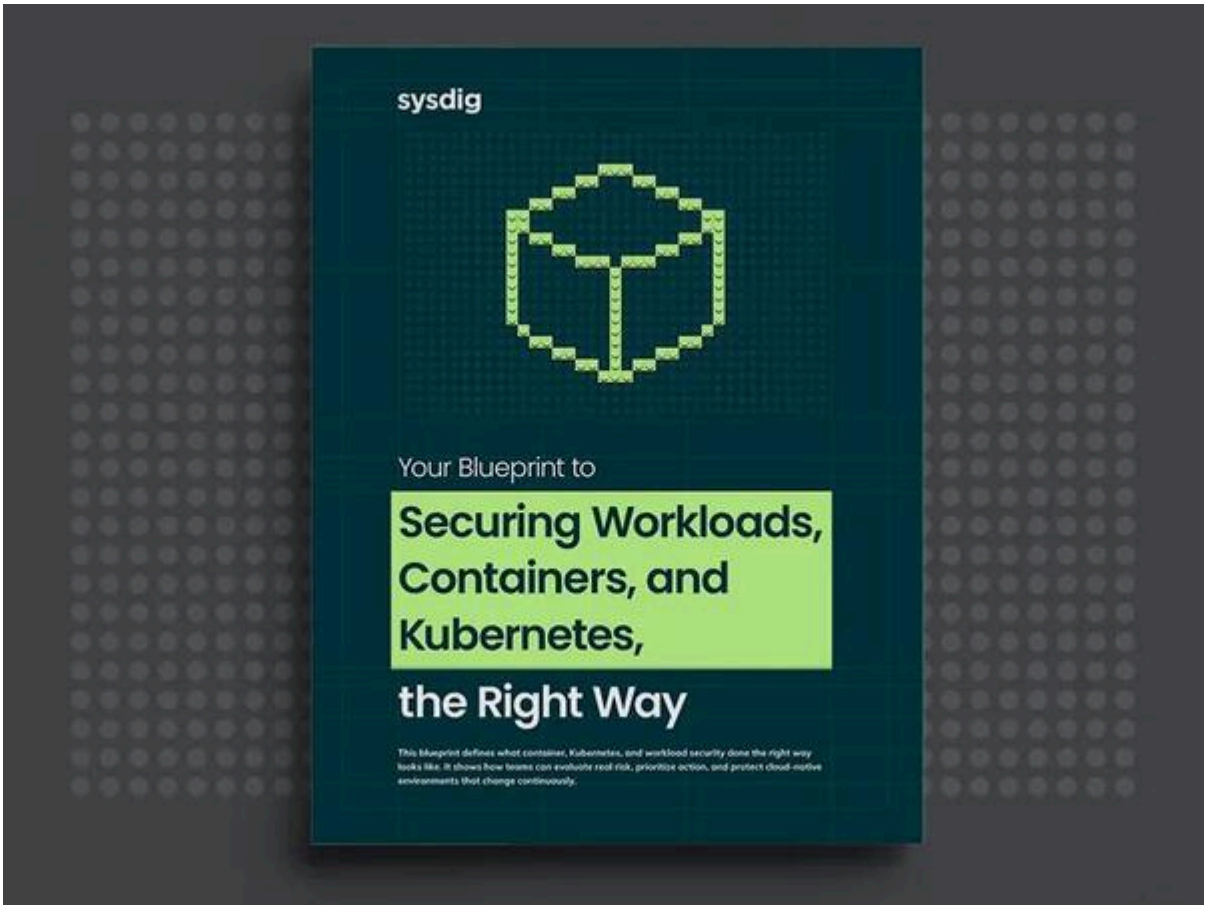

A technology reference architecture is outlined above for reference. Here are the six keys for scaling Prometheus:

WHITEPAPER. Six Keys for Scaling Prometheuspdf

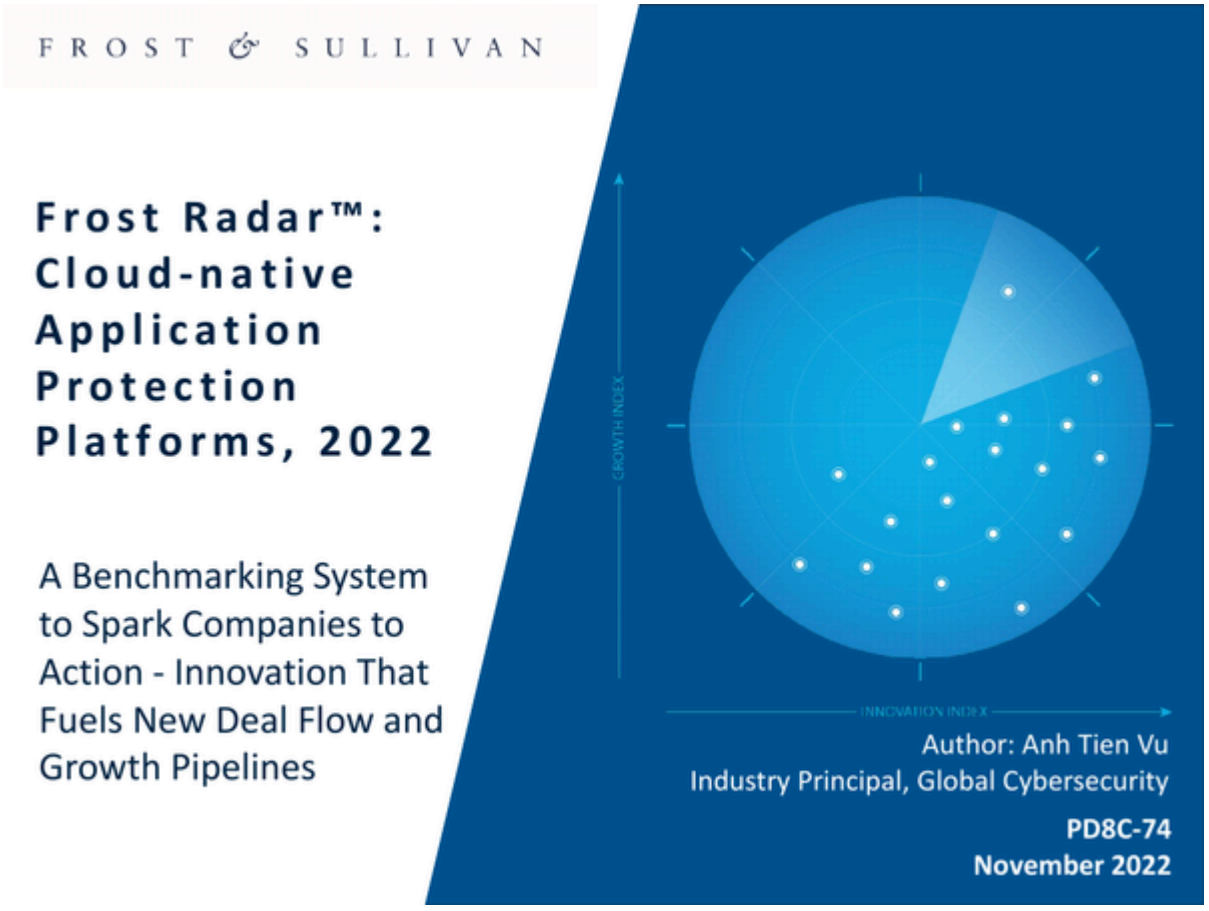
PrometheusSysdig Monitor


BRIEF: Kubernetes and Cloud Monitoring for Financial Servicespdf

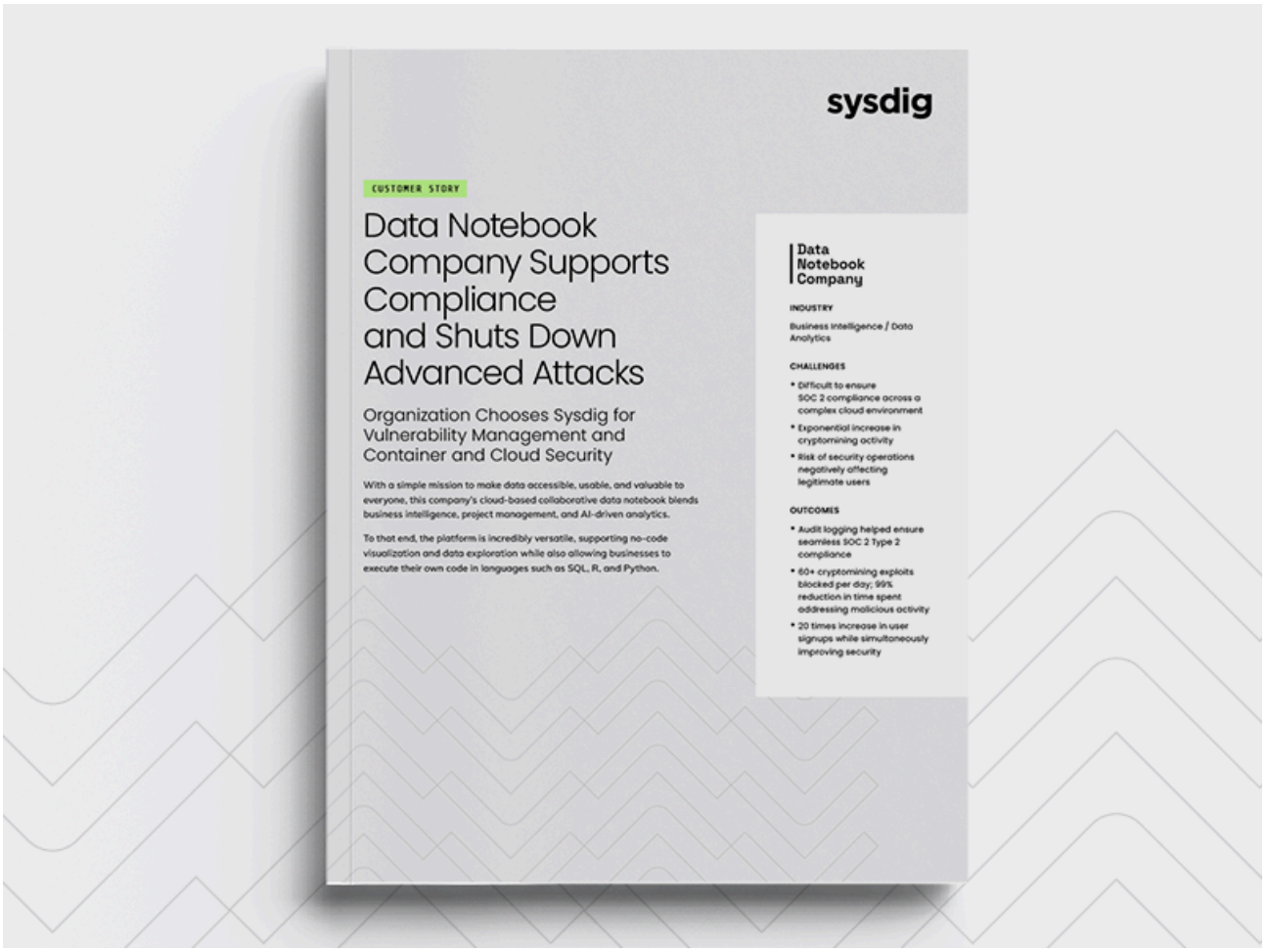
Cloud MonitoringKubernetes




BLUEPRINT. Your Blueprint to Securing Workloads, Containers, and Kubernetes, the Right Waypdf



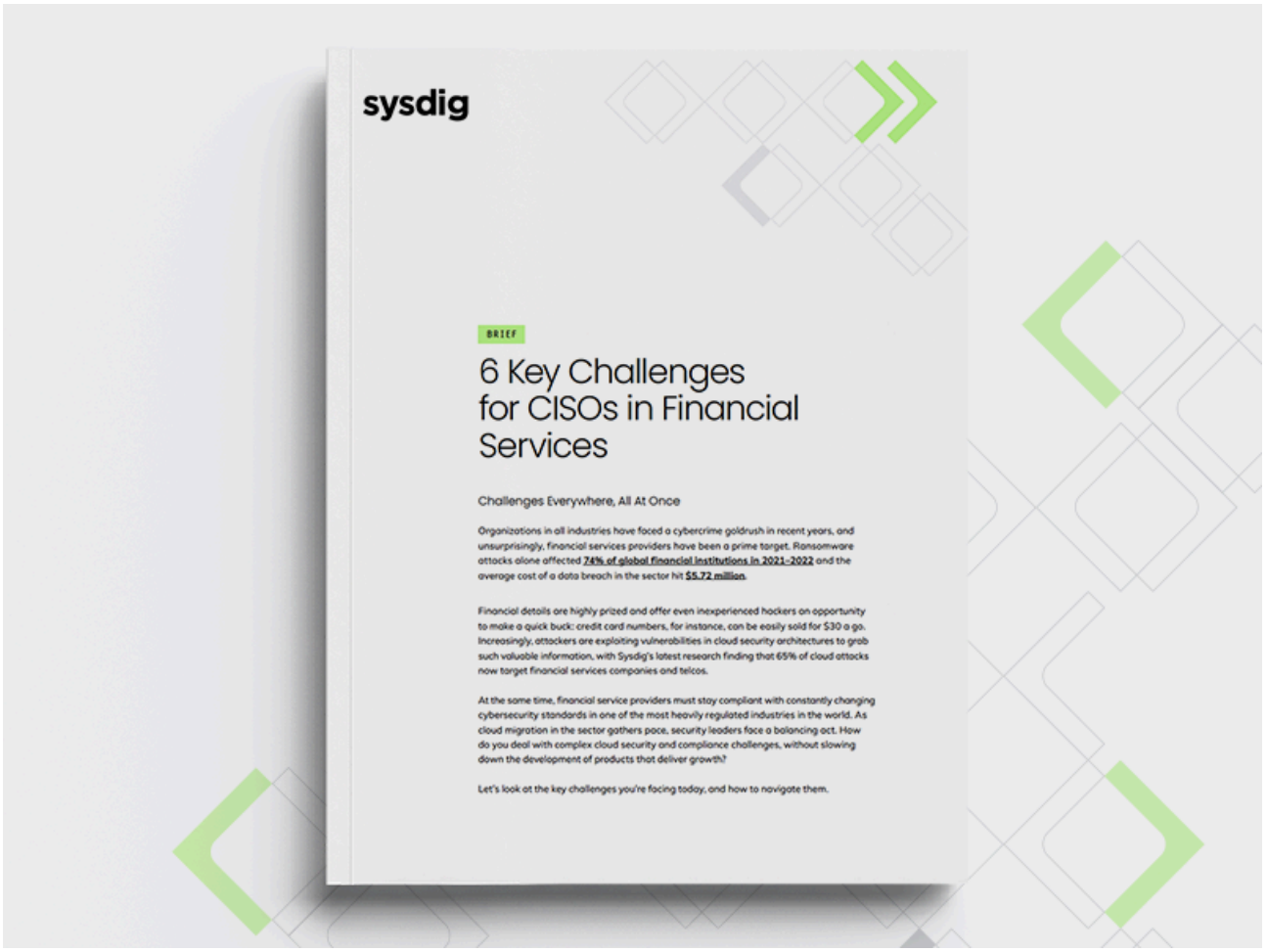

REPORT. Frost Radar Cloud Native Application Protection Platforms 2022pdf




CASE STUDY. Data Notebookpdf

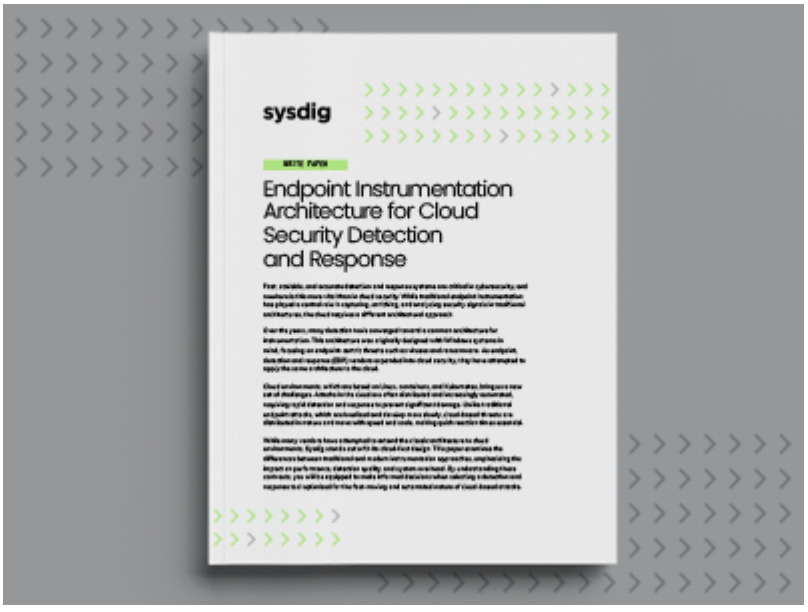
Cloud MonitoringSysdig Monitor


CASE STUDY: Partiorpdf




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

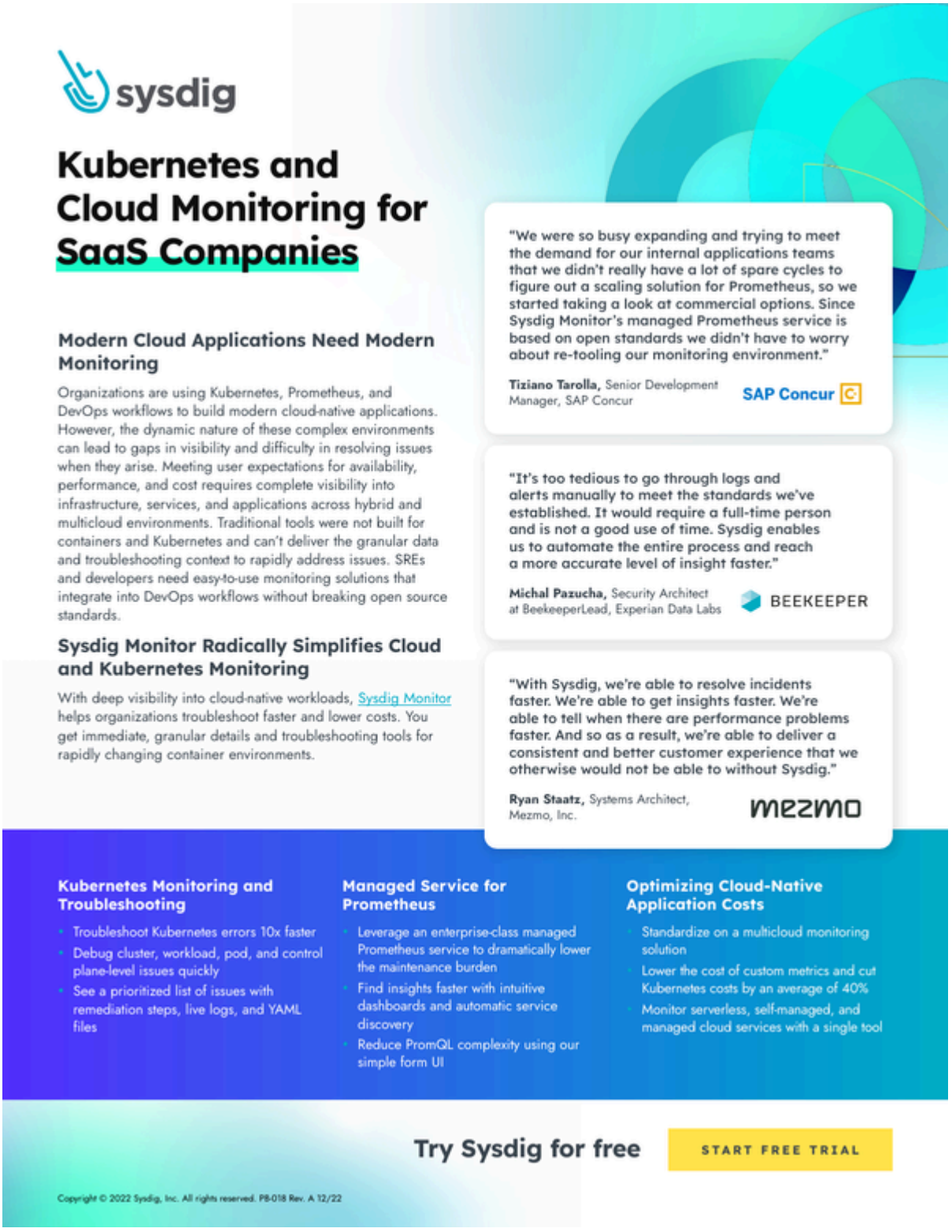

WHITEPAPER JP. AIBOM: The infrastructure, risks, and how to secure AI modelspdf




Endpoint Instrumentation Architecture for Cloud Security Detection and Responsepdf

VIDEO. The Sysdig vision.video


REPORT. ESG Survey Report: Cloud Detection And Responsepdf




[BRIEF: Kubernetes and Cloud Monitoring for SaaS Companiespdf]

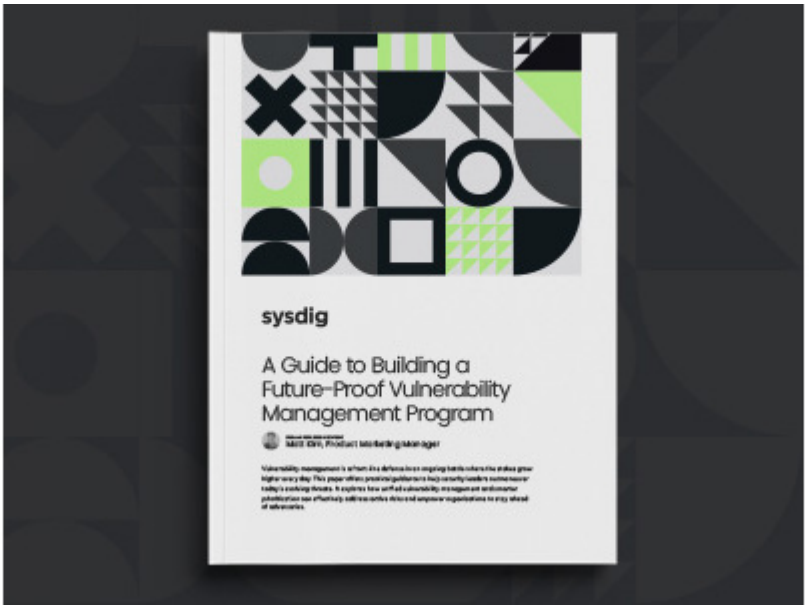
[Kubernetes]


WHITEPAPER. AIBOM: The Infrastructure Risks And How To Secure AI Modelspdf

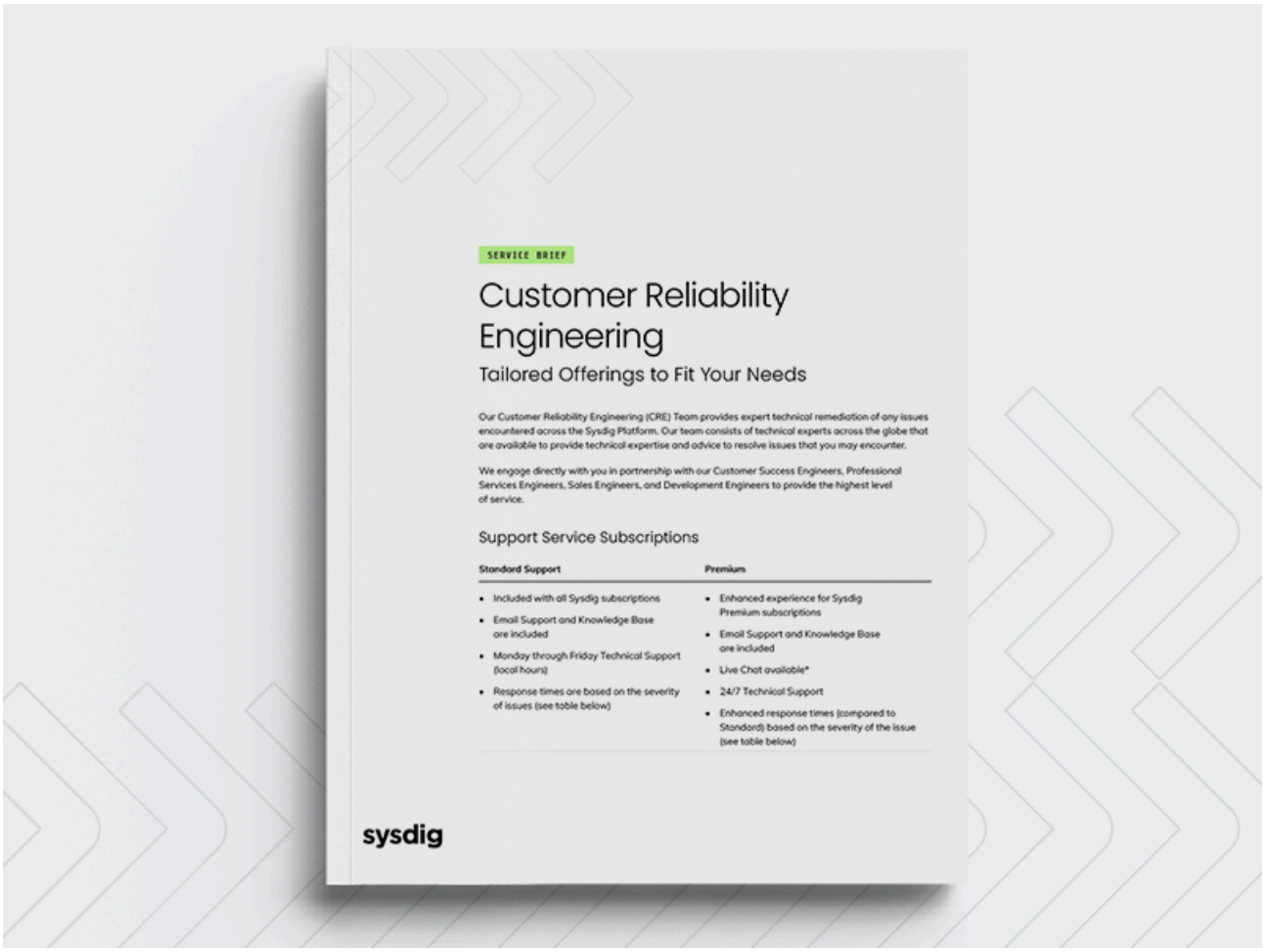

Cloud Identity Insightspdf


BRIEF. Cloud Threat Detection Built On Open Sourcepdf

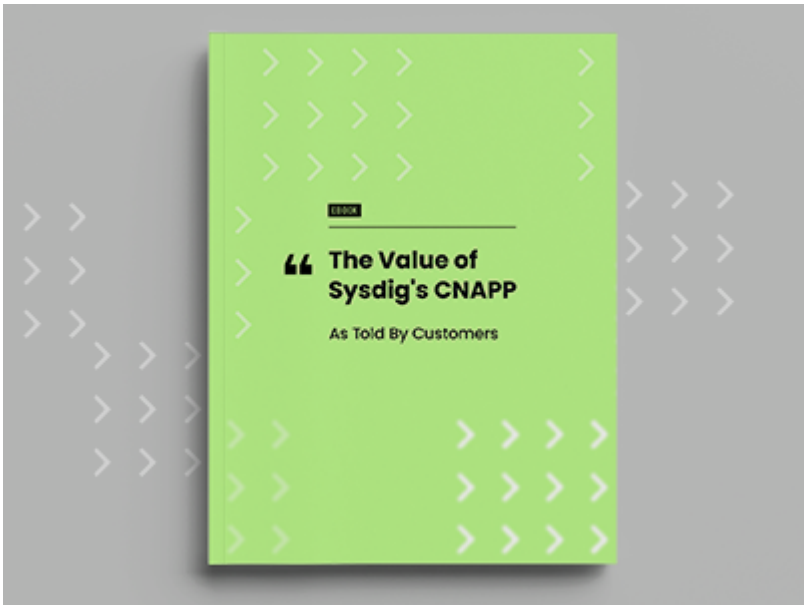
FalcoOpen Source




GUIDE. A Guide to Building a Future-Proof Vulnerability Management Programpdf

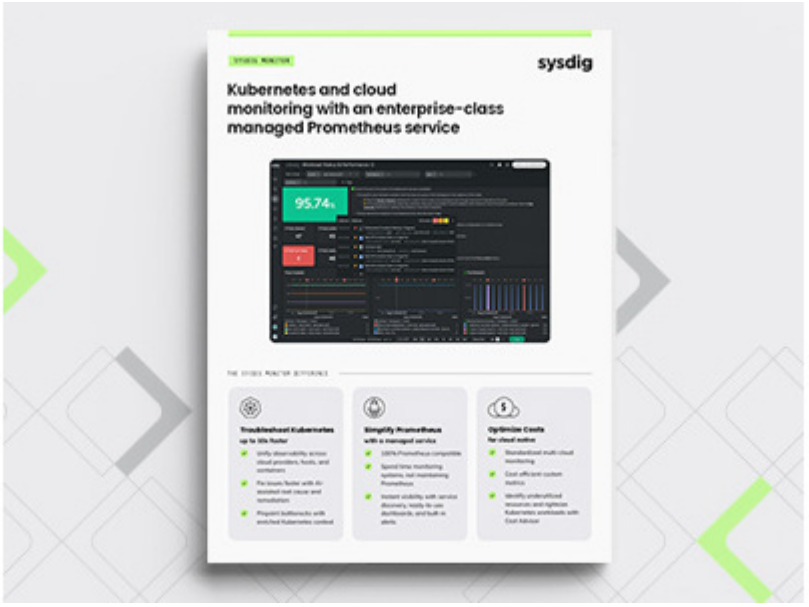



SERVICE BRIEF. Customer Reliability Engineeringpdf



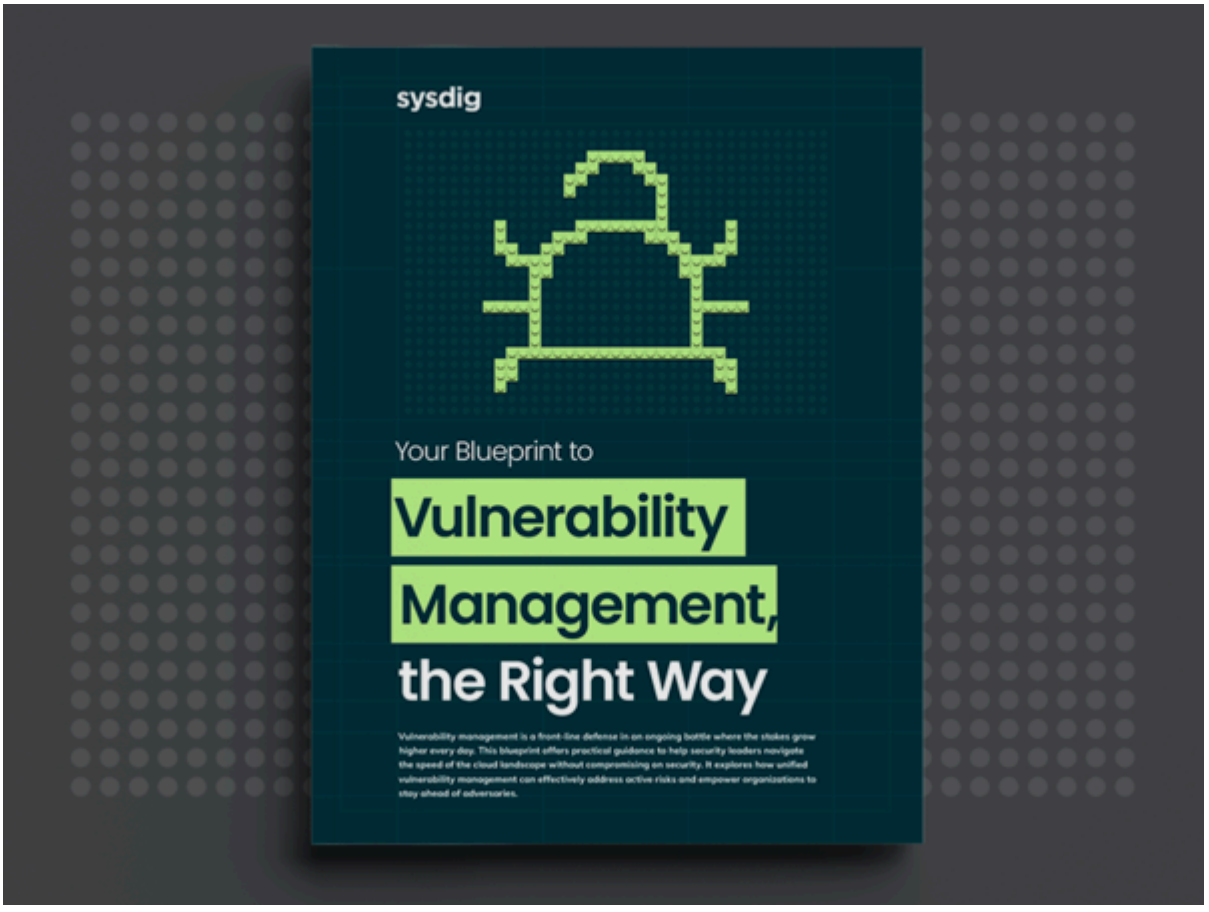

The Value of Sysdig's CNAPPpdf

CSPM




PRODUCT BRIEF. Sysdig Monitorpdf

Sysdig Monitor



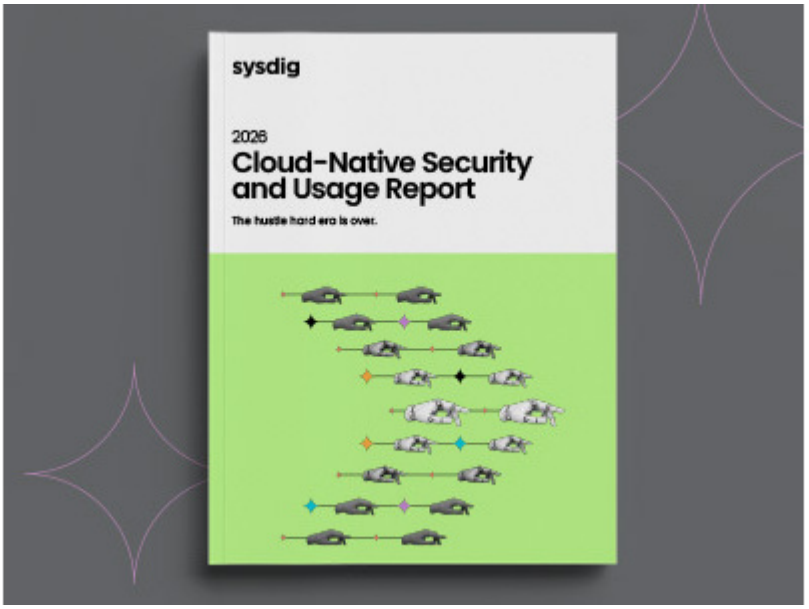

Blueprint. Vulnerability Management, the Right Way.pdf


GUIDE. Kubernetes Rightsizing Guidepdf

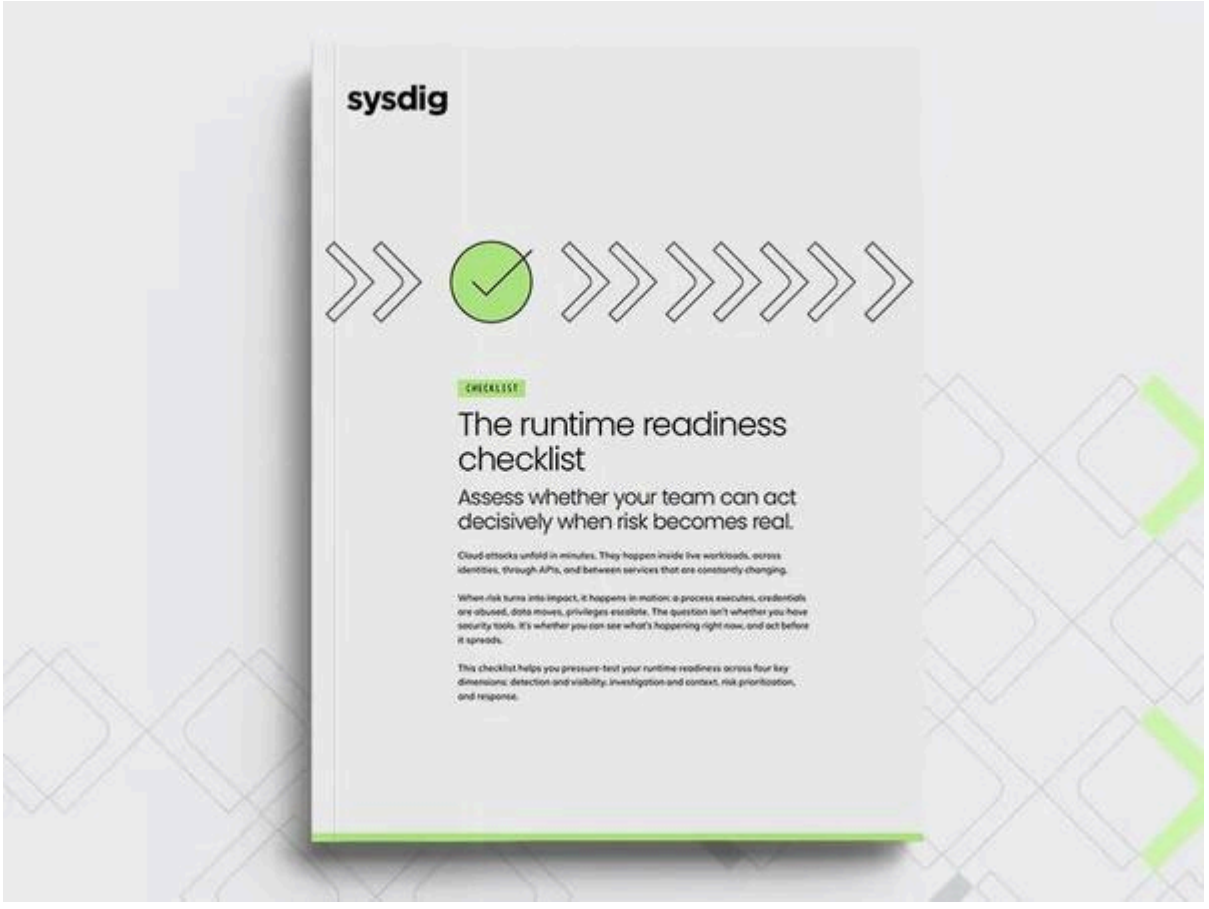
Kubernetes


[BRIEF. Stop Watching, Start Defending for Practitionerspdf]


[Frost Sullivan Company Of The Year Container Kubernetes Securitypdf]



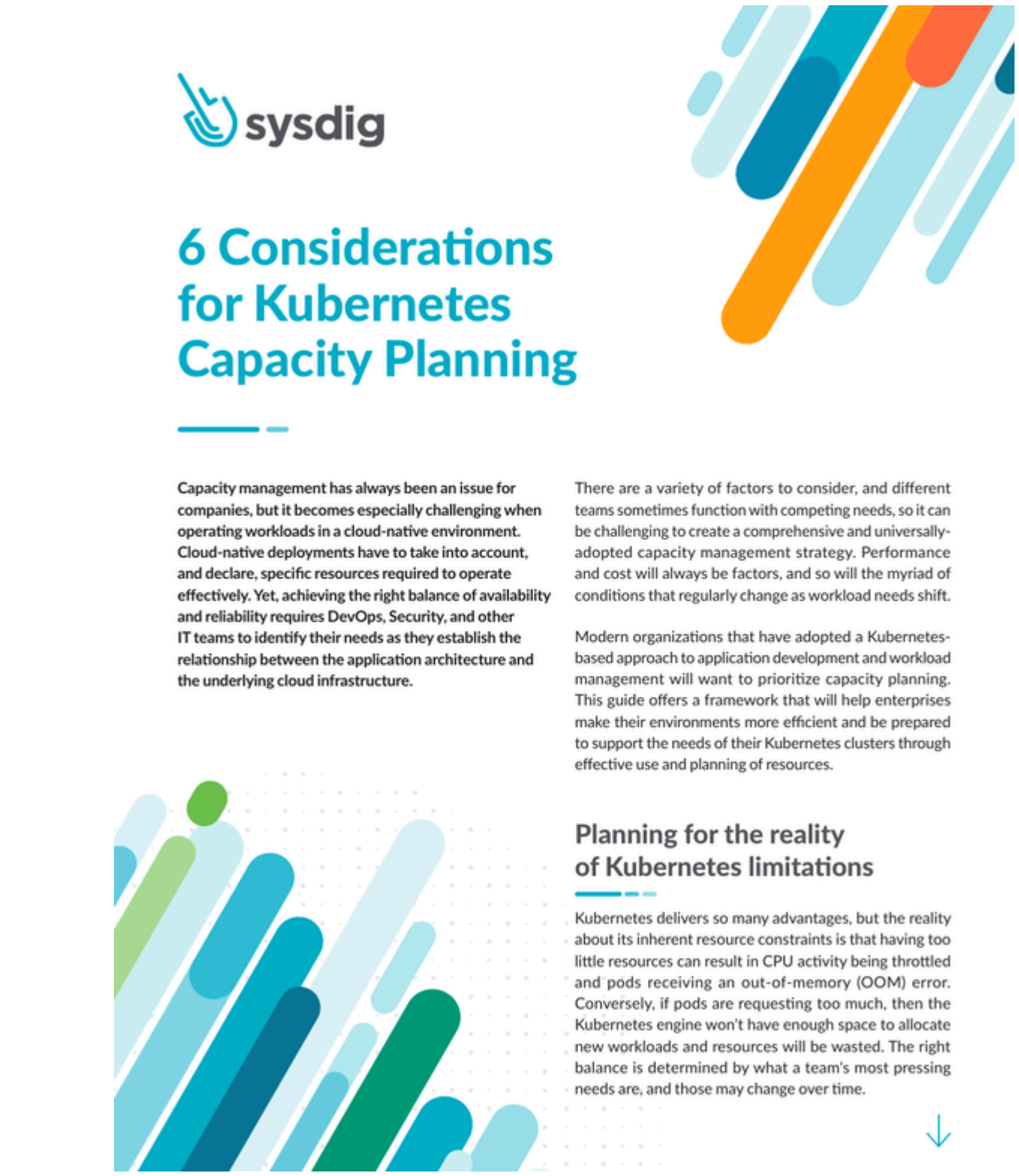

REPORT. 2026 Cloud-Native Security and Usage Reportpdf




CHECKLIST. The runtime readiness checklistpdf


VIDEO. Sysdig Monitor: Overview of Alertsvideo

Cloud MonitoringKubernetesPrometheusSysdig Monitor

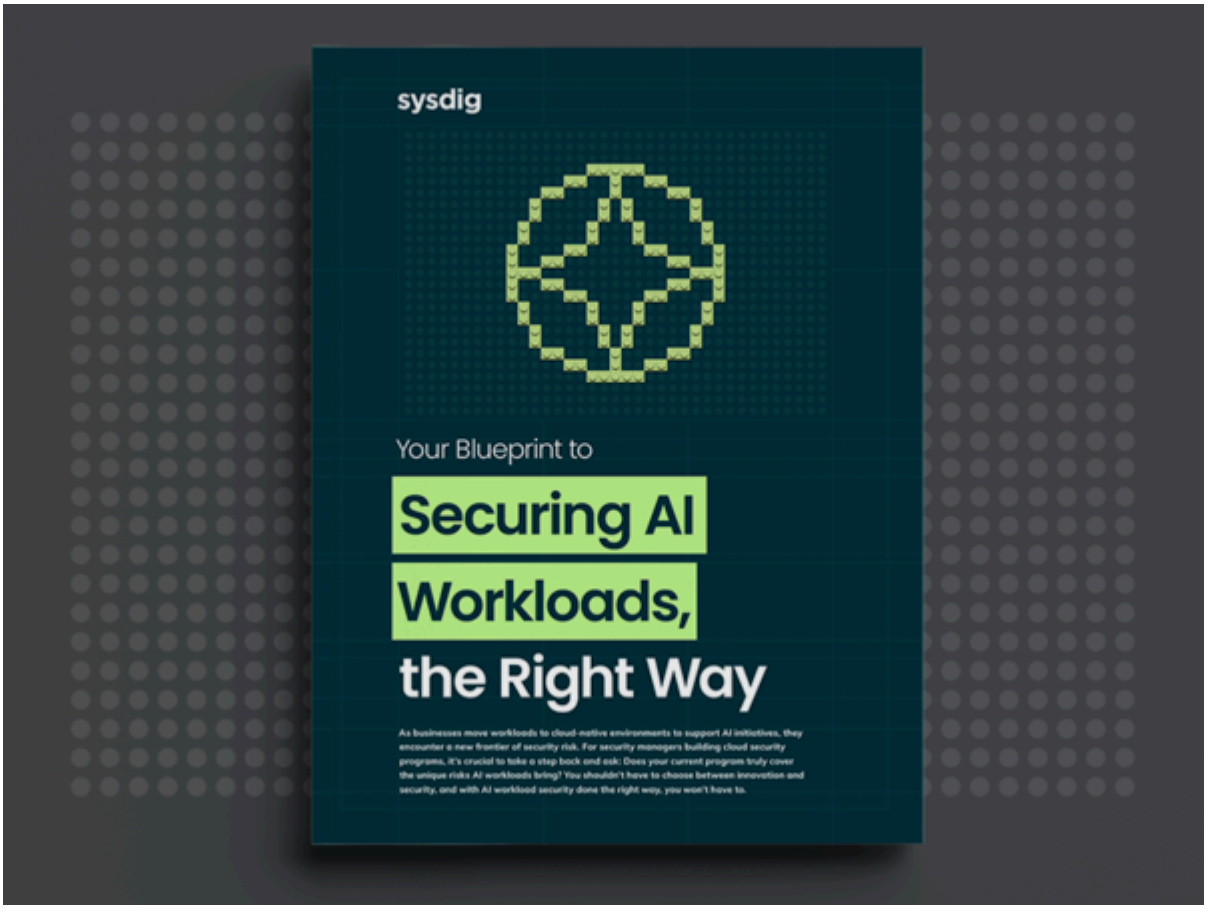



BRIEF: 6 Considerations For Kubernetes Capacity Planningpdf

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
```

## 2

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
```

## 3

REPLICATION

### Replication lag

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

```
pg_replication_lag > 10
```

## 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
```

## 5

STORAGE

### 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
```

## 6

NETWORKING

### 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
```

## 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_containe
r_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
```

sysdig

INFOGRAPHIC. Top 10 Metrics In Postgresql monitoring with Prometheuspdf

Cloud MonitoringOpen SourcePrometheusSysdig Monitor


BRIEF: 5 Keys to Optimizing Costs of Running Cloud-Native Appspdf

Cloud MonitoringCost OptimizationSysdig Monitor


VIDEO. Scaling Prometheus Monitoring: IBMvideo

Cloud MonitoringIBMPrometheusSysdig Monitor


[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.[1]

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.[2]

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.[3] 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.

[1] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.
[2] Ibid.
[3] 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



WHITE PAPER. The Power of Native Cloud Detection and Response Servicespdf


### 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.

sysdig SECURE EVERY SECOND.

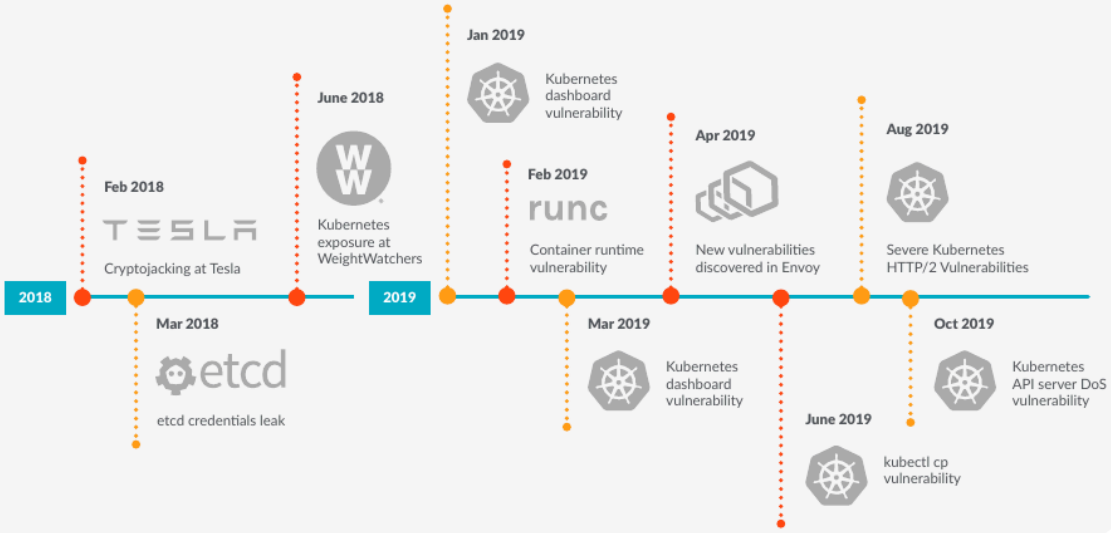
BRIEF. Company Overviewpdf

sysdig

# Securing Kubernetes in Production

## Are you ready?

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




* IDC TechBrief: Containers

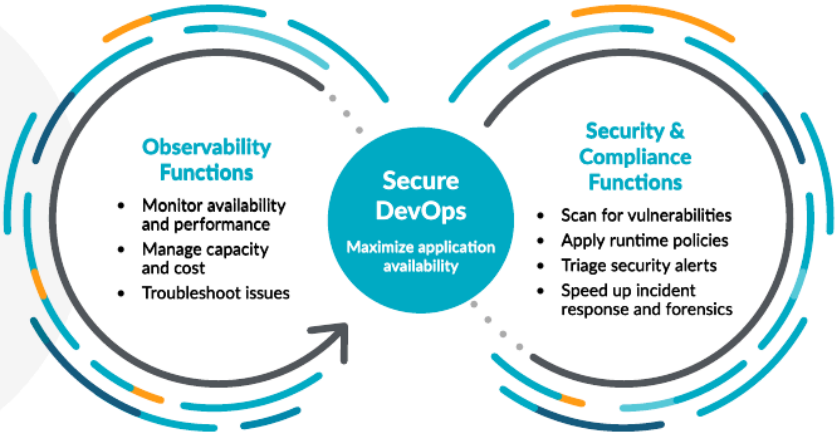
| | | |
|---|---|---|
| **Vulnerabilities or misconfigurations were not addressed before deployment** | **Best practices for runtime prevention and detection were not in place** | **Most container breaches are often undetected until it is too late** |
| **52% container images fail scans with high severity* that leaves applications exposed to attacks*** | **On average, 21 containers per node are running as root, opening the door for container breakouts*** | **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

**1**

Scan for vulnerabilities early and ensure configuration meets CIS best practices

CIS Benchmarks

Vulnerability Feeds

*Examples*

- "Containers must not run as root"
- "Block images with high severity vulnerabilities"

**2**

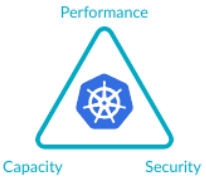
Apply precise runtime policies for prevention and detection


*Examples*

- "MITRE ATT&CK framework for container runtime security"
- "Did someone launch a privileged container?"

**3**

Use the same data for security, performance and capacity monitoring

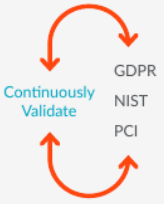



*Examples*

- "Who are my top talkers?"
- "Is this CPU spike related to a DoS attack?"

**4**

Continuously validate compliance (PCI, NIST) across the Kubernetes lifecycle

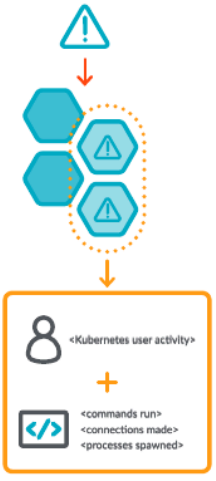



*Examples*

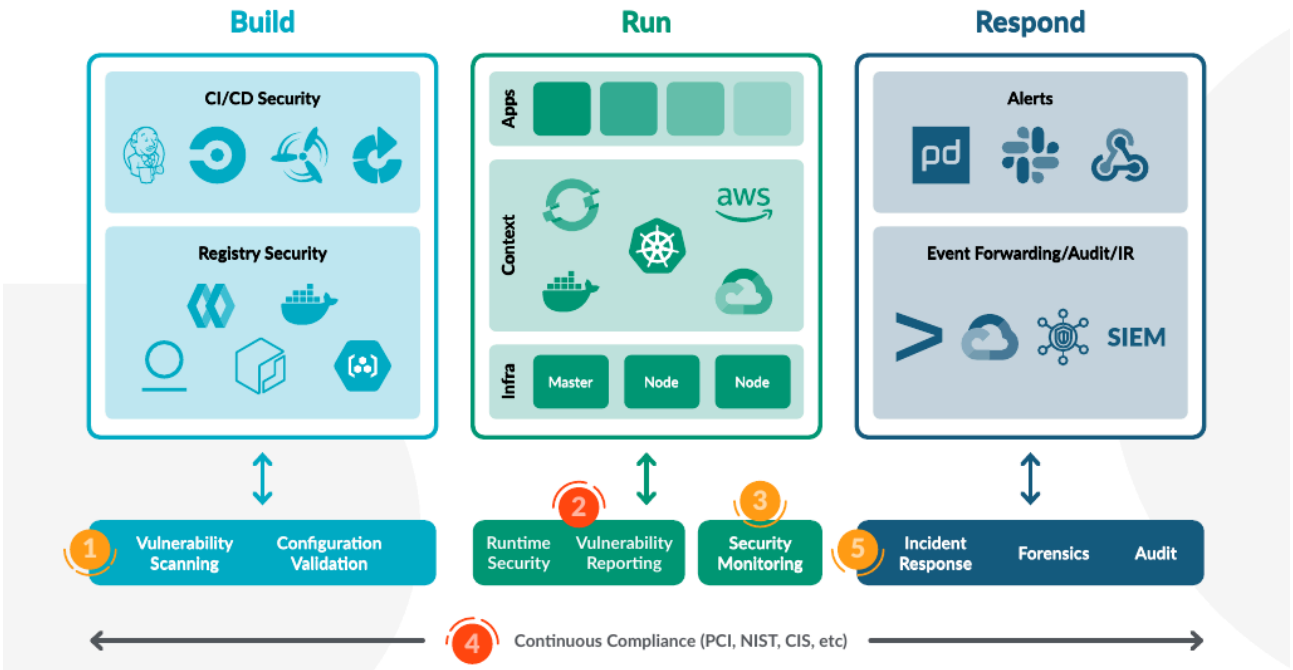
- "Is it a malicious attack or configuration error?"
- "PCI Req. 11.4 – Use IDS/IPS to Detect and Prevent Network Intrusion"

**5**

Implement a response framework for troubleshooting and forensics




## 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

sysdig

[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

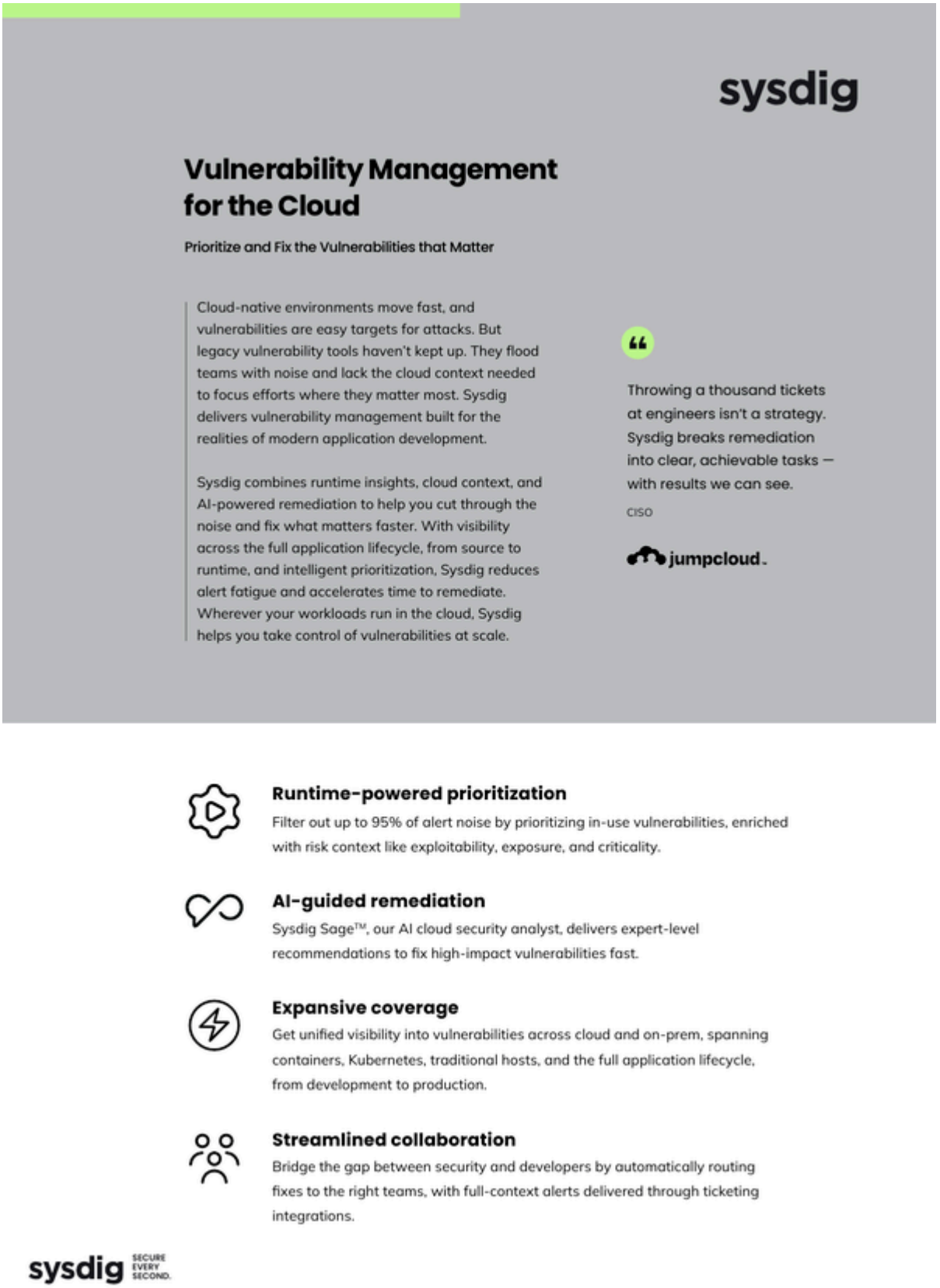
While code, container, and IaC security best practices provide protection from known issues and misconfigurations, these practices alone are not enough. A host of security threats, by their very nature, only manifest during runtime. Detecting and responding to malicious activity such as privilege escalation attempts in containers requires new vantage points and cloud-native controls.

## Prioritize security alerts that matter

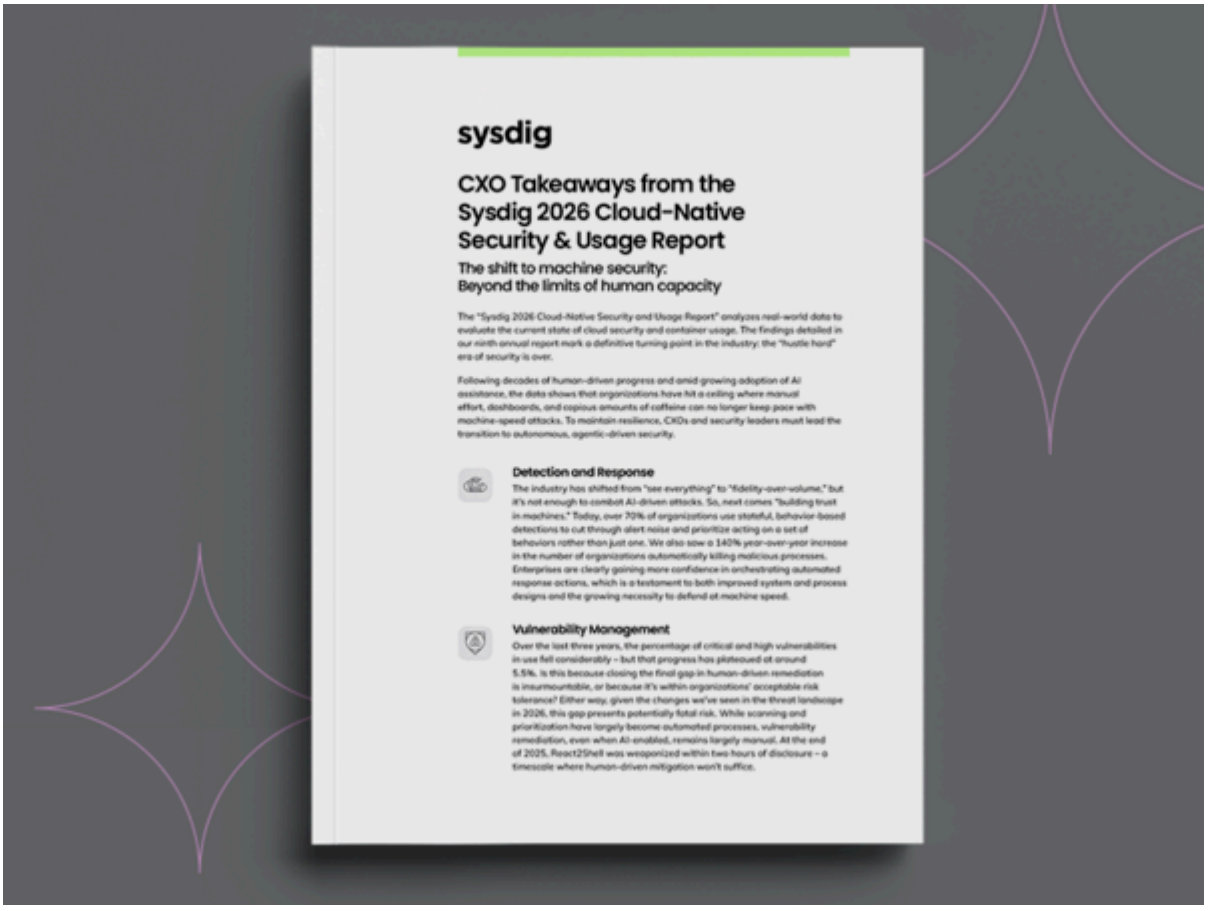
Containers are often bloated with contents and packages, overwhelming developers with vulnerabilities. Attempting to wade through an unmanageable number of issues takes precious time away from coding and leaves organizations open to risk. Techniques such as using runtime intelligence will help developers 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]




SOLUTION BRIEF. Vulnerability Management for the Cloudpdf




BRIEF. CXO Takeaways from the Sysdig 2026 Cloud-Native Security & Usage Reportpdf

sysdig

# 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 |
|---|---|---|
| Build and manage Prometheus. Customize monitoring capabilities to fit your teams, applications, and cloud-native rollout. | Configuration and Maintenance | Free up valuable resources with a completely vendor-supported On-Prem or SaaS solution that offers full Prometheus compatibility. |
| Identify exporters to monitor applications and services from the open source community. | Integrations | Access managed integrations for applications via PromCat, paired with the right dashboards and alerts. |
| Gain visibility with metrics ingested every 10 seconds and limited retention for each Prometheus server. | Scale | Centralize on a scalable platform that offers millions of time series data with 10-second resolution and 13 months of retention. |
| Trial and error to understand what is important to monitor in a cloud-native context. | Troubleshooting | Get access to deep container visibility with the ability to troubleshoot faster and proactively with service and container level context. |
| Secure Prometheus data connection and control access to the metrics on a server by server basis. | Access | Use enterprise access controls like RBAC, SSO, LDAP or Sysdig Teams. |

Learn more about turnkey Prometheus scaling solution, **Sysdig Monitor**

LEARN MORE

sysdig

ING-005 Rev. A 4/20

[INFOGRAPHIC. Need to Extend Prometheus Monitoring?pdf]

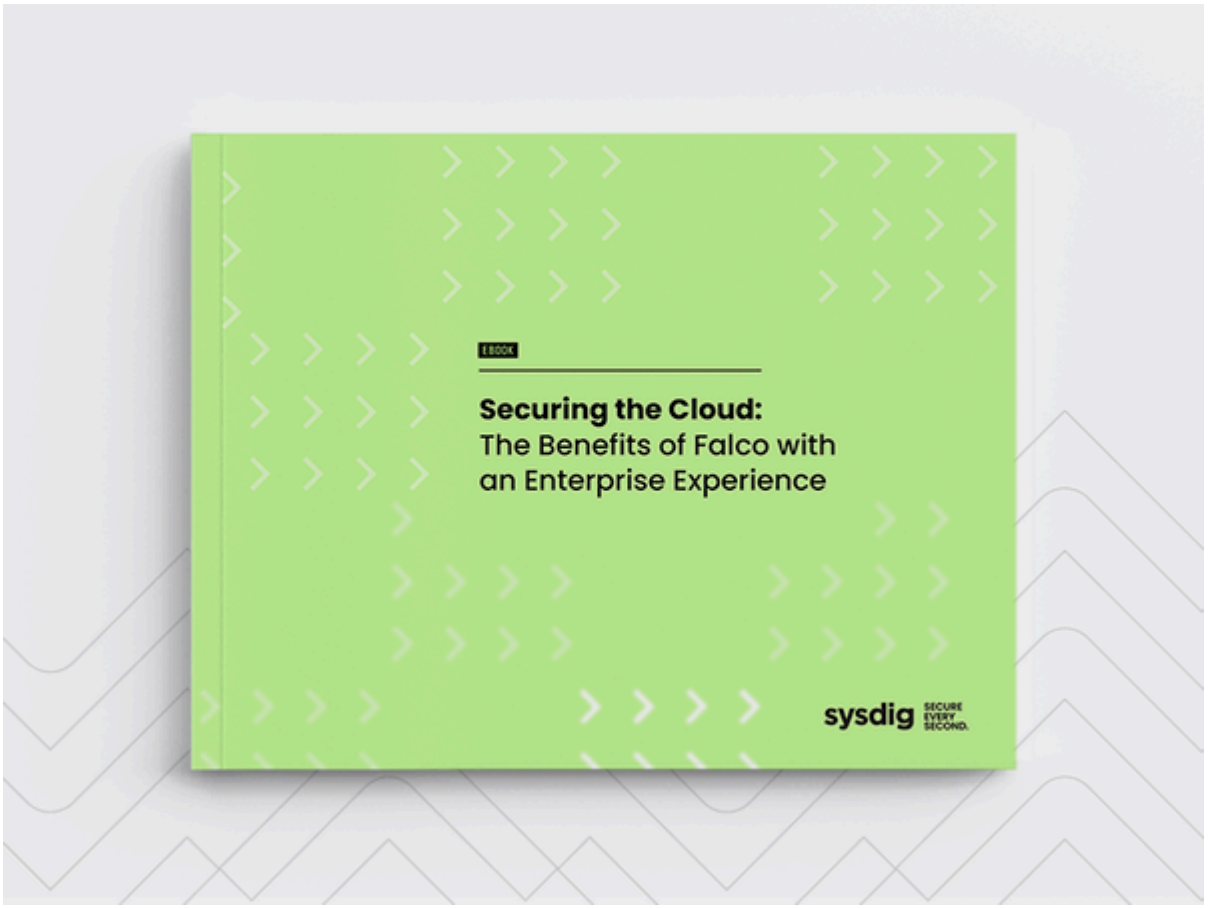
[Open SourcePrometheusSysdig Monitor]


[VIDEO. KubeCon Intro: Falco - Loris Degioanni, Sysdigvideo]

CASE STUDY. Global Digital Infrastructure Providerpdf

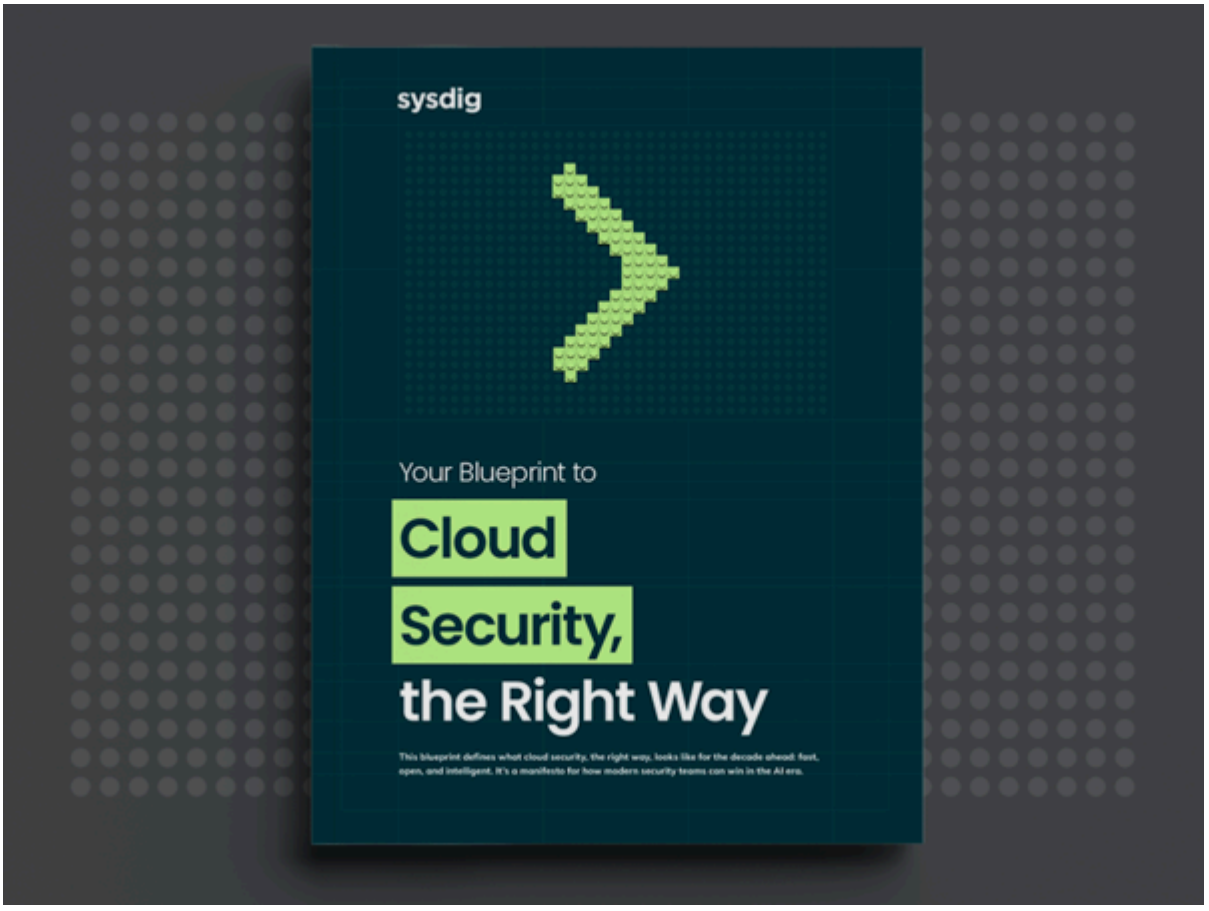

BLUEPRINT. Agentic Cloud Security, the Right Way.pdf


BRIEF: 4 Critical Business Values Delivered By Sysdig Cloud Detection And Responsepdf




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 Wrongvideo

KubernetesSysdig Monitor


VIDEO. Extending security with Sysdig and IBM Cloud Pak for Multicloud Management (MCM)video


**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.

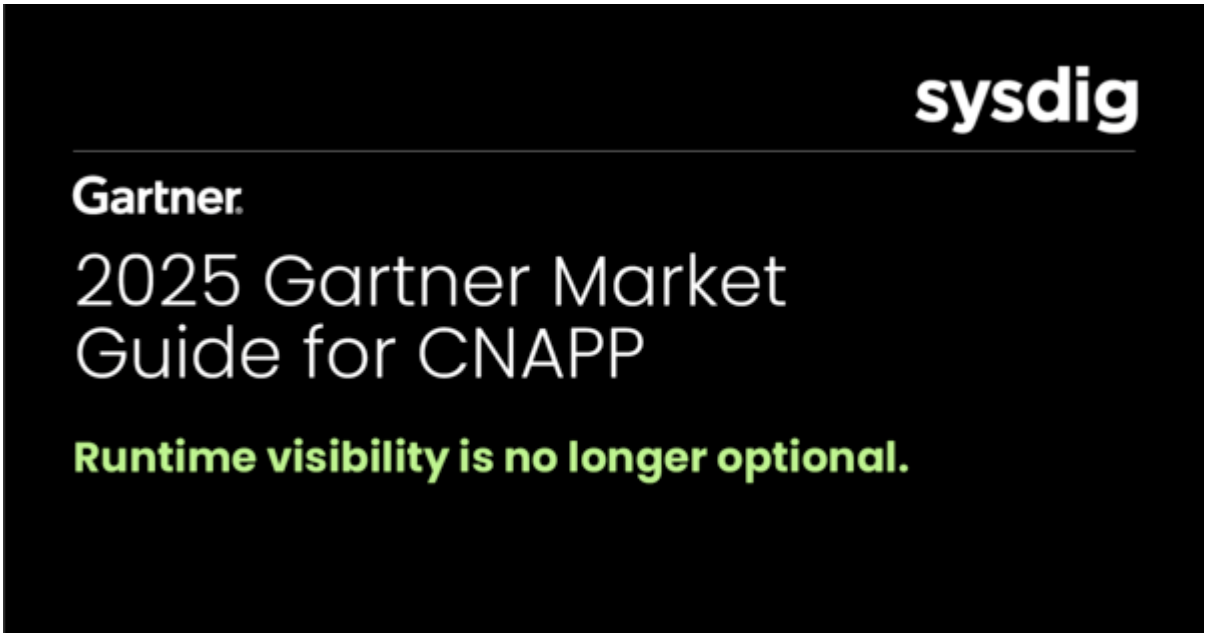
sysdig SECURE EVERY SECOND.

Solution Brief: Sysdig Sagepdf

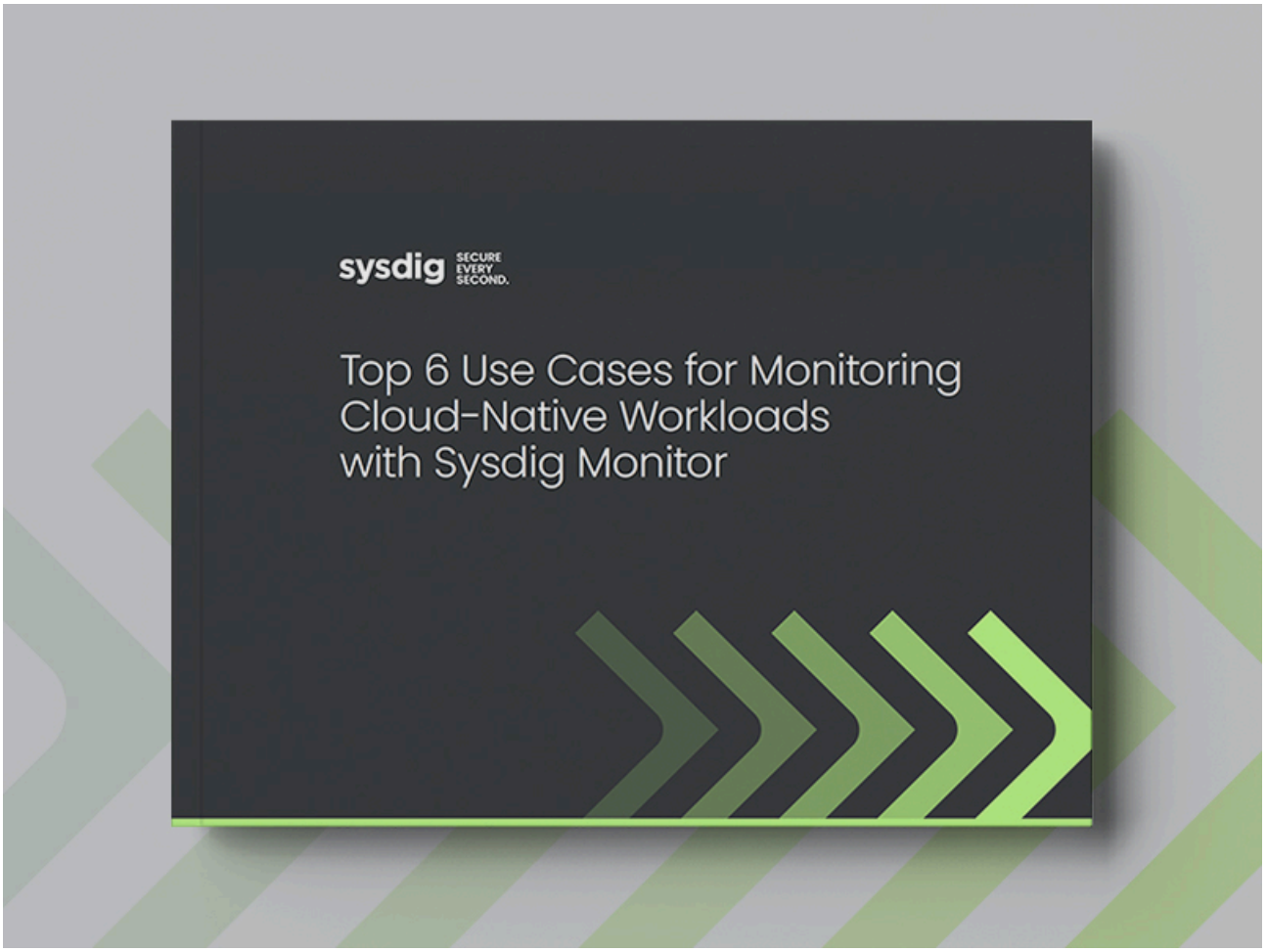
Sysdig Sage


TOOLKIT. The Practitioner's Toolkit for Securing Workloads, Containers, and Kubernetespdf


Why it's time to rethink vulnerability management | Sysdigwebpage

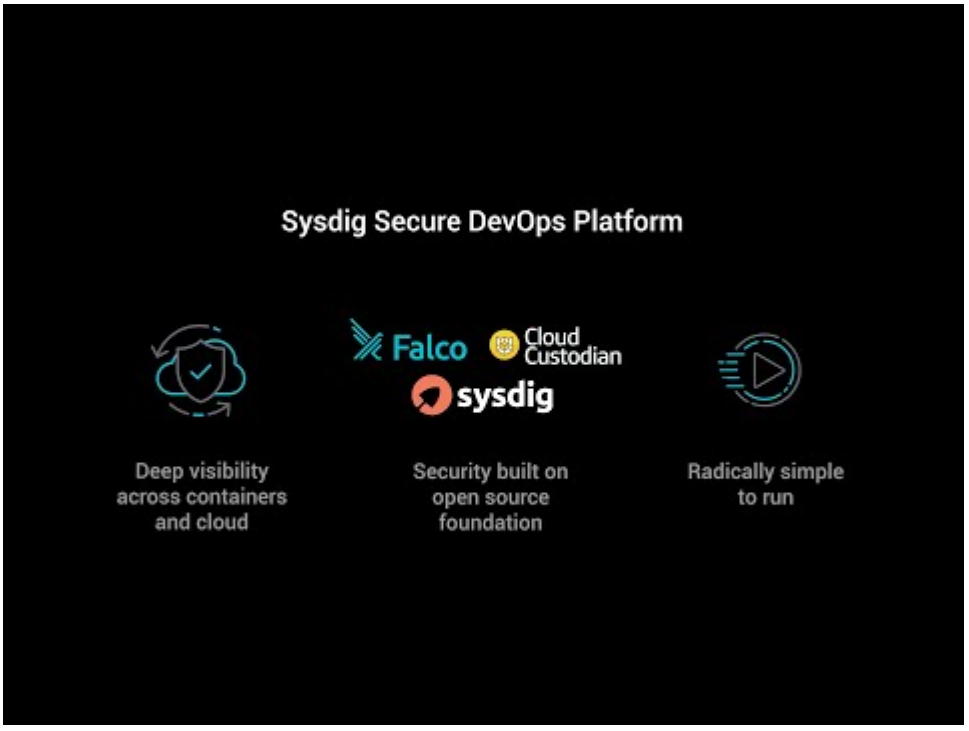



2025 Gartner® CNAPP Market Guide: Runtime visibility is no longer optional | Sysdigwebpage




EBOOK. Top 6 Use Cases Monitoring Cloud Native Workloads With Sysdig Monitorpdf

KubernetesSysdig Monitor



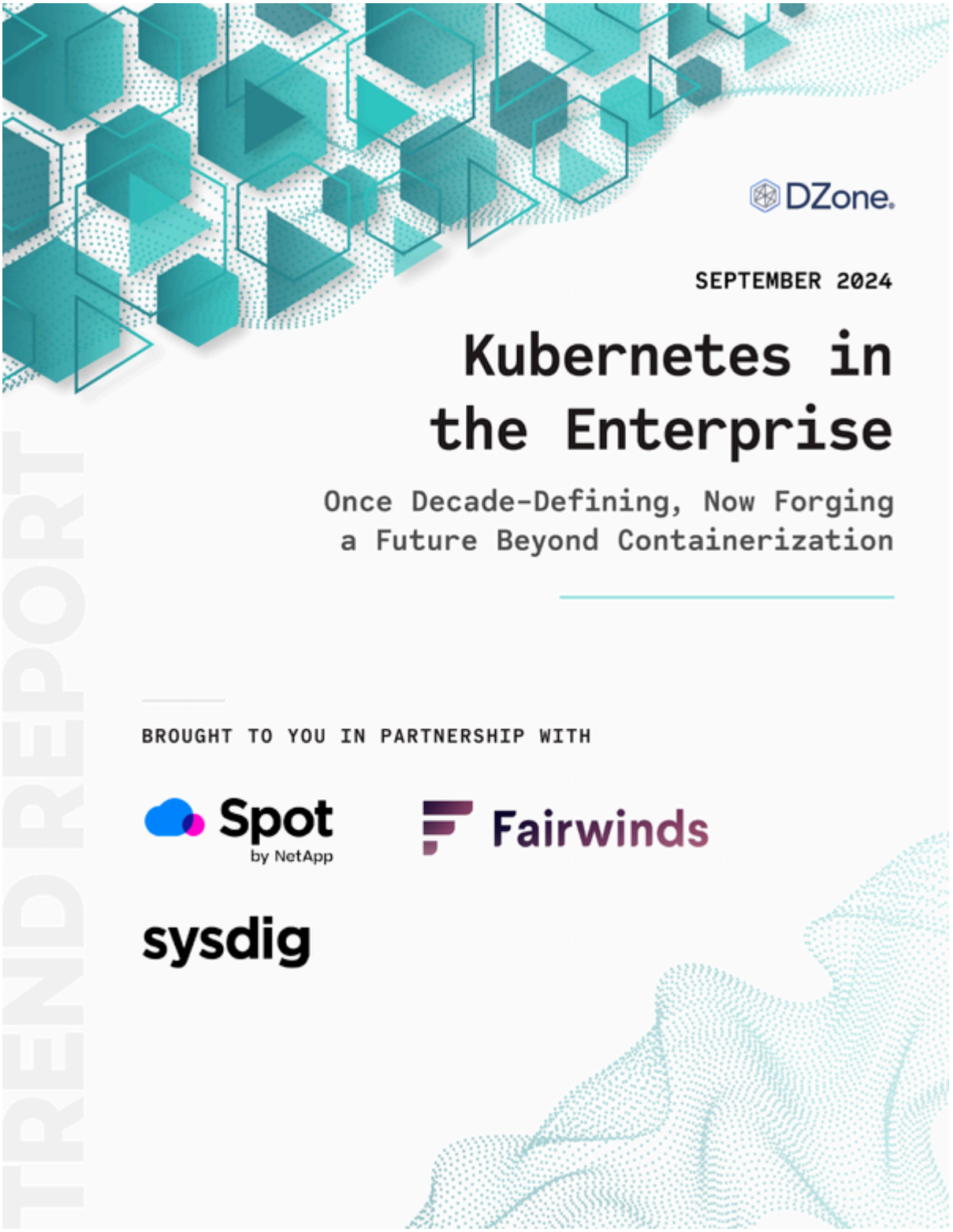

VIDEO. Unified threat detection across containers and cloud with Sysdigvideo


[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]




[REPORT. DZone Kubernetes in the Enterprise Trend Report 2024pdf]

[KubernetesSoftware development]


CASE STUDY. Retail Tech Companypdf


INFOGRAPHIC. The Grand Atlas of Software Securitypdf

sysdig

# 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.

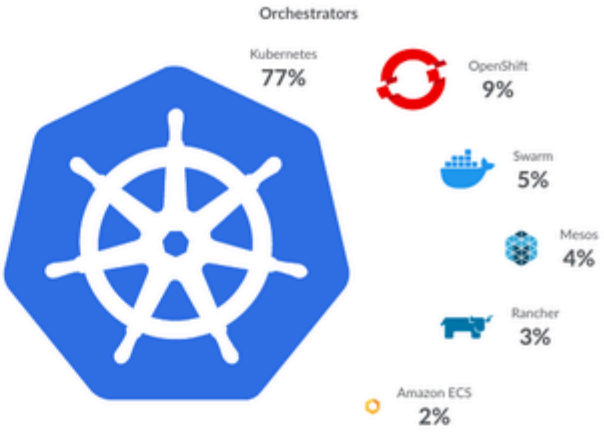
We've collected insights from real-time, real-world usage of over 2 million running containers to shed light on the current state of infrastructure, applications, security, and compliance practices.

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.

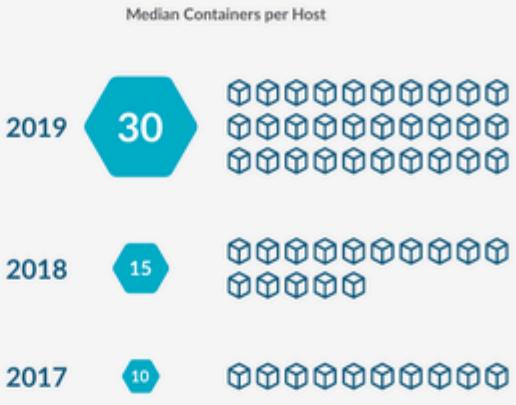
The results change significantly when looking at on-prem deployments. Read the full report to see how.




Container Density

### Containers-Per-Host Density Increases 100%

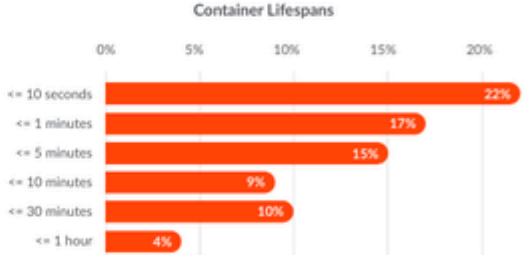
The median number of containers per host doubled to 30 in the past year. More apps and more compute power = more containers.



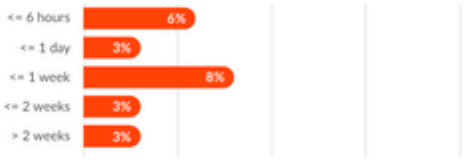

Lifespan

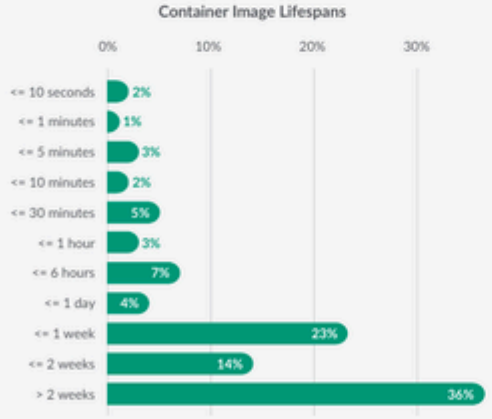
### The Short Life of Containers

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



doubled since 2018 to 22%. The growth of batch processing and serverless frameworks on Kubernetes is likely responsible for the shift.




Lifespan

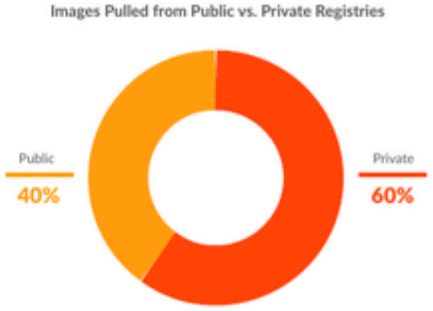
## Container Image Churn

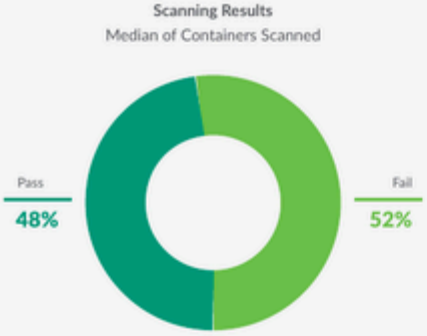
Over half of container images are replaced – aka churn – in a week or less. The use of CI/CD pipelines that help developer teams deliver code faster, and turn great ideas into reality faster, results in more new images, more often.

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.




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

Security

Attempt to access sensitive volumes, directories, or files

## 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

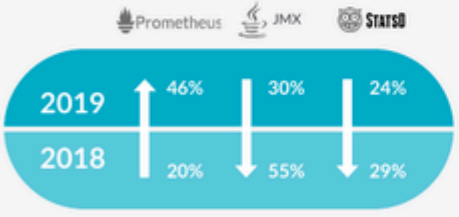
## Container Compliance Issues

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.


Custom metrics

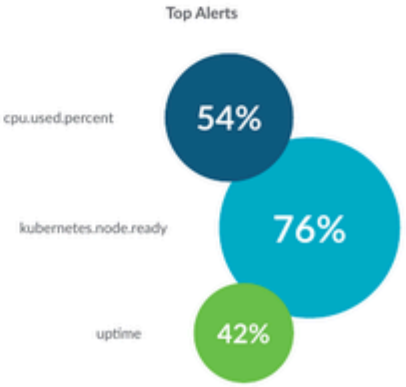
## Prometheus Rises

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

sysdig

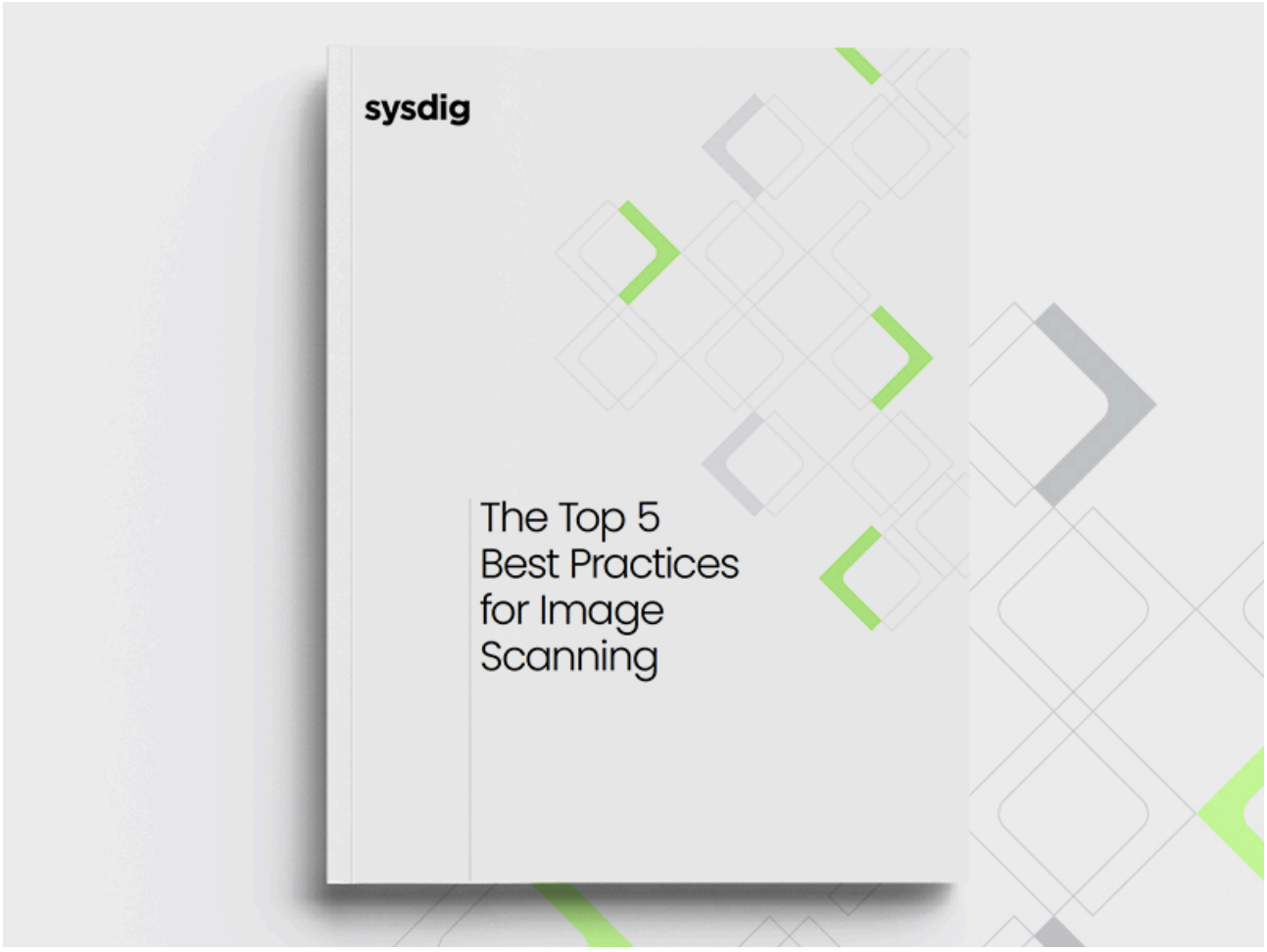
2019 Container Usage Snapshotpdf

Kubernetes


EBOOK JP. Top 5 Use Cases for Securing Cloud and Containers with Sysdig Securepdf

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