



# Managed Detection and Response (MDR)

*Battling Breaches with Delegating the Watchtower*

2024 CONSTELLATION SHORTLIST

The Constellation ShortList™ presents vendors in different categories of the market relevant to early adopters. In addition, products included in this document meet the threshold criteria for this category as determined by Constellation Research.

This Constellation ShortList of vendors for a market category is compiled through conversations with early adopter clients, independent analysis and briefings with vendors and partners.

## ABOUT THIS SHORTLIST

In today's complex cybersecurity landscape, detecting and responding to threats can be overwhelming for organizations lacking dedicated security teams or expertise. Managed Detection and Response (MDR), a growing service offering that combines human expertise with advanced technology to continuously monitor your environment, detect threats, and take decisive action.

Hiring and retaining skilled cybersecurity professionals is increasingly difficult and expensive. MDR provides access to a team of security experts who can continuously monitor your environment, detect threats, and respond to incidents effectively. Internal security teams are often overwhelmed with various tasks, leaving them vulnerable to missing critical threats. MDR frees up internal resources by taking on the responsibility of security monitoring and threat detection. Compared to building and maintaining an internal security team, MDR can offer a more cost-effective solution for many organizations. Think of it as having a dedicated cybersecurity team on call, working tirelessly to protect your organization from ever-evolving threats.

The MDR market is booming, projected to reach a staggering \$25 billion by 2030. This rapid growth reflects the increasing cyber threats, shortage of skilled security professionals, and the need for proactive threat detection and response capabilities.













## LIKE WHAT YOU SEE?

Consider partnering with Constellation Research on your go-to-market-strategy. Email [ShortList@ConstellationR.com](mailto:ShortList@ConstellationR.com) for more info.

To learn more about Constellation Research Shortlists visit: [www.constellationnr.com/ShortList](http://www.constellationnr.com/ShortList)

## 12 SOLUTIONS TO KNOW

Constellation evaluates more than 34 solutions categorized in this market. This Constellation ShortList is determined by client inquiries, partner conversations, customer references, vendor selection projects, market share and internal research.

-  ARCTIC WOLF
-  CROWDSTRIKE
-  DEEPWATCH
-  ESANTIRE
-  IBM
-  MANDIANT
-  OPTIV
-  RAPID7
-  RED CANARY
-  SECUREWORKS
-  SENTINELONE
-  SOPHOS

## THRESHOLD CRITERIA

Constellation considers the following criteria for these solutions:

- **24/7 Monitoring and Threat Detection:** Continuously monitors your network, endpoints, and cloud environments for suspicious activity using advanced tools and techniques like SIEM, EDR, and threat intelligence.
- **Expert-led Investigation and Response:** Leverages experienced security analysts to investigate detected threats, determine their severity and scope, and take swift action to contain and remediate them.
- **Threat Hunting and Proactive Defense:** Actively searches for potential threats using advanced threat hunting techniques, anticipating and preventing attacks before they occur.
- **Reporting and Compliance Support:** Provides comprehensive reports on security incidents and helps organizations comply with relevant security regulations.
- **Scalable Service:** Adapts to your organization's evolving needs and security posture, ensuring ongoing protection as you grow.
- **Threat intelligence integration:** Leverages real-time threat intelligence feeds to stay ahead of emerging threats.
- **Incident response planning and testing:** Collaborates with you to develop and test incident response plans for effective mitigation.
- **Integration with existing security tools:** Integrates seamlessly with your existing security ecosystem for centralized management and visibility.

## ABOUT CONSTELLATION RESEARCH

As an award-winning Silicon Valley-based strategic advisory and futurist analyst firm, Constellation Research serves leaders and organizations navigating the challenges of digital strategy, business-model disruption and digital transformation. Constellation works closely with solution providers, partners, C-suite executives, board of directors, and its Constellation Executive Network of buy-side leaders to lead the way in research coverage and advise clients how to achieve valuable business results.

## FREQUENCY OF EVALUATION

Each Constellation ShortList is updated at least once per year. Updates may occur after six months if deemed necessary.

## EVALUATION SERVICES

Constellation clients can work with the analyst and the research team to conduct a more thorough discussion of this ShortList. Constellation can also provide guidance in vendor selection and contract negotiation.

## BUSINESS THEMES



Digital Safety & Privacy



### Chirag Mehta VP & Principal Analyst

Chirag Mehta is Vice President and Principal Analyst focusing on cybersecurity, next-gen application development, and product-led growth. With over 25 years of experience, he has built, shipped, marketed, and sold successful enterprise SaaS products and solutions across startups, mid-size, and large companies. As a product leader overseeing engineering, product management, and design, he has consistently driven revenue growth and product innovation. He also held key leadership roles in product marketing, corporate strategy, ecosystem partnerships, and business development, leveraging his expertise to make a significant impact on various aspects of product success.

