![sysdig logo]

Navigating **Cloud and Container Security Risk** and Optimising **Cloud Spend**

Bruno Gabriel da Silva

Sysdig 2023 Cloud-Native Security and Usage Report

Based on data *from Sysdig customers* for **billions of containers,** thousands of cloud accounts, and thousands of applications over the course of the last year

How long do you think containers will live?

- Two to three days
- A week or more
- Minutes
- Hours

72%

of containers live
less than **5 minutes**

3 Themes For 2023

1

Container risks
are growing

2

Zero trust
is difficult in cloud

3

Cloud cost
is running away

sysdig

What trends are keeping you up at night?

- ❑ Vulnerabilities
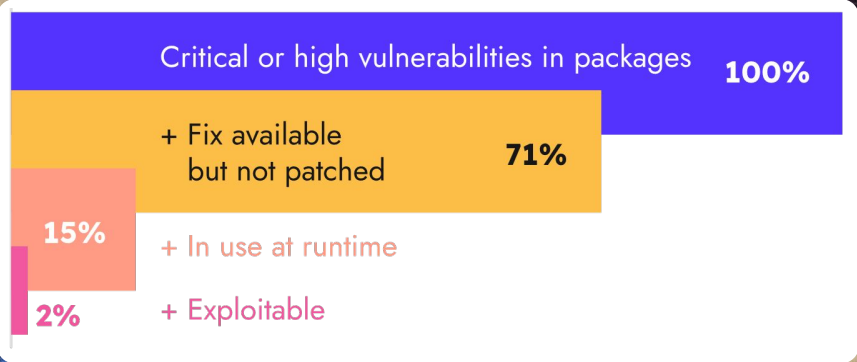- ❑ Cost
- ❑ Identity and Access Management
- ❑ All of them

Severe vulnerabilities lurk in container images

87%
of container images have
high or critical vulnerabilities

Critical or high vulnerabilities in packages — 100%

+ Fix available but not patched — 71%

15% + In use at runtime

2% + Exploitable

Security teams struggle to prioritize risk

15%
of high or critical vulnerabilities
are in-use at runtime and need addressing
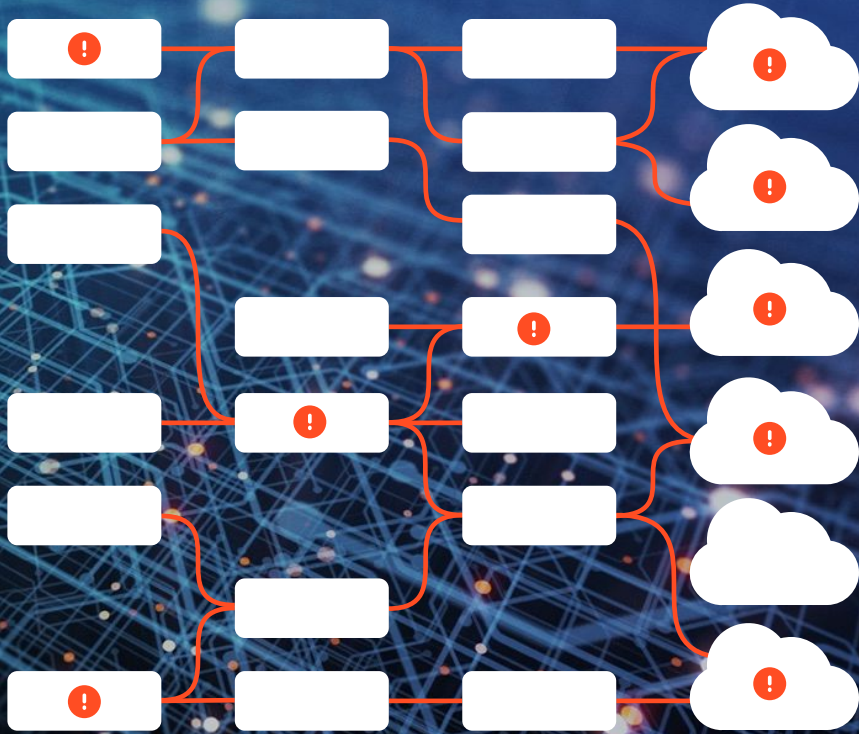
Container risks amplify supply chain risk

Cloud permissions erode zero trust efforts

90%
of granted permissions are not used

Cluster sizing impacts cost dramatically
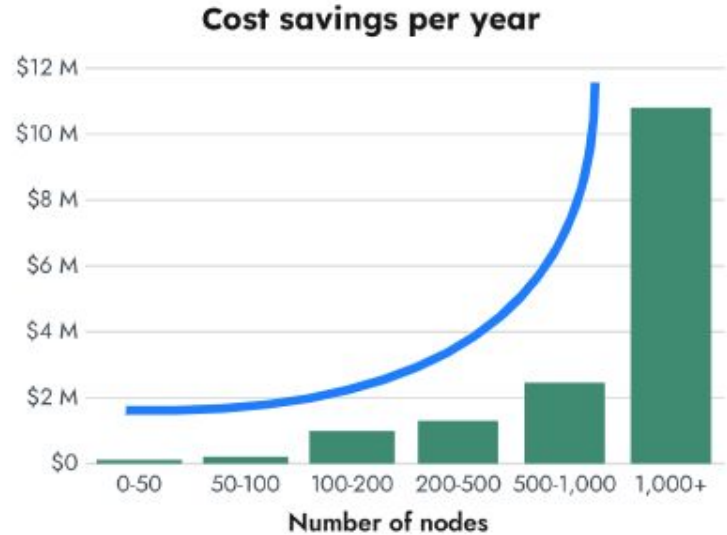
Organizations running more
than 1000 nodes could save
$10M Annually

Cluster sizing impacts cost dramatically

On average, organizations are **overspending by 40%**

Cost savings per year

Container lifetimes complicate operations

72%
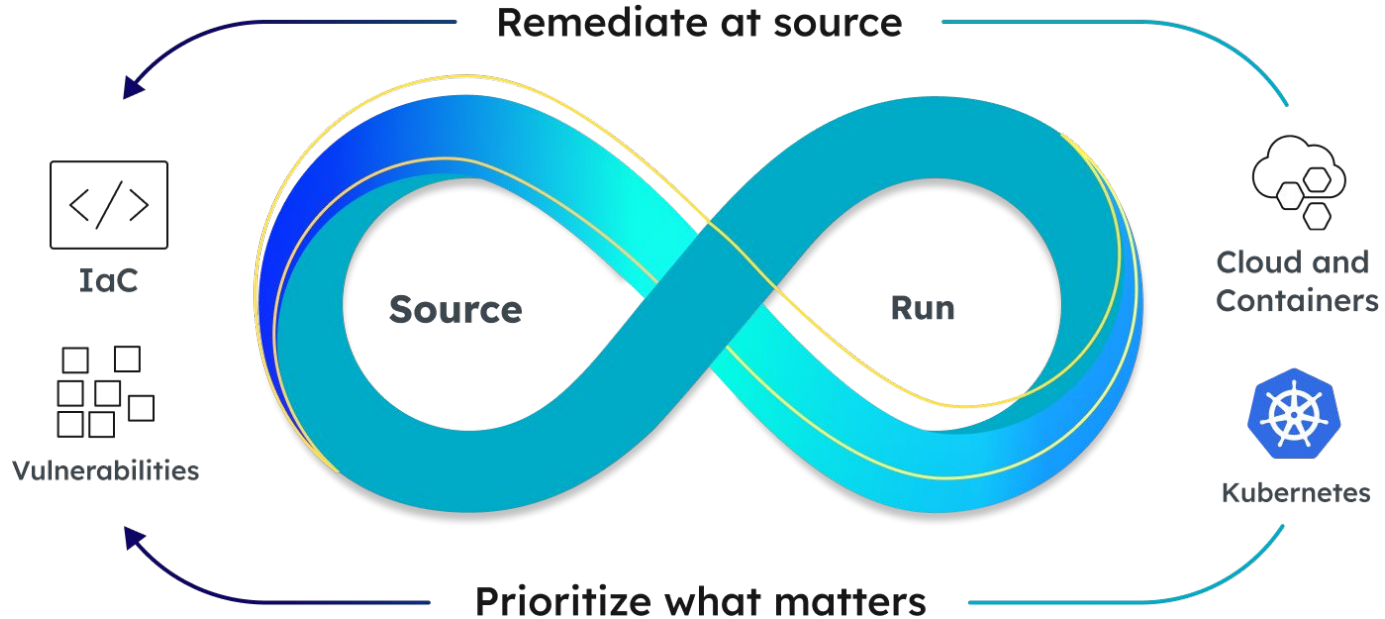of containers live less than
5 minutes (up from 44%)

Workload right-sizing is elusive

69%
of CPU resources are unused
(up from 34%)

Sysdig: Cloud & Workload Security from Source to Run

Remediate at source

IaC

Vulnerabilities

Source

Run

Cloud and Containers

Kubernetes

Prioritize what matters

Our Mission: To Accelerate & Secure Cloud Innovation

We are Builders.

The open source standard for cloud-native threat detection

Deep container forensics and troubleshooting

aws · Microsoft Azure · Google Cloud · IBM Cloud

We are Trusted.

CISCO · COMCAST · Alaska AIRLINES

Ford · Goldman Sachs · IBM

experian · SOCIETE GENERALE · McKinsey & Company

MERCARI · Arkose Labs · SAP Concur

finra · worldpay from FIS · YAHOO! JAPAN
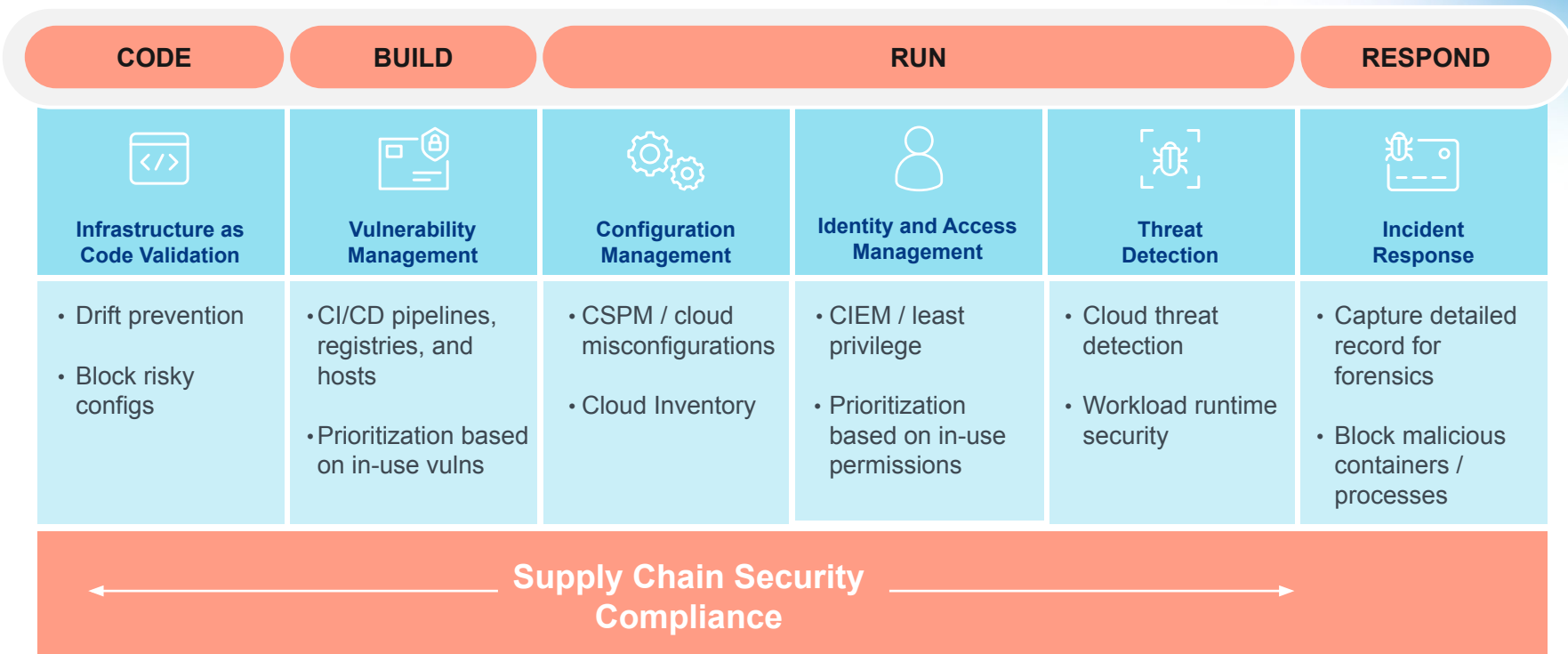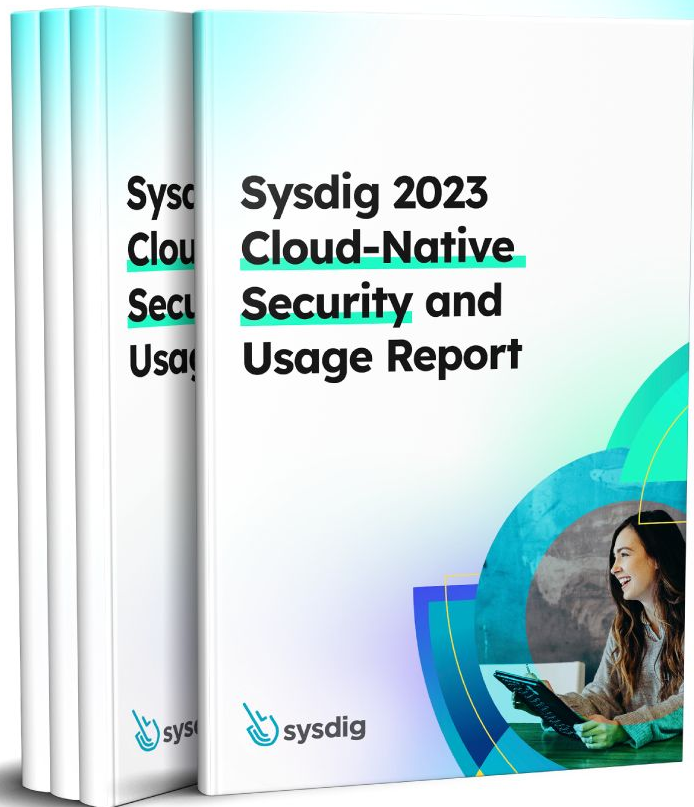
We Lead.

- Leader in cloud detection & response

- **7 Million** containers analyzed daily

- **60 Million** Falco downloads

- **700+ valued** customers

- **$750M** in Funding

FORRESTER
Cloud Workload Security Wave, Q1 2022
A Top Innovation Player

FROST & SULLIVAN
2022 SYSDIG COMPANY OF THE YEAR
Global Container Security Industry

sysdig

Securing VMs, Hosts, Kubernetes and Cloud Services

CODE	BUILD	RUN			RESPOND
Infrastructure as Code Validation	**Vulnerability Management**	**Configuration Management**	**Identity and Access Management**	**Threat Detection**	**Incident Response**
• Drift prevention • Block risky configs	• CI/CD pipelines, registries, and hosts • Prioritization based on in-use vulns	• CSPM / cloud misconfigurations • Cloud Inventory	• CIEM / least privilege • Prioritization based on in-use permissions	• Cloud threat detection • Workload runtime security	• Capture detailed record for forensics • Block malicious containers / processes

Supply Chain Security Compliance

Q & A

sysdig