Falco

Detect threats in real time with Falco on AWS

The ultimate line of defense is runtime security

Falco is the open source runtime security solution for threat detection across containers, hosts, Kubernetes and the cloud.

Container Security

Secure containerized applications, no matter what scale, using the power of eBPF.

Host Security

Protect your applications in real time wherever they run, whether bare metal or VMs.

Kubernetes Security

Falco is Kubernetes-compatible, helping you instantly detect suspicious activity across the control plane.

Cloud Security

Detect intrusions in real time across your cloud, from AWS, GCP or Azure, to Okta, Github and beyond.

Use Falco to protect your apps at runtime

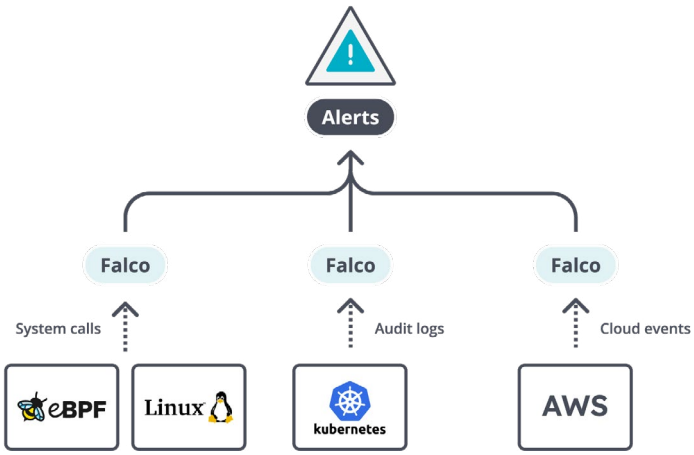
Falco gives you real-time visibility into unexpected behaviors, config changes, intrusions, and data theft. Falco makes it easy to consume Linux kernel syscalls, and enrich those events with information from Kubernetes and the rest of the cloud native stack. Falco has a rich set of out of the box security rules specifically built for Kubernetes, Linux and the cloud.

- Threat detection for your workloads and cloud infrastructure
- Highly scalable, with containerized architecture and Kubernetes integration
- Performant and low-latency due to a low overhead, streaming event architecture
- Richly connected to a growing ecosystem of plugins and integrations
- Works out-of-the-box, but is highly customizable thanks to a single policy language

Efficient cloud-native security capabilities

Falco provides runtime security monitoring for containers and the cloud: your final line of defense against attacks and malware. It increases your security and compliance posture with these capabilities:

- Captures events from kernel syscalls using eBPF, or from cloud sources
- Detects threats such as privilege escalation, malware activation or unauthorized access
- Triggers alerts based on a customizable rule set
- Forwards alerts to destinations such as a SIEM system or response engine



Responding to threats with Falcosidekick

Use Falco with its companion application, Falcosidekick, as a full response engine to protect your environments. Falcosidekick connects Falco to your ecosystem by distributing events to more than 50 systems, such as email, chat, message queues, serverless functions, databases and more. It's easy to configure and use, and has a great web UI to view events and summaries in dashboard format.

Falco and Falcosidekick are highly integrated with the AWS ecosystem

Falco can collect runtime security findings from multiple AWS accounts running one or more workloads on AWS container orchestration platforms, such as Amazon Elastic Kubernetes Service (Amazon EKS) or Amazon Elastic Container Service (Amazon ECS).

Falco and Falcosidekick are deeply integrated with AWS right from the start. You can find both as container images through the Amazon ECR Registry. Plus, there are pre-built driver modules for AWS kernels, whether you are using the kernel module driver or the eBPF probe.

Plugins

With the Amazon CloudTrail and Amazon CloudWatch plugins, Falco can collect events from these AWS sources and detect threats.

- **Amazon CloudTrail plugin:** read CloudTrail logs and emit events for each entry. Includes out-of-the-box rules to identify potential threats, such as console logins that don't use multi-factor authentication, disabling multi-factor authentication for users and disabling encryption for S3 buckets.
- **Amazon CloudWatch plugin:** extends Falco's ability to forward Kubernetes audit logs to Amazon EKS, so you can emit events into a CloudWatch log stream and monitor your EKS clusters.

Falco is a CNCF incubated project.
Contributions and feedback are welcome!

CLOUD NATIVE
COMPUTING FOUNDATION

Integrations

Falcosidekick lets you forward events from Falco into a variety of different AWS services.

- **Amazon CloudWatch:**
  Emit events into a CloudWatch log stream
- **Amazon Kinesis:**
  Send Falco events as streaming data
- **Amazon S3:**
  Add events in JSON format to an S3 bucket
- **Amazon Security Lake:**
  Add Falco events to a security data lake
- **Amazon Simple Email Service (SES):**
  Send email messages
- **Amazon Simple Notification Service (SNS):**
  Create a push notification to apps or people
- **Amazon Simple Queue Service (SQS):**
  Send a message into an SQS queue
- **AWS FireLens:**
  Routes Falco events from several clusters into Amazon CloudWatch
- **AWS Lambda:**
  Invoke a Lambda function in response to a Falco event
- **AWS Security Hub:**
  Falco events can be populated in this service

Learn more and join the Falco community

www.falco.org

Rev. A 06/23