

Anomali Copilot

Supercharge security analysts with integrated artificial intelligence

Turn Threat Intelligence into Actionable Insight. Immediately.

Threats are increasing exponentially while security talent is in short supply. SOC analysts must work faster and smarter than ever to protect your business. Anomali Copilot puts the power of cloud-native AI at their fingertips to analyze newly reported threats, determine vulnerabilities, and deliver insights in minutes—for an efficient, prioritized response.

Anomali Copilot uses large language models (LLMs) trained on the world's largest threat repository to understand anomalous activity with unprecedented speed and accuracy. Generative AI lets analysts perform complex queries in natural language and create business-level reports that make the situation clear for executives. Saving up to 90 percent of the time needed for threat investigation, security professionals can stay one step ahead of cybercriminals.

Capable of searching petabytes of data in seconds, Anomali Copilot is built with the speed, scale, and cost efficiency businesses need to keep pace with an intensifying threat landscape. Integration across the entire Anomali Security Operations Platform makes every part of your security stack more effective—for the fastest, most comprehensive solution on the market.

Understand Faster and Respond Better.

Accelerated response

Instant analysis, noise suppression, and generative AI-powered reporting increase the speed and efficiency of threat investigation and response.

Visibility with insight

Anomali Copilot immediately correlates external threat intelligence with your internal telemetry to highlight the context and relevance of IOCs and IOAs.

Intelligent automation

Automated workflows triggered by immediate, prioritized detection enhance collaboration across your SOC.

Natural language queries

Analysts can create sophisticated searches without requiring complex query languages, allowing faster insights and greater job satisfaction.



Improve cybersecurity productivity, effectiveness, and talent retention.

Empower analysts

Provide a better work experience for analysts—and get better results. With natural language queries, gaining insight can be as simple as asking, “Have we been affected by this exploit”? AI-powered correlation eases alert fatigue. Automation frees analysts from hours of tedious daily tasks, including 90 percent of the time needed to investigate newly reported threats, so they can uplevel their skills and the impact they deliver for your business.

Gain a 360-degree perspective

Anomali Copilot, Security Analytics, and ThreatStream provide a clear, forward-looking perspective on relevant threat intelligence and a lookback perspective on threats and anomalous activity across your entire attack surface.

Communicate clearly

Deliver the understanding executives and practitioners need when they need it. Anomali Copilot automatically generates clear, business-level summaries of threats for executive review. Actionable insights provide prioritized next steps for response and remediation, helping SOC teams collaborate more quickly and efficiently.

Enrich your security ecosystem

Operationalize security insights at scale. Anomali Integrator makes it simple to distribute Copilot threat intelligence across your internal security infrastructure, including over 200 security and IT tools directly integrated into the Anomali Security Operations Platform, as well as ISACs and other stakeholders across your broader ecosystem.

Key capabilities

- Plain-language queries for NLP at scale
- AI-powered automation
- AI-enhanced decision-making, intel gathering, hunting, and blocking
- Playbooks and response workflows
- Report and dashboards built in minutes
- Navigates a true cloud-native big data engine that delivers actionable insights from LLM based on the world’s largest threat intelligence database.

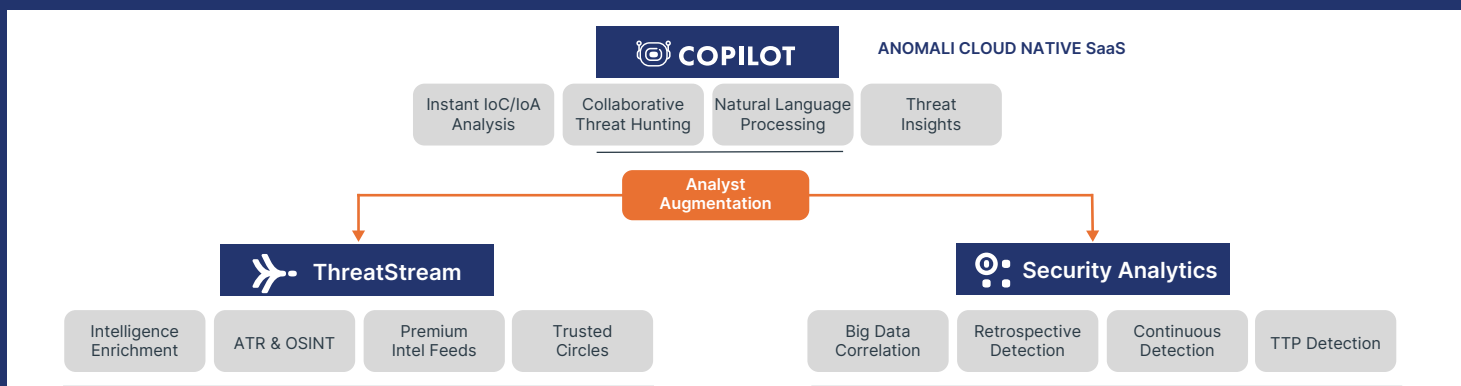


Fig. 1 Anomali Copilot accelerates both threat detection as well as your security operation through AI enablement of your analysts



Fig. 2 Anomali Copilot delivers configurable dashboards that show what you need, when you need it.

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 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 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 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.