ANOMALI

GUIDE

From ThreatStream to Total Threat Protection

4 Ways to Mature Your Security Posture

From ThreatStream to Total Threat Protection

4 Ways to Mature Your Security Posture

Customers of Anomali ThreatStream — the industry's most comprehensive threat intelligence platform (TIP) — are all too aware that the stakes in security have never been higher. What's more, with the advent of AI, the massive proliferation of data volume, and the shift to the cloud, defense has never been more challenging.

Traditional cybersecurity solutions weren't developed with these requirements in mind. Security-conscious companies have been forced to continually add to their toolsets to avoid threats. Unfortunately, bolting on single-purpose tools can lead to complexity, higher costs, and expanding attack surfaces. It's time to completely reimagine the way we approach security.

Anomali has always been a leader in cybersecurity innovation. Anomali integrated production-grade artificial intelligence (AI) into its solutions years before the world became aware of ChatGPT. In addition to ThreatStream, the other components of Anomali's AI-Powered Security and IT Operations Platform combine ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR and TIP capabilities into one easy-to-use, intelligent solution. Cloud-native, serverless, agentless, and AI-Powered, the Anomali platform is purpose-built for the rigors of today's security landscape.

Adding these capabilities to your existing stack can dramatically uplevel your organization's security posture. Fortunately, it's not an all-or-nothing proposition: you can augment ThreatStream with Anomali's groundbreaking AI-Powered Copilot, add Security Analytics to your existing SIEM, or adopt the entire end-to-end Anomali Security and IT Operations Platform. No matter what you choose, you'll come out ahead.

Option 1: Customize Your Threat Feeds for a Targeted Defense

Because your environment is unique, Anomali provides access to more than 200 threat intelligence sources, including curated and enriched feeds from Anomali Threat Research (ATR), premium specialized feeds, information sharing and analysis centers (ISACs), and open-source OSINT feeds.

You can easily evaluate and purchase threat intelligence streams and investigation enrichment offerings from Anomali partners directly within the ThreatStream admin console. You can also customize your included subscriptions.

Specialized threat intelligence feeds

Anomali's partner ecosystem is pre-integrated with leading global research vendors, providing indicators and insights across the threat categories essential for securing your business. This ensures comprehensive intelligence coverage across various industries, verticals, and niche areas, including fraudulent activity, geopolitical threats, adversary monitoring, brand monitoring, phishing, social media threats, and more.

Option 2: Uplevel ThreatStream's Investigation IQ with Anomali Copilot

Anomali's AI-Powered Copilot is ThreatStream's perfect complement. It provides more actionable insights, prioritizes threat intel, aids analysis, and facilitates stakeholder communication.

Raise your threat confidence

Anomali ThreatStream with Copilot can assign a confidence score to each threat based on source credibility, the historical impact of similar threats, and the presence of indicators of compromise (IoCs). The higher the score, the greater the risk.

Next, it adds contextual information, including attack vector details, targeted vulnerabilities, and affected systems, helping you make better decisions based on the likelihood of the threat and its possible impact. Automated enrichment provides additional detail, such as associated IP addresses, domains, and malware hashes.

Integrating this additional context and enriched data into your SecOps workflows lets security teams focus on high-severity threats first, optimizing resource allocation and response time. With the help of Anomali Copilot, ThreatStream continuously updates threat intelligence and severity analysis based on the latest threat data. This real-time approach ensures that organizations stay aware of — and a step ahead of — emerging threats.

See threat summaries

Anomali Copilot with ThreatStream summarizes threat information using visual dashboards. These dashboards provide graphical representations, such as heat maps and threat timelines, that make it easier for security teams to spot trends and patterns at a glance. Viewing key information, such as the type of threat, associated IoCs, potential targets, and geographic spread, all facilitate quick, intuitive analysis.

In addition to helping prioritize, this extra information enables more focused, effective response when integrating with other security tools and platforms, such as SIEM, SOAR, and UEBA — capabilities also included in Anomali's comprehensive Security and IT Operations Platform.

Streamline reporting

Anomali Copilot distills complex threat intelligence into clear, actionable summaries with relevance and potential impact. These reports are great for management, helping business leaders understand the impact and criticality of threats and make informed decisions about resource allocation, policy changes, and incident response protocols.

Option 3: Augment Your SIEM with the Anomali Security and IT Operations Platform

The Anomali Security and IT Operations Platform, including ThreatStream, Copilot, and Security Analytics, will supercharge your existing SIEM, providing enhanced visibility, access to rich historical data, and exceptional speed.

See it all, defend it all

Your organization is exposed and vulnerable if your SIEM doesn't give you visibility into every data source in your environment — every endpoint, server, network, website, cloud application, and device.

Most traditional SIEMs provide only partial coverage, leaving you to add extra tools to achieve comprehensive visibility. The addition of Anomali's Security and IT Operations Platform provides visibility into every data source in your environment right out of the box.

Take a longer look back

Lookback data is critical for comprehensive security. It helps you identify and understand long-term patterns, uncover dormant threats, and investigate breaches that may have originated months or even years ago.

However, traditional SIEMs are designed for near real-time analysis of log data. They usually only provide immediate access to data from the last three to six months of activity, preventing deep retrospective analysis. You'll never know if a malware time bomb was injected three years ago, lurking in the shadows, waiting to deploy.

In contrast, Anomali is purpose-built to collect and store a record of all internally logged activity dating back more than seven years. It doesn't matter whether an event was logged five days or five years ago. Unlike traditional SIEMs that keep older data in cold storage (and make it cost-prohibitive to keep it in hot storage), Anomali's groundbreaking Security Data Lake keeps all data hot and at your fingertips at no extra charge.

Speed up detection, investigation, and response

Speed matters, particularly when your organization is under attack. That's why Anomali's Security and IT Operations Platform is designed to extract meaningful insights from vast volumes of data faster than attacks can unfold.

How fast? Fast enough to search four petabytes of data — up to a billion records — in just 10 seconds. No legacy SIEM can keep up.

Here's how:

Cloud-native architecture: Anomali's agentless, cloud-native design makes it scalable enough to handle petabytes of data without compromising performance. It leverages lossless compression algorithms to reduce data storage requirements. It 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. Anomali's reduces data storage requirements without compromising integrity.

Agentless: Deploy faster and more efficiently with no-installation-required agentless deployment. The simplified architecture makes it easier to manage and scale. Not having agents to update or patch reduces ongoing maintenance. Additionally, agentless deployment reduces your attack surface, decreases endpoint load, and eases compliance headaches.

Integrated Security Data Lake: At the heart of Anomali's revolutionary approach is its integrated Security Data Lake. This powerful feature efficiently manages the exponential growth of security data, providing high-speed collection, processing, and analysis at scale. With Anomali's Data Lake, all of your data is hot.

Simplifying analysis: Another way that Anomali speeds up security operations is by using Copilot's advanced AI and natural language processing (NLP) to enable users of all skill levels to conduct sophisticated threat-hunting tasks simply by asking questions in plain language (it supports over 80 languages!). By eliminating the need to master proprietary query languages or write complicated

detections, Anomali cuts threat research time in half and empowers junior analysts to perform at the level of far more experienced team members.

Imagine asking, "Is this exploit impacting organizations like mine, and if so, where am I at risk?" and receiving an answer almost immediately. One Anomali customer recently reported that using Copilot reduced their investigation and correlation search time from an average of 44 minutes to under 40 seconds.

Match external threats to internal telemetry

You already know that ThreatStream gives you curated access to the world's largest repository of threat intelligence. However, integrating threat intelligence with AI and world-class Security Analytics elevates your security posture to a whole new level.

Imagine investigating a suspicious IP address and seeing relevant high-fidelity threat intel alongside your internal log data in real time, immediately drawing your attention to the connection. This holistic view allows analysts to make faster, more informed decisions, reducing the time from detection to resolution.

Anomali also integrates data from vulnerability assessment tools like Qualys, allowing for risk prioritization based on real-world activity. By leveraging the MITRE ATT&CK framework, Anomali provides deep context across strategic intelligence, enabling analysts to assess and respond efficiently. Also, various sources can be directed to Anomali without increasing SIEM storage, licensing, processing power, or overall budget.

Automating these workflows streamlines processes, letting you quickly ingest, prioritize, enrich, score, and distribute intel to those who need it, such as ISACs. It also eliminates routine tasks, reduces human error, enhances analyst efficiency, lowers costs, and drives faster response.

Option 4: Adopt the Whole Solution to Get Unparalleled Intelligence, Speed, and Scale, While Dramatically Lowering Costs

Adopting Anomali's full platform will transform your security posture for all of the reasons outlined above. However, the benefits don't stop there. Scaling analyst efforts, optimizing compute, and consolidating your security tech stack also translate into significant cost savings.

Help your current team do more while working less

As mentioned earlier, Anomali Copilot's conversational AI enables junior analysts to perform at senior levels using natural language instead of a proprietary query language. It also cuts analysis time in half. These capabilities reduce hiring needs, foster team growth, and ease workloads.

Use resources more efficiently

Anomali's integrated Security Data Lake lets you store only the data you need (saving money on storage costs). Its serverless architecture lets you optimize your use of computing resources by scaling in response to workload demand.

Simplify your stack

Anomali combines ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one efficient platform. It empowers you to bind threat-hunting and security operations into one discrete workflow, eliminating the need for multiple tools.

Save on storage

The integrated Anomali Data Lake saves money because (unlike many competitive offerings) we don't sit on top of another big data provider and we pass the savings back to you, our customers.

Boost your bottom line

Overall, Anomali's comprehensive approach to security operations and cost efficiency delivers enhanced capabilities while significantly reducing your total cost of ownership. This integrated solution empowers organizations to achieve more robust security with streamlined resources.

One Anomali customer recently reported that using Copilot reduced their investigation and correlation search time from an average of 44 minutes to under 40 seconds.

No Matter What You Choose, You Come Out Ahead

As a ThreatStream customer, you already know the power of the industry's leading TIP. Whether you enhance with specialized threat feeds, add Anomali Copilot to your stack, augment your current security operations with Anomali Security and IT Operations Platform, or choose Anomali as an end-to-end solution, you'll substantially strengthen your cybersecurity defenses.

Today's increased data volume, sophisticated threats, and cloud architectures require a tectonic shift in our approach to security. Anomali's AI-Powered Security and IT Operations Platform gives you comprehensive visibility, speed, AI, and world-class threat intelligence in one easy-to-use integrated platform. Anomali provides first-in-market speed, scale, and performance, consolidates your tech stack, and empowers your team to do more with less.

Ready to explore the Anomali difference? Contact your account manager or customer service manager to learn more about how Anomali's Security and IT Operations Platform can transform your organization's cybersecurity.

Security and IT Operations Done Differently.

Anomali is the leading AI-Powered Security and IT Operations Platform that delivers mind-blowing speed, scale, and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

Request a demo to learn more about the Anomali AI-Powered Security and IT Operations Platform.

ANOMALI