Container and Cloud Security Comparison Checklist: Sysdig vs Stackrox

66 features compared

Don't rely on a tool that is blind to runtime threats. Tools like Stackrox lack the visibility you need to accurately detect and respond to container attacks. You will also need an additional tool to manage cloud security posture.

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 Stackrox.

Coverage Areas

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

Platform	Sysdig	StackRox
Self hosted (On-premise and air-gapped environments)	**Yes**	Yes
Available as SaaS	**Yes**	No
Built on open-source	**Yes (based on Falco, sysdig oss, Cloud Custodian)**	No
Unified security and monitoring	**Yes**	No
Unified container and cloud security platform (CSPM and CWPP)	**Yes** **Common policy interface for threat detection** **Single security event store with rich context**	No

CSPM	Sysdig	Stackrox
Asset Discovery	**Yes**	No CSPM offering
Cloud services coverage	**Broad and based on open-source**	No CSPM offering
Static configuration management	**Yes**	No CSPM offering
Compliance coverage (CIS benchmarks)	**Yes**	No CSPM offering
Cloud Threat Detection (via AWS CloudTrail, GCP audit logs)	**Yes (native integration with activity logs in your account)**	No CSPM offering
Cloud risk insights (Consolidated, risk-based visibility into CPSM, activity logs, and container threats)	**Yes**	No CSPM offering
Cloud security pricing	**Simple, based on cloud accounts**	No CSPM offering

CWPP	Sysdig	Stackrox
Full non-invasive Instrumentation model	Yes	No. Limited detections.
Deep visibility through granular data based on process, network, file system, and system call activity	Yes	Limited to certain calls
Deep visibility into Kubernetes orchestration activity and Kubernetes event audit	Yes	Partial
Actionable insights using customizable views of detailed data enriched with metadata from Cloud/Kubernetes	Yes	Yes
Serverless containers support	Yes (inline Fargate scanning and Fargate runtime security)	No

Image Scanning	Sysdig	Stackrox
OS package scanning	Yes	Yes
Non-OS package scanning (python PIP, ruby GEM, go modules, java JAR, etc.)	Yes	Yes
Ability to scan images locally in the pipeline or registry (inline scanning)	Yes	Yes
Advanced scanning policy checks (license validation, metadata, file attributes, package type, fix availability, CVE age, exposed credentials, etc.)	Yes	Limited
Registry Scanning	Yes (ECR, automatic scanning)	No
Host Scanning with container/K8s/cloud context	Yes	No
Vulnerability diff capability	Yes	No
Runtime vulnerability analysis	Continuously updated	Periodic rescans required
Runtime vulnerability reporting based on application and Kubernetes metadata	Yes	Yes
Flexible alerting (unscanned image, CVE update, result changes)	Yes	Limited

Runtime Security	Sysdig	Stackrox
Threat detection based on open-source	Yes, based on Falco	No
Rich set of out-of-the-box policies and rules for maximum coverage (network, file, workload, user, etc.)	Yes (100+)	Limited
Supported frameworks like MITRE ATT&CK	Yes	Yes
Precise scoping of policies based on any label (container tags, Kubernetes application context, and cloud metadata)	Yes	Yes
Threat prevention using Pod Security Policies	Yes	No
Machine learning-based image profiling	Yes	No
Policy editor and flexible language to create and customize policies	Yes (Falco language)	Limited
Pre-built security rules for specific apps	Yes (SecurityHub open source)	Partial
Kubernetes Network Security	**Sysdig**	**Stackrox**
Built on open standards	Yes	Yes
Microsegmentation approach	Kubernetes native	Kubernetes native
Automatic Kubernetes enrichment	Yes	Yes
Performance/ Stability impact	No	No
Network topology maps based on any K8s lens (service, namespace, deployment, etc.)	Yes	Yes
Automatic K8s network policy generation	Yes	Yes
Network security Prevention & Detection in SaaS	Yes	Only detection
Visual network policy builder	Yes	No

Incident Response/Forensics	Sysdig	Stackrox
Investigate executed commands	Yes	Limited
Investigate top network talkers	Yes	No
Investigate sensitive files changes	Yes	No
Investigate Kubernetes activity via events audit	Yes	Partial
Correlate system activity with Kubernetes user, service, and application context	Yes	Yes
Search and scope findings by time, host, and Kubernetes context	Yes	Yes
Reconstruct kubectl exec / attach sessions	Yes	No
Capture all system activity for post-mortem analysis	Yes	No
Investigate network activity	Yes	No
Investigate file system activity	Yes	No
Understand performance metrics	Yes	No
Capture syscall-based container events	Yes	Partial

Compliance	Sysdig	Stackrox
Out-of-the-box NIST 800-190 policies	**Yes**	Yes
Out-of-the-box NIST 800-53 policies	**Yes**	Limited, Docker Benchmarks.
Out-of-the-box PCI DSS policies	**Yes**	Limited, Docker Benchmarks
Out-of-the-box SOC2 policies	**Yes**	No
CIS benchmark for Docker, Kubernetes	**Yes**	Yes
CIS benchmark for Linux	**Yes**	No
OpenShift hardening guide benchmark	**Yes, OCP3**	No
Benchmarks for AWS	**Yes**	No
Compliance metrics reporting and dashboards	**Yes**	Yes
Guided remediation	**Yes, CIS AWS**	Yes, Docker Benchmarks
Runtime compliance rules, based on open-source	**Yes, based on Falco**	No

Sysdig Secure provides unified security for containers, Kubernetes and cloud. Secure the build, detect and respond to threats and continuously validate cloud posture and compliance. Sysdig is a SaaS platform, built on an open-source stack that includes Falco, Cloud Custodian and sysdig OSS. Hundreds of organizations rely on Sysdig for security and visibility.

Start a 30 day free trial today at https://sysdig.com/company/free-trial/