



# SECURE EVERY SECOND.

Cloud security powered by runtime insights.

For businesses innovating in the cloud, every second counts. Development teams must shorten time to market, while security teams must protect the business without slowing it down.

However, operating in the cloud is different — from the infrastructure to the organizational dependencies to the very anatomy of modern applications. Attackers exploit the complexity and automation of the cloud to move laterally, elevate privileges, and maximize blast radiuses.

To outpace attackers, security teams need to detect, triage, and respond to threats in real time. Disparate point solutions are insufficient and create silos. Operating in the cloud **requires a different approach to security** — one that tells the whole story of what is happening across interconnected environments.

At Sysdig, we've built a unique cloud security platform that combines **runtime** insights, **real-time** detection, and **AI** to secure innovation at cloud speed. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

**10 MINUTES is all it takes to execute a cloud attack.**

## Why Sysdig



### Get Complete Visibility

Eliminate visibility gaps created by disparate solutions. Sysdig provides a unified view of risk across your entire cloud estate and the context needed to take action.



### Eliminate 95% of the Noise

Identifying your top risks shouldn't require scouring through a mountain of alerts. Sysdig leverages the knowledge of what's in use to prioritize what you need to focus on.



### Detect Threats Within Two Seconds

Sysdig accelerates threat detection and response in real time with end-to-end coverage and correlation across workloads, identities, cloud services, and third-party applications.

## Secure Cloud Innovation

Innovation is in our DNA. We created Falco, the open source solution for real-time cloud threat detection. Falco has over 100 million downloads, and today, it is the engine that enables the Sysdig platform to deliver runtime insights.

## The Sysdig Platform

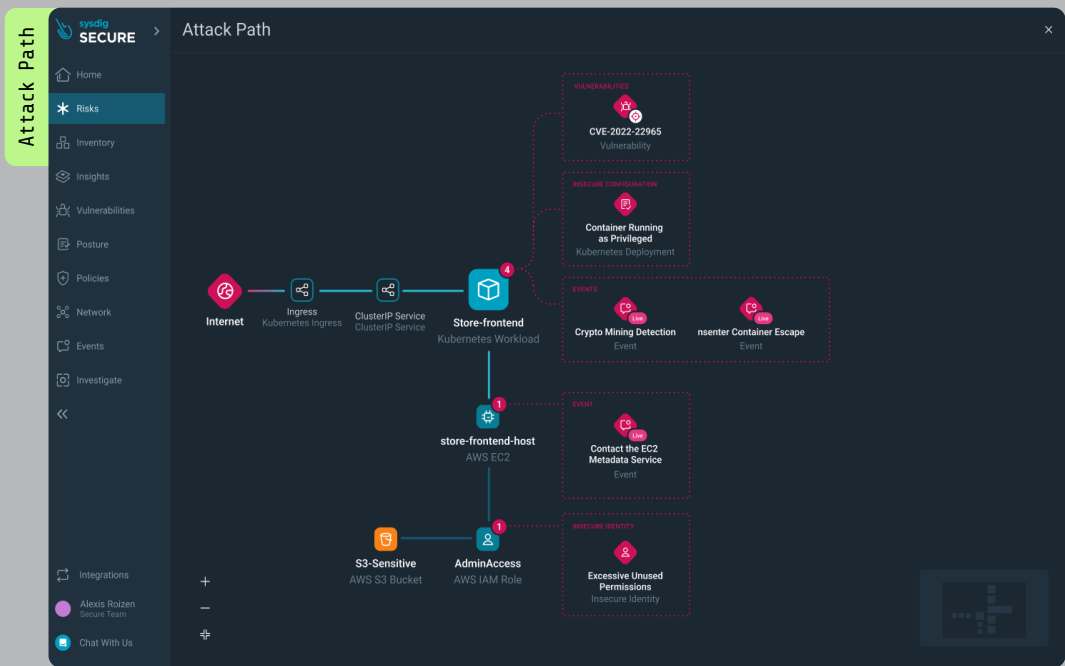
Sysdig is the only cloud-native application protection platform (CNAPP) that truly provides the visibility, coverage, and context required to **secure every second** of innovation. Our Cloud Attack Graph acts as the neural center of the Sysdig platform, delivering:

- **Real-time threat detection**  
Stop attackers in their tracks. Get end-to-end coverage that expands your defense surface.
- **Multi-domain correlation**  
Uncover the top risks. Get the context needed to identify risky combinations of assets, users, and risks across cloud environments.
- **In-Use Prioritization**  
Know which risks need your attention. Get a stack-ranked view of risks based on what's in use.
- **Advanced GenAI**  
Get advanced recommendations to prioritize and mitigate attacks smarter and faster. Sysdig Sage uncovers risks and attack paths.

## Powered by Runtime Insights

Innovation is in our DNA. We created Falco, the open source solution for real-time cloud threat detection. Falco has over 100 million downloads, and today, it is the engine that enables the Sysdig platform to deliver runtime insights.





**Inventory**

Showing 50 of 120 resources found.

CVSS	Vulnerability	Package / Path	In Use	Package Type	CVE Context
9.8	CVE-2022-291625	libcrypto1.0 - 1.0.2h-r0	Yes	JavaScript	🔍 📄 🔄
9.8	CVE-2021-44228	openssl-client - 1.7.9p1-10+deb10u2	Yes	JavaScript	🔍 📄 🔄
9.8	CVE-2022-29162	...apache.tomcat.tomcat-dbp - 8.5.5	Yes	Golang	🔍 📄 🔄
9.8	CVE-2022-2916	libcrypto1.0 - 1.0.2h-r0	Yes	JavaScript	🔍 📄 🔄
9.8	CVE-2022-3410	libcrypto1.0 - 1.0.2h-r0	Yes	JavaScript	🔍 📄 🔄
9.1	CVE-2022-3729	...e.tomcat.tomcat-dbp - 8.5.5	Yes	Golang	🔍 📄 🔄
7.8	CVE-2021-2912	busybox - 1.24.2-r8	Yes	JavaScript	🔍 📄 🔄
7.8	CVE-2021-3256	...ython2.7-minimal - 2.7.16-2+deb10u1	Yes	JavaScript	🔍 📄 🔄
7.8	CVE-2022-3256	python2.7 - 2.7.16-2+deb10u1	Yes	JavaScript	🔍 📄 🔄
7.8	CVE-2022-3256	libpython2.7-stdlib - 2.7.16-2+deb10u1	Yes	JavaScript	🔍 📄 🔄

## Key Features

- Real-Time Detections, not Snapshots**  
 Intermittent snapshots create blindspots that attackers can exploit. Real-time detections provide visibility into multi-domain cloud activity across data sources, leaving attackers nowhere to hide.
- End-to-End Threat Detection**  
 Sysdig combines drift control, machine learning, and Falco detections to deliver comprehensive coverage across workloads, identities, cloud services, and third-party applications.
- Attack Path Analysis**  
 Visualize risks and uncover ways attackers can move laterally across your environment to exploit different resources. Take immediate action to remediate risks and prevent attacks.
- Risk Prioritization**  
 Runtime visibility delivers valuable information that automatically flags risk exposure. Sysdig provides prioritization and recommendations based on what's in use.
- Agentless and Agent-Based Scanning**  
 Combine the best of agent-based and agentless scanning to cover the entire lifecycle, gaining speed, flexibility, and real-time visibility.
- Sysdig Sage**  
 Stop attacks faster with GenAI that employs multi-domain correlation and multistep reasoning to unify cloud asset inventory, vulnerability prioritization, and compliance risk assessment.



### Cloud Detection and Response

- End-to-end coverage across containers, Linux and Windows servers, cloud logs, and serverless.
- Multiple defense layers using drift control, machine learning, and Falco detections.
- Accelerate investigation and response with rich context and metadata.



### Cloud Security Posture Management

- Correlate assets with activity and visualize attack paths and exploitable links across resources.
- Search compromised resources and quickly check for high-severity risks.
- Surface top risks, combining context from runtime insights with static assessments.



### Vulnerability Management

- Reduce vulnerability noise with in-use prioritization.
- Deploy and scan in seconds with a consolidated agent-based and agentless approach.
- Secure your CI/CD pipeline from source to run.



### Container and Kubernetes Security

- Get real-time threat detection with out-of-the-box managed policies based on Falco and machine learning.
- Integrate image scanning into CI/CD pipelines and runtime.
- Surface broader cloud context surrounding container and Kubernetes threats.



"I want to immediately know when someone's in my environment – not 15 minutes or several hours later. With Sysdig, we can identify and address potential threats in real time."  
Senior Infrastructure Security Engineer, BigCommerce



"With Sysdig, we consolidated six tools down to one, saving money and time."  
IT Security Manager, Arkose Labs



"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

#### Open Standards Commitment



And More...

#### Trusted Globally



#### 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. Sysdig correlates 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.**