threat stack

PRODUCT AND SERVICE SOLUTION TIERS

Threat Stack Solution Tiers

Threat Stack offers three different solutions to meet your company's Cloud SecOps needs. Whether you have an in-house team managing your security alerts or you need support with your monitoring and proactive risk reduction strategy, Threat Stack will help you meet your security goals.

		INCLUDED FOR ALL CUSTOMERS	THREAT STACK OVERSIGHT	THREAT STACK INSIGHT
PLATFORM	Host Security Monitoring	●	●	●
	Container Security Monitoring	●	●	●
	Container Orchestration Security Monitoring	●	●	●
	Unlimited Platform Seats	●	●	●
	API Access and Data Export	●	●	●
SUPPORT	Platform Onboarding Service	●	●	●
	Dedicated Customer Success Manager	●	●	●
	Break Fix Technical Support	●	●	●
INCIDENT RESPONSE	Active Alert Monitoring and Escalation		●	●
	Incident Investigation		●	●
	Remediation Recommendations and Guidance		●	●
RISK REDUCTION	Trend and Anomaly Reporting			●
	Recommendations to Reduce Risky Behavior			●
	Cloud SecOps Strategy Session and Ongoing Coaching			●

DESCRIPTION

Threat Stack Cloud Security Platform

Get full-stack cloud security observability.

PLATFORM

HOST OR CONTAINER AGENT

AWS INTEGRATION

INFRASTRUCTURE SECURITY MONITORING

Host Security Monitoring	The Threat Stack Cloud Security Platform® monitors user, system, and file activity on the hosts, using a combination of: • Host Intrusion Detection • File Integrity Monitoring • Vulnerability Assessment • Threat Intelligence Correlation Threat Stack offers rulesets to detect risky and suspicious behavior as well as non-compliant activity.
Container Security Monitoring	The Threat Stack Cloud Security Platform integrates with Docker to monitor suspicious container behavior or misconfigurations. The platform offers out-of-the box, customizable Docker rulesets for CIS benchmarks and general insecure behaviors.
Container Orchestration Security Monitoring	The Threat Stack Cloud Security Platform monitors Kubernetes for suspicious behavior or misconfigurations. The platform offers an out-of-the box, customizable Kubernetes ruleset.
Cloud Management Console Security Monitoring	The Threat Stack Cloud Security Platform integrates with AWS APIs to monitor AWS CloudTrail and AWS EC2. Threat Stack CloudTrail monitoring detects suspicious behaviors and changes to configurations. Threat Stack's EC2 integrations offers visibility into all active EC2 instances.

PLATFORM ACCESS

Unlimited Platform Seats	Threat Stack does not limit the number of users who can access the Threat Stack Cloud Security Platform.

DATA PORTABILITY

API Access and Data Export	Threat Stack offers the ability to store and consume alerts in third-party tools and services. Threat Stack's Webhook and RESTful APIs give users the ability to build triage and response workflows. Threat Stack also gives users the ability to export all events to an S3 bucket for long-term storage, forensics, or custom reporting.

Threat Stack Services

SUPPORT

ONBOARDING

Platform Onboarding Service	A dedicated onboarding specialist will enable customers to use the Threat Stack Cloud Security Platform. This includes deployment assistance, alert tuning, training, and supported integration assistance.

ONGOING SUPPORT

Dedicated Customer Success Manager	A dedicated customer success manager will serve as an ongoing point of contact and proactively ensure that customers are meeting their cloud security goals.
Break Fix Technical Support	The Threat Stack Technical Support team is available to answer questions and support customers through technical issues.

INCIDENT RESPONSE

THREAT STACK OVERSIGHT℠ SERVICE

Active Alert Monitoring and Escalation	A Threat Stack Security Operations Center (SOC) team member will monitor the customer's Threat Stack Cloud Security Platform for critical alerts.
Alert Investigation	A SOC team member will investigate alerts and collect customer-specific data.
Remediation Recommendations and Guidance	If an alert is deemed suspicious or risky, SOC team member will notify customer of alert within 24 hours of receiving the alert and will provide an explanation and recommendations for remediation.

SUPPORT

THREAT STACK INSIGHT℠ SERVICE

Trend and Anomaly Reporting	Create and deliver monthly reports using customer data in the areas of: • User Access Management Report • Network Behavior Report • CloudTrail Activity Report • File Behavior Report • Vulnerability Report
Recommendations to reduce risky behavior	On a monthly basis, a Threat Stack security analyst will provide written recommendations for risk reduction based on reports.
Cloud SecOps Strategy Session and Ongoing Coaching	Depending on need, each customer may request a 1 hour call each month to discuss the report, analysis, and recommendations.

About Threat Stack

Threat Stack enables DevOps and SecOps teams to innovate and scale securely by providing full-stack cloud security observability from the control plane to the application layer. Leveraging powerful insights from the industry's leading cloud-optimized intrusion defense platform, the **Threat Stack Cloud Security Platform®**, the **Threat Stack Cloud SecOps Program℠** works directly with customers through a series of co-managed services to proactively reduce risk and improve cloud security posture with real-time alerts and trended threat intelligence. With a powerful combination of technology and services, Threat Stack customers can efficiently detect security incidents, achieve compliance, and deploy containers securely.

www.ThreatStack.com