ANOMALI

ANOMALI AGENTIC SOC PLATFORM

The Platform That Turns Data and Intelligence into Actionable Decisions

Anomali Agentic SOC Platform unifies complete telemetry, curated threat intelligence, and AI driven guidance to deliver operational speed, precision, and confidence. Built for modern security operations, it accelerates detection, investigation, and response across SOC and CTI teams, ensuring teams can act decisively and consistently at enterprise scale.

TRANSFORMING SECURITY OPERATIONS FROM INSIGHT TO ACTION

Security teams grapple with fragmented data, disconnected intelligence, and alert overload. Standalone analytics and automation lack context and consistency, while traditional threat intelligence platforms generate signals that are difficult to operationalize. The Anomali Agentic SOC Platform changes that.

By combining a data foundation, continuously enriched intelligence, and AI assisted investigations, the platform transforms data → context → action.

THE THREE LAYERS OF THE ANOMALI AGENTIC SOC PLATFORM

Legacy SIEMs can't keep up with today's data volumes. Standalone threat intelligence feeds fail to operationalize, and automation without context creates noise, not outcomes. The Anomali Agentic SOC Platform unifies telemetry, enriched intelligence, and AI-driven investigations to enable SOC and CTI teams to detect, investigate, and respond faster and more confidently.

UNIFIED SECURITY DATA LAKE: REAL-TIME OPERATIONAL DATA

Traditional data lakes and SIEM backends were designed for log retention, not active security operations. Anomali's Unified Security Data Lake powers the Agentic SOC by centralizing and retaining massive volumes of security telemetry — across cloud, endpoint, network, identity, and more — without the performance constraints or escalating costs of legacy SIEMs. This isn't cold storage. It's always-on, always-searchable, and built for real-time and historical analysis at scale.

- Search and correlate years of data in seconds
- Eliminate SIEM bottlenecks and retention tradeoffs
- Build detections, investigations, and hunts on complete, unmodified data

THREATSTREAM NEXT-GEN: INTELLIGENCE THAT BECOMES CONTEXT

Traditional threat intelligence platforms were built for research, not operations. They deliver static feeds, indicator overload, and manual analysis disconnected from security workflows.

ThreatStream Next-Gen continuously enriches your data lake with real-world threat intelligence actors, infrastructure, TTPs, and campaigns so you understand who, why, and what next, not just what happened.
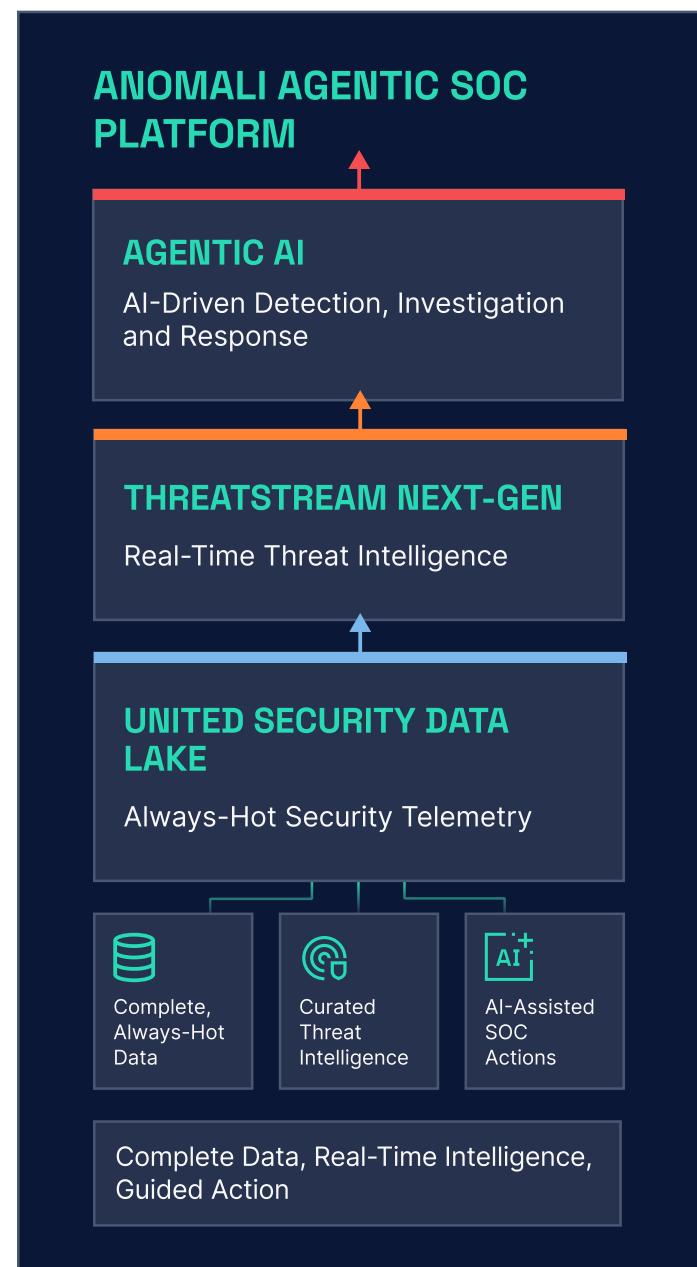
- Enrich alerts with adversary and campaign context
- Prioritize what matters and suppress what doesn't
- Operationalize threat intelligence across detection, investigation, and response

AGENTIC AI: AI-ASSISTED INVESTIGATIONS

Traditional SIEM alerts and threat intelligence feeds generate signals but leave SOC and CTI teams buried in manual triage, correlation, and prioritization. Context is fragmented, decisions are inconsistent, and response slows.

AI-driven agents reason across your unified security data lake and threat intelligence automatically enrich alerts, power investigations, and support response workflows. The result is consistent, repeatable, high-confidence decisions — shared across SOC and CTI teams — so intelligence is operationalized from detection through response AI-driven investigations with transparent, explainable reasoning

- Automated enrichment for that delivers deep, actionable context
- Analysts focus on judgment and response, not manual busywork

ANOMALI AGENTIC SOC PLATFORM

AGENTIC AI
AI-Driven Detection, Investigation and Response

THREATSTREAM NEXT-GEN
Real-Time Threat Intelligence

UNITED SECURITY DATA LAKE
Always-Hot Security Telemetry

Complete, Always-Hot Data

Curated Threat Intelligence

AI-Assisted SOC Actions

Complete Data, Real-Time Intelligence, Guided Action

BENEFITS

ACCELERATE DETECTION AND TRIAGE

Surface high confidence threats faster by combining complete data with enriched intelligence and AI driven investigations.

INVESTIGATE WITH FULL CONTEXT

Pivot across alerts, entities, and historical telemetry instantly — with AI-powered investigations that shorten time to root cause.

RESPOND WITH CONFIDENCE

Reduce guesswork and manual effort with intelligence backed investigations tailored to your environment.

REDUCE NOISE, FOCUS ON WHAT MATTERS

Intelligence ready context and AI prioritization cut through alert fatigue, enabling teams to act on meaningful threats.

UNIFY INTELLIGENCE AND OPERATIONS

Connect SOC and CTI workflows into a single operational plane where data, context, and AI-powered investigations work together.

PLATFORM CAPABILITIES

SCALABLE, CLOUD NATIVE ARCHITECTURE

Built on microservices that decouple compute from storage, the platform processes and queries massive telemetry volumes without performance tradeoffs.

NEAR REAL-TIME, INVESTIGATION READY DATA

Telemetry is easily accessible — no blind spots.

SECURITY AWARE NORMALIZATION AND CORRELATION

Data from diverse sources is normalized and correlated into consistent context, providing a single operational view.

REAL-TIME THREAT INTELLIGENCE ENRICHMENT

Threat intelligence is embedded across the platform, continuously monitoring over a billion indicators of compromise in real time to deliver the context that powers detection, investigation, and response.

HIGH PERFORMANCE SEARCH AND ANALYTICS

Search and analyze petabytes of security data in seconds, enabling rapid pivoting and deep historical analysis across all telemetry without performance degradation.

AI ASSISTANCE FOR DETECTION AND RESPONSE

Continuously analyzes telemetry, intelligence, and historical context tailored to each scenario.

BEHAVIORAL AND IOA DRIVEN INSIGHT

Attack patterns and intent are made visible using enriched models that go beyond static indicators.

INVESTIGATIVE PLATFORM

Unifies data, intelligence, enrichment, and analysis to streamline triage and root cause discovery.

RETROSPECTIVE AND HISTORICAL CONTEXT

Deep, searchable history enables in-depth analysis, threat hunting, and validation of detection logic.

SEAMLESS INTEGRATION ACROSS THE SECURITY STACK

Integrates with SIEM, SOAR, EDR, XDR, firewalls, and cloud systems. Native Model Context Protocol (MCP) server integration ensures that intelligence, context, and insights flow directly into agentic AI workflows without loss of meaning.

WHY LEADING ENTERPRISES RELY ON THE ANOMALI AGENTIC SOC PLATFORM

Organizations trust Anomali because it delivers operational results, not just more data or alerts:

- Accelerates detection and response with intelligence and AI embedded, not bolted-on

- Unifies telemetry, intelligence, and guidance for instant context and precise prioritization

- Reduces tool sprawl and manual correlation with a single integrated platform

- Enables consistent, repeatable decisions across SOC and CTI teams

- Powers agentic SOC operations with confidence and control

OPERATIONALIZE SECURITY AT SCALE

The Anomali Agentic SOC Platform transforms raw logs, threat data, and alerts into actionable decisions. By combining security telemetry, continuous intelligence enrichment, and AI-assisted investigations, it enables security teams to detect, investigate, and respond faster.

SEE ANOMALI IN ACTION

Request a Demo

ANOMALI