

MANAGED DETECTION AND RESPONSE (MDR)

A RAPID7 SERVICE BRIEF

Around-the-clock expert monitoring to help 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. Establishing an effective detection and response program isn't as simple as buying and implementing the latest security products. It requires a dedicated Security Operations Center (SOC), staffed with highly skilled and specialized security experts, and 24/7 vigilance using premium 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.

Rapid7's MDR service uses a combination of security expertise and technology to help 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

Rapid7 MDR Elite Benefits¹:

24/7 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 helping improve 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*

24/7 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 counter measures 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

Help strengthen your security posture with an extended team

Rapid7's mission is to accelerate your security program—no matter your current maturity level—with the tools, resources, and human capital necessary to help 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 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 help 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

¹Source: Rapid7 - <https://www.rapid7.com/services/managed-services/managed-detection-and-response-services/>
Please see Rapid7 Scope of Services for further service details

Rapid7 Detection and Response by the Numbers¹:

150+
BILLION

Daily security observations

1,500+

Detections that trigger
Active Response action

10
MINUTES

Maximum response time
to contain users and
endpoints with Active
Response

*Not available for MDR
Essentials customers

Canon

CANON SOLUTIONS AMERICA

1-800-815-4000 CSA.CANON.COM/SECURITY

Canon Solutions America does not provide legal counsel or regulatory compliance consultancy, including without limitation, regarding Sarbanes-Oxley, HIPAA, CCPA, GDPR, GLBA, Check 21, or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Some security features may impact functionality/performance; you may want to test these settings in your environment.

Canon is a registered trademark of Canon Inc. in the United States and may also be a registered trademark or trademark in other countries. All other referenced product names and marks are trademarks of their respective owners. Specifications and availability subject to change without notice. Not responsible for typographical errors.
© 2024 Canon Solutions America, Inc. All rights reserved.

24-0054-9923