Navigating the ‘Knowns and Unknowns’ of Cloud Security

The Threat Stack Cloud Security Platform® with threatML™ and Oversight℠ and Insight℠ professional services

Workloads are on the Move

According to IDC, by 2022, over 90% of enterprises worldwide will be relying on a mix of on-premises/dedicated private clouds, multiple public clouds, and legacy platforms to meet their infrastructure needs. IDC expects 2021 to be the year of multi-cloud, with the vast majority of enterprises deploying combinations of on-premises, off-premises, public, and private clouds as their default environments.

Due to the fact that customer trust and confidence is often won or lost by a company's ability to protect its critical systems and sensitive information, security teams need to efficiently identify and respond to security and compliance risk and threats across their entire infrastructure and application stack, irrespective of whether those workloads run on-premises, private cloud, public cloud and/or in containerized environments.

A major security incident or breach can result in significant financial penalties and irreparable damage to a company's brand and reputation.

When transitioning workloads to modern deployment models it behooves security organizations to consider the following:

- What infrastructure is staying on premises?
- What workloads are moving to the cloud and/or containers?
- How can changes within these environments be monitored?
- What types of security threats and risks should be considered?
- How can we stay current with audit and compliance requirements?

Securing the Entire Cloud Infrastructure and Application Stack

As workloads become more dynamic and complex, security teams need visibility and control of risk at every layer of their infrastructure, to include the cloud management consoles, virtual machine hosts, containers, and applications. What's more, they must maintain consistent security observability across all of these attack surfaces, regardless of how they change over time.

Threat Stack actively monitors and collects telemetry related to OS user activity, container runtimes and services, network processes, file integrity monitoring (FIM), system access, cloud management console settings, and server vulnerabilities.

It combines this rich telemetry data with an out-of-the-box and configurable rules engine, ML-based anomaly detection, and the human expertise of Threat Stack's own SOC analysts to proactively reduce security incidents and the risk of widespread breaches.

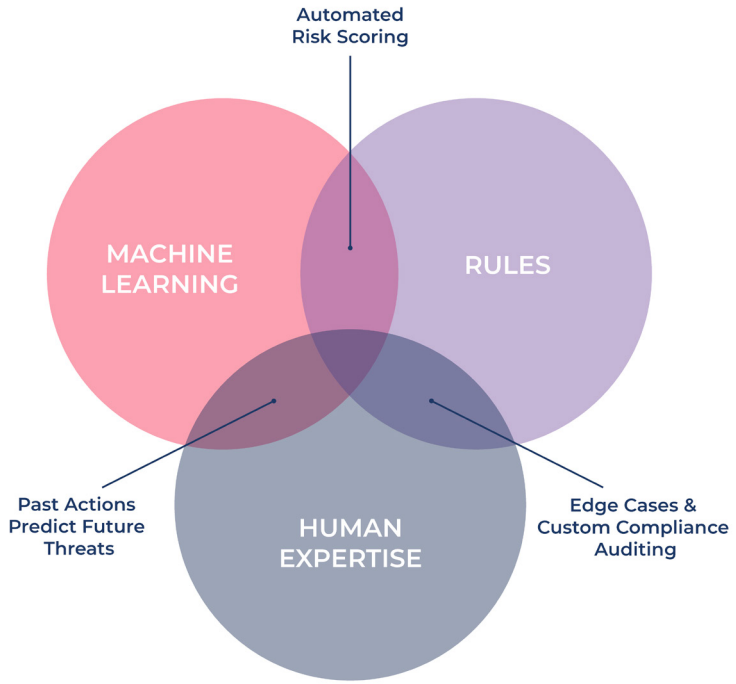
A Layered Approach to Overcoming Known and Unknown Threats

In today's digital era, security organizations need to help drive business transformations. However, striking the right balance between technology enablement and keeping up with the growing number of security and compliance requirements can feel like an uphill battle.

Threat Stack's human in the loop approach to ML takes into account the growing complexity of today's IT environment and incorporates the value of our rich security telemetry data and alerting rules to help address this challenge.

By combining relevant security data and alerting rules with ML and human expertise, security teams can optimize their investigation and remediation efforts by improving mean-time-to-detect (MTTD), mean-time-to-know (MTTK), and mean-time-to-respond (MTTR).

As a result, security organizations can empower their organizations to embrace strategic and transformational technologies, while also ensuring appropriate security and compliance measures are in place to protect their critical systems and sensitive information.



Monitoring the Known

Rules-based methods of risk detecting and alerting excel in environments with well-known behavioral patterns. The security organization can define specific parameters in advance, such as which event types trigger alerts and their associated severity.

Once established and set, rules watch for specific and predefined conditions to take place and alert on them, reliably, every time. This consistency is important for identifying issues like insider threats and for providing a detailed history of system access as part of a compliance audit.

Monitoring the Unknown

ML-based methods surface unknown risk. They excel at learning and baselining behavior to uncover anomalous activities at their first appearance, most notably suspicious activity that would be virtually impossible to predict when setting alerting rules.

To that end, ML anomaly detection can add valuable context to complement rules. For example, with ML anomaly detection, security analysts can be made aware of suspicious trends, resulting from a wide range of activities that, in and of themselves, may not trigger an alert. But when these activities are grouped and looked at holistically, they can uncover significant security and compliance vulnerabilities and threats.

STEP 1: DETECT

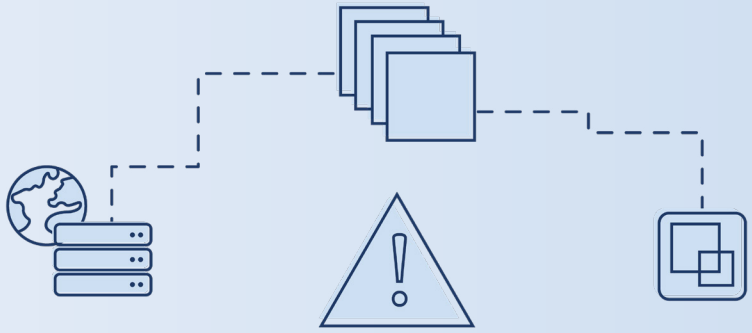
Threat Stack processes 60 billion events a day across our customer base, creating truly comprehensive cloud security monitoring which includes:

- Security telemetry for every layer of the cloud infrastructure and application stack, with support for Linux servers, Windows servers, Kubernetes clusters, AWS Fargate workloads, and frameworks for Node.js, Python and Ruby
- Configurable rules-based engine that identifies known threats, risky behavior, and deviations from established security, privacy, and compliance policies
- Flexible consumption of findings via API support and data lake integration, for faster mean-time-to-detect (MTTD) and mean-time-to-know (MTTK)

Using multiple disconnected tools to monitor and detect threats and anomalies across the infrastructure and application stack leads to operational inefficiencies, as security analysts toggle between siloed dashboards and consoles in an attempt to identify activities that could indicate a security incident or breach.

Security teams need a way to discover threats holistically and faster.

Threat Stack continuously monitors system activity and user behavior for workloads running across the full cloud stack, including containers, Kubernetes, virtual servers, AWS Fargate, etc., and send the telemetry data directly to the Threat Stack platform in real-time. Security organizations gain a full forensic view into the raw telemetry, which serves as the foundation for advanced analytics, timelier insights, and faster risk mitigation and remediation.



STEP 2: VISUALIZE

Security teams can export all host OS events and file integrity monitoring (FIM) events out of Threat Stack and into their own Amazon S3 buckets. This data portability provides several key benefits:

- **Reporting and visualization workflows:** Incorporate Threat Stack data into advanced analytics and threat hunting activities
- **Security information and event management tools (SIEM):** Aggregate Threat Stack events alongside data from other infrastructure monitoring and orchestration systems
- **Cold storage:** Store Threat Stack data over long time periods, in services like Amazon Glacier, to meet compliance requirements

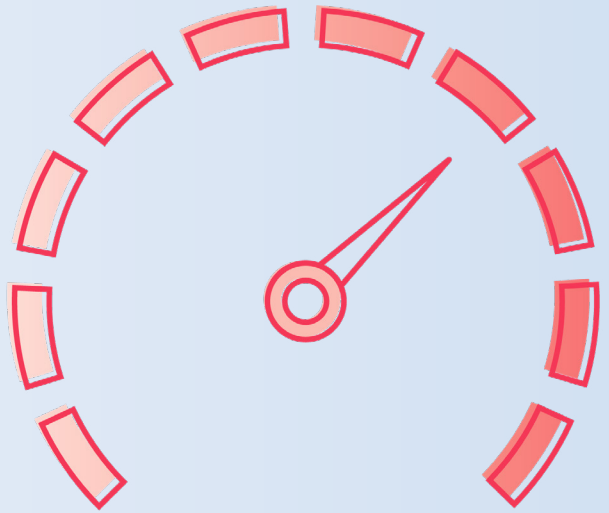
Threat Stack enhances communication and collaboration across Security and Ops teams, enabling them to identify and respond to risk faster, while continuing to leverage their existing tools and workflow.

Learn more here.

Gathering and contextualizing the data that underpins risk across environments is essential. Additionally, security analysts need to have this information at their fingertips. Through Threat Stack's intuitive and real-time dashboards, security organizations get a comprehensive view of their cloud security and compliance risk posture.

Threat Stack also provides API support and data portability capabilities that allow the telemetry we collect to be consumed within an organization's existing workflows and integrated into DevOps tools, to include PagerDuty, Slack, VictorOps, and a range of SIEM products.

Learn more here.



STEP 3: UNDERSTAND

Full-stack telemetry with ML-based insights

Alerting rules and machine learning must exist together.

Threat Stack's rich telemetry informs our ML models, which results in better risk and anomaly detection and alerting. Leveraging both a rules and ML-based approach greatly expands the context related to suspicious activity, making alerts more actionable and increasing the speed and accuracy of security investigations.

What's more, Threat Stack's ML models continuously learn from how users interact with the platform in terms of alert dismissals, escalations, and/or rule modifications, and use the knowledge to enhance anomaly detection, scoring capabilities, and alerting rules over time.

Leveraging rules coupled with ML-based anomaly detection enables security teams to improve their risk visibility and context for both known and unknown threats.

As any security professional will tell you, finding the signal through the noise has never been easy. And with the increase in disparate infrastructure and application workloads, coupled with an onslaught of new threats and compliance mandates, the challenge, and risk associated with failing to act, has never been greater.

Surfacing meaningful security alerts from massive amounts of event data from multiple sources requires distinct methods of detection. These methods should include behavior-based alerting rules, IP reputation scoring, and ML-driven anomaly detections. Unfortunately, most solutions only utilize a small subset of these capabilities, resulting in poor risk visibility and slow responses.

Threat Stack leverages all of the aforementioned methods and provides a robust out-of-the-box and configurable rules engine that identifies known threats, risky behavior, and deviations from established security and compliance policies. In addition, the platform adds a layer of ML-based insights to uncover anomalies and apply risk scores to suspicious user behaviors that would otherwise go unknown.

To that end, ML-based risk scoring provides statistical insight into the significance of an anomaly in the context of an alert. This insight not only helps make alerts more actionable, but it can also be used to create and/or refine existing rule sets.

STEP 4: RESPOND

Human in the Loop

Even the best rules and ML technology can't replace human intuition, reasoning, and decision making skills.

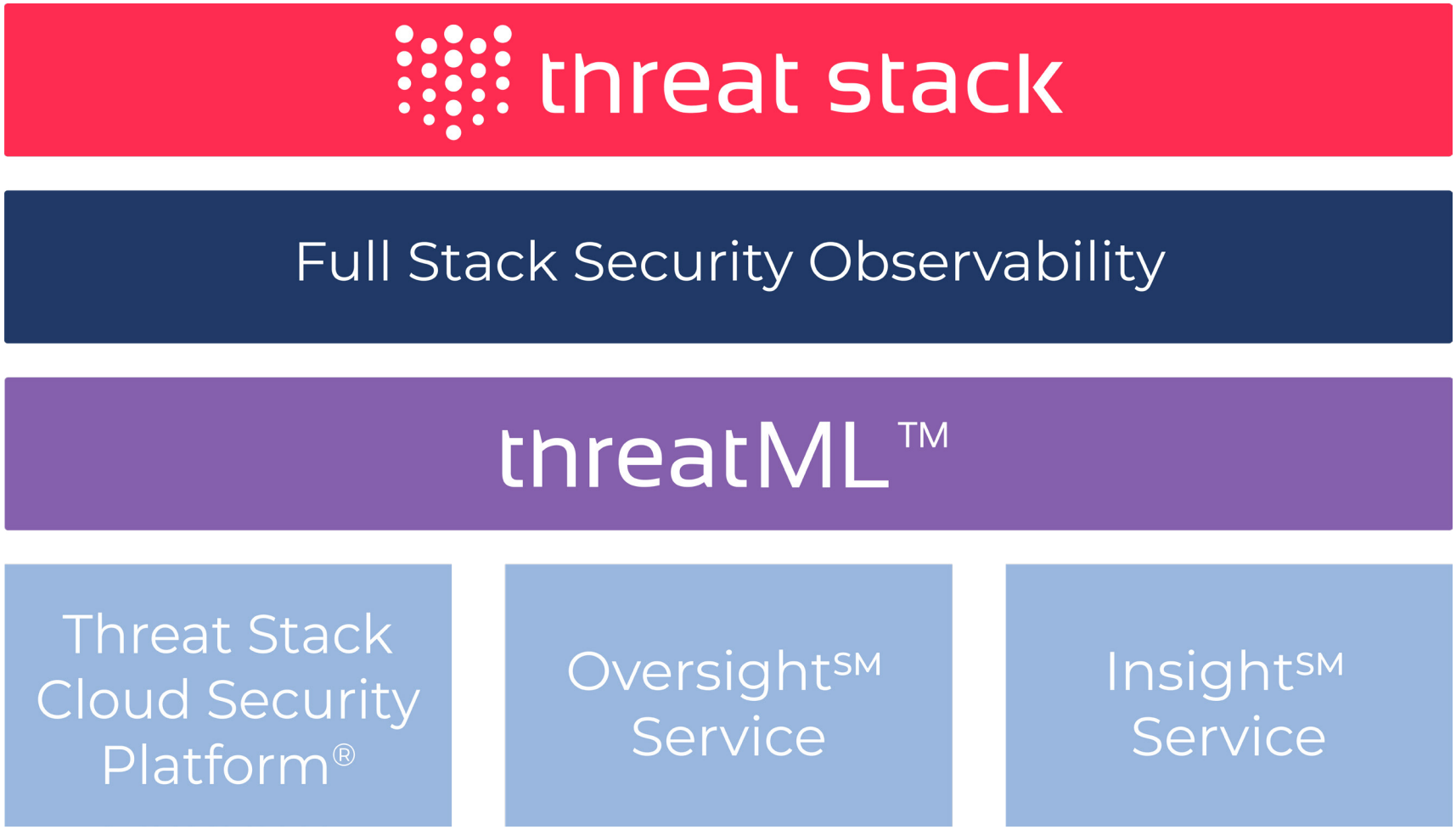
Threat Stack leverages multiple sources to train our ML models, to include the deep cloud infrastructure and application security expertise of our in-house security solution architects and well-trained SOC analysts. Threat Stack with ThreatML™ encodes proven cloud expertise gained through our Oversight℠ and Insight℠ professional services, which includes the coverage of hundreds of customers and their unique production cloud architectures. This experience underpins Threat Stack's anomaly detection capabilities.

The more our experts work with your team, and you interact with the platform, the more ThreatML models learn over time — adding valuable context that improves future findings.

While improved risk and anomaly detection can reduce alert volume, fewer alerts shouldn't mean less security insights. Rich, relevant telemetry must be made readily available when needed for deep forensic investigations and audits. It should also be used as a primary source for rules and alert creation.

Likewise, Threat Stack's ML models automate event and alert correlation, further extending the value of our rich telemetry data. Packaging related activity together makes it easier for security teams to quickly investigate and more accurately respond to suspicious activity.

Applying in-context alerts for security and compliance related issues, anomalies, and non-compliant changes to the infrastructure and application stack, reduces the need for human-intensive triage work. Therfore, security teams can reduce operational costs and allocate more of their time and resources towards threat hunting and remediation efforts.



threat stack WITH threatML™

55 Summer Street, Boston, MA 02110 1+ 617.337.4270 threatstack.com

Threat Stack is the leader in cloud security and 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℠. For more information or to start a free trial, visit threatstack.com.