Container and Cloud Security Comparison Checklist: Sysdig vs Qualys

55+ features compared

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

Your security stack needs to be:

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

Secure Your Cloud from Source to Run.

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

Coverage Areas

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

Platform type	Sysdig	Qualys
Self hosted (On-premise and air-gapped environments)	Yes	Yes
Available as SaaS	Yes	Yes
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 Context from cloud/ K8s/container is not shared within the platform

CWPP	Sysdig	Qualys
Full non-invasive Instrumentation model	Yes	No - Instrumented using Glibc per container image
Deep visibility through granular data based on process, network, file system, and system call activity	Yes	No
Deep visibility into Kubernetes orchestration activity and Kubernetes event audit	Yes	No
Actionable insights using customizable views of detailed data enriched with metadata from Cloud/Kubernetes	Yes	No
Serverless containers support	Yes (inline Fargate scanning and Fargate runtime security)	Fargate scanning only

Vulnerability Management	Sysdig	Qualys
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	No
Registry Scanning	Yes	Yes
Host Scanning with container/K8s/cloud context	Yes	No
Runtime vulnerability analysis	Continuously updated	Manually triggered
Runtime vulnerability reporting based on application and Kubernetes metadata	Yes	No
Flexible alerting (unscanned image, CVE update, result changes)	Yes	No

Runtime Security	Sysdig	Qualys
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	Limited (network, file, and application)
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	No
Machine learning-based image profiling	Yes	Limited
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)	Very Limited

Incident Response/Forensics	Sysdig	Qualys
Investigate executed commands	Yes	No
Investigate top network talkers	Yes	No
Investigate sensitive files changes	Yes	No
Investigate Kubernetes activity via events audit	Yes	No
Correlate system activity with Kubernetes user, service, and application context	Yes	No
Search and scope findings by time, host, and Kubernetes context	Yes	No
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
Capture syscall-based container events	Yes	No

Kubernetes Security	Sysdig	Qualys
Built on open standards	Yes	No
Microsegmentation approach	Kubernetes native	No
Automatic Kubernetes enrichment	Yes	No
Performance/Stability impact	No	No
Network topology maps based on any K8s lens (service, namespace, deployment, etc.)	Yes	No
Automatic K8s network policy generation	Yes	No
Network security Prevention & Detection in SaaS	Yes	No
Visual network policy builder	Yes	No

CSPM	Sysdig	Qualys
Asset Discovery	**Yes**	Yes
Cloud services coverage	**Broad and based on open-source**	Yes, proprietary
Static configuration management	**Yes**	Yes
Compliance coverage (CIS benchmarks)	**Yes**	Yes
Cloud Threat Detection (via AWS CloudTrail, GCP audit logs, Azure activity Audit)	**Yes**	No, based on CSP detection capabilities
Cloud risk insights (Consolidated, risk-based visibility into CPSM, activity logs, and container threats)	**Yes**	No, based on CSP detection capabilities
Cloud security pricing	**Simple, based on cloud accounts**	Pricing depends on your selection of Cloud Platform Apps, the number of network addresses (IPs), web applications, and user licenses.

Compliance	Sysdig	Qualys
Out-of-the-box NIST 800-190 policies	Yes	No
Out-of-the-box NIST 800-53 policies	Yes	Yes
Out-of-the-box PCI DSS policies	Yes	Yes
Out-of-the-box SOC2 policies	Yes	No
Out-of-the-box HIPAA policies	Yes	Yes
Out-of-the-box GDPR policies	Yes	Yes
Out-of-the-box FedRAMP policies	Yes	Yes
Out-of-the-box ISO 27001 policies	Yes	Yes
CIS benchmark for Docker, Kubernetes	Yes	No
CIS benchmark for Linux	Yes	No
OpenShift hardening guide benchmark	Yes, OCP3	No
CIS Benchamarks for AWS, GCP & Azure	Yes	Yes
Compliance metrics reporting and dashboards	Yes	Yes
Guided remediation	Yes	Limited (only cloud)
Runtime compliance rules, based on open-source	Yes, based on Falco	No, black box

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/