From ThreatStream to Total Threat Protection

4 Ways to Level Up Your Security Posture

You already rely on Anomali ThreatStream, the industry's leading threat intelligence platform. You know the stakes keep rising: more data, more attackers, more cloud. And yes, more tools. But bolting on point solutions only adds complexity and costs. There is a better way.

Anomali has delivered production-grade AI in security long before the hype. Today, our AI-Powered Security Operations Platform brings together ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP in one platform built for speed, clarity, and scale.

You do not have to rip and replace to get more protection. Here are four easy ways to build on the power of ThreatStream and evolve your security operations at your own pace.

Option 1: Customize Threat Feeds for Sharper Defense

Your environment is unique and your intel should be as well. ThreatStream gives you access to more than 200 intelligence sources including ATR enrichment, premium feeds, ISACs, and OSINT.

You can shop streams, tune subscriptions, and instantly activate intel that aligns with your industry, risks, and mission. Fraud, geopolitical threats, brand monitoring, phishing, social media abuse. There is a feed for that.

Small change. Big boost in relevance.

Option 2: Give ThreatStream a Brain Upgrade with Copilot

Copilot turns powerful intelligence into intelligence that works for you.

- Better prioritization with automated risk scoring and enrichment
- Instant clarity with context on vectors, vulnerabilities, and targets
- Visual dashboards with heat maps and timelines for faster understanding
- Shareable insights that make leadership updates simple

One customer reduced investigation and correlation time from 44 minutes to 40 seconds. Faster research means faster response.

Option 3: Supercharge Your SIEM with Anomali Security Analytics

Your SIEM does not have to do everything. Let it focus on what it does best and let Anomali handle what your SIEM was never designed for.

- Hot data stays where it is useful: Keep real-time and recent data in your current SIEM. You can continue to support immediate alerts, investigations, and compliance workflows with no disruption.
- Historical data moves to Anomali: Offload long-term telemetry to the Anomali Security Data Lake for years of cost-efficient retention. We keep all data instantly accessible, not in slow or expensive cold storage.

This unlocks major advantages:

- Complete visibility across your environment without adding point tools
- Look back across more than seven years of activity to uncover dormant threats
- Ultra-fast searches across petabytes of data in seconds, not minutes or hours
- Correlate ThreatStream intelligence with internal logs in real time
- Free your SIEM from storage strain and runaway cost

Your security operations get a massive upgrade while your budget gets a break.

Option 4: Go All-In for Maximum Impact and Lower Cost

When you adopt the full AI-Powered Security Operations Platform:

- Analysts work at superhuman speed with natural language search
- Compute scales on demand for maximum efficiency
- Point tools consolidate into one seamless workflow
- Storage savings go directly back into your security program
- Total cost of ownership decreases while resilience increases

It is the easiest way to go from strong to unstoppable.

No Wrong Moves. Every Option Makes You Safer.

As a ThreatStream customer, you are already ahead of the game. Now choose your next power-up:

1. Add specialized feeds
2. Bring in Copilot
3. Offload your long-term data and supercharge your SIEM
4. Go full platform for complete intelligence, visibility, and speed

Today's threats require visibility, automation, and AI working together. Anomali delivers exactly that in one modern platform that helps your team do more with less.

Ready to level up your security program?

Your Anomali account team is here to help build your perfect next step.

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