Monitoring AWS Fargate to Minimize Active Security Threats

AWS Fargate abstracts away the infrastructure that containers run on, but creates challenges for traditional security techniques. As infrastructure becomes more short-lived, it's vital to know ASAP about suspicious access to containers, or if there are behaviors which may indicate an active threat. Use of Fargate alone does not eliminate all security concerns.

Deep Visibility

While AWS provides a robust set of native access controls, if you need to deeply audit all activity within running Fargate tasks, you'll need more visibility into workloads. F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, augments existing Fargate security controls by adding runtime observability at the application, process, and network levels.

As a partner in both the Security and Containers competencies, Distributed Cloud AIP is designed from the ground up for cloud security, and is production-proven since 2014 to help customers scale securely. We've applied this experience to introduce container security monitoring for AWS Fargate, which comes as part of the Distributed Cloud AIP solution.

This paper aims to outline our approach to monitoring Fargate environments, describes general use-cases, and reviews available deployment options.

Full Stack Visibility, Even for Fargate

Fargate shifts the AWS shared responsibility model, but there's still interplay between layers that you need to account for from a security standpoint. Distributed Cloud AIP secures multiple layers at runtime by monitoring four key aspects:

1. Process activity inside Fargate containers
2. Network flow data within, and external to, Fargate tasks

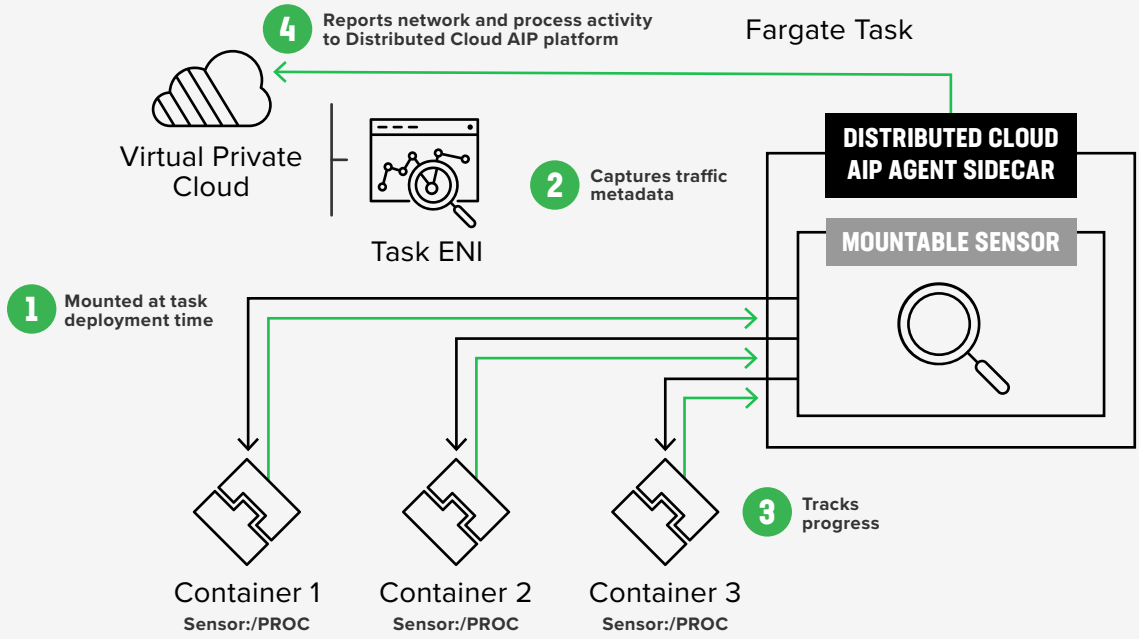
3. Application code running on top of Fargate

4. AWS CloudTrail logs alongside Fargate

Distributed Cloud AIP gives you the visibility you need as risky behaviors traverse these layers. Our application security monitoring protects Node.js, Python, and Ruby code that Fargate supports. Distributed Cloud AIP's AWS integration allows you to easily customize alerts for specific behaviors observed within Fargate-related CloudTrail events, such as Amazon ECS, Amazon VPC, and AWS IAM. And with a monitoring agent specifically built for Fargate, our solution provides network flow monitoring and process tracking within Fargate tasks running on ECS.

Fargate Agent Instrumentation

Our Fargate Agent uses the sidecar design pattern that's familiar to containerized microservices architectures. The Agent receives its own vCPU and memory and does not compete for the same resources as monitored workloads. This ensures predictable performance as it monitors network and process activity within tasks.



Netflow Monitoring

For the network monitoring component, the Distributed Cloud AIP Fargate Agent captures traffic metadata off of the task's shared ENI. The Agent observes all packets and will track unique TCP netflows until completion or timeout. Since it runs as a sidecar within the task itself,

DISTRIBUTED CLOUD AIP PROVIDES DEFAULT DETECTIONS FOR FARGATE, INCLUDING:

- Interactive Sessions
- SSHD Binaries
- Data Exfiltration Attempts
- Unexpected Network Connections

Distributed Cloud AIP can also surface intra-task traffic between individual containers, capturing metadata that does not appear in VPC flow logs. The Agent packages this data and ships it off to the Distributed Cloud AIP platform for alerting, search indexing, and downstream analytics.

Process Monitoring

For the process monitoring piece, the Agent hosts a binary that is mounted into the tasks's containers at deploy time. As containers run, it scans the /proc folder and communicates this metadata back to the Agent to track process activity. And since the binary mounts dynamically as part of the task provisioning process, you won't need to rebuild existing containers in your image repository.

Security Monitoring Use Cases

Distributed Cloud AIP's approach to full-stack security observability into AWS Fargate allows customers to address the following monitoring use-cases:

Are Containers Making Unexpected Network Connections?

For the network monitoring component, the Distributed Cloud AIP Fargate Agent captures traffic metadata off of the task's shared ENI. The Agent observes all packets and will track unique TCP netflows until completion or timeout. Since it runs as a sidecar within the task itself, Distributed Cloud AIP can also surface intra-task traffic between individual containers, capturing metadata that does not appear in VPC flow logs. The Agent packages this data and ships it off to the Distributed Cloud AIP platform for alerting, search indexing, and downstream analytics.

Are There Unexpected Processes Running In Fargate Containers?

Know when there are unexpected processes executing within Fargate containers, so you can investigate for signs of risky activity. Since tasks should be immutable and processes are predefined, it's an instant red flag to observe unique new processes in Fargate. Distributed Cloud AIP alerts are easily customizable, enabling customers to extend process-tracking rule logic with their own executable names and computed hashes.

Are There Unexpected Logins To Fargate Containers?

Know when untrusted entities access running containers. There's rarely a good reason for remote logins to a container, making it a serious issue that could signify a bad configuration, a foolish engineer, or the initial stages of an attack. Distributed Cloud AIP provides out-of-the-box detections for SSH activity within Fargate, so you can investigate ASAP.

Deployment

Deploy the Distributed Cloud AIP Fargate Agent by adding it to your Fargate task definitions. The Agent runs as a sidecar container as part of each task instantiation. (We recommend storing Agent deployment keys via AWS Systems Manager Parameter Store.) Monitoring is priced per task.

Distributed Cloud AIP supports monitoring of the Fargate launch type on ECS. Amazon EKS on AWS Fargate is not currently supported. Traditional EC2-backed EKS and ECS deployments are supported, however, through other Distributed Cloud AIP Agent versions, which include options for Kubernetes DaemonSet and Helm chart deployment.

You Can't Secure What You Can't See

With Fargate, AWS assumes more responsibility for infrastructure security, but there's still attack surface to account for. Distributed Cloud AIP's instrumentation is easy to deploy so there are no security blindspots.

Be prepared for your next compliance audit or forensics investigation. See more of your security data with Distributed Cloud AIP.

Threat Stack: Now Part of F5

Threat Stack is now F5 Distributed Cloud App Infrastructure Protection (AIP). If you'd like to learn more about this solution, the company's Security Operations Center (including Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights), and more, feel free to contact our cloud security and compliance experts.

Let our experts take your cloud security worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, visit our website today.