ANOMALI

GUIDE

Anomali vs Cyware

5 Ways to Compare and Evaluate

Anomali vs Cyware

5 Ways to Compare and Evaluate

Legacy threat intelligence platforms (TIPs) can't keep up with today's cyber threats as they continue to grow in volume, speed, and sophistication. The modern threat landscape demands a TIP powered by advanced AI, enriched with diverse intelligence sources, and seamlessly integrated into the security workflow.

While they are both TIPs, Anomali ThreatStream and Cyware Threat Intelligence Management take alternate approaches and provide different levels of support for intelligent automation and information sharing.

Cyware offers a range of specialized products designed to work together within its ecosystem, providing a modular approach to security operations. While this introduces an element of flexibility, the modules are disconnected and have no unified interface. Additionally, each product must be purchased and deployed separately.

ThreatStream is part of the Anomali Security and IT Operations Platform, integrating seamlessly with Anomali's AI-Powered Copilot and Security Analytics. It features an intuitive, unified user interface that enables security teams to manage everything from threat intelligence to remediation in one integrated platform.

Here are five other key differences between the two platforms and their potential impact on your security strategy.

1. Superior Intelligence, Enhanced with Context

While Cyware does not come bundled with any premium or proprietary feeds, it is designed to enable security operations teams to collect, manage, and integrate data from customers' (separately licensed) threat intelligence feeds, open source intelligence (OSINT), and internal telemetry data.

Anomali ThreatStream delivers a comprehensive solution, providing access to a curated collection of 200+ diverse threat intelligence sources. Handpicked by the Anomali Threat Research (ATR) team over the span of a decade, these sources include proprietary feeds sourced by Anomali, OSINT feeds, specialized premium feeds (expandable through the Anomali App Store), and feeds from information sharing and analysis centers (ISACs).

While the quantity, quality, and diversity of threat intelligence data sources is important, the ability to transform that data into actionable intelligence is also critical. ThreatStream uses Macula, Anomali's proprietary ML engine, to enrich threat data, adding context that informs decision-making.

ThreatStream does this by:

- Filtering, deduping, and scoring data based on relevance, credibility, and potential impact
- Analyzing, predicting, and classifying cyber threats
- Automating threat scoring

As a result, ThreatStream delivers an enhanced layer of automated cyber defense benefits, including:

- Reducing false positives to remove dangerous and time-consuming distractions
- Eliminating alert fatigue through incident scoring, filtering, and prioritization to minimize pressure on your cyber defenses
- Making the most efficient use of limited analyst resources
- Automating enrichment of intelligence from external sources

Macula operates in the background, processing, analyzing and scoring potential threats on ingest. ThreatStream's intelligent, intentional defense comes from combining this deep contextual analysis with curated access to the world's largest threat intelligence repository, based on over a decade of threat research.

The upshot: Anomali ThreatStream provides actionable intelligence that significantly reduces time spent on distractions, such as false positives and low-priority alerts.

2. Collaboration and Intelligence Sharing

Cyware enables secure collaboration and intelligence sharing among teams and partners but requires the purchase of multiple products for comprehensive functionality. Cyware's collaboration stack includes Intel Exchange, Collaborate, Respond, and Orchestrate — each module adding specific sharing or response features. While this model may provide tailored options for larger organizations, the additional expense and deployment complexity is a hefty trade-off.

Anomali ThreatStream takes a more sophisticated and secure approach to collaborative intelligence by allowing organizations to customize and control intelligence distribution in a granular fashion. Whether establishing two-way sharing among industry peers or implementing one-way flows from ISACs or parent organizations to downstream partners, every sharing relationship is explicitly defined and secured.

Automated ML-driven enrichment: Rather than depending solely on community contributions, ThreatStream uses ML to automatically enrich and validate threat intelligence. This automated approach includes advanced scoring and prioritization mechanisms that reduce the risk of errors or malicious activity.

Trusted Circles framework. Instead of open communities, ThreatStream enables organizations to create defined, secure networks for intelligence sharing. These Trusted Circles can be configured to support:

- Industry-specific collaboration among vetted peers
- Geographic or vertical-specific intelligence sharing
- Parent organization distribution to downstream partners
- ISAC integration for critical infrastructure protection

The bottom line: ThreatStream enhances threat intelligence sharing by leveraging ML-validated data and controlled sharing networks built on industry standards like STIX/TAXII.

3. Streamlined Automation and Integration

TIP workflow automation is critical because it transforms overwhelming volumes of threat data into actionable intelligence while eliminating time-consuming manual processes. Particularly when dealing with large and diverse intelligence feeds from a broad range of sources, automation enables analysts to stay focused on what they do best — strategic analysis. Automation also makes it easier to optimize threat intelligence to suit an organization's unique risk profile.

Cyware's approach to automation and integration is centered around Cyware Orchestrate, which focuses on workflows and playbooks. However, organizations must make additional investments and manage the integration separately since Orchestrate is a standalone product. This slows deployment and increases costs for teams looking to achieve fully automated intelligence workflows while controlling budgets.

Cyware playbooks allow security teams to create custom workflows — a structured approach to threat response and remediation. However, this rigid framework can become limiting when teams face variable, complex threats that require sophisticated workflows.

Anomali ThreatStream delivers robust automation and orchestration capabilities, facilitating workflows across your entire security infrastructure. Based on high-quality curated threat intelligence, it confers immediate value through:

- Built-in integration capabilities that ensure broad compatibility with existing security controls — including firewalls, SIEMs, proxies, DNS, messaging systems, and endpoint protection platforms — reducing incident response times by up to 30%
- Automated filtering, prioritization, and distribution of threat intelligence by relevance and criticality, enabling analysts to work more efficiently
- Flexible deployment options supporting on-premises, air-gapped, or cloud environments

The takeaway: ThreatStream enriches security events with relevant threat data, providing automation and context to help analysts quickly understand and respond in real time.

4. Investigation and Incident Management

Cyware's built-in case management enables teams to track and respond to incidents within the platform. However, its inability to integrate with external case-management tools means teams must purchase additional solutions to connect its incident tracking with other systems.

Anomali ThreatStream offers investigative tools that help analysts research threat actors, observables, and other intelligence, enabling them to identify and document relationships. At the incident level, ThreatStream addresses case management through investigation and tracking capabilities, providing detailed, incident-specific workflow tools. It also offers built-in case management, integrates with external help desk, SIEM, and SOAR platforms — such as ServiceNow and XSOAR — and accelerates workflows through Anomali Copilot.

The result: Unlike Cyware, Anomali ThreatStream provides native flexibility and seamless connectivity with existing case-management tools, eliminating the need for extra purchases.

5. Advanced AI for Adaptive Threat Analysis

Agility is essential in today's rapidly shifting cybersecurity landscape. To adapt to evolving threats, security teams need solutions that provide immediate, sophisticated analysis — a level of responsiveness that only advanced ML and AI can provide.

Cyware integrates machine learning for threat scoring, AI-driven confidence scoring, and automated threat correlation. Its AI-powered Quarterback interface emphasizes workflow automation and streamlined operations through large language model (LLM) integration. While effective for operational efficiency, Cyware's AI capabilities focus more on process automation than ThreatStream's dynamic threat prioritization and advanced analytical insights.

ThreatStream uses Macula for integrated scoring and prioritization. This functionality enables teams to assess threats more quickly and effectively without the need for additional integration. ThreatStream users can further enhance their security operations with Anomali's GenAI Copilot, which delivers deeper insights, analysis, and automation. Copilot's advanced AI-driven analysis streamlines intelligence prioritization and simplifies stakeholder reporting.

The bottom line: While both platforms offer ML and AI capabilities, ThreatStream's Macula and Copilot provide more sophisticated threat analysis and dynamic prioritization than Cyware's automation-focused approach.

The Clear Choice for Modern Security Operations

Anomali ThreatStream delivers a complete, scalable threat intelligence solution that enhances outcomes across the board. With premium intelligence feeds, superior AI capabilities, automation, secure collaboration features, and sophisticated threat modeling, it empowers organizations to stay ahead of evolving threats.

ThreatStream seamlessly integrates with the other components of Anomali's industry-leading AI-Powered Security and IT Operations Platform, which combines ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one easy-to-use solution at a fraction of the cost of other solutions.

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