Embedded, Unlimited Breach Response

Standard with Rapid7 Managed Detection and Response

We think your Managed Detection and Response (MDR) service should actually respond. That's why we embedded Incident Response Consultants into your MDR service to take detection and response completely end-to-end. You get simplicity, cost savings, and speed. Your outcome is our single minded priority.

For years, organizations that needed Breach Response assistance had limited options:

- Purchase high-cost, off-the-street Incident Response (IR) services
- Pre-pay a significant IR Retainer
- Rely on their managed service providers to handle it (spoiler: most can't, won't, or charge hourly to try)

They all monetize your pain in your greatest time of need, and your outcome isn't the priority.

We built our MDR service to be unlike any other, providing you with a true Incident Response partner when you need it. That means that for any security incident – minor or major – our MDR team delivers the same level of Incident Response expertise you'd get with an IR Retainer, at no additional cost, and without limits.

Incident Response Process

Incident Notification	Incident Investigation and Analysis	Incident Remediation	Post-incident Activities

The Rapid7 DFIR Difference:

Unlimited Breach Response

The mission is simple. If there's an incident, we respond. No limits to hours worked, resources needed, or number of breaches responded to. Whether it's a user that's been phished, a vulnerability was exploited, or widespread lateral movement across your environment, or signs of something more sinister, Rapid7 MDR has you covered. Our Incident Response team responds to ALL in-scope incidents, regardless of their magnitude. Unlike other MDR providers, there's no line where a breach is too big for Rapid7's service to handle.

Key Outcomes

- **Faster, More Robust Response with Embedded DFIR**
- **"Unlimited" Means No Caps on Hours Worked or Staff Used**
- **Expert Guidance Throughout the Incident**
- **Maintain Business Continuity and Customer Trust**

Seamless pivot from the SOC to DFIR

Only Rapid7 MDR has all the expertise you need operating daily as one, unified team. We merged our SOC and IR Consulting teams to make escalation to Breach Response as easy as swiveling a chair and tapping a shoulder. Our Incident Response Consultant team is instantly engaged to conduct meticulous investigation and deep forensic analysis to discover the root cause, assess the impact to your business, and guide you through eradicating the threat to leave your environment more secure.

No waiting: DFIR technology is deployed and ready

Incident Response relies on multiple sources of telemetry including XDR, endpoint agents, and our open-source DFIR tool, Velociraptor, to enhance our ability to retrieve forensic artifacts and analyze data. Best of all, because we utilize the technology already deployed in your environment, you'll never need to wait to pivot directly into IR. It's all right there, ready to be actioned by our expert team. Plus, transparent technology allows your team a window into our investigation as it's happening.

Top tier IR that follows the sun (so you can sleep)

When an incident happens, we're ready. Our team of global DFIR experts have seen it all and work on hands-on-keyboard attacks every day. With 3 global SOCs in Arlington, Virginia; Dublin, Ireland; and Melbourne, Australia; we're able to perform IR around the clock while monitoring your environment for any other threats. No compromises.

"

Rapid7 has been vital to our security posture. The service that we received when a security breach has been detected has been excellent.

IT Manager, Non-Profit
via TechValidate

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research—using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

		CUSTOMER SUPPORT
Cloud Security	Application Security	Call +1.866.380.8113
XDR & SIEM	Orchestration & Automation	
Threat Intelligence	Managed Services	
Vulnerability Risk Management		

To learn more or start a free trial, visit: **https://www.rapid7.com/try/insight/**