Anomali Match

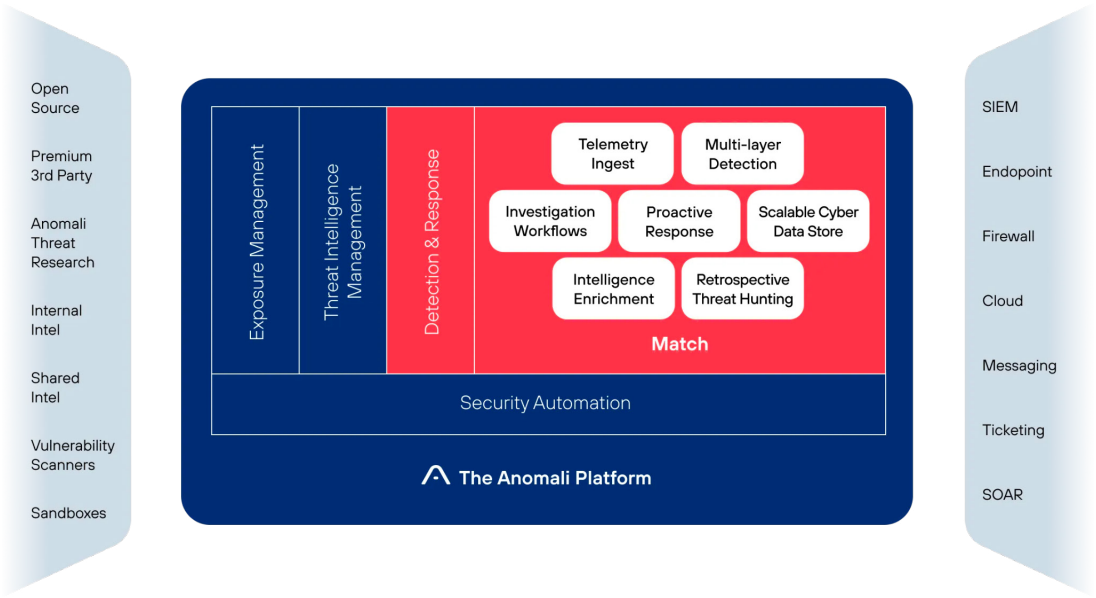
BENEFITS

- **Real-Time Monitoring:** Continually collect, store, analyze, and report on log data for real-time threat detection and incident response.
- **Secure, Search, Visualize:** Analytical engine for deep-diving into security logs, surfacing patterns, and turning raw security data into actionable insights.
- **Retrospective Forensic Analysis:** If a breach does occur, the historical data collected and stored by The Anomali platform can drive the forensic analysis and investigation of the security incident.
- **Automated Incident Response:** Offer automated responses to specific types of incidents, reducing the manual labor required in responding to them.
- **Reduced False Positives:** Through smart correlation rules and machine learning algorithms, significantly reduce the number of false-positive security alerts, freeing up analysts' time.
- **Cost Effective:** Store years' worth of security logs at a fraction of the cost, reduce the operational footprint to manage and secure your infrastructure.

Security teams frequently face challenges when it comes to identifying "blind spots" in their IT infrastructure, and employees and partners use of and interaction with these systems, resulting in limited visibility of critical assets. Acquiring visibility can be costly due to reliance on outdated security incident and event management solutions that do not offer cost-effective management of telemetry data across all security controls. This hampers the ability to retain data over extended periods and forces a trade-off between security effectiveness and cost. Additionally, the stored information often lacks the necessary context for taking actionable measures in a timely manner.

Anomali Match Security Analytics gathers security telemetry from various security controls, such as endpoints, firewalls, cloud platforms, proxies, and DNS. This data is stored in a scalable cloud-native data lake, ensuring efficient storage and significantly reduced costs. The Match Security Analytics Engine engine uses multiple detection layers to identify threats in real-time and conduct retrospective hunts across petabytes of data within seconds. These detection layers encompass billions of indicators of compromise (IoC), behavioral rules or indicators of attack (IoA), and domain generation algorithms (DGA). To provide valuable insights to analysts, the detections are contextualized with carefully curated intelligence on attackers and their tactics, techniques, and procedures (TTPs). This information equips analysts with not only alerts but also knowledge about the adversaries and attack flows, enabling them to predict and proactively defend against subsequent steps. This Match Security Analytic capability is further enhanced by artificial intelligence (AI) and automation, simplifying and accelerating analyst workflows through features like natural language search, automated scoring and enrichment, workflow integrations, and more.

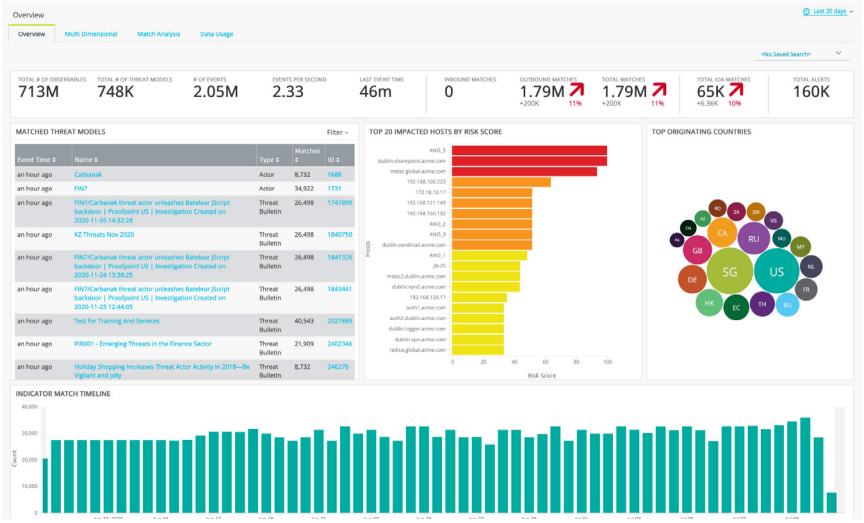
Anomali Match Security Analytics delivers complete visibility at scale and performance with contextual insights to drive real-time decision-making. Anomali Match enables customers to do more with less.



Amplify and action your visibility and drive automated enrichment and response with AI powered Security Analytics

Key Capabilities

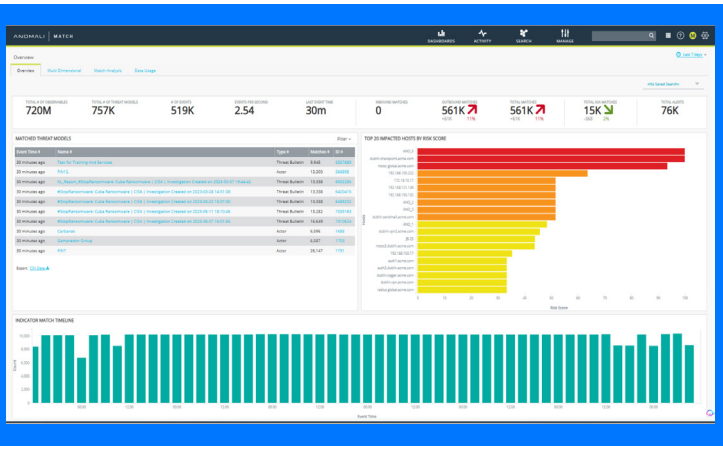
- **Automated Threat Detection:** Detect threats with multi-layer detection powered by indicators of compromise (IoC), behavioral detection or indicators of attack (IoA), and domain generation algorithms (DGA).
- **Log Aggregation:** Ingest telemetry from all your security controls. Store years of data for compliance or security use cases.
- **Anomali Analytics Engine:** Search through petabytes of data at scale and create dashboards, visualizations, and actionable insights.
- **Scalable Data Lake:** Store years of data at a fraction of the cost and gain timely, retrospective insights for critical events.
- **Advanced Analytics:** Investigate security events, analyze compliance, or translate security telemetry to business risk. The Anomali Platform enables customers to search and analyze in seconds - delivering >140 billion records in < 45 seconds or running simultaneous real-time analytics at 10x the current market scale. Do it all in plain language.
- **Behavior Analytics:** Identify behavioral anomalies with curated indicators of attack to stay one step ahead of the adversary
- **Domain generation algorithm:** Predict the malicious command & control domains using DGA
- **Investigation workflows:** Enrich and accelerate investigative workflows, and action alerts with an interactive investigation workbench
- **Alert enrichment:** Inform alert prioritization and response actions with insights on actors, campaigns, TTPs, and more
- **Threat hunting:** Power hypothesis-based threat hunting with adversary insights. Hunt years of data. Go from threat bulletins to action in seconds with the power of AI.
- **GPT-powered:** Improve analyst experience with the power of generative AI. Generate GPT-powered threat & incident summaries and executive reports.
- **Response automation:** Predict the attacker's next steps, and proactively defend with integrated response workflows with Anomali Integrator. Or integrate the response with your preferred SOAR.



Customize your dashboard, know the top active threats, identify at-risk assets, and more

Use Cases

- **Precision attack detection:** Identify breaches with high precision using the largest curated repository of intelligence with insights into attack indicators and attacker behavior.
- **Compliance:** Aggregate years of logs scalably and cost-effectively, and make them searchable to achieve your compliance objectives.
- **Advanced security analytics:** Investigate security events, search through petabytes of data using natural language, enrich security events with intelligence insights to make them actionable, and translate security telemetry to business risk.
- **Enriched investigations:** Prioritize alerts and fast-track critical incidents with attacker insights and breach context.
- **Informed and automated incident response:** Know the adversary, predict their next steps, and stop the breach impact. Accelerate and automate response with integrated workflows across the security controls or integrate with your SOAR.
- **Accelerated threat hunting:** Bring the power of your data to your fingertips. Store and search years of security telemetry at a fraction of the cost. Leverage the power of AI to go from bulletins to hunting in seconds.
- **Collaborative security workflows:** Break the silos and partner with peer groups to speed up time to detection and response. Share threat and risk insights with peers and executives, ingest data from disparate sources, and align security to the business needs.



Search petabytes of data going back years in seconds with natural language

ANOMALI