

2021 Frost & Sullivan Customer Value Leadership Award

The Global Cyber Threat Intelligence Market
Excellence in Best Practices

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. Intel 471 excels in many of the criteria in the Cyber Threat Intelligence space.

AWARD CRITERIA	
<i>Business Impact</i>	<i>Customer Impact</i>
Financial Performance	Price/Performance Value
Customer Acquisition	Customer Purchase Experience
Operational Efficiency	Customer Ownership Experience
Growth Potential	Customer Service Experience
Human Capital	Brand Equity

Financial Performance

Intel 471 is a cyber threat intelligence (CTI) vendor that specializes in adversary and malware intelligence. The company enables its customers to adapt to the rapidly evolving threat landscape by providing them with relevant and curated information. Intel 471 is a bootstrapped company with no debt. Its operating expenses and research & development initiatives are funded by customer revenue. Founded in 2014, the company has already established itself as one of the most competitive vendors in the cyber threat intelligence market. It has grown its annual revenues by an average of 45% over the last three years, a rate well above the industry average. Intel 471’s ability to disrupt the market without reliance on investments from private equity firms is a testimony to the competitiveness of its cyber threat intelligence offering. Overall, Intel 471’s growing success and financial performance speak to the value its customers and prospects see in its product.

Growth Potential

Most of Intel 471’s competitors have chosen to position themselves as SaaS (software as a service) vendors and invest in expanding the use cases for their intelligence platforms. While this enables such companies to address a broader market, they may be at risk of losing the focus on their core cyber threat intelligence capabilities. Intel 471’s main objective is to provide best-in-class cyber threat intelligence that customers can seamlessly operationalize in their environments. Although Intel 471

“As opposed to some of its competitors that predominantly track tactical indicators, Intel 471 specializes in monitoring malware families and actors’ tooling. The company’s focus on the causes rather than consequences of an attack allows Intel 471’s customers to take on a truly preventative approach to cyber security.”

- Mikita Hanets, Research Analyst

enables customers to consume intelligence on its proprietary platform, the company goes an extra mile to provide its customers with context-rich machine-readable feeds accessible via an API. Such an approach allows Intel 471 to meet clients' operational requirements and fit into their security stack while maintaining its core focus on the quality of cyber threat intelligence rather than SaaS functionality. In light of the growing competition in this market and the strategy adopted by most of its competitors, Intel 471’s differentiated focus positions the company well

for continued success in the coming years. Apart from attracting a growing number of customers, the company will see substantial growth due to partnerships with other security vendors that are seeking to incorporate Intel 471 intelligence into their solutions.

Operational Efficiency

A growing number of organizations recognize the limitations of reactive cyber defense and consider threat intelligence as a critical enabler of a more proactive approach. While threat intelligence can power organizations on their journey to predictive and preventative security, not all threat intelligence is well suited for this purpose; some threat intelligence can only reveal information about past attacks. Although there is a clear benefit in utilizing such information, it provides only part of what organizations need if they intend to stay a step ahead of cyber adversaries. Intel 471 understands the limitations of threat intelligence solutions that rely on customer threat telemetry and is committed to developing cutting-edge technologies that bring additional value to its clients. As opposed to some of its competitors that predominantly track tactical indicators, Intel 471 specializes in monitoring malware families and actors’ tooling. The company’s focus on the causes rather than consequences of an attack allows Intel 471’s customers to take a truly preventative approach to cyber security.

Customer Purchase Experience

Intel 471 recognizes the challenges that organizations face in operationalizing threat intelligence. Threat feeds are large in volume. They often contain irrelevant information and false positives that lead to wasted analyst time and the involvement of other organizational resources. In addition, poorly curated threat intelligence may inadvertently harm an organization by diluting analysts’ focus on the information that matters. In contrast to threat intelligence vendors that provide their customers with generic threat data collected in bulk, Intel 471 develops a unique intelligence collection plan based on the individual needs of its clients. The company has a very structured approach to determining customers’ intelligence requirements and goes above and beyond to ensure that its clients receive a subset of only relevant and tailored threat data with few to no false positives.

Customer Service Experience

Intel 471 provides excellent customer service. The company is committed to meeting the unique intelligence requirements of each customer by not only establishing an intelligence collection plan but also providing a tailored service to its clients throughout the customer journey. All Intel 471 customers receive support from a dedicated member of the collection management team, which is comprised of seasoned information security professionals whose responsibility is to understand the client's intelligence needs and serve as the single point of contact at Intel 471. If the customer is not sure about their intelligence use cases, a collection manager will help the client determine the key areas where threat intelligence can benefit their organization. Intel 471 is also committed to helping its clients build a more mature intelligence program as a result of a close business relationship.

Customer Acquisition

Intel 471 acquired most of its largest clients through word-of-mouth recommendations. The fact that Intel 471's customers willingly recommend the company's solution to its partners suggests remarkable product and customer service leadership. At the same time, with threat intelligence being a relatively new area of cyber security, vendors in this market face significant pressure from prospects and customers to demonstrate a return on their investment. As opposed to the benefits of traditional categories of security products, the benefits of cyber threat intelligence solutions are hard to quantify. Intel 471 addresses this problem by determining clients' unique intelligence requirements and delivering on the promise of meeting them. Intel 471 provides its customers with a clear view of how a particular intelligence deliverable relates to their unique needs.

Conclusion

Intel 471 is a fast-growing cyber threat intelligence vendor with a strong value proposition. While the company is relatively young, the competitiveness of its offering has enabled Intel 471 to acquire security-conscious customers and rapidly grow its recognition in the cyber threat intelligence market. Intel 471's core differentiators are strong adversary and malware intelligence capabilities coupled with an exceptional focus on meeting clients' unique intelligence requirements. For its strong overall performance, Intel 471 is recognized with Frost & Sullivan's 2021 Customer Value Leadership Award.