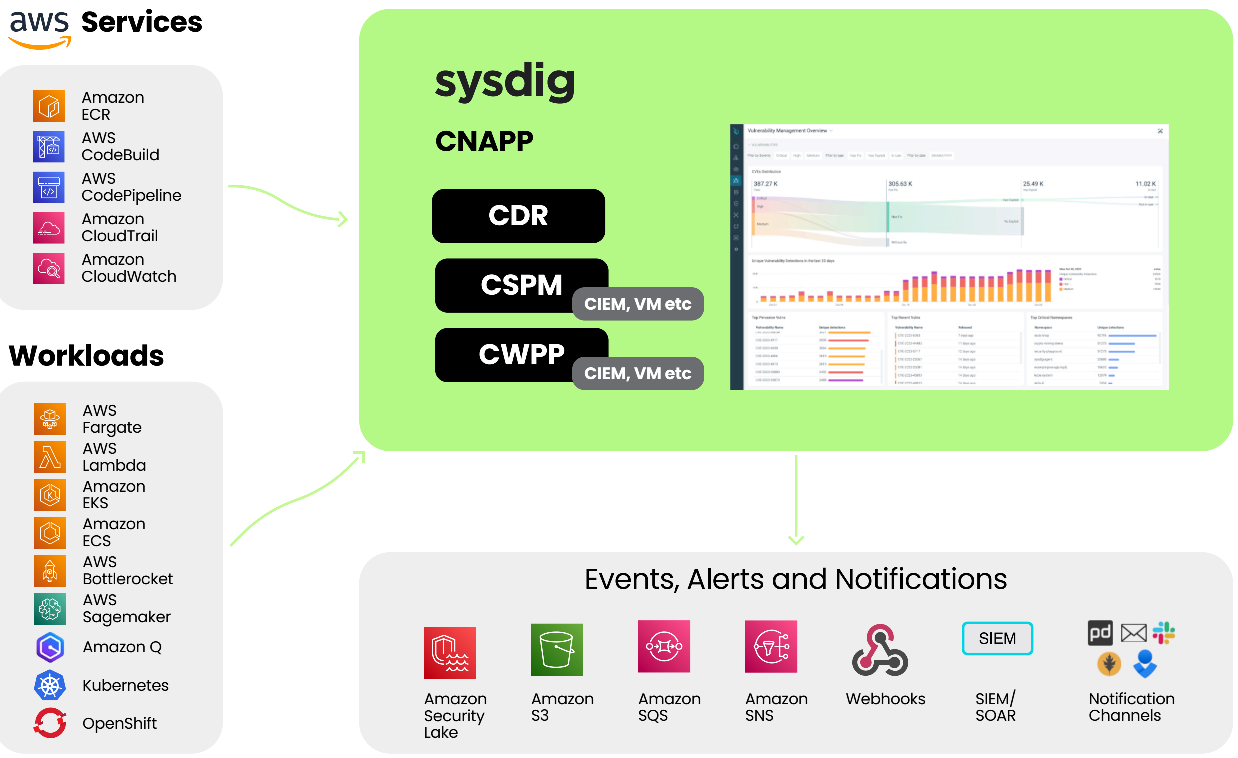
BRIEF

Sysdig for Amazon Web Services

Sysdig's CNAPP protects AWS, hardening security posture and detecting attacks immediately.

LEARN MORE →

10 minutes is all it takes to execute an attack in the cloud after discovering an exploitable target. Outpacing attackers in the cloud requires security teams to meet the 5/5/5 Benchmark. That means five seconds to detect, five minutes to triage, and five minutes to respond to threats. Sysdig's Cloud Native Application Protection Platform (CNAPP) helps AWS customers meet this benchmark's expectations, thus securing and accelerating their cloud innovation.



aws Services

- Amazon ECR
- AWS CodeBuild
- AWS CodePipeline
- Amazon CloudTrail
- Amazon CloudWatch

Workloads

- AWS Fargate
- AWS Lambda
- Amazon EKS
- Amazon ECS
- AWS Bottlerocket
- AWS Sagemaker
- Amazon Q
- Kubernetes
- OpenShift

sysdig

CNAPP

- CDR
- CSPM (CIEM, VM etc)
- CWPP (CIEM, VM etc)

Events, Alerts and Notifications

- Amazon Security Lake
- Amazon S3
- Amazon SQS
- Amazon SNS
- Webhooks
- SIEM/ SOAR
- Notification Channels

Customer Highlights

worldpay from FIS, FINRA, Goldman Sachs, bloomreach, IBM

Arkose Labs, COMCAST, BIGCOMMERCE, Alaska AIRLINES, Calendly

Key Benefits

Cloud Detection & Response
Detect, investigate & stop attacks faster

Vulnerability Management
Reduce vulnerabilities by up to 95%

Posture Management
Instantly detect risk changes in cloud environments

Permissions And Entitlements
Gain visibility into cloud identities

Uncover Active AI Risk
Automatically identify popular engines such as AWS SageMaker, Amazon Q, and AWS Bedrock

Ben Visa Vale, Santander Group operates in the financial services industry and is bound by strict security regulations, such as PCI-DSS. After integrating Sysdig into its CI/CD pipeline for vulnerability management, its security team no longer has to engage in a back-and-forth with developers to explain issues or remediation requests. Sysdig automatically creates and assigns Jira tickets when it detects vulnerabilities. There is an estimated reduction in time to remediation by at least 60%. In the future, the team will connect Sysdig's Cloud threat detection to its security information and event management (SIEM) solution. Read more →

Arkose Labs works with some of the most recognizable consumer brands in the world. A key to scaling its security strategy has been giving developers the tools and insights they need to prioritize where to focus time and effort to address security issues. With Sysdig, the Arkose Labs teams are easily able to get a good view of cloud risks and security posture, as well as report quickly on the entire pipeline's dependencies. Arkose Labs is equipped to act fast and reassure customers that its supply chain is not at risk when new threats emerge, such as Log4j. Learn more →

TRUSTED AT CLOUD SCALE

- 1B events scanned daily
- 7M containers analyzed daily
- 5/5 G2 and Gartner Peer Insights
- 700+ valued customers
- 60M+ Falco downloads

KEY AWS INTEGRATIONS

AWS Fargate
Amazon EKS
Amazon ECS
Amazon ECR
AWS CloudTrail
AWS Lambda
Amazon SNS
AWS Bottlerocket
Amazon Cloudwatch
AWS Outposts
AWS Codebuild

aws
PARTNER

- DevOps Software Competency
- Security Software Competency
- Containers Software Competency
- Cloud Operations Software Competency

sysdig

PB-009 REV. J 6/24

Secure Every Second.

See Sysdig in action

REQUEST DEMO →

Contact sales

SALES@SYSDIG.COM →