DATASHEET

threat stack
Part of F5

Cloud Security and Compliance for Infrastructure and Applications

Threat Stack enables customers to securely leverage the business benefits of the cloud with our unique combination of industry leading security telemetry collection, behavioral rules for known threats, ML powered anomaly detection for unknown threats, and in-house SOC for 24/7 security coverage across cloud workloads.

aws partner network
Advanced Technology Partner
Containers Competency
Security Competency

> **Working with Threat Stack provides us with the expertise, tools, and roadmap we need to keep our team aligned while executing an effective cloud security strategy. Threat Stack's highly experienced Security Engineers work with our Security and Operations teams to optimize the company's platform so we can best leverage its automation, real-time alerting, and investigative capabilities for our unique environment.**
>
> *Ken Ieeser, CISO at Chrome River*

Threat Stack gives organizations the technology and services needed to achieve full stack cloud security across cloud workloads.

RICH TELEMETRY COLLECTION

The Threat Stack Cloud Security Platform® provides the industry's most comprehensive cloud security and compliance telemetry collection across the full cloud infrastructure and application stack

ML-BASED ANOMALY DETECTION

Threat Stack Cloud Security Platform® with ThreatML™ combines rich telemetry and advanced machine learning models to enable security teams to quickly detect, prioritize, and respond to both known and unknown threats.

REAL-TIME RISK DETECTION

Threat Stack provides pre-built, customizable rulesets for detecting known security and compliance risk, enabling you to accelerate compliance with all major frameworks including SOC 2, PCI, HIPAA, GDPR, ISO 27001, and SOX, along with the automated reports you need for audit purposes.

SECOPS EXPERTS

Threat Stack Insight℠ and Threat Stack Oversight℠ services help you proactively identify risk and respond to threats in real time with Threat Stack's dedicated in-house SOC experts and security analysts actively monitoring your cloud environment 365/24/7.

Threat Stack Use Cases

- Cloud Intrusion Detection
- Compliance
- Insider Threat Detection
- Incident Response
- Vulnerability Assessment
- Secure Applications and Microservices

Threat Stack Helps You

REDUCE RISK

Together our industry-leading cloud security telemetry, robust rules engine, ML-based anomaly detection, and human expertise helps you identify patterns of risky behavior, increases your likelihood of detecting a breach, and significantly reduces your time to respond.

SECURELY LEVERAGE THE CLOUD

Build trust with your customers that their data is safe, while you build trust between teams in your organization. When security's goals are aligned with the rest of the organization, everyone wins.

ACHIEVE DEVSECOPS

Threat Stack extends security observability across the entire software development lifecycle including both build-time and runtime environments, enabling you to seamlessly integrate Development, Security, and Operations teams.

FULL STACK SECURITY AND COMPLIANCE

Services

Threat Stack Cloud SecOps Program

The Threat Stack Cloud SecOps Program leverages the power of the Threat Stack Cloud Security Pvlatform to inform your cloud security strategy.

Threat Stack Insight

Make Data-Driven Decisions With Curated Analytics and Personalized Advisory

With Threat Stack Insight, a Threat Stack Security Engineer will curate data on your behalf to help you understand patterns of risky behavior from the results of your ongoing activity across the Threat Stack Cloud Security Platform. You'll also receive support with third-party integrations and advanced rule tuning for your use of the platform.

Threat Stack Oversight

Monitor for Potential Security Incidents

With Threat Stack Oversight, our in-house Threat Stack Security Engineers will monitor your environment 356/24/7, alerting you to potential incidents and helping you understand what happened. Our experts leverage the automation, real-time alerting, and unparalleled investigative capabilities of the Threat Stack Cloud Security Platform.

Technology Integrations

puppet · slack · graylog · docker · ANSIBLE · OpsGenie · pagerduty · CHEF · SALTSTACK · VictorOps · splunk>

Technology

Threat Stack monitors all layers of the infrastructure stack from the cloud management console, hosts, container, orchestration, and applications. This enables customers to achieve the full stack security and compliance needed to leverage the business benefits of the cloud, securely.

FULL STACK SECURITY OBSERVABILITY

Application	Monitor for vulnerabilities and block attacks against applications, microservices, and APIs
Orchestration	Monitor for risky behavior and misconfigurations in Kubernetes
Container	Deploy as a container for automated security Trace suspicious activity across Docker containers
Host	Host-based intrusion detection with out-of-the-box and customizable rulesets
Cloud Management Console	Apply behavioral detection to CloudTrail API logs

ACTIONABLE CONTEXT

- Contextualized signals provide real-time alerts of risky behavior and indicators of compromise
- Proactive risk reduction across every layer of your infrastructure and application stack
- Behavioral analysis identifies internal and external threats
- Faster incident response with real-time threat detection and alerting

FLEXIBLE CONSUMPTION

Alerts and telemetry can be consumed in whatever way fits best with your security or DevOps workflow, whether that's in the Threat Stack Cloud Security Platform, a third-party tool or storage solution, or through co-managed services in the Threat Stack Cloud SecOps Program.

CONTINUOUS CLOUD COMPLIANCE

Leverage pre-built rulesets that map to compliance controls and prove continuous compliance to regulators, auditors, and customers.