ANOMALI

White Paper

MODERNIZE YOUR SIEM

Why Leading SOC Teams Are Augmenting — Not Replacing — Their SIEM with Anomali's Agentic SOC Platform

THE CHALLENGE WITH SIEMS

Your SIEM was built to aggregate logs and satisfy compliance mandates, and it does that well. But today's threat landscape demands something it was never designed to deliver: real-time correlation across hundreds of millions of threat indicators, sub-second retrospective hunting across years of telemetry, and AI-driven analyst workflows that eliminate manual triage.

Modern SOCs don't need to start over; they need to get more from what they already have. Traditional SIEMs remain central to detection and alerting, but they were never designed for the AI era with exploding data volumes and automated attacking from adversaries.

Traditional SIEMs create trade-offs between cost, scale, and search speed that leave analysts struggling to keep up. Replacing them can feel daunting, disruptive, and expensive — especially when detection logic, workflows, and compliance controls are built around them.

The result is a widening gap. Analysts spend hours enriching alerts manually. Threat intelligence sits in a separate platform, disconnected from detection. Historical searches grind to a halt. And costs spiral upward as data volumes grow faster than budgets.

Common challenges for today's SOC teams include:

- **Exploding data volumes** overwhelm ingestion budgets
- **Limited retention** restricts visibility for threat investigations, hunting, and compliance
- **Slow searches and manual correlation** delay incident response
- Limited context slows investigations and increases dwell time
- **Legacy licensing costs** force trade-offs between visibility and insight

The answer is not a costly, disruptive rip-and-replace. The answer is SIEM augmentation. Modernization does not have to cost operational burden. Optimizing your SIEM delivers faster ROI and prepares your SOC for the AI-driven future.

> **YOUR SIEM IS GREAT AT COLLECTING LOGS. ANOMALI IS GREAT AT MAKING SENSE OF THEM — AT UNLIMITED SCALE, WITH INSTANT THREAT CONTEXT, AND WITHOUT SLOWING YOU DOWN OR BREAKING THE BANK.**

WHAT IS SIEM AUGMENTATION?

SIEM augmentation means layering Anomali's Agentic SOC Platform on top of your existing SIEM investment to close specific capability gaps without replacing what is already working.

Modernize your SIEM without migrating. With Anomali, you can keep your current SIEM and processes intact while unlocking faster investigations, broader visibility, and richer context. By adding a high-speed data lake built for intelligence and scale, Anomali extends your existing SIEM's reach and performance without changing the way a security operations center (SOC) works.

Your existing SIEM continues handling compliance, log aggregation, and current workflows. Anomali adds the intelligence layer, the analytics engine, and the AI-driven decision support your analysts need to move faster and see further.

TWO WAYS TO DEPLOY ANOMALI ALONGSIDE YOUR SIEM

OPTION 1: SIT ON TOP	OPTION 2: SELECTIVE OFFLOAD
Anomali becomes your analytics and intelligence layer. Your existing SIEM continues handling compliance and log aggregation — zero disruption, immediate uplift in detection and investigation capability.	Route high-volume, high-cost telemetry — cloud logs, endpoint data — to Anomali's Unified Security Data Lake at flat-rate cost. Your legacy SIEM handles legacy data at significantly reduced cost.
Best for: Organizations that want advanced analytics without touching existing SIEM workflows.	**Best for**: Organizations facing SIEM cost pressure or nearing capacity limits.

THE ANOMALI ADVANTAGE: OPTIMIZE WITHOUT DISRUPTION

Anomali enhances and accelerates a SIEM by pairing it with a scalable, open data lake that feeds intelligence, speed, and automation, while maintaining existing workflows, dashboards, and alerting logic.

No Retraining. No Re-Architecture. No Disruption. Just Optimization.

SEAMLESS COEXISTENCE

Works alongside your current SIEM; alerts, dashboards, and playbooks stay intact.

FULL AND CENTRALIZED VISIBILITY

Consolidates all security and IT telemetry — logs, identities, cloud events, and threat feeds — into one accessible platform, with the ability to retain 7+ years of searchable, hot data at storage level economics.

FLEXIBLE ARCHITECTURE WITH COST-EFFICIENT SCALE

Built on open standards that integrate with any analytics engine, AI technology, or SIEM vendor, giving organizations the flexibility to evolve, adapt, and scale as the security ecosystem grows.

FAST SEARCH AND ANALYTICS

Sub-second queries at petabyte scale across all telemetry enable faster investigation and response.

NATIVE THREAT INTELLIGENCE ENRICHMENT

Automatically enriches all data with threat intel to strengthen triage and prioritization.

GOVERNANCE AND CONTROL

Ensures compliance and audit readiness by retaining 7+ years of hot, fully searchable data, meeting regulatory mandates without relying on costly SIEM storage or archived cold data.

HOW ANOMALI WORKS WITH YOUR EXISTING SIEM

Anomali acts as a power source for your SIEM, fueling it with accessible, enriched data and AI-ready insights.

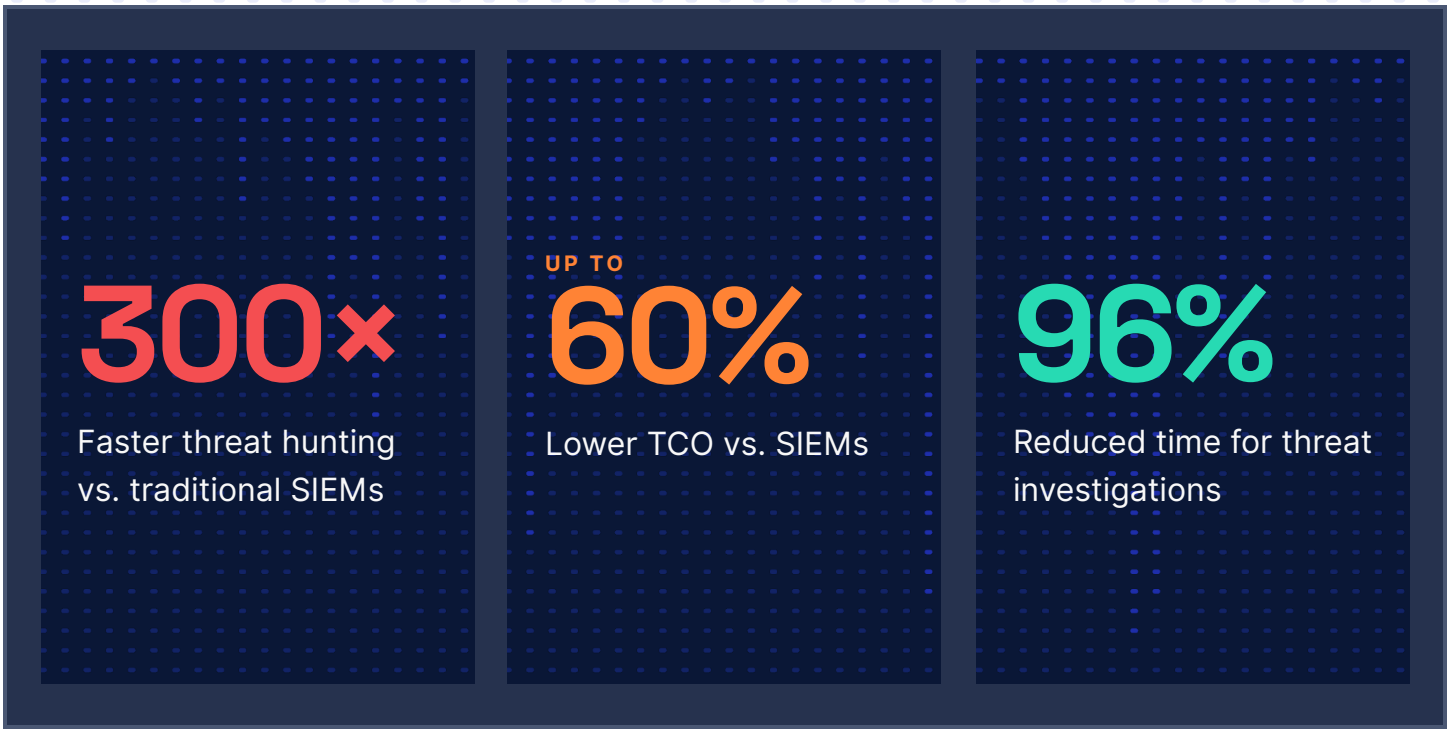
CATEGORY	CURRENT SIEM	WITH ANOMALI
Data Integration	Structured, costly to scale	All data types, storage-level economics
Visibility	Limited by license	Complete telemetry coverage
Search and Correlation	Manual, slow	Sub-second search and automated correlation
Intelligence	Minimal context	ThreatStream Next-Gen enrichment and AI-assisted analysis and reasoning
Workflows	Existing dashboards and alerts	No change; just faster insight across 7+ years of retained data

SIX HIGH-IMPACT USE CASES

Anomali augments where legacy SIEMs consistently fall short. Each of these use cases represents an immediate opportunity to reduce risk, reduce cost, or both.

IOC Correlation at Unlimited Scale	**Retrospective Threat Hunting in Seconds**	**AI-Driven Analyst Triage**
Anomali correlates against billions of indicators with zero performance impact, closing the gap that sophisticated actors exploit by continuously rotating infrastructure.	When a new threat bulletin drops, Anomali searches billions of logs in seconds across years of always-hot data. Reduce threat investigation time by up to 96%. No archive restores, no complex query building, no waiting.	Agentic AI handles enrichment, prioritization, and initial investigation reasoning before alerts reach analysts. Teams spend less time on manual triage and more time on high-value decisions. Value is typically realized within 30

Vulnerability Prioritization	**Rich, Contextual Alert Quality**	**SIEM Cost Reduction**
Correlate CVEs and critical vulnerabilities against live telemetry and real-time threat intelligence. Focus remediation efforts on what is actually exploitable in your environment, not just what the vendor says is critical. Reduce noise, accelerate patching where it matters most.	Generic “bad IP detected” alerts waste analyst time and miss context. Anomali alerts identify the IOC, the threat actor, the campaign, the confidence level, and recommended next actions, enabling automated response based on intelligence rather than manual investigation.	Route high-volume cloud and endpoint telemetry to Anomali’s Unified Security Data Lake instead of expensive SIEM storage. Customers consistently achieve up to 60% TCO reduction vs. SIEMs, without sacrificing visibility or detection capability.



BUILT-IN INTELLIGENCE, WHEN YOU NEED IT

While optimization starts with data and speed, it's amplified by intelligence. With Anomali Agentic AI, SOC analysts can use natural-language queries to explore data, surface patterns, and automatically correlate related events across systems. Agentic AI doesn't just retrieve information; it thinks and reasons across data sets, connecting users, assets, alerts, and threat intelligence to build a clear investigative storyline. It's an added layer of agentic AI that helps analysts work smarter, not differently.

USE CASES IN DEPTH

FULL VISIBILITY WITHOUT REWORK

Many SOCs can't afford to expand SIEM ingestion but still need access to complete telemetry for threat hunting, investigations, and compliance. The Anomali Intelligence-Native Agentic SOC Platform solves this by mirroring and extending the SIEM's view, centralizing all security and IT telemetry in an open data lake that feeds enriched insights back into existing workflows. The result is full visibility across all data sources without the need to reconfigure tools, rebuild workflows, or retrain teams.

FASTER INCIDENT INVESTIGATION

Analysts often wait minutes or even hours for search results during incident response, delaying containment and increasing dwell time. Anomali eliminates these delays with searches done in seconds across petabytes of historical and live data. Analysts can investigate, correlate, and act in real-time while maintaining the same workflows. With AI support, analysts achieve outcomes dramatically faster as the platform reasons through complex investigations and surfaces connections that might otherwise be missed.

THREAT INTELLIGENCE EVERYWHERE

SOC analysts often lack adversary context when triaging alerts, potentially wasting time on low-value signals. Anomali ThreatStream Next-Gen enrichment automatically adds relevant campaign data, risk scores, and related indicators to every alert and dataset — enabling smarter prioritization, reducing alert fatigue, and accelerating decision-making.

CONTINUOUS COMPLIANCE AND RETENTION

Meeting long-term log retention and audit requirements is a growing burden as SIEM storage costs rise. Anomali stores and indexes years of telemetry affordably while keeping it instantly searchable and audit-ready, helping security teams meet compliance mandates without the trade-offs of traditional storage limits.

YOUR SIEM CHALLENGES AND HOW ANOMALI SOLVES THEM

SIEM CHALLENGE	THE IMPACT	ANOMALI SOLUTION
High per-GB ingestion pricing	Costs scale faster than budgets; teams disable log sources, creating blind spots	Unified Security Data Lake at flat-rate cost — ingest everything, pay less
IOC volume limits (2K–15K)	Sophisticated actors rotate infrastructure faster than SIEMs can track	Real-time correlation against billions of IOCs at ingest — zero performance impact
Storage caps (1–2 year hot data)	Historical searches take days; archive restores required	5–7 years of always-hot data; full-speed retrohunt in seconds
No intelligence layer	Every alert is raw; analysts waste hours manually enriching data	Embedded CTI enrichment — every event auto-enriched from the intelligence graph
Reactive detection rules	Threats execute before they're detected; dwell times extend to weeks or months	Proactive, intelligence-led detection with hundreds of pre-built detections from day one

REAL-WORLD IMPACT: BEFORE & AFTER ANOMALI

Scenario: Enterprise healthcare organization. Their SIEM contract renewal came in 38% higher due to data growth. Security team had already disabled 12 log sources to stay within budget, creating known blind spots in cloud and OT environments.

WITHOUT ANOMALI	WITH ANOMALI
SIEM vendor quoted 38% more at renewal — facing an impossible choice: pay more, reduce coverage, or both.	Anomali's data lake ingested all 12 sources plus new cloud logs at 45% less than the SIEM renewal cost.
12 log sources disabled. OT network and cloud workloads unmonitored — AI deployment impossible.	OT, cloud, identity, and endpoint all flowing into unified platform. SIEM handles compliance. Anomali handles detection.
Ransomware lateral movement discovered from an unmonitored OT device. Dwell time: 47 days.	CTI intelligence graph flagged a known-malicious C2 domain from an OT device. Alert enriched and contained in 4 hours.
Compliance audit flagged coverage gaps. CISO explained in writing why log sources were disabled.	Complete telemetry coverage with documented ingestion at next audit. CISO presented a cost savings story — not a justification.

THE COST SAVINGS CASE

Organizations consistently achieve up to 60% total cost of ownership (TCO) reduction when deploying Anomali alongside their existing SIEM. Here's where the savings come from:

INGESTION COST REDUCTION

Route high-volume telemetry to Anomali's flat-rate data lake instead of per-GB SIEM storage. Ingest 10–100× more data at the same spend.

Up to 60% savings

ANALYST EFFICIENCY

AI-driven triage eliminates manual enrichment. Analysts reclaim 30–40% of their time and focus on high-value investigations instead of noise.

3–5× faster triage

INCIDENT RESPONSE SPEED

Faster detection and richer context dramatically reduce dwell time and investigation cost.

96% reduced time for threat investigations

THE FOUR STEPS TO MODERN SIEM OPTIMIZATION

SIEM modernization doesn't have to be a massive overhaul or a risky rip-and-replace project. Organizations see the biggest gains when they take a structured, phased approach. Instead of trying to migrate everything at once, security teams can progressively expand visibility, intelligence, and efficiency. Meanwhile, your current SIEM continues to run as the system of record.

1. ASSESS

UNDERSTAND YOUR DATA AND GAPS

The first step is evaluating your current SIEM environment: data sources, blind spots, and ingestion costs. Many SOCs find that valuable telemetry (cloud, endpoint, identity) isn't captured because of license limits or siloed tools. Anomali helps unify and enrich that data, building a foundation for true visibility without costly ingestion trade-offs.

2. DEFINE

SET CLEAR, MEASURABLE GOALS

Modernization is more than a technology upgrade; it's aligning capabilities with organizational risk tolerance and maturity goals. Anomali works with teams to define KPIs, such as mean time to investigate, data coverage percentage, and alert fidelity, then builds towards a "system of action" model that blends intelligence, automation, and human decision-making.

3. IMPLEMENT

MODERNIZE IN PHASES

A full rip-and-replace introduces risk; a phased rollout ensures continuity. Anomali's modular architecture allows SOCs to start small, integrating one high-impact data source, proving value quickly, and scaling iteratively. This approach delivers early wins, gains stakeholder confidence, and avoids operational gaps.

4. OPTIMIZE

MEASURE, IMPROVE, AUTOMATE

Once visibility and enrichment are in place, the final phase focuses on continuous improvement. With Anomali Agentic AI, teams can track time-to-detect, time-to-contain, and investigation accuracy, while AI models automatically surface correlations and context. This keeps your SOC's efficiency above the industry's average "breakout time" and ensures the platform continuously learns and adapts.

WHY ANOMALI

Anomali is the only platform that unifies a full-featured security data lake, next-generation threat intelligence (ThreatStream Next-Gen), and Agentic AI into a unified experience.

INTELLIGENCE-NATIVE BY DESIGN

Threat intelligence applied at ingest — not bolted on later. Every event enriched in real time, producing high-fidelity detections instead of raw alerts.

UNIVERSAL INGESTION, ZERO LOCK-IN

Any log, any format, any cloud, any vendor — normalized and correlated instantly. No schema constraints, no ecosystem bias, no per-GB ingestion tax.

A NATURAL PATH TO FULL MODERNIZATION

SIEM augmentation is the fastest path to value and the natural on-ramp to a full Agentic SOC Platform. Start by augmenting, then expand at your own pace.

Anomali can make your SOC smarter and your SIEM cheaper today, and we can become the Enterprise Security Brain for your security operations when you're ready.

SEE ANOMALI IN ACTION

Request a Demo