Secure AWS Fargate Workloads with Sysdig Secure for AWS

Accelerate secure innovation with serverless compute for containers

Containers continue to grow in popularity, providing an agile and efficient approach for developing and deploying applications for organizations. But scaling containers securely in a serverless environment can present challenges to enterprise organizations. Abstraction layers can obstruct visibility, which can make it harder to spot vulnerabilities and threats, identify misconfigurations, and detect abnormal activity.

For those running AWS Fargate containers, Amazon Web Services (AWS) is responsible for the security OF the cloud. But you are responsible for the security of what's running IN AWS. How can your organization better meet those security needs?

Sysdig, an AWS Security Competency Partner, has deep expertise in container security and can help minimize risk across cloud services and containers running on AWS.

Up to 15% of enterprise applications will run in a container environment by 2024

→

72% of containers live less than five minutes, complicating security, monitoring, and compliance

→

Secure Your Environment and Optimize Costs with Sysdig

With deep visibility into cloud-native workloads, Sysdig simplifies observability, helping AWS customers monitor performance, rapidly troubleshoot issues, and manage cloud costs.

Optimize the performance and availability of AWS Fargate containers with comprehensive monitoring

Quickly identify and resolve issues with detailed dashboards, alerts, and a prioritized list of remediation recommendations.

Analyze resource utilization to improve capacity management planning, optimize cloud usage, and reduce costs.

aws PARTNER

Secure AWS Fargate Containers at Runtime and Across their Lifecycle with Sysdig Secure for AWS

AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without managing servers. AWS Fargate is compatible with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).

Powered by runtime insights, Sysdig Secure provides deep visibility to more easily detect threats, block attacks, and speed incident response for serverless containers. Flexible serverless security policies help AWS Fargate users safeguard applications and data and meet compliance.

With Sysdig Secure, you can:

Identify suspicious activity across serverless workloads with threat detection based on open-source Falco.

Perform File Integrity Monitoring (FIM) and capture detailed activity audit trails.

Automate AWS Fargate image scanning in your AWS environment and block vulnerabilities from reaching production.

Conduct incident response and forensics even after AWS Fargate tasks have stopped.

Sysdig and AWS Fargate in Action

A large US digital payments firm operating an AWS Fargate environment with over 800 serverless tasks was able to use Sysdig and AWS Fargate to:

- Reduce risk to data and applications
- Detect and respond faster to container threats
- Free up developers to focus on developing code and core tasks

Take the Next Step!

Learn more about the Sysdig integration with AWS Fargate, find Sysdig solutions in AWS Marketplace, or get started with a free trial.

TRY FOR FREE

sysdig