Cloud Security Powered by Runtime Insights

Sysdig provides real-time cloud-native security for Fargate, EKS, and ECS at scale, to help customers migrate or modernize their container and cloud workloads on AWS. Powered by Runtime Insights, Sysdig's Cloud Native Application Protection Platform (CNAPP) stops threats in real time, reduces vulnerabilities by up to 95%, and helps you prioritize and remediate security posture risks.

Sysdig Use Cases for AWS

Challenges	I need to...	Services	Key Features and Benefits
72% of containers live less than five minutes*	Secure serverless containers	AWS Fargate	Sysdig automates image scanning as an accessible registry for AWS Fargate. It gives deep, real-time visibility to confidently run serverless container workloads on AWS Fargate.
99% of breaches start with cloud misconfigurations**	Detect and respond to cloud threats	AWS Cloudtrail Any AWS services with AWS Cloudtrail logs	Sysdig's Runtime Insights monitors active tasks, in use packages and configurations to detect threats across running containers, hosts, clusters, and cloud services. With open source Falco rules, it can identify suspicious activity across AWS infrastructure.
87% of container images have high or critical vulnerabilities*	Manage container and cloud vulnerabilities	Amazon ECS Amazon EKS Amazon ECR AWS CodeBuild AWS CodePipeline Multiple AWS services	Sysdig profiles running containers to identify in-use vulnerable packages that create a risk in production. It reduces 60-95% of noise by prioritizing vulnerabilities tied to active packages based on this runtime context and risk. Further, it automates image scanning in CI/CD pipelines and Amazon ECR within your AWS environment.
41% cite compliance as top 3 barriers vis-a-vis cloud outcomes***	Manage cloud and container compliance	Across the entire AWS stack	Sysdig's real-time drift detection complements static posture management to minimize visibility gaps. Information about differences in configuration between the in-use resource vs its intended configuration is used to generate suggested fixes and pull requests. Sysdig scans IaC files pre-deployment and maps misconfigs in production back to the source. It automates AWS cloud and container compliance for PCI, NIST, SOC2, FedRAMP, and more.
Over 90% of cloud permissions never get used*	Manage Permissions and Entitlements	Amazon S3 AWS IAM Across the entire AWS stack	With Sysdig, its easy to get visibility into cloud identities, manage permissions, and identify inactive users and identities with excessive permissions. It optimizes access policies to grant just enough privileges and helps restrict permissions to those truly in-use.
59% Containers are instantiated with no CPU limits and 49% with no memory limits*	Maximize performance and reduce costs	Amazon EKS Kubernetes	Sysdig identifies areas in your Kubernetes environments to optimize where there is room to add more pods or move workloads to smaller instances to reduce costs. It helps you predict costs and savings estimates for Kubernetes.

*Sysdig 2023 Cloud-Native Security and Usage report **Gartner 2021 Hype Cycle for Cloud Security ***Accenture The race to cloud