Overview
What are your containers doing? Sysdig Secure is the most powerful container-native security and forensics solution with intelligent Red Hat container technology integration.

Executive Summary
Enterprises are moving to container and microservices architectures to achieve faster, more effective development, software portability, and dynamic scaling. Container-based environments drastically change what is required to understand how your application is performing. Sysdig partners with Red Hat to deliver deep visibility into Red Hat Enterprise Linux and Red Hat OpenShift Container Platform deployments. Sysdig Secure gives you everything you need to detect vulnerabilities and protect your applications and microservices.

Statement from Partner
“As enterprises move to deliver applications and services in containers, they want seamless integration across solutions. Sysdig is committed to working closely with Red Hat to ensure this simplicity for our customers,” said Loris Degioanni, CEO and Founder of Sysdig. “Red Hat container solutions – including OpenShift – are being rapidly adopted for production-class deployments. Sysdig’s security, monitoring, and forensics tools help Red Hat customers stay on top of what’s happening in their environment.”

Statement from Red Hat Connect
“Customers are looking to migrate their applications to the cloud leveraging containers as the deployment model,” said Mike Werner, senior director, Global Technology Partners, Red Hat. “Red Hat container certification assures a supportable and performant platform for all types of customer deployment models. Red Hat is thrilled to work with software partners like Sysdig, resulting in the world’s largest commercial ecosystem for containers.”

FAST FACTS

Company: Sysdig
Website: www.sysdig.com

Company Description
Sysdig is the container intelligence company. We have created the only unified platform to deliver monitoring, security, and troubleshooting in a microservices-friendly architecture. Our open source technologies have attracted a community of over a million developers, administrators and other IT professionals looking for deep visibility into systems and containers. Our container intelligence platform monitors and secures millions of containers across hundreds of enterprises, including Fortune 500 companies and web-scale properties.

Product Profile
Sysdig Secure is the most powerful run-time security and forensics solution for your containers and microservices. Sysdig Secure, part of the Sysdig Container Intelligence Platform, comes out-of-the-box with unmatched container visibility and deep orchestrator integrations, including Kubernetes, Docker, AWS ECS, and Mesos. It is available as both a Cloud and an On-Premise Software offering.

Contact: info@sysdig.com
Product Benefits

Sysdig Secure delivers a highly scalable, distributed intelligence system to monitor and secure your containers via two core technologies:

**ContainerVision™** provides deep, sys call level visibility inside containers without invasive instrumentation. This approach succeeds for container security where legacy security fails, and at the same time makes securing applications and microservices simpler and more robust.

**ServiceVision™** provides an automatic interface with OpenShift container orchestration to collect metadata and tags about deployments, services, containers, and hosts. All metadata is applied directly to our data stream, and provides data enrichment to slice and dice policies as needed.

**Comprehensive Security Capabilities** - Sysdig Secure’s run-time security approach includes the capabilities of endpoint security, network security, host intrusion detection/prevention and forensics within one point of instrumentation and one interface.

**Enterprise Production Ready** - Sysdig already serves hundreds of enterprises around the globe. Sysdig Secure is built on Sysdig Falco, the open source container security project, has been hardened in use across some of the largest web scale properties.

Use Cases

- **Adaptive Run-time defense** - Don’t just detect an attack - block it. Automatically kill containers you suspect to be compromised based on application, container, or network activity. All without per-pod instrumentation or code changes.

- **Full-stack forensics** - Drill down from policy violation, to system call, all the way down to the actual data written to file. See pre- and post-attack activity. Our forensics allow you inspect data outside of production, even if the containers are long gone.

- **Complete Audit & Governance** - Capture a complete audit trail down to user actions, container activity, and command-line arguments. Review any policy violation with rich, service-oriented context. Send audit trails downstream into a SIEM or any compliance software.

See Sysdig Secure in action
Follow us on our blog
Check out our monthly container newsletter