Managed Detection and Response (MDR)

Around-the-clock expert monitoring to defend against threats and stop attackers in their tracks

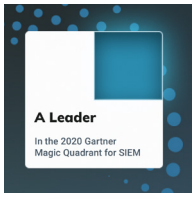
MDR means Managed Detection **and** Response. You deserve confidence that your MDR provider can deliver an end-to-end experience for both.

Standing up an effective detection and response program isn't as simple as buying and implementing the latest security products. It requires a dedicated SOC, staffed with highly skilled and specialized security experts, and 24/7 vigilance using the best technology to ensure stealthy attackers have nowhere to hide. Creating such a program can be expensive, difficult to maintain, and provides limited assurance that you've advanced your overall security.

Rapid7 MDR is built from the ground up to help security teams of all sizes and maturities strengthen their security posture, find attackers, and stay ahead of emerging threats.

Our MDR service uses a combination of security expertise and technology to detect dynamic threats quickly across your entire ecosystem, providing the hands-on, 24/7/365 monitoring, proactive threat hunting*, effective response support, tailored security guidance, and a team of Active Response* experts to stop malicious activity and help you accelerate your security maturity.

Detection and Response at Rapid7



Rapid7 MDR Elite Benefits:

- 24x7 security operations from detection and response experts
- Detection coverage across the SOC Triad to find network, user, and endpoint threats
- Assigned security advisor offers guidance tailored to improving your security program
- Real-time incident validation and Active Response contains malicious endpoint and user threats within 10 minutes
- Full access to InsightIDR, a Gartner-leading cloud SIEM solution with SOAR capabilities
- Gain unmatched visibility by connecting to unlimited event sources— with no data ingestion limits
- Transparency into SOC operations and detailed reporting
- Leading security research and MDR-sourced threat intelligence to stay ahead of attackers
- Emergency remote breach response support from Rapid7's MDR and IR experts

**Not available for MDR Essentials customers*

24x7 end-to-end detection and response

Have peace of mind and sleep easily knowing that Rapid7's MDR experts are continuously monitoring your environment and will take action for you at any time, day or night. Our team will monitor threats, validate them, and take on the initial countermeasures to paralyze the attacker for you.

- **MDR monitoring starts detecting threats within the first 60 days of onboarding**
- **Three layers of analysts for complete 24/7 coverage**
- **Alert validation leads to near zero false-positive rate**
- **True threats reported, no customer validation required**

Strengthen your security posture with an extended team

Our mission is to accelerate your security program—no matter your current maturity level—with the tools, resources, and human capital necessary to protect your business. From Security Advisors to our SOC, consider us an extension of your team.

- **Tailored service based on a deep knowledge of your environment and security goals**
- **Security Advisors with strong technical expertise to help guide your security maturation**
- **Board, executive, and CISO security advisorship**

Find attackers across network, user, and endpoint layers

Rapid7 MDR leverages seven proven detection methodologies to find known and unknown attackers: threat intelligence, proactive threat hunting*, Network Traffic Analysis, Network Flow data*, deception technologies, User Behavior Analytics, and Attacker Behavior Analytics derived from monitoring millions of endpoints.

- **Machine learning allows real-time event correlations at scale**
- **On-premises and cloud environment visibility**
- **Threat intelligence automatically applied to your data**

Stop attackers in their tracks

MDR with Active Response* will react as early in the kill chain as possible by containing compromised endpoints or user accounts. Taking action to respond within minutes of finding a threat will prevent malware propagation, cut off lateral movement, or stop data exfiltration attempts.

- **Action taken on your behalf to stop attacks in less than 10 minutes***
- **Prioritized security guidance and incident analysis**
- **Remote Incident Response assist in the event of a confirmed breach**

Not available for MDR Essentials customers

Rapid7 Detection & Response by the Numbers:

Daily security observations

Detections that trigger Active Response action

Maximum response time to contain users and endpoints with Active Response

To learn more about Rapid7 MDR, visit www.rapid7.com/MDR.

Support

call +1.866.380.8113

Customer Portal