5
best practices to securing cloud and containers

sysdig SECURE EVERY SECOND.

5 best practices to securing cloud and containers

As container and cloud adoption accelerates, visibility into container and cloud environments continues to be a challenge for enterprises. The convergence of cloud migration and widespread adoption of DevOps practices has pushed containerization as a prevailing trend. Gartner predicts that through 2029, more than 95% of global organizations will be running containerized applications in production, which is a significant increase from less than 50% in 2023.[1] This explosive growth is revolutionizing how applications are built, deployed, and managed, but it also expands the potential attack surface, leaving organizations vulnerable to new sophisticated threats.

Containers are essentially black boxes. It's hard to see what's going on inside, and the lifespan of a container is very short. In fact, 70% of containers now live five minutes or less[2], according to our research. Traditional security tools can't see inside containers, handle the dynamic nature of Kubernetes, or scale across multi-cloud deployments. Proprietary security tools can't keep up with the standardization and speed of innovation possible with open source software.

How can you automate security and compliance controls to implement an efficient and secure DevOps workflow? With the right set of integrated tools, you can efficiently manage cloud and container security risks.

It is important to reduce your risk from cloud misconfigurations, continuously scan for cloud and container vulnerabilities, detect abnormal activity, and prioritize threats to ensure your cloud resources and applications are secure across their entire life cycle. These five key workflows will enable you to cover the most critical security and visibility requirements so you can confidently run containers, Kubernetes, and cloud.

[1] Gartner, Reference Architecture Brief: Cloud-Native Infrastructures Using Containers, Lucas Albuquerque. GARTNER is a registered trademark and service mark of Gartner Inc., and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

[2] Sysdig 2024 Cloud-Native Security and Usage Report
https://sysdig.com/content/c/pf-2024-report-cloud-native-security-and-usage?x=u_WFR

01

Continuous cloud security

Continuous cloud security is required to immediately identify configuration errors and suspicious behavior. The following steps can help you validate your cloud security posture.

- ✓ Improve visibility with an inventory of your cloud resources across multi-cloud environments.
- ✓ Improve your security posture by checking your cloud configuration periodically against CIS benchmarks (e.g., public storage buckets, exposed security groups and access controls, etc.) and take steps to remediate violations.
- ✓ Standardize security controls across environments and apply policies consistently with a shared policy model preferably.
- ✓ Prioritize combinations of findings that create the most significant risks, encompassing vulnerabilities, real-time configuration changes, risky identity behavior, and active threats.
- ✓ Incorporate context from multiple cloud domains to visualize potential attack paths and uncover lateral movement.
- ✓ Eliminate excessive permissions by enforcing least privilege access and adhering to a zero trust for cloud model.
- ✓ Reduce drift by mapping misconfigurations in production to infrastructure as code (IaC) manifests.
- ✓ Detect unexpected changes and suspicious activity across all cloud accounts, users, and services by parsing cloud activity logs.

02

Prioritize vulnerabilities based on runtime intelligence

As application development accelerates with the adoption of CI/CD pipelines and the widespread use of open source software used to build containers, the number of reported vulnerabilities grows sharply. The proliferation of container images and running containers in production introduces new challenges, making it easy for organizations to lose control of security risks. Without effective prioritization, security teams may become overwhelmed, and developers spend valuable time addressing low-priority vulnerabilities. To prevent this, vulnerability management must be seamlessly integrated throughout the entire application lifecycle. Here are steps you can follow to take control of risk from vulnerabilities:

```
FROM Alpine
EXPOSE 22
```

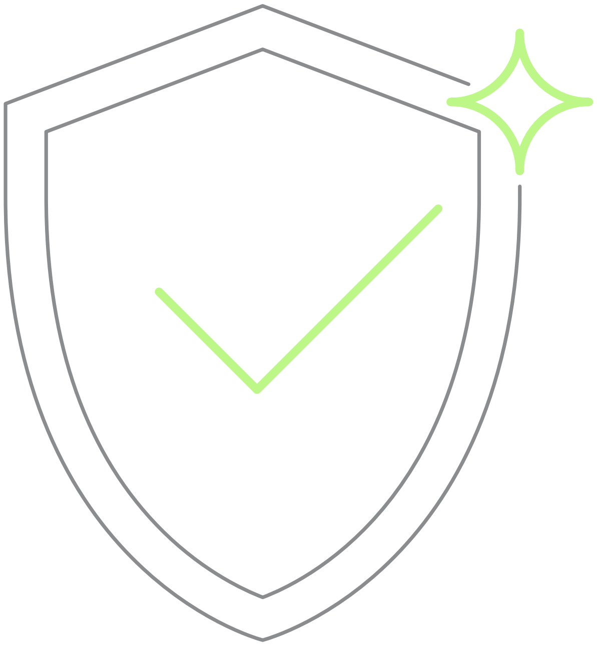
- Automatically prioritize vulnerabilities by leveraging context of which packages are active at runtime.
- Embed scanning into CI/CD pipelines and registries to prevent risky images from being deployed.
- Validate images by checking instructions, user privilege, presence of secrets, and labels.
- Identify new vulnerabilities impacting containers deployed in production.
- Scan for vulnerabilities in containers, as well as hosts (baremetal, VMs, cloud instances).
- Implement layered analysis to identify the specific container image layer where vulnerabilities are introduced, enabling more efficient remediation workflow and clear responsibility assignment.
- Alert the right team for each issue and integrate response within their CI/CD tool.
- By integrating security analysis and compliance validation into this process, you can address issues earlier so you don't slow down deployment. This is known as "shifting security left."

03

Detect and respond to threats

Cybercrime is thriving in the complex and growing attack surface of cloud-native workloads and cloud services. By weaponizing cloud automation, threat actors can fully execute an attack in 10 minutes or less. Threats must be detected early in the attack chain in real time to prevent incidents from becoming breaches. Look for context-rich events, automatic actions, and high-fidelity incident data, making sure that you can investigate even after containers are gone.

- ✓ Implement unified threat detection across containers, cloud services, servers, and user activity.
- ✓ Utilize curated policies, if available, to start with strong protection from day one and stay protected against emerging threats.
- ✓ Leverage multiple detection layers, including detection rules, behavioral analytics, and machine learning, to enhance coverage against zero-day threats.
- ✓ Block attacks and enforce immutability principle by preventing container drift.
- ✓ Analyze identity behavior to identify the earliest signs of account compromise and privilege escalation to get ahead of container and workload threats.
- ✓ Capture syscall data, interactive commands, audit logs, and other activity enriched with Kubernetes and cloud context. Quickly answer the key questions for container security incidents. This detailed record allows you to quickly answer the key questions for container security incidents, conduct analysis and determine root cause, even after containers are gone.
- ✓ Correlate security events with identities and other key findings to speed up investigations and streamline incident response.
- ✓ Implement AI strategically to analyze security events and accelerate human response with contextual awareness.

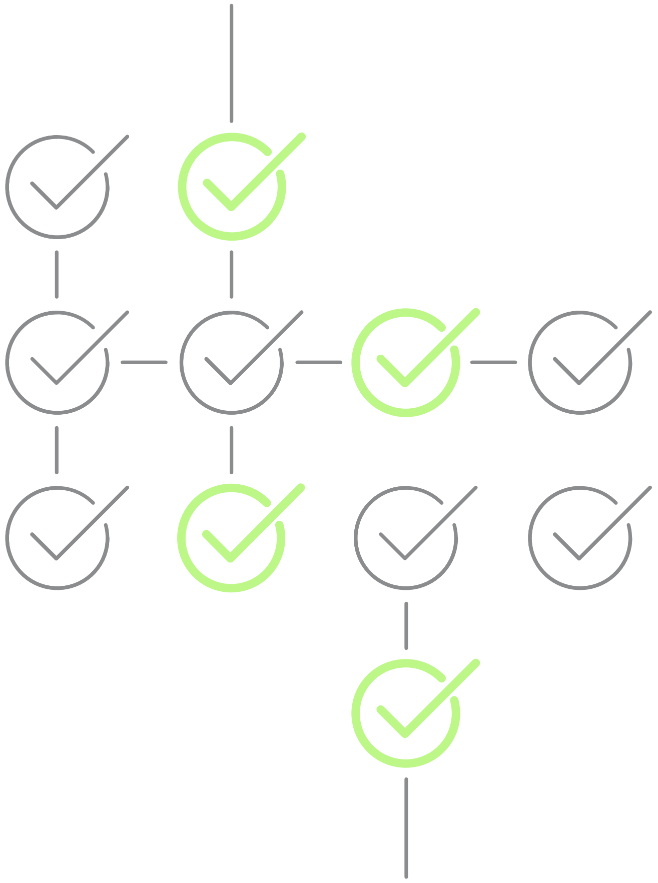


04

Continuously validate compliance

Implement compliance checks to meet regulatory compliance standards (CIS, SOC 2, PCI, NIST 800-53, etc.) across containers, Kubernetes, and cloud environments. Monitor cloud services continually for configuration drift that can impact compliance. Measure compliance progress with scheduled assessments and detailed reports.

- ✓ Check your cloud control plane, containerized applications, and platform configuration against CIS benchmarks and industry best practices.
- ✓ Validate compliance during the build, mapping container image scanning policies to standards (e.g., NIST, PCI, SOC 2, or HIPAA) or internal compliance policies (e.g., blacklisted images, packages, or licenses).
- ✓ Manage compliance at runtime through a rich set of Falco rules for security standards.
- ✓ Implement File integrity Monitoring (FIM) to detect tampering of critical system files, directories, and unauthorized changes.
- ✓ Enable automation, eliminate manual processes, and enforce compliance with automated remediation, mapping misconfigurations in production to infrastructure as code (IaC) manifests.
- ✓ Show proof of cloud and container compliance using cloud audit logs and container forensics data



05

Monitor and troubleshoot containers, K8s, and cloud

Containers are short-lived, dynamic, and churn constantly. Once a container dies, everything inside is gone. You cannot Secure Shell (SSH) or look at logs, and most of the traditional tools used for monolithic applications don't help when something goes wrong.

✓ Monitoring the dynamic nature of container-based applications is critical for the high availability and performance of cloud services. Microservices-based applications can be distributed across multiple instances, and containers can move across multi-cloud infrastructure. Monitoring the Kubernetes orchestration state is crucial to understanding if Kubernetes is keeping all of the service instances running.

- Monitor health and performance with deep visibility into infrastructure, services, and applications. Get the operational status of your cluster with Kubernetes orchestration monitoring.
- Immediately identify owners for issue resolution using container and cloud context.
- Identify pods consuming excessive resources and monitor capacity limits. Control unexpected billing and application rollouts and rollbacks of deployment by monitoring auto-scaling behavior.
- Reduce cost by optimizing capacity across clusters and cloud.

✓ Improve application performance and rapidly solve issues with deep container visibility and granular metrics enriched with Kubernetes and cloud context. You can monitor the impact of a given security incident on service availability.

In the cloud, every second counts. Sysdig stops cloud attacks in real time by instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across workloads, identities, and services to uncover hidden attack paths and prioritize the risks that matter most.

Sysdig. Secure Every Second.

GET PERSONALIZED DEMO →

sysdig

5 BEST PRACTICES TO SECURING CLOUD AND CONTAINERS

CL-001 REV. H 9/24