Binary Defense Is A Leader Among Managed Detection And Response Providers

Excerpted From The Forrester Wave™: Managed Detection And Response, Q1 2021

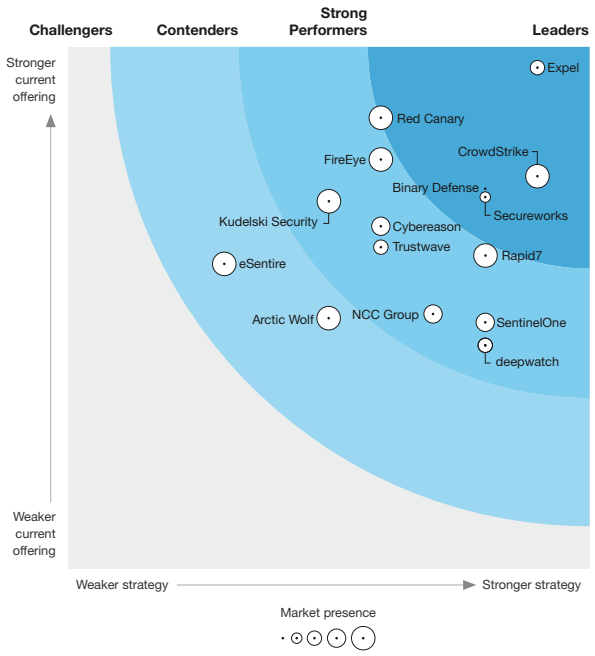
by Jeff Pollard, Claire O'Malley with Joseph Blankenship, Shannon Fish, Peggy Dostie | March 24, 2021

Binary Defense Exhibits Its Defense Mission Belief Through Its MDR Service

The vendor combines strong practitioner leadership, exceptional cybersecurity research, and a strong consulting sister company to bring a comprehensive MDR service to market. While most MDR vendors think like defenders, Binary Defense differentiates by starting with the attackers' perspective as the foundation for its MDR offering. Collaboration and partnership stand out as key elements behind its service delivery to ensure that security practitioners have what they need to detect, investigate, and respond to security incidents. Binary Defense's emphasis on cybersecurity research leads to sophisticated threat hunting capabilities.

Client references mention rapid detection of innovative threat actor techniques and the skills of service delivery personnel when assisting clients as strengths. Weaknesses client references discussed include challenges with the general pricing structure and a noticeable drop-off between the skill of junior analysts versus more experienced personnel. Security buyers looking for a rapidly growing MDR-focused provider with a clear emphasis on security research and threat detection should evaluate Binary Defense.

FORRESTER WAVE™:
Managed Detection And Response, Q1 2021



Binary Defense Evaluation Overview

CURRENT OFFERING

Time-to-value	Binary Defense demonstrates expected levels of client work effort necessary for service activation compared with others in this evaluation.
Threat hunting	Compared with others in this assessment, Binary Defense demonstrates superior threat hunting capabilities driven directly by practitioners, with high levels of customization, and tailored to specific client environments. The vendor demonstrated threat hunts significantly accelerated detection time frames and provided assurance across a comprehensive range of adversary TTPs for clients.
Threat intelligence	Compared with others in this assessment, Binary Defense demonstrates superior organic threat intelligence collection capabilities leading to substantial improvements in detection time frames, alert context, and decision-making for clients.
Collaboration	Compared with others in this assessment, Binary Defense demonstrates expected levels of collaboration capabilities across a standard set of methods leading to improved client outcomes in detection, investigation, and response.
User interface	Compared with others in this assessment, Binary Defense demonstrates an average user interface that provides details aimed at security practitioners on the status of detection, and investigation, and response actions as well as guidance on how to improve detection and response workflows.
ML/AI	Compared with others in this assessment, Binary Defense demonstrates expected processes linking threat intelligence, threat hunting, and analytics to ML/AI use cases and consistently proved that ML and AI techniques led to some acceleration in detection time frames and improved context during investigations across a market expected set of adversary TTPs.
MITRE ATT&CK framework mapping and use	Compared with others in this assessment, Binary Defense demonstrates superior integration and use of the MITRE ATT&CK framework for completed, in-process, and resolved items linking it to the customer environment resulting in superior improvements in detection engineering and the overall detection and response process across a wide range of adversary TTPs.
Managed detection	Compared with others in this assessment, Binary Defense demonstrates conclusive proof of superior capabilities in detecting intruder activity well before clients could and provides clear, detailed contextual information detailing severity, impact, and concerns that incorporate above-average external knowledge of threat actor TTPs and detailed internal awareness of the customer environment.
Managed response	Binary Defense offers expected choices in managed response actions across an expected set of technology types, including network, cloud, and endpoint, and also provides workflow options in approving response actions leading to improvements in faster, more accurate resolution of incidents.

Binary Defense Evaluation Overview

XDR collection, correlation, and APIs	Compared with others in this assessment, Binary Defense demonstrates subpar capabilities by relying on EDR tools for managed detections.
Automation and orchestration	Compared with others in this assessment, Binary Defense demonstrates an expected level of interactive security playbooks across a common set of incident types that are customizable by clients on request and execute detection steps and a limited set of response actions.
System criticality	Compared with others in this assessment, Binary Defense demonstrates expected capabilities primarily relying on the client to inform it of the importance and criticality of systems to the client's organization when initiating detection and response workflows.
Metrics	Compared with others in this assessment, Binary Defense demonstrates an average level of metrics primarily focused on SLA attainment and handling of detection and response activities to identify potential areas of improvement in detection and response workflows.

STRATEGY

Performance	Binary Defense's performance indicates a strategy that aligns with most MDR clients, with a commitment to cybersecurity as a means to an end and its business efforts designed to balance its growth needs with its service delivery capabilities.
Product vision	Compared with others in this assessment, Binary Defense demonstrates a superior view of where the MDR market and clients were headed, with a clear plan to ensure approach to service delivery would satisfy future buyer needs.
Roadmap	Compared with others in this assessment, Binary Defense demonstrates an average MDR portfolio roadmap that, if executed on, should position them to address the needs of most buyers. In addition, the vendor demonstrates success historically in executing successfully on most roadmap initiatives.
Vision and milestones	Compared with others in this assessment, Binary Defense demonstrates unique vision and value proposition for MDR that exhibit a clear understanding of buyer needs, has a successful plan to continually address those needs, and allows security practitioners to drive its innovation and service delivery efforts.