Advance Your Threat Detection Program with Rapid7 MDR

Rapid7's security experts, technology, and threat intel goes beyond what traditional MSSPs can offer.

Rapid7 Managed Detection and Response (MDR) replaces your typical MSSP model with a service designed to strengthen your security posture, regardless of your current maturity level. We focus on advancing your program—layering industry experts, workflow processes, and industry-leading technology—to see a faster time to value than previous security investments.

PEOPLE	PROCESS	TECHNOLOGY
• 24/7 monitoring by our expert SOC analysts augments your security team. • Threat hunters proactively identify unknown malware and attacker behaviors each month.[1] • Your Customer Advisor helps you understand impacts of malicious activity and guides remediation.[2]	• Initial Compromise Assessment exposes historical and live breaches. • Each Finding Report offers containment and remediation recommendations. • Proactive Threat Intelligence and monthly Service Reports keep you informed and prepared. • Immediate Incident Escalations aid recovery in the event of a breach.	• Monitors and analyzes all endpoint, network, and cloud service data to find attackers. • Full access to underlying SIEM technology for visibility, log management, and compliance. • Included deception technology exposes traces of attackers in addition to log analysis.

Security Analytics to Detect Across the Attack Chain

MOST MSSPs		RAPID7 MDR		
SIEM Rules		User Behavior Analytics	Attacker Behavior Analytics	Deception Technology
Static rule sets without user context.	vs.	Baselines user activity to detect compromise.	Detects key behaviors attackers use daily.	Finds attacks invisible to log analysis.

[1] Not included with Rapid7 MDR Essentials
[2] Rapid7 MDR Essentials customers are supported by a team of Customer Advisors

Investigating Incidents in Your Environment

STAGE	TRADITIONAL MSSP	RAPID7 MDR
Detect	Detection by existing tools or third-party solutions from the MSSP leave gaps around user endpoints and cloud services.	Rapid7 InsightIDR integrates with your environment. Pre-built detections within InsightIDR to provide defense across the attack chain.
	What it means for you: Static rules detect alerts with no context to users, attack behaviors, or actions invisible to log analysis.	What it means for you: You get a combination of methodologies to detect both known and unknown threats.
Validate	MSSP analyst teams of false-positive alerts with little context around user or asset activity.	Multi-layer validation process weeds out benign events and only report true positive threats.
	What it means for you: Fewer false positives, but alerts thrown over the fence with no context or guidance on next steps.	What it means for you: Near 0% false positives; actionable reports with tailored recommendations on confirmed threats.
Investigate	MSSPs don't collect the right data sources or only have sensors on the network, omitting remote workers and cloud services.	Beyond detecting, validating, and reporting, our MDR service includes breach investigations to support our customers in the time of highest stress.
	What it means for you: MSSPs lack complete visibility, making it difficult to provide the IR support needed to scope and investigate a breach.	What it means for you: Our incident responders scope, investigate, and work with you on remediation recommendations.
Contain & Remediate	MSSPs are skilled at data integrations and providing hardware, less so guiding incident response efforts to remediation.	Threat and Findings reports include tailored containment, remediation, and mitigation recommendations prioritized for your business.
	What it means for you: To take any action, you either need to do it yourself, buy a separate incident response retainer, or work with another vendor.	What it means for you: Utilize containment functionality inside of InsightIDR to stop in-motion attacks. If it's critical, utilize your Incident Escalation to get immediate help.
Find Unknown Attackers[3]	MSSP infrastructure is typically designed around rule-based detection and perimeter defense, showing only known threat.	Rapid7 analysts use forensics data collected from our Insight Agent to proactively hunt for persistent, stealthy indicators of compromise.
	What it means for you: If you want proactive threat hunting for unknown attackers, prepare to buy an additional service module (if the MSSP offers it).	What it means for you: Our experts conduct monthly hunts that expose misconfigurations and potential attackers in your environment.

See the benefits of Rapid7 MDR for yourself: +1–866–7RAPID7 (Toll Free) | www.rapid7.com/MDR

[3] Not included with Rapid7 MDR Essentials