sysdig SECURE EVERY SECOND.

2025 Cloud-Native Security and Usage Report

Real data. Real threats. Real benchmarks.

Table of Contents

Key trends 03

Executive summary 04

Cloud detection & response in minutes 05

Manage humans, machines, and every identity in between 10

Navigate risk and reward with secure AI 14

Manage risk in containerized environments 18

The adoption of Falco and open source security 22

Security starts with foundational compliance 27

Methodology 31

Conclusion 32

Key trends

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

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

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

60% of containers live for 1 minute or less

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

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.

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.

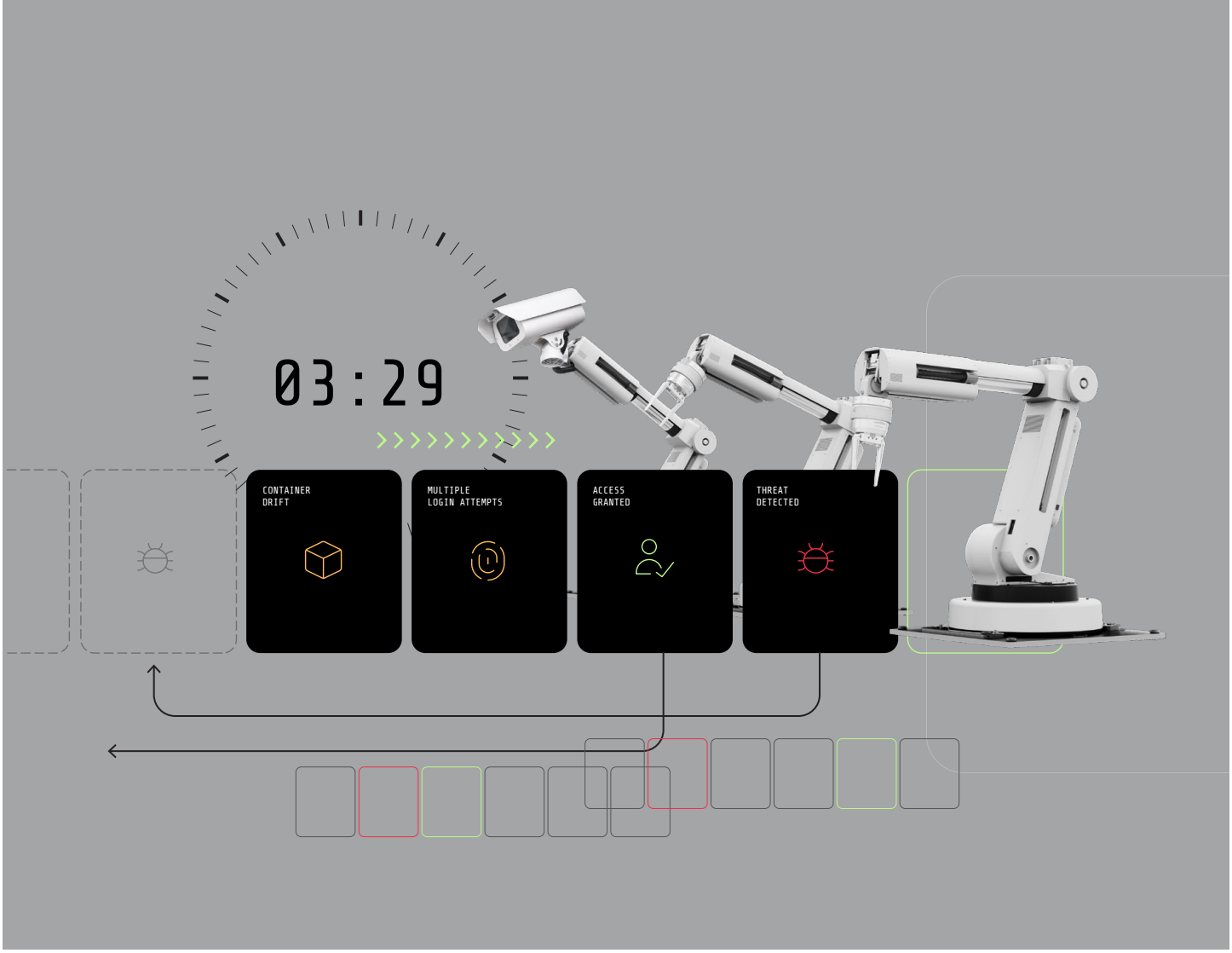
In October 2023, the Sysdig Threat Research Team (TRT) concluded that cloud attacks can take place in 10 minutes or less. In this report, we have detailed how organizations today are detecting, investigating, and responding to real-world threats within this time frame using innovative tools and techniques. 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 on to get the statistics for all of this year's findings.



Cloud detection & response in minutes

At the end of 2023, the Sysdig TRT set the benchmark for cloud threat detection and response, stating that cloud attacks happen in 10 minutes on average. 5 seconds to detect, 5 minutes to investigate, and 5 minutes to initiate a response might seem like a high bar, but it is both possible and necessary for organizational security. Among the most common threats to cloud infrastructure this year, as noted in the 2024 Global Threat Year-in-Review, was the exploitation of anything open source, a trend that shows no signs of stopping.

Real-time detection in 5 seconds

Unfortunately, alerts don't just go from an event straight to security teams. Believe it or not, there are several "hops" that data has to take to get from the scanner to the inbox or notification dashboard, and that time can quickly add up. Errors in the data transfer life cycle can cause detection alerts to be delayed by minutes, effectively eliminating the opportunity for a timely response.

What does this mean in practice? After analyzing hundreds of thousands of alerts from hosts and containers across production regions, we found that the average time it takes our users to receive an event notification is less than five seconds, right on par with the 555 Cloud Detection and Response Benchmark. Real-time threat detection and response is imperative when an attacker can wreak havoc on an organization in minutes, and slower methods that take 15 minutes or longer have become severely outdated.

> "I don't want to know 15 minutes after a potential threat has been identified in our environment. I need to know instantly so we can shut it down before the threat has material impact.
>
> - Jordan Bodily, Senior Infrastructure Security Engineer, BigCommerce

Sysdig processes 2 BILLION EVENTS DAILY

Incident investigation in less than 5 minutes

Traditionally, organizations receive alert notifications for high-fidelity detections, and manually review low and medium alerts daily. This practice is time-consuming and risky, especially for newly established or small security teams.

Instead, the initial response to a potential incident should be hands-off. Security teams should have automated response actions in place. They should also build confidence and risk reduction right into their operating practice. They can achieve this by using high-fidelity detections that cover a large swath of the MITRE ATT&CK framework, especially for threats concerning their particular environment, tools, software, and business sector.

Incident investigation presents a key use case for the implementation of a generative AI (GenAI) security assistant. Even if manually processing security alerts is the preferred method of analysis, the right tool can help find, understand, and correlate alerts much faster **and** reduce the risk of missing a key indicator.

The best option for rapid and robust incident investigation that allows security teams to keep pace with cloud attacks is automating the collection and correlation of the misbehaving identities to all related events, postures, and vulnerabilities. We found, for example, that Sysdig customers using enhanced investigation and real-time identity correlation features can visualize and understand the relationships between resources and their impact on the attack chain, **completing their investigations and moving on to response in less than three-and-a-half minutes on average.** Again, this is well within the 555 Benchmark's "5 minutes to investigate" suggestion.

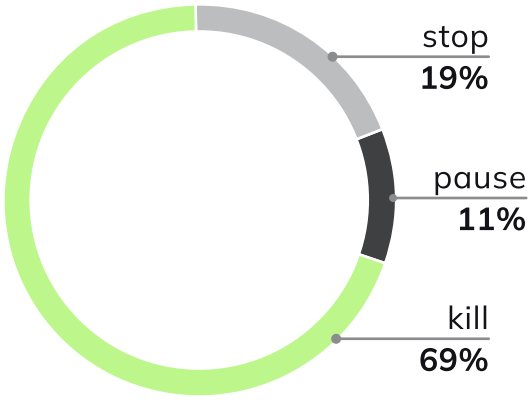
> In the cloud, you may be managing multiple environments, thousands of identities, and an untold number of workloads. Without clear and comprehensive runtime visibility across those components, investigations take weeks. If you're not ready to investigate in minutes, you're going to lose.
>
> - Cat Schwan, Senior Manager, IT Security, Apree Health

> In the past, an investigation could take up to a week. With Sysdig, it's a 5-10 minute job.
>
> - Information Security Leader, Security Operations Provider

...and incident response must be automated

While most users are still cautious and prefer to alert only on container drift, the number of drift control policy users who enabled automated preventive actions — such as kill, stop, or pause at the indication of container drift — nearly **tripled over the last year**. The image below represents the automated actions organizations choose to respond to container drift.

More than 11% of customers chose one of the following automated drift actions



There are, however, multiple actions and behaviors that can be misidentified as drift, such as a virtual machine in a container, or third-party-owned self-updating containers. The automated and inadvertent pausing or stopping of these benign container actions could cause undue operational issues; therefore, automated drift control response is an indicator of advanced maturity, and more importantly, **confidence,** in an organization's security program.

Define your prevention

As container security practices have matured over the last year, Sysdig has added options for additional, high-confidence automated response actions for threat detections and malware indicators. For example:

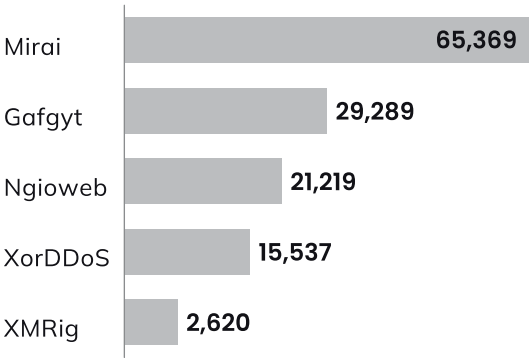
- We began by defining a drifted binary as any binary that was not part of the original image of the container, but was typically downloaded or compiled within the running container.
- We then introduced the ability to detect volume-based binaries that would treat all binaries from mounted volumes as drifted. With great drift detection comes great responsibilities.
- Recently, we granted users the power to define regular expression (RegEx) statements to define exceptions. These fine-grained exceptions allow specific files or binaries to run without being incorrectly detected as drift by the Sysdig agent.

In addition to autonomously killing, stopping, or pausing a misbehaving container, users may also automatically issue a **"kill -9"** command on the process following a threat detection alert. In addition, it is also possible to autonomously prevent drift and malware at the system level via hooks. With this additional step, every execution attempt will ask the agent and confirm or deny the action based on whether or not the policy is applicable, since the policy must be enabled **and** scoped. The confirmation is important because it ensures real-time enforcement of security policies, which prevents unauthorized or malicious activities before they can compromise the runtime environment.

The hottest Linux malware is open source

The Sysdig TRT analyzed over 272,000 malware hashes to determine the most commonly used Linux malware families over the last year. It came as no surprise that the most common malware variant was Mirai because of its accessibility and adaptability. The Sysdig TRT often reports on attacks using this open source malware code, including the RebirthLtd distributed denial of service (DDoS)-as-a-service botnet group.

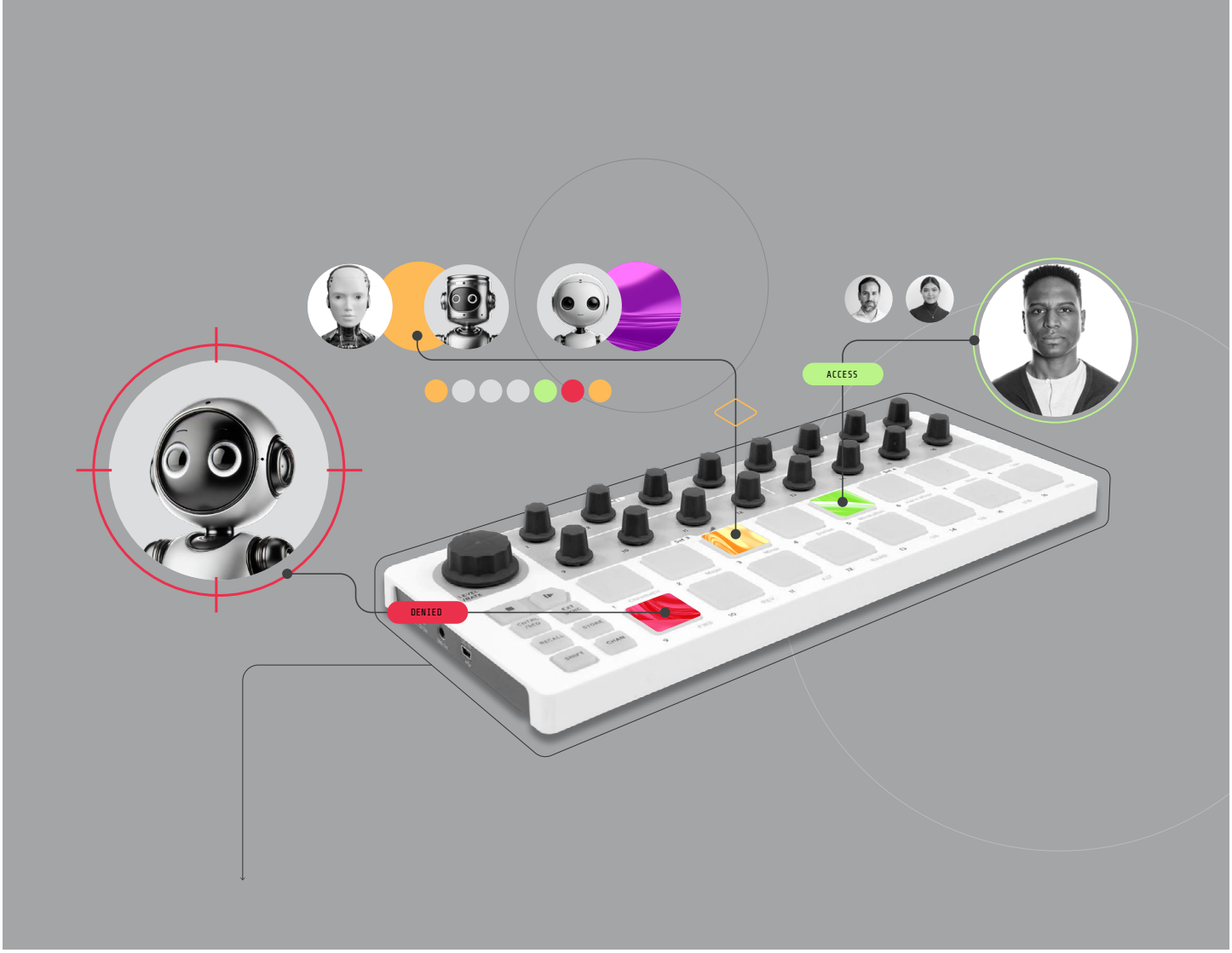
The chart below lists 2024's five most common Linux malware families:



Security teams should regularly use threat intelligence to refine and enhance their static threat detections. Last year, we found that 35% of attacks could be identified with indicators of compromise (IoC)-based detections. Attackers can easily modify malware hashes to avoid these detections, however, rendering them useless. It is imperative to have a layered approach to threat detection and response that captures the broader threat landscape. The number of attacks requiring behavior-based detection will continue to increase as attackers mature and bypass traditional, signature-based detections.

One of the trends from the 2024 threat landscape was the surge in attackers leveraging open source tools for malicious purposes.

READ THE 2024 GLOBAL THREAT YEAR-IN-REVIEW →



Manage humans, machines, and every identity in between

It is no secret that ironclad identity management and strong identity security are necessary in cloud security. Weak or missing credentials were the initial access vector for 47% of cloud environments in the first half of 2024, according to Google Cloud's "H1 2024 Threat Horizons Report." Effective and well-governed identity management is one of the most basic (but also complicated) ways to reduce the risk of attack. Let's explore a few reasons why.

Compare identities across cloud service providers

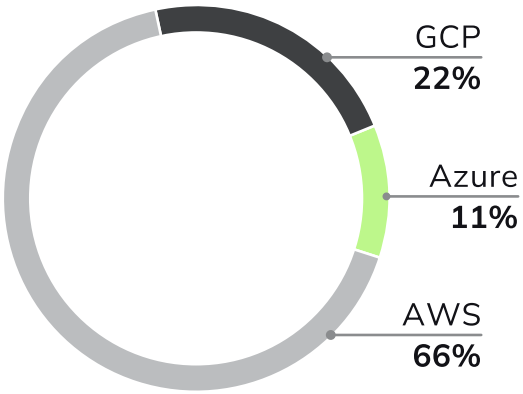
When analyzing identity usage data, we identified a fascinating anomaly in the number of users that organizations maintain within each cloud service provider (CSP). This anomaly was present even among multicloud users. Azure had up to 67x more "users" than Amazon Web Services (AWS) and Google Cloud Platform (GCP). Intrigued, we dug in.

We quickly realized that every time a user logged into a new application that relied on Entra ID (formerly known as Azure Active Directory) for identity verification, a new Azure user was tallied. This includes Microsoft Office applications, service emails, mailing lists, and more. In other words, while some of these "users" may be humans with access to their organization's Azure cloud portal, the vast majority very likely have Microsoft usage limited to single sign-on (SSO) and Office.

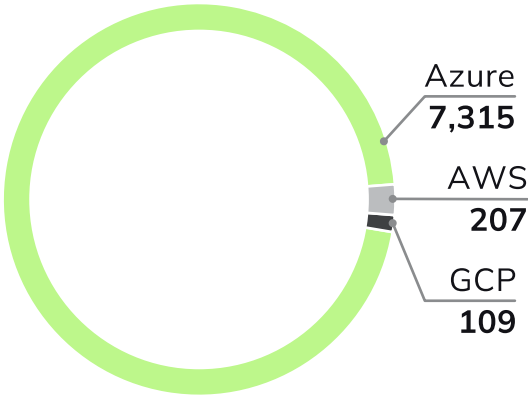
For example, an employee with access to Outlook, OneDrive, OneNote, PowerPoint, Excel, and Word accounts for seven users in Azure.

Google and AWS do not have a directory or identity solutions like this; therefore, the user count for Azure CSP organizations is greatly skewed.

Percentage of organizations maintaining identities per CSP



Average number of users per CSP



Move past excessive permissions

Identity management is often time-consuming and challenging to maintain. In the 2024 report, we found that organizations maintained an excessive amount of risk, with 98% of granted permissions going unused. Overpermissioning is the fastest and easiest way to get work done, although nearly all security experts advise against it.

While excessive permissions are (much) less than ideal — and they significantly increase the risk of a cloud breach by giving malicious actors undue opportunities for initial access, lateral movement, and access to sensitive data — some organizations consider them an accepted and tolerable risk that expedites business operations. If this is the case, proactively implementing security practices such as multifactor authentication (MFA) can reduce the risk of identity attacks, and detect and mitigate potential attacks.

Minimize unnecessary risk of excessive identities

So if excessive permissions are being tolerated, how many identities are organizations managing? We found that, on average, organizations have 915 users and 41,605 service accounts: no wonder identity management is hard! This is a **40,000x difference** between the types of identities connected to CSPs.

Fortunately, one could argue that this statistic is skewed by noise from poor provisioning, and that these excessive identities are a low security risk. However, as much as an organization with more than 1.6 million unassigned service accounts might be an accident waiting to happen, the unused accounts are low priority compared to vulnerabilities in use. After applying some data manipulation and filtering out 11% of organizations with excessive users (organizations using Azure) or excessive service account numbers, the averages were more realistic — 152 users to 5,330 service accounts. That's still 35x more service accounts to manage than users, but an easier pill to swallow.

With that said, we found that nearly 15% of organizations have no connected user accounts. This — organizations properly managing cloud identity access — is a sure sign of security maturity. These organizations likely use a third-party-provided SSO verification process to log into cloud accounts rather than establishing and maintaining traditional, local user, and password combinations for access to cloud environments and resources. There are still human users logging in, but they aren't counted as users because of the added security layer of using a third-party verification service.

Nearly 15% of organizations have no connected user accounts.

Define your identity risk

An organization's perception of risk depends on the definition it subscribes to.

During data collection and analysis for this report, we defined a "risky" user as one without MFA enabled or rotating access keys. With that definition, only 8% of organizations maintain risky users.

On the other hand, we defined a "risky" service account as an AWS service identity, Azure principal, or GCP account that had administrator-level access without rotating access keys. By this definition, a whopping 60% of enterprises maintain risky service accounts, making them 7.5x more risky than users.

This means that organizations are doing a better job configuring user accounts, and possibly prioritizing user identity management.

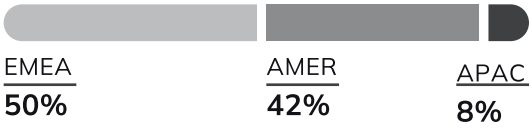
However, there are still risk concerns for the other 92% of non-risky users. Attackers can still gain access through targeted spearphishing attempts, risky user or not. Training all employees within an organization to recognize these threats is still imperative.

This is especially true as attackers use AI to improve the targeting, success, and scale of their spearphishing campaigns. Cybersecurity is an organizationwide responsibility. These risky users are likely known and acceptable risk profiles for administrators or test accounts.

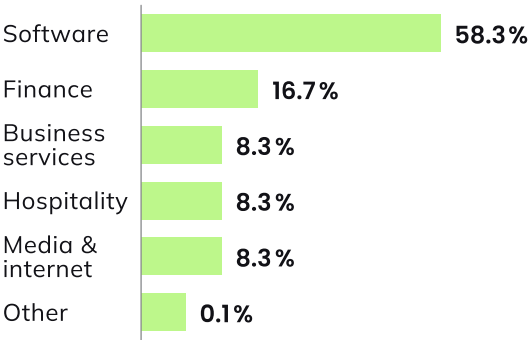
For risky service accounts start with a simple measure: add hygiene to old security methods. Legacy vendors still permit the use of long-lived keys and, if an organization is using these, they need to be stored securely and rotated. Organizations can also use precisely defined trust relationships to allow human users or service accounts to assume other identities and access other resources temporarily. Trust relationships also enhance security and simplify management because credentials and excessive permissions are not required, reducing an attacker's opportunity for initial access.

Risky users

Location

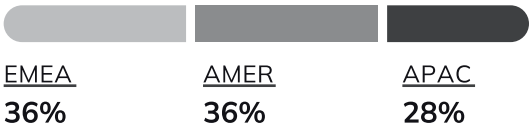


Location

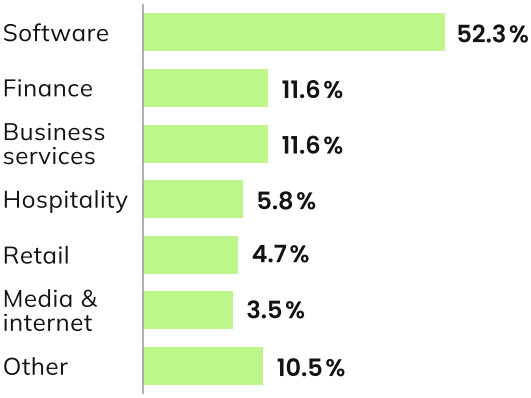


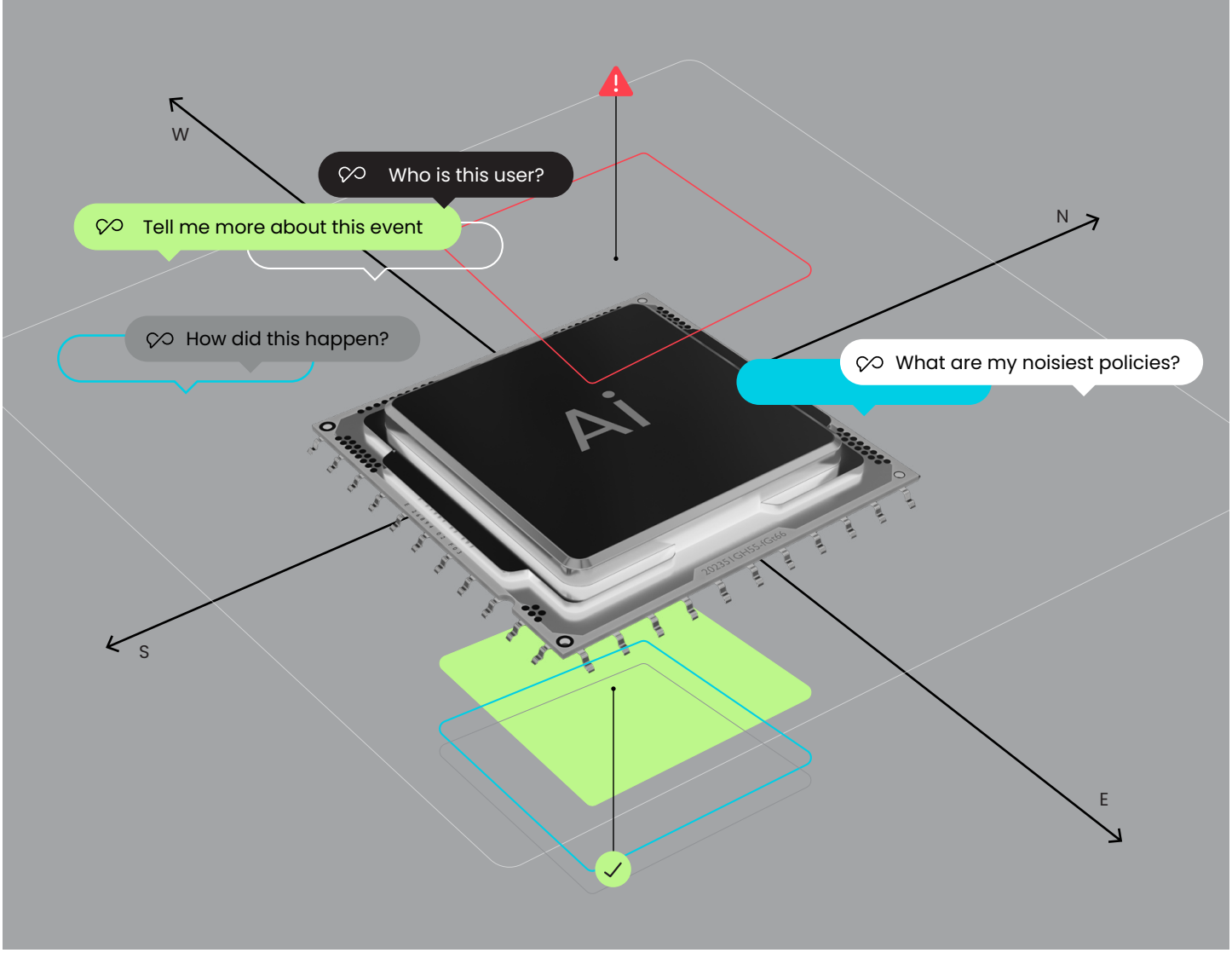
Risky service accounts

Location



Industry





Navigate risk and reward with secure AI

With ChatGPT's viral public launch in November 2022, we've now experienced more than two years of widespread AI use — and security concerns have been plentiful. AI security concerns generally fall into two buckets: how to use AI to enhance security practices and how to secure AI itself, both of which are valid. But alongside increased usage, we've also seen many AI security trends to be optimistic about.

Adoption of AI for security is on the rise

According to the Cloud Security Alliance's "State of AI and Security Survey Report" published in April 2024, 55% of organizations planned to implement GenAI solutions in 2024. Companies were indeed eager to adopt GenAI! Within four months of Sysdig Sage™ becoming generally available — it's the first GenAI cloud security analyst — 45% of Sysdig customers had enabled it.

GenAI has worked itself into many professionals' daily routines, and cybersecurity is no different. 75% of Sysdig Sage users identify themselves as part of a security operations (SecOps) team. Sysdig Sage has effectively helped them triage alerts, identify threats, and spot abnormal patterns.

> Attackers are already using AI every day, so security teams can't afford to fall behind. I wouldn't rely on a security platform today that doesn't leverage AI to some degree, but I'm also not blindly buying into the hype. Not all AI is created equal—glorified chatbots just don't move the needle. Real value comes from AI that actually enhances efficiency, speeds up human response, and acts as a force multiplier.
>
> - Brayden Santo, Senior Security Engineer, Sprout Social

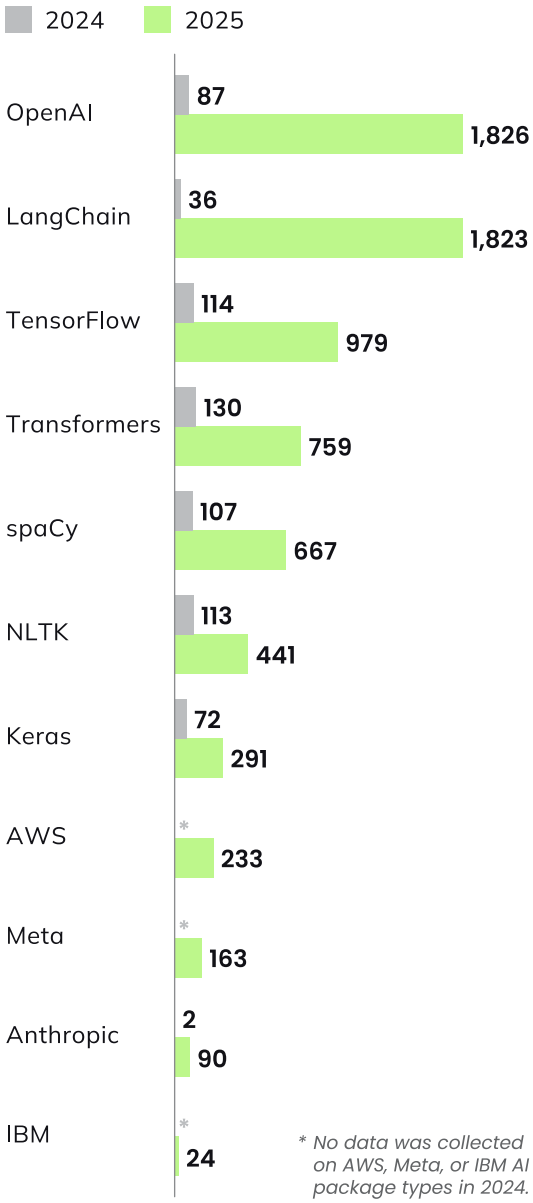
Secure workloads that use AI

The use of AI tools in an enterprise environment, specifically large language models (LLMs), raises concerns about data governance, security, and sovereignty. With users potentially feeding some of their most sensitive proprietary data and customer information into AI models, many have begun to prioritize vulnerability management with tools such as Sysdig's AI Workload Security.

75% of our customers are using AI or ML packages in their environments, which has more than doubled since last year's report. In addition, **the number of AI/ML packages running in workloads has also grown by nearly 500% over the last year.**

In our 2024 report, only 15% of customers' AI/ML packages were specifically GenAI, while the rest were tools typically used for data correlation and analysis. The percentage of GenAI packages has more than doubled in the last year, from 15% to 36%. See the breakdown of package types in the figure to the right.

AI package types



** No data was collected on AWS, Meta, or IBM AI package types in 2024.*

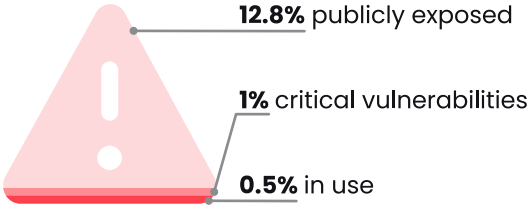
The percentage of GenAI packages has more than doubled in the last year, from 15% to 36%.

But how secure are those packages? In April 2024, 34% of customers' workloads containing AI packages were publicly exposed. Public exposure, which refers to a workload's accessibility from the internet or another untrusted network without appropriate security measures in place, puts the sensitive data potentially leveraged by AI models unnecessarily at risk. Even through the rapid growth in AI adoption, that public exposure rate has been reduced to less than 13% — a reduction of 38% in eight months.

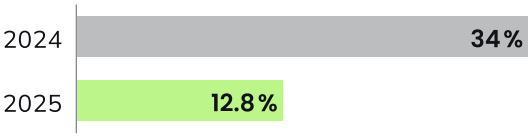
This risk reduction is likely attributable to the novelty of AI tools' capabilities, and coincides with the deserved scrutiny around security concerns that bubble up in every mention of AI and cybersecurity. This quickly improving AI security posture should come as no surprise, since many of the early adopters that have implemented AI in their enterprise environments are at the forefront of both innovation and security prioritization.

Public exposure of workloads containing AI

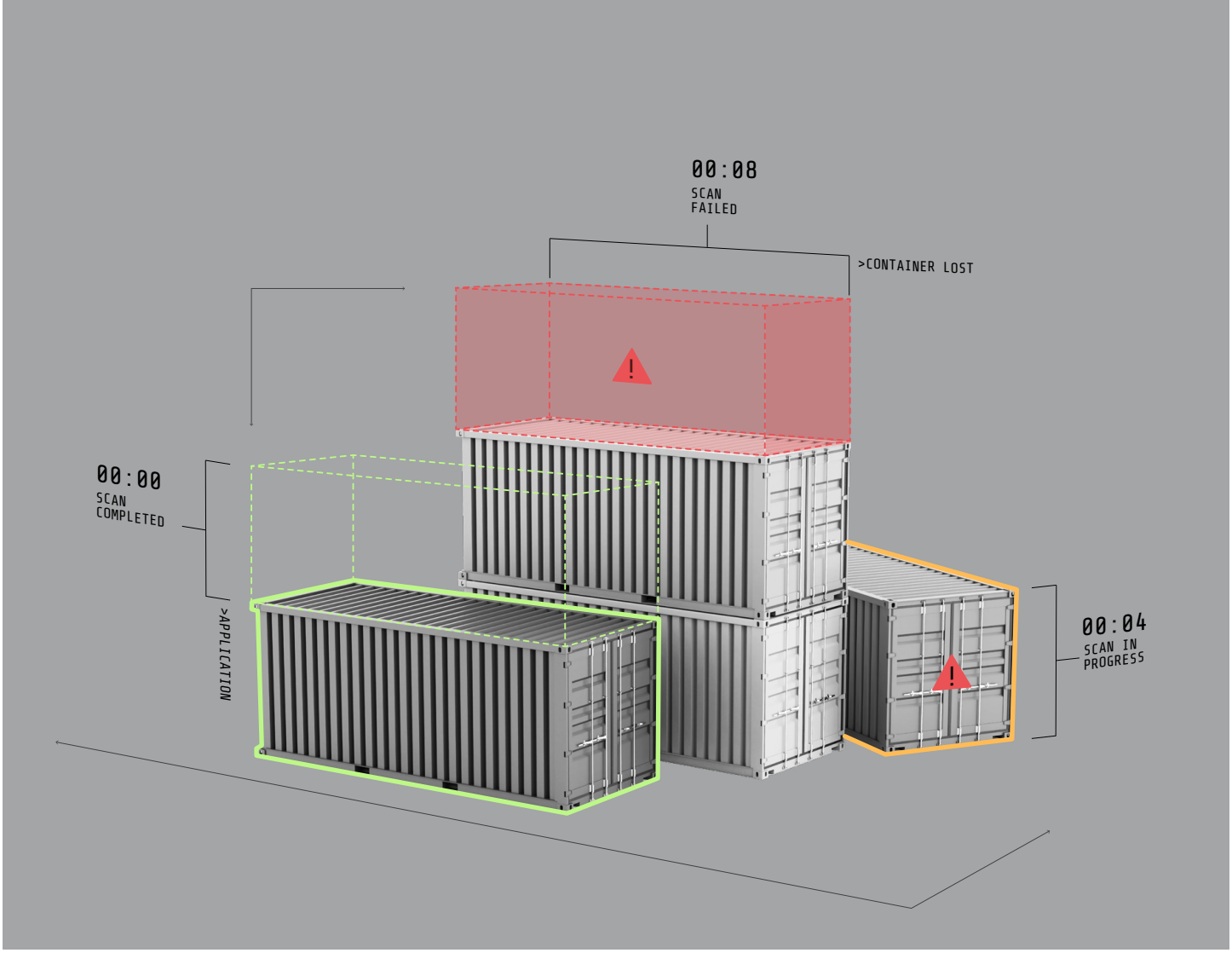
In 2025, **12.8%** of workloads containing AI packages are publicly exposed



Year over year comparison



Public exposure rate has been reduced to less than 13% — a **reduction of 38% in eight months.**



Manage risk in containerized environments

Prioritize vulnerability management

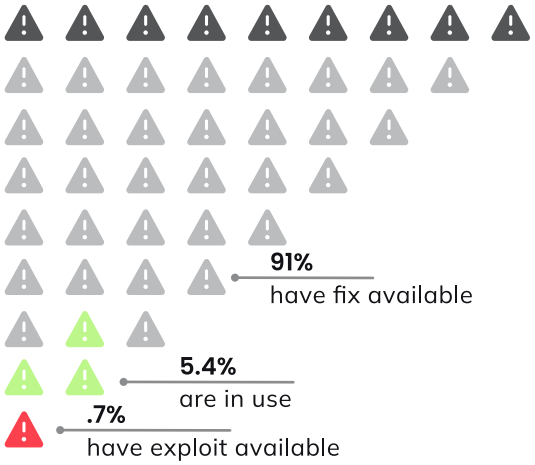
Security providers, Sysdig included, have been beating the vulnerability management drum consistently for the last few years. We analyzed the vulnerability landscape two years ago and presented the best and most effective prioritization method: in use. We define in-use vulnerabilities as any vulnerability associated with a package actively loaded and used in a running environment. Year over year, we have reviewed this data and found that organizations continue to drastically reduce operational risk by properly prioritizing the vulnerabilities that matter most before the thousands that don't.

Since we began tracking the prioritization and remediation of critical and high risk in-use vulnerabilities, we have witnessed a remarkable improvement in organizational vulnerability management. Each year, we analyze a greater number of workloads than the year before, and as shown below, the focus on vulnerabilities in use works. Of all of the images we analyzed, less than 17% had critical or high vulnerabilities.

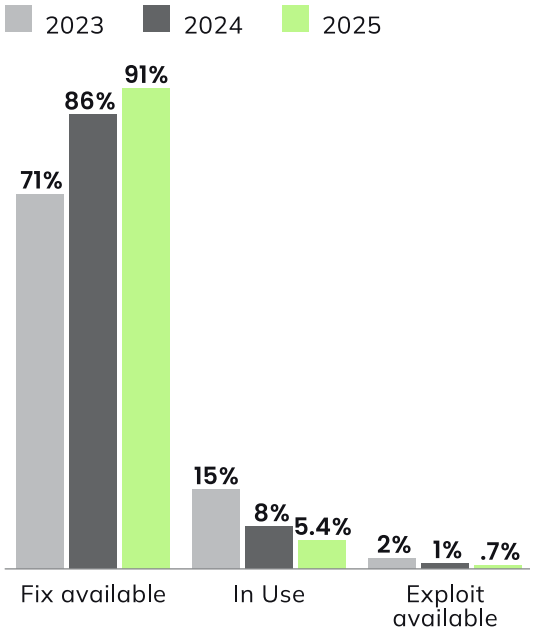
The percentage of critical and high-risk vulnerabilities with only a fix available has gone up each year. This is OK, though, because we can assume that these vulnerabilities are not in a production environment, and therefore have taken a backseat in prioritization to those that are.

Critical & high vulnerabilities

Out of 100 workloads with critical or high vulnerabilities



Year over year comparison



Shrink image bloat

Image bloat, or the inclusion of excess packages that are not required for an application to run properly, poses another risk and unnecessary cost. Ideally, an image should only contain the code necessary to successfully carry out its job. Unfortunately, the problem of image bloat seems to be on the rise.

Image bloat quintupled over the last year, and although bloated images still only make up a small fraction of all container images, we've also seen a 300% increase in the overall number of packages in container images. Again, that portends added cost and security risks.

There could be several reasons for the expansion of packages and image bloat, but these increases are likely due to developers simply adding readily available libraries and bloated open source software to expedite development. One reason could be attributed to the rapid growth and reliance on open source and vendor-managed workloads containing AI, as noted in the section "Security workloads that use AI," which has grown by 500%. Put simply, many are "throwing in the kitchen sink" to ship new or modified applications faster.

Reducing image bloat can be time-consuming, but regular audits of base images make it less painful — as does building efficient container images from the beginning. Consider using an AI tool to scan for and identify unused packages. Review of the findings can still be manual if desired.

With reduced image sizes, there are fewer vulnerabilities and a smaller attack surface. Application delivery, continuous integration/continuous deployment (CI/CD) pipelines, and vulnerability scanners will run faster with smaller images. There are cost savings as well. Running smaller workloads results in less storage, greater network bandwidth, and fewer computing resources used. It's a win-win.

Image bloat **quintupled** over the last year!

Optimize container lifespans

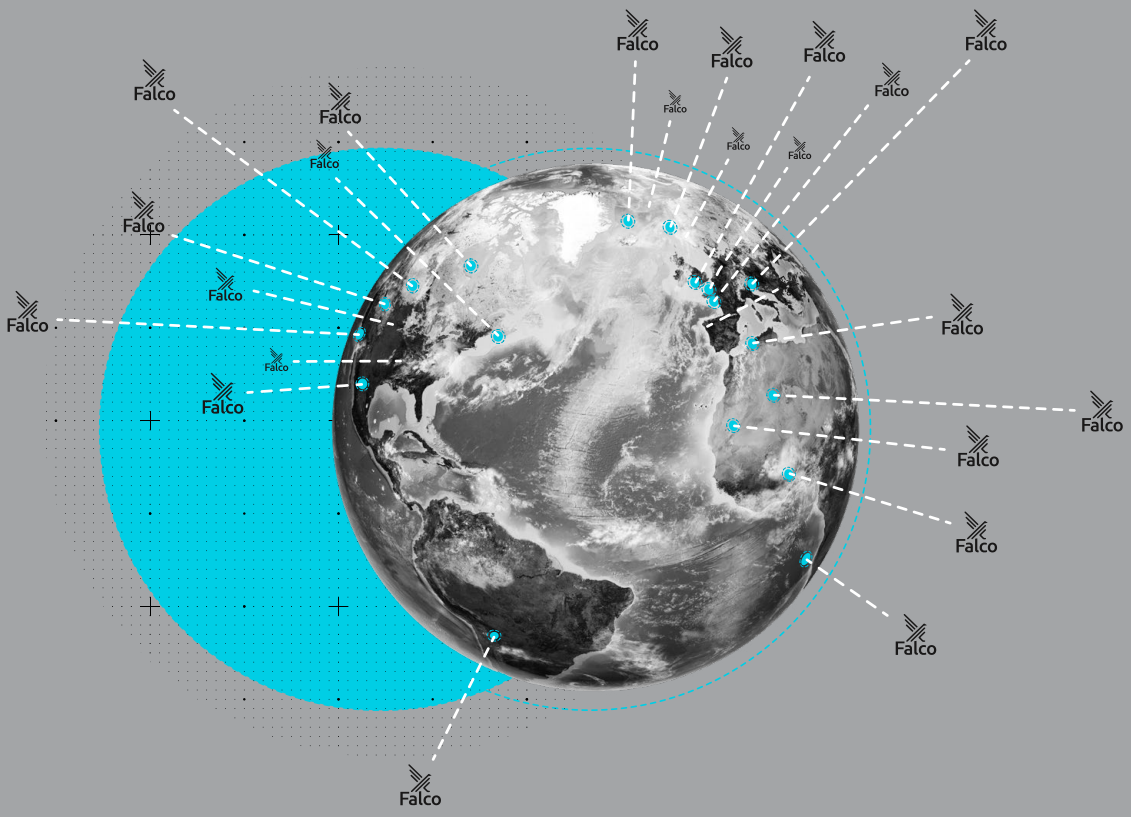
Since 2018, Sysdig has reported on the ephemerality of containers in our annual report, and since 2023, over 70% of containers have lived for five minutes or less. This year, the data says that 74% of containers now live for five minutes or less. **We also found that 60% of containers live for one minute or less**, and only a fraction of these are caused by errors.

Let's explore a few reasons why a container's lifespan could be less than one minute:

- **Purpose-built short-lived tasks:** A container can house and run the entirety of an application faster and more cost-effectively than a virtual machine. In modern application development, containers are used in a more compartmentalized manner. A container is used for brief tasks, such as running only a portion of a script or process that happens very quickly. This could be batch processing, test execution, data transformation, or running a CI pipeline. Once the task is complete, the container no longer exists.
- **Serverless or microservices design:** In serverless and microservices cloud architectures, functions or services are designed to run briefly in order to handle a single request or job, similar to purpose-built short-lived tasks. For instance, a container might spin up to process a single API request and terminate upon completion.
- **Resource constraints:** Sometimes, containers are intentionally limited by resource constraints or orchestrator policies. For example, if a Kubernetes pod's readiness or liveness probe fails, the policy check may initiate an alert and pause or shut down the container to save resources until a human can review the error and restart the container.
- **Health checks:** Kubernetes workloads may have aggressive health-check settings, which will cause a container to be terminated if it doesn't pass a readiness check within a short, specified time frame.
- **Crash or misconfiguration:** If there's an issue with the application code or configuration, the container may fail shortly after it starts. Common causes include missing environment variables, incorrect dependencies, or runtime errors.

Given how quickly things move in container-based environments, real-time security isn't just nice to have — it's mandatory. There is not enough time to manually submit a Jira ticket to kick off incident response before a container stops.

Implementing two security processes will combat short-lived containers. First, use admission controllers to define and customize what is allowed to run in clusters. This proactive measure will block a pod from running if the image is not secure. Second, implement high-fidelity automated response actions such as container drift control so that when there is potentially malicious behavior in an active production environment, the container can be paused or stopped in real time. This will mitigate further malicious access and allow some breathing room for incident response.



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. 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.

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

Open source is for everyone

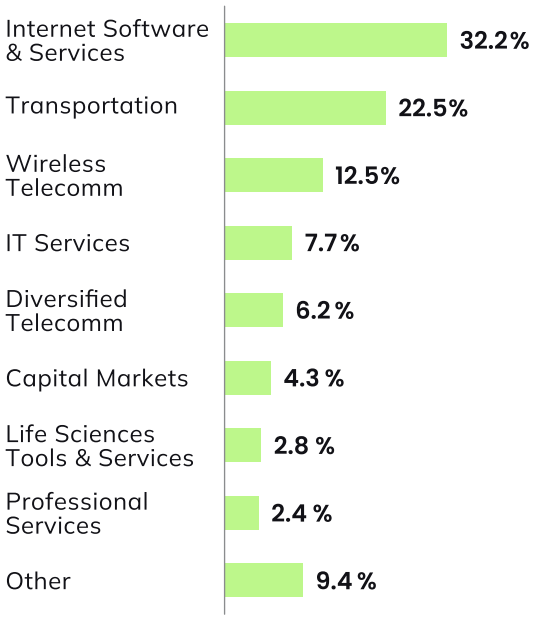
The breakdown of business sectors to the right considers only those organizations using Falco within self-hosted data centers. Companies using public CSPs, for example, are attributed to the CSP's Internet Protocol (IP) addresses and not their own, making those sector distinctions impossible. For this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

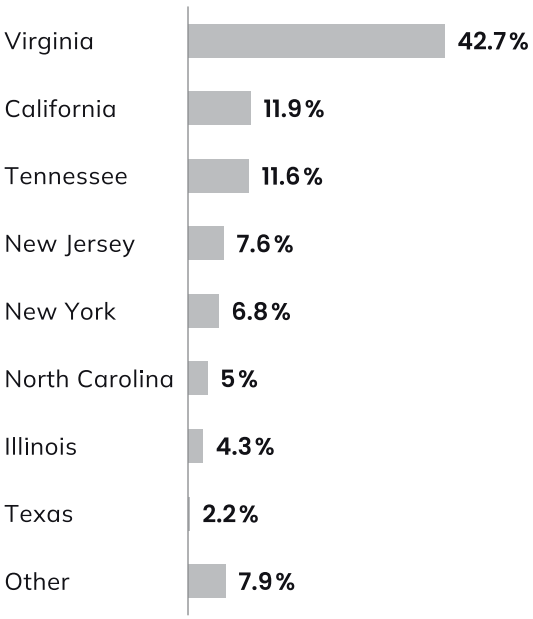
What's more surprising though is that more than 22% of users work in transportation. This significant usage of Falco in the transportation sector may be attributable to very large enterprises with widespread implementation across their organizations, resulting in fewer transportation businesses using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

Falco users by business sector



Falco users by U.S. state



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.

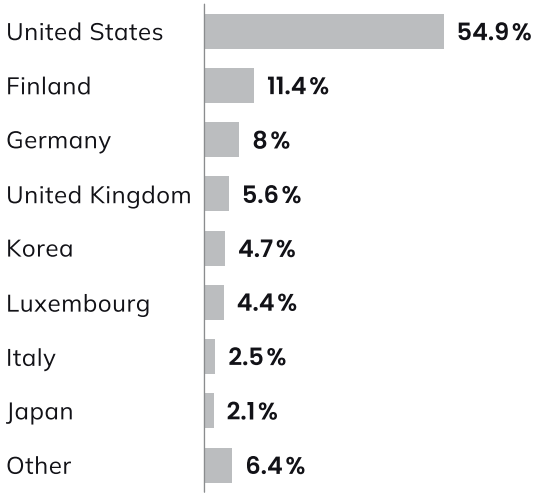
The company size of Falco users shows a healthy mix of small organizations and large enterprises. As expected, there is a large number of users, nearly 34%, at companies with fewer than 250 employees. These are likely early startups and SMBs that do not have the capital for paid threat detection and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

The sky is the limit with open source detection

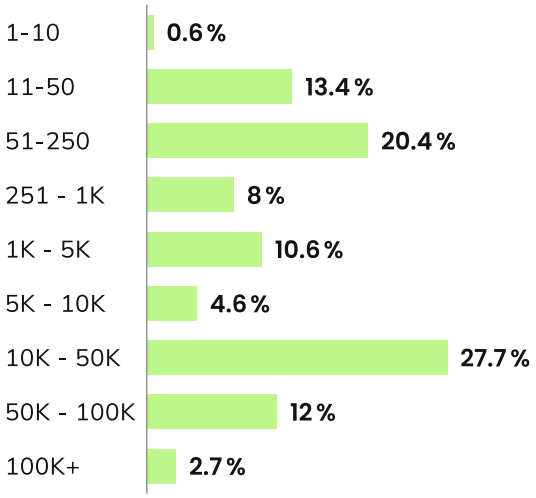
One of the many facets of open source software that many people treasure is the community itself. Not only does the community contribute to the improvement of open source tools directly, but it also contributes to the growth of a tool's operative ecosystem. When it comes to Falco, there are a handful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

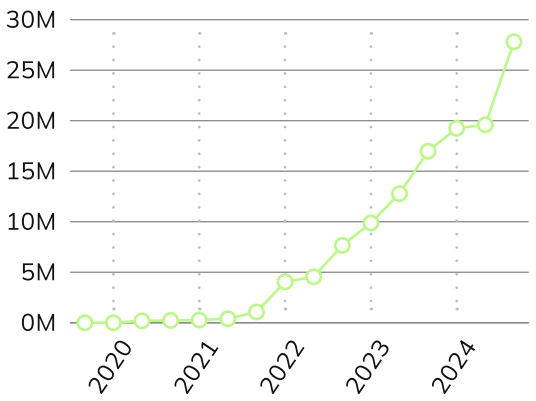
Falco users by country



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.

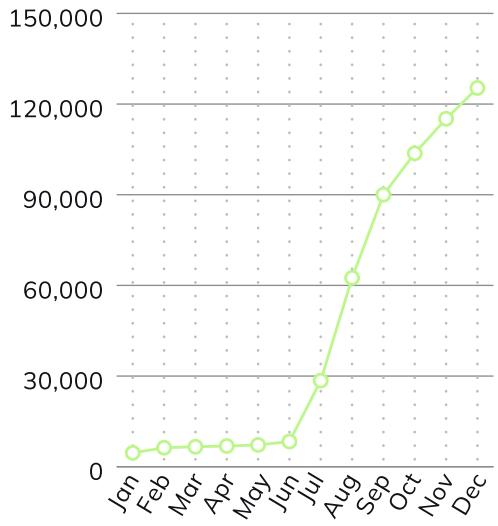
Falco is also able to integrate with many popular security and business tools via plug-ins. The adoption and interest in Falco outside of the application scope is noticeable in the number and variety of plug-ins being created by the community and the rate at which new plug-ins are added.

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.**

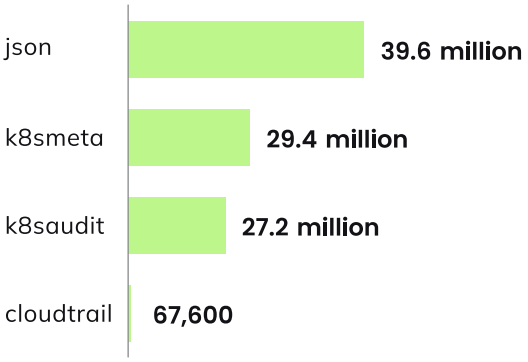
Some of the most popular Falco plug-ins are **json** for field extraction from JSON payloads, **k8smeta** for enriching Falco system call flows with Kubernetes metadata, **k8saudit** for reading Kubernetes audit events and monitoring Kubernetes clusters, and **cloudtrail** for reading Cloudtrail JSON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

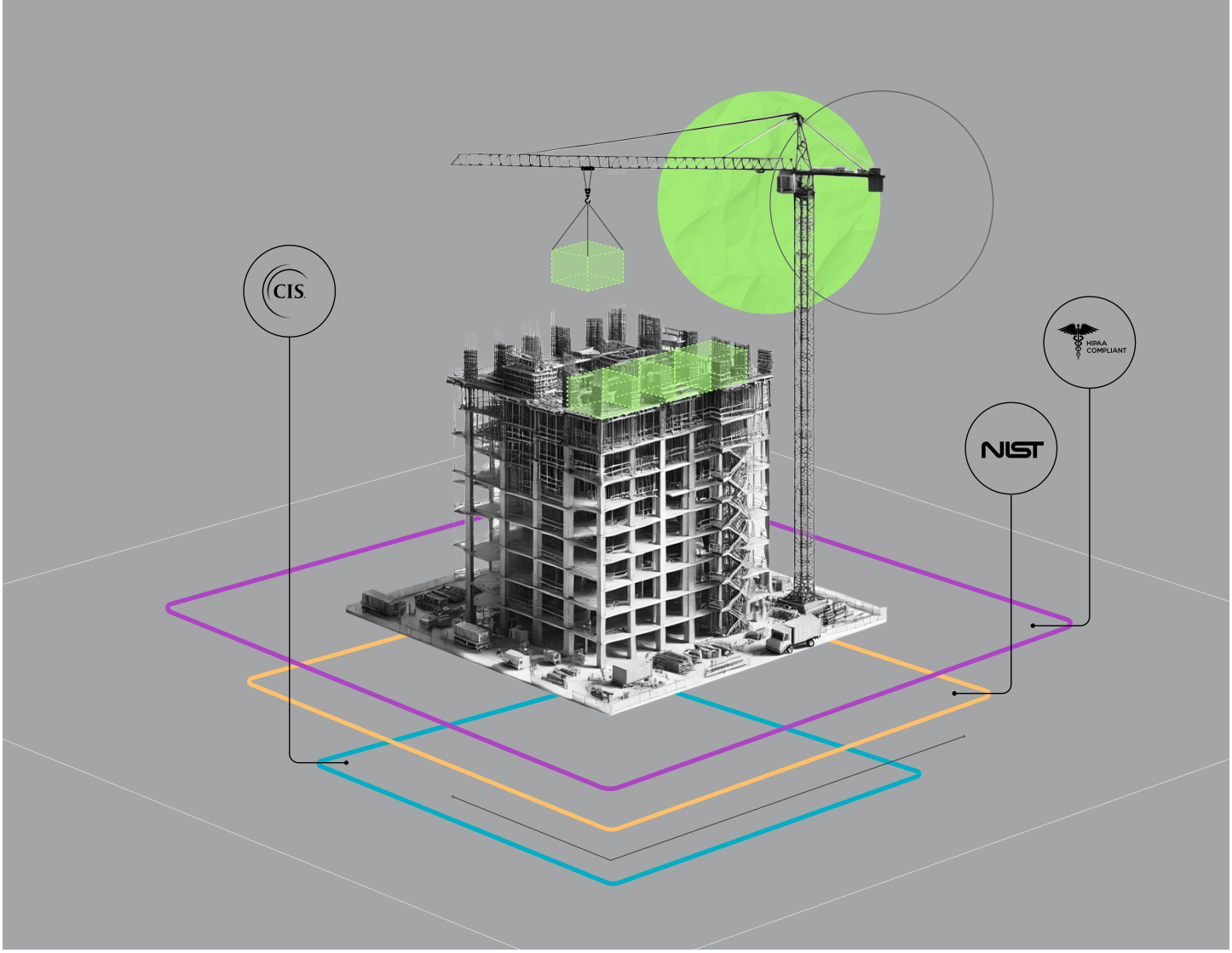
Some of the most creative and unique plug-ins created by Falco users include one for **Salesforce** runtime threat detection and audit logging, one for **Keycloak** user and admin identity access management events, and one for **Box** threat detection and audit logging.

Falco Talon downloads in 2024



The most popular Falco plug-ins by downloads





Security starts with foundational compliance

Every organization desires a strong foundation in security and compliance. While well-known regulations like the Health Insurance Portability and Accountability Act (HIPAA) and Digital Operational Resilience Act (DORA) have security requirements, the specificity of their security controls is not sufficient enough to provide the assurance that companies require for their cloud services and IT infrastructure. Like assembling an engine, where every component is crucial to its function, every individual part of a cloud environment must be configured properly and securely to function as needed. When managing a cloud environment, a strong policy-based configuration at the foundation makes compliance with regulations easier.

When assessing compliance postures, we found that of over 80 compliance policies, many organizations prioritize compliance with foundational security benchmarks. These benchmarks offer the most granular compliance policies at the Kubernetes network and server levels. Successful compliance at such levels allows practitioners to build broader, strategic compliance policies on top of secure foundations to then adhere to other guiding regulations. The implementation of these policies, as users have effectively shown, provides a solid security foundation to facilitate compliance with broader security regulations, standards, and frameworks.

The Center for Internet Security (CIS) Benchmarks and the United States Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs) provide prescriptive assessments of security best practices for specific operating systems, applications, devices, and microservices. The CIS benchmarks and DISA STIGs prioritized by organizations, as shown in the table below, averaged a 93% compliance score. It is possible, however, that the scores shown below are skewed and lower than they are in actuality given the non-applicability of some aspects of a benchmark to an organization's environment.

CIS Distribution Independent Linux Benchmark (Level 1 – Workstation)	100.00%
CIS Kubernetes V1.15 Benchmark	100.00%
DISA Kubernetes STIG Category II (Medium)	98.72%
DISA Kubernetes STIG Category I (High)	97.16%
DISA Kubernetes STIG	96.33%
CIS Distribution Independent Linux Benchmark (Level 2 – Workstation)	94.37%
CIS Kubernetes V1.23 Benchmark	90.14%
DISA Docker Enterprise 2.x Linux/Unix STIG	88.34%
CIS Kubernetes V1.26 Benchmark	81.81%
CIS Kubernetes V1.24 Benchmark	81.35%

CIS and DISA each have security benchmarks tailored specifically for securing Kubernetes clusters, plainly addressing the unique challenges of container orchestration. These are ideal for practitioners who manage and maintain Kubernetes environments, making them pragmatic for day-to-day security.

CIS Kubernetes benchmarks offer some of the most granular security benchmarks at a technical level, designed to mitigate risks inherent in containerized environments. CIS offers specific security benchmarks for cloud providers, server software, operating systems, desktop software, and more. DISA Kubernetes STIGs are ideal for highly regulated or high-security environments given their government-grade defense-specific guidance for operating systems, endpoints, applications, cloud computing, and more. Broader frameworks such as the Network and Information Security Directive (NIS2) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) are high-level and principled-based. They are incredibly valuable for addressing general cybersecurity strategies and providing overarching governance, but do not address the granular requirements for container security and mitigating specific threat vectors.

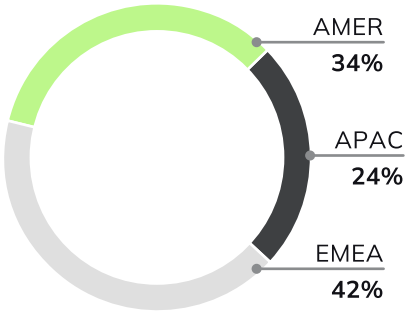
> We use DISA STIGs to guide the security practices of our Kubernetes cloud environment because they are comprehensive, frequently updated, and foundational for the broader compliance policies we need to adhere to like NIST 800-53.
>
> - Senior Infrastructure Security Engineer, Healthcare IT Organization

We've found that organizations benefit from prioritizing security at the container level initially to then complement the mandated strategic security processes such as those described in regulatory benchmarks. This makes sense considering that highly technical users and those maintaining security compliance are practitioners who can likely translate their Kubernetes security posture to a bigger picture.

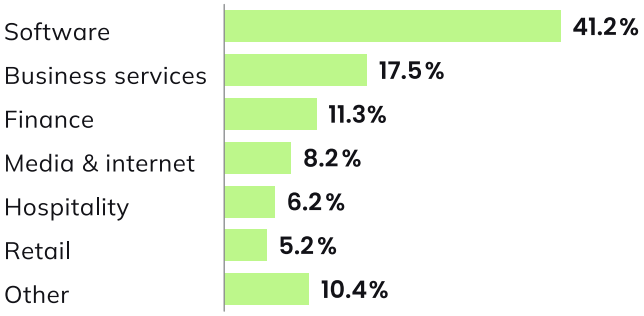
Additionally, we see that organizations operating in the European Union (EU) must comply with some of the strictest international data, privacy, and cybersecurity regulations in the world. This may explain why EU-based organizations appear to have a larger adoption of compliance policies in our data analysis. For example, we sampled the statistics for the CIS benchmarks for each major CSP, and the results below show that organizations in Europe, the Middle East and Africa (EMEA) tend to enable these policies more than other regions. This held true for a majority of other policies as well.

CIS AWS

Location

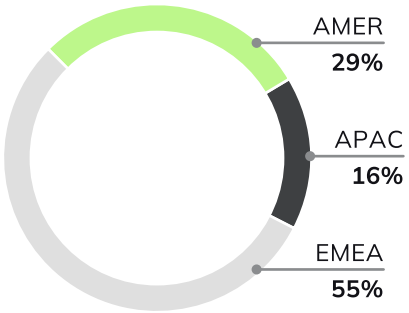


Industry

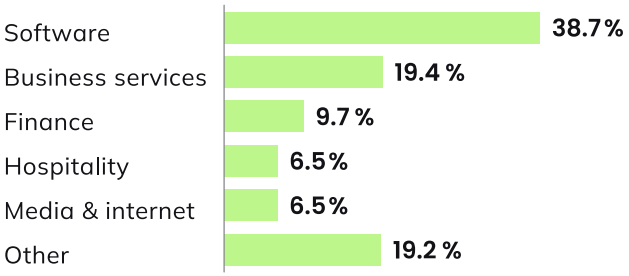


CIS GCP

Location

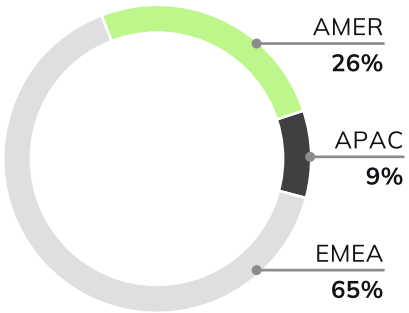


Industry

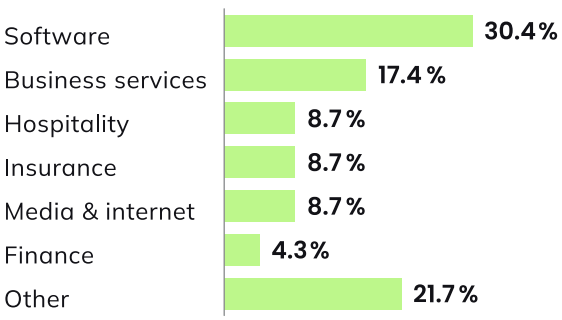


CIS Azure

Location



Industry



Methodology

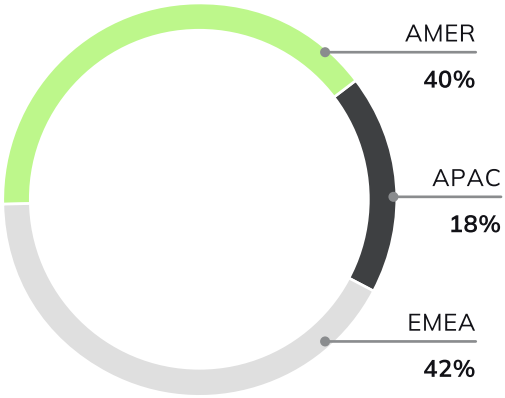
The data in this report is derived from the careful and methodical analysis of millions of cloud accounts and Kubernetes containers that Sysdig customers run and secure daily. We also used Scarf, a platform for open source project usage analysis that facilitates data gathering and correlation. Our representative sample spans a wide range of cloud-savvy industries across the globe.

The organizations studied vary in size and security maturity, from early-stage startups to well-established multinational enterprises.

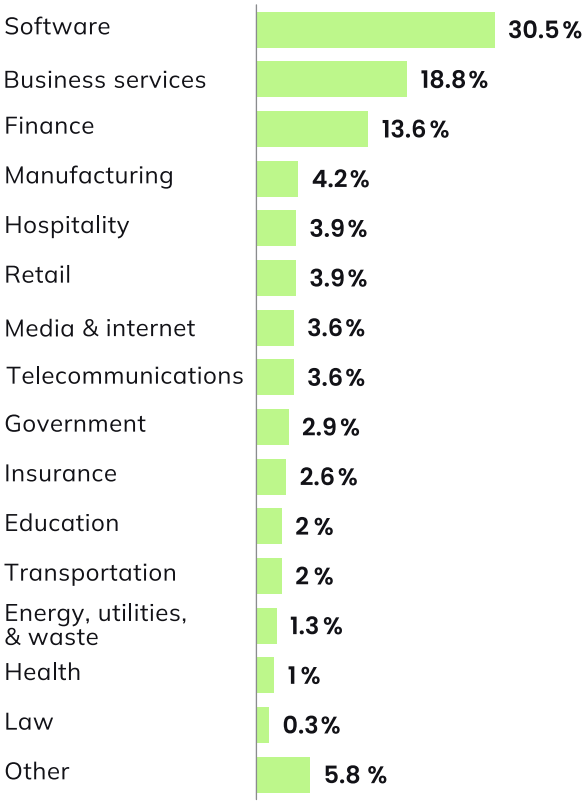
Sysdig, with open source roots in Wireshark, Falco, and recently Stratoshark, is passionate about information sharing and real-world data. The concepts and analyses in this report are a culmination of insights from engineers, product managers, threat researchers, marketers, and executives whose perspectives span the organization — providing you with the actual changing aspects of cloud, container, and security trends.

Where does our data come from?

Location



Industry



Conclusion

From the startling speed of cloud attacks to the widespread reliance on open source tools like Falco, the “Sysdig 2025 Cloud-Native Security and Usage Report” provides an invaluable snapshot of the ever-evolving cloud security and container usage landscape. The real-world data used to derive the report’s findings highlights the challenges and opportunities in modern cloud environments for the year to come. This year’s analysis also underscores meaningful progress in vulnerability management and AI workload security while revealing a staggering imbalance between service and user accounts, regardless of how risky they may be.

As organizations look to adapt and continue to thrive over the next 12 months, this report serves as both a benchmark and a roadmap for navigating the complexities of the cloud-native world. To that end, open source software has truly cemented itself as a cornerstone of cloud security, bridging the gap between enterprises and small businesses alike. Until next year, keep up the good work and secure every second of your cloud journey!

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 →

RP-011 REV. A 03/25