Securing Containers and Kubernetes

Workload Protection Needs Cloud Context

Cloud-native services like containers, Kubernetes, and serverless have changed the way applications are built and secured. Traditional security tools fail to provide visibility of containerized workloads and create an endless list of alerts. Sysdig is purpose built for the cloud and helps enterprises secure their workloads at cloud speed by leveraging runtime insights.

Sysdig takes container security and workload protection to the next level by enriching findings with broader cloud context. It is no longer enough to view container vulnerabilities and threats in isolation. Sysdig combines them with findings across your entire cloud infrastructure to prioritize the most important risks and reveal active lateral movement.

"Sysdig has helped automate what would otherwise be a mountain of manual work. We can now not only see our entire Kubernetes environment, but also take more immediate action to address problems or threats."

Senior Manager of Information Security

Falco

The open source solution for threat detection across containers and cloud. Detect workload threats with policies and rules curated and managed by Sysdig's Threat Research Team, supplemented with ML and drift detection.

Investigation and Response

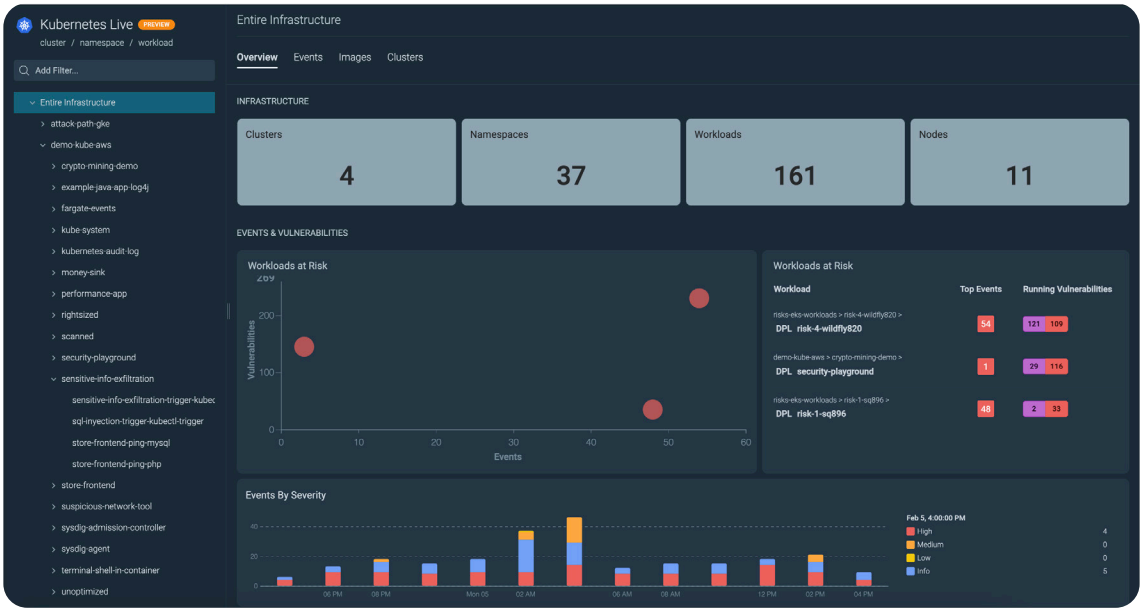
Capture rich context and metadata to accelerate investigation, and respond in minutes with granular incident response workflows.

Agent + Agentless

Simplify setup and maintenance with agentless scanning, while leveraging our agent for runtime visibility and prioritization of in-use vulnerabilities.

Risk Prioritization and Visualization

Go beyond identifying individual workload risks. Reveal combinations of findings to prioritize top risks and visualize exploitable links between your workloads and broader cloud infrastructure.



Container Security is Evolving

Sysdig provides unique visibility of containers and Kubernetes, giving users the context they need to identify the most impactful vulnerabilities and detect workload threats instantly. Going beyond this, Sysdig approaches workload protection from a risk-centric perspective. By correlating container risks with findings from other cloud domains, Sysdig prioritizes the most significant risks to stop attackers in their tracks.

Use Cases

Real-Time Detection and Response

- Full visibility across containers, servers, Kubernetes, and serverless to detect threats within two seconds.
- Capture all interactive commands and system calls to investigate and respond in minutes.

Vulnerability Management

- Identify in-use packages to prioritize the most critical vulnerabilities to fix first.
- Simplify setup and scanning using an agentless approach to find vulnerabilities across your cloud environment.

KSPM

- Tie Kubernetes security violations with the Infrastructure-as-Code (IaC) manifest that defines your Kubernetes resources
- Auto-generate pull requests for remediation directly at the source

Agentless Cloud Context

- Multidomain correlation between containers and cloud to automatically identify the riskiest combinations without any manual stitching
- Alert on log activity via Falco in real time to highlight active cloud risk

sysdig SECURE EVERY SECOND.

www.sysdig.com

REQUEST DEMO →