LACEWORK

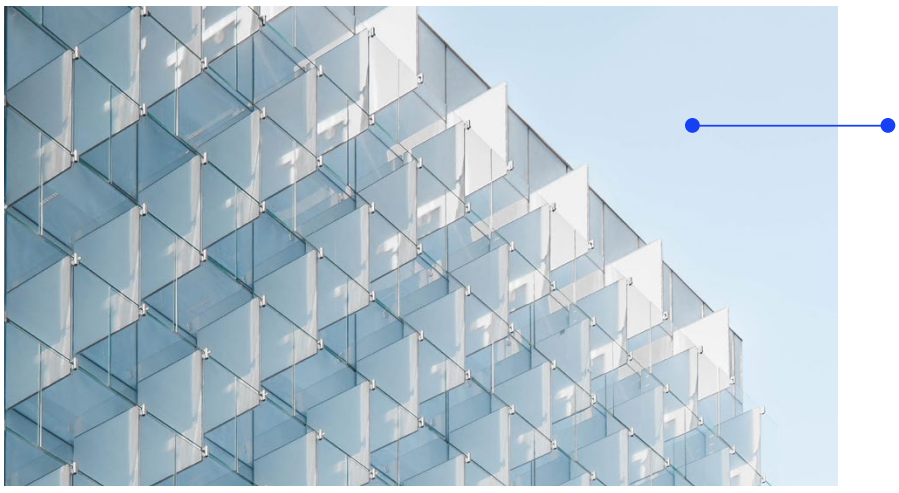
PARTNER INTEGRATION BRIEF

Visibility and security for your AWS Fargate attack surface

AWS Fargate is a container-as-a-service offering from Amazon Web Services (AWS) that helps developers build their applications without having to worry about the infrastructure. It works with Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). It removes the need to manage the servers or clusters of Amazon Elastic Cloud Compute (EC2) so that you only need to worry about the containers, network interfaces between them, and IAM permissions. This is beneficial, but it also creates challenges for traditional security techniques. As infrastructure becomes increasingly complex and short-lived, it's imperative to know as soon as possible about suspicious access to containers, or if there are behaviors present that could indicate an active threat. Use of Fargate in and of itself does not eliminate all security concerns. Together with Lacework, we help you build better.

The Lacework Polygraph® Data Platform

The Polygraph Data Platform delivers comprehensive and continuous end-to-end AWS security and configuration support for both workloads and accounts running in AWS. As more organizations move their critical workloads to the cloud, there is an increasing need for a single, unified solution like our Polygraph Data Platform to identify, analyze, and report on misconfigurations, vulnerabilities, and behavioral anomalies in user and account behavior.



Why Lacework?

Unique container and Kubernetes workload protection features that allow your organization to embed security in your software delivery pipeline from code build to deployment.

Embedded security at multiple stages of your software supply chain that provides multiple redundant and overlapping layers of security.

Rich security context of detection alerts allow developers and security analysts to quickly identify issues; send them to Jira or ServiceNow for triage and resolution.

Security protection through the scanning of images when they are pushed to the Amazon Elastic Container Registry (ECR).

Product features

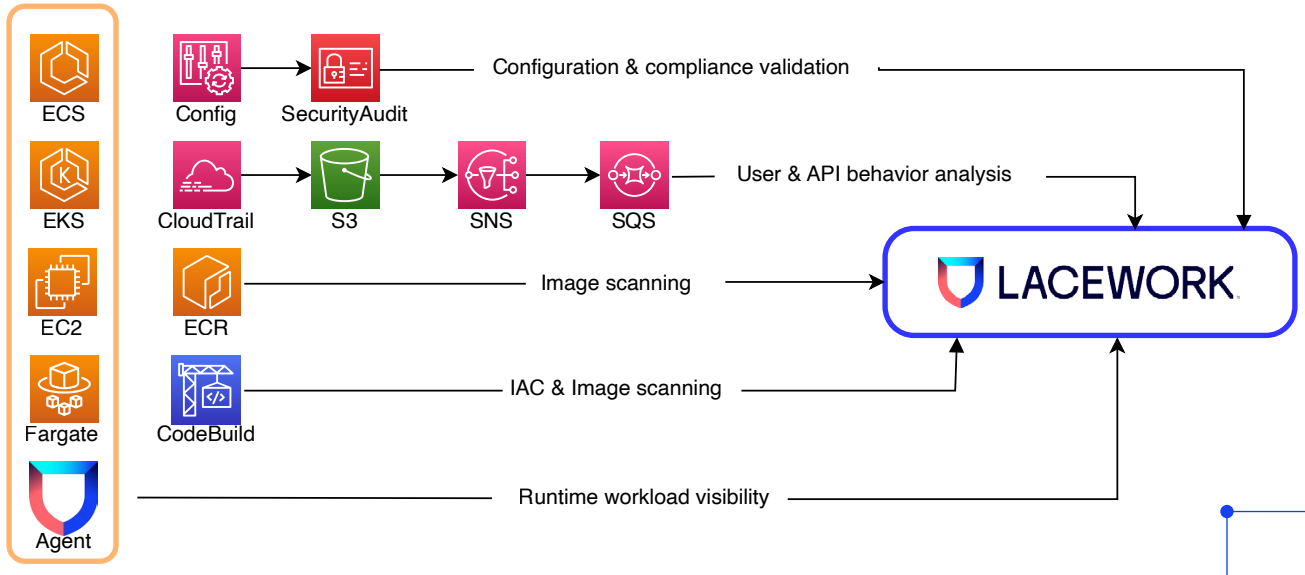
With the Polygraph Data Platform - Fargate integration, you can visualize your applications by providing a clear understanding of communications, launches, and other cloud runtime behaviors. This allows you to:

- Visualize inventory and detect breaches on container-based applications that utilize Fargate serverless compute running on both ECS and EKS
- Understand which containers are running, the applications running within them, and the relationships of those applications to other applications and services
- Eliminate the need to write cumbersome rules to detect threats
- Discover IaC and container vulnerabilities from build time through runtime
- Deploy with flexible models that meet your environment's needs:
  - Secure-base-image / embedded-agent model
  - Sidecar model that utilizes a volume map

How it works

The Polygraph Data Platform provides workload security visibility into all processes and applications within an organization's cloud environments such as workload/runtime analysis, and automated anomaly and threat detection. After you install the Lacework agent, Lacework scans hosts and streams select metadata to the Lacework data warehouse to build a baseline of normal behavior, which is updated hourly. From this, the Platform can provide detailed in-context alerts for anomalous behavior by comparing each hour to the previous one. For example, we alert you to an unknown IP or if a user logs in from an IP that has not been seen before.

Lacework offers two methods for deployment into AWS Fargate. The first method is by embedding the agent directly into secure base images or as part of an automated build process, and the second is a sidecar based approach that utilizes a volume map (defined within the task definition). In both deployment methods, the Lacework agent runs inside the application container.



Differentiators

Lacework helps you achieve the following outcomes:

- **Understand your AWS cloud** by seeing what's deployed by builders, automatically make sense of how and why the cloud changes, and uncover and prioritize risk.
- **Gain expert-level security** by empowering existing staff to find early signs of trouble without extensive querying.
- **Fix what matters earlier** by eliminating noise, removing reliance on static and complex rulesets, and spotting and fixing issues before production.
- **Prove cloud compliance in a fraction of the time** by expediting the most tedious part of meeting compliance.
- **Lower overall total cost of ownership** by concentrating efforts on maintaining one (vs multiple) cloud security solutions and decrease the operational risk from employee turnover.

> "With Lacework, we can see which of our Fargate containers are running, the applications running within them, and the relationship of those applications with other applications and services. We also take advantage of the historical views so we can understand what happened in our Fargate containers, long after they have been deleted."
>
> FRANCOIS DESCHENES
> DIRECTOR OF ENGINEERING TINT, FILESTACK

Get started now.

Solution available in AWS Marketplace.

Contact alliances@lacework.net.

Visit Lacework.com/aws for more details, demo videos, whitepapers, case studies, and customer testimonials.

Lacework is the data-driven cloud security company. The Lacework Polygraph® Data Platform delivers end-to-end visibility and automated insight on risks across multicloud environments, collecting, analyzing, and correlating data. Customers depend on Lacework to drive revenue, bring products to market faster and safer, and consolidate security solutions into a single platform. Get started at www.lacework.com

LACEWORK

 | 888.292.5027 | lacework.com

aws Available in AWS Marketplace

07/22