Secure Your Cloud from Source to Run

Security for containers, Kubernetes and cloud

Cloud apps need a new security stack

Modern cloud apps are built using CI/CD and run as containerized microservices. Traditional tools cannot keep up with cloud-native due to rapid application deployment cycles and dynamic container environments. Unless security is automated and embedded into the development lifecycle it slows down innovation. Securing the cloud requires a security stack built on open standards that automates security within the development lifecycle, from source to run.

Secure cloud, Kubernetes and containers

With the Sysdig platform, you can find and prioritize software vulnerabilities, detect and respond to threats and anomalies, and manage cloud configurations, permissions and compliance. You get a single view of risk from source to run with no blind spots, no guesswork, no black boxes. The company pioneered cloud-native runtime threat detection and response by creating Falco and open source Sysdig as open source standards and key building blocks of the Sysdig platform.

MANAGE VULNERABILITIES

- Automate scanning within CI/CD pipelines and registries without images leaving your environment
- See all vulnerabilities across containers and hosts
- Better prioritize vulnerabilities based on runtime context

DETECT AND RESPOND TO RUNTIME THREATS

- Detect threats across containers, hosts and Kubernetes with Falco
- Catch runtime drift and remediate at the source
- Prevent lateral movement using Kubernetes network policies
- Conduct incident response using detailed records

CONTINUOUSLY VALIDATE COMPLIANCE

- Save time with out-of-the-box policies and reports for PCI, NIST, SOC2, etc.
- Automate compliance and governance via policy as code based on OPA
- Implement File Integrity Monitoring across containers and hosts

MANAGE CLOUD CONFIGURATIONS AND PERMISSIONS

- Identify misconfigurations and compliance violations
- Enforce least privilege access for cloud identities
- Detect cloud threats in real time by analyzing cloud logs without expensive exporting to SIEM

MONITOR KUBERNETES AND CLOUD

- Prevent and resolve issues by monitoring performance and capacity
- Accelerate troubleshooting using granular data
- Simplify Prometheus monitoring by using our Managed Prometheus Service

Sysdig At-a-Glance

LAUNCHED: 2013

HEADQUARTERS: San Francisco, CA

VALUATION: $2.5 B

CEO: Suresh Vasudevan

CTO AND FOUNDER: Loris Degioanni, Wireshark Co-Creator

FUNDING: $744 M total funding by Accel, Bain Capital, DFJ Growth, Glynn Capital, Goldman Sachs, Guggenheim Investments, In-Q-Tel, Insight Venture Partners, Next47, Permira, Premji Invest, and Third Point Ventures

> "We've instrumented Sysdig into our pipelines where it is executing container vulnerability and compliance checks on containers as they're promoted into our production environment. Those automated checks allow us to move faster."

SAP Concur | Director Engineering, SAP Concur

Company Key Milestones

Open Source Key Milestones

2013
- Sysdig founded by Loris Degioanni, co-creator of Wireshark.

2014
- Launches Sysdig open source Linux visibility tool.

2015
- Sysdig Monitor, the first container-native monitoring service launches.
- Sysdig introduces Kubernetes support in Sysdig Inspect open source. Declared a linux.com "project to watch."

2016
- Sysdig team launches Falco, the open source Kubernetes runtime security project.

2017
- Introduces Sysdig Secure.
- Sysdig launches support for Prometheus metrics.

2018
- Sysdig Monitor 3.0 delivers enterprise-grade Prometheus Monitoring.
- Introduces "IBM Cloud Monitoring with Sysdig" service for IBM Cloud customers.
- Contributes Falco to Cloud Native Computing Foundation® (CNCF®), sandbox project.

2019
- Availability on Google Cloud Anthos.
- More than 10M open source downloads. Introduces eBPF instrumentation.

2020
- IBM Cloud Monitoring with Sysdig expands to include Sysdig Secure.
- Sysdig named to the Deloitte 2020 Technology Fast 500™ List.
- Falco accepted as a CNCF® incubation-level hosted project.

2021
- Introduces cloud security posture management.
- Apolicy acquisition, infrastructure as code security.
- Introduces cloud infrastructure entitlements management.
- Contributes Falco system call capture stack to CNCF.
- Cloud security monitoring functionality added for Falco.

2022
- Sysdig becomes primary sponsor of Wireshark.

Sysdig: Secure Your Cloud from Source to Run

> "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 | Vice President of Engineering, Goldman Sachs

Falco Highlights

43M+	40+	400%
Docker Hub pulls	Integrations	Increase YoY
4,600+	4,300+	318%
GitHub stars	Total stars	Increase in contributors

Sysdig is Built on an Open Source Foundation

Falco · Prometheus · sysdig · Open Policy Agent

Sysdig Works with Leading Cloud and Container Platforms

kubernetes · RANCHER · Red Hat OpenShift · Google Cloud · aws · IBM Cloud · Microsoft Azure · ORACLE