ANOMALI

Data Sheet

ANOMALI THREATSTREAM NEXT-GEN

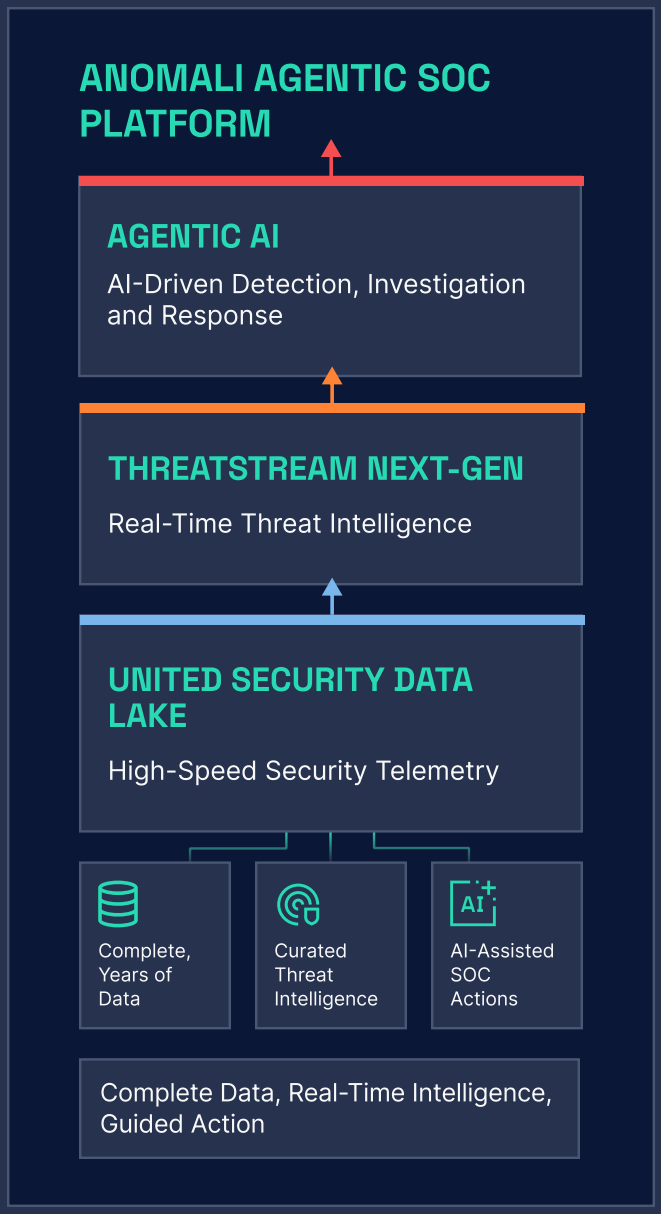
TURN THREAT INTELLIGENCE INTO OPERATIONAL ADVANTAGE

Continuously curated, intelligence-driven context that sharpens detections, accelerates investigations, and powers security decisions.

Threat intelligence only delivers value when it drives action. ThreatStream Next-Gen transforms raw indicators into operational context that travels with every alert, investigation, and decision enabling SOC and CTI teams to act faster, prioritize accurately, and reduce noise across the enterprise.

THE INTELLIGENCE LAYER OF THE ANOMALI AGENTIC SOC PLATFORM

Raw telemetry alone doesn't explain risk. Automation without intelligence lacks precision. ThreatStream Next-Gen provides the intelligence layer where context is created, ensuring detections, investigations, and responses are guided by real-world threat insight.



WHY THIS ISN'T TRADITIONAL THREAT INTELLIGENCE

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 IS BUILT FOR THE MODERN CTI TEAM.

It delivers curated, confidence-scored intelligence that continuously enriches security telemetry, ensures context travels with alerts and investigations, and produces intelligence outputs designed to support analytics, automation, and workflows.

AI-POWERED, ANALYST-LED INTELLIGENCE

ThreatStream Next-Gen uses AI to reduce complexity, accelerate analysis, and eliminate analyst overload. Machine learning drives indicator correlation, confidence scoring, threat enrichment, prioritization, and pattern recognition across campaigns and actors.

BENEFITS

VISIBILITY WITH CONTEXT

Connect internal telemetry with external threat intelligence to reveal what truly matters — understanding both the path of the attack and attacker intent.

PRODUCTIVITY WITHOUT COMPLEXITY

Reduce analyst workload by prioritizing high-confidence threats and streamlining investigation and response workflows.

FASTER, MORE CONFIDENT DECISIONS

Deliver intelligence-backed context at the moment decisions are made, reducing uncertainty and accelerating response.

REDUCED RISK

Distribute enriched intelligence across the security ecosystem to enable proactive blocking, detection, and threat mitigation.

PLATFORM CAPABILITIES

COMMAND CENTER

Anomali Command Center provides a personalized at-a-glance view of the current threat landscape relevant to your organization and about your industry vertical surfacing active attacker operations, key intelligence signals, and a unified Intelligence search across all threat data providing instant access to all historical IOCs, Threat Bulletins, Threat Models, and feed data.

Instead of switching between disconnected threat intelligence screens, analysts get a single, streamlined experience that consolidates the intelligence they need to quickly understand risk and take action. Remove complexity by presenting curated insights upfront, helping teams orient faster and prioritize with confidence.

INTELLIGENCE SEARCH

Intelligence Search provides unified search across threat models, observables, and intelligence. Analysts receive search results that are AI-generated natural language explanations of how observables relate to threat motivations and threat models.

PRIORITY INTELLIGENCE REQUIREMENTS (PIRS)

Priority Intelligence Requirements (PIRs) Manage PIRs with an automated way to monitor the threat landscape, ensuring analysts get only the most relevant, net new intelligence without duplicate data and repetitive manual effort.

PIRs automate ongoing intelligence monitoring and reporting on a continuous schedule. PIRs continuously ingest the threat data analysts define—such as observables and threat models—producing actionable outputs, including new threat models, tagged IOCs, workflow tickets, and alerts.

CASE MANAGEMENT

Case Management brings a modern, AI-powered case and ticketing experience directly into ThreatStream Next-Gen, giving analysts everything they need to create, manage, and resolve intelligence-driven investigations — all in one place. Cases link directly to observables and threat models, ensuring analysts always view the complete intelligence picture alongside the work item.

SCALABLE, CLOUD-NATIVE ARCHITECTURE

Enterprise-grade performance and scale without resource waste, ensuring threat intelligence operations can grow seamlessly with organizational needs.

PURPOSE-BUILT FOR AI

AI is woven throughout the platform — not bolted on — enabling efficient correlation, analysis, prioritization, and response across intelligence workflows. Every action, from scoring and enrichment to investigation recommendations, is enhanced by AI.

CURATED, ENRICHED THREAT INTELLIGENCE

Continuous confidence-scored intelligence enriched with behavioral signals, infrastructure data, and attacker context, moving far beyond static IOC feeds. AI-generated threat profiles automatically unify threat actor aliases, campaigns, infrastructure, and behaviors into a single, risk-scored view, while behavioral and IoA-based intelligence provides insight into attacker intent and techniques.

AUTOMATIC INTELLIGENCE AND TELEMETRY CORRELATION

Correlates curated intelligence with internal security telemetry, mapping campaigns, attack flows, malware trends, and TTPs directly to business-relevant data – ensuring operational context travels with every alert, investigation, and decision.

REAL-TIME ALERT PRIORITIZATION AND TRIAGE

Machine learning evaluates threats based on confidence, severity, intent, and environmental relevance, reducing noise and focusing analyst effort on high-impact issues.

INVESTIGATION WORKBENCH

Accelerate triage and incident response to complete research and analysis, with a publication workbench that includes an integration sandbox for detonation of suspicious files for investigation. Analysts gain an immediate view of global threats impacting the organization's security posture, including the ability to zoom out from specific indicators to higher-level threat models.

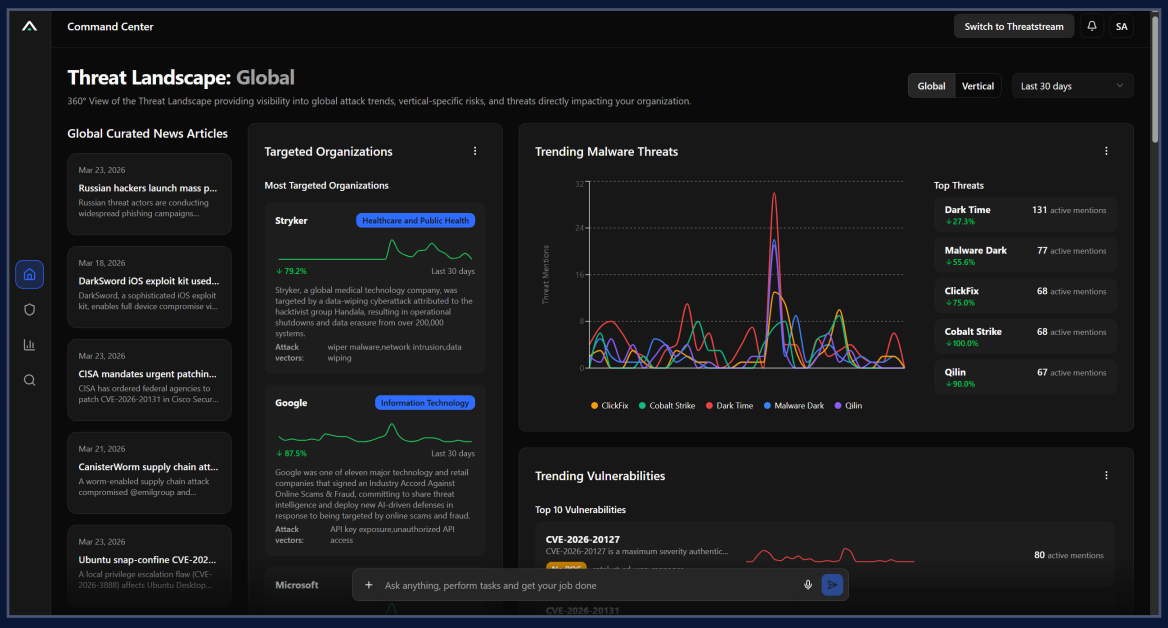
ADVANCED THREAT DETECTION

Uncover hidden threats and breach indicators through detection of DGAs, malicious infrastructure, and command-and-control activity, surfacing adversary behavior that would otherwise remain invisible.

CUSTOMIZED DASHBOARDS AND REPORTING

Role-based dashboards provide real-time, industry- and region-specific intelligence tailored to organizational risk profiles, enabling teams to focus on the threats that matter most.

Publish AI powered reports enabled by report templates to choose from. Reports are saved and organized by date, name, author, shared visibility, TLP, and draft status.



RETROSPECTIVE SEARCH

Historical intelligence and telemetry analysis strengthens defenses by identifying prior exposure, clarifying attack paths, and providing full context for ongoing and future investigations.

BUILT-IN COLLABORATION

Secure sharing of finished intelligence and threat bulletins across internal teams and trusted partners. Unified workflows connect SOC and CTI teams to ensure intelligence is operationalized consistently throughout the organization.

MITRE ATT&CK® MAPPING

Visual mapping connects indicators and campaigns to attacker tactics and techniques, providing a deeper operational understanding and aiding in comprehensive threat analysis.

ASSET BASED CONTEXTUALIZATION

Leverage asset data from scanners, such as Tenable and Qualys, and correlate it with incoming logs within the Anomali platform to contextualize detections.

SEAMLESS INTEGRATION

ThreatStream integrates with SIEM, SOAR, EDR, XDR, firewalls, and cloud platforms to distribute intelligence and coordinate response.

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

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.

Feature	ThreatStream AI Professional	ThreatStream AI Enterprise
Threat Intelligence Collection		
Open Source Intelligence (OSINT) Feeds	✓	✓
Commercial Intelligence Feeds (individually licensed, some free)	✓	✓
Anomali Malware Intelligence Channel	✓	✓
TAXII Feed Client	✓	✓
Community Intelligence Sharing (Trusted Circles)	✓	✓
ISAC feeds and channels	✓	✓
Intelligence Enrichment		
Hash Enrichments	**30,000/month**	**60,000/month**
IOC Search Enrichment	**100/month**	**1,000/month**
Anomali Sandbox	**2 detonations per day**	**3 detonations per day**

Feature	ThreatStream AI Professional	ThreatStream AI Enterprise
Threat Intelligence and Analytics		
Command Center	✓	✓
Intelligence Search	✓	✓
Priority Intelligence Requirements (PIRs)	✓	✓
AQL	✓	✓
NLP	✓	✓
Intelligence Analytics	**30 Days**	**30 Days**
AI Chat Interface	✓	✓
AI-Generated Threat Summaries	✓	✓
TTP Mapping with MITRE ATT&CK Framework	✓	✓
Threat Investigation Tool		✓
Attack Flow Visualization		✓
Custom Data Integration for AI Chat		✓
Intelligence Sharing		
Interorganizational Intel Sharing (Trusted Circles)	✓	✓
TAXII Server	✓	✓
STIX Export	✓	✓
Automated Integrations	**On Premises**	**SasS**
Threat Detection and Response		
Ingestion of Relevant Telemetry		**50GB (included) or more of relevant telemetry**
Autonomous IoC Detection		✓
DGA Detection		✓
Browser-based IoC Detection		✓
Threat Model Associations		✓
Forensics and Retrospective Search		**90 Days (included) or more**
Real-Time Alert and Alert Triage		✓
Asset Criticality Management		✓
Detection Mapping to MITRE ATT&CK Framework		✓
Add-Ons		
Attack Surface Assessment	**$**	**$**
Digital Risk Protection	**$**	**$**

WHY LEADING ENTERPRISES RELY ON THREATSTREAM NEXT-GEN

Hundreds of Fortune 1000 organizations trust ThreatStream Next-Gen to operationalize threat intelligence because it delivers real-world results.

- Accelerates detection and response by seamlessly distributing intelligence across the security ecosystem
- Unifies intelligence and telemetry for instant context and precise prioritization
- Reduces tool sprawl with a single, integrated intelligence platform
- Empowers analysts with flexible search — from advanced queries to natural language
- Enables collective defense through secure intelligence sharing

OPERATIONALIZE THREAT INTELLIGENCE

ThreatStream Next-Gen transforms intelligence into action to deliver real-time visibility, AI-driven insight, and operational context that cuts through noise.

SEE ANOMALI IN ACTION

Request a Demo