SERVICE OVERVIEW

Managed Detection & Response Service

Rapid7 Managed Detection and Response (MDR) extends your team's ability to detect, analyze, investigate, and actively respond to threats across your modern environment through 24/7/365 monitoring and tailored security operations designed to stop attackers and advance your security program.

v02102021

RAPID7 MDR SERVICE

Buying and implementing the latest security products is a great start toward standing up an effective detection and response program. However, without the right people leveraging those tools and using the right processes to ensure your team can eradicate threats efficiently, your security program can fall flat and threats can slip through the cracks.

Threat detection and incident response 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 and difficult to maintain, with limited assurance that you've actually advanced your overall security. That's where partnering with a Managed Security Service Provider (MSSP) comes in.

But the challenge is, most MSSPs today can only help as far as their third-party tools enable them to, and they consider "response" an incident report with a few canned suggestions.

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

That's why Rapid7 MDR is built from the ground up to help security teams of all sizes and experience levels strengthen their security posture, stay ahead of emerging threats, and stop attackers.

Rapid7 MDR offers a combination of expertise and technology to quickly detect and respond to dynamic threats across your users, endpoints, networks, and cloud environments.

Our MDR service provides hands-on, 24/7/365 threat monitoring and hunting customized to your business profile, powered by Rapid7's purpose-built technology stack. This includes the Rapid7 Insight Cloud, Threat Intelligence infrastructure, and our Security Operations Center (SOC) experts who work to help you stop attackers and strategically improve your overall program based on learnings from over 1.2 trillion security events per week.

Most importantly, Rapid7 MDR enables your team to focus on what matters most to you and your business. Consider us an extension of your internal team and a partner in your security success.

At the end of the day, no one gets into security to look at a list of alerts—we all got into security to find and stop evil. Let MDR become a force multiplier for your security program and free up your team to provide more value to your business.

Rapid7 is dedicated to your success, no matter how large or small your organization. Everyone at Rapid7, from the MDR team to our customer success experts all the way up to senior leadership, is deeply invested in helping raise the bar so that, ultimately, **we can all build a more secure future—together**.

TABLE OF CONTENTS

Rapid7 MDR Vision 2

Introduction to MDR 4

Our Approach 8

Top Five Advantages with Rapid7 MDR 9

Six Layers of the Service 16

Proprietary Threat Intelligence & Research 17

Industry-Leading Technology 21

Detection Methodology 27

SOC Operations 36

Incident Investigations & Active Response 41

Program Advancement 44

Value Adds of Rapid7 MDR 50

Compromise Assessment 51

On-Demand Remote Incident Response 52

Purple Team Exercises 53

How it Works 54

MDR Responsibilities Matrix 55

MDR Investigation Workflow 59

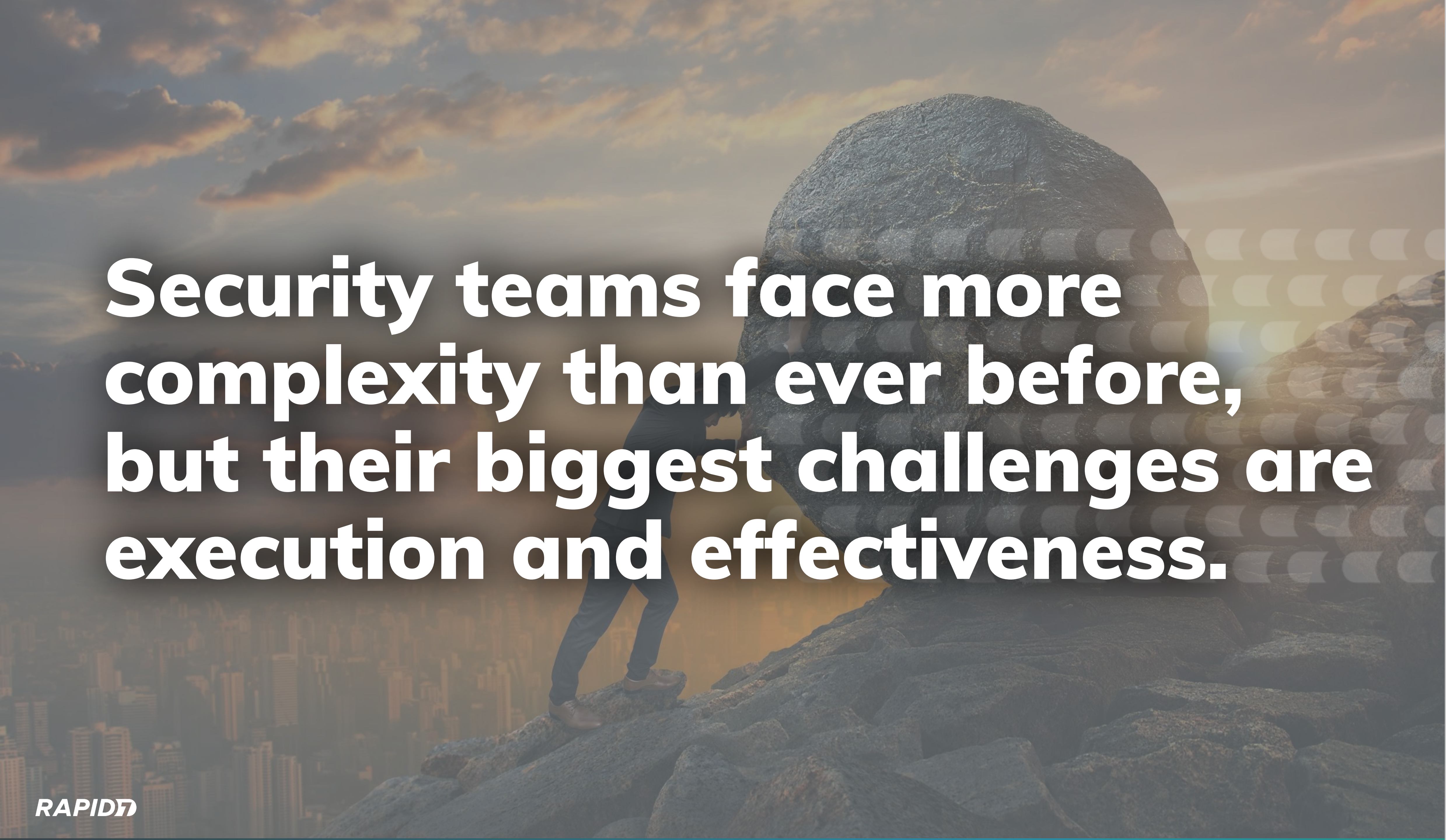
MDR Deployment 60

Appendix 70

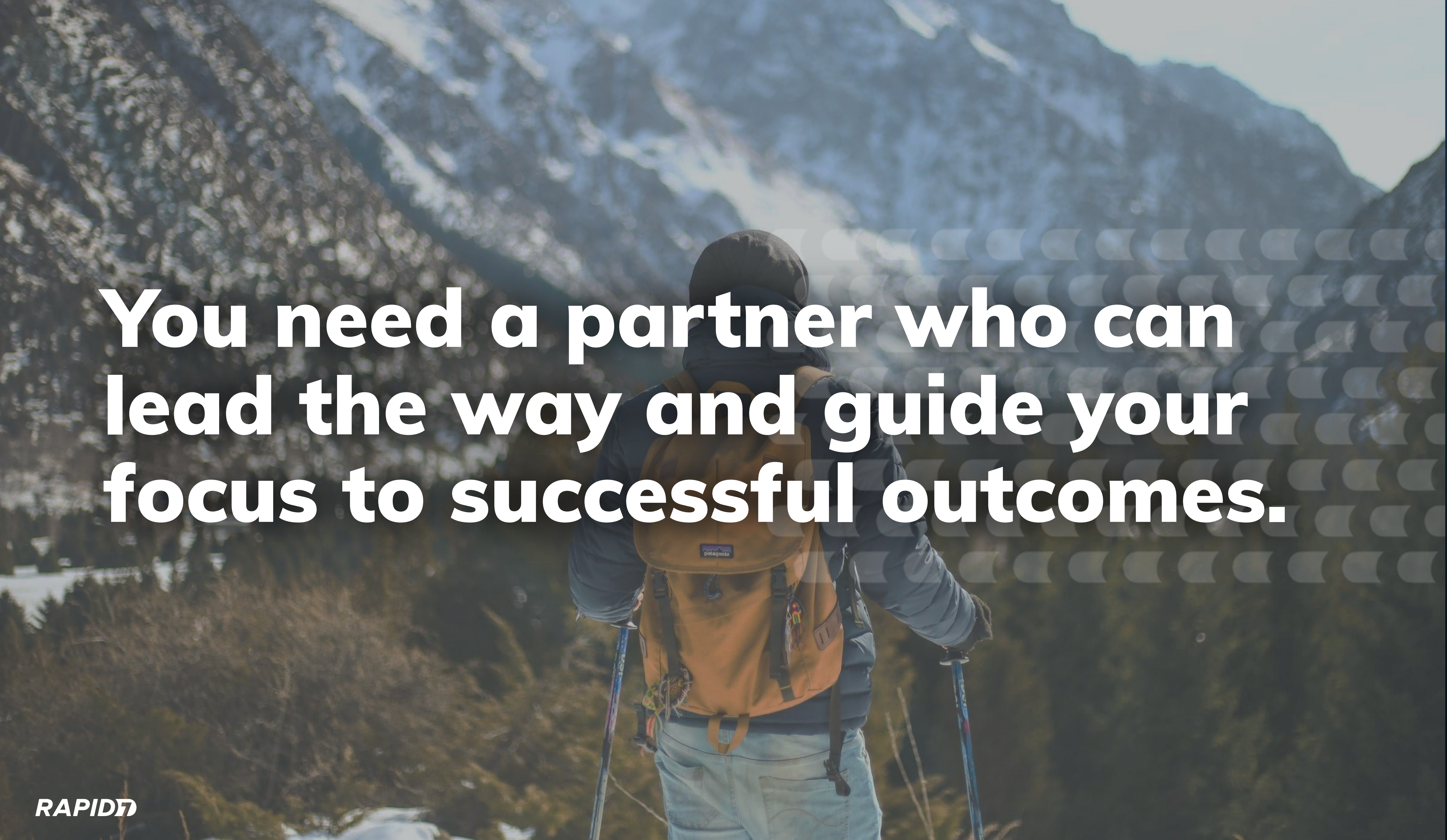
MDR Package Comparison 71

MDR Technology Overview 74

Introduction



Security teams face more complexity than ever before, but their biggest challenges are execution and effectiveness.



You need a partner who can lead the way and guide your focus to successful outcomes.

Rapid7 MDR advances cybersecurity decision making through expert collaboration.

OUR APPROACH

INCIDENT DETECTION & VALIDATION

- 24/7/365 monitoring
- Initial Compromise Assessment
- Investigations of threats and alerts
- Alert validation
- Proactive threat hunting*

INCIDENT RESPONSE

- Detailed threat analysis
- Remediation guidance
- Mitigation guidance
- Active Response*
- Remote Incident Response*

TECHNOLOGY ACCESS

- Full Access to InsightIDR capabilities
  - Cloud SIEM
  - Attacker Behavior Analytics
  - User Behavior Analytics
  - Endpoint Detection & Response
  - Network Traffic Analysis
  - Network Traffic Flow**
  - Deception Technologies
  - SOAR
- No additional data charges

WHITE-GLOVE SERVICE

- Named Customer Advisor
- Threat intelligence team
- Custom threat profile
- Findings Reports
- Proactive Threat Reports
- Monthly Hunt Reports*
- State of Service Reports*
- Deployment assistance included

* Service and deliverables differ for MDR Essentials customers

** Optional additional capability for MDR Elite customers

At its core, Rapid7's MDR service is a strategic partnership that allows your business to defend against attackers, identify and respond to threats, and strengthen your security program.

Partnering with Rapid7 MDR will extend your team's security capabilities, expertise, and resources to give you time back so your team can focus their energy on the other things that matter most to your business.

In addition to tactical detection and response, you'll gain a strategic security partner who can provide the mentorship and guidance necessary to simplify the complexities of cybersecurity and help you securely advance your business.

Our multi-layered approach provides you with 24/7/365 monitoring, leveraging proven cloud SIEM technology, cutting-edge endpoint technology, and world-leading threat intelligence to stay ahead of attackers.

Rapid7's approach ensures there is full visibility and an organized response to incidents that occur in your environment. This encompasses four areas of service delivery with Rapid7 MDR.

Top Five Advantages with Rapid7 MDR

Five Advantages with Rapid7 MDR

Rapid7's MDR offering goes far beyond the capabilities of traditional Managed Security Service Providers (MSSPs), who often provide incomplete technology solutions without the required expertise to manage the systems and provide guidance.

A typical MSSP rarely offers threat hunting, and the experience is an impersonal, one-size-fits-all approach that merely focuses on the detection of malware and sending sterile tickets rather than a strict focus on advancing your security program.

Our belief in delivering the Rapid7 MDR service is to be more than a vendor, and for our team to do more than just alert you of threats.

For more detailed analysis, please review our **Rapid7 MDR vs. MSSP comparison brief**.

Rapid7's Managed Detection and Response (MDR) service provides customers with five key advantages.

1

Improved Security Maturity & Effectiveness.

Rapid7 MDR is positioned to meet our customers at any level of security maturity and help **accelerate your maturity**, not just manage a SIEM.

The team—from SOC analysts to your Customer Advisor—takes the time to truly understand your business processes, environment, and industry so they can provide customized guidance at each interaction point with the MDR service.

This includes tailored reporting and recommendations, with remediation and mitigation strategies that align your investment in MDR with long-term security improvement across all 20 CIS critical controls.

We go above simply looking at alerts by having our team respond on your behalf, offer advice and mentorship from your Customer Advisor, and focus on helping you improve your security program.

Powerful Agent, Sensor, and SIEM Technology.

MDR is powered by the **Rapid7 Insight Platform**, with data fed from the Insight Agent and Insight Network Sensor to perform endpoint and network traffic investigations and hunt for threats in your environment. The lightweight Agent unifies data collection for the MDR team to effectively view and correlate endpoint data, including detailed asset information, Windows registry information, file version and package information, running processes, authentication information, local security and event logs, and more. The sensor feeds network data to InsightIDR to effectively enable our team of SOC experts to expand coverage beyond your endpoint assets.

This data is encrypted at rest and in transit as it's sent to InsightIDR for log correlation and investigation. Combined, the Insight Agent, Insight Network Sensor, and InsightIDR provide the MDR team with system-level visibility to spot real-time detections on the endpoint—the closest point to the attacker. As a customer of the MDR service, your team will have direct access to your instance of InsightIDR, giving you full transparency into our service and the ability to interact with the MDR team.

Learn From Leading Threat Intelligence & Industry Research.

Customer defenses leverage Rapid7's **primary threat intelligence** on attacker behaviors and common indicators of compromise, all powered by Rapid7's Managed Threat Intelligence Engine, cybersecurity research projects, vulnerability disclosures, insights from our customer endpoints, and Rapid7 SecOps Services engagements.

In addition, Rapid7 leverages top third-party threat intelligence from security partners in the community, most notably Rapid7's involvement as an Affiliate member of the Cyber Threat Alliance (CTA) with Board and Committee seats.

Our World-Class Managed Services Team acts as an Extension of Yours.

The global **MDR SOC teams** are composed of security experts with unparalleled experience—both red team and blue team—and work in teams ("Pods") assigned to customer clusters.

Our pod design enables our analysts to become subject-matter experts in your user behavior, endpoints, and networks. Each analyst pod uses this in-depth knowledge of attacker tools, tactics, and procedures to catch malicious activity early in the attack lifecycle and validate each threat.

Each SOC analyst acts as an extension of your security team and tailors the MDR service specifically to your industry and business. This includes threat hunting, validation of threats, and guidance (e.g., containment, remediation, and mitigation recommendations) for only true threats.

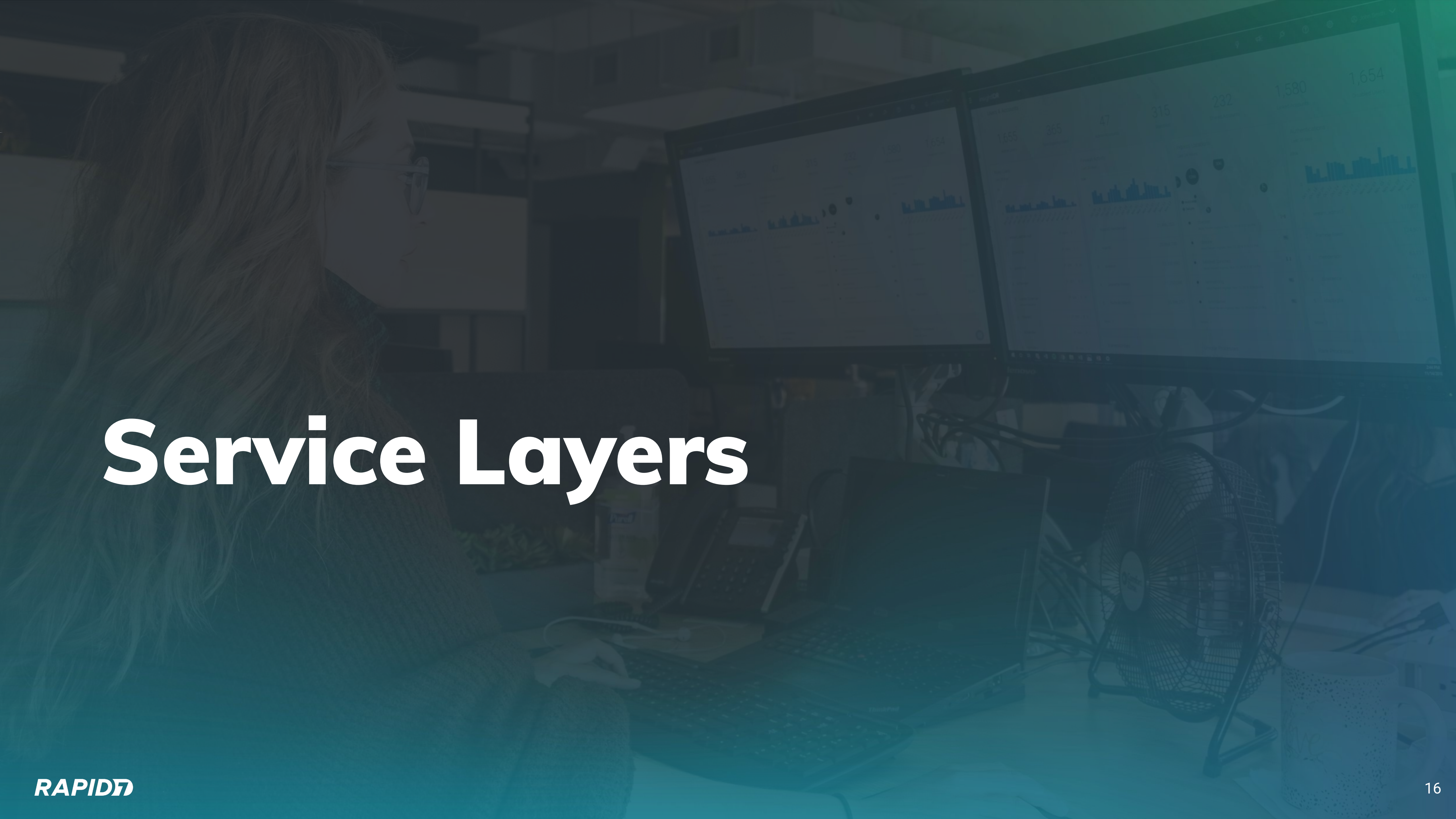
5

Unmatched Incident Response Support When You Need It.

When something happens that can be a threat to your environment, you want to make sure that you're protected—both for detecting that event and also for responding to the threat. After all, you're paying for a Managed Detection and Response service. From a response standpoint, we'll assist your team in two significant areas:

1. **Active Response:** Rapid7 MDR with Active Response extends your team with 24x7 end-to-end threat detection and response to protect your business, reduce attacker dwell time, and accelerate your time to response. Active Response puts the power of responding to threats directly into the hands of Rapid7's MDR SOC experts, allowing our team to contain users or endpoints on your behalf within minutes (not hours or days).

2. **Remote Incident Response:** Rapid7 MDR includes an ability to engage our skilled IR personnel in the event of a confirmed compromise as part of your service. Feel confident that MDR can support your business with response support, regardless of whether it's a detectable attacker or a new zero-day compromise.



Service Layers

LAYER 1

Proprietary Threat Intelligence & Industry Research

As attackers evolve and new threats are discovered, our Threat Intelligence team develops signatures and analytic detections to stay ahead of existing and emerging threats.

This data is combined with sourced threat intelligence feeds to enrich the data and deepen our contextual knowledge. All detections ensure coverage for various IOCs that malicious actors use in the wild mapped to the MITRE ATT&CK framework.

- Intel based on 115+ billion daily security events
- Constantly evolving detections as new TTPs emerge
- Tailored tuning and alert suppression

LAYER 1

Proprietary Threat Intelligence & Industry Research

Rapid7 Threat Intelligence and Detection Engineering (TIDE), part of Managed Services, leads Rapid7's proprietary, global threat intel program. Together with Rapid7's research initiatives, TIDE analysts provide customers and MDR SOC analysts with the surrounding context needed to defend against threats with new detection mechanisms for vulnerability exploits and attack campaigns.

Threat Intelligence and Detection Engineering Team

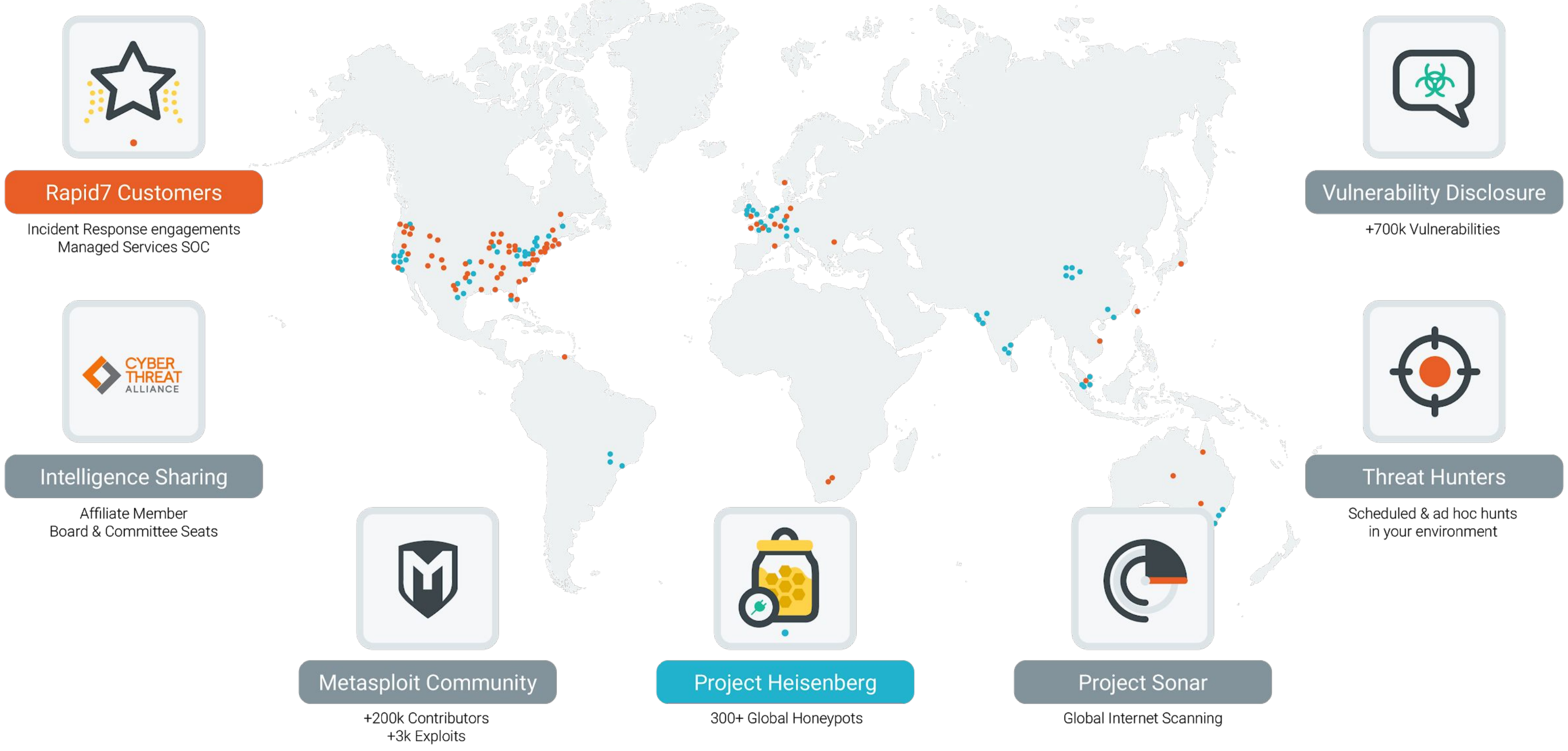
As attackers evolve and new threats are discovered, TIDE develops signatures and analytic detections for existing and emerging threats. These detections ensure coverage for various IOCs that malicious actors use in the wild, informed by over 1.2 trillion weekly security events observed across our detection and response platform from the sources listed below. All detections improve in fidelity over time as our MDR analysts inform the threat intelligence team of rule suppressions to provide a tailored approach for customers, add granularity, reduce noise, and avoid recurrency.

Rapid7 Research and Threat Intelligence Sources

We're committed to openly sharing security information that not only helps the entire cybersecurity community to learn, grow, and address issues in the security world, but also to improve our products and detections. Below are the common sources that lead to Rapid7's security expertise and intelligence advantage.

LAYER 1

Proprietary Threat Intelligence & Industry Research



Rapid7 Customers
Incident Response engagements
Managed Services SOC

Intelligence Sharing
Affiliate Member
Board & Committee Seats

Metasploit Community
+200k Contributors
+3k Exploits

Project Heisenberg
300+ Global Honeypots

Project Sonar
Global Internet Scanning

Vulnerability Disclosure
+700k Vulnerabilities

Threat Hunters
Scheduled & ad hoc hunts
in your environment

Applied Threat Research: This component describes our methods of gathering, evaluating, analyzing and institutionalizing threat data. We analyze emerging threats at a fast-paced, operational level, and produce actionable tactical intelligence and detections as a result. Our sources include internal intel and frontline threat data from IR engagements and analyst workflows. The single most important source of threat data that we transform into our detections is the data derived from MDR & IR intrusion reports.

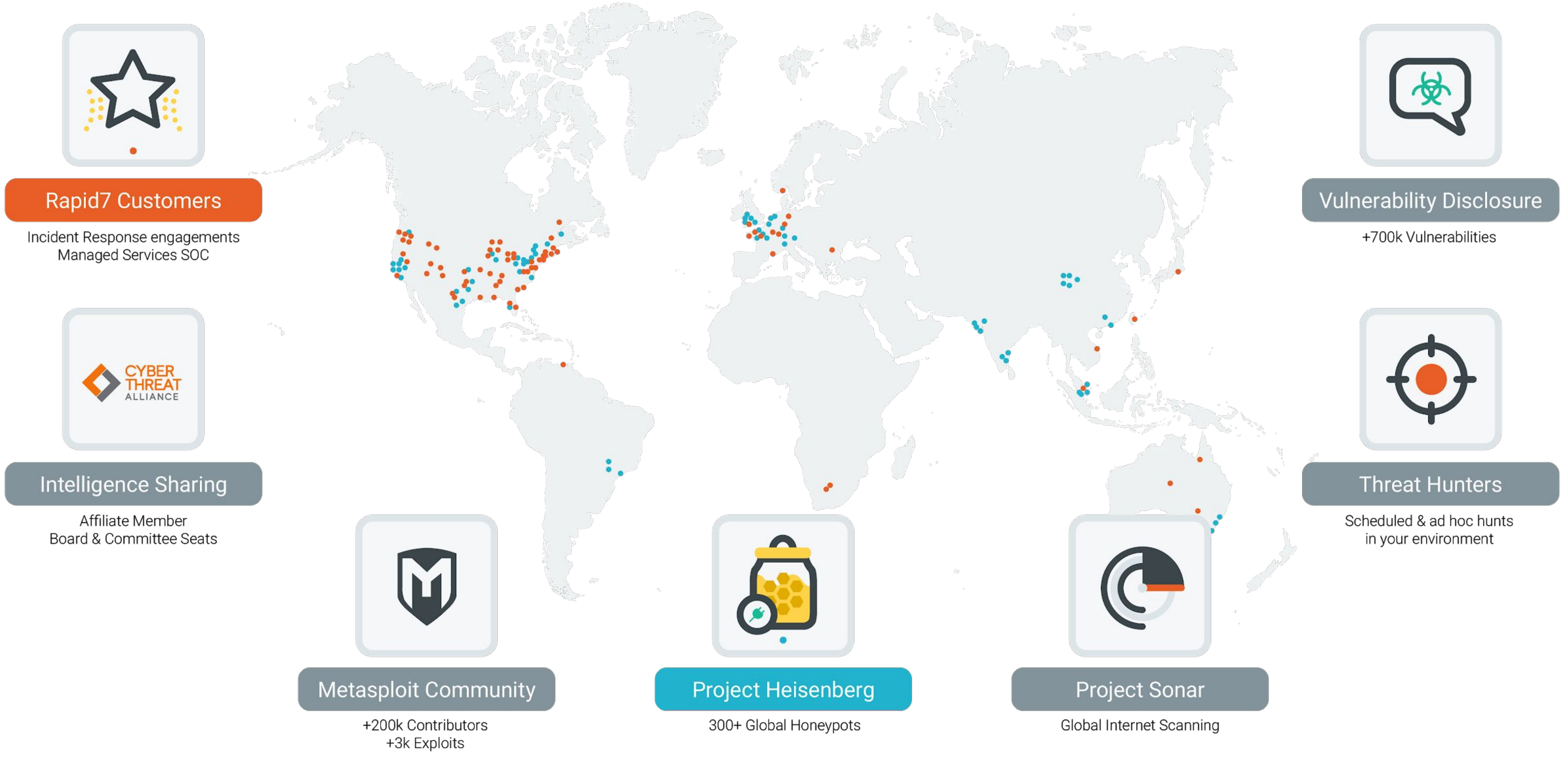
Rapid7 Customers: Our detections are further enhanced from learnings across the 150+ billion daily security events captured by our Insight Agents deployed on Customer endpoints, MDR Customers, and Incident Response engagements.

Intelligence Sharing: As a Affiliate member of the Cyber Threat Alliance with Board & Committee Seats, we are active in the cyber community and share learnings.

Metasploit Community: Metasploit is the world's most-used penetration testing software used to uncover weaknesses in defenses, with over 3,000 exploits and over 200,000 active contributors.

LAYER 1

Proprietary Threat Intelligence & Industry Research



Project Heisenberg: A collection of over 200 low-interaction, global honeypots distributed both geographically and across IP space. The honeypots offer the front end of various services to learn what other scanners are up to (usually no good), and to conduct "passive scanning" to help enhance our understanding of attacker methods.

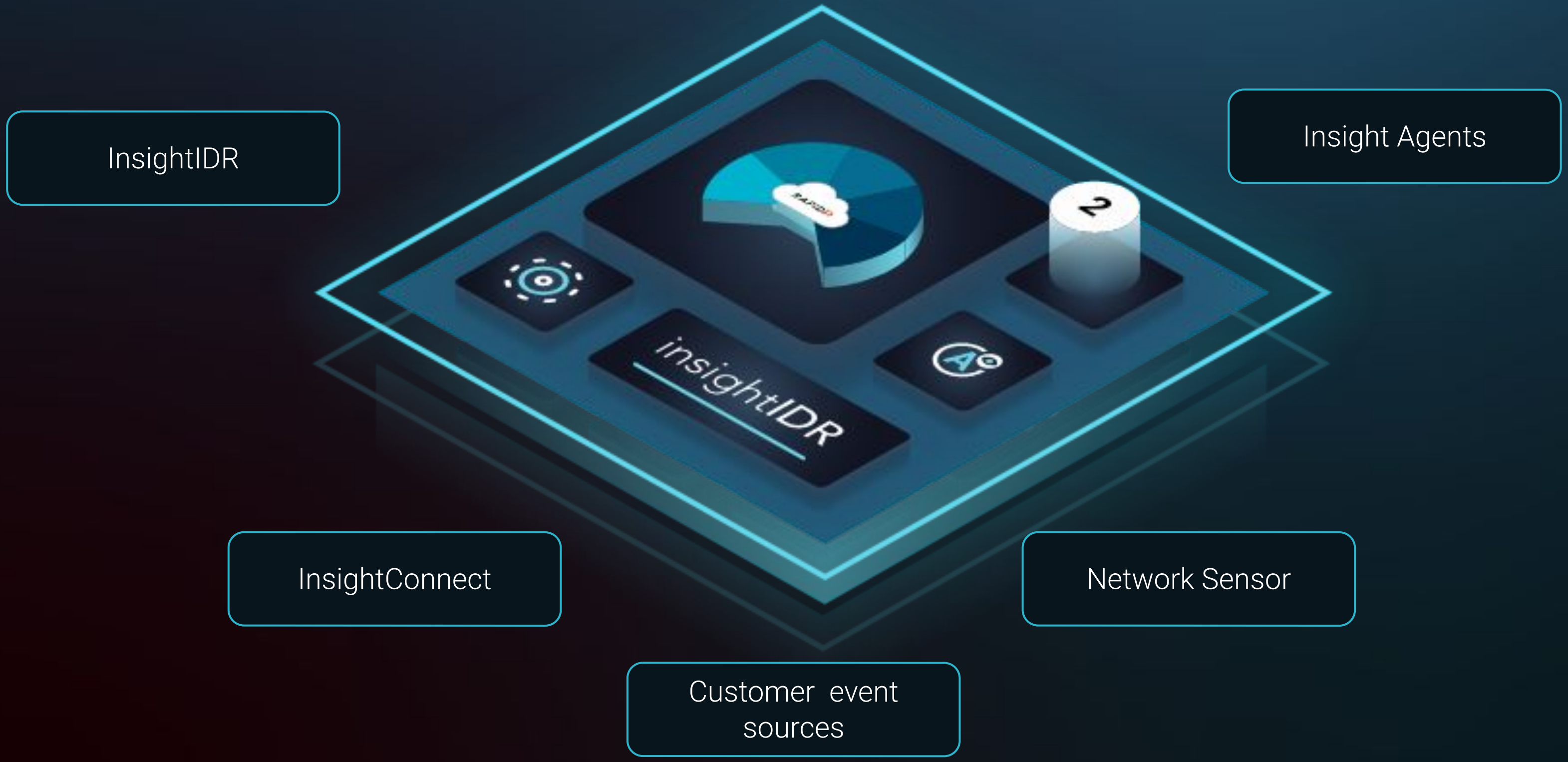
Project Sonar: A security research project by Rapid7 that conducts internet-wide scans across different services and protocols to gain insight into global exposure to common vulnerabilities.

Pen Test Engagements: Rapid7 service engagements allow us to leverage real-world experiences of our engineers and investigators gathered over thousands of pen tests.

Vulnerability Disclosure: As a CVE numbering authority, we understand vulnerabilities and how attackers exploit them better than almost anybody. This helps our MDR team stay in lock-step with the latest threat tactics, techniques, and procedures so we can better protect each of our customers.

LAYER 2

Industry-Leading Technology



The MDR service is powered by Rapid7's Insight Platform. Data from our endpoint agent and other event sources help us gain network- and system-level visibility across your environment.

This data is crunched by our Gartner-Leading cloud SIEM, InsightIDR, to analyze user, endpoint, and network data using analytics to uncover threats across your internal network and cloud services to detect advanced attacks early. And, as a customer of MDR, you'll have full access to see InsightIDR, search logs, and run your own investigations.

- Unlimited data and event source connections
- Leverage and integrate your existing security investments across endpoint, network, infrastructure, and cloud solutions
- Fast deployment and exceptional time to value

LAYER 2

Industry-Leading Technology

The Rapid7 Managed Detection and Response service is powered by Rapid7’s Insight Cloud, specifically:

- **InsightIDR**, a Gartner ‘Leader’ for SIEM
- **Insight Agents**
- **Insight Network Sensor**
- **InsightConnect**, if Active Response is configured

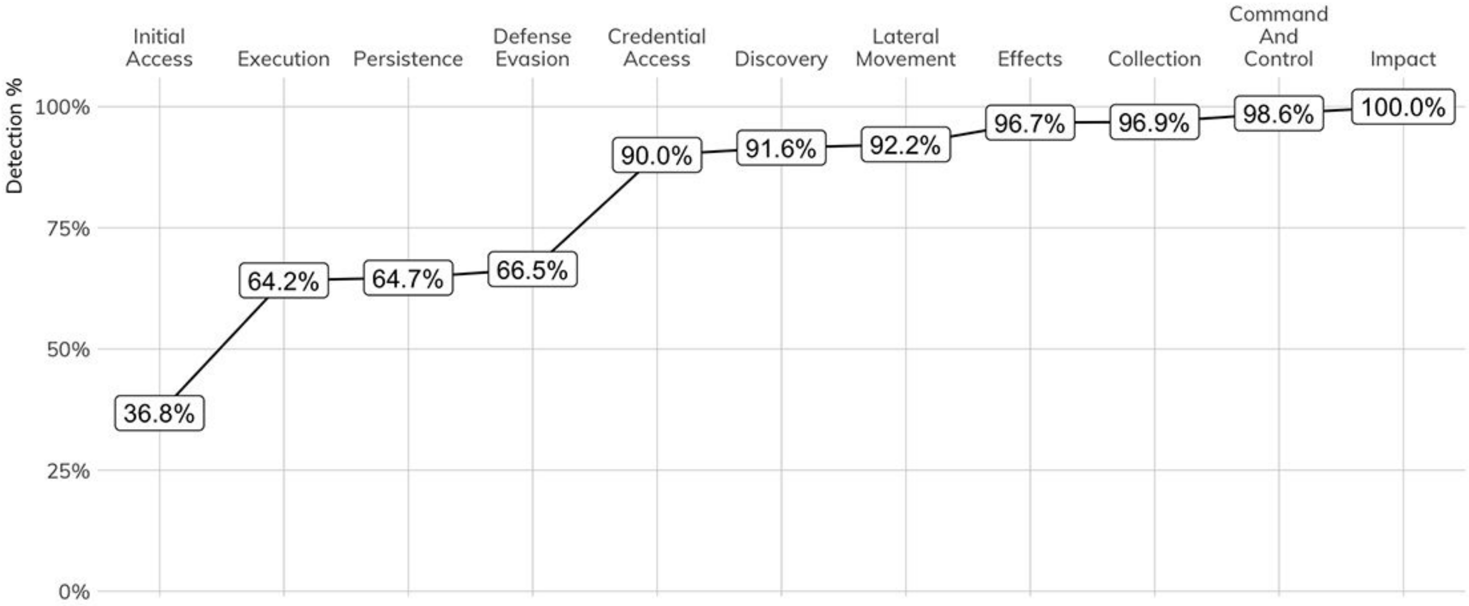
Combined, your MDR service will be operating using products recognized as leaders across the industry.

LAYER 2

InsightIDR

Cloud SIEM

InsightIDR allows the MDR SOC team to integrate feeds from your existing security infrastructure, giving the Rapid7 MDR team even greater visibility into possible threats across your environment. This combination gives you real-time visibility and detection for malware, fileless attacks, and the use of stolen credentials. In fact, over 90% of all InsightIDR detections occur at or before “Credential Access,” well before any significant attacker impact, as shown in the graphic below.



Source: Rapid7 Managed Detection and Response Q1 2019 InsightIDR Detections

RAPID7

The back-end of the MDR service is InsightIDR, Rapid7’s modern cloud SIEM that leverages both User and Attacker Behavior Analytics to detect intruder activity, cutting down on false-positives and days of work for security professionals.

InsightIDR goes beyond traditional SIEM monitoring, uniting data from endpoints, logs, and cloud services in a single tool to hunt all of the most common attack vectors behind breaches.

By alerting on stealthy intruder behavior as early as possible in the attack chain, InsightIDR provides the comprehensive information and automation capabilities needed to take swift action on threats before they get out of hand.

As a customer of Rapid7 MDR, you’ll have full access to InsightIDR, giving you visibility into the product to perform log searches, create custom alerts for your team, and conduct incident investigations leveraging InsightIDR and all data available in the tool.

LAYER 2

Insight Agents

Endpoint Detection & Response Agent

InsightIDR's primary data source for detection and response comes from the Insight Agent, a lightweight yet powerful software you can install on any asset—whether in the cloud or on-premises—to collect and analyze endpoint data from critical and remote assets across your IT environment.

The data passed to the analyst team by the Insight Agents allows the MDR analysts to get as close to the attacker as possible and perform endpoint investigations and threat hunt with system-level visibility. This endpoint data is parsed against real-time threat intelligence insights from the Rapid7 customer base and sophisticated behavioral analytics (tuned with an in-depth understanding of your business) to uncover threats across your internal network and cloud services.

Without an agent to collect and analyze critical data on the endpoint, customers are unable to detect advanced threats and cannot query the asset, either for incident investigation or response.

The Rapid7 Insight Agent provides critical, real-time visibility across your Windows, Mac, and Linux assets—no matter where they are in the world. You can detect modern malware that evades today's antivirus tech, gain visibility into your assets, and even take action through the agent to contain a found threat.

The Insight Agent is able to provide context to anomalous behaviors by analyzing:

- Running processes
- Security events
- System event codes
- Registry data
- Intruder traps
- Asset and user data
- File audit logs
- File and package data

LAYER 2

Insight Sensor

Network Traffic Sensor

While the Insight Agents are responsible for collecting data on your assets, they do not account for network traffic, which is the data moving between your assets. To provide the network traffic visibility that's needed to detect attackers, Rapid7's Insight Network Sensor allows you to monitor, capture, and assess the end-to-end network traffic moving throughout your physical and virtual environment.

Network traffic monitoring is an increasingly significant security gap for organizations today. As a security practitioner looking to minimize your attack surface, you need to know of the types of network data traversing your network and how much of that data is moving, which are two critical areas that could indicate malicious activity in your environment.

InsightIDR can use network sensor data to generate investigations and alerts based on the network traffic traversing your environment based on IPv4 flow data. InsightIDR also leverages DNS and DHCP information that the network sensor extracts from network packets to produce other actionable alerts.

After the data becomes available in InsightIDR, the processed network traffic can be further leveraged as a foundation for log searching, data analysis, building custom reports and dashboards, top external clients making inbound connections, and other data points.

The Insight Sensor is able to provide this while adding several benefits to ensure the tool provides value without downside:

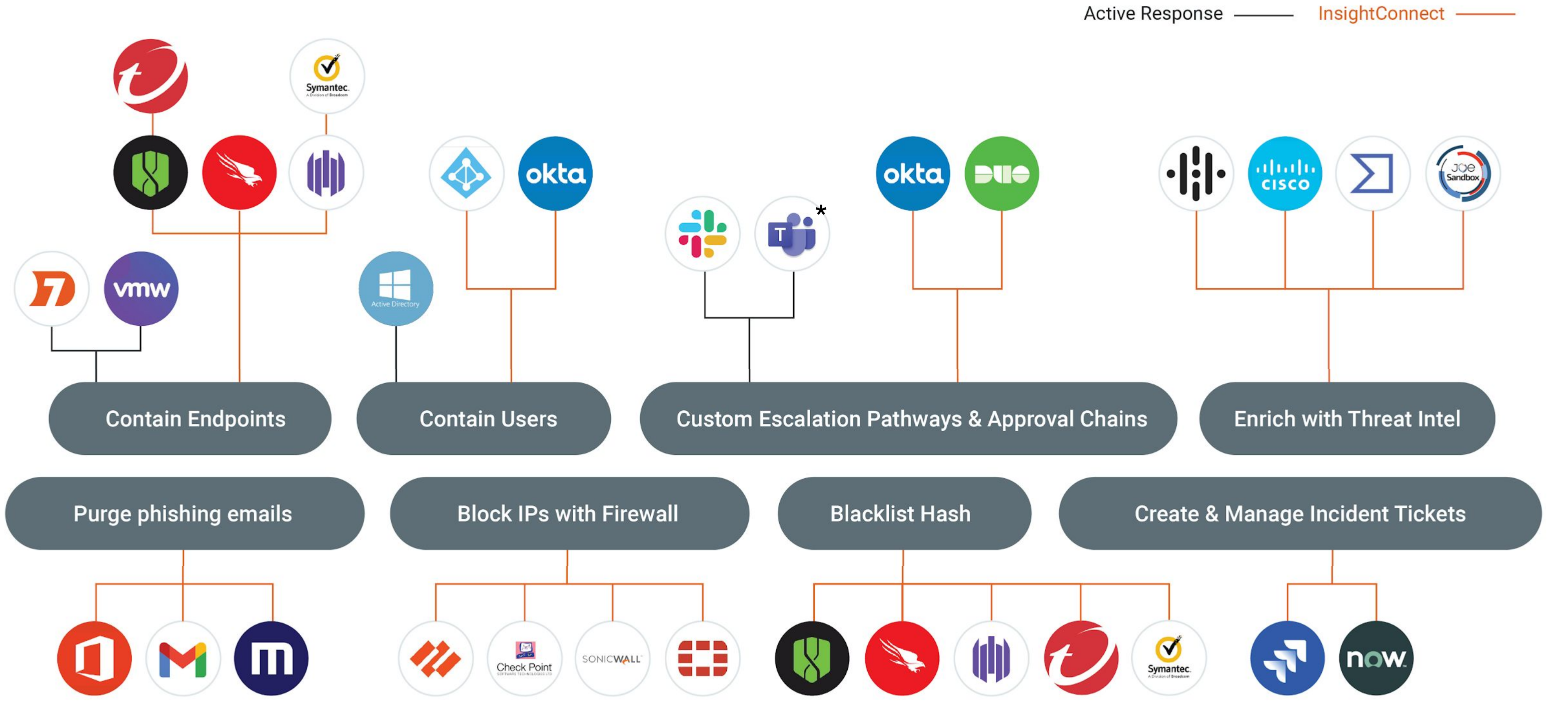
- Passive monitoring
- Works on any network
- Efficient data collection
- Ideal for sensitive environments
- One data set for multiple use cases
- Rapid time to value

LAYER 2

InsightConnect

Security Orchestration and Automated Response

MDR Elite customers have the option of enabling **Active Response** which leverages a limited license of Rapid7's SOAR solution, InsightConnect, to drive advanced workflows for immediate response to endpoint- and/or user-based threats. Customers can further extend their SOC automation capabilities and streamline IT and security operations with a full license of InsightConnect.



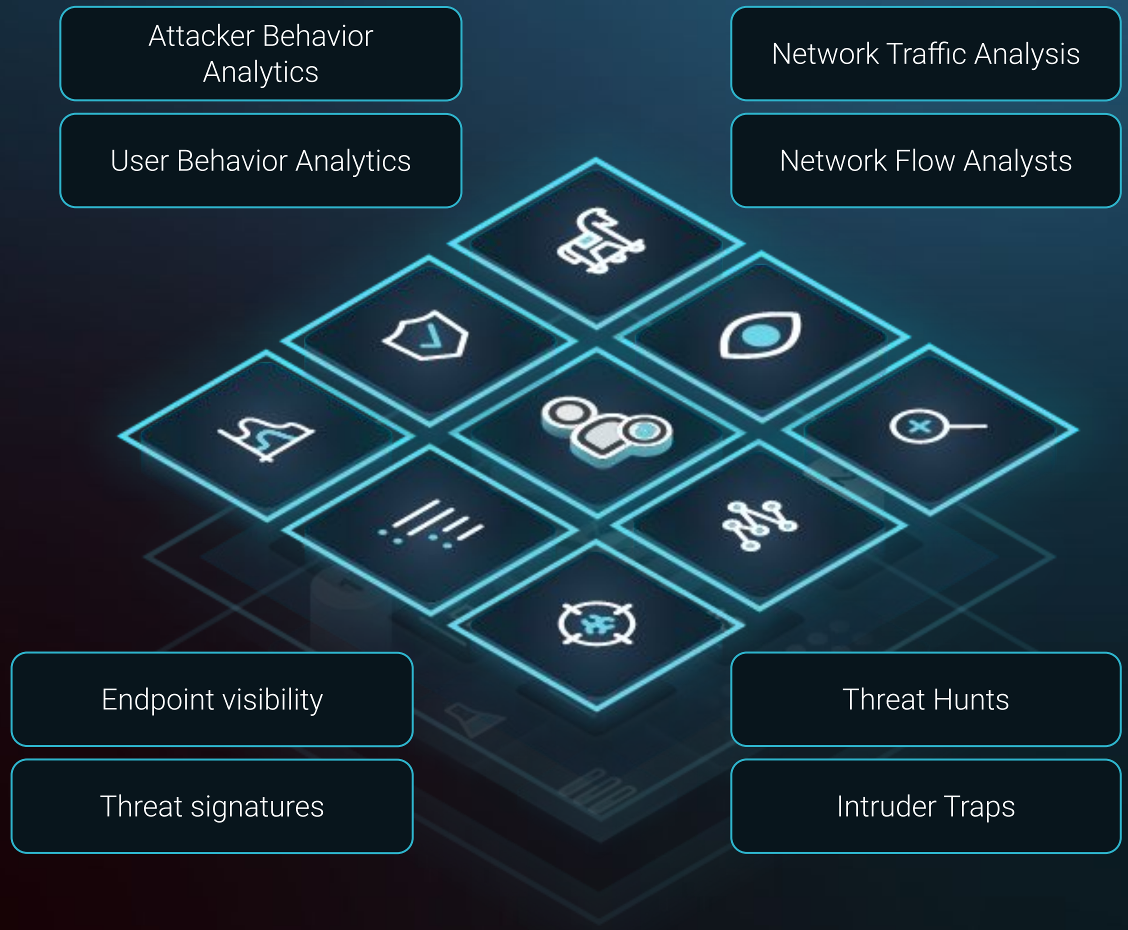
* Integration coming soon

Strengthen your defenses and create efficiencies across your entire security program with Rapid7 Managed Detection & Response (MDR) and InsightConnect.

- Respond quickly and effortlessly by automating workflows
- Let our SOC contain threats immediately with Active Response and lower your Mean Time to Respond (MTTR)
- Have confidence your team can respond to any threat - either through MDR with Active Response or by using automation
- Automate tedious, manual tasks to free your analysts time to take on greater challenges
- Connect disparate technology solutions so your workflow works for you, not the technology

LAYER 3

Detection Methodologies



Attacker Behavior Analytics

User Behavior Analytics

Network Traffic Analysis

Network Flow Analysts

Endpoint visibility

Threat signatures

Threat Hunts

Intruder Traps

LAYER 3

Rapid7 MDR SOC employs a multi-dimensional approach to detect malicious activity across the attack chain for both known and unknown threats.

Each detection through InsightIDR is validated by our SOC analysts to ensure we only pass true threats in our reports.

- Behavioral detections for user and host anomalies
- IDS, DNS, DHCP, and Network Traffic and Flow detections
- Monthly proactive human threat hunting by your SOC Pod
- Threat intelligence-based detections
- Intruder trap technologies such as honeypots, honey users, and honey files.

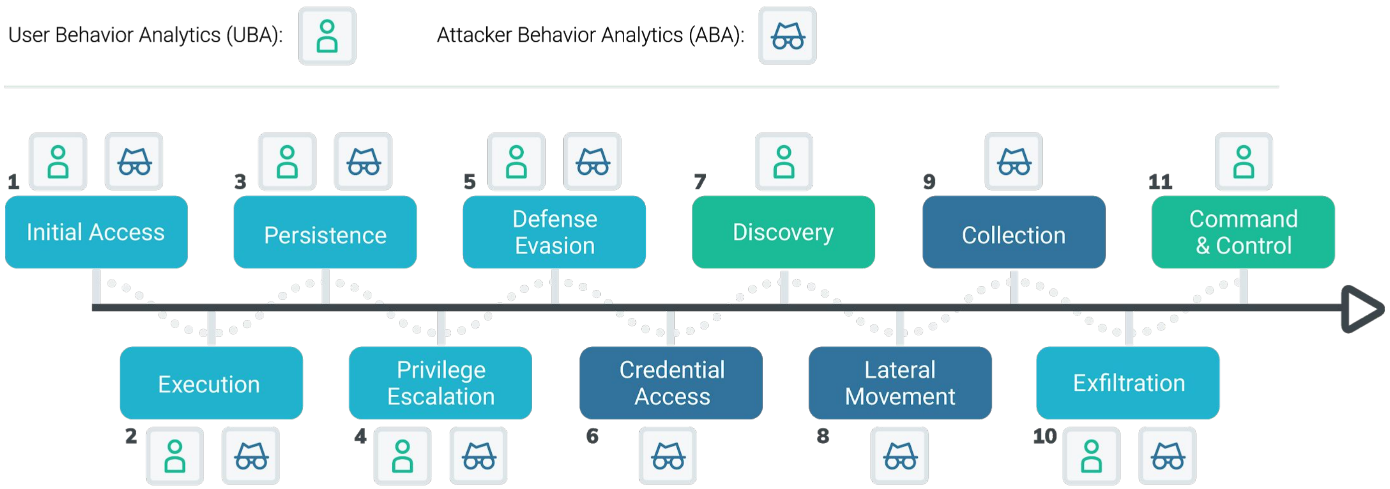
LAYER 3

Detection Methods

Behavior-Based Detections

The detection our team provides across the attack chain stems from a combination of User and Attacker Behavior Analytics, endpoint data, and deception technologies that can detect threats across the MITRE ATT&CK framework.

Effective implementation of user- and deviation-based detection methodologies requires deep visibility into endpoints, network metadata, authentication/authorization events, and logs, coupled with purpose-built technology and subject-matter expertise provided by the Rapid7 SOC.



User Behavior Analytics (UBA):

Attacker Behavior Analytics (ABA):

1 Initial Access

2 Execution

3 Persistence

4 Privilege Escalation

5 Defense Evasion

6 Credential Access

7 Discovery

8 Lateral Movement

9 Collection

10 Exfiltration

11 Command & Control

InsightIDR includes thousands of pre-built detections in InsightIDR to identify intruder activity, cutting down false positives and enabling analysts to only alert you to true threats.

Additionally, InsightIDR baselines all users and actions to augment these pre-built rules with analytics detections to find anomalous and concerning activity. These behavior analytics detections are bolstered with intruder traps, additional data sources, and explicit indicators of attack behaviors.

All potential malicious detections are manually validated by our SOC analyst team prior to reporting any alert to you to remove benign, unnecessary, or redundant behaviors from your **Findings Reports**.

As a key advantage of our cloud deployment model, our detections are updated automatically to our entire user population—including MDR customers—after a thorough prototyping, testing, and validation process. All new indicators are applied to one month’s historic data so your environment is instantly protected.

LAYER 3

Detection Methodologies

Attacker Behavior Analytics (ABA)

Attacker Behavior Analytics (ABA) applies Rapid7's existing experience, research, and practical understanding of attacker behaviors to generate investigative leads based on known attacker tools, tactics, and procedures (TTP). These include:

- Malware, malware droppers, maldocs, and fileless malware (opportunistic and targeted)
- Cryptojacking (stealing CPU cycles to mine cryptocurrency)
- Pen testing and attack tools
- Suspicious persistence
- Anomalous data exfiltration
- New attacker behavior

ABA detection methods are constantly updated by MDR SOC investigations, combined with Rapid7's research and threat intelligence analysts to extract key behaviors from threats identified in our customer environments. After performing research on related attacks and behaviors, we craft new ABA detections that are deployed across all MDR customers to simplify and accelerate detection and reduce the time to remediation.

Found once, applied everywhere: Your security team gets the benefit of the learnings from other MDR customer investigations.

When our SOC team finds new attack methodologies—either by way of our SOC, threat intelligence team, or Rapid7 research—those TTPs are updated in InsightIDR and applied to all MDR customers and investigations

Detections based on behaviors, not signatures: Through InsightIDR, our SOC team is armed with high-fidelity endpoint data to identify novel variations of new attacker techniques.

High-fidelity alerts grant context to take action: Alerts include context from our analysts and threat intel teams, so you can make better decisions, remediate the problem, mitigate risk, and contain the alert from directly inside your **Findings Report**.

Constantly evolving ABA detections: Whenever possible, the alert will detail known, recent adversary groups using a similar technique in a confirmed attack.

Detection Methodologies

User Behavior Analytics (UBA)

User Behavior Analytics (UBA) enables our SOC team to more easily determine whether a potential threat is an outside attacker impersonating an employee or an actual employee who presents an internal risk, whether through negligence or malice.

UBA connects activity on the network to a specific user as opposed to an IP address or asset. This is then compared against a normal baseline of event activity for that user. Once collected and analyzed, it can be used to detect the use of compromised credentials, lateral movement, and other malicious behavior.

InsightIDR provides our SOC team with a technological advantage by utilizing our proprietary attribution engine with models that are purpose-built to detect behaviors indicative of true threats, while sorting out users who may be doing unusual tasks but are not actually compromised or performing malicious actions. Many traditional SIEM solutions claim to utilize UBA detections, but SIEM engines aren't built for real-time attribution, unlike Rapid7's InsightIDR technology. This is because users and assets constantly move around in a modern network architecture, leading to an engine that cannot accurately map events to entities.

Our SOC leverages these UBA indicators to dynamically prioritize and rank alert criticality based on the presence or absence of notable behaviors associated with the alert by:

- Detecting unknown threats based on single occurrences, or groups of notable events based on specific user behaviors or deviations from known-good baselines.
- Detecting insider threats based on groups of notable events describing the sequence of events typically associated with information theft by an authorized party.
- Associating user behaviors based notable events to alerts and investigations to improve the validation and investigation analyst workflows.
- Providing the data needed to associate technical evidence with human understandable behavior for threat reporting.

Detection Methodologies

Network Traffic Analysis (NTA)

IDS, DNS, & DHCP Network Traffic

Traditional Intrusion Detection System (IDS) tools can be incredibly noisy. The Rapid7 MDR team has carefully filtered IDS events to capture only the most critical and actionable detections for teams to focus on, helping cut down on noise and increase analyst's confidence in taking action. This means when malware, botnets, or other compromises are detected, our team won't have to go through tedious cycles to determine their validity. Our analysts can confidently take action on reliable, vetted alerts.

Network Flow Data

In addition to the IDS, DNS, and DHCP network traffic analysis detections, Rapid7 also leverages a proprietary Deep Packet Inspection (DPI) engine to capture all raw network traffic flows, extracting rich metadata. Rapid7's proprietary DPI engine captures and analyzes traffic in readable, interpretable details, without the complexity and overhead of full packet capture. This passive analysis approach drastically reduces data volume while retaining the critical data ideal for investigations, deeper forensic activities, and custom rule creation. With this rich flow data, our analysts have deep detail with which to track attacker entry and movement across the network so they can accelerate investigations and better inform response action.

With the lightweight Insight Network Sensor, our MDR team can continuously monitor network traffic at any location or site across your network.

This data helps minimize the attack surface and detect intrusions (or other potential security events) on the network. Network traffic detections are generated by two data sets.

Together, these network analytics help analysts ensure continuous visibility everywhere, recognize compromise quickly, and trace the steps of potential attackers across systems and applications.

Detection Methodologies

Threat Intelligence-Based Detections

Rapid7 leverages proprietary threat intelligence derived from our TIDE and research teams, previous investigations and monitoring findings, and third-party sources. SOC analysts apply TIDE detections and incident response learnings across all MDR customer environments, leveraging expertise and data sources from the public sector, private sector, and open sources to fuel threat detection and incident response.

- **Strategic threat intelligence** is provided per industry sector and is aimed at decision-makers to help shape strategies to prevent threats from materializing.
- **Tactical threat intelligence** is applied in our attacker behavior analysis methodologies and leverages complex rules to generate investigative leads across multiple event sources and over time.
- **Operational threat intelligence** is provided by way of proactive threat reports and indicates the likelihood of an impending attack. Our reports include mitigation recommendations to increase resilience against specific threats to your organization.
- **Technical threat intelligence** in the form of indicators of compromise are applied across our customer base. The Rapid7 Threat Intelligence team actively maintains the quality of the technical threat intelligence to ensure fidelity, context, and timeliness for our MDR threat analysts.

LAYER 3

Detection Methodologies

Threat Hunting

Along with daily alert triage and Remote Incident Response, analysts also perform monthly threat hunting for MDR Elite Customers. Rapid7 MDR Threat Hunting is used to identify any potential threats that may have been left undetected by technology detections.

Hunts are initiated every month on a set schedule for every MDR Elite Customer. Additionally, threat hunts can be initiated ad hoc based on ongoing incident discoveries or critical research discovered by the MDR TIDE team.

Rapid7 MDR uses a combination of forensic and real-time data in order to perform proactive monthly threat hunting as well as an initial Compromise Assessment. The approach leverages human analysis as well as rule-based detection on the data in order to identify threats that would have otherwise not been observed through real-time alerting. The forensic artifacts that are collected focus on persistence-based detection rather than execution-based (covered by real-time).

Results from Threat Hunts are conveyed to MDR Elite Customers through monthly Threat Hunt reports.

Detection Methodologies

Deception Technologies

Some types of stealthy behavior can be difficult to discern from normal activity, allowing the attacker to sneak past your security tools and into your organization undetected. Deception technology can often help you find attackers earlier and take action to block them before they access something they should not.

Deception technology, also known as Intruder Traps, allows the MDR SOC team to create an illusion for attackers that they have found something of interest in your environment. When these intruder traps are deployed in your network, they act as a virtual trip wire. Once an attacker is tricked into accessing the trap, InsightIDR fires an alert to flag the suspicious activity.

Rapid7 MDR includes honeypots, honey files, honey users, and honey credentials with the service.

Explicit attack behavior indicators

MDR uses advanced analytics to detect compromised users/assets that don't require an established baseline of behavior to trigger. One example is the ability to detect spear phishing attempts where the domain has been spoofed (i.e., rapid7.co instead of rapid7.com).

Detection Methodologies

Enhanced Endpoint Telemetry

MDR uses Enhanced Endpoint Telemetry (EET) to gather and analyze detailed logs for every time a process starts on a monitored endpoint. Basically - everything that's happening on your endpoint - is captured by the agent and allows our team to understand what other activity happened on that endpoint leading up to any and all process executions.

This rich metadata unlocks our analysts to go beyond isolated events to understand what other activity may have happened on an endpoint, if other assets have been compromised, find other potentially compromised assets, and hunt for lurking threats.

Analysts can more easily piece together the attack and understand with high fidelity if something happening has malicious intent, or deem it to be benign and close out the investigation without needing to get your team involved.

Additionally, this rich enhanced endpoint telemetry metadata is useful for creating ABA detections, accelerating threat investigations, and facilitating complete incident response on your behalf.

Additional Data Sources

InsightIDR integrates with your third-party offerings to ingest additional data sources. These are used to add context around suspicious events, identify suspicious processes, URLs, hosts, and IPs. Alerts generated from these event sources are not investigated by Rapid7 MDR.

LAYER 4

Security Operations

Your environment will be monitored 24/7/365 by world-class SOC analysts, each with years of experience building detection and response programs, and hunting for and validating threats.

They'll act as an extension of your team for tactical detection and analysis to validate threats in your environment.

These analysts are augmented by your Security Advisor, who acts as your point of contact to the Rapid7 SOC and Threat Intelligence teams.

They'll be a trusted security resource, offering suggestions and guidance to mature your security program. Feel free to reach out to them whenever you have a question.

- Around-the-clock security operations delivered from multiple global SOCs
- Service delivery experts have an average of five years detection and response experience
- SOC experts have over 500 collective security certifications

Security Operations

The Rapid7 MDR team consists of multiple functional groups working together to ensure you receive world-class incident detection and response, providing 24/7 monitoring, unsurpassed service, and contextualized reporting that delivers real value. Consider us an extension of your internal team!

Your environment is assigned to a “SOC Pod” of security experts with unparalleled experience—both red and blue teams—that monitor your environment around the clock. Each pod is made up of six analysts and one Customer Advisor with an average of five years of security detection and response experience. Even our most junior analysts already have at least two years of experience detecting threats.

MDR Customer Engagement Model

We pride ourselves on becoming a true extension of customer teams through attentive service, visibility into our backend systems, and by providing a named resource (your Customer Advisor) to whom you can reach out for all things related to security.

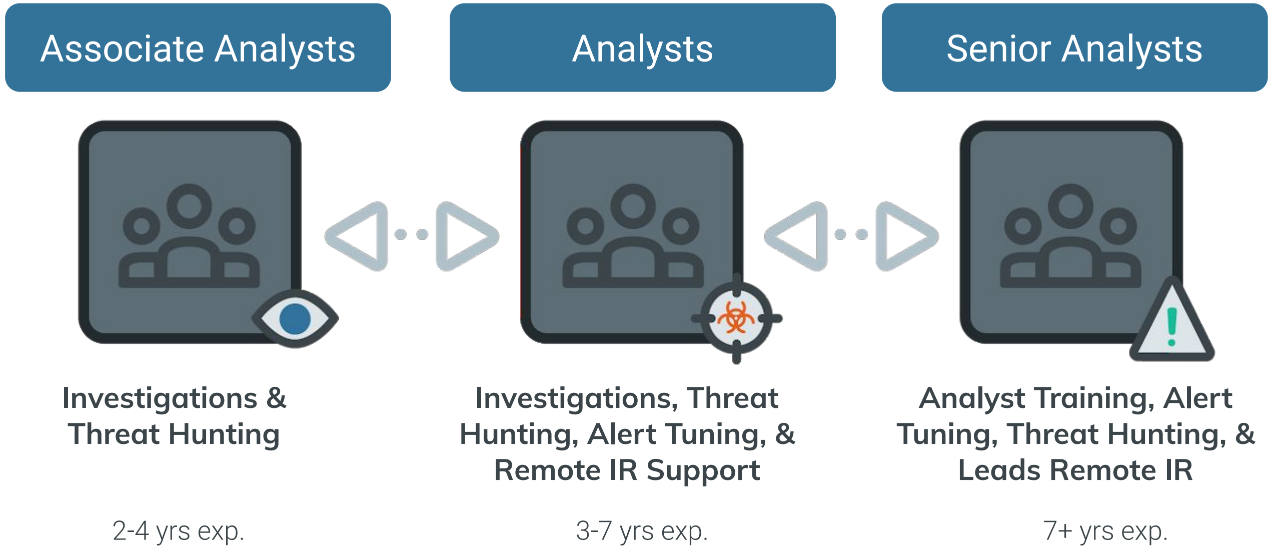
SOC Pod

Your environment is monitored 24/7/365 by world-class SOC analysts, each with years of experience building detection and response programs, and hunting for and validating threats. SOC Analysts leverage specialized toolsets, malware analysis, tradecraft, and forward-looking collaboration with Rapid7’s Threat Intelligence researchers to make detection and remediation of threats possible.

LAYER 4

Security Operations

Our SOC pod implementation ensures each customer receives continuous monitoring coverage for high- and low-fidelity alerts while giving our team scale to thoroughly identify known and unknown threats, including via threat hunts, across all customer environments.



Associate Analysts

Investigations & Threat Hunting

2-4 yrs exp.

Analysts

Investigations, Threat Hunting, Alert Tuning, & Remote IR Support

3-7 yrs exp.

Senior Analysts

Analyst Training, Alert Tuning, Threat Hunting, & Leads Remote IR

7+ yrs exp.

Together, the MDR SOC teams maintain 24/7/365 vigilance of your network, from alert validation through in-depth forensics and malware analysis of your network and users. Our combination of these roles provides optimal coverage for all threats and attacker challenges.

Associate Analysts (two per Pod) are responsible for alert triage and investigation and threat hunting. Associate Analysts have between two and four years of experience validating and hunting for threats.

Analysts (three per Pod) are responsible for alert triage and investigation, threat hunting, alert tuning, and supporting Remote Incident Response engagements. Analysts have between four and seven years of experience validating and hunting for threats.

Senior Analysts (one per Pod) serve as an escalation point and training resource for other analysts, alert tuning, threat hunting, and leading Remote Incident Response engagements. Additionally, these individuals assist in developing customer-specific detections (e.g., specific types of activities happening in the network) and work alongside our Threat Intelligence team to write new threat detections. Responders have over seven years of cybersecurity experience, including incident response.

SOC Pod Lead (one per Pod) manages the SOC teams. Leads are responsible (along with your Customer Advisor) for the MDR service delivered to their team's assigned customers.

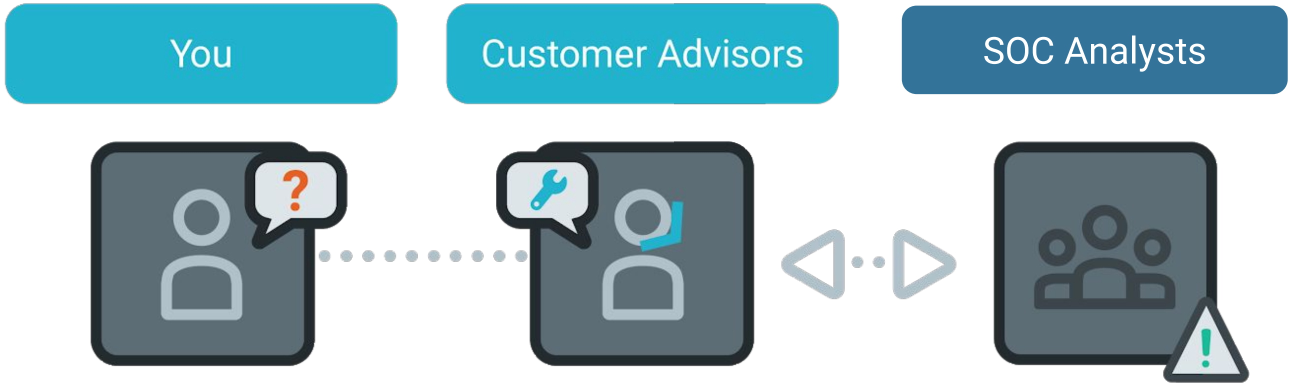
LAYER 4

Security Operations

Customer Advisor

Your SOC Pod includes an assigned Customer Advisor (CA) who is your interface with your SOC Pod and the Rapid7 TIDE team. Having risen through the ranks of technical service delivery and customer success, each CA brings domain expertise, technical acumen, and white-glove customer service.

CAs are provided to help you advance your program—from understanding the threat landscape to your MDR service to reviewing your progress. With a deep knowledge of your technical environment, they'll be your trusted advisor for tailored recommendations to strengthen your security posture.



Customers have unlimited access to talk to their CA regarding the MDR service, Rapid7 technologies, or other solutions.

Throughout the service, your CA will communicate with you frequently to:

- Act as your main point-of-contact and trusted Security Advisor
- Provide service delivery updates, contextualize metrics, and provide updates about analysis activities
- Explain every incident **Findings Report** and all recommendations for your team to take
- Educate your team on what any new threat intelligence insights mean for your specific environment and business
- Assist you with ensuring you're reaching your security outcome goals
- Aid in CISO, Executive, and Board presentations, QBRs, and changes in the threat landscape

Security Operations

Additional Members of Rapid7's Team

A unique value point for Rapid7's MDR service is the strength and expertise of our employees who work with your organization to advance your security maturity. Throughout your service, you may come in contact with many of our excellent team members, including:

- **Account Executives:** Your introductory point of contact for all presale needs. The Account Executive takes the time to understand your business challenges, explains how our technology works to solve them, and proposes solutions to help accelerate your security maturity.
- **Project Managers:** The Deployment Project Manager leads MDR deployment coordination between Rapid7 and you, the customer. This person is responsible for ensuring a seamless experience during the deployment phase and can address any issues that arise during the deployment process.
- **Deployment Consultant:** Rapid7's InsightIDR solution specialist is responsible for implementing and configuring the InsightIDR solution and for confirming configuration of all other related technology (e.g., log sources, event sources, collectors, etc.)
- **Customer Success Manager (CSM):** A Rapid7 CSM is assigned to your account for the entirety of your relationship with Rapid7. The CSM is an internal advocate who ensures your team's success by facilitating the best use of Rapid7 solutions and driving resolution on technology-related issues and requirements. This person is also your point of contact for adopting new Rapid7 solutions or expanding your solution coverage.
- **Security Operations Center (SOC) Manager:** Rapid7 SOC managers oversee and manage Rapid7 SOC operations, analyst teams, and MDR's internal infrastructure to ensure your ongoing success and coverage of your environment.

LAYER 5

Investigations & Active Response

Incident investigation & validation

Active Response

Let our experts handle investigation, validation, and response.

Whenever there's an alert, our SOC Pods perform forensic analysis to validate each alert based on endpoint and log data to eliminate false positives and document the entire attack storyboard.

If it's a true threat, our team will take action using our **Active Response** service to stop attackers in their tracks and provide you with a written summary of the incident with prioritized recommendations and clear guidance for what to do next.

- 24x7 end-to-end MDR service, including Active Response to stop threats
- Full Investigations and **Findings Reports** on validated threats
- Prioritized containment, remediation, and mitigation recommendations

Investigations & Active Response

Human Validation

Each critical alert triggered by InsightIDR is manually validated by our expert SOC analyst team. Validation is defined as the Rapid7 MDR SOC performing initial triage and investigation to determine, with a high degree of confidence, that the event is non-benign and requires customer communication. Our multi-step process weeds out these events so our team will only report threats that are actually considered malicious and need direct action taken to resolve.

Rapid7 validates alerts based on two key factors: attacker intent and observed capability. By combining adversary threat intelligence and knowledge of attack tools, Rapid7 determines the risk and potential impact of each incident ("criticality") and delivers that context in detail. This is determined during the course of an investigation, since it's not possible to assign criticality before the scope of the event is determined.

Once confirmed, we'll only report the true, real threats and suspicious lateral movement, and provide prioritized recommendations for your team in the form of a **Findings Report**. At the same time, we'll kick off a workflow through our **Active Response** service to contain the threat.

In addition to notifying your team of any validated incident that needs action, our SOC analysts also offer actionable, tailored recommendations in the Findings Report to contain the threat (if Active Response is not configured), remediation, and mitigation guidance.

The MDR SOC analyst team uses a series of detection methodologies and data analysis to validate each threat by gathering context related to the alert from your endpoints and logs to assess severity.

The result: MDR customers quickly identify and respond to attacker activity without wasting time investigating a mountain of false alerts.

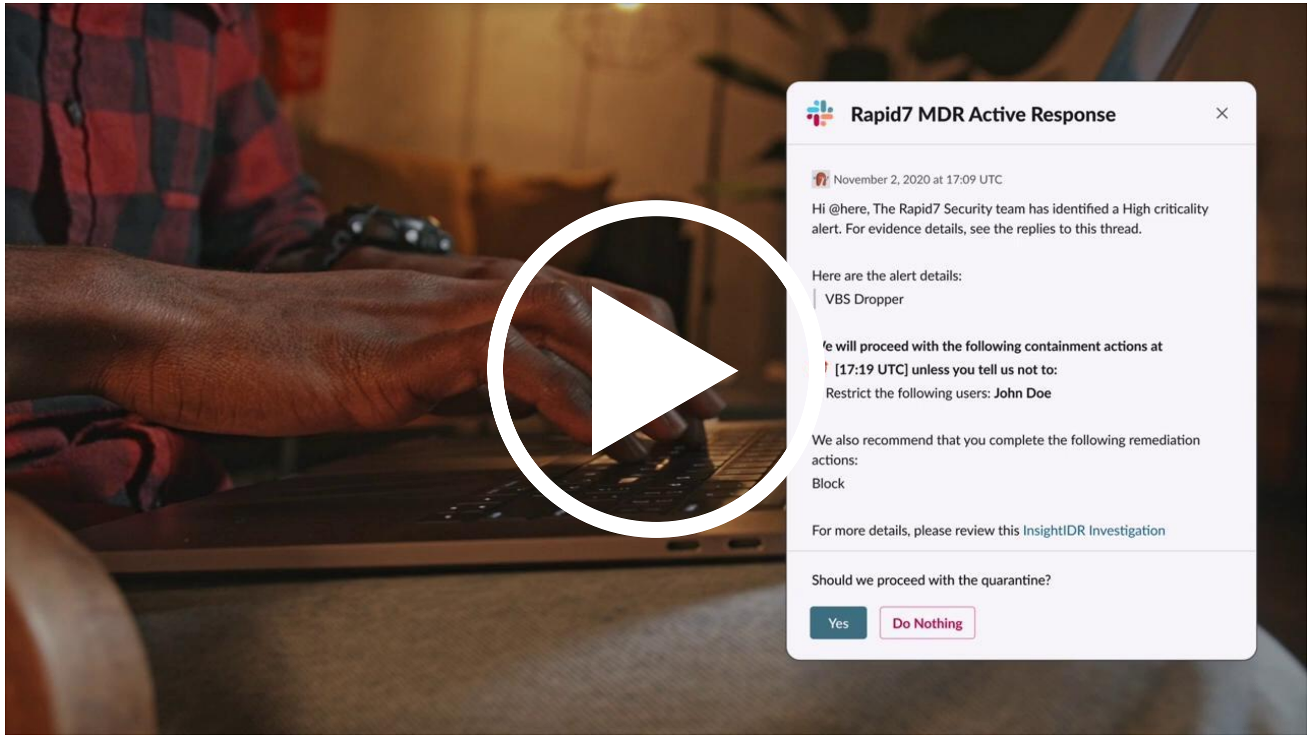
Additionally, the TIDE and the MDR SOC work closely together to tune detections to minimize alert noise and ensure alerts are as high-fidelity as possible. Alerts are assigned an internal priority to ensure the most high-fidelity detections (alerts most likely to result in a Critical or High severity threat) are prioritized and highlighted for SOC triage and investigation. This process limits the likelihood for our SOC analysts to prioritize investigation of benign and false-positive alerts over actual suspicious or malicious events, and produces extremely low false-positive reports.

LAYER 5

Investigations & Active Response

Active Response

Threats at 2AM? Let us handle it. Active Response further extends your team with 24x7 end-to-end threat detection and response to protect your business, reduce attacker dwell time, and accelerate your time to response.



Rapid7 MDR Active Response

November 2, 2020 at 17:09 UTC

Hi @here, The Rapid7 Security team has identified a High criticality alert. For evidence details, see the replies to this thread.

Here are the alert details:

VBS Dropper

e will proceed with the following containment actions at [17:19 UTC] unless you tell us not to:

Restrict the following users: **John Doe**

We also recommend that you complete the following remediation actions:

Block

For more details, please review this InsightIDR Investigation

Should we proceed with the quarantine?

Available for MDR Elite customers only, Active Response puts the power of responding to threats directly into the hands of Rapid7's MDR SOC experts, allowing our team to immediately contain users or endpoints on your behalf.

When our team detects and validates malicious activity, our SOC team kicks off containment workflows to quarantine users and/or endpoints. You can be as hands-off or as hands-on as you'd like, with options to cancel any action from your desktop or mobile device.

Unlike fully automated approaches, our approach leverages our own SOAR solution, InsightConnect, to respond using advanced workflows and humans to actually "push the contain button" so our Customers don't have to. Some MDR providers may offer a similar service that performs generic containment based on automated rules or blanket actions to cut network traffic. The difference with Active Response is that our SOC team only executes actions on validated threats and provides the flexibility for your team to configure or cancel responses. This allows us to remove the headaches of false-positive quarantines or cause more work for your team to undo the action down the line or impact users that were incorrectly quarantined.

LAYER 6

Threat Detection & Response Program Advancement

Multi-Org Support
Tailored Recommendations
Monthly Security Advisory Meetings
Ask unlimited questions any time
Quarterly Business Reviews
C-Suite & Board Presentations
6

Rapid7 MDR is designed to help any security team, regardless of size, maturity, or existing technology stack.

Our goal is to ensure we align your investment in MDR with long-term security improvement across all 20 CIS critical controls.

Our team is your team. From SOC analysts to your Security Advisors, we take the time to understand your business processes, environment, and industry so we can provide customized guidance and clear direction for your team.

Between regularly scheduled meetings and QBRs with your Security Advisor to ad-hoc questions for the SOC, you can rest assured you'll have a partner in your success.

- Easy to understand reporting with tactical guidance and recommendations
- Experts on call, whenever you need
- Regularly scheduled meetings with your trusted Security Advisor
- Get prioritized recommendations to strengthen your security program

LAYER 6

Program Advancement

As a core part of your MDR service, your team is assigned a Customer Advisor (CA) who's responsible for shepherding your program development and team along your security maturity journey. Throughout the service, your CA will communicate with you frequently via your preferred communication method and cadence, though never less than once a month for Elite customers (quarterly for Essentials customers).

Typical communications provide updates on service delivery, walk you through **Findings Reports**, and assist you with reaching your security goals. Alternatively, you can proactively reach out to your named CA or call the Customer Advisor hotline whenever you'd like to chat about the service or your environment.

It should be mentioned that many customers have leveraged Rapid7 MDR and the CA mentorship as a "do it with me" stepping-stone as they develop their own in-house detection and response program leveraging the already familiar InsightIDR SIEM.

Security Operations

Key Customer Advisor Engagements

As part of being a true partner in your security success with MDR, Customer Advisors go above and beyond in creating report read-outs, answering questions about your service, and assisting with InsightIDR.

Scheduled Meetings

As part of the monthly or quarterly check-ins, Rapid7 CAs will provide metrics and context surrounding analysis activities performed by the MDR analysts, technology health, and findings summaries. These reports serve as an at-a-glance overview of MDR activities. Your CA will also provide additional context for what any emerging threats discovered by TIDE mean for you and your business.

Ad-Hoc Questions and Meetings

Whenever you have a question, you can always reach out to your CA to chat or speak with someone in the CA organization through our 24x7 hotline for any service or product questions or concerns. For Elite customers, you can reach out an unlimited number of times—every day, if you'd like! Consider your CA an extension of your internal team.

Quarterly Business Reviews

In addition to scheduled meetings, each customer receives a Quarterly Business Review (QBR). These QBRs are designed to review the past quarter's activities and review how MDR can best support you to advance your security maturity.

Quarterly Business Reviews include:

- Review of the MDR service
- How you're tracking against our program success scorecard
- Helping you showcase your ROI to executives
- Trend reporting for alerts, incidents, and threat findings
- Education about the latest in the attack landscape
- Guidance to improve your holistic security posture

Program Advancement

MDR Deliverables

Rapid7 MDR's deliverables are created with program advancement in mind. Our reports are designed to give you confidence that your program and your knowledge will improve as a customer.

Findings Reports

Once alerts are investigated and verified, our SOC analysts produce a Findings Report—also called an "incident report" in some instances—delivered via the Customer Services Portal (with alerts via email or phone call, per the customer's request). This report is a summary of the incident, with detailed evidence of the threat, recommended containment actions, remediation guidance, and mitigation recommendations.

Quarterly Threat Landscape Reports

This report is a highly targeted analysis that leverages the power of our threat intelligence infrastructure, including **Project Heisenberg**, **Project Sonar**, and third-party threat intel with a global footprint to monitor and detect patterns in the wild. Many of these findings could impact your environment; we'll use this information to develop rules to scan your environment, which can be used to perform more real-time asset hardening. Often, these reports are requested for key briefings to help prepare teams for potential attacks, and to focus resources on critical risks.

A sample Quarterly Threat Landscape report can be viewed here.

Findings Reports contain:

- Investigation details
- Written analysis
- Incident criticality
- Containment recommendations (how to contain the endpoint or user)
- Remediation recommendations (how to resolve this finding)
- Mitigation recommendations (potential ways to prevent future recurrence)

View a sample Findings Report.

View a Quarterly Threat Landscape Report.

View a Quarterly Incident Summary Report.

LAYER 6

Program Advancement

Monthly Service Reports

This report will provide you with metrics and context for analysis activities performed by the MDR analysts, as well as technology health and findings summaries. These reports serve as an at-a-glance overview of MDR activities and can be used to prove the value and ROI of MDR to executive leaders.

The Customer Advisor will review this recap summary with all stakeholders of MDR on the scheduled call to make recommendations to reduce risk over time. This occurs at a monthly cadence for Elite customers, and on a quarterly cadence for MDR Essentials customers.

Urgent Threat Intel Reports

Urgent Threat Intel reports are generated ad hoc when Rapid7's Threat Intelligence infrastructure or third-party threat intelligence partners identify new vulnerabilities or detection patterns. This report is a detailed analysis of the threat to inform you of our team's findings and to help you better understand the global risk environment. The MDR team will also leverage this information to develop rules to scan your environment.

Monthly Service Reports include:

- Alerts generated and resulting Findings Reports created
- Closed alerts by disposition (criticality and type)
- List of all closed alerts
- Endpoints, users, and administrators under monitoring
- Event Source connectivity health

View a Service Report.

View an Urgent Threat Intel report.

LAYER 6

Program Advancement

Monthly Threat Hunt Reports (MDR Elite Only)

Each month, our team combs through data from your environment to conduct proactive threat hunts. These hunts will uncover unknown threats in your environment and present data from the MDR analyst's forensic acquisition.

Hunt Reports contain metrics and findings related to proactive threat hunts using analyzed data from our endpoint metadata and forensics collected by the Insight Agent to identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies.

Threat Hunt reports can include, but are not limited to:

- Evidence of threats from MDR-curated indicators of compromise
- Remote access solutions
- Cloud storage solutions
- Potentially unwanted programs (PUPs)
- Administrator utilities
- PowerShell invocation
- Webshell activity
- Lateral movement
- Ingress authentication
- Server Message Block (SMB) egress
- Potentially vulnerable open ports

View a Hunt Report.

Value Adds

Compromise Assessment

The Compromise Assessment ensures there is not active malicious activity in your environment or evidence of previous compromise(s). If the Compromise Assessment finds that there is currently a compromise or detected malicious activity, Rapid7 will suggest the customer utilize one of their Remote Incident Response engagements.

Additionally, the Compromise Assessment allows our SOC analysts to familiarize the Rapid7 team with your security environment and provide actionable recommendations to bolster your security posture, and—if enacted—reduce the risk of future compromise.

The Compromise Assessment appraises your environment to validate evidence of attacker infiltration, active or historic compromises, potential avenues for future breaches, and actionable steps for remediation and mitigation, including:

- **Operating system-specific malware persistence mechanisms and process injection methods:** We review currently running processes, scheduled tasks, and common hiding places to detect anomalies in behavior and communications.
- **Common attacker tools:** We find evidence of attacker activity, including modified registry keys or executable files left behind, to validate suspected compromise.
- **Attacker lateral movement:** We apply threat intelligence and User Behavior Analytics to uncover the attacker pathway in real time by analyzing common attacker behaviors, including compromised credentials and ingress from suspicious locations.
- **Indicators derived from investigations:** We evaluate an exhaustive list of compromise indicators, such as privileged user account anomalies, geographical irregularities, or suspicious registry changes. InsightIDR detections are constantly updated with IOCs from MDR investigations, Remote Incident Response, penetration testers, Incident Response team engagements, and Rapid7-hosted events (e.g., Capture the Flag challenges) to improve the product's capabilities to detect anomalous activities.
- **Environment-specific considerations:** We take the time to understand your environment and the relationships between users, hosts, and processes (UHP) to identify any artifacts in the kill chain.

View a Compromise Assessment Report.

On-Demand Remote Incident Response

If our SOC team validates a confirmed breach that expands the scope of a typical **Findings Report** or your team identifies an internal security incident, you can utilize one of your "On-Demand Remote Incident Response" engagements included in your MDR service.

A Remote Incident Response (RIR) is a technical process handled by the Managed Services SOC triggered upon compromise. RIRs scope, investigate, and respond to a customer threat urgently with the optimal goal to prevent the issue expanding to need to engage a dedicated emergency IR response team.

Examples of reasons MDR would initiate a Remote Incident Response:

- Evidence of previously unknown attacker activity
- Evidence of attacker activity affecting multiple endpoints
- Evidence of lateral movement, data exfiltration or staging

Since the goal of RIR is to remove attackers and secure your environment, the RIRs included in your MDR service is not time- or resource-capped and can be used at any time from the time the contract is signed during the calendar year. MDR Elite customers are allotted two RIRs per contract year. MDR Essentials customers are allotted one RIR per contract year.

Once you have transitioned to RIR, the MDR team (led by Senior Analysts with Incident Response experience), will analyze the security incident to identify the scope of compromise, affected systems and accounts, malware used by the attacker, and attacker command and control channels. This includes:

- **Remote technical analysis and incident scoping:** Analysis of any data source, including data generated by the Insight Agent, and other analysis techniques to include full disk forensics.
- **Communications and updates:** Daily debrief of the day's investigation results and progress. Substantive findings (such as an increase in incident scope or impact) will be communicated regularly as discovered. Written weekly Summary Status Reports will be produced if the engagement exceeds a week.
- **Final report:** At the conclusion of the Remote Incident Response, Rapid7 will provide a final report detailing attacker activity supported by evidence with executive summary, findings details, analysis, root cause, and recommendations after the completion of the RIR investigation.

Purple Team Exercises

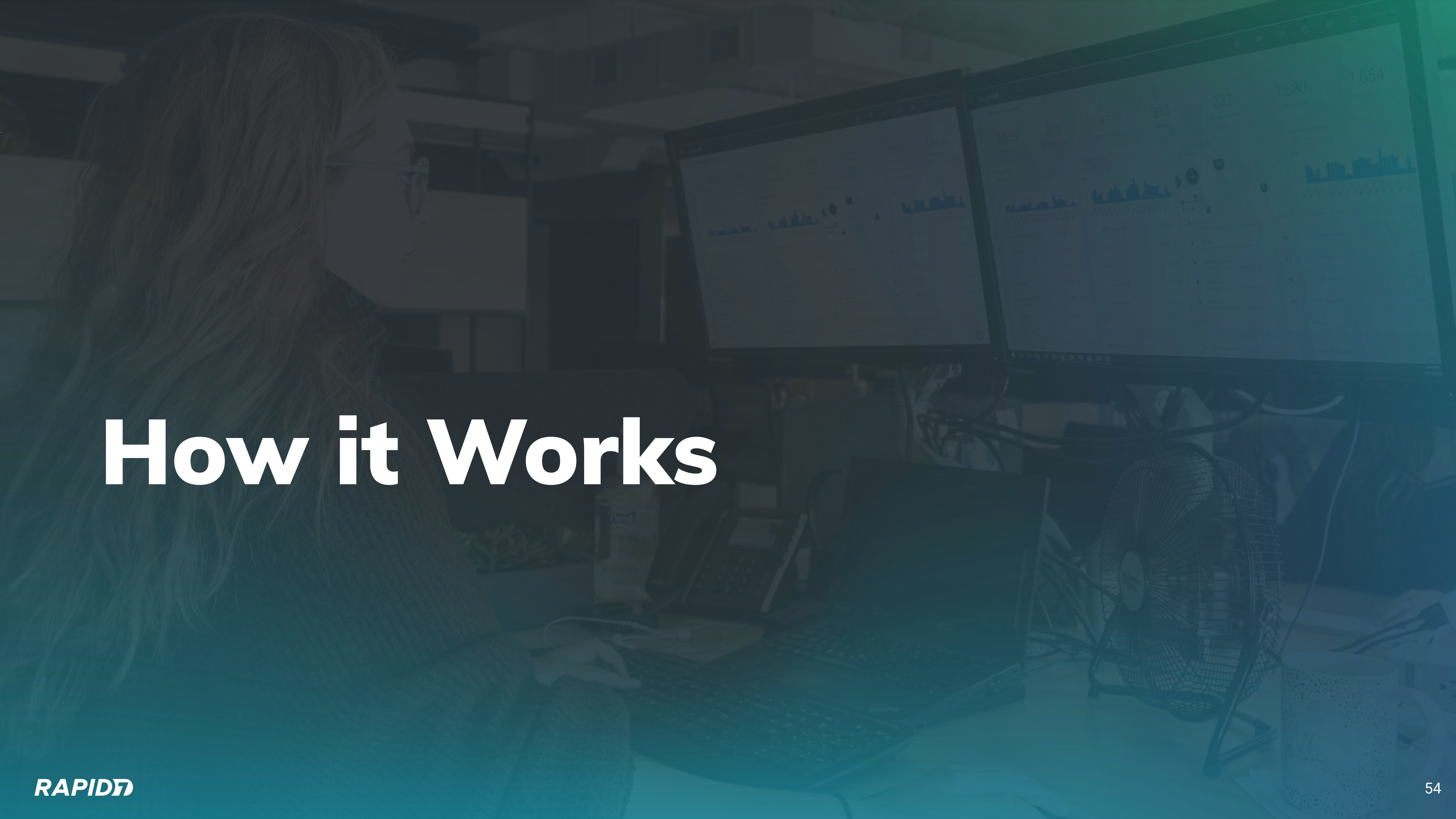
Many MDR customers integrate routine penetration testing into their holistic security strategy to perform end-to-end evaluations of all cybersecurity measures, including prevention, detection, and response. As an integral aspect of your cybersecurity controls, MDR works on your behalf to identify malicious activity, provide initial containment actions (if **Active Response** is enabled), and guide your team with detailed remediation and mitigation steps.

If your team wishes to test Rapid7 MDR's capabilities, we offer the option for a "Purple Team Exercise" where our SOC will treat the penetration test as an actual attack with all the resulting deliverables and updates. These include:

- All Remote Incident Response deliverables
- Optional: An "After Action Report" may be generated upon request to address any specific detection and response gaps (if applicable) and planned/recommended remediation steps. In order for Rapid7 to generate this report, your team must provide Rapid7 with sufficient detail about the activity performed during the penetration test (dates, systems, usernames), ideally in the form of the final penetration test report.

As part of the engagement, we'll partner to test both MDR and your capabilities to respond, including taking all recommendations for containment, remediation, and mitigation to simulate a live response to these attacks.

If Active Response is enabled, Rapid7 will perform actions to contain the threat as it relates to the Active Response service. Performing response actions in real-time will result in a more accurate simulation of an attack and subsequent response. Additionally, this prevents the MDR SOC against "unbounded" engagements that impact Rapid7's service delivery to all customers.



How it Works

MDR Responsibilities Matrix

	Rapid7 MDR	Main POC	Security & IT	C-Suite
Initiation Phase				
Define Internal Remediation contact(s) for Reports		✓		
Set up customer in InsightIDR	✓			
Enable Customer in Customer Services Portal	✓			
Deployment Phase				
Deploy Insight Agent to all servers and workstations		✓		
Download and Install Collectors		✓		
Deploy Deception Technologies		✓	✓	
Deploy Insight Network Sensor	✓	✓		
Install orchestrator and Active Response workflows		✓	✓	
Configure all available event sources	✓	✓		
Firewall rules complete		✓		
InsightIDR Walkthrough	✓	✓		

MDR Responsibilities Matrix

	Rapid7 MDR	Main POC	Security & IT	C-Suite
Service Delivery Phase				
Compromise Assessment (If in Full Service)	✓			
Customer Advisor Communication Process				
Monthly Meeting	**Elite Only**			
Quarterly Meeting	✓			
Board and Executive calls (optional)	**Elite Only**	✓		✓
Ad-Hoc Calls	**Elite Only**	✓	✓	
Monitoring Phase				
SIEM Tuning	✓			
24x7 Environment Monitoring				
Triage & Investigate MDR, ABA, UBA, & Network Traffic alerts	✓			
Validate investigated alerts to remove false positives (includes requests for customer information)	✓	✓		
Validate alerts and remove false positives from Customer's custom alerts and third-party alerts		✓	✓	

MDR Responsibilities Matrix

	Rapid7 MDR	Main POC	Security & IT	C-Suite
Monitoring Phase (continued)				
Detailed malware and/or malicious activity analysis	✓			
Attack storyboarding	✓			
Write and assemble Findings Report	✓			
Customer outreach to ensure Findings report and all recommendations are understood	✓	✓		
Initial containment (via Active Response)	Elite Only			
Additional remediation and mitigation actions		✓	✓	
Monthly Threat Hunting				
Analyze historical data	Elite Only			
Threat hunting	Elite Only			
Threat reporting	Elite Only			
Remediation and mitigation actions performed		✓	✓	

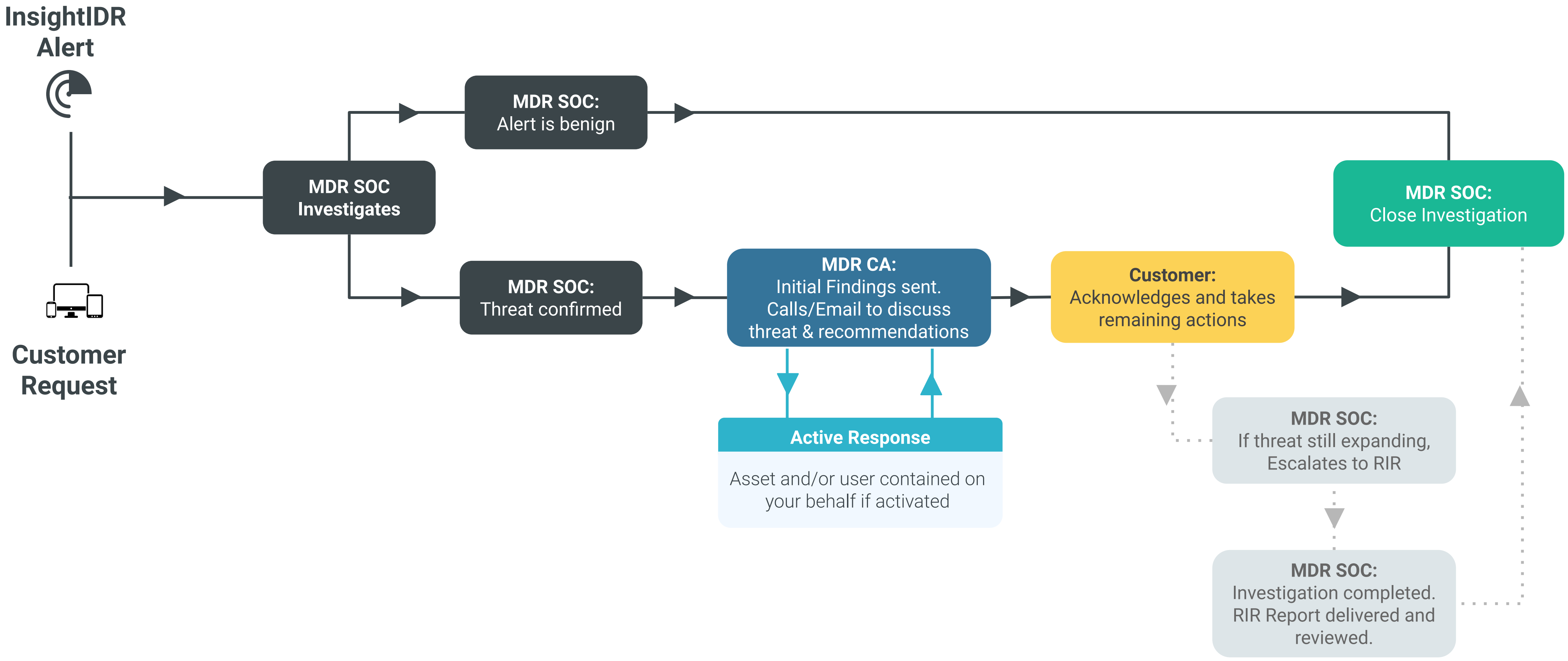
INTRODUCTION
YOUR ADVANTAGE
SERVICE LAYERS
VALUE ADDS
HOW IT WORKS
DEPLOYMENT
APPENDIX

MDR Responsibilities Matrix

	Rapid7 MDR	Main POC	Security & IT	C-Suite
Monitoring Phase (continued)				
Threat Intelligence				
Monitor global attacks and vulnerabilities	✓			
Share research and findings in Threat Intel reports	✓			
Add Threat Intel findings to monitoring detections	✓			
Remediation and mitigation actions performed		✓	✓	
Remote Incident Response (with service, otherwise need IR Retainer)				
Suggestion for Remote Incident Response in the case of a confirmed breach (after actions taken in Findings Report do not remove threat)	✓			
Acceptance of Remote Incident Response	✓			
Scoping of breach	✓			
Reporting of findings	✓			
Presentation of findings	✓			
Remediation and mitigation actions performed		✓	✓	

MDR Investigation Workflow

CA = Customer Advisor
RIR = Remote Incident Response


InsightIDR Alert

Customer Request

MDR SOC Investigates

MDR SOC: Alert is benign

MDR SOC: Threat confirmed

MDR CA: Initial Findings sent. Calls/Email to discuss threat & recommendations

Active Response

Asset and/or user contained on your behalf if activated

Customer: Acknowledges and takes remaining actions

MDR SOC: Close Investigation

MDR SOC: If threat still expanding, Escalates to RIR

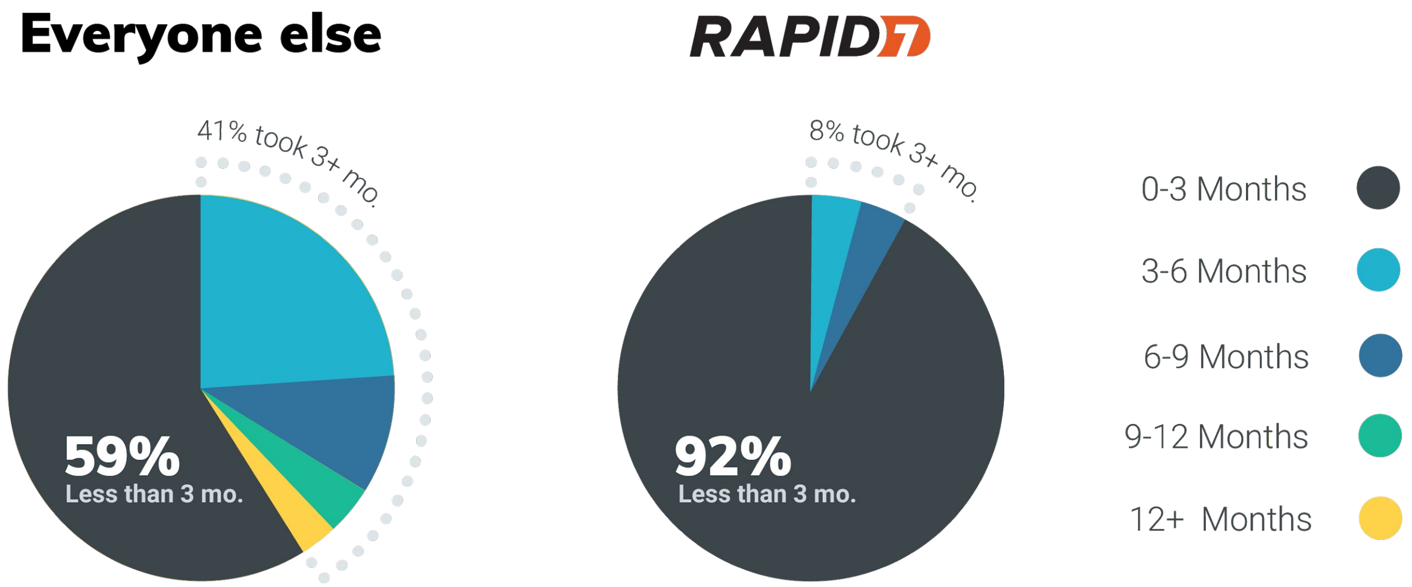
MDR SOC: Investigation completed. RIR Report delivered and reviewed.

Deployment

Deployment & Success Plan

MDR Technology Deployment

As the only true SaaS SIEM on the market today, InsightIDR deploys faster then competing SIEM solutions. With this advantage, our team is able to stand up our MDR service within weeks.



Customers that already have the Insight Agent deployed in their environment significantly reduce the level of effort required to be 100% optimized as a Managed Services customer.

We work with our customers to deploy as quickly as possible to see value in your MDR purchase fast.

The deployment process relies on your assistance to set up the technology and deploy agents. For that reason, we provide guidance to ensure all necessary tasks are completed and product expert resources to set your environment up for success.

We rely on our customers to ensure all necessary tasks are completed on their end. All required actions are outlined in the deployment timeline in this document.

Week-by-Week Success Plan

Customers should expect the following milestones and operational results as a Rapid7 MDR customer:

Onboarding Phase	Weeks	Milestones
Pre-Deployment	**1 - 2**	● Rapid7 MDR provisions your InsightIDR License ● Complete your Pre-Deployment Tasks ● Complete Deployment Introduction Call ● Complete your Customer Advisor Kickoff Call
Deployment & Baselining	**3 - 6**	● Deployment completed! ● MDR SOC verifies your environment is ready to move into monitoring! ● MDR starts alerting on malicious activity
	7 - 9	● Product Training and MDR Education Completed ● Monthly Threat Hunts begin ● You're able to use Log Search for all available sources
Ongoing Service Delivery	**10 - 12**	● Compromise Assessment completed
	12+	● You'll begin receiving service deliverables: ○ Monthly alert roll-up ○ Proactive threat hunt findings ○ Threat intelligence review ○ Quarterly goal review

MDR Launch Phases

Rapid7 MDR Onboarding in broken into three phases, including:

1. Pre-Deployment
2. InsightIDR Configuration and Enablement
3. Baselining

Once Deployment is completed and full insight agent coverage is verified, Rapid7 SOC will begin the monitoring and threat assessment phase.

The following hypothetical deployment timeline is for an MDR Elite customer.

1) Pre-Deployment Phase

What to Expect

In Pre-Deployment, you will be introduced to your Product Consultant, who will assist you with InsightIDR configuration and enablement, and a Customer Advisor representing the Managed Services team, who will be responsible for verifying your environment and kicking off your service. MDR Deployment follows a flexible schedule approach, allowing you to more freely book time that aligns with your team's availability.

Task	MDR Milestones	Duration	Details
1.1	Set you up with your InsightIDR instance	1 day	You'll receive Log In details for InsightIDR via email
1.2	Set you up with access to your Customer Portal	1 day	You can access the Customer Portal. This Portal will contain all MDR deliverables.
1.3	Enable your team with Support Credentials	1 day	Enable Support credentials enabled
1.4	Receive the MDR Welcome Email from Operations Coordinator	1 day	The Welcome Email will Introduce you to your Security Consultant and Customer Advisor Representative. The email also includes: ● MDR Deployment Guide ● Service Activation Request Form ● Deployment introduction call booking link
1.5	Deployment Introduction Call	1 day	Your Product Consultant will review: Your current state, resources for pre-deployment tasks, outline requirements for Service Activation, and define specific roles and responsibilities for your team
1.6	Complete Deployment Prerequisites	3 day	Pre-deployment tasks outlined in the resources provided in the welcome email are completed and your environment is ready to move to the "Deployment" phase. Deployment Sessions must be scheduled by the customer via the booking link that will be provided after the Deployment Introduction call.

2) Deployment Phase

What to Expect

Deployment phase is split into three stages:

1. InsightIDR configured with Collectors, Agents, Sensors deployed, and set up validated
2. Event source validation
3. InsightIDR enablement

During your deployment, Rapid7 will provide three sessions of remotely dedicated time with our deployment consultant to assist in configuring your event and log sources into the platform service. During this stage, the Rapid7 deployment team will also help your team set up dashboards inside the InsightIDR product.

You can also choose to self-deploy. Step-by-step deployment instructions will be provided in the welcome email. Your Product Consultant can still be utilized to validate InsightIDR setup and InsightIDR enablement after self-deployment.

Following this, the Rapid7 team will provide best practices training and help configure advanced configurations in the InsightIDR dashboards. It is important to ensure you're following the recommended **deployment guide** for successful deployment.

Note: *You may choose to be placed into monitoring during deployment by completing the Service Activation Request Form that will be provided in the welcome email. In order to be moved into monitoring, at least on InsightAgent must be configured.*

2) Deployment Phase

InsightIDR Setup Collectors, Agent, Event Sources

Task	MDR Milestones	Duration	Details
2.1	Set up Collector(s)	1 day	Use the wizard in InsightIDR to set up first Collector
2.2	Deploy Rapid7 Insight Agent to all servers and workstations	2 weeks	Deploy Agents using Token Installation to all endpoints in your environment
2.3	Deploy Rapid7 Insight Network Sensors in the environment	2 weeks	Deploy Network Sensor into the environment using advice from the Rapid7 Customer Advisor and Deployment experts
2.4	Configure all available event sources	2 weeks	To get the most out of your service, Rapid7 MDR recommends configuring and connecting all available Event Sources to InsightIDR. These include: DHCP, LDAP, DNS, Active Directory, and others. A complete list is available here.

2) Deployment Phase

Validate InsightIDR Setup

Task	MDR Milestones	Duration	Details
3.1	Verify Collectors & Agents	2 days	Rapid7 will assist you in verifying all Collectors and Agents are deployed properly. We recommend Agent deployment to at least 80% of in-scope environments to receive the full benefits of your MDR service.
3.2	Configure/Validate Event Sources	2 days	Rapid7 will assist you in configuring and validating all event sources connected to InsightIDR.
3.3	Custom Event Source Syslogs	2 days	Rapid7 will assist you in adding any custom event source syslogs to InsightIDR.
3.4	Set up custom alerts	2 days	Your CA will assist you in setting up custom alerts for your team to monitor using InsightIDR. Custom alerts are not monitored by MDR.
3.5	Set up Dashboards	1 day	Your CA will assist you in setting up custom dashboards for measuring what's most important to you from the pre-built cards available in InsightIDR.
3.6	Log Search Overview	1 day	Your CA will enable you and your team on how to leverage log search for your use and when conducting your own investigations.

3) Baselining Phase

What to Expect

At least one Insight Agent must be configured in order to begin Baselining.

Your Rapid7 Customer Advisor will place you into monitoring, which commences the Baselining phase. Baselining is an iterative process that helps identify what is normal activity and can run in parallel with deployment. As more agents are added, the more additional norms are identified.

After Baselining has built a map of normal activity, InsightIDR will be configured to understand typical user, asset, and account behaviors. At the completion of Baselining, InsightIDR will understand the interactions between IP addresses, machines, and the user accounts on those machines. This baseline also starts to identify regular users from service accounts and admin accounts.

Additionally, at the end of the Baselining phase, Rapid7 MDR delivers a Compromise Assessment report that identifies and validates potential or present threats to your system environments, and will be continuously monitored using the platform service and other tools.

3) Baselining Phase

Task	MDR Milestones	Duration	Details
4.1	Kickoff Call	1 hour	Once the Service Activation Request has been completed, the CA invites the Customer to a kick-off call to introduce the next phase of the service. The CA will explain the reports that the Customer will receive on an ongoing basis and set-up communications protocols and processes as defined by the customer.If the Service Activation Request was submitted during pre-deployment or deployment, the kickoff call can be scheduled earlier and baselining started in conjunction with deployment
4.2	Set up for SOC monitoring	1 day	As agent deployment is occuring, our Security Operations Center ("SOC") team will activate your environment for SOC monitoring using our tools.
4.3	SOC pod assigned	1 day	Your environment will be assigned a SOC Pod and be transitioned into monitoring.
4.4	Baselining Period	2 weeks	SOC begins baselining period
4.5	Findings Report created (if applicable)	1 hour	During baselining, if malicious threats are found (such as an active malware event or if SOC notices the presence of an adversary) a Findings Report will be created for each threat as soon as they are discovered.
4.6	Compromise Assessment Hunt Period	2 weeks	Our team will start to retrieve agent data, analyze potential compromises, and assemble your Compromise Assessment once more than 80% of agents are deployed in your environment.
4.7	Deliver Compromise Assessment	1 day	This report contains any detected active or historic compromises, potential avenues for future breaches, and prioritized remediation and mitigation recommendations.

Ongoing Service Delivery

What to Expect

Once Baselining is complete, your environment will be monitored by the Rapid7 MDR SOC, commencing the ongoing Monitoring phase. At this point, Rapid7 will deliver **Findings Reports** within one hour of a validated threat being confirmed.

Task	MDR Milestones	Duration	Details
5.1	Receive Service Reports	Monthly (Elite), Quarterly (Essentials)	Rapid7 will provide you with metrics and context surrounding analysis activities, technology health, and findings summaries for an at-a-glance overview of MDR activities.
5.2	Receive Hunt Reports (Elite Only)	Monthly	Our analysts leverage the Rapid7 Insight Agent to collect metadata from multiple locations on your endpoints to identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies.
5.3	Receive Threat Intel reports	Ad-hoc	Highly targeted analysis that leverages the power of Rapid7's threat intel infrastructure (Project Heisenberg, Project Sonar, third-party threat intel) to develop rules to scan your environment and perform real-time asset hardening.
5.4	Receive Finding Reports	Ad-hoc	Findings reports provide written analysis, criticality, raw details, remediation recommendations, suggested containment actions, and mitigation recommendations for each validated incident.

Appendix

MDR Package Comparison

	Elite	Essentials
MDR SOC Team		
Continuous (24/7/365) alert monitoring by SOC analysts	✓	✓
Full incident validation to eliminate false positives	✓	✓
Security advisor as named point-of-contact	✓	✓
Quarterly Business Reviews	✓	✓
Unlimited access to security advisors and/or SOC resources	✓	
Scheduled consultations with security advisor	✓	
Detections		
Threat Intelligence & signature detections	✓	✓
Attacker Behavior Analytics	✓	✓
User Behavior Analytics	✓	✓
Network Traffic Analysis	✓	✓
Enhanced Endpoint Telemetry (process data)	✓	✓
Deception technologies (honeypots, honeyfiles, honey credentials)	✓	✓
Monthly proactive human threat hunts	✓	
Enhanced Network Traffic (east-west flow)	**Add-On**	

MDR Package Comparison

	Elite	Essentials
Response		
Recommendations to contain, remediate, and mitigate future threats	✓	✓
SOAR-powered response workflows	✓	✓
Rapid7 MDR SOC team responds to contain user incidents on your behalf	✓	
Rapid7 MDR SOC team responds to contain endpoint incidents on your behalf	✓	
Remote Incident Response assistance if there's a confirmed breach	**2 per year**	**1 per year**
Reporting		
Alert, compliance, and custom dashboards	✓	✓
Findings Reports with tailored guidance and recommendations	✓	✓
Compromise Assessment prior to monitoring	✓	✓
Emerging Threat Reports from threat intelligence	✓	✓
Incident Escalation reports	✓	✓
Monthly Threat Hunt reports	✓	
State-of-the-Service reporting	**Monthly (12)**	**Quarterly (4)**

MDR Package Comparison

	Elite	Essentials
Technology		
Full license to InsightIDR Cloud SIEM	✓	✓
Technology setup and deployment assistance	✓	✓
Endpoint, network, cloud, and infrastructure monitoring	✓	✓
Real-time event alerting	✓	✓
Centralized log management and search	✓	✓
Asset-based pricing for predictable payments	✓	✓
Unlimited data ingestion	✓	✓
Unlimited event source connections	✓	✓

MDR Technology Overview

The Rapid7 MDR service leverages our Insight Cloud and Rapid7 solutions to provide comprehensive protection against intruders in your internal network, across devices, users, and cloud services. Additionally, the MDR SOC integrates event sources from your existing security infrastructure, granting the Rapid7 MDR team greater visibility into threats across your environment.

Customer-Deployed Software and Configuration

Insight Agent

The universal Insight Agent is lightweight software you can install on any asset—whether in the cloud or on-premises—to automatically collect data from endpoints (even those from remote locations) to enable the Rapid7 MDR team to have real-time visibility to identify malicious activity on your endpoints.

The endpoint agent enables our analysts and behavioral analytics tools to get as close as possible to the attacker, with the complete set of evidence needed to assess a threat. Each agent can be leveraged to perform on-demand containment actions to quarantine an endpoint asset or kill a process.

Insight Network Sensor

The Insight Network Sensor allows InsightIDR to monitor, capture, and assess the end-to-end network traffic moving throughout your physical and virtual environment for both north-south and east-west traffic.

Insight Collector

The Insight Collector is responsible for receiving log data and agent data from your environment. All collected data is compressed and encrypted before being forwarded to the Insight cloud. The Collector also acts as a proxy for endpoint agents to reduce bandwidth constraints and increase endpoint

The Rapid7 MDR service leverages our Insight Cloud and Rapid7 solutions to provide comprehensive protection against intruders in your internal network, across devices, users, and cloud services. Additionally, the MDR SOC integrates event sources from your existing security infrastructure, granting the Rapid7 MDR team greater visibility into threats across your environment.

InsightIDR

Rapid7 MDR provides full access to jointly manage your InsightIDR instance, including access to functionality such as investigations, log search, dashboard cards, and reporting. Your team can also establish custom alerts in InsightIDR. Please note, however, that Rapid7 will be unable to act on these custom alerts beyond the monitoring that MDR typically covers. Your team should not modify or close out alerts within InsightIDR without first contacting your CA to ensure the Rapid7 MDR team maintains complete visibility.

InsightIDR also ingests data from multiple event sources, each configured in InsightIDR to create a unique log in Log Search. The standard MDR subscription includes 13 months of hot, immediately searchable log data and storage. Longer-term retention is fully available to meet your business and compliance needs. Since the Insight architecture runs in the cloud, no external hardware is required for storage.

Event Sources

Rapid7 MDR ingests additional event sources to grant the SOC analysts additional context and information to complete their analysis. The most critical event sources for the optimal service are Active Directory (for Windows assets), DHCP, DNS, and LDAP directory services (or equivalent as agreed upon with Rapid7). That said, it is not a requirement to move forward with the service without these. We suggest for best results to connect as many data sources to InsightIDR as possible.

Deception Technology (optional)

InsightIDR comes included with honeypots, honey users, honey credentials, and honey files designed to identify malicious behaviors using fake assets, users, credentials in memory, or files.

INTRODUCTION
YOUR ADVANTAGE
SERVICE LAYERS
VALUE ADDS
HOW IT WORKS
DEPLOYMENT
APPENDIX

MDR Technology Overview

Rapid7 Cloud Technology Architecture and Capabilities

Insight Cloud

Responsible for all log management, data processing, enrichment, and storage of customer data aggregated from each endpoint with the Insight Agent. Each customer instance on the Insight cloud is isolated from other instances.

InsightIDR

Rapid7's purpose-built cloud SIEM for incident detection and response combines real-time threat intelligence insights with a deep understanding of your environment and sophisticated behavior analytics to identify threats. InsightIDR aggregates endpoint behavior, user behavior, and log history in a single solution offering a comprehensive view of the core technical environment.

Rapid7 Threat Intelligence infrastructure

Primary Rapid7-developed intelligence paired with additional third-party sources to enrich the attack detection and response processes in near-real time. This intelligence is fed back into the InsightIDR solution to update the behavioral analytics and detections within the product. A full review of Rapid7's Research and Threat Intelligence infrastructure can be found **here**.

RAPID7

Learn more at rapid7.com/mdr