ANOMALI

Data Sheet

MSSPs POWERED BY ANOMALI AGENTIC SOC PLATFORM

DELIVER SMARTER, FASTER, MORE PROFITABLE SECURITY OUTCOMES

Managed Security Service Providers (MSSPs) must protect diverse customer environments while operating efficiently, scaling profitably, and delivering consistent outcomes. The Anomali Intelligence-Native Agentic SOC Platform is built to meet these demands by turning raw security data and threat intelligence into actionable, repeatable decisions across every customer you manage.

By unifying complete telemetry, continuously enriched threat intelligence, and AI-driven investigations in a single, cloud-native platform, Anomali enables MSSPs to accelerate detection, investigation, and response, without adding operational complexity.

BUILT FOR MSSPs NAVIGATING SCALE, COST, AND COMPLEXITY

Security operations break down when data is fragmented, intelligence is disconnected, and alerts overwhelm analysts. Legacy SIEMs struggle with modern data volumes, and traditional threat intelligence produces signals that are difficult to operationalize. Automation is essential for productivity, but without context it just creates noise instead of successful security outcomes.

The Anomali Agentic SOC Platform changes that by transforming **data → context → action**. MSSPs gain a unified operational foundation that supports faster investigations, consistent decisions, and measurable efficiency across tenants.

WHY MSSPS CHOOSE ANOMALI

A UNIFIED PLATFORM BUILT FOR ACTION

Anomali replaces fragmented SIEM, TIP, and automation stacks with a single Agentic SOC Platform that connects telemetry, intelligence, and AI-assisted investigations. This consolidation reduces tool sprawl, lowers infrastructure costs, and simplifies day-to-day operations across customer environments.

INTELLIGENCE THAT BECOMES CONTEXT

Threat intelligence is continuously enriched and operationalized across detection, investigation, and response. Instead of static feeds and indicator overload, MSSPs gain adversary, infrastructure, TTP, and campaign context directly embedded into security workflows.

AI DESIGNED FOR SOC AND CTI TEAMS

AI-driven agents reason across unified telemetry and intelligence to automatically enrich alerts, guide investigations, and support response workflows. The result is consistent, high-confidence decisions shared across SOC and CTI teams.

PROVEN AT ENTERPRISE AND MSSP SCALE

Anomali supports petabyte-scale data volumes with serverless, elastic compute and low-cost hot storage. MSSPs retain 7+ years of instantly searchable data without SIEM bottlenecks, cold-storage delays, or escalating licensing costs.

PURPOSE-BUILT CAPABILITIES FOR MSSPS

UNIFIED SECURITY DATA LAKE

Anomali's Unified Security Data Lake centralizes and retains massive volumes of security telemetry across cloud, endpoint, network, identity, and more. Unlike traditional SIEM backends, this data remains always searchable and investigation-ready and supports both real-time detection and deep historical analysis.

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

MANAGED INTELLIGENCE AS A SERVICE (MIAAS), POWERED BY THREATSTREAM NEXT-GEN

MIaaS continuously enriches telemetry with real-world threat intelligence, connecting indicators to adversaries, campaigns, and intent. This context allows MSSPs to prioritize meaningful threats and suppress noise automatically.

AGENTIC AI FOR ASSISTED INVESTIGATIONS

AI-driven agents automatically enrich alerts, correlate related activity, and surface investigative insights with transparent, explainable reasoning. Analysts focus on judgment and response rather than manual triage and data stitching.

SIMPLIFIED MULTI-TENANT OPERATIONS

- Multi-Tenant Management: Single console to provision, monitor, and manage environments.
- Flexible Deployment: Optimize existing security stacks with flexible deployment options.
- AI-Native Workflows: Automate ingestion, enrichment, detection, investigation, and response.
- Custom Bundles: Tailored offerings from threat intel to full-stack SOC modernization.

PLATFORM CAPABILITIES THAT SUPPORT MSSP SERVICES

- Cloud-native, microservices architecture with decoupled compute and storage
- Near real-time, investigation-ready telemetry
- Security-aware normalization and correlation across data sources
- High-performance search and analytics across petabytes of data
- AI assistance for detection, investigation, and response
- Behavioral and intent-driven insight beyond static indicators
- Seamless integration with SIEM, SOAR, EDR, XDR, firewalls, and cloud platforms

PARTNERSHIP BEYOND TECHNOLOGY

The Anomali MSSP partnership program aligns platform capabilities with managed service business models. Flexible licensing, go-to-market support, and enablement resources help MSSPs deliver differentiated services and better security outcomes at scale.

SEE ANOMALI IN ACTION

https://www.anomali.com/request-a-demo