threat stack

JASK and Threat Stack: A Safer Cloud Environment

Key benefits of Threat Stack and JASK:

Enhanced Visibility

Delivers context across users, network, alerts, devices, and applications, prioritizing the information needed to speed response times.

Improved Productivity

Automates the manual, repetitive validation tasks that limit efficiency, freeing analysts to make advancements in identifying new threats.

Unlimited Scalability

Supports growth with a cloud-native, open source, and big data architecture.

Focused Workflows

Enables analysts to perform high-value, risk-reduction activities like threat hunting, response, and remediation.

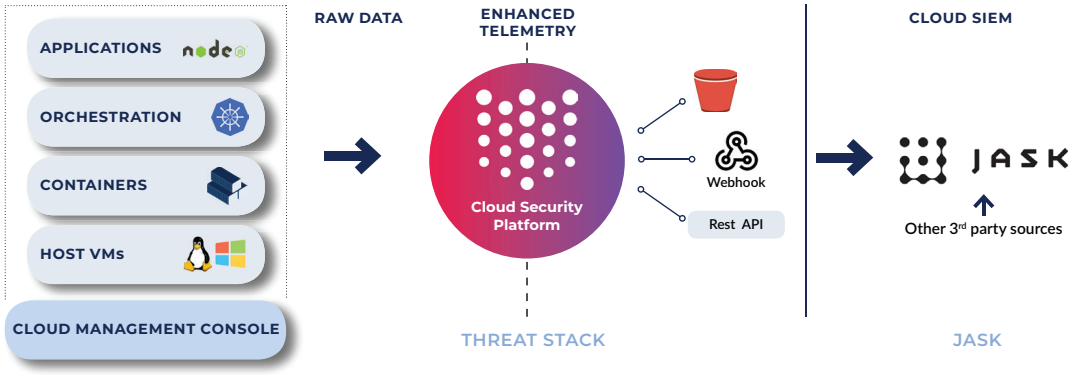
Advanced Insights

Groups related threat signals into JASK Insights using the power of AI and the cloud, alleviating manual triage efforts.

JASK and Threat Stack

Threat Stack and JASK help security operations teams reduce the time and effort needed to detect and respond to security incidents across cloud infrastructure. With Threat Stack, customers get deep visibility into security telemetry from cloud infrastructure and applications. When paired with the JASK ASOC platform, Threat Stack alerts will be fused with additional contextual events and data to automate the correlation and analysis of threats and enable analysts to become proactive threat hunters, reduce the time of investigations, and run new investigations driven by business insights.

THE THREAT STACK AGENT COLLECTS:



Threat Stack: Full Stack Security Observability

Threat Stack gathers telemetry from across your cloud workloads, including Linux and Windows, container orchestration, and applications, alerting you of suspicious, malicious, and risky behavior. Threat Stack takes a behavioral-based approach to intrusion detection — not signature-based — so it can detect early signs of a breach, even if the attacker or attack vector is unknown. Because Threat Stack was built exclusively for highly automated cloud-native environments, it scales up and down with your business needs and does not create friction for your teams.

JASK ASOC: Cloud-Native SIEM

The JASK Autonomous Security Operations Center (ASOC) Platform is modernizing security operations by giving analysts prioritized and contextualized threat data — thus removing the technology limitations that burden SOC speed and effort to stop compromises. As an open, cloud-native framework, the JASK ASOC Platform has auto-scaling capabilities that adapt to peaks in event data and volume to streamline investigations. Additionally, JASK's open, flexible architecture built for big data analytics, integrates to virtually any existing solution, automating parsing of massive amounts of data and supporting analyst workflows to improve the efficiency of manual triage efforts.

WHAT THREAT STACK DETECTS:

- Data Exfiltration
- Services Running as Root
- System Users Connecting to Databases
- Suspicious Commands
- Time Stomping
- EC2 Metadata Communication
- Lateral Movement
- SSH Proxy Use and Creation
- Suspicious System Modifications
- Persistence Mechanisms
- Credential or Secrets Access
- And more

About JASK

JASK is modernizing security operations to reduce organizational risk and improve human efficiency. Through technology consolidation, enhanced AI and machine learning, the JASK Autonomous Security Operations Center (ASOC) platform automates the correlation and analysis of threat alerts, helping SOC analysts focus on highest-priority threats, streamlining investigations, and delivering faster response times.

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. Purpose-built for today's infrastructure, the Threat Stack Cloud Security Platform® and Cloud SecOps Program℠ combine cloud optimized intrusion defense, continuous security monitoring, and proactive risk assessment to help Security and Operations teams detect security incidents, achieve compliance, and deploy containers securely.

To learn more, contact:

Business Development, *Threat Stack*
BD@threatstack.com

Oren Arar, *JASK Director of Business Development*
oren.arar@jask.com

threat stack

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

Threat Stack enables growth-driven companies to scale securely and meet complex cloud security needs by identifying and verifying insider threats, external attacks, and data loss in real time. Purpose-built for today's infrastructure, the Threat Stack Cloud Security Platform and Cloud SecOps Program combine continuous security monitoring and risk assessment to empower security and operations teams to better manage risk and compliance across their entire infrastructure, including cloud, hybrid-cloud, multi-cloud, and containerized environments.