# Combat Active Cloud Risks with **Runtime Insights**

Cloud Security Posture Management (CSPM) requirements have shifted as cloud adoption has accelerated. The first wave of cloud adoption required periodic posture assessments to ensure compliance and provide visibility into cloud assets. Today, that is not enough. With more cloud workloads moving to production and attackers exploiting the speed of cloud automation to launch attacks within minutes, you need a CSPM solution that shifts from periodic point-in-time assessments to continuous posture assessments to identify, prioritize, and mitigate active cloud risks and prevent attacks from spreading.

> “We also like that Sysdig uses knowledge of what is in use during production to help us make better-informed posture decisions. It can help filter out 80% or more of the noise. The bottom line is, CSPM is Sysdig’s bread and butter, and that inspires confidence.”
>
> Senior Infrastructure Security Engineer
>
> BIGCOMMERCE

### Get Full Visibility Across Your Cloud Estate

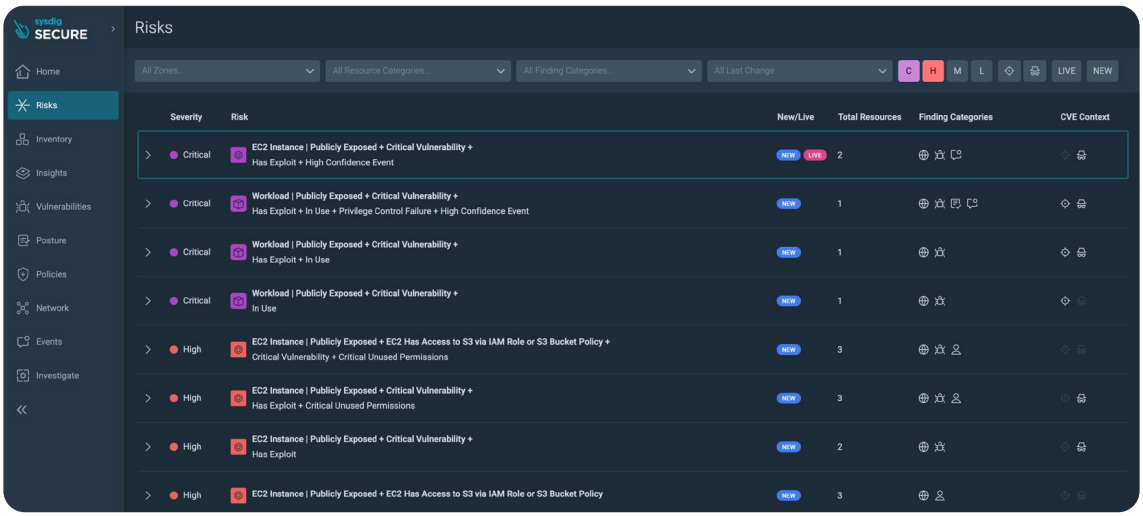
Get full inventory and assess risk and compliance for all cloud assets including IaaS, PaaS, hosts, containers, vulnerabilities, identities, and more. Search and filter assets based on both static (e.g. public exposure, permissions) and dynamic risk factors (e.g. in-use packages).

### Prioritize Active Cloud Risks and Uncover Unknowns

Eliminate alert fatigue and noise by up to 95%.  Prioritize top risks that are exploitable and actively running like in-use software packages with critical vulnerabilities. Connect the dots and uncover hidden attack paths that are enriched with in-use packages and live events.

### Shift to Continuous Assessment

Cut your visibility window from hours or minutes down to seconds. Sysdig Runtime Insights helps you continuously assess your cloud environment for real-time posture drift, configuration changes, and live events that can expose new risks or an imminent attack.




# Why Sysdig

## Active Cloud Risks Requires Runtime

### Runtime Insights

Gain visibility into real-time configuration changes and in-use assets at runtime to help you prioritize the most critical risks. Continuously assess your security posture with no visibility gaps.

### Best of Agentless and Agents

Simplify scanning, setup, and maintenance with agentless. Get near continuous assessment with agentless cloud logs. Gain deep insights and runtime visibility with a lightweight agent.

### Extensible CNAPP Platform

Prevent attacks faster by extending posture assessment with real-time detection and response. Consolidate multiple tools onto a single platform to cut costs and improve security operations.

## Use Cases

- → Cloud Security Posture Management
- → Kubernetes Security Posture Management
- → Cloud Identity and Entitlement Management
- → Inventory and Asset Tracking
- → Vulnerability Management
- → Compliance

## Key Capabilities

- **Agentless Scanning** for cloud assets, configurations, permissions, vulnerabilities, and more.
- **Agentless Detection** of near real-time events and configuration changes using cloud logs.
- **Agent-based Detection** prevents mistakes from cascading and attacks from spreading.
- **Runtime Enrichment** identifies in-use assets and packages to prioritize risks and reduce noise.
- **Multidomain Correlation** uncovers the riskiest combinations across various assets and users.
- **Inventory Search** finds and filters assets across multiple clouds and platforms in a few clicks.
- **Attack Path Analysis** visualizes interconnected risks and exploitable links across resources.
- **Vulnerability Prioritization** of in-use packages with critical and exploitable vulnerabilities.
- **Remediation at Source** with automated Infrastructure as Code (IaC) template changes.
- **Out-of-the-box Policies** for 60+ common frameworks (GDPR, SOC2, HIPAA, NIST, and more).

sysdig SECURE EVERY SECOND.



www.sysdig.com

REQUEST DEMO →