AWS Security Tools and Threat Stack

Threat Stack has a strong connection to Amazon as a certified AWS Advanced Technology Partner in the Amazon Web Services (AWS) Partner Network (APN) and as an AWS Advanced Partner with a Security and Container Competency. We're deeply integrated into the platform to provide AWS customers with unprecedented visibility, more advanced security capabilities, and a cloud-native user experience.

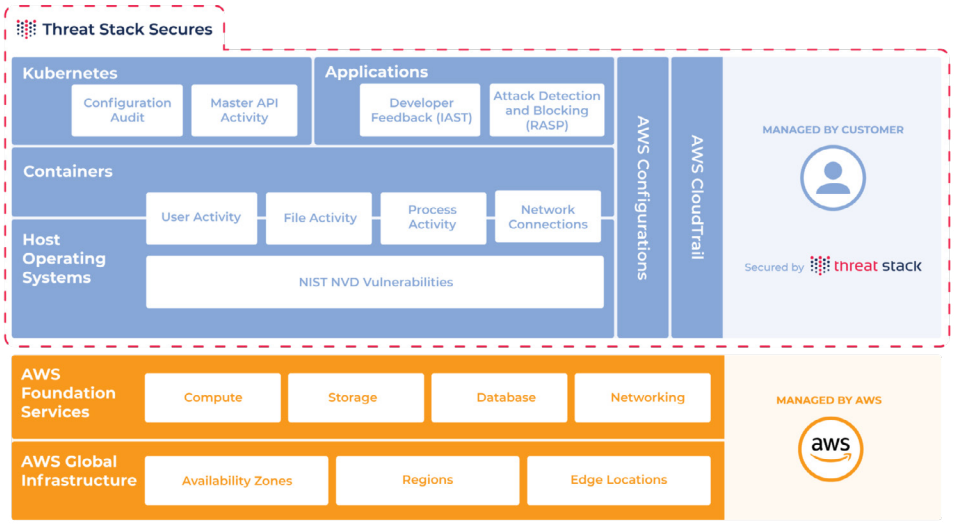
But AWS offers their own long list of security and compliance services, and you may wonder how they all fit together. This document explains how the Threat Stack Cloud Security Platform® complements AWS tools to offer full stack security observability.

threat stack

Deep Visibility Across Running Operating Systems and Containers

The Threat Stack Cloud Security Platform monitors behaviors across your infrastructure and combines this metadata with AWS tags and CloudTrail events to create a context-rich intrusion detection system. Some platform capabilities are similar to certain AWS-native security tools, but the goal is to provide visibility into running systems where the AWS Shared Responsibility Model leaves off.

Threat Stack uses agents to continuously monitor and provide visibility into operating systems across Amazon EC2 instances and Docker containers. The platform layers AWS context on top of this data, but at its core, Threat Stack starts with this base and runs it through a comprehensive and customizable rules engine for alerting. Threat Stack also monitors Kubernetes and Fargate, and provides runtime protection for web applications, microservices, and APIs written in Node.js, Python, and Ruby — allowing you to see your attack surface in its entirety (the same way an attacker would), and to correlate suspicious activity across each layer.



Shared Responsibility Model

CloudWatch

Performance metrics and logs about your AWS resources

Amazon CloudWatch is a general-purpose tool for collecting logs, tracking metrics, creating dashboards & alarms, hooking into microservices performance, and emitting events based on resource state. It is not fundamentally a security tool, although some security information — such as CloudTrail logs or GuardDuty findings — may be included, depending on additional manual configuration.

Many Threat Stack customers use CloudWatch in addition to Threat Stack. CloudWatch provides performance dashboards of their resources, and custom application logs indicate overall system health and insight into their AWS bill. Threat Stack adds runtime security monitoring, forensics investigations, compliance audits, and other specialized infosec use cases.

GuardDuty

Continuous threat detection with a focus on network flow and threat intel

Amazon GuardDuty is a specialized cloud security tool, focused on a different set of metadata than Threat Stack. Since it's an AWS service, GuardDuty can natively access a parallel stream of VPC Flow Logs under the hood. It's important to note this distinction because GuardDuty can efficiently combine network flow logs with CloudTrail data, DNS logs, and threat intel feeds. It then applies machine learning to this mix to identify anomalies.

Many Threat Stack customers also use GuardDuty's intelligent anomaly detection to complement Threat Stack's deep view into EC2 hosts and containers. While Threat Stack does see network activity from the perspective of process-level network connections, GuardDuty's access to VPC Flow Logs paints a fuller picture of network activity, in this specific case.

Security Hub

SIEM functionality for AWS native security tools, plus third-party integrations

AWS Security Hub consolidates data from across the ecosystem of specialized AWS governance and security tools. AWS Config is a requirement for using the service, but Security Hub can also pull data from these Amazon services: GuardDuty, Inspector (scheduled EC2 security assessments), Macie (ML-based PII discovery in S3 object storage), Detective (graph modelling for threat hunting), IAM Access Analyzer, and Firewall Manager.

As a security incident event management tool, Security Hub automatically transforms data from these AWS services into a standard format called a "finding." The same finding format allows third-party vendors to integrate their data too. Customers can use Threat Stack's bulk `s3export` API to land detailed runtime telemetry in a bucket, transform it using AWS Lambda functions, and load it into Security Hub via its `BatchImportFindings` API.

Threat Stack: Securing EC2 Since 2014

Threat Stack was originally built to enhance the security of EC2, with monitoring and alerting to address specific compliance regulations requiring visibility into running systems. From there, we've grown alongside AWS, expanding to offer true full stack security observability which complements and augments the native security services available in AWS. For a more detailed discussion on how Threat Stack data can combine with your existing AWS security architecture, please schedule a call with your Threat Stack sales and technical team.

threat stack
Part of F5

55 Summer Street, Boston, MA 02110 threatstack.com

Threat Stack is the leader in cloud security & compliance for infrastructure and applications, helping companies securely leverage the cloud with proactive risk identification, real-time threat detection, and full stack security observability through the powerful combination of the Threat Stack Cloud Security Platform® and the Threat Stack Cloud SecOps Program℠.