Anomali ThreatStream

Elevate SOC performance with intelligence-led security

Capture threat data in real-time for faster, more effective prevention and response

As cybersecurity becomes a matter of survival for businesses, security teams need smarter, faster ways to work. Peacetime activities like intelligence curation, attack surface assessment, threat hunts, and playbook creation are critical to understanding and countering potential adversaries. Teams must move quickly and decisively when an attack strikes to mitigate its impact and keep their business running.

Anomali ThreatStream empowers analysts with the AI-enriched threat intelligence they need to understand their threat landscape, security posture, and actual attacks in progress. Powered by the world's largest repository of threat intelligence, the solution filters and prioritizes data by relevance to focus, accelerate, and optimize decision-making at pace. Security controls are updated automatically to reduce the attack surface and speed remediation and response.

ThreatStream democratizes threat intelligence by making it immediately accessible and usable across the business as a foundation for preparedness and resilience. Analysts can use Anomali Copilot to perform complex queries in natural language and generate business-level reports in seconds. ThreatStream Trusted Circles safely extend communication and collaboration beyond the organization to the broader cybersecurity community.

Prepare, decide, and act

Focused intelligence

Security teams can cut through the noise to focus on the most relevant emerging threat

Rapid response

Machine-readable threat intelligence is distributed automatically across your security stack to update controls in real-time

Accelerated insight

Analysts can research, investigate, and act on prioritized threats and potential attacks in progress with new levels of productivity and efficiency

Collective defense

Security teams can collaborate and share threats securely within your organization and across trusted communities

The mission control for intelligence-led security operations

Transform data into insight

Capture, curate, and enrich raw threat data to help security teams quickly understand the context of SIEM and SOAR alerts. ThreatStream goes beyond base IOCs with IOAs, attack flows, campaign incidents, signatures, malware trends, and TTPs correlated to your specific business context. Individual threats are assessed and scored for confidence and severity.

Operationalize threat intelligence

Respond quickly to emerging threats and potential attacks with real-time, automated blocking and monitoring. ThreatStream integrates with security controls, including SIEMs, firewalls, EDRs, and SOARs for intelligence distribution and response orchestration, maximizing your security investments.

Speed research and investigations

Accelerate triage and incident response with a complete research, analysis, and publication workbench. Analysts gain an immediate view of global threats impacting your organization's security posture, including the ability to zoom out from specific indicators to higher-level threat models. Copilot removes technical barriers to understanding with a natural language interface that saves analysts up to 90 percent of the time needed to investigate newly reported threats.

Distribute and collaborate on intelligence

Share high-quality threat bulletins and finished intelligence products with stakeholders within and beyond your organization. Copilot automatically generates summaries of the intelligence at the right levels of detail for diverse stakeholder personas across your business. Used by over 2,000 organizations, ThreatStream Trusted Circles help you work with industry peers to discover, identify, and stop threats.

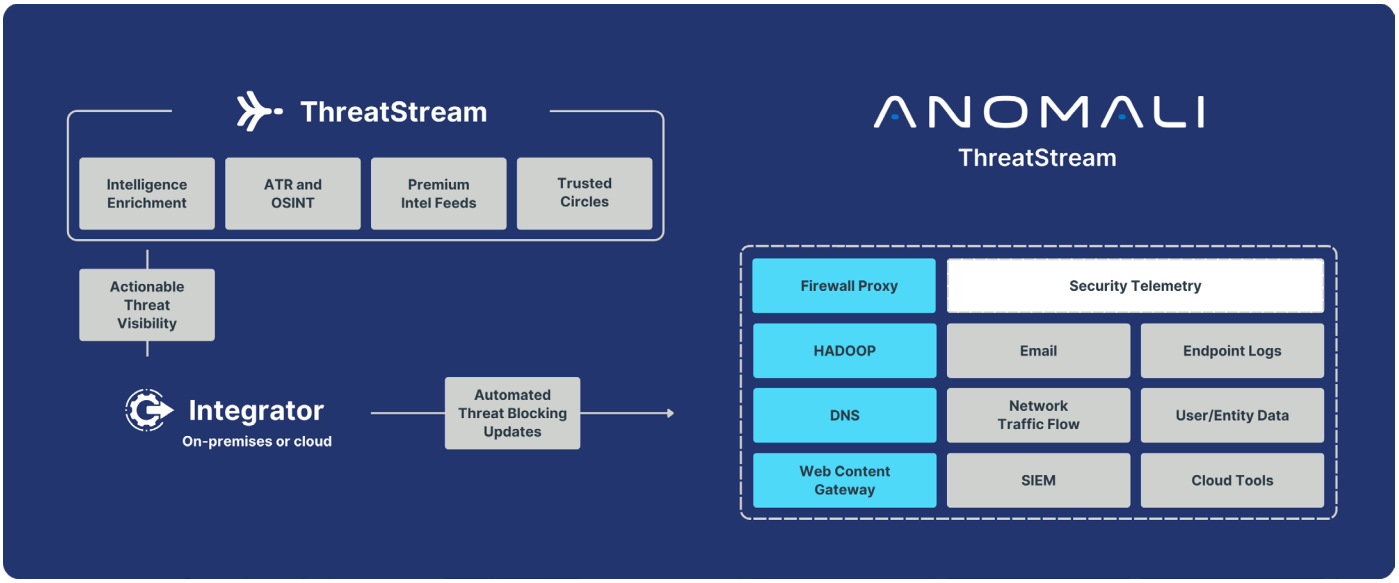

Figure 1.

ThreatStream is the industry's largest threat repository, and includes ATR/OSINT feeds, as well as a broad range of premium intel feeds.

Key capabilities

- Hundreds of diverse threat intelligence sources, including Anomali Labs curated feeds, open-source OSINT feeds, specialized premium feeds, and information sharing and analysis centers (ISACs)
- Automated real-time intelligence collection, curation, and distribution for proactive blocking and monitoring
- Real-time dashboards and machine-readable threat intelligence to assess, prioritize, and proactively stop threats
- MITRE ATT&CK mapping with visual link analysis investigation to expand from indicator to associated higher-level threat models
- SIEM and SOAR alert enrichment with analysis across actors, campaigns, incidents, malware, signatures, vulnerabilities, IOCs, IOAs, and TPPs
- Integrated platform and investigations workbench for analyst research, analysis, and finished intelligence publication
- Integrated sandbox for detonation of suspicious files for investigation
- Turnkey integration with leading enterprise security controls, including SIEMs, firewalls, EDRs, and SOARs
- Real-time, automated blocking, and monitoring
- Threat intelligence sources are assessed and optimized based on quality and relevance to your organization
- Individual threats are scored for confidence and severity using a powerful ML algorithm

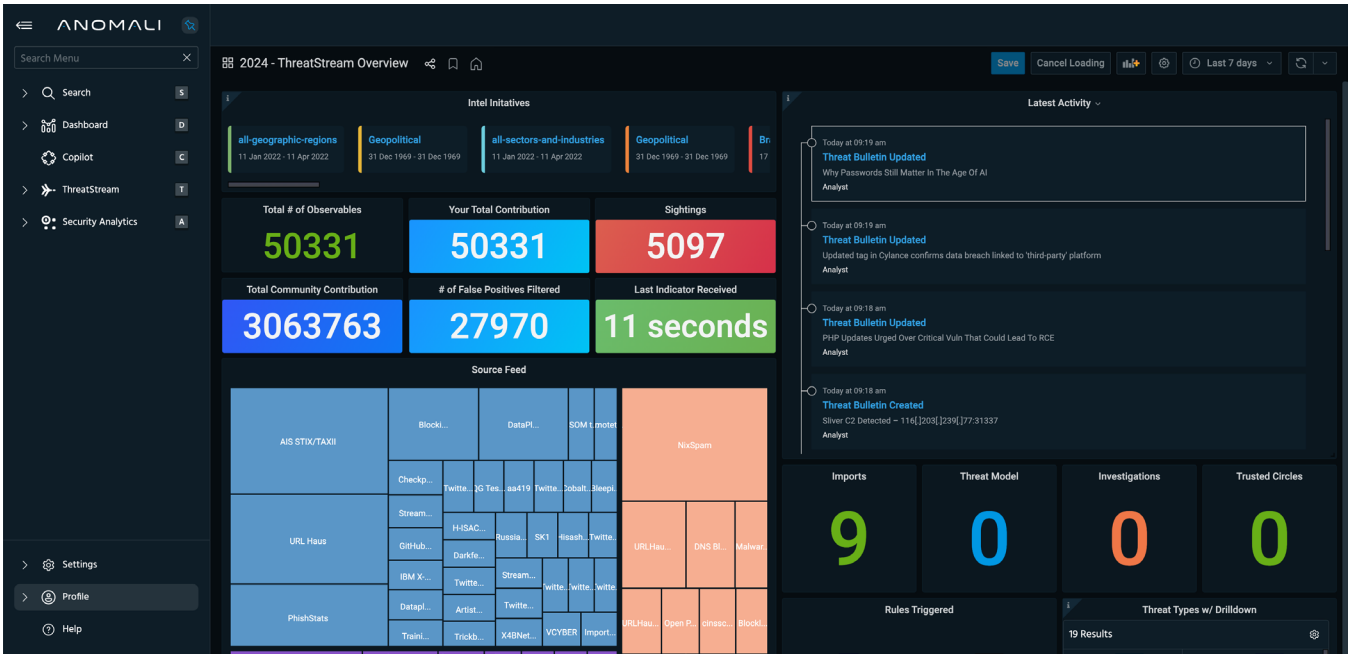

Figure 2.
Get relevant information immediately, enrich the data, and correlate to your internal telemetry

The Anomali Security Operations Platform

Anomali ThreatStream

The world's largest threat repository, Anomali ThreatStream captures raw threat data in real time to power the LLM at the heart of the Anomali Security Operations Platform. IOCs and IOAs are immediately correlated with relevant telemetry to drive actionable insights.

Anomali Security Analytics

Built in the cloud for massive scale and speed, Anomali Security Analytics consolidates SIEM, SOAR, UEBA, and TIP capabilities into a best-in-class, AI-driven solution at a fraction of the cost of competing offers.

Anomali CoPilot

The integrated generative AI capabilities of CoPilot makes our Security Operations Platform the fastest and most comprehensive solution in the market. Based on an LLM using the industry's largest threat repository, CoPilot mitigates hallucinations for accurate, actionable insights in plain language. The perfect partner for every analyst at every level.

Anomali ASM

Anomali Attack Surface Management provides comprehensive visibility into all your IT assets, including shadow IT, to fuel actionable security analytics. Real-time monitoring flags outdated policies, misconfigured assets, and other at-risk entities.

Security Operations Done Differently.

Anomali is the leading AI-Powered Security Operations Platform that delivers mind-blowing speed, scale, and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, NG SIEM, XDR, UEBA, SOAR, and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

Request a demo to learn more about the Anomali AI-Powered Security Operations Platform.

ANOMALI