ANOMALI

GUIDE

The Speed of Now:

How Anomali Outpaces Next-Gen SIEMs

The Speed of Now:

How Anomli Outpaces Next-Gen SIEMs

Artificial intelligence (AI) is transforming attack methodologies, with threat actors deploying adaptive malware and orchestrating multi-vector attacks that simultaneously target cloud infrastructures, endpoints, and human vulnerabilities.

To forge an effective defense, security teams need more than a next-generation security information and event management (Next-Gen SIEM) solution — they need a unified platform that combines advanced threat intelligence with powerful AI-driven security analytics capabilities.

Anomali's groundbreaking Security and IT Operations Platform does just that. Unlike Next-Gen SIEMs, Anomali delivers:

- Integrated threat intelligence platform (TIP) capabilities and seamless correlation with internal telemetry
- Unprecedented investigation speed that delivers answers in seconds instead of minutes
- Access to seven-plus years of hot data via an innovative Data Lake
- A consolidated tech stack that lets your team do more while reducing budget and operational overhead

The Next-Gen SIEM Landscape is So Last Gen

Next-Gen SIEM solutions represent an evolution of traditional security monitoring, incorporating detection, advanced analytics, machine learning (ML), orchestration, and automated response capabilities. These platforms are designed to handle both the scale and complexity of modern security operations (SecOps) and the demands of elastic networks that extend across multiple cloud instances, SaaS applications, firewalls, and user endpoints.

However, most Next-Gen SIEMs face two significant limitations:

- **Lack of integrated TIP capabilities.** Without a platform that spans the entire security workflow, organizations must purchase and manage separate TIPs. This fragmented approach creates gaps in data integrity and streamlined threat detection and response and adds significant licensing costs and operational complexity.
- **Expensive and complex licensing tiers.** By making customers dependent on big data providers and their associated costs, Next-Gen SIEM vendors limit ready access to historical data and slow investigations to a crawl. Comprehensive security monitoring is prohibitively expensive and hinders critical investigations.

Anomali is security operations done differently. Anomali delivers a unified platform with native threat intelligence and integrated Data Lake, resulting in significant time and cost savings for your security operations center (SOC) team. Anomali transforms how security teams detect, investigate, and respond to threats, making it easier to retain and upskill talent.

Integrated Native Threat Intel

Standalone Next-Gen SIEM solutions disrupt security teams' workflows by requiring them to switch between their SIEMs and their TIPs to get threat intelligence. Anomali streamlines operations by correlating log data with threat intelligence directly within its core platform. It is the only unified SIEM and threat intelligence platform — other solutions require integrations for threat intelligence.

Built around the threat intelligence lifecycle, Anomali ThreatStream is the leading TIP. With a dedicated threat research team, ThreatStream provides curated access to more than 200+ native threat intelligence feeds from diverse sources, including open source intelligence (OSINT), commercial feeds, dark-web monitoring, and proprietary research. Users can also add premium threat intel feeds (often with free trials) via the Anomali App Marketplace. This diverse, customizable library covers a wide spectrum of potential threats and attack vectors mapped to the MITRE ATT&CK® framework.

Anomali's threat intelligence doesn't live in a silo.

Unifying log data and threat intelligence across ingestion, correlation, and real-time monitoring enables seamless data analysis and better contextualization of threats. This results in more efficient detection and response. Anomali correlates this enhanced threat intel with security telemetry, enabling analysts to quickly understand threat severity, relevance, and potential impact on their environments. With Anomali Copilot, you can even do this automatically.

These capabilities significantly reduce alert fatigue, helping analysts prioritize their work queues and allowing them to focus on what they do best — strategic analysis.

Additionally, only Anomali supports unlimited indicators of compromise (IoCs), including threat actors. Other solutions will limit how many IoCs can be stored or simply cannot store or manage that type of data.

The bottom line: Anomali's holistic approach integrates every stage of the security workflow to eliminate manual processes, boost analyst productivity and effectiveness, and uplevel security posture.

Hot Data at Your Fingertips

Anomali's Data Lake architecture eliminates the complicated, expensive licensing models that make access to historical data cost-prohibitive for most organizations. While most Next-Gen SIEMs limit hot storage to 90 days (and charge more for increased data volume), Anomali gives security teams instant access (via hot storage) to seven-plus years of lookback data at a fraction of the cost of competitive SIEM solutions.

Anomali can search up to 100B logs in under 10 seconds. In fact, one Anomali customer reduced correlation search time from 48 minutes to 44 seconds!

This extended lookback capability is crucial for detecting sophisticated attacks that unfold over months or years. Analysts can trace attack patterns back to their earliest indicators, uncovering dormant threats that might otherwise go unnoticed.

What Makes Anomali So Fast?

Anomali's Data Lake analyzes queries and precisely calculates the resources needed to run them efficiently. As a result, it can spin up the exact amount of CPU resources only for the time required, reducing analysis time and resource utilization. Cloud-native and serverless, you won't be running an inefficient environment mismatched to your needs 24x7.

The advantage: Anomali enables security teams to conduct rapid threat hunts and investigations across years of historical data, revealing any long-term threat activities in their networks without performance penalties or additional costs.

Tools to Empower the Tier-1 Analyst

Anomali uses LLMs with access to the industry's largest repository of curated global threat intelligence, providing actionable insights in plain language. Anomali's AI-Powered Copilot enables analysts to ask questions in natural language to search petabytes of security data dating back over seven years, receiving crystal-clear answers and guidance in seconds.

During critical security incidents, this speed advantage can mean the difference between containing a threat and suffering a breach. Analysts can rapidly investigate suspicious behaviors, trace attack patterns, and identify compromised assets without waiting for queries to return answers from archived data.

The result: Your team gets answers and actionable insights in seconds, not minutes, so you can neutralize attacks before they gain traction.

A Consolidated Tech Stack

SOC teams are all too familiar with tool sprawl — multiple platforms, multiple licenses, and the operational complexity that comes with managing it all. Having separate SIEMs and TIPs aggravates the problem.

Anomali takes a different approach. By consolidating SIEM, extract-transform-load (ETL), extended detection and response (XDR), user and entity behavior analytics (UEBA), security orchestration and response (SOAR), and TIP capabilities into a single platform, Anomali simplifies licensing and streamlines the security workflow.

The upshot: Your security team spends less time juggling tools and more time protecting your organization.

How the Anomali Security and IT Operations Platform Satisfies Your Need for Speed

Anomali is purpose-built to offer the fastest search in the industry. Here's how it's done:

- **Cloud-native architecture:** Anomali's cloud-native design makes it scalable enough to handle petabytes of data without compromising performance. Anomali uses lossless compression algorithms to reduce data storage requirements and efficiently ingests logs to ensure rapid data availability.
- **Serverless:** Anomali's serverless architecture enables SOCs to scale resources on demand. This efficiency significantly improves response times and overall performance.
- **Agentless:** Deploy faster and more efficiently with Anomali's agentless design — there's nothing to install, update, or patch. It also makes deployment easier to manage and scale. Moreover, an agentless architecture eases compliance headaches, reduces the attack surface, and decreases endpoint load (since there is no consumption of endpoint resources, such as CPU or memory). Not to mention it reduces the risks posed by agents, as witnessed in recent global outages.
- **Integrated Data Lake:** The heart of Anomali's groundbreaking approach, the integrated Data Lake efficiently manages the exponential growth of security data, providing high-speed collection, processing, and analysis at scale — all while keeping costs low. With Anomali's Data Lake, all of your data is hot.

Business Benefits:

Time Savings:

A robot for your SOC: Automation saves up to 50% of your team's time, delivering reports, dashboards, and results in seconds.

Faster analytics for a faster world: As threats grow in scale and sophistication, you need to process and search massive amounts of data quickly. Anomali does this in seconds, not hours or days.

Do more with less complexity: Simplify your tech stack to reduce risk and improve visibility for use cases such as risk management, insider and external threats, intelligence, compliance, and fraud detection.

Find the needle in the haystack: Pinpoint critical threats in seven-plus years of data at unprecedented speed. Optimize security controls like EDR by uncovering missed insights.

Cut out the middleman: Unite the CTI and SOC functions into one discrete workflow to immediately assess critical risk:

- Which threat actors should we be worried about?
- What tactics are they using?
- Are we impacted?

Retain and Upskill Talent

Anomali's natural language processing (NLP) simplifies and accelerates search, bridging the gap between novice SOC analysts and threat hunters with easy-to-use AI-based tools and automated threat summarization. With Anomali Copilot, analysts of all skill levels can extract actionable insights from raw data without learning a complex query language.

Analysts can pull web-based threat summaries into Anomali to compare with internal telemetry, enabling them to flag suspicious events as soon as they occur. Anomali's AI empowers your Tier-1 analysts to be more proactive in fighting threats.

Cost Savings

Batteries (a.k.a. Data Lake) included: The integrated Anomali Data Lake saves money because we don't sit on top of another big data provider — and we pass the savings back to our customers.

The bottom line: Anomali is security and IT operations done differently. Only Anomali provides mind-blowing speed, scale, and performance in a unified platform and at a reduced cost compared to competitive solutions.

The Anomali Advantage

Anomali stands out in the Next-Gen SIEM market, thanks to four game-changing capabilities.

- Integrated TIP capabilities with seamless threat correlation
- Lightning-fast investigations with results in seconds, not minutes
- Seven-plus years of instantly accessible lookback data for a fraction of the cost
- A unified platform approach that eliminates costly tool sprawl

Security teams need more than just another Next-Gen SIEM. They need a platform that combines comprehensive threat intelligence with advanced AI-Powered Security Analytics in one unified, cost-effective solution. Anomali delivers this complete package, enabling analysts to detect, investigate, and respond to threats faster and more effectively than ever before.

Innovative, Effective Technology

An AI-Powered intelligence-driven platform for a more secure world. That's Anomali.

Discover how Anomali can help you create a robust, highly adaptive security solution. Schedule a demo of Anomali's Security and IT Operations Platform to see why it's different and how it can transform your organization's security posture.

Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. **Request a demo** to learn more.

ANOMALI