sysdig

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

Platform	Sysdig	Rapid7
Self hosted (On-premise and air-gapped environments)	Yes	Yes
Available as SaaS	Yes	Yes
Core built on open-source	Yes (Falco, sysdig oss, Cloud Custodian)	No
Unified security and monitoring	Yes	No
Unified container and cloud security platform (CSPM and CWPP)	Yes	No. Multiple tools: InsightCloudSec for CSPM, InsightVM for vulnerability management, or Nexpose for on-prem vulnerability mgmt.
Pricing	Simple, based on the number of cloud accounts and hosts.	Complicated with multiple products

CSPM	Sysdig	Rapid7
Cloud services coverage	Broad	Broad
Static configuration management	Yes	Yes
Compliance coverage	Yes	Yes
Cloud Threat Detection	Yes	Yes
Out-of-the-box, easy to use cloud risk insights (Consolidated, risk-based visibility into CPSM, activity logs, and container threats)	Yes	Yes

CWPP	Sysdig	Rapid7
Full non-invasive Instrumentation model	Yes	No
System call rules are aware of container and kubernetes context, like the ability to detect “terminal shell in a container”	Yes	No
System call captures with the deepest level of forensic information, and Activity Audit log of command line instructions are executed	Yes	No
Serverless containers support	Yes (inline Fargate scanning and Fargate runtime security)	No

Image Scanning	Sysdig	Rapid7
IaC Scanning	Yes	Yes
OS package scanning	Yes	Yes
Ability to scan images locally in the pipeline or registry (inline scanning)	Yes	Limited
Advanced scanning policy checks (license validation, metadata, file attributes, package type, fix availability, CVE age, exposed credentials, etc.)	Yes	No
Host Scanning	Yes	Yes
Runtime vulnerability analysis	Continuously updated	No
Flexible alerting (unscanned image, CVE update, result changes)	Yes	No

Runtime Security	Sysdig	Rapid7
Threat detection based on open-source	Yes	No
Rich set of out-of-the-box policies and rules for maximum coverage (network, file, workload, user, etc.)	Yes (100+)	No
MITRE ATT&CK mapping	Yes	No
Precise scoping of policies based on any label (container tags, Kubernetes application context, and cloud metadata)	Yes	No
Policy editor and flexible language to create and customize policies	Yes	No
Pre-built security rules for specific apps	Yes (SecurityHub open source)	No

Kubernetes Network Security	Sysdig	Rapid7
Network topology maps based on any K8s lens (service, namespace, deployment, etc.)	Yes	No
Automatic K8s network policy generation	Yes	No
Visual network policy builder	Yes	No

Incident Response/Forensics	Sysdig	Rapid7
Investigate executed commands	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
Understand performance metrics	Yes	No
Capture syscall-based container events	Yes	No

Compliance	Sysdig	Rapid7
Out-of-the-box NIST 800-190 policies	Yes	Yes
Out-of-the-box NIST 800-53 policies Rev.4	AWS, workload	Yes (combining different products)
Out-of-the-box NIST 800-53 policies Rev.5	AWS, workload	No
Out-of-the-box PCI DSS policies	workload	Yes (combining different products)
Out-of-the-box SOC2 policies	AWS, workload	Yes (combining different products)
Out-of-the-box GDPR policies	AWS, workload	Yes (combining different products)
Out-of-the-box HIPAA policies	AWS, workload	Yes (combining different products)
Out-of-the-box ISO 27001:2013 policies	AWS, workload	Yes (combining different products)
CIS Benchmark for Kubernetes	Yes	Yes
CIS Benchmark for Docker	Yes	No
CIS Benchmark for Linux	Yes	Yes
CIS Benchmarks for AWS	Yes	Yes
CIS Benchmark for Amazon EKS	Yes	No
CIS Benchmark for Google GKS	Yes	No
OpenShift3 hardening guide Benchmark	Yes	No
Guided remediation	Yes	Yes
Runtime compliance rules	Yes	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/