



Cloud Threat Detection Built on Open Source

Runtime Security for Modern Cloud Environments



Falco is the open source solution for real-time detection of threats and anomalies across containers, Kubernetes, and cloud services. Falco acts as your security camera, continuously detecting unexpected behavior, configuration changes, intrusions, and data theft in real time. It was created by Sysdig and contributed to the Cloud Native Computing Foundation (CNCF). Falco is a battle tested technology with a strong, rapidly-growing community of users and adopters in established organizations and has been downloaded over 100 million times.

With a robust open source foundation, users benefit from transparency and agility in new detection thanks to the Falco's rule language.

Sysdig's cloud-native application protection platform (CNAPP) is built on Falco. While open-source Falco can be used to detect cloud-native threats, Sysdig Secure offers additional features and functionality that help customers secure their cloud infrastructure. Sysdig enhances everything that is wonderful about Falco, making operationalizing simple and helping users get more out of Falco at scale.



Having a technology as complex as Falco packaged together with professional support and a SaaS infrastructure allows us to focus on the integration instead of spending time on setup and maintenance."

Security Engineer



BENEFITS



Enterprise-grade support

Technical support from Sysdig experts to get the most out of Falco



Ease of operation

Rule management, event management, integrations, and automated rule tuning



Advanced threat detection

Custom rules/policies curated by Sysdig's Threat Research Team and threat feed-based detections



Investigation and response

Accelerate investigation by capturing all interactive commands and system calls and troubleshoot directly within your environment through a remote shell






















Enhanced performance

Optimized metadata collection for large environments and lower agent footprint

Get More Out of Falco

Our products have Falco at their core, delivering detection and runtime insights that power a suite of security solutions. Sysdig helps users leverage Falco to its full potential with simplified operations and scalability to larger environments. With additional functionality like CSPM and vulnerability management, Sysdig Secure provides end-to-end coverage for cloud-native environments, from prevention to defense.

	sysdig	
Open Source Based Agent		
Threat Detection		
Event Sources (Syscalls, K8s Audit Logs, Cloud Logs)		
Alert Outputs	 Event Forwarding	 Via Sidekick
Customizable Policies		
Automated Rule Tuning		
Automated Policy Suggestions		
K8s Network Security		
Additional Capabilities		
Vulnerability Management		
IAC Security		
CSPM (Attack Path Analysis, Inventory, Risk Prioritization)		
Compliance (Out-of-the-box)		
Auditing / Forensics		
Enterprise-Grade Support and Scalability		
Snyk Integration		



Secure Every Second.

See Sysdig in action

REQUEST DEMO 