

FROST & SULLIVAN

ANOMALI

2022
MARKET
LEADER

GLOBAL THREAT INTELLIGENCE
PLATFORMS INDUSTRY

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Anomali excels in many of the criteria in the Threat Intelligence Platforms space.

AWARD CRITERIA	
Growth Strategy Excellence	Technology Leverage
Implementation Excellence	Price/Performance Value
Brand Strength	Customer Purchase Experience
Product Quality	Customer Ownership Experience
Product Differentiation	Customer Service Experience

Anomali: a leader in the evolution journey of Threat Intelligence Platforms

Over recent years, cyberattacks have grown in sophistication and volume: threats are harder to detect and are more targeted, dynamic, damaging, and diverse in nature. Threat actors have become more specialized and organized in recent years; the growing number of attacks by career criminals and nation-state groups has created concern among organizations of all sizes and across all industries.

“Keeping up with market trends has certainly paid off for Anomali – the different information inputs have allowed it to make a key strategic move: expanding its TIP to encompass a broader Extended Detection and Response (XDR) focus. Anomali’s ThreatStream, a cloud-native SaaS offering, is the market-leading TIP/threat intelligence management solution.”

**- Clara Dello Russo,
Research Analyst**

This complex and ever-evolving threat landscape has led to an overload of information and alerts that security teams cannot keep up with. Furthermore, security teams must manage more tools and data while often being under-resourced because of a shortage of qualified security professionals.

In this context, threat intelligence solutions can be a key asset for organizations, enabling faster and more informed security decision making. Threat Intelligence Platforms (TIPs) can collect, aggregate, and organize data from different sources, thus allowing security teams to deal with the information overload.

However, the evolution of the threat landscape, as well as the challenges presented by adjacent market segments such as the Cyber Threat Intelligence (CTI) space, has led to TIP's traditional value proposition becoming insufficient.

Anomali, a US-based cybersecurity company founded in 2013, was one of the first TIP providers to identify the need to evolve. The company continually tracks market trends, leveraging analyst reports and competitive intelligence. It also regularly engages with customers and prospects to better understand the market, as well as potential areas of improvement for its products. Keeping up with market trends has certainly paid off for Anomali – the different information inputs have allowed it to make a key strategic move: expanding its TIP to Threat Intelligence Management and encompass an even broader focus on the adversary, including introducing an Extended Detection and Response (XDR) solution.

Anomali's ThreatStream, a cloud-native SaaS offering, is the market-leading TIP/threat intelligence management solution. However, it is only one component of the company's intelligence-driven threat detection and response platform, which also includes Match (threat detection) and Lens (threat insights). With The Anomali Platform, the company has been able to evolve its value proposition, in line with the changing needs of the market.

ThreatStream – the core of The Anomali Platform

ThreatStream, a core part of The Anomali Platform, is the company's TIP/Threat Intelligence Management solution. It automates the collection and processing of raw data and transforms it into actionable threat intelligence for security teams. Moreover, it profiles adversaries and allows users to securely collaborate with internal colleagues and peers to speed threat identification and receive advice to help manage threats.

ThreatStream can ingest and normalize billions of Indicators of Compromise (IoC). To minimize false positives, Anomali's machine learning algorithm, Macula, assigns a confidence score to each IoC, thus reducing the volume at the point of ingestion. The scoring engine identifies false positives, but customers can also provide input and contribute to the noise reduction process. This capability is essential for the security teams that need to deal with information overload with insufficient security resources.

ThreatStream also harnesses machine learning and artificial intelligence to enrich IoCs with context, using reputation, WHOIS data, DNS history, and port behavior-based models. Therefore, by leveraging the

platform, users can investigate, enrich, and automatically associate IoCs with strategic intelligence – something that is crucial for any organization looking to deal with the current threat landscape. Today, organizations need more than IoCs to effectively prevent and address cyberattacks; they need access to relevant intelligence that provides context.

Making sure that customers receive the most relevant intelligence is of utmost importance to the Anomali team. For that reason, ThreatStream includes two core features that help to tailor intelligence to the specific

ThreatStream's innovative capabilities and customer focus have allowed Anomali to build a strong brand over the years – Anomali is one of the most renowned vendors in the threat intelligence space. Its extensive partnership network is solid evidence of that: the leading CTI providers' feeds are available for Anomali's customers via the Anomali Preferred Partner (APP) Store."

**- Clara Dello Russo,
Research Analyst**

needs of a customer: *Intelligence Initiatives*, which provides a foundational guide for organizations to integrate the CTI (Cyber Threat Intelligence) lifecycle as part of their working process to reach organizational goals, and *Rules*, which finds relevant data based on keywords or advanced search queries configured by the users themselves. As a result, customers only receive filtered data that is relevant to them.

The key to a successful brand: focusing on customers

ThreatStream's value proposition resonates extremely well with customers, as Anomali's high net promoter score confirms. The company's outside-in approach to product development is vital for this success: Anomali's executive team continually meets with customers to understand their needs and how the company's solutions can address their challenges and guarantee high ROI. In fact, Anomali's portfolio is purpose-built to deliver on differentiated use cases, as defined by the company's target customers: Chief Information Security Officers (CISOs), Security Operations Centers (SOCs), and threat analysts, among others.

The company's customer focus is not limited to product development processes. Anomali wants its more than 1,500 customers worldwide to have a positive experience throughout the whole product cycle, with its Customer Success Organization (CSO) serving as an extension of customers' security teams. The CSO is integrated by cybersecurity veterans with expertise in different areas of threat intelligence; it offers a variety of services to help customers successfully deploy their threat intelligence programs, ensuring that they receive full value from Anomali's solutions.

ThreatStream's innovative capabilities and customer focus have allowed Anomali to build a strong brand over the years – Anomali is one of the most renowned vendors in the threat intelligence space. Its extensive partnership network is solid evidence of that: the leading CTI providers' feeds are available for Anomali's customers via the Anomali Preferred Partner (APP) Store. The company offers over 250 open source, freemium, and premium intelligence feeds, while customers can also submit their own intelligence to the platform.

Anomali believes that building and investing in an innovative ecosystem of technology partners is essential to delivering exceptional business outcomes for customers. For that reason, it partners not only with threat intelligence feed vendors, but also with ISACs and ISAOs, as well as other security companies offering SIEM, SOAR, and EDR solutions¹. The result: Anomali currently has more than 180 supported partners as part of its Technology Partner Program (TPP).

¹ Acronyms and terms defined: ISACs (Information Sharing and Analysis Centers), ISAOs (Information Sharing and Analysis Organizations), SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), and EDR (Endpoint Detection and Response).

Conclusion

Although Anomali has traditionally been the market leader, it has not rested on its laurels. The company's ongoing market analysis helped it to understand that TIPs needed to go a step further to remain competitive. By expanding its TIP to a broader Threat Detection and Response focus, Anomali has been able to maintain its leadership position, while also providing an answer to the needs of its customers. With its strong overall performance, Anomali earns Frost & Sullivan's 2022 Global Market Leadership Award in the threat intelligence platforms industry.

What You Need to Know about the Market Leadership Recognition

Frost & Sullivan's Market Leadership Award recognizes the company that achieved the greatest market share resulting from outstanding performance, products, and services.

Best Practices Award Analysis

For the Market Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Growth Strategy Excellence: Company demonstrates an ability to consistently identify, prioritize, and pursue emerging growth opportunities

Implementation Excellence: Company processes support efficient and consistent implementation of tactics designed to support the strategy

Brand Strength: Company is respected, recognized, and remembered

Product Quality: Products or services receive high marks for performance, functionality, and reliability at every stage of the life cycle

Product Differentiation: Products or services carve out a market niche based on price, quality, or uniqueness (or some combination of the three) that other companies cannot easily replicate

Technology Leverage: Company is committed to incorporating leading-edge technologies into product offerings to enhance product performance and value

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers are proud to own the company's product or service, and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and of high quality

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at <http://www.frost.com>.

The Growth Pipeline Engine™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.

[Learn more.](#)

Key Impacts:

- **Growth Pipeline:** Continuous Flow of Growth Opportunities
- **Growth Strategies:** Proven Best Practices
- **Innovation Culture:** Optimized Customer Experience
- **ROI & Margin:** Implementation Excellence
- **Transformational Growth:** Industry Leadership



The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- **Mega Trend (MT)**
- **Business Model (BM)**
- **Technology (TE)**
- **Industries (IN)**
- **Customer (CU)**
- **Geographies (GE)**

