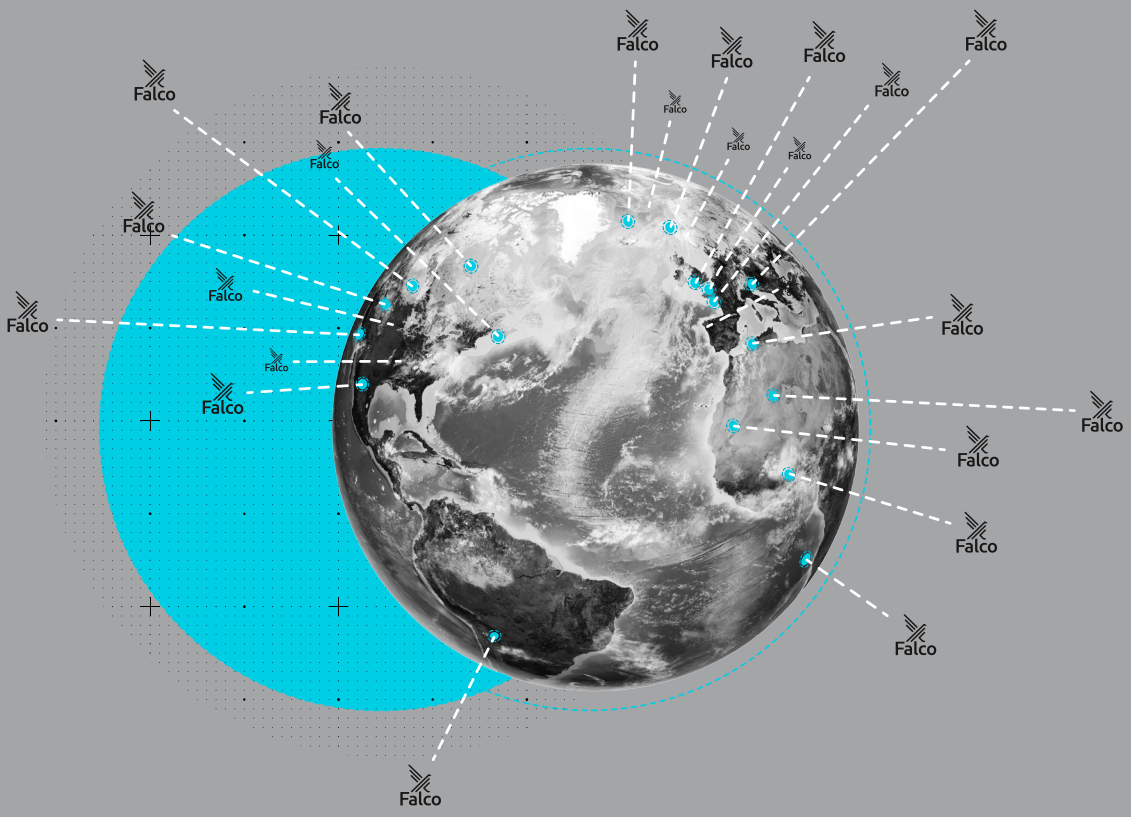
sysdig SECURE EVERY SECOND.

# 2025 Cloud-Native Security and Usage Report

## Highlighting Falco Usage Trends



# Key trends

**Machine identities are 7.5x more risky** than human identities and there are up to 40,000x more of them to manage

**Real-time detection and response in under 10 minutes** — when tools alert within seconds — is possible, and companies are initiating response actions in under 4 minutes

**In-use vulnerabilities have decreased to less than 6%**, but image bloat quintupled year over year

**Workloads using AI/ML packages grew by 500%** and public exposure decreased by 38% over the last year, showing that secure AI implementation has become a clear organizational priority

**60% of containers** live for 1 minute or less

Organizations across the globe in all business sectors are **leveraging open source software**, like Falco, regardless of their size

**Cybersecurity regulations are essential**, and EU-based organizations are leading the charge by prioritizing compliance more than their global counterparts.

*This is a special edition of Sysdig's 2025 Cloud-Native Security and Usage Report, providing only the usage and analysis of the open source detection tool, Falco.*

# Executive summary

The "Sysdig 2025 Cloud-Native Security and Usage Report" is back for its eighth year, analyzing real-world data and the current state of cloud security and container usage. The findings detailed here indicate that security teams have made significant advancements across key areas, not only year over year, but also looking back on previous reports. With this in mind, our 2025 report provides benchmarks for maturity and efficiency, helping security teams, developers, and organizational leaders measure progress in the coming year.

In October 2023, the Sysdig Threat Research Team (TRT) concluded that cloud attacks can take place in 10 minutes or less. In this report, we have detailed how organizations today are detecting, investigating, and responding to real-world threats within this time frame using innovative tools and techniques. We've also found that open source software is not just a trend, but has become a dependency for today's cloud security. The open source threat detection tool Falco has been downloaded over 140 million times and is used across large enterprises and small businesses (SMBs) alike, signaling that organizations of all sizes have found value in the power of open source security.

The security community has also made advancements in vulnerability management and AI workload security. For the second year in a row, we've identified a significant reduction in runtime vulnerabilities. We also saw significant growth in the number of workloads that use AI and machine learning (ML) packages and — despite this growth — the percentage of workloads publicly exposed to the internet has decreased significantly, an indication that organizations are prioritizing AI security.

In assessing identity management from a different perspective than years past, we found that organizations are managing exponentially more service accounts than user accounts, and that these service accounts present higher risk profiles. No wonder supply-chain attacks have become increasingly common!

Finally, in a few surprising turns of events, it turns out that organizations are prioritizing nuanced technical security benchmarks for compliance policies over the federally prescribed regulations we often read about in the news. And last but certainly not least, our beloved container lifespan statistic of many years has taken a new form. Short-lived workloads are purpose-built for speed and only live long enough to complete their task — all the more reason for real-time detection and continuous monitoring.

**Read the full report** for all of this year's findings.

# The adoption of Falco and open source security

Falco is an open source tool that detects anomalous activity within containers, hosts, Kubernetes environments, and more. It has gained widespread adoption across the cloud-native community for its real-time threat detection and continuous monitoring of system calls and application behaviors with customizable rules.

Falco reached a significant milestone in February 2024, achieving graduation within the Cloud Native Computing Foundation (CNCF). This reflects Falco's maturity, widespread use, governance, and proven success in production environments. Falco was originally developed by Sysdig, and contributed to the CNCF in 2018. Falco's momentum is undeniable. It took eight years to reach 100 million downloads, a number which has surged by nearly 50% since its CNCF graduation. The project now has over 140 million downloads from users across the globe.

## Development and maturity of the Falco ecosystem

Since Falco is a community-driven threat detection project, its use and evolution reflect the needs of security and developer teams. Falco began as an intrusion detection system (IDS) and has evolved into a fully functional open source cloud detection and response (CDR) tool.

Falco first appeared on GitHub in May 2016 with a kernel module to monitor system calls. Two years later, it introduced its first Extended Berkeley Packet Filter (eBPF) probe and, more recently, a modern compile once-run everywhere (CO-RE) eBPF probe.

**303**

**out of 500**

Fortune 500 companies downloaded Falco in 2024

Falco

### The dawn of Falco

- 2016 — First commit
- 2017
- 2018 — eBPF; CNCF sandbox
- 2019 — Falcosidekick
- 2020 — CNCF incubation
- 2021 — Plugins; Sysdig donates eBPF libraries
- 2022 — falcoctl
- 2023 — eBPF CO-RE
- 2024 — Talon; CNCF graduation

Although eBPF is now the preferred method for collecting system calls, many hosts still run kernels that are too old for eBPF support. Falco still covers all of these scenarios by offering three drivers — kernel module, eBPF probe, and CO-RE eBPF probe — to ensure comprehensive threat detection on any host.

## Open source is for everyone

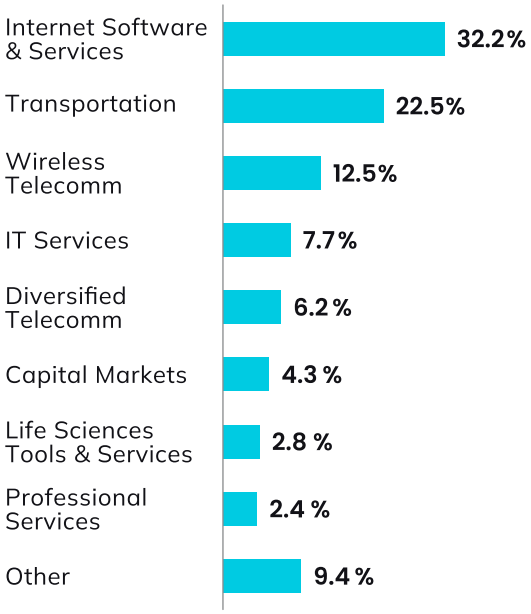
The breakdown of business sectors to the right considers only those organizations using Falco within self-hosted data centers. Companies using public CSPs, for example, are attributed to the CSP's Internet Protocol (IP) addresses and not their own, making those sector distinctions impossible. For this reason, the business sector classification across Falco users is limited.

Otherwise, it should come as no surprise that the majority of users are classified as internet software and services businesses. These organizations tend to support the use of, collaboration with, and contribution to the open source software community, which helps expedite innovation in such a fast-paced business sector.

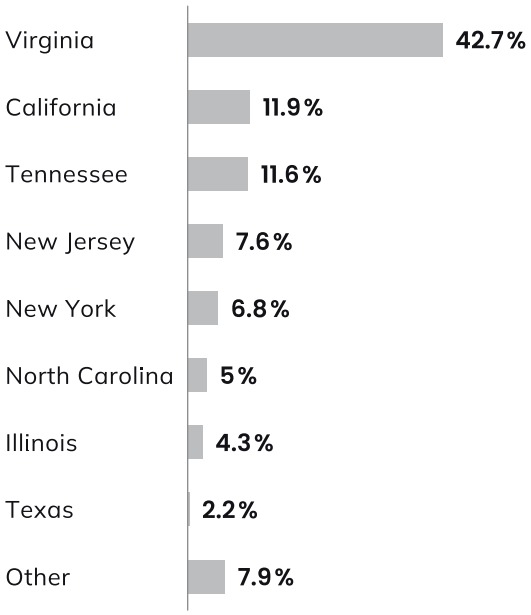
What's more surprising though is that more than 22% of users work in transportation. This significant usage of Falco in the transportation sector may be attributable to very large enterprises with widespread implementation across their organizations, resulting in fewer transportation businesses using Falco than internet software and services businesses, but more individuals using the tool within the sector.

In the U.S., there is a great concentration of contracting companies to various entities of the federal government that are qualified as SMBs, startups, and enterprises. These contractors form a large presence close to the nation's capital, Washington, D.C., which likely accounts for the large number of users in Virginia. The affordability of open source threat detection cannot be overlooked for small, early-stage businesses in this area.

### Falco users by business sector




### Falco users by U.S. state



The large number of users in Tennessee is likely from an established industrial presence in Oak Ridge, and the mass movement and growth of business and technology companies in Nashville.

The global breakdown of Falco users indicates the passion and drive for open source and innovation for security all over the world. Still, the large number of users in Finland (being that it is a small country) comes as a surprise. As we saw with Falco usage in the transportation sector, this is likely a result of broad individual implementation within a limited number of organizations headquartered in the country; unexpected, but not inaccurate.

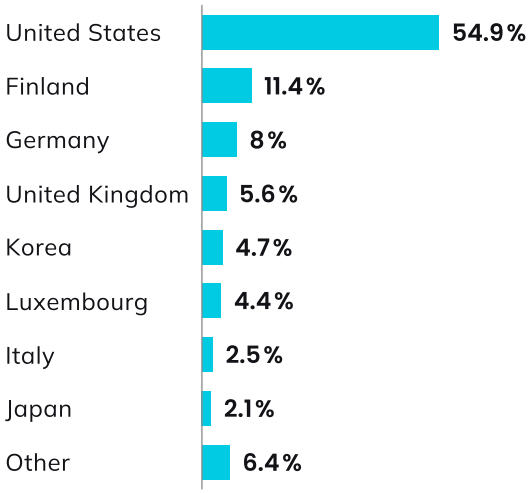
The company size of Falco users shows a healthy mix of small organizations and large enterprises. As expected, there is a large number of users, nearly 34%, at companies with fewer than 250 employees. These are likely early startups and SMBs that do not have the capital for paid threat detection and response services.

## The sky is the limit with open source detection

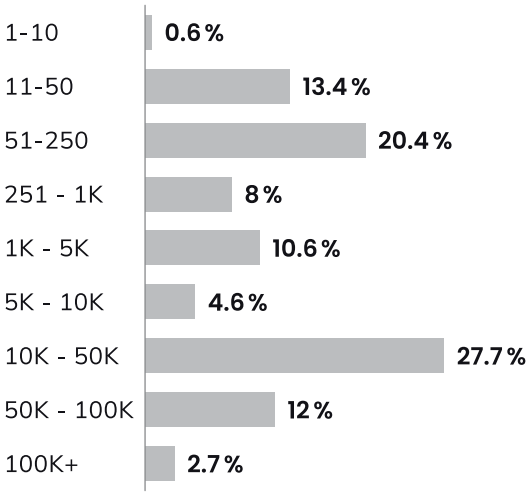
One of the many facets of open source software that many people treasure is the community itself. Not only does the community contribute to the improvement of open source tools directly, but it also contributes to the growth of a tool's operative ecosystem. When it comes to Falco, there are a handful of companion tools to consider.

**Falcosidekick** is a companion tool for Falco that extends alerting and notification capabilities, helping users forward alerts from Falco to various third-party services and tools. The first GitHub release was in October 2018; since then, there have been over 28 million lifetime downloads and over 9 million downloads in 2024 alone, most of which followed a highly anticipated version release on July 1, 2024.

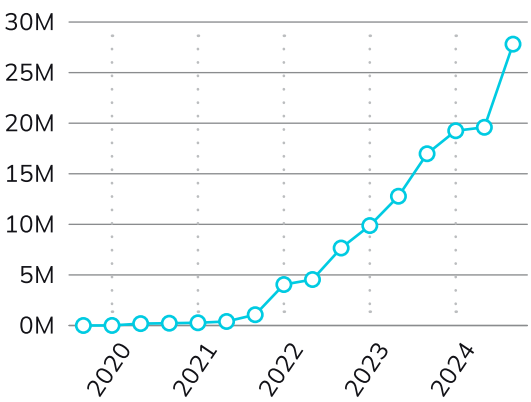
### Falco users by country




### Falco users by organization size




### Falcosidekick downloads by date



**Falco Talon** is a command and control framework that allows users to take immediate response actions following a Falco alert. First created in July 2023, the generally available version was only just released in September 2024 and had nearly 140,000 downloads at the end of 2024.

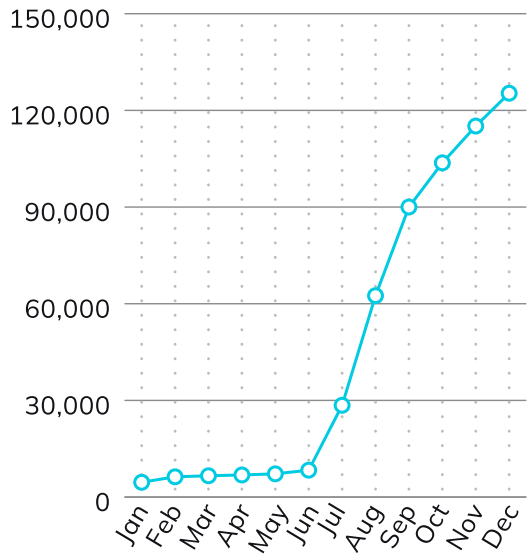
Falco is also able to integrate with many popular security and business tools via plug-ins. The adoption and interest in Falco outside of the application scope is noticeable in the number and variety of plug-ins being created by the community and the rate at which new plug-ins are added.

This trend is an indication that organizations are no longer just protecting runtime, but using Falco to detect anomalies within their Kubernetes control plane (managed or not), cloud accounts, CI environments, and more. **The Falco community embodies the "one team, one fight" mentality that is necessary in today's cyberdefense industry.**

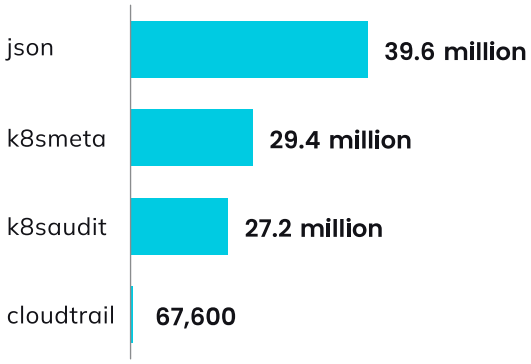
Some of the most popular Falco plug-ins are **json** for field extraction from JSON payloads, **k8smeta** for enriching Falco system call flows with Kubernetes metadata, **k8saudit** for reading Kubernetes audit events and monitoring Kubernetes clusters, and **cloudtrail** for reading Cloudtrail JSON logs from files and S3 buckets and injecting them as events into Falco.

Some of the most creative and unique plug-ins created by Falco users include one for **Salesforce** runtime threat detection and audit logging, one for **Keycloak** user and admin identity access management events, and one for **Box** threat detection and audit logging.

## Falco Talon downloads in 2024




## The most popular Falco plug-ins by downloads



sysdig SECURE EVERY SECOND.

In the cloud, every second counts. Sysdig stops cloud attacks in real time by instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across workloads, identities, and services to uncover hidden attack paths and prioritize the risks that matter most.

**Sysdig. Secure Every Second.**

LEARN MORE →




FALCO-RP-012 REV. A 03/25