



Microservices and Container Monitoring

60+ Feature Comparison
Vendor Scorecard

Like every major platform shift, the move to containers and microservices triggers the need to rethink the tooling required to secure your infrastructure effectively. In this scorecard we'll cover the key areas you need to think about to support your microservice infrastructure and secure your dynamic technical and business requirements.



WE'LL COVER

Installation & Data Collection. What is the instrumentation model and flexibility for installation across a wide range of environments? What are the available metrics?

Integrations. What out-of-the-box and custom integrations exist for the platforms, applications, and ecosystem components in your environment?

Dashboarding. What pre-built dashboards are available and what facility exists for you to build your own views?

Exploration. How are you able to explore and visualize your environment and the available metrics?

Alerting & Troubleshooting. How simple and adaptive is alert configuration and what are the possible triggers? What is available for pinpointing root cause of issues?

Administration. What level of work is required to onboard users? Does the solution integrate with existing tooling?

Events. Does the solution recognize and record events across the infrastructure and applications?

Company Execution. Does the vendor have experience in legacy environments or are they cloud native?

SCORING SCALE


Please input the response in the boxes below that you feel best describe the capabilities of each vendor you're considering using the following scale.

- 0** – Missing or not supported
- 1** – Deficient, needs significant improvement
- 2** – Functional but inferior to peers
- 3** – Good, capable and effective
- 4** – Robust, superior to peers
- 5** – Best-of-breed, the role model



FEATURES	SYSDIG MONITOR	VENDOR B	VENDOR C	EVALUATOR NOTES
INSTALLATION & DATA COLLECTION				
Offers cloud solution				
Offers on-prem software solution				
AWS CloudWatch				
Google Cloud API integration				
Kubernetes integration				
Docker Swarm / EE integration				
Mesos / DCOS integration				
kube-state-metrics collection				
StatsD collection				
JMX collection				
Prometheus collection				
Complexity of agent installation				
Single instrumentation point for all containers & apps on host				
Linux agent				
Windows agent				
Agent deploys on AWS				
Agent deploys on Azure				
Agent deploys on Google Cloud				
Agent deploys on GKE (Google Container Engine)				
Agent deploys on AWS ECS (Elastic container Service)				
Same agent provides monitoring in addition to security policy enforcement				
Red Hat Enterprise Linux (RHEL) support				
Sub Total				






FEATURES	SYSDIG MONITOR	VENDOR B	Vendor C	EVALUATOR NOTES
INTEGRATIONS				
Robust set of base policies				
Ability to create custom app integrations				
Auto-discovery of applications with base integrations				
Auto-discovery of applications with custom integrations				
Auto-discovery of StatsD metrics (no endpoint required)				
Auto-discovery of JMX metrics (no endpoint required)				
Auto-discovery of Prometheus metrics (no endpoint required)				
Sub Total				

DASHBOARDING				
Provides pre-built dashboards for popular applications				
Configurable dashboards				
Many visualization choices (time, bar, number, histogram, etc)				
Easy-to-use time controls				
Ability to share dashboards across users and teams				
Ability to share and distribute read-only dashboards via public URL				
Ability to compare time frames				
Dynamically create physical (host-based) topology maps with zoom in				
Dynamically create logical (app/service-based) topology maps with zoom in				
Sub Total				






FEATURES	SYSDIG SECURE	VENDOR B	Vendor C	EVALUATOR NOTES
EXPLORATION				
Provides method to explore entire environment without creating a dashboard				
Enables "grouping" by tags or orchestration data				
Aggregates data across containers in a service				
Automatically scopes dashboards based on selected environment view				
Displays system level data (host & container)				
Displays app level data (specific to applications)				
Enables metric search				
Displays network data (response times & traffic)				
Sub Total				

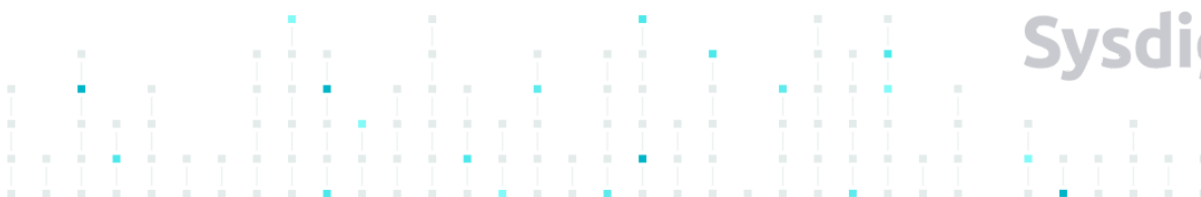
ALERTING & TROUBLESHOOTING				
Alert scope configurable by physical and logical groups				
Multi-condition logic for alerts				
Alert previews				
Anomaly detection				
Integrations for alert outputs				
Robust integrations for alert outputs (PagerDuty, Slack, VictorOps, etc)				
Webhook output				
Ability to capture system traces upon alert trigger				
Integrated trace file explore tooling for correlating metrics and finding root cause				
Sub Total				






FEATURES	SYSDIG SECURE	VENDOR B	Vendor C	EVALUATOR NOTES
ADMINISTRATION				
Ability to isolate users to specific data based on physical resources (Teams)				
Ability to isolate users to data based on logical resources via orchestrator (Teams)				
LDAP Integration				
Single sign on (SSO)				
API access				
Administrator dashboard for status of all agents, metrics, etc.				
Tools to automatically onboard new users (wizard, walkthroughs, or spotlight)				
Sub Total				

EVENTS				
Supports event correlation in addition to metrics				
Auto-creates events for alert triggers				
Allows for custom events				
Slack integration to input events				
Automatically discover Docker events				
Automatically discover Kubernetes events				
Sub Total				





FEATURES	SYSDIG SECURE	VENDOR B	Vendor C	EVALUATOR NOTES
COMPANY / EXECUTION				
Responsive Support				
Customer Success / Technical Account Management				
Live Chat within Application				
Roadmap				
Stable company				
Experienced team / track record				
Pricing Structure				
Sub Total				

SUMMARY SCORECARD

FEATURES	SYSDIG MONITOR	VENDOR B	VENDOR C
INSTALLATION & DATA COLLECTION			
INTEGRATIONS			
DASHBOARDING			
EXPLORATION			
ALERTING & TROUBLESHOOTING			
ADMINISTRATION			
EVENTS			
COMPANY / EXECUTION			
Total Scores			

