Securely Run Cloud Native in Production

Sysdig makes securing cloud-native workloads a reality

As cloud native becomes the standard for application deployment, IT roles must adapt. Cloud teams are taking ownership for security, as well as application performance and availability. Tools must support a secure DevOps workflow to run Kubernetes and containers in production.

Sysdig Secure DevOps Platform

Confidently run cloud-native workloads in production using the Sysdig Secure DevOps Platform. Embed security and compliance into your build, run, and respond workflows. Deliver the performance and availability your users expect with context-based monitoring and troubleshooting. Open by design, with the scale, performance, and usability enterprises demand.

Sysdig makes securing cloud-native workloads a reality

As cloud native becomes the standard for application deployment, IT roles must adapt. Cloud teams are taking ownership for security, as well as application performance and availability. Tools must support a secure DevOps workflow to run Kubernetes and containers in production.

Sysdig Secure DevOps Platform

Confidently run cloud-native workloads in production using the Sysdig Secure DevOps Platform. Embed security and compliance into your build, run, and respond workflows. Deliver the performance and availability your users expect with context-based monitoring and troubleshooting. Open by design, with the scale, performance, and usability enterprises demand.

Run Kubernetes in production with Sysdig

- EMBED SECURITY
  - Detect vulnerabilities and misconfigurations with a single workflow
  - Block threats without impacting performance
  - Conduct forensics even after the container is gone

- MAXIMIZE AVAILABILITY
  - Prevent issues by monitoring performance and capacity
  - Accelerate troubleshooting with a single source of truth
  - Scale Prometheus monitoring across clusters and clouds

- VALIDATE COMPLIANCE
  - Verify configuration meets CIS best practices
  - Ensure application compliance with NIST, PCI
  - Accelerate audit by correlating Kubernetes activity

Troubleshooting, forensics and audit can be handled at scale when you have a single source of truth across the teams. This shared understanding allows the team to address issues more quickly and maximize application availability.”

Goldman Sachs

Chetan Mehendiratta
Vice President of Engineering, Goldman Sachs

Sysdig At-a-Glance

LAUNCHED: 2013
HEADQUARTERS: San Francisco, CA
CEO: Suresh Vasudevan

CTO AND FOUNDER: Loris Degioanni, Wireshark co-creator
FUNDING: $121.5 M Total Funding, Round D, Insight Venture Partners, Bain Capital, Accel

“Troubleshooting, forensics and audit can be handled at scale when you have a single source of truth across the teams. This shared understanding allows the team to address issues more quickly and maximize application availability.”

Goldman Sachs
Chetan Mehendiratta
Vice President of Engineering, Goldman Sachs
We also see a lot of value in what Sysdig is doing with container security. The ability to expand beyond performance monitoring into security with the same agent and SaaS backend for us means not having to manage another set of agents, another set of deployments and another set of upgrades over time. No other solution can give us this.

Varun Tagore Korrapati
DevOps Architect at Steelcase