ANOMALI

Data Sheet

ANOMALI AGENTIC AI

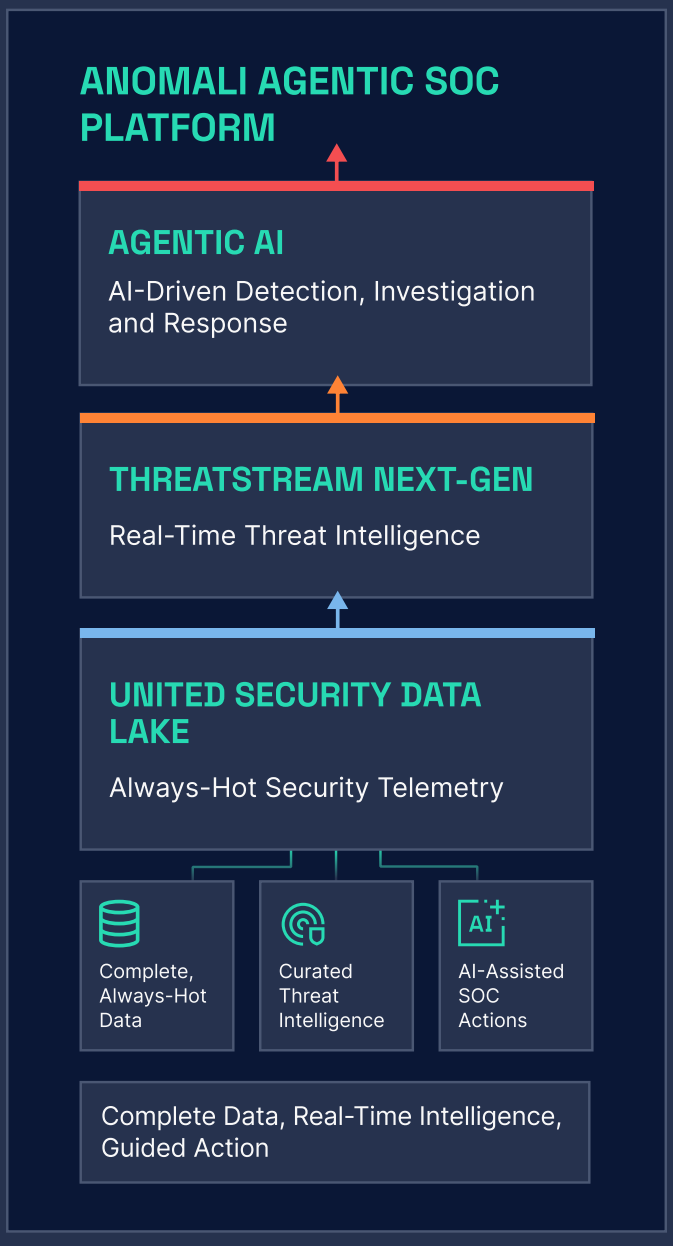
Built for Security Decisions with Agentic AI

Agentic AI delivers real-time insights that accelerate threat detection, investigation, and response. By combining context-rich telemetry, enriched threat intelligence, and AI-powered investigations, it helps modern security teams make faster, more precise security decisions.

THE AGENTIC OPERATIONS LAYER OF THE ANOMALI AGENTIC SOC PLATFORM

Raw alerts and complex security data can overwhelm SOC teams. Automation without context lacks precision and disconnected intelligence cannot guide action effectively.

Anomali Agentic AI operates at the decision layer, providing actionable, AI-driven context that informs every detection, investigation, and response. It transforms data and intelligence into operational decisions that reduce noise, prioritize threats accurately, and support consistent, repeatable security outcomes.



WHY THIS ISN'T TRADITIONAL SECURITY ANALYTICS OR THREAT INTELLIGENCE

Traditional SIEM alerts and threat intelligence feeds deliver signals but leave SOC and CTI teams overwhelmed and forced to manually prioritize and correlate data. Anomali Agentic AI continuously analyzes telemetry, threat intelligence, and context to provide AI-driven investigations. Unified workflows ensure SOC operations and CTI programs can operationalize intelligence consistently across detection, investigation, and response.

AI-POWERED, ANALYST-LED GUIDANCE

Anomali Agentic AI leverages intelligence and security telemetry to prioritize alerts, detect emerging threats, and help guide investigations. Workflows ensure modern security teams retain full control while benefiting from AI-driven context that powers speed and precision.

BENEFITS

INVESTIGATE SMARTER

AI analyzes complex alerts and correlates real-time telemetry with threat intelligence to power investigations, accelerating resolution and reducing triage time.

RESPOND WITH CONFIDENCE

Translate intelligence into action, enabling security teams to act decisively without guesswork.

REDUCE NOISE, FOCUS ON WHAT MATTERS

AI prioritizes alerts, enriches context, and identifies critical threats, eliminating distraction from low-value events.

UNIFIED, INTELLIGENCE-DRIVEN WORKFLOWS

Agentic AI powers context to deliver detection, investigation, and response into cohesive workflows, ensuring consistent operational decisions across SOC and CTI teams.

PLATFORM CAPABILITIES

EMBEDDED AGENTIC AI ASSISTANT

Provides quick investigations and historical context for alerts, enabling teams to pivot quickly between indicators, campaigns, and high-level threat models.

INTELLIGENCE-READY GUIDANCE

Leverages enriched telemetry and threat intelligence to produce actionable recommendations that travel with every alert, investigation, and operational decision.

AUTOMATED, CONTEXT-AWARE RECOMMENDATIONS

AI evaluates threat context, historical patterns, and telemetry to suggest response and mitigation actions.

BEHAVIORAL AND IOA-BASED ANALYTICS

Focuses on attacker intent and tactics, techniques, and procedures (TTPs), moving beyond static IoC feeds to provide predictive guidance for detection and response.

UNIFIED WORKFLOWS FOR SECURITY TEAMS

Integrates detection, investigation, and response across multiple teams, ensuring intelligence is consistently operationalized.

HIGH-SPEED DECISION SUPPORT

Real-time processing enables rapid recommendations across large-scale telemetry, ensuring AI guidance keeps pace with live security operations.

KNOWLEDGE GRAPH

Provides a semantic bridge between NLP and Anomali Query Language (AQL), aligning business terms to underlying schemas and supporting multi-hop reasoning across threat intelligence and log data for advanced investigations.

SEMANTIC SEARCH

Delivers precise, context-aware answers inside by understanding analyst intent and applying domain-specific threat intelligence context. Unlike keyword-based search, Semantic Search filters noise and surfaces only relevant, actionable intelligence—accelerating investigations and improving decision-making.

MODEL CONTEXT PROTOCOL (MCP) SERVER FOR THREATSTREAM NEXT-GEN

Provides a maintained, secure bridge between threat intelligence and MCP-compliant AI clients, enabling low-configuration, real-time access to enriched threat intelligence inside AI-driven analyst workflows.

WHY LEADING ENTERPRISES RELY ON ANOMALI AGENTIC AI

Organizations choose Anomali Agentic AI because it accelerates operational decisions, reduces risk, and maximizes the impact of security teams:

- Provides AI-informed investigations at scale
- Unifies detection, investigation, and response workflows for consistent operations
- Reduces alert fatigue while highlighting high-value threats
- Powers agentic SOC operations using clean, normalized, intelligence-ready context
- Integrates seamlessly with existing SOC tools and intelligence platforms

MOVE FROM INFORMATION TO ACTION

Anomali Agentic AI transforms alerts, intelligence, and telemetry into actionable decisions for the modern security team. With AI-driven insights, it enables teams to investigate faster, respond smarter, and operationalize threat intelligence and analytics with confidence.

SEE ANOMALI IN ACTION

Request a Demo