ANOMALI

Anomali Security Analytics

Aggregate, search, and analyze vast amounts of security information at incredible speed

As IT infrastructure becomes more complex, security teams must spend more time and money trying to gain visibility into potential vulnerabilities, behavioral anomalies, and attacks in progress. Understanding the full context of this data—and its relevance for current threats—can be even more challenging. Meanwhile, cybercriminals are moving faster and smarter than ever to take advantage of blind spots and security operations friction.

Anomali Security Analytics gathers petabytes of data in seconds, providing complete real-time and historic security telemetry across your environment, including SIEM, SOAR, TIP and UEBA data sources. Curated threat intelligence enriches alerts with the context to understand potential adversaries and their attack flows, helping analysts work proactively to prevent a breach. Using a highly scalable data lake, Anomali Security Analytics allows storing years of security logs at a fraction of the cost of traditional solutions. At the same time, custom dashboards, queries, and easy-to-use tools for advanced analytics provide a clear understanding of current vulnerabilities, business risks, and compliance status.

Anomali Security Analytics keeps security teams one step ahead of cybercrime by delivering actionable insights with unprecedented speed and cost efficiency.

Operationalize security data in real-time

Information in seconds

Petabytes of security telemetry and custom data sets can be scanned in seconds

Scalable data

Our use of cybersecurity data lakes lets companies aggregate and store years of logs at a fraction of the cost to gain retrospective insights and achieve compliance goals

Insights on demand

Custom dashboards and simple-to-use queries help analysts surface patterns and turn raw security data into actionable insights

Increase the speed and scale of security analytics—while reducing its cost

Detect attacks

Continually collect, store, analyze, and report on log data for real-time threat detection and incident response. Analysts can identify breaches with precision using the industry's largest repository of threat intelligence. Alerts are enriched with insights into attackers and their tactics, techniques, and procedures (TTPs) to guide prioritization and response.

Hunt threats

Store and search years and petabytes of security telemetry at a fraction of the cost. Using the power of AI, analysts can go from threat intelligence bulletins to proactive hypothesis-based threat hunting in seconds.

Enrich investigations

Gain a full understanding of breaches through retrospective forensic analysis. In the event of a breach, analysts can search petabytes of historical data using natural language to drive investigations, prioritize alerts, and fast-track critical incidents based on attacker insights and breach context.

Respond automatically

Predict and prevent the attacker's next steps. Analytical insights can be fed across the Anomali Security Operations Platform or other security controls to trigger integrated workflows for an automated incident response.

Key capabilities

- Multi-layer automated threat detection powered by IOCs, IOAs, and domain generation algorithms (DGA)
- Security telemetry log aggregation across all your security controls
- Scalable data lake to search and store petabytes of data at a fraction of the cost
- Advanced analytics to investigate security events, analyze compliance, or translate security telemetry to business risk.
- Plain-language search and analysis delivering >140 billion records in < 45 seconds
- Behavior analytics to identify behavioral anomalies with curated indicators of attack
- Interactive workbench and integrated workflows to enrich and accelerate investigation
- Alert enrichment to inform alert prioritization and response actions with insights on actors, campaigns, and TTPs
- Hypothesis-based threat hunting powered with adversary insights to go from threat bulletins to action in seconds
- Generative AI-powered threat & incident summaries and executive reports
- Response automation with integrated response workflows via Anomali Integrator or your preferred SOAR

Security Analytics Architecture

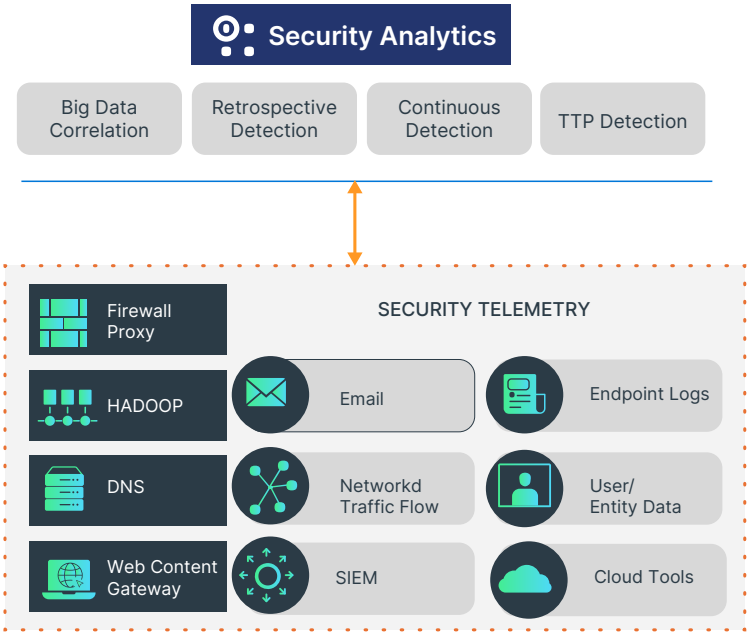

Fig.1 Gain detailed insight across petabytes of data in a matter of seconds

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.

ANOMALI