ANOMALI

Anomali Security Operations Platform

Understand and take action on threats and vulnerabilities—immediately

Increase Cybersecurity Speed and Impact while Lowering Costs

As attack surfaces expand and evolve, security operations teams struggle to understand where they're vulnerable, which threats are relevant to their environment, and how best to respond. The Anomali Security Operations Platform provides an integrated, AI-driven security operations platform to turn information into action immediately.

Consolidating complete security operations tools in a cloud-native solution, the Anomali platform helps teams work quickly and efficiently at all stages of threat detection, prioritization, analysis, and remediation. Analysts can scan years of log data in seconds and use plain-language queries to uncover indicators of compromise or attack. Real-time security telemetry is correlated with the world's largest threat intelligence database for actionable insights with full context. Security orchestration and automation enable an immediate and effective response. Throughout the cycle, generative AI helps personnel at all levels of expertise work quickly and efficiently.

Modernize security operations

Exceptional speed

Analysts can search petabytes of log and telemetry data in seconds using plain language

Lower cost

A single cloud-native platform delivers best-of-breed SIEM, XDR, SOAR, and threat intelligence with 80% lower storage costs

Infinite scale

Up to seven years of internal security telemetry can be correlated with unlimited IOCs and IOAs to stop attacks in real-time

Embedded AI

Security analytics, GenAI-powered reporting, and intelligent task and workflow automation help teams do more

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

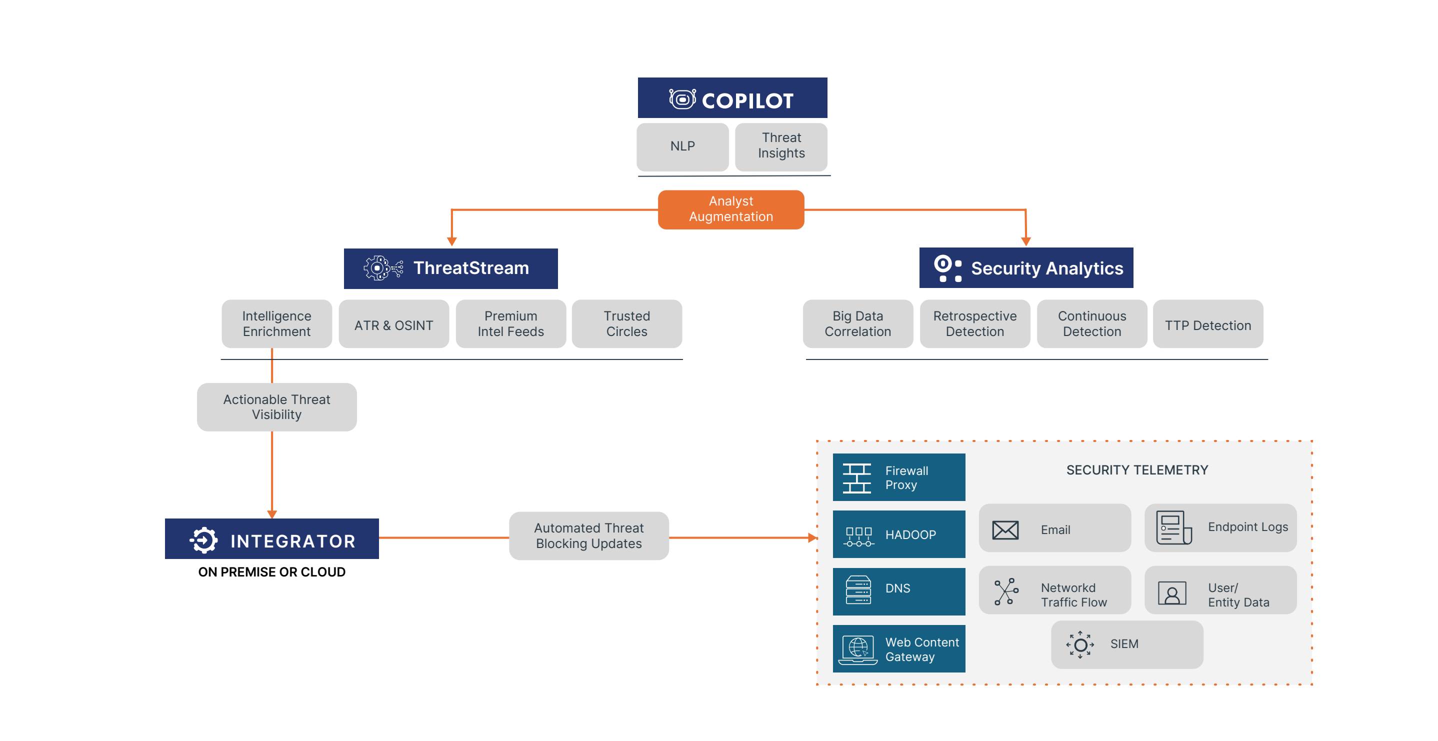
Built in the cloud for massive scale and speed, Anomali Security Analytics consolidates SIEM, SOAR, UEBA, and TIP capabilities into a best-in-class, AI-driven solution at a fraction of the cost of competing offers.

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.

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.



Key use cases for AI-driven security operations

Aggregate

- Automate the collection and correlation of security telemetry, asset data, vulnerability scan data, and active threat intelligence
- Leverage big data security management and machine learning analytics for supporting event/alert correlation

Detect

- Continuously correlate millions of indicators of compromise (IOCs) with all relevant security telemetry and log data
- Perform automated retrospective search and correlation of historical event logs with newly identified threat intelligence
- Predictively detect malicious Command and Control domains created by attacker DGAs (domain generation algorithms)

Hunt

- Conduct TTP-based hunting by actor, threat bulletin, or vulnerability using advanced detection analytics
- Access contextual threat intelligence in the form of actors, TTPs, campaigns, threat bulletins, and vulnerabilities, including MITRE ATT@CK details on the TTPs for any selected actor
- Identify bots in your network making connections to Command and Control servers

Investigate

- Research and prioritize alerts with advanced threat analytics and a powerful investigation workbench
- Enrich alerts with comprehensive threat intelligence context, including TTPs, actors with correlated MITRE ATT@CK techniques events, asset indicators, and links to raw system logs
- Perform real-time and retrospective search on an indicator, TTP, actor, or vulnerability across years of event data to uncover previously hidden incursions

Respond

- Get an immediate view of globally matched threat impacts on your organization's security posture with MITRE ATT@CK mapping
- Continuously monitor detected indicators and associated threat models for response and ROI assessment
- Align critical asset ID with known vulnerabilities and observed IOCs for response prioritization

Collaborate

- Collaborate with industry peers on threat visibility and identification in ThreatStream Trusted Circles (used by over 2,000 organizations and ISACs)
- Achieve STIX/TAXII compliance for bi-directional intelligence exchange between TAXII servers and clients
- Publishing and distributing high-quality threat bulletins and other finished intelligence products to stakeholders at customized levels of detail

The Anomali difference

- **Navigate differently** with actionable insights, natural language queries, and dashboards built in minutes to help analysts turn raw data into action.
- **Analyze differently** with lightning speed, cloud-level scale, broad and deep data integrations, and fully integrated threat hunting and SOAR capabilities.
- **Operate differently** with intelligence-enriched detection, GenAI interfaces, playbooks, and automation that accelerate workflows and uplevel analyst skills.
- **Manage differently** with a consolidated, cloud-native platform that integrates easily with existing cybersecurity investments for simpler, more cost-effective ownership.

Key capabilities

- High-performance correlation of indicators at a rate of 190 trillion EPS
- Appliance and cloud-to-cloud based ingestion of any security control telemetry
- Global intel management across open, commercial, and proprietary resources
- STIX/TAXII for bidirectional intelligence exchange between TAXII sources and clients
- Interactive simplified dashboard and visualization of all IOCs
- Global intelligence feed optimization and scoring
- Out-of-the-box appliance/API integration for response orchestration with security tools
- Vulnerability enrichment aligning global threats with potential organizational impact
- Turnkey integration with leading enterprise SIEMS, firewalls, EDRs, and SOARs
- Extensible platform with restful APIs and SDKs for feeds, enrichments, and security system integrations
- Security tool integration for inbound data ingestion and outbound response orchestration via API/appliance

ANOMALI