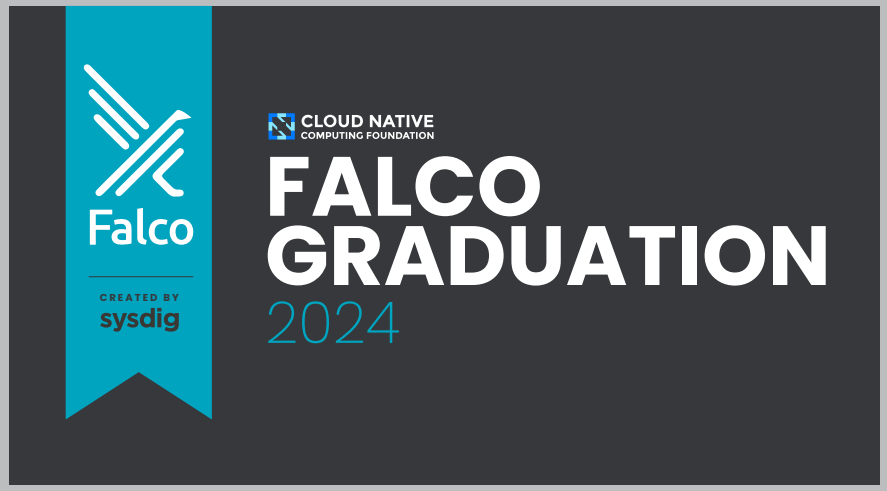
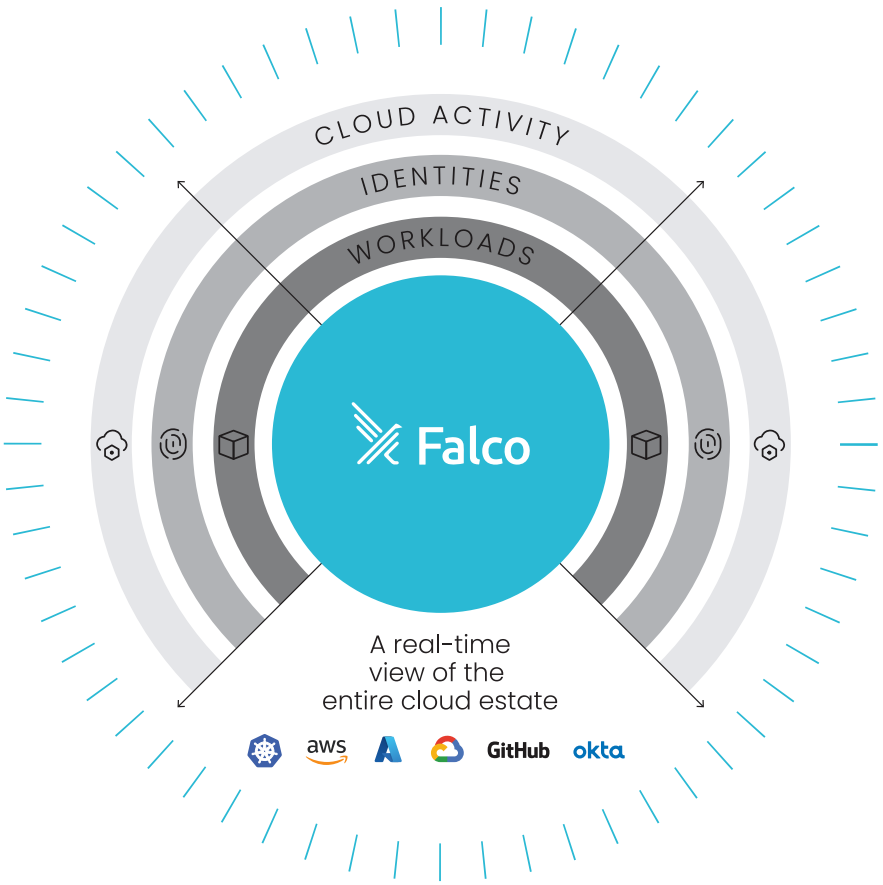
EBOOK

Securing the Cloud: The Benefits of Falco with an Enterprise Experience

sysdig SECURE EVERY SECOND.



Since its initial release in 2016, Falco has become the threat detection engine of choice for containers, cloud, and Kubernetes. Downloaded over 130 million times, Falco is used by big tech, cloud providers, and startups across every major cloud platform.



Sysdig, as the creator and a maintainer of Falco, is committed to making its open source threat detection engine a powerful and accessible tool for everyone. Falco was the first runtime security project accepted into the CNCF Sandbox in 2018. To officially graduate — that is, to achieve the highest position in the CNCF — the Falco project underwent a strict, nearly six-year due diligence process, which was monitored by the CNCF Technical Oversight Committee (TOC) team. The project completed a third-party security audit in order to validate Falco's growth and maturity, which cemented the project's status as the de facto standard for cloud-native threat detection.

Sysdig has built its own cloud detection and response engine on top of Falco. By combining Falco's leading threat detection engine with Sysdig's comprehensive cloud-native application protection platform (CNAPP), our customers are empowered to not only detect but also investigate and respond to threats at cloud speed.

Read on to discover how businesses are using Sysdig's managed threat intelligence in Falco to better secure their cloud and containers in real time.

Case Study

ICG Consulting securely accelerates development in the cloud

> Between AWS and Falco, we had a strong multi-level security strategy to help ensure we had security shored up across a compliant network. As we scaled, Sysdig was the natural next step for us — between the strength of the Sysdig technology based on Falco and its partnership with AWS, we knew we could deliver even more quickly by adopting Sysdig."
>
> *— Technical Consultant at ICG Consulting*

The Challenge

ICG Consulting is a long-standing, trusted expert in back-office applications. To ensure the cloud-based services ICG offers its clients are secure, the company relied on Falco. But as ICG's cloud services grew, it needed a way to simplify cloud security without slowing development.

The Results

By expanding its cloud security to include Sysdig's platform alongside Falco, ICG was able to increase visibility across cloud, container, and hosts, quickly identifying issues at a node, pod, and user level. Within just a few weeks, ICG had already reduced alerts by 30% — without sacrificing security.

15% cost savings in cloud resources

10% weekly increase in release pace

Case Study

BlaBlaCar empowers developers to manage security risk

> Sysdig customers benefit from community contributions, just as Falco users benefit from Sysdig's contributions to Falco. The fact that Sysdig extends Falco was really enticing to us. With Sysdig, we knew we were getting the best tool integrated with Falco."
>
> — *Security Engineer at BlaBlaCar*

The Challenge

BlaBlaCar is the world's leading community-based travel network. After deciding to add more than 120 nodes to Google Cloud Platform (GCP) and Google Kubernetes Engine (GKE), BlaBlaCar needed a new security solution that would allow developers to build and run applications in production.

The Results

With Sysdig, BlaBlaCar's developers were able to reduce risk with rapid identification of suspicious activity and misconfigurations, thereby enabling the security team to operate more efficiently. Moreover, since Sysdig adds professional support and a SaaS infrastructure to Falco's powerful capabilities, BlaBlaCar's security team could focus on integration instead of spending time on setup and maintenance.

200+ developers empowered to own applications throughout the lifecycle

Overhead reduced with an efficient, secure DevOps model

Case Study

Syfe simplifies threat detection and compliance

> While Falco gave us foundational security, Sysdig enabled us to fully integrate security into how we deploy applications. With Sysdig, security isn't just a checkpoint — it's seamlessly embedded into our workflows, giving us the visibility and control needed to protect our cloud environments effectively."

— Director of Engineering at Syfe

The Challenge

As a digital investment platform operating in heavily regulated markets, Syfe has to ensure its cloud-native infrastructure meets the highest security standards. This made Falco a crucial part of Syfe's security strategy, but once the company upgraded its Elastic Kubernetes Service (EKS) servers, it saw an opportunity to adopt a more efficient, scalable solution.

The Results

By implementing Sysdig, Syfe was able to scale the benefits of Falco with prebuilt, continuously updated threat detection rules. Syfe was also able to consolidate its security stack with Sysdig's centralized dashboard and alerts for vulnerability data, making its development pipeline faster and more secure.

90% reduction in threat response time

95% reduction in time spent on manual threat detection rule updates

Manage threats at cloud speed with Sysdig and Falco

Not every company wants to move from Falco to Sysdig, and that's okay. Protecting your cloud with Falco is now easier than ever with the introduction of Falco Feeds by Sysdig. With Falco Feeds, you can stay ahead of the evolving cloud-native threat landscape without affecting your deployment of open source Falco in production environments. Backed by an active Threat Research Team, Falco Feeds provides continuously updated rules and incorporates regulatory compliance tagging, noise reduction through clearly defined exclusions, and advanced detection context. Users gain a frictionless approach to enterprise-level threat detection with a fully updated detection ruleset, without having to deploy Sysdig.

Discover how Falco Feeds by Sysdig can help you secure every second, while maintaining an open source stack.

Learn more →

sysdig

E-BOOK

EBK-014 Rev. C 3/25

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.