threat stack
WITH threatML™

Four Steps of the Compliance Lifecycle

Automate security functions and simplify compliance audits using the Threat Stack Cloud Security Platform® with Oversight℠ and Insight℠ professional services

Keeping Pace with Regulatory Change

There's no denying that security and compliance are increasingly interconnected. As regulations become stricter to protect customer data, organizations must overhaul IT security and data management protocols to remain compliant. As a result, achieving compliance is no longer a linear checklist of actions but rather anevolutionary journey that keeps Infosecurity professionals on their toes.

Although meeting different compliance requirements can be challenging, especially in modern complex cloud environments, it can also open up new markets, speed up your sales process, and improve your company's overall security posture. When it comes to improving your security maturity, compliance has proved to be a valuable part of the strategy. Whether you're targeting specific industry verticals or international customers, entering new markets requires continuous education and adherence to the latest compliance and regulatory standards.

In the case of many Threat Stack customers and those of you reading this ebook, you're most likely already operating as a cloud-native organization. This puts you at a great advantage when it comes to working towards and achieving compliance as you're more agile and able to adapt your infrastructure to evolve with technology. But being cloud-first comes with a great deal of responsibility to protect the growing amount of data your organization processes.

Therefore, achieving compliance for common frameworks such as SOC 2, HIPAA, PCI DSS, and ISO 27001 are essential milestones for cloud-native organizations. Protecting customer data is crucial to building customer trust, and prospects often require it before becoming customers. But preparing for and passing the security portions of compliance audits can be complicated for resource-strapped organizations. Security leaders tasked with passing one, or multiple compliance standards face the challenge of relying on arduous, manual methods to set the proper controls ahead of an audit and generate new reports from siloed data points to satisfy specific requests.

Getting Started on Your Compliance Journey

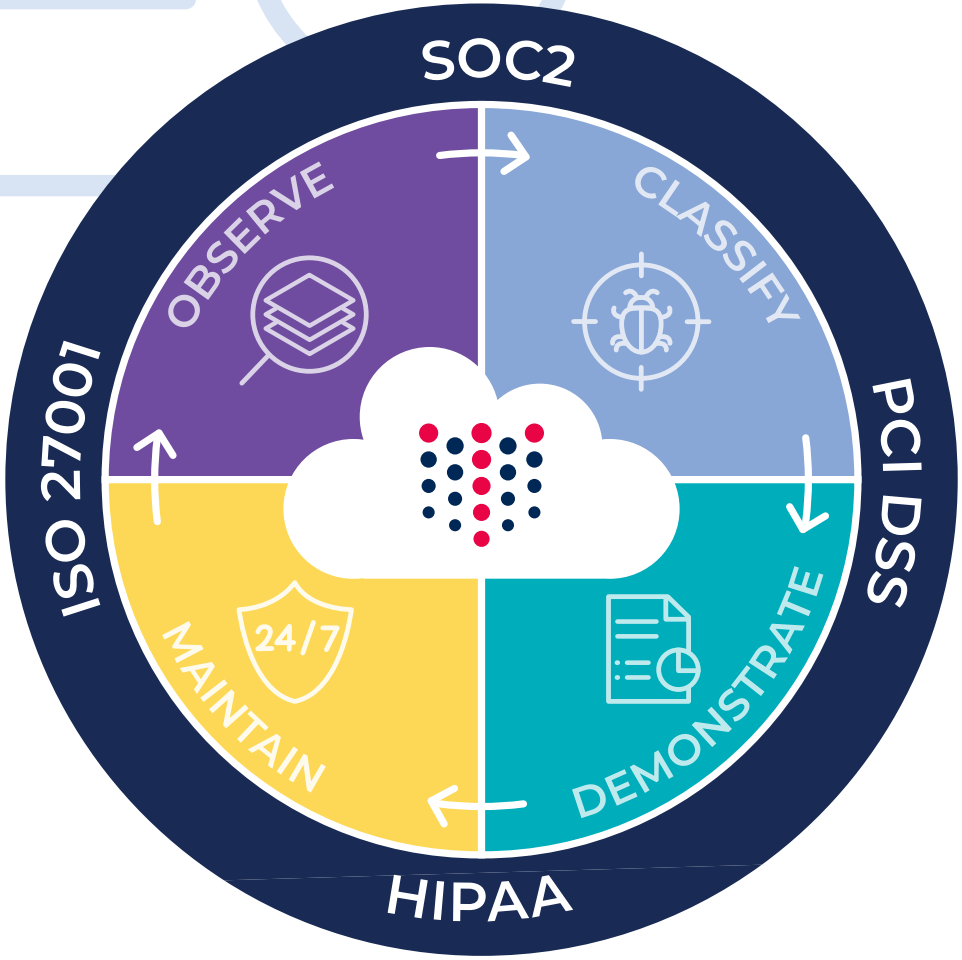
If you're not familiar with Threat Stack, it's critical to understand that we are first a cloud security company. But due to the interconnectedness of compliance and security, we're able to apply our rules methodology to our customer's compliance initiatives, we call these compliance classifiers. Why is this important? For starters, by working to mature your cloud security posture, you're also able to achieve your compliance goals faster. Let's discuss.

Suppose you are operating in Amazon Web Services (AWS), as many SaaS companies are. In that case, you'll want to make sure your infrastructure is configured in accordance with CIS benchmarks and AWS Security Checklist. Doing so can help you meet many security and compliance requirements, simplifying your compliance journey from the start.

Once you've secured your AWS infrastructure, your next move should be to determine which compliance regulations apply to you now and which you want to adopt in the future, and, if you are already compliant, what changes and updates you need to be aware of. This will help determine where your company should focus its compliance efforts as you move ahead.

Threat Stack's Four-Step Approach to the Compliance Lifecycle

As we've discussed, compliance is a journey, not a destination. This continuous lifecycle encompasses your initial efforts to become compliant with frameworks that drive business value for your organization, all the way through audits and maintaining a continuous compliance posture.

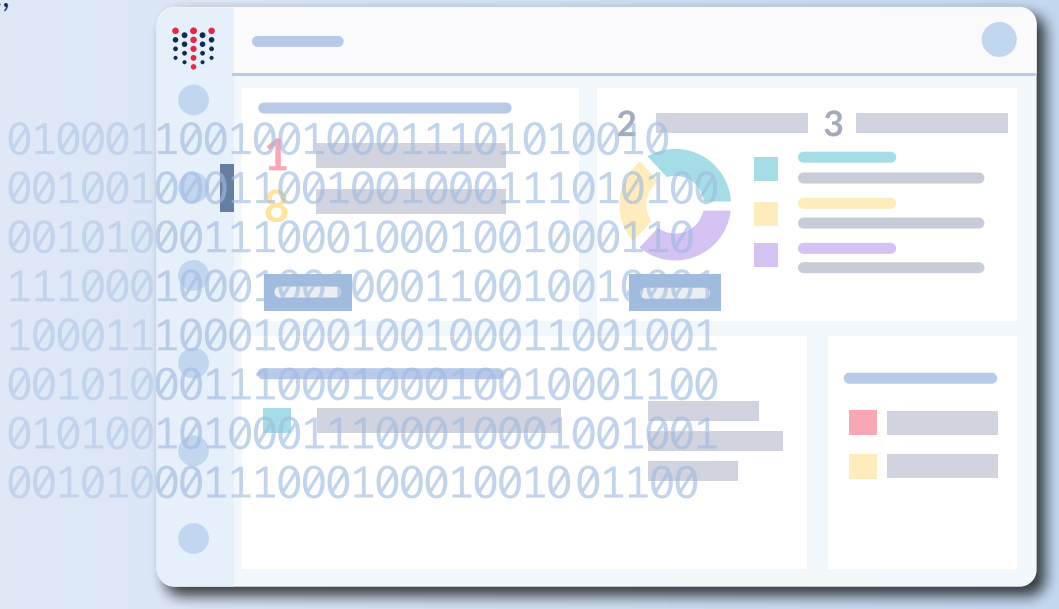


> "We have to make it easy for an assessor to validate that we're doing what we say we're doing, and Threat Stack provides insights into who is doing what, where, and when—along with an audit trail and reports that can be passed along to an auditor."
>
> —Brian Daily, Co-Founder and CTO at Stratasan

Threat Stack helps organizations accelerate compliance and streamline audits by automating security and compliance functions through the Threat Stack Cloud Security Platform. We provide unique pre-built rulesets for common frameworks, enabling customers to quickly achieve and maintain compliance. We then provide automated comprehensive compliance reports to help you satisfy audit requirements and accelerate the process.
To simplify your compliance journey, we break it down into a four-step lifecycle: observe, classify, demonstrate and maintain. Let's explore.

STEP 1: OBSERVE YOUR STACK WITH TELEMETRY COLLECTION.

Threat Stack processes 60 billion events a day across our customer base, creating truly comprehensive cloud security and compliance monitoring. We monitor across your cloud management console, hosts, containers, Kubernetes, and applications to give you full observability into your environment to support your compliance journey.



Threat Stack provides:

- Security and compliance telemetry for every layer of the cloud infrastructure and application stack, with support for Linux servers, Windows servers, Kubernetes clusters, AWS Fargate and EC2 workloads, and frameworks for Node.js, Python, and Ruby.
- Configurable pre-built rule sets associated with known threats, risky behavior, and deviations from established security 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).

STEP 2: CLASSIFY YOUR BEHAVIOR WITH CUSTOM RULES.

Threat Stack's complete telemetry collection from across the entire cloud infrastructure and application stack informs a robust set of rules to give customers full visibility into their cloud security operations and compliance posture. These are known as compliance classifiers.

Our platform gives organizations:

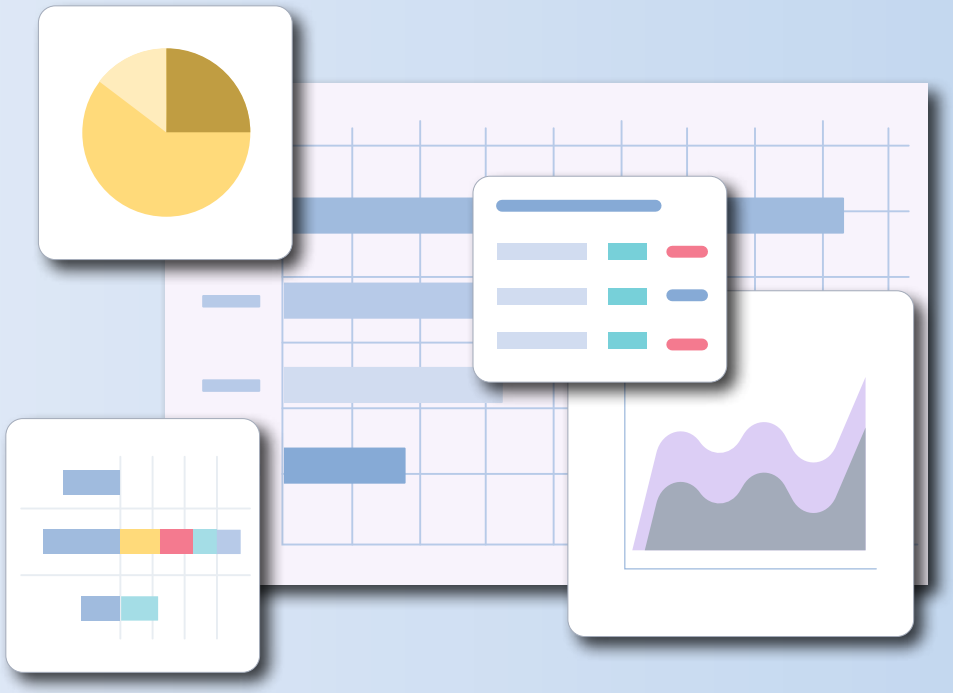
- Rules that are tailored to compliance frameworks (SOC 2, PCI DSS, HIPAA, and ISO 27001) so customers can better prepare for security compliance certifications and satisfy ongoing audit requests.
- The ability to leverage rules coupled with ML-based anomaly detection enables security teams to improve their risk visibility and context for known and unknown threats.
- The context into compliance-focused rules, so security leaders can make changes and implement the security controls required to satisfy compliance certifications.

STEP 3: DEMONSTRATE COMPLIANCE WITH ADVANCED REPORTING.

Threat Stack's latest comprehensive compliance reporting is a monthly report (delivered within the application) that collects and centralizes the required information needed to pass compliance audits e.g., proof of rules in place to protect specific data and the corresponding controls for implementing the regulations. Reports are aligned to the particular compliance frameworks and are easily accessible in order to respond to additional requests during the audit.

Key reporting features include:

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



STEP 4: MAINTAIN YOUR POSTURE WITH THREAT STACK OVERSIGHT AND INSIGHT SERVICES.

Our services offerings (Oversight and Insight) augment your security program and help support continuous compliance.

Even the best rules and ML technology can't replace human intuition, reasoning, and decision-making skills. Take advantage of our 24/7/365 SOC and advisory support for help with maintaining your compliance posture and passing audits.

- **Threat Stack Oversight:** With Oversight, Threat Stack Security Analysts will monitor your environment, alerting you to potential security and compliance incidents and helping you prioritize and resolve them. Our in-house experts leverage the automation, real-time alerting, anomaly detection, and unparalleled investigative capabilities of the Threat Stack Cloud Security Platform.
- **Threat Stack Insight:** Our security analysts curate essential security and compliance data from the Threat Stack Cloud Security Platform and provide advice to help you proactively identify and understand risky behavior patterns in your environment. You'll also receive support with third-party integrations and advanced rule tuning to effectively detect and remediate issues to achieve and prove compliance quickly. integration, for faster mean-time-to-detect (MTTD) and mean-time-to-know (MTTK).

A Hardened Cloud Security Strategy Drives Seamless Compliance

In addition to accelerated compliance, 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 visibility and the control needed to leverage the business benefits of the cloud confidently.
In turn, providing **actionable context**:

- Contextualized signals provide real-time insight into risky behavior and indicators of compromise.
- Proactive risk reduction across every layer of your infrastructure and application stack.
- Robust rulesets, behavioral analysis, and ML-based anomaly detection work together to identify internal and external threats.
- Faster incident response with real-time threat detection, context, and remediation recommendations.

Threat Stack's rich security and compliance insights can be consumed within your existing security, compliance, and DevOps workflow, whether that's in the Threat Stack Cloud Security Platform, a third-party tool, or through co-managed services with Threat Stack Oversight and Threat Stack Insight.

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 and trace suspicious activity across Docker containers.

Host: Host-based intrusion detection and out-of-the-box rulesets.

Cloud Management Console: Integrates with cloud service providers for runtime monitoring of cloud account activity.

Threat Stack's Commitment to Innovation

Hopefully, the biggest takeaway from this ebook is that creating a solid and actionable compliance roadmap is well worth the effort. With technology like the Threat Stack Cloud Security Platform, we can help you meet a significant number of compliance requirements, allowing you to more seamlessly communicate compliance to auditors and customers alike.

Traditional approaches to compliance no longer scale with today's complex stack of diverse infrastructures and applications. But the Threat Cloud Security Platform diminishes the nuisances surrounding compliance and accelerates the audit process through advanced reporting.

Here at Threat Stack, we're committed to continuing on our path of innovation by maturing our platform and compliance capabilities with key enrichments like advanced rule labeling for compliance and comprehensive reporting, giving you the added support needed to achieve your security and compliance goals.

Compliance is a powerful business driver, one that allows you to inspire trust and confidence that will help you stand out in the highly competitive SaaS market. If you'd like to learn more about how Threat Stack can address your security and compliance requirements, contact us for more information.

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.