# 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.

## 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 is not storage for compliance. It is data designed to operate security.

**ANOMALI AGENTIC SOC PLATFORM**

**AGENTIC AI**
AI-Driven Detection, Investigation and Response

**THREATSTREAM NEXT-GEN**
Real-Time Threat Intelligence

**UNITED SECURITY DATA LAKE**
High-Speed Security Telemetry

Complete, Years of Data

Curated Threat Intelligence

AI-Assisted SOC Actions

Complete Data, Real-Time Intelligence, Guided Action
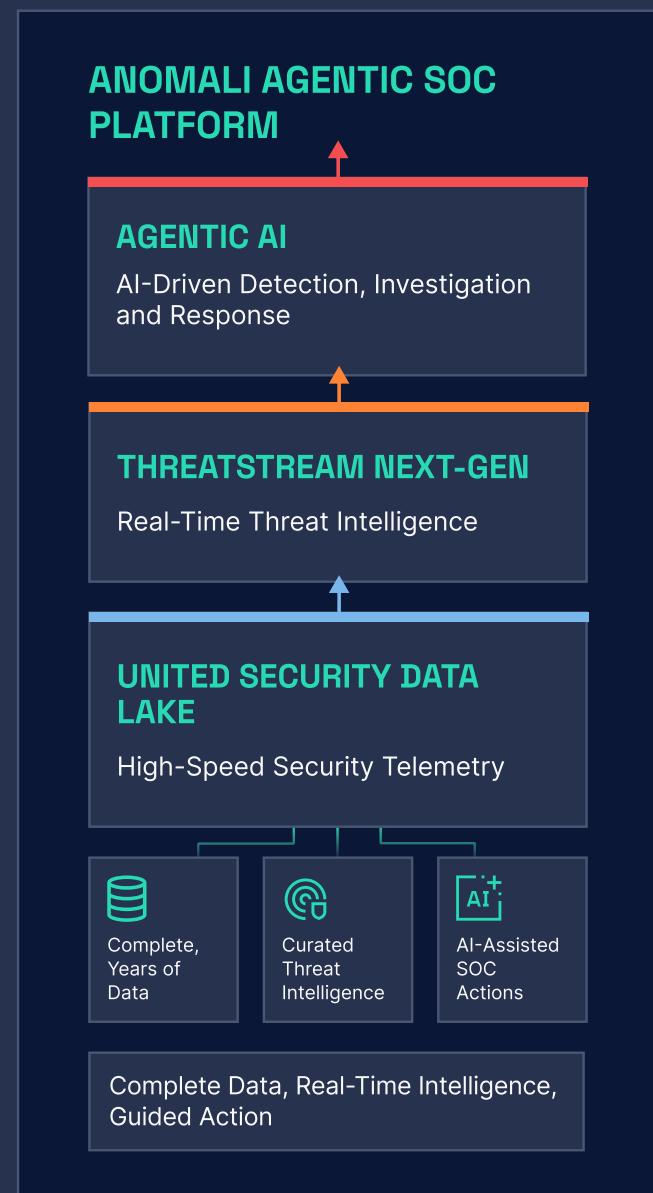
## THE DATA LAYER OF THE ANOMALI AGENTIC SOC PLATFORM

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.

## 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.
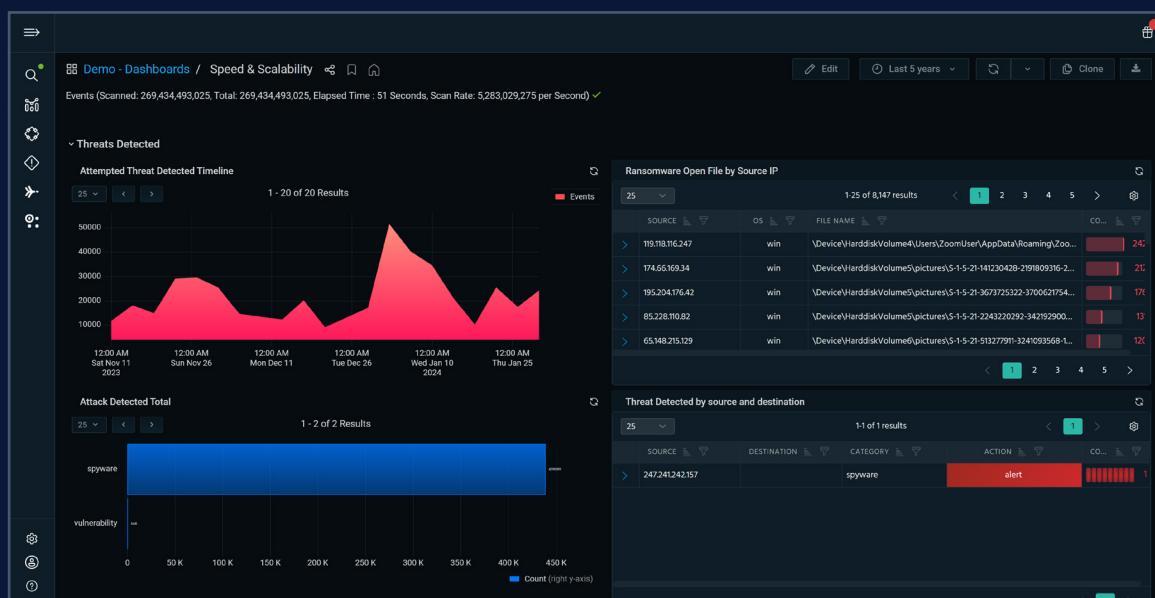
## BENEFITS

### INVESTIGATE AT SPEED

Instantly search and correlate months or years of telemetry at lightning-fast speed. 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.

## 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, normalized, 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.

## 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

## 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

ANOMALI

2