FROST & SULLIVAN

EXPEL

2022 ENABLING TECHNOLOGY LEADER

GLOBAL MANAGED DETECTION AND RESPONSE 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. Expel excels in many of the criteria in the global MDR space.

Expel – Fostering Growth through Innovation and Creative Thinking

The cybersecurity industry has been facing a growing problem in recent years: the lack of skilled professionals to cover unfilled positions globally. In light of this issue, organizations have been looking for ways to automate the processes of threat detection and response. The new generation of security solutions promises to deploy machine learning and artificial intelligence to counteract the increasing deficiency of personnel. Currently, security vendors can provide capabilities for the integration of playbooks, behavior-based analytics and threat detection, and other tools to improve the performance of the security stack.

Managed Detection and Response seeks to answer the industry's plea for skilled professionals, visibility over the expanding security perimeters, and drive for automation. MDR leverages the latest technology developments to provide 24/7 monitoring through the entire security ecosystem. The goal of machine learning and automation within MDR is not to replace human labor, but to complement and enhance it, to unlock its full potential. The result is a combination between the expert critical thinking skills and decision-making delivered by the MDR provider's security team, with the computers' capability of detecting changes in patterns and behaviors across colossal volumes of data. Security personnel can dedicate more time to the things that matter, while machine-learning algorithms take on the tedious tasks.

Expel is a Virginia-based cybersecurity company that perfectly understands the careful balance and symbiotic relationship between automation technology and skilled professionals. Expel was founded in

2016, which makes the company a relative newcomer in an industry with vendors that have been delivering security solutions for a few decades. Nonetheless, Expel is one of the leading vendors in the Managed Detection and Response Frost Radar by Frost & Sullivan, with above-average growth in an already booming market.

Expel was born out of the co-founders' necessity to deal with three of cybersecurity's problems: alert fatigue from dozens of disconnected security products, lack of security talent globally, and the apparent failure of MSSPs to deliver on their promises. Since its founding, the company has secured a total of $257.9 million in funding and has grown beyond the borders of the US to deliver MDR services in the European, Asia-Pacific, and Latin American markets.

Technology that Enhances Analysts and Unlocks their Potential

Alert fatigue is a primary concern for cybersecurity professionals. The innate tediousness of going through thousands of false alerts before getting to a real one is one of the factors that drove the inception and later adoption of MDR as a solution category. Expel is keenly aware of this overarching cybersecurity issue, and uses a combination of a proprietary platform and a managed alert process to surpass it and deliver a world-class MDR service.

Expel's most meaningful tool in its arsenal is the Expel Workbench™ platform. The vendor delivers its services through this transparency-focused platform that aims to provide a vehicle for its analysts to focus on performing high-quality decision-making. Expel tasks its analysts with asking investigative questions first. What is this activity? Where is it? When did it start? How did it start? And finally, what does the customer need to do? The Expel Workbench provides analysts with many tools to automatically answer these questions before they need to dive deep into an alert.

The first step of any investigation involves triaging alerts or other signals, focusing on the 'what' question. Expel's bots, Josie™ and Ruxie™, enrich the alerts with information coming from the customers' environment, perform automated alert triage to detect false positives, and provide more context in case the analysts need it. Once this step is complete, the analysts have three options. They can dismiss it as benign, decide it represents a threat, or investigate further. The Expel Workbench provides tools and enhances the analysts' capabilities to uncover more about the alert. Analysts can take advantage of the platform's integrations, querying the customers' security solutions for more information through the investigative actions on the platform, or get the help of Ruxie to run additional automated actions.

If the alert is declared an incident after the triaging or investigative processes, Expel will focus on determining the level of compromise, answering more investigative questions. How many hosts are affected? When did it start? And most importantly, will decide how to mitigate and neutralize the threat, and will initiate automated remediation if the situation warrants it. Regardless of the outcome, Expel notifies the customer about the result of the investigation. If the alert turns out to be false and the activity is deemed benign, Expel will provide a close category and reason. Expel also categorizes some alerts as interesting or potentially risky, and will also notify customers about them with an explanation for the categorization.

In this way, Expel leverages technology to take a step-by-step approach to managed detection and response. By making clever use of the platform, coupled with machine learning and automation, the vendor enhances and augments the analyst's abilities. Through the Expel Workbench, the vendor provides its team and its customers with the tools to detect and respond to threats while focusing on meaningful alerts, and avoiding fatigue and tedious tasks.

A Commitment to Research and Innovation

The Expel Workbench has extensive visibility over the entire security stack to provide more information to analysts for their investigations. Expel extends its platform's reach and control over the cloud and SaaS applications through the use of API integrations with existing customer technology. Expel's MDR service can connect with a growing list of over 80 security tools, including endpoint, SIEM, network, cloud, and SaaS apps. These integrations provide essential support for analysts that need to run investigative actions or automated requests on the platform. They also enhance the value proposition for customers that have a stack of security solutions in place. In addition to this out-of-the-box integration, the company makes it easier with an onboarding process that takes a matter of hours.

In a bid to commit to the development of new technology and adapting to new and changing industry's standards, Expel spends a significant portion of its revenue on R&D. Over the past few years, Expel has boosted its MDR service with the inclusion of the MITRE ATT&CK framework alignments, ServiceNow and OpsGenie integration, a NIST CSF dashboard with importing and exporting capabilities, and proprietary cloud-native detections that have allowed the company to expand its cloud services across AWS, Azure, and GCP.

Expel also supports its platform with a Managed Phishing Service, which provides automated triaging of suspected emails and automated remediation to quickly stop phishing attempts. The tool goes beyond the email and integrates with the customers' EDR solution to reconstruct the impact of the phishing attempt. Having the complete story allows Expel analysts to detect every compromised user, and check if they entered any credentials, inadvertently ran any executable files, or downloaded malicious attachments. After the exhaustive investigation, the company delivers a report with detailed recommendations and an actionable course on remediating the incident.

Expel's roadmap includes Vulnerability Management capabilities and enhancements in its container security for Kubernetes. Expel also continues to invest heavily in more automated remediation capabilities.

Conclusion

Cybersecurity threats are becoming increasingly complex and numerous. Security vendors and service providers need to leverage machine learning and automation technology to gain an edge in the fight to secure organizations' businesses against attackers. Expel understands the need for these technologies and has interwoven them with other innovations in its Expel Workbench platform. But most importantly, the vendor has realized that technology alone does not necessarily make for a great product. To provide increased value and unlock growth opportunities for its customers, technology must deeply interact with and enhance MDR's most important aspect: the security teams. Expel's platform, together with the company's managed alert process, reduce the workload on analysts, allowing them the time and space to engage the threats most effectively. By clever use of a mixture of processes, technology, and empathy, Expel Workbench augments every aspect of MDR and helps Expel deliver world-class security services to its customers. For its strong overall performance, Expel earns Frost & Sullivan's 2022 Enabling Technology Leadership Award in the global managed detection and response market.

What You Need to Know about the Enabling Technology Leadership Recognition

Frost & Sullivan's Enabling Technology Leadership Award recognizes the company that applies its technology in new ways to improve existing products and services and elevate the customer experience.

Best Practices Award Analysis

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

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization Success: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

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

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™

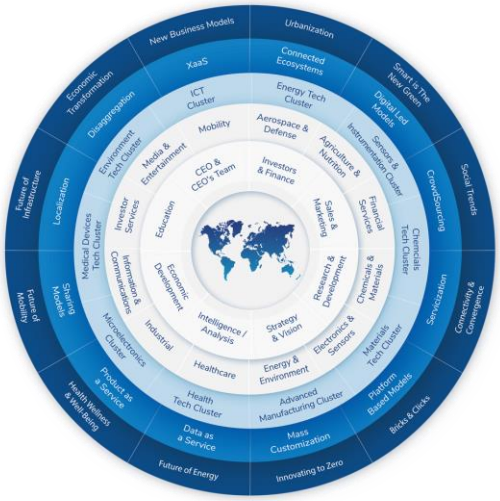
Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

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)