Rapid7 Active Response

Accelerate Response with Expert-Led Detection and Automation

In 2023, the mean time to identify (MTTI) a security breach was 204 days, and the mean time to contain (MTTC) was 73 days[1]. These averages have been consistent over the last 5 years. Finding and eradicating attacker activity in modern environments is tough. Breaches are costly and erode customer trust.

The longer an adversary is left to dwell in an organization's environment, the more damage they can cause, and the wider the possible blast radius of a breach. Effective detection and response programs not only isolate attacker behavior, but halt an attack immediately.

Rapid7's Active Response - included in all Managed Threat Complete subscriptions - brings the power of expert-led containment to your SOC. Within seconds of a validated threat, analysts can quarantine an endpoint or user group, stopping an attack before it can cause costly damage or expand the scope of impact.

- Configure response actions that work best for your structure and needs, directly within InsightIDR.
- Access complete visibility into actions taken on your behalf with investigation trees and audit logs.
- Use the tools that work for your environment, with support for the Insight Agent and pre-built integrations across your ecosystem.
- Unquarantine with the click of a button for complete oversight and control.

Containment on Your Terms:

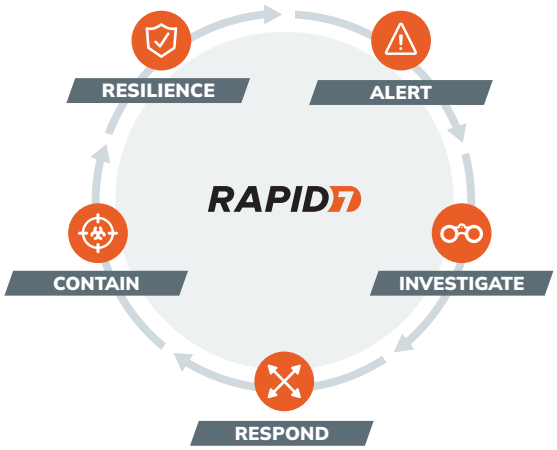
- **24x7, End-to-End Detection and Response**. No frantic "drop everything and respond now" moments. Sleep easy knowing that Rapid7's MDR experts will take action for you at any time, day or night. Our team will monitor threats, validate them, and take on the initial countermeasures to paralyze the attacker for you.
- **Contain users and hosts on-premise or remotely**. 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, and stop data exfiltration attempts.

1 IBM's 2023 Cost of a Data Breach Report

> **Rapid7 MDR provides the depth of support we need. It does more than just collect and send logs, it is actively looking for threats. And, if it spots one, it will intercept that threat immediately. It is that proactive piece that makes Rapid7 MDR an effective program for us.**
>
> AMN Healthcare Partners

- **Set configurations and guidelines for any response action.** You can create containment guardrails to prohibit response actions to critical servers, users, or devices. We won't treat a typical user the same as your domain admin credentials.
- **Deal with eradication and recovery on your terms.** Following an Active Response engagement, you'll receive a detailed remediation and mitigation guide in your Incident Report to help build resilience against future attacks. From there, you can remove the device from quarantine directly within the investigation in InsightIDR.

How Active Response Works



Report + Follow-up
MDR Analyst determines full attacker timeline and actions for final Incident Report.

Attacker Activity Detected
Rapid7 MDR Team detects suspicious behavior on an endpoint or with a user.

Attacker Contained
Customer takes additional initial remediation and mitigation recommendations provided by MDR analyst. Rapid7 Customer Advisor reaches out to ensure actions are taken and answer any questions.

Investigation Begins
Rapid7 analyzes available data, determines activity is malicious.

Active Response Kicks Off
MDR analyst kicks off Active Response automation to quarantine and take impacted users or assets offline. Details are available in InsightIDR for customer visibility.

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

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

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