ANOMALI

Data Sheet

ANOMALI UNIFIED SECURITY DATA LAKE

Built for Security Operations, Not Just Storage

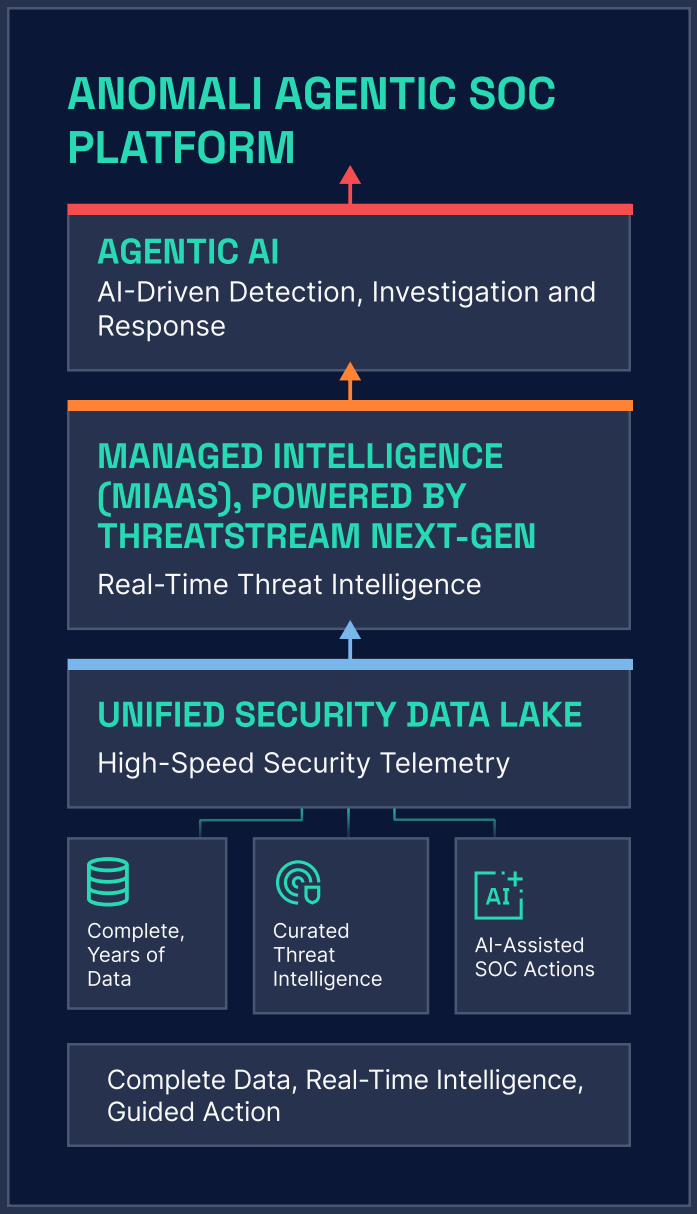
Accessible security telemetry that accelerates investigations, enables long-term threat hunting, and provides the data foundation for analytics, intelligence, and agentic AI. Built on that foundation, Anomali's Agentic SOC capabilities triage detections into confidence-scored alerts, test hypotheses before they ever reach an analyst, and compile audit-ready cases, all human-in-the-loop, so security teams spend their time on genuine threats instead of noise.

DATA ONLY DELIVERS VALUE WHEN IT DRIVES OPERATIONS

Security teams rely on data to investigate incidents, hunt threats, and respond decisively. But traditional SIEM backends and generic data lakes impose retention limits, performance degradation, and costly tradeoffs that restrict how data can be used.

The Anomali Unified Security Data Lake centralizes, retains, and operationalizes security telemetry at scale, ensuring SOC teams always have fast access to complete, normalized, and investigation-ready data.

This data is built to run detection, investigation, and response, with the historical depth that compliance needs as a byproduct.



THE DATA LAYER OF THE ANOMALI AGENTIC SOC PLATFORM

Analytics without complete data lack accuracy. Intelligence without historical depth lacks clarity. The Anomali Unified Security Data Lake provides the data layer where security operations begin, ensuring investigations, analytics, and decisions are powered by complete, security telemetry and threat intelligence with no blind spots or delays. It is the unified data layer the rest of the platform builds on: ThreatStream Next-Gen fuses intelligence into it, and Anomali Agentic AI acts on it.

That AI layer runs on AURA (Anomali Unified Response Agent), the brain of Anomali's agentic fleet, orchestrating specialized capabilities that all reason over the same enriched, correlated data rather than raw, disconnected logs.

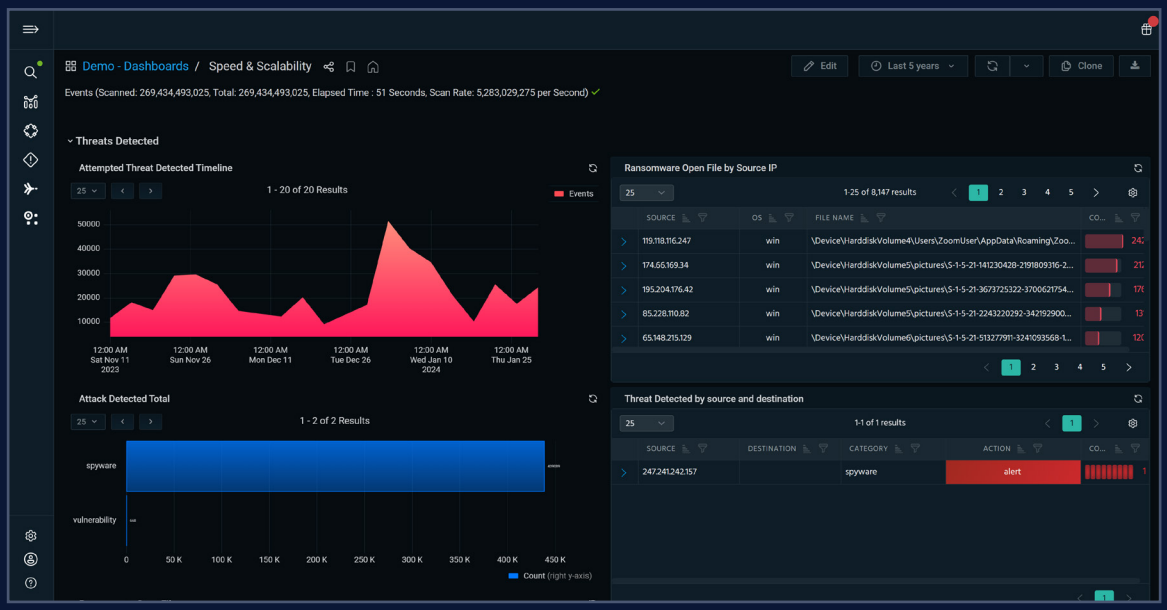
WHY THIS ISN'T A TRADITIONAL DATA LAKE OR SIEM BACKEND

Traditional data lakes and SIEM backends were built for log retention, not security operations. They have performance tradeoffs and delayed access to data that slows investigations and weakens downstream analytics.

The Anomali Unified Security Data Lake is built for the SOC. It delivers security-normalized data with native threat intelligence enrichment and operational outputs designed to support investigations, analytics, and AI workflows, all at the speed of threats.

AI-READY, ANALYST-LED DATA

The Unified Security Data Lake provides the high-fidelity, accessible data foundation AI requires to operate effectively. AI accelerates investigations, powers advanced detections, and supports agentic workflows.



AGENTIC SOC: BUILT INTO THE DATA LAKE

The Unified Security Data Lake is the foundation the Anomali Agentic SOC Platform reasons over. AURA, the brain of Anomali's agentic fleet, orchestrates specialized capabilities on top of it, all running on Anomali Hyper Enrichment and every recommendation human-in-the-loop.

ANOMALI HYPER ENRICHMENT

Continuously enriches telemetry with ThreatStream intelligence, IOC and DGA matching, MITRE ATT&CK mapping, and third-party feeds, building the confidence scores every other capability reasons over, rather than making triage decisions itself.

ALERT TRIAGE

Qualifies detections into actionable signals using a hypothesis-driven approach instead of a fixed playbook, correlating related activity around an entity, scoring confidence, and recommending promote to incident, monitor, or close as false positive, with full reasoning shown at every step.

INCIDENT & INVESTIGATION

Rigorously tests each hypothesis with an adversarial, five-worker review: one biased to prove it, one to disprove it, and three at points in between. AURA then issues a verdict and produces a plain-language summary with recommended actions.

CASE MANAGEMENT & REPORTING

Compiles incidents, alerts, and investigation evidence into a single governed record with a full audit trail and evidence locker, and generates export-ready reports for auditors, executives, and law enforcement.

None of this works without clean data underneath it: because the Data Lake normalizes and correlates telemetry at ingest, every one of these capabilities reasons over consistent, reliable context instead of raw logs.

BENEFITS

INVESTIGATE AT SPEED

Instantly search and correlate months or years of telemetry at a demonstrated scan rate above 5 billion events per second. Run context-less, brute-force searches for any indicator, without knowing where the data lives. Surface results in seconds, accelerating investigations and dramatically reducing time to resolution.

DETECT WITH COMPLETE CONTEXT

Power accurate detection logic using clean, normalized, and continuously available telemetry enriched with intelligence-ready context.

ELIMINATE DATA FRICTION

Remove delays caused by architecture limitations, fragmented sources, and workflows that slow investigations and disrupt response.

ENABLE CONFIDENT, AGENTIC DECISIONS

Power detection, investigation, and response workflows with reliable, normalized, and intelligence-ready data for consistent, high-confidence outcomes.

ACCELERATE TRIAGE WITH AGENTIC AI

AURA auto-resolves clear false positives and reserves investigator time for genuinely high-confidence signals, typically narrowing a day's raw telemetry down to roughly 1% of detections that reach an alert.

CAPABILITIES

SCALABLE, CLOUD-NATIVE SECURITY DATA ARCHITECTURE

Built on a cloud-native architecture that maximizes compute and storage, delivering enterprise-grade performance at scale. It can ingest and retain massive volumes of telemetry without delays, ensuring SOC teams always have access to the data they need.

ACCESSIBLE, INVESTIGATION-READY TELEMETRY

Telemetry remains immediately accessible, enabling high-speed search, historical investigations, and long-term threat hunting without performance penalties.

SECURITY-NATIVE NORMALIZATION AND CORRELATION

Telemetry is structured and correlated at ingest, providing consistent context across cloud, endpoint, network, identity, and application data. This ensures downstream detection, investigation, and response workflows operate on clean, reliable data.

INTELLIGENCE-READY DATA FOUNDATION

Native integration with ThreatStream Next-Gen enriches telemetry with real-time threat intelligence, including indicators, campaigns, infrastructure, and behavioral context. Intelligence travels with the data, supporting investigations and operational decisions.

PURPOSE-BUILT FOR AI AND AGENTIC WORKFLOWS

Complete, OCSF, and contextualized data to power detection, investigation, and response. Enriched telemetry enables workflows to operate reliably at scale across historical and current events.

HIGH-SPEED SEARCH AND ANALYSIS

Optimized indexing and query performance allow SOC teams and new agentic agents to pivot seamlessly across alerts, entities, and timelines, accelerating investigations and improving triage without delays.

RETROSPECTIVE INVESTIGATIONS AND HISTORICAL CONTEXT

Years of telemetry are fully searchable, allowing reconstruction of attack paths, validation of threats, and improved detection logic. Historical depth strengthens investigative and detection outcomes.

OPERATIONAL OUTPUTS FOR SOC WORKFLOWS

Data is structured to produce actionable, operational outputs that feed detection logic, investigation workflows, and response actions across the SOC. Through open integrations with common SOC platforms such as ticketing systems, IR tools, SOAR platforms, and case management, intelligence and analytics seamlessly flow into existing workflows, ensuring consistent execution, faster coordination, and reduced manual effort.

ENTITY & GROUP SYSTEM: RISK-SCORED CONTEXT FOR EVERY IDENTITY AND ASSET

The Data Lake continuously tracks every identity and asset in the environment and assigns each a live risk score, a foundational SOC capability that delivers value independent of the agentic layer.

CASE MANAGEMENT

Compiles incidents, alerts, and investigation evidence into a Kanban-style workflow with a full audit trail and evidence locker for every action taken. Supports export packages tailored for auditors, executives, or law enforcement, with optional redaction before external release.

WHY LEADING ENTERPRISES RELY ON THE ANOMALI UNIFIED SECURITY DATA LAKE

Organizations rely on the Anomali Unified Security Data Lake as the foundation of their security operations because it delivers the speed, scale, and depth that modern SOCs require.

- Enables high-speed investigations across years of accessible security data
- Powers accurate analytics, detections, and AI-driven investigations with complete telemetry
- Eliminates performance tradeoffs between cost, query speed, and data retention
- Simplifies security architecture by unifying log storage, analytics, and enrichment
- Provides the trusted data foundation required for confident agentic AI decisions
- Turns enriched telemetry into agent-ready action through AURA: human-in-the-loop triage, investigation, and reporting built directly into the data lake

BUILT FOR SECURITY OPERATIONS, NOT JUST LOG STORAGE

The Anomali Unified Security Data Lake transforms raw security telemetry into an always-accessible, intelligence-ready foundation for detection, investigation, and response. By delivering complete historical visibility and real-time performance, it enables SOC teams to move faster, act with confidence, and stay in control.

SEE ANOMALI IN ACTION

Request a Demo