ThreatQuotient Recognized for

2021

Competitive Strategy Leadership

Global Extended
Detection and Response Industry
Excellence in Best Practices

FROST & SULLIVAN

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. ThreatQuotient excels in many of the criteria in the XDR space.

Powering XDR as a Movement

Extended detection and response (XDR) is generating a tremendous deal of interest from security operations professionals, becoming one of the most discussed topics in the cybersecurity industry. Over the past few months, vendors have released a spree of announcements signaling their readiness to deliver XDR capabilities, with many more preparing to unveil their new products. In such a competitive environment, Frost & Sullivan notes that it is more important than ever to see past marketing claims.

Frost & Sullivan defines XDR as a vendor-agnostic solution that aggregates data from a wide range of security controls (e.g., endpoint, cloud, network), enabling security teams to detect, investigate, and respond to threats in a holistic manner. In light of the shortage of cybersecurity professionals and the siloed nature of the market, XDR has emerged to deliver on three key promises: cross-layered detection and response, third-party integration, and meaningful automation[1]. Although more than a dozen vendors already claim to have a commercially viable product, most solutions fall short of meeting Frost & Sullivan's full definition of XDR. At this point, XDR represents a product vision or a destination towards which the market is evolving. However, many vendors do not hesitate to position their solutions as full-blown XDRs, at least insofar as press releases and marketing materials are concerned. While such an approach may help vendors generate leads, customers may be quite disappointed to learn that the benefits of these solutions simply do not fully coincide with market claims.

[1] *XDR: The Journey Towards Revolutionizing Cybersecurity Operations and Generating Triple-Digit Growth in the Coming Years - Frost & Sullivan, 2021.*

> *"In contrast to most early XDR offerings, the ThreatQ Platform enables security operations teams to ingest data from a wide array of security controls, whether they are from a single vendor or multiple providers. The company has an extensive list of out-of-the-box integrations that allow ThreatQuotient's customers to start benefiting from those partnerships in a matter of minutes."*
>
> ***- Mikita Hanets, Research Analyst***

Headquartered in the United States and operating since 2013, ThreatQuotient's innovative security operations platform supports a wide range of use cases. The company follows a differentiated XDR strategy. In contrast to other competing vendors that claim to have XDR capabilities but fall short on delivery, ThreatQuotient recognizes that XDR is a destination.

At the end of 2020, chief marketing officer Marc Solomon published an article on powering XDR as a movement, outlining ThreatQuotient's strategy[2]. The company expressed its commitment to supporting XDR use cases while abstaining from calling itself an XDR provider. As customers and the industry more broadly learn about vendor offerings and the market noise fades, Frost & Sullivan believes that ThreatQuotient will emerge as a transparent and reliable vendor that supports security operations aligned with XDR's vision.

Powering XDR as an Open Platform

In contrast to popular opinion, XDR is not simply an evolution of endpoint detection and response. Vendors from different cybersecurity markets are simultaneously evolving towards XDR to address growing customer demand for more efficient and streamlined security operations. While vendors are still early in their XDR journey, companies that operate in this market segment have distinct competitive differentiators. For example, most vendors focus on enabling cross-layered detection and response in their ecosystems - but lack deep integrations with third-party security controls or data. While this might not be a problem for an organization whose security stack is comprises solutions from a single vendor, this is rarely the case for most customers. Since organizations typically follow a best-of-breed strategy, integrations are truly imperative to fulfilling the XDR vision.

Frost & Sullivan's own research positions ThreatQuotient is clearly distinct, as it originated from the threat intelligence platform (TIP) space. TIPs emerged to address use cases (such as aggregation and threat intelligence sharing), subsequently evolving into platforms that power security operations teams with knowledge and tools for effective investigation and response processes. ThreatQuotient has substantial experience in ingesting, normalizing, and correlating both internal and external threat data. Frost & Sullivan notes that ThreatQuotient's background as a TIP vendor allows it to address the limitations of early XDR solutions by opening them up to integrations. The company positions its solution as a security operations platform that empowers customers to embrace XDR by "serving as a central repository for data and intelligence from internal and external sources."[3]

Unlike most early XDR offerings, the ThreatQ Platform enables security operations teams to ingest data from a wide array of security controls - whether from a single vendor or multiple providers. The

[2] *Enabling eXtended Detection & Response (XDR) – ThreatQuotient, 2020. https://www.threatq.com/documentation/ThreatQ-Enabling-XDR.pdf*
[3] *ibid.*

company has an extensive list of out-of-the-box integrations that allow ThreatQuotient's customers to start benefiting from those partnerships in a matter of minutes.

Powering XDR to Simplify Security Operations

The ultimate purpose of XDR is to facilitate simpler and more effective security operations. The journey towards this objective is not limited to a cross-layered correlation of threat data and integrations with third-party solutions. While aggregating threat telemetry from a range of security solutions is the first step towards XDR, more extensive and complex data does not necessarily lead to better security outcomes. If anything, in the absence of the right instruments, it will make security operations even more difficult.

Analysts need the right tools to investigate alerts, understand relationships between indicators of compromise, and determine their severity. Most XDR vendors only begin to equip their customers with tools that simplify security operations. While predominantly focusing on data from their ecosystem, many XDR vendors also lack the experience to address security operations use cases in line with the promises of XDR. ThreatQuotient, on the other hand, already enables advanced threat hunting, investigations, and incident response on its platform. Apart from having powerful technology under the hood, the company goes the extra mile to create visual, simple-to-navigate interfaces. Organizations can easily pivot from alert triage to learning strategic information about a known advanced persistent threat behind an attack. Should the analyst want to take action, they can do so from the ThreatQ Platform - all without having to switch over to a different management console.

ThreatQuotient also goes the extra mile to enable automation. While most XDR vendors focus on creating playbooks, they typically overlook the complexity of threat data. Because of that, ThreatQuotient takes a data-driven approach to simplifying detection and response. In 2021, the company announced the introduction of the ThreatQ TDR Orchestrator. ThreatQ TDR Orchestrator shifts the traditional focus of automation from merely following playbooks to learning from the outcomes of security processes. It allows organizations to use historical data to improve the timeliness and appropriateness of playbook activation and facilitates more effective detection and response.

Conclusion

Extended detection and response (XDR) is generating significant interest due to its ambitious promise to solve security operations challenges. Although many vendors claim to have an XDR product, they clearly fall short of meeting the definition of XDR and only partially address its use cases.

ThreatQuotient's innovative platform positions itself as a company that will power the industry evolution towards the XDR vision. The company's vendor-agnostic security operations platform already outperforms most early XDR offerings by enabling the correlation of threat data, integrating with a wide range of third-party solutions, and taking a data-driven approach to automation.

With its strong overall performance, ThreatQuotient earns the 2021 Frost & Sullivan Global Competitive Strategy Leadership Award.

What You Need to Know about the Competitive Strategy Leadership Recognition

Frost & Sullivan's Competitive Strategy Leadership Award recognizes the company with a stand-out approach to achieving top-line growth and a superior customer experience.

Best Practices Award Analysis

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

Strategy Innovation

Strategy Effectiveness: Effective strategy balances short-term performance needs with long-term aspirations and overall company vision

Strategy Execution: Company strategy utilizes Best Practices to support consistent and efficient processes

Competitive Differentiation: Solutions or products articulate and display unique competitive advantages

Executive Team Alignment: Executive team focuses on staying ahead of key competitors via a unified execution of its organization's mission, vision, and strategy

Stakeholder Integration: Company strategy reflects the needs or circumstances of all industry stakeholders, including competitors, customers, investors, and employees

Customer Impact

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 proudly 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 high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

© Frost & Sullivan 2021

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™

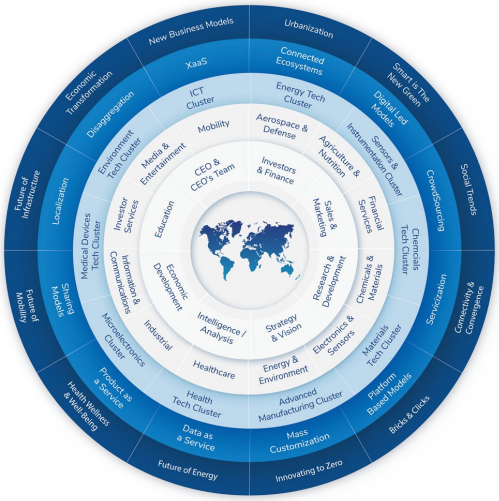
Frost & Sullivan's proprietary model to systematically create on-going growth opportunities and strategies for our clients is fuelled by the Innovation Generator™. Learn more.

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 six 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)

© Frost & Sullivan 2021