Scope of Service

Rapid7 Managed Detection and Response (MDR Elite)

The mission of Rapid7's MDR service is to rapidly detect, investigate, contain and eradicate threats in your environment, and is delivered as a collaboration between Rapid7 and your team ("you", "customer", "your organization", "your environment").

Rapid7 prides itself on becoming a true extension of your security team by providing hands-on 24x7x365 monitoring, threat hunting, incident response, and customized security guidance to stop malicious activity and strengthen your security posture.

Security Expertise

Your Rapid7 MDR team is composed of a named Cybersecurity Advisor, the MDR SOC Tactical Operations team, and the Rapid7 Incident Response team.

Cybersecurity Advisor

Your Cybersecurity Advisor ("CA") is the main point-of-contact for your Rapid7 MDR service. This named resource works with your team as a strategic security partner—from initial technology deployment through incident remediation and ongoing security consultation—to shepherd your organization's security maturity. Your CA will be assigned to your organization once the service enablement sessions are completed.

Throughout your MDR service term, your CA will frequently communicate with your team to provide updates on service delivery, reporting, metrics, technology health, and to ensure Rapid7 is helping you address your security goals. Additionally, your CA will communicate with your MDR SOC team to understand information relevant to any investigations and incidents.

MDR Tactical Operations Team

Our 24x7x365 Tactical Operations team is responsible for the most time-critical tasks for all customers, such as alert triage and investigation; in addition to investigating and triaging security alerts, and the initial response to urgent customer communications. In order for Rapid7 to provide 24x7x365 service, Rapid7 will provision its MDR Analyst team to your InsightIDR instance. Rapid7 MDR Analysts will only have access to the functionality of InsightIDR/Log Search and no other parts of your Insight Platform.

Incident Response Team

Rapid7's Incident Response Team is a dedicated team of experienced incident response professionals who provide ongoing incident response training and support to MDR analysts, and lead any responses to complex and/or high impact incidents in your environment as needed. See Incident Response for additional details.

Cybersecurity Advisor Engagement

During the term of your MDR service, you will regularly engage with your CA. Your CA will be available to answer any questions about your MDR service, and advise you toward advancing your security maturity.

Your CA team will be available by phone and via the Customer Portal for inquiries during normal business hours. During non-business hours, a member of the CA team will be on-call via the CA Hotline for urgent issues. Outlined below are frequent interaction touchpoints that your team will have with your CA:

Communication	Frequency	Method	Description
Customer Questions	Unlimited, Ad-Hoc	Online Customer Portal	• You can leverage the Platform's Customer Portal to request help or raise concerns/questions
Monthly Meeting	Scheduled Monthly	Virtual Meeting	• Review monthly service reports • Address questions about alerts • Answer questions related to the program • Present recommendations for how to further advance your security maturity
Periodic Business Review (PBR)	As Requested	Virtual Meeting or in-person	During the PBR your CA will review trends and metrics from the prior quarter. To include such topics as Remote Access solutions, Alert trends, and Investigation summaries. This helps your team identify any potential security gaps or room for improvement to reduce the volume of alerts generated in your organization.

Cybersecurity Advisor Response Times

Below are response times to inquiries from your team:

Response Trigger	Time to Action	Action
Inbound Urgent Request	2 hours	Reactively acknowledge an urgent request from your team made via the Customer Portal or MDR Hotline. Urgency is based on the discretion of the Cybersecurity Advisor team. If an incident reported by you is confirmed by Rapid7, the incident response process will be initiated (see 'Incident Response').
Inbound Non-urgent Request	24 hours	Reactively respond to a non-urgent request from your team made via the Customer Portal. Urgency is based on the discretion of the Cybersecurity Advisor team.

Service Reports

MDR service reports are delivered via the secure file transfer system located in the Rapid7 Services Portal. These include:

Deliverable	Description
Security Posture Assessment Report	This report describes potential avenues for future breaches and active or historic compromises detected by Rapid7 in your environment during the initial onboarding phase. The report will also include prioritized remediation and mitigation recommendations to reduce the likelihood of a potential breach. If a breach is detected, our team will immediately pivot into Incident Response (see Incident Response for additional details).
Incident Response Reports	Details incident management activities, key findings, the timeline of attacker activity, and recommended corrective actions to prevent the likelihood of recurrence and/or improve your ability to detect and respond to similar incidents in the future. Detailed analysis will be provided upon request.

Monthly Service Reports	Provides metrics and context about threat detection and incident response activities conducted in the previous month, along with information about the health of detection and response controls in your environment.

InsightIDR Instance Set-Up

Your MDR service includes a single instance of InsightIDR for your entire organization. All log sources will be onboarded to this single instance. All of your users will be assigned to and will have access to all data stored within this single instance.

In some cases, you may want to deploy the MDR service to multiple internal organizations as separate InsightIDR instances to provide separate visibility and reporting across these logically separated organizations or business units. Details on the MDR service delivery options for additional organizations can be provided in an addendum to this Scope of Service.

In-Scope Environment for MDR

The 'in-scope environment' refers to the assets (and supporting infrastructure) you have licensed for MDR. All assets within this environment must have unique IP addresses. Your MDR service requires licensing and deploying the Insight Agent across your organization's entire environment to enable effective threat detection and incident response activities. You may choose to license only a portion of your environment for MDR as long as the in-scope environment is 'logically separated' from the rest of your environment. Examples of logically separated environments include an internet-facing production data center that is separate from your corporate IT end-user environment, or multiple subsidiaries with logically separate IT infrastructures.

Rapid7 considers an environment logically separated if it meets all of the following criteria:

- The in-scope environment must be on a network that is logically separated and isolated from the rest of the organization. Specifically, the in-scope environment must have its own networking infrastructure (firewalls, Web proxies, and DNS servers). The environment must have separate Internet egress points, and inbound network traffic from out-of-scope environments is not permitted.
- The in-scope environment(s) must have its own authentication and access control infrastructure (such as active directory and other identity providers). Specifically, all users supported by this infrastructure must be active users of the systems in the in-scope environment.
- Any cloud services that will be in-scope for MDR must be accessed only by active users of the systems in the in-scope environment.

Insight Agent Updates

Rapid7's MDR service is designed for the latest version of our Insight Agent. Rapid7's Insight Agent is configured by default to automatically receive updates as our teams release new features, improve agent performance and fix known bugs. Rapid7 reserves the right to push Insight Agent updates without notice when Rapid7 determines serviced agents need to be upgraded to ensure efficacy of the delivered service. You do have the option to disable this automatic update feature; however disabling automatic updates may prevent Rapid7's ability to improve agent performance, detect penetration testing, detect attacker activity, investigate and respond to malicious activity in your environment, and/or enable new features for your MDR Service.

Event Sources

Rapid7 supports a wide range of security-relevant event sources, which can be configured in the 'Event Sources' page of InsightIDR.

Event source log data is stored in InsightIDR and available for search for thirteen months from the time of collection. We recommend that you onboard all supported event sources that are present within your in-scope environment. At a minimum, we strongly recommend you onboard the following event sources:

- For organizations that have Microsoft Windows domains, send the Windows Security event logs from each Microsoft Active Directory Domain Controller to InsightIDR – without this event source, many InsightIDR Legacy Detection Rules will not be supported.
- For organizations that have Microsoft Windows domains, Microsoft Azure AD Domain Services, or Amazon AWS Domain Services, connect at least one LDAP event source for each domain– without this event source, Rapid7 MDR will not have vital contextual information about users in your environment.
- Connect all supported DHCP log sources to InsightIDR–without this event source, Rapid7 may not be able to accurately attribute network traffic to the appropriate assets in your environment.
- Connect all supported network logs - DNS, firewall, VPN, and Web Proxy - to InsightIDR, particularly network devices at your internet ingress and egress points. Without these event sources, some InsightIDR Legacy Detection Rules and all NBI (Network Based Indicator) ABA detection rules will not be supported. In addition, this data is leveraged by Rapid7 to further investigate suspicious or malicious activity in your environment.
- Connect all supported Cloud Services logs to InsightIDR. Without these event sources, some InsightIDR Legacy Detection Rules will not be supported. In addition, this data is leveraged by Rapid7 to further investigate suspicious or malicious activity in your environment.

Rapid7 MDR leverages InsightIDR event sources as described below:

Source	Real-time Detection[1]				Threat Hunting	Investigation	
	Legacy Detection Rules	Detection Rules	NTA	Intel		Asset/User Attribution	Log Search
Insight Agents	✓	✓		✓	✓	✓	✓
Active Directory	✓	✓		✓	✓		✓
VPN	✓	✓		✓	✓		✓
Cloud Services	✓	✓		✓	✓		✓
Deception Technology	✓				✓		✓
DNS				✓	✓		✓
Firewall		✓		✓	✓		✓
Web Proxy		✓		✓	✓		✓
Insight Network Sensor			✓	✓	✓		✓
DHCP						✓	✓
LDAP						✓	
Third Party Alerts	✓	✓			✓		✓
All Other Log Types					✓		✓

Real-time Detection

These event sources are processed by our threat detection engine and may generate alerts that are reviewed by our 24x7x365 SOC (see the 'Detection Rules' page of InsightIDR for a list of all current detection rules, and see the 'Detection Rules' section below for more details about which detection rules are in-scope for the MDR service).

Threat Hunting

Data from these event sources are aggregated and leveraged by analysts when performing threat hunts (see 'Threat Hunting' for additional details).

Investigation

Data from these event sources may be leveraged to accurately attribute other activity to an asset or user, and to provide other useful context data in the course of investigating alerts or performing incident response.

[1] Alerts generated by these event sources are reviewed by either your organization or the MDR SOC, per the guidelines described in the 'Detection Rules' section below.

Third Party Security Tools

A third-party event source is an external data stream that connects to InsightIDR with an associated detection library owned and operated by an established third-party security vendor. To be accepted as a third-party event source for triage, investigation, and response by the Rapid7 SOC, the source must have an existing alert stream, inherited criticality, a presence in the majority of our MDR customers' environments, and a substantial market presence. Accepted third-party products are included in the list provided on our managed MDR docs page.

The number of third-party products monitored by Rapid7 is determined by the service purchased.

- MTC Advanced, MTC Ultimate, and MDR Elite customers are entitled to monitoring for two (2) third-party products, with the option to purchase additional monitoring if needed.
- MTC Essential and MDR Essentials customers must purchase third-party product monitoring as an add-on.

Third-party coverage is managed through entitlements. To initiate monitoring, your selected product(s) must first be activated by your CA. Once initiated, your CA can update your elected third-party monitored products as needed. Please reach out to the CA once you have decided which third-party products you would like the Rapid7 MDR SOC to monitor and/or if you have any changes to these selections.

Third Party Alert Triage

The Rapid7 SOC will triage, investigate, and respond to alerts from select third-party security tools. Rapid7 will only perform these actions within InsightIDR. Rapid7 will not close alerts in third-party systems via manual process or API access and/or integrations.

Alerts from third-party security tools are integrated into InsightIDR by configuring the appropriate event sources. As with all event sources in InsightIDR, Rapid7 assists with event source configuration but does not have control over potential disruptions in data flow from third-party tools to InsightIDR. While such disruptions are not common, they can result in gaps in detection or services. Because these outages are often due to factors outside of Rapid7's control, Rapid7 cannot be held responsible for disruptions in the flow of data from third parties.

The Rapid7 SOC will triage, investigate, and respond to standard third-party alerts classified by their top severity/priority at the time of ingestion to InsightIDR. These alerts will inherit the priority level given by the third-party provider and will be subject to the same service level objectives and tuning activities as all other high-priority alerts as set forth herein. Rapid7's "Critical" priority is reserved for Rapid7 authored detections, and select third-party detections that meet strict efficacy requirements administered by Rapid7's Service Delivery Team. Rapid7's Threat Intelligence and Detection Engineering will regularly review the efficacy of third-party detections to tune and adjust priority as needed.

For clarification, Rapid7's service level objectives for alerts from third-party sources are based on the creation time within InsightIDR, not the original event time recorded in the third-party system. To minimize the risk of third-party system failures, Rapid7 advises customers to integrate their security tools directly with InsightIDR, ensuring the most straightforward connection possible to reduce the potential for third-party integration data interruptions.

Custom alerts generated by a third-party product—or alerts passed through a third-party product that is of a different origin— are out of scope and will not be triaged by the Rapid7 MDR SOC, regardless of their assigned priority. Alerts whose severity has been manually elevated to High or Critical by the customer are out of scope, and will not be triaged. Rapid7 understands that customers may configure and set up third-party sources through integrations of additional SIEMs. In this case, Rapid7 will review the information in the alert evidence that directly matches the source system with the event source ingested. Alerts passed to Rapid7 through a third-party SIEM of a different origin or source are not supported, and any mismatch of source data and a third-party supported tool will disqualify alerts from Rapid7 triage and support.

Detection Strategy

Rapid7's Detection Strategy dictates how we develop detections for first and third-party event sources. We focus on finding attacker behavior from Initial Access through Impact (prioritizing earlier stages) on servers, endpoints, networks, and cloud systems. Alerts created by our detections must provide sufficient context for an analyst to triage and investigate effectively. Coverage of individual third-party event sources may vary depending on alert context, licensing considerations, and the MDR SOC's scope (e.g., vulnerability, containerized workloads, contextual/posture management-related detections are out of scope. If an alert would immediately require customer input to triage, the detection will be classified as Custom and Contextual. This includes but is not limited to OT/IOT, DLP, Insider Threat, and 3rd party alerts that would require access to the third-party console to view all necessary context.

Detection Rules

InsightIDR detection rules generate alerts based on activity from your configured event sources, the Insight Agent, and the Rapid7 Network Traffic Analysis (NTA) network sensor. Rapid7 regularly re-evaluates our detections for efficacy, accuracy, and efficiency for both you and our MDR SOC. At any time, Rapid7 may update any attribute of a non-customer authored detection including, but not limited to category, priority, or logic. Additionally, Rapid7 may retire a detection entirely if, based on customer-wide data review, it is determined that the detection is found to have low efficacy.

These detection rules are available in the 'Detection Rules' page of InsightIDR. These detection rules are grouped into the following detection libraries:

Detection Library	Description	Initial Triage
Legacy User Behavior Analytics (UBA), Basic Detection Rules, Community Threats	Detection libraries that include: • UBA activity: InsightIDR creates a baseline of normal user activity within your environment and generates investigations when there is a deviation • Basic Detection Rules: Detection rules written by your organization using information from Log Search. • Community Threats: Detection rules powered by community-managed threat intelligence feeds	Your organization is responsible for configuring and tuning these detection rules, and for the initial triage of any resulting investigations. **Should you identify suspicious activity from resulting alerts or investigations, please contact Rapid7 for further investigation and (if needed) incident response. Incidents discovered as a result of these investigations are eligible for MDR incident response as described in the Incident Response section.**
Detection Rule Library (formally - Attacker Behavior Analytics (ABA))	A Detection library that includes: • Detections created from behavioral analytics and curated threat intelligence, built from our experience and understanding of attacker tools, tactics, procedures, and methodologies • User Behavior Alerts migrated over from the legacy library • Third Party Alerts: Alerts generated by third-party security vendors • Custom Detection Rules: Detection Rules written by your organization using the same mechanisms as	Each rule in the Detection Rule Library rule has a 'category' attribute which determines whether the detection rule (and resulting alerts) are managed by the MDR SOC. Rapid7 is responsible for configuring, tuning, and handling any detection rules marked as 'Rapid7 Managed'. See 24x7x365 Security Monitoring for details on how Rapid7 handles these alerts. Your organization is responsible for configuring, tuning, and handling any detection rules marked as 'Custom and

	our internal threat teams	Contextual.'

InsightIDR Deployment and Configuration

Deployment Process

We encourage your team to begin the deployment process as soon as possible by self-deploying InsightIDR in your environment. After purchasing Rapid7 MDR, you will be sent a welcome email that contains links to the self deployment guide as well as an invitation to schedule time with a Rapid7 Product Consultant ("Deployment Sessions").

Deployment Sessions

During the Deployment Session(s), your Rapid7 product consultant will assist your team with any InsightIDR deployment-related tasks, including the configuration of collectors, event sources, and product settings. Rapid7 will provide documentation to assist with Insight Agent deployment. Custom integrations, additional deployment time, training, and other services are not included in the Deployment Sessions and must be purchased separately. For those who have opted to self deploy, this session will be used to validate the deployment and verify that Rapid7 is receiving the logs that are being sent.

Activating Your MDR Service

Rapid7 can begin monitoring your environment (See '24x7x365 Security Monitoring' below) as soon as your deployment begins. The MDR Team will conduct a service enablement session to verify agent deployment, and will then begin monitoring your environment.

InsightIDR Access

A list of users who have access to InsightIDR can be seen inside the product. In the event that all of your organization's existing Insight Platform Admins are no longer with the organization, someone from your organization must provide Rapid7 a written request for access.

Threat Detection

Rapid7 leverages security posture assessments, 24x7x365 security monitoring, and threat hunting to identify malicious activity within your organization.

Security Posture Assessment

Once your team has deployed the Insight Agent to 80% or more of the existing assets in your in-scope environment, a security posture assessment will be performed to identify any historical or active compromises.

If the security posture assessment finds that there is an active compromise, the incident response process will be initiated (see Incident Response) and you will be notified by email and phone (depending on incident severity).

24x7x365 Security Monitoring

InsightIDR alerts are created when a detection rule is triggered based on activity in your environment. The 'category' attribute of an alert is determined based on the 'category' attribute of the detection rule that generated the alert (see Detection Rules for details).

Rapid7 will fully investigate all InsightIDR alerts categorized as 'Rapid7 Managed,' by gathering context from your endpoints and log data in order to determine whether the activity is benign or malicious.

.

When the investigation is completed:

- If the activity is determined to be malicious, Rapid7 will initiate incident response (see 'Incident Response') and you will be notified by email and phone (depending on incident severity).
- If the activity is determined to be benign, Rapid7 will close the investigation and will not notify you.

Rapid7 prioritizes these alerts based on a combination of the likelihood of malicious activity and the potential impact of the detected activity, and our objective is to begin our investigation promptly in accordance with the following:

Alert Priority	Time to Begin Alert Investigation
Critical	15 minutes
High	1 hour
Medium	12 hours
Low	48 hours
Informational	Not applicable; used only as supporting context

Critical

An event in your environment which contains behavior that highly correlates to tactics, techniques, and procedures utilized by threat actors. Critical alerts require immediate response and are the highest priority for MDR analyst review.

High

An event in your environment which contains behavior that often correlates to tactics, techniques, and procedures utilized by threat actors and are prioritized for MDR analyst review.

Medium

An event in your environment which contains behavior that can correlate to tactics, techniques, and procedures that may be utilized by threat actors, but overlaps with normal administrator or user activity and requires MDR analyst review.

Low

An event in your environment which contains behavior that infrequently correlates to tactics, techniques, and procedures utilized by threat actors, often overlaps with normal administrator or activity, and still requires MDR analyst review.

Informational

An event in your environment which, while notable, does not independently warrant investigation. Informational alerts are designed to enrich managed investigations by providing additional context for SOC analysts. These alerts do not require direct action or review by your team but contribute additional context to a more comprehensive threat analysis when correlated with higher-priority activity.

Requests for Information (RFI)

In some cases, Rapid7 may need additional input from you in order to complete an investigation, in which case Rapid7 will reach out to you via a Customer Portal case.

Threat Hunting

Rapid7 performs regular hunts for new or novel threats within your environment by leveraging access to historical log data, alert data, and forensic endpoint artifacts. Details about these hunts can be found in the Monthly Service Report.

If a threat hunt identifies an active compromise in your environment, Rapid7 will initiate incident response (see 'Incident Response' below).

Incident Response

If an eligible incident is discovered by you or Rapid7 within your in-scope environment at any time during your MDR term, Rapid7 will initiate incident response. Incidents eligible for incident response are compromises of customer's in-scope systems or data, as confirmed or reasonably suspected by Rapid7. Rapid7 will not respond to an incident that occurs in an environment that is not in-scope. All incident response services will be provided remotely.

Incident Severities

It is important to note that the same initial activity can result in incidents of different severities. Rapid7 determines the final severity of an incident based on a holistic analysis of a number of factors, including:

- **Intent:** Whether the threat appears to be targeted, opportunistic, or automated, and the likely objectives of the attack.
- **Scope:** The number of systems and users impacted.
- **Ongoing Activity:** Whether the incident appears to have been fully contained, and whether the attacker remains active within the environment.
- **Impact:** The business criticality of in-scope assets or users, evidence of data exfiltration, operational disruption, etc.

Incident Severity	Incident Definition	Example Incident(s)
Low	A non-targeted, low-impact threat that resulted in contained **execution** on a small number of systems or users.	A non-targeted commodity malware attack which security controls are contained, but there is still evidence of execution.
Medium	A non-targeted, low-impact threat impacting a small number of systems or users, but requiring additional actions from you to fully contain and eradicate the threat.	Malware delivered via a non-targeted phishing attack that is not blocked on an endpoint.
High*	A high risk or high impact threat, often involving a large number of systems or users and ongoing attacker activity.	Unauthorized interactive network access with evidence of reconnaissance, privilege escalation, lateral movement, data exfiltration, or other signs of a late-stage compromise.

Security events automatically prevented by security solutions without resulting in the successful compromise of a system or account are classified as routine security operations and not as incidents. Examples include, but are not limited to, blocked malware, quarantined phishing emails, and denied login attempts based on security policy.

*For all high-severity incidents, the Rapid7 MDR service includes leading the investigation as the primary response partner.

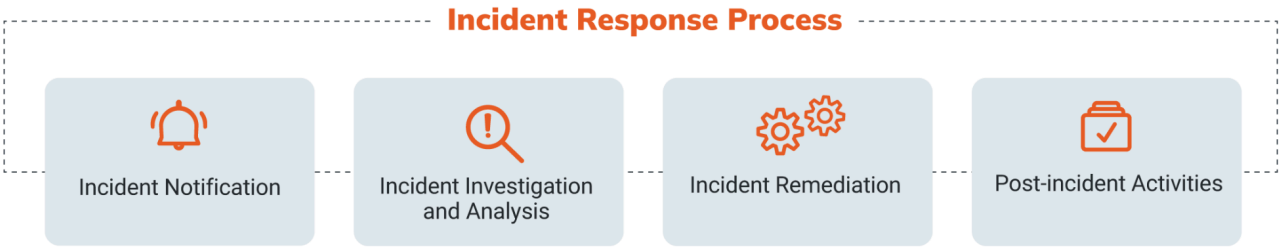
Should you choose to engage a separate third-party for incident response, our team will facilitate a structured handover to ensure a smooth transition. This process includes:

- A handover meeting with the third party and your team.
- Delivery of all investigation findings, status updates, and relevant forensic artifacts acquired by Rapid7.
- Allowing you to provide platform access for the third-party response team.

Upon completion of this handover, Rapid7's direct involvement in the incident investigation will conclude, and the MDR service will return to its standard monitoring function.

Incident Response Process

Once an incident is identified by Rapid7 (or reported by you and confirmed by Rapid7) we will initiate the incident response process.



Incident Response Phase	Activity	Definition	Incident Severity
Incident Notification	**Incident Notification - Email**	Initial notification immediately via a Customer Portal case and e-mail notification to your designated contacts.	All
	Incident Notification - Phone Call	Rapid7 will call your designated contacts within 30 minutes of incident identification. Contacts will be called in the order defined by you, until Rapid7 is able to reach someone.	Medium and High
	Incident Kickoff Call	The Incident Manager will schedule a 'kick off call' to share initial incident details, gather information, and discuss planned incident response activities. This call will be scheduled to occur within 1 hour of the initial notification call (customer availability permitting).	High
Incident Investigation and Analysis	**Forensic Analysis**	Investigation of incident scope, impact, and root cause using data sent to InsightIDR, data generated by the Insight Agent, and other forensic analysis techniques will begin immediately.	All
	Incident Updates	For incidents that are in progress for more	High

		than 24 hours, Rapid7 will provide a daily written incident update (and host a video or phone conference as needed) to communicate the progress of the ongoing response efforts. Significant or urgent findings will also be communicated as they are identified.	
Incident Remediation	**Containment and Eradication**	During incident response, Rapid7 will communicate recommended remediation actions to contain and eradicate the threat in your environment. Rapid7's approach includes: ● Fully scoping the incident before recommending remediation activities ● Recommendations for removing all attacker remote access capabilities, restoring prioritized business processes, and securing compromised user accounts You will also have the option to enable Rapid7's Active Response service. Active Response gives your security program immediate response capabilities—initiated by MDR—to stop attacks and contain confirmed threats in your environment. More information is described in the Active Response section.	All
Post-Incident Activities	**Incident Response Report**	An Incident report as described in 'Service Reports'. This report will be delivered to you within 10 business days of the conclusion of the incident investigation.	All
	Incident Debrief	After the incident report is delivered, Rapid7 will schedule a formal debrief. This debrief, usually designed for executives and management teams, summarizes the investigation and provides meaningful metrics, significant findings, and recommendations for program improvement.	High
	Corrective Action Tracking	Your Cybersecurity Advisor will partner with you to ensure that all corrective actions identified in the Incident Response Report are implemented in your environment in order to reduce the likelihood of incident recurrence and to improve your ability to detect and respond to similar incidents in the future.	All

Incident Response Roles

Cybersecurity Advisor: Your Cybersecurity Advisor (or another member of Rapid7's Cybersecurity Advisor team) will notify you about a security incident, will be included on any ongoing incident communications, and will partner with you to discuss the implementation of recommended corrective actions at the conclusion of an incident response engagement.

Incident Manager: Each incident will be assigned an Incident Manager responsible for:

- Serving as the primary point of contact and managing all incident communications between you and Rapid7
- Coordinating the investigation and analysis
- Documenting all findings relating to the investigation
- Performing the incident debrief with your team (high severity incidents only)

Incident Handler: For larger, more complex incidents, the Incident Manager may be supported by one or more Incident Handlers who perform incident investigation tasks as directed by the Incident Manager.

Customer Responsibilities

- **Timely engagement with Rapid7 during incident response:** Rapid7 partners with you to take action to investigate threats and limit the potential scope and impact of incidents. If a customer is unavailable to partner with Rapid7 during the IR process, the IR engagement may be paused or discontinued.
- **Investigation support:** Provide Rapid7 with the support necessary to investigate the incident. This includes deployment of the Rapid7 agent to all in-scope systems (if not already deployed), and providing access to relevant log data not already collected by InsightIDR. If our agent is not present and cannot be deployed to these systems and/or requested log data cannot be provided, the ability of Rapid7 to effectively investigate and respond to the incident will be limited.
- **Implementation of recommended remediation actions:** During an IR engagement, Rapid7 will provide time-critical remediation recommendations (such as isolating an asset, disabling a user account, or stopping a running service). It is important that you take these actions in a timely manner in order to limit the scope and impact of an incident. An incident response engagement may be paused or discontinued if a reasonable effort is not made to implement these actions.
- **Implementation of recommended corrective actions:** Following an IR engagement, Rapid7 will provide you with recommended corrective actions to reduce the likelihood of incident recurrence or improve your (and Rapid7's) ability to detect and respond to similar incidents in the future. Rapid7 acknowledges that not all recommendations are feasible in all environments, and these recommendations must be balanced with your other organizational priorities. However, in rare cases, if your inability to implement these recommendations results in recurring major (high severity) incidents, Rapid7 may decline to provide full incident response support for these incidents until these corrective actions are taken.

Joint Requirements For Ensuring Success

To ensure your organization realizes the full value of Rapid7 MDR, it is critical that both parties share in the responsibilities and requirements of the partnership for effective delivery of the MDR service:

Rapid7 Responsibilities and Requirements

	Responsibilities and Requirements
1	Monitor your environment as set forth in this Scope of Service, with the visibility provided by the Rapid7 MDR

	technology stack (InsightIDR & Insight Agent) and in conjunction with the event sources configured in InsightIDR from your environment
2	Assist with the deployment of required and optional product features
3	Provide a named security advisor ("Cybersecurity Advisor") as the point-of-contact for the MDR relationship and to help accelerate your organization's security maturity
4	Perform incident response in order to investigate, contain, and eradicate threats discovered in your environment
5	Deliver reports via the Rapid7 Services Portal
6	Notify you of any Cybersecurity Advisor or service delivery changes

Your Responsibilities and Requirements

	Responsibilities and Requirements
1	Acknowledge, accept, and adhere to all requirements and actions outlined in this Scope of Service
2	License all assets within the in-scope environment, which must be 'logically separated' from any other out-of-scope environments
3	Designate a point of contact to work with Rapid7 for deployment and onboarding
3a	Deploy at least one Insight Agent and then work with the onboarding team to begin monitoring
3b	Provide Rapid7 with an incident escalation path including a list of names, email addresses, and phone numbers as well as the order in which they should be notified in the event of an incident (conditional escalation paths based on asset or time of day are not supported)
4	Deploy Insight Agents to all workstation, desktop, and server assets in the in-scope environment(s) and connect all Insight Agents to InsightIDR ● Assets without the Insight Agent deployed will not be fully supported by the MDR service ● You must deploy Insight Agents to at least 80% of existing assets in the in-scope environment in order for Rapid7 to perform a security posture assessment
4a	Ensure you are running a supported version of the Insight Agent on all assets in your in-scope environment. The Rapid7 SOC may be unable to effectively detect and respond to threats on assets running unsupported versions of the agent
5	Allocate and configure at least one Insight Collector(s) in order to: ● Collect the event sources described in 6 and 7 ● Proxy connections from 'on premise' Insight Agents to the Insight Platform
6	Connect all available recommended data sources to InsightIDR (see 'Event Sources' on [page 4]) for each in-scope environment and ensure availability and connectivity to Rapid7 infrastructure for all MDR technology and event sources
6a	Deploy Insight network sensors in your environment to analyze and log network traffic data
6b	Set up honey users, honey files and honeypots
7	Connect any other security-relevant event sources to InsightIDR *Note: All connected event sources may be leveraged for investigation, threat hunting and incident response purposes.*
8	Notify Rapid7 of any personnel, technology, event source, or point of contact changes or modifications
9	Configure the InsightIDR instance in accordance with the recommendations from your deployment team and Cybersecurity Advisors
10	Review investigations that are not in-scope for the MDR service as these investigations will not be reviewed by the MDR service. See the 'Detection Rules' section on [page 5] for details on investigation categorization.

11	Respond to 'Requests for Information' (RFIs) and MDR Notifications from your MDR team regarding specific investigations, which may be sent via e-mail or through the Customer Portal, in order for Rapid7 to accurately assess this activity.
12	Partner with Rapid7 during and after an incident response engagement, as described in the incident response 'Customer Responsibilities' section.

Active Response Service

Rapid7 Managed Detection and Response (MDR) Elite and Managed Threat Complete (MTC) customers have the option for Rapid7's experts to initiate responses in the customer's production environment for validated threats (herein named "Active Response service"). If the Active Response service is enabled, the Rapid7 Managed Services team will have the ability to contain impacted assets and users when responding to an incident in your environment.

The following is an overview of the service requirements, capabilities, and terms and conditions that must be accepted prior to enabling the Active Response service.

Eligibility Requirements

To be eligible for Active Response, you must meet the requirements outlined in this section. If you have any questions about whether or not you are eligible, please contact your Cybersecurity Advisor.

General Requirements

- You must be an MDR Elite or MTC customer.
- You must have or be willing to have an InsightConnect Orchestrator installed and activated if you want to leverage user containment via Active Directory.
- You must have less than 1,000 endpoints or 1,000 users that you want to exclude from quarantine actions.

User Containment Requirements

In each LDAP domain, primary domain controllers must allow communication over port 389 or 636 to the InsightConnect Orchestrator.

Endpoint Containment Requirements

Rapid7 supports the Endpoint Detection & Response (EDR) technologies listed below for isolating endpoints in your environment. You must ensure the selected EDR technology is deployed on all systems in your environment. Note that regardless of which EDR technology is used for Active Response, you must still deploy the Rapid7 InsightAgent to all endpoints (as described in the MDR and MTC Scope of Service).

Rapid7 Insight Agent

- In order to take containment actions using the Insight Agents please see - The Insight Agent Requirments

Other Supported Agents (CrowdStrike Falcon, SentinelOne, Carbon Black Cloud, Microsoft Defender, Cisco Secure Endpoint)

- Optionally, you can configure the EDR to permit network connections from contained assets to the Rapid7 Insight Platform (reference the connectivity requirements for the Rapid7 Insight Agent documented here). This will enable the MDR team to perform post-containment forensic investigation on these assets.

Customer Responsibilities

To enable the Active Response service, you are required to perform the following:

	Responsibilities
1	Ensure that the selected endpoint technology (see list of supported endpoint technologies above) has been deployed to all assets. The Insight Agent is still required if you are using a different endpoint technology for containment.
2	Install the InsightConnect Orchestrator if leveraging user containment with Active Directory.
3	Authenticate all applicable InsightConnect connections using your security credentials between third party apps:
3a	If using **LDAP & Active Directory** for Active Response user containment, connect it to InsightConnect as described here.
3b	If using **Carbon Black Cloud** for Active Response asset containment, connect it to InsightConnect as described on the documentation tab here. Note: multi-domain is not supported for Carbon Black Cloud.
3c	If using **Microsoft Defender** for Active Response asset containment, connect it to InsightConnect as described on the documentation tab here or using the setup guide here.
3d	If using **SentinelOne** for Active Response asset containment, connect it to InsightConnect as described on the documentation tab here.
3e	If using **CrowdStrike Falcon** for Active Response asset containment, connect it to InsightConnect as described on the documentation tab here.
3f	If using **Cisco Secure Endpoint** for Active Response asset containment, connect it to InsightConnect as described on the documentation tab here.
4	If using the Insight Agent for Active Response, enable **Windows Firewall** on all endpoints in accordance with the Insight Agent Requirements
5	Define all environment exceptions and configurations (such as excluding users and endpoints) for all response actions performed from within InsightConnect. The MDR team will not update these Exclude Lists on behalf of you, the customer.
6	All unquarantine actions must be completed by you, the customer, unless you have also opted in to the Active Remediation service.

Active Response Service Responsibilities

Active Response service will be responsible for the following:

	Responsibilities and Requirements
1	Deliver a 24x7 response service.

2	Provide you with a license of InsightConnect for the sole purpose of enabling the Active Response service.
3	Manually perform validation and appropriate recommendations to respond to the threat.
4	Perform response actions as defined and outlined below in "Active Response Actions."
5	Engage you, the customer with requests, and continuously notify the customer, for any proposed action or change in response status.
6	Active Response service will update you to status changes via the InsightIDR Investigation Timeline and Audit Log.
7	All Active Response actions will be taken immediately.
8	If you, the customer, have also opted in to the Active Remediation service, and the remediation process completed successfully, unquarantine the asset on your behalf.
9	Maintain an audit in InsightIDR for the quarantine and unquarantine actions initiated by the Rapid7 Insight Agent.

Active Response Service Capabilities

The following response actions will be taken on your behalf in accordance with Rapid7's best practices and at the discretion of the Rapid7 Managed Services team responsible for the Active Response service:

Users

For threats such as user activity associated with potentially malicious, anomalous, or suspicious activity associated with common attacker behaviors leveraging user credentials, the Active Response service will **quarantine a user** on your behalf.

Endpoints

For threats such as malware (indicators of Ransomware, Trojan backdoors, etc.) or other indications of an attacker's presence (webshell evidence, etc.) on endpoints in the environment, the Active Response service will **quarantine an endpoint** on your behalf.

Time to Action

Immediately after a threat analyst validates malicious or suspected malicious activity associated with an InsightIDR Investigation, the Active Response service will initiate the customer configured quarantine response action.

Additional Terms & Conditions

WARNING - The Active Response service is designed to take action in the customer's production environment and can disrupt users, endpoints, and business operations. By enabling the Active Response service, the customer has read, understands, and agrees to the following:

Communication

When the Rapid7 SOC performs an Active Response action, this is communicated to the customer in the following ways:

- Details of the Active Response action will be posted to the Investigation Timeline in InsightIDR.
- An email incident notification (and incident report) will be sent as described in the 'Incident Response' section..

Workflow Management

- You, the customer agrees to manage and configure MDR-specific automation response snippets within InsightConnect in accordance with the defined parameters during setup.
- The Active Response service will not configure, modify or customize the automation response snippets.
- If a customer has an InsightConnect license and would like to create or install additional automation workflows or snippets leveraging InsightConnect, the Active Response service will not act on workflows or snippets outside the scope of the above service capabilities.

Active Response Actions

- While the Rapid7SOC strives to quickly identify and contain all threats, there is no guarantee that enabling the Active Response service will ensure that the SOC team is able to catch and contain all threats in the customer environment. The Active Response service will take action on all appropriate threats within the set guidelines for their ability to detect and respond.
- The customer grants the Active Response service permission to take the recommended response action in the customer's production environment, within the conditions self-configured and defined by the customer inside of InsightConnect.
- Rapid7 will not be held liable for any actions performed by Active Response service.
- If a containment action is not successful, the MDR SOC team will reach out to the customer to request manual containment of the user or endpoint.

In no event shall Rapid7 or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information) arising out of the use of, or inability to use, software, service, or capabilities related to action taken by the Active Response service, even if Rapid7 has advised customer of the possibility of such damages.

Active Remediation with Velociraptor Service Capabilities

Rapid7 MDR Elite and MTC customers who have opted into the Active Response service can additionally opt-in to Active Remediation with Velociraptor. This feature allows Rapid7's experts to remove qualifying, validated threats from an endpoint after initiating Active Response . If the Active Remediation with Velociraptor service is enabled, and a network connection is configured by the customer to be sustained between the contained assets and the Rapid7 Insight Platform, the Rapid7 Managed Services team will have the ability to remove remnants of compromise from quarantined endpoints when responding to an incident in your environment.

Eligibility Requirements

To be eligible for Active Remediation, you must first enable Active Response as described in the section above.

Customer Responsibilities

If you are using one of the other supported agents (**CrowdStrike Falcon, SentinelOne, Carbon Black Cloud, Microsoft Defender, Cisco Secure Endpoint)** to quarantine an asset via Active Response, you, the customer, must configure your EDR to permit network connections from contained assets to the Rapid7 Insight Platform (reference the connectivity requirements for the Rapid7 Insight Agent documented here). Successful execution of remediation actions is subject to you conducting a correct configuration and granting permissions within your environment.

Active Remediation Service Responsibilities

Active Remediation service will be responsible for the following:

	Responsibilities and Requirements
1	Perform response actions as defined and outlined below in "Active Remediation Actions."
2	Engage you, the customer, with requests, and continuously notify you for any proposed action or change in response status.
3	Take all Active Remediation actions only after successfully quarantining the endpoint.
4	Perform all Active Remediation actions using standardized Velociraptor Artifacts. They will not be performed by issuing commands directly to the Windows shell or via custom VQL queries.
5	Run Active Remediation actions in a "test mode" that will report the potential results of the action, but not commit the changes on the endpoint. After validating the test results, the action will be run again to commit the changes.
6	Maintain an audit logs for the remediation actions initiated by the Rapid7 Insight Agent's Velociraptor process.
7	Provide remediation action results and logs from Hosted Velociraptor.

Active Remediation Service Capabilities

The following response actions will be taken on your behalf in accordance with Rapid7's best practices and at the discretion of the Rapid7 Managed Services team responsible for the Active Remediation service:

Endpoints

For threats that can be removed from an endpoint with minimal risk of continued or escalating compromise, the Active Remediation service will **remove files and other remnants of compromise from an endpoint** using Hosted Velociraptor.

Potential Active Remediation targets are designated by Rapid7 Managed Services from among the most prevalent commodity malware threats observed across the customer base. To ensure the likelihood of successful remediation, conditions for targets include:

- Targets must have a well-understood set of Indicators of Compromise (IoCs).
- Alerts related to the target must be of medium severity and no higher, where the infection is most likely to be commodity malware that was not directed specifically to your environment.
- Malware remnant locations must be within scheduled tasks, registry keys, or files on Windows endpoints.

Time to Action

After a threat analyst identifies valid remediation targets during an Investigation, they will first follow the Active Response actions described in the previous section. After the endpoint is successfully quarantined, they will begin the Active Remediation workflow.

Additional Terms & Conditions

WARNING - The Active Remediation service is designed to take action in the customer's production environment and can disrupt users, endpoints, and business operations. By enabling the Active Remediation service, the customer has read, understands, and agrees to the following:

Communication

When the Rapid7 SOC performs an Active Remediation action, this is communicated to the you in the following way: an email incident notification (and incident report) will be sent as described in the 'Incident Response' section of the MDR and MTC Scope of Service.

Workflow Management

- The Active Remediation service depends upon successful completion of the quarantine step of Active Response workflow.
- After the asset is successfully quarantined, the SOC will begin the Active Remediation workflow.
- If all intended remediation actions succeed, the SOC will unquarantine the asset instead of requiring you, the customer, to do so.

Active Remediation Actions

- While the Rapid7 SOC strives to quickly identify and contain all threats, there is no guarantee that enabling the Active Response service will ensure that the SOC team is able to catch and contain all threats in the customer environment. The Active Remediation service will take action on all appropriate threats within the set guidelines for their ability to detect and respond.
- The customer grants the Active Remediation service permission to take the recommended remediation action in the customer's production environment using Hosted Velociraptor.
- Rapid7 will not be held liable for any actions performed by Active Remediation service.
- If a containment or remediation action is not successful, the MDR SOC team will reach out to the customer to request manual containment of the endpoint.

In no event shall Rapid7 or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information) arising out of the use of, or inability to use, software, service, or capabilities related to action taken by the Active Remediation service, even if Rapid7 has advised customer of the possibility of such damages.

Velociraptor

Velociraptor is a unique, advanced open-source endpoint monitoring, digital forensic, and incident response (DFIR) platform developed by DFIR professionals. Velociraptor provides the ability to more effectively respond to a wide range of digital forensic and cyber incident response investigations and data breaches. Velociraptor mitigates the need to acquire large amounts of data from endpoints for post-processing through targeted queries run directly on the endpoints that return only the data of interest.

MDR Usage

The MDR team members responsible for your service delivery have access to Velociraptor so that they can more thoroughly evaluate alerts when they need additional context than provided in the alert data. If the MDR analyst suspects more widespread activity, they can hunt across endpoints for indicators of compromise. If an endpoint cannot be reached through Velociraptor, the MDR team may send an Offline Collector package for you to run on the endpoint and return the data via the secure file share.

You may see Velociraptor activity within your environment that appears suspicious, but any action SOC analysts may perform as part of an investigation is authorized, and the user will be identifiable as a "Rapid7 analyst."

Access

Direct access to the Hosted Velociraptor UI is only available for customers who:

- Have an InsightIDR Ultimate, Managed Threat Complete Ultimate, Threat Complete Ultimate license, or
- Have purchased the Hosted Velociraptor add-on for InsightIDR.

Velociraptor Endpoint Technology Overview

Hosted Velociraptor communicates with the Insight Platform via two components running under the Insight Agent:

- Agent Core (rapid7_agent_core): The Agent Core manages the communications between the endpoint and the Insight Platform. Agent Core is also included in the Insight Agent installers as of version 4.0.0 and may already be installed on your endpoints.

- Rapid7 Velociraptor (rapid7_velociraptor): This component works with Agent Core to deliver Velociraptor integrated with the Insight Platform.

You do not need to take any action to install these two components. We deploy the Velociraptor on eligible clients via the Insight Agent to all endpoints with auto-updates enabled (you must have platform-managed updates enabled) , and update them as new versions are tested and verified.

Additional Terms

This Scope of Services is governed by the Rapid7 Master Services Agreement available at https://www.rapid7.com/legal/terms/ unless the parties have a fully executed Master Services Agreement which supersedes such standard terms. Any responsibilities and/or actions not explicitly defined in this Scope of Service are not considered part of the Rapid7 MDR Elite service. Rapid7 may modify this Scope of Service at any time by posting a revised version here, which modifications will become effective as of the first day of the calendar month following the month in which they were first posted. Customer deployed software and related services are governed by the Rapid7 Terms of Service available at https://www.rapid7.com/legal/terms.

APPENDIX A

MDR Responsibilities Matrix

	Rapid7	Main POC	Security & IT	C-Suite
Initiation Phase				
Complete Solution Alignment Survey		✓	✓	
Define internal remediation escalation path(s) for MDR reporting		✓		
Set up customer in InsightIDR	✓			
Enable customer in customer's services portal	✓			
Deployment Phase				
Deployment Intro call	✓	✓		
Download and install Collectors		✓		
Deploy Insight Agent to all servers and workstations		✓	✓	
Deploy Insight Network Sensor(s)		✓	✓	
Install Orchestrator and workflows		✓	✓	
Configure event sources	✓	✓		
Ensure collector/agent network connectivity to InsightPlatform		✓		
InsightIDR walkthrough	✓	✓		

	Rapid7	Main POC	Security & IT	C-Suite
Service Delivery Phase				
Service Delivery Kickoff call	✓	✓		
Security Posture Assessment	✓			
Cybersecurity Advisor communication process				
Monthly Meeting	✓	✓		
Periodic Business Review	✓	✓		
Availability for Board and Executive calls (optional)	✓	✓		✓
Ad-Hoc Calls	✓	✓	✓	

	Rapid7	Main POC	Security & IT	C-Suite
Service Delivery Phase (Continued)				
Real-time Security Monitoring				
Investigate alerts categorized as "Rapid7 Managed" as described in the 24x7x365 Security Monitoring.	✓			
Request additional information ("RFIs") from customers as needed to complete investigations resulting from alerts categorized as "Rapid7 Managed."	✓			
Respond to RFIs from Rapid7 with the information requested to complete investigations resulting from alerts categorized as "Rapid7 Managed."		✓		
Investigate investigations categorized as "Custom and Contextual."		✓	✓	
Notify Rapid7 of any investigations categorized as "Custom and Contextual" that may be indicative of malicious activity so that Rapid7 can initiate incident response.		✓		
Detection Rule Tuning (Detection rules categorized as "Rapid7 Managed.")	✓			
Detection Rule Tuning (Detection rules categorized as "Custom and Contextual.")		✓		
Threat Hunting				
Perform regular threat hunts for new or novel threats within the customer's environment	✓			
Provide summary information about threat hunts performed as part of the Monthly Service Report	✓			
Initiate incident response if an active compromise is discovered during a threat hunt	✓			
Threat Intelligence				
Monitor global attacks and vulnerabilities	✓			
Notify customers of significant 'emergent threats', including assessment of threat scope and potential impact, and details of all steps Rapid7 is taking to protect customers from this threat	✓			
Add new detection and response capabilities based on emergent threats	✓			
Incident Response				
Incident identification and notification	✓			
Incident investigation	✓	✓		
Recommend remediation actions (containment and eradication)	✓			
Perform containment actions (assets and users)				
Without Active Response set up		✓	✓	
With Active Response set up	✓			

	Perform containment actions (other)		✓	✓	
	Perform eradication and recovery actions		✓	✓	
	Incident report creation and delivery	✓			
	Recommend corrective actions	✓			
	Perform corrective actions		✓	✓	

APPENDIX B

Technology-Dependent Service Limitations

Some aspects of the Rapid7 MDR service may be degraded as described below if technology deployment or coverage requirements are not fully met.

Service Limitations of a Partially Deployed Environment

Rapid7 MDR recommends full deployment of Insight Agents to all in-scope assets. However, in the event of a partial deployment of the Insight Agent to your environment, your organization understands, agrees, and accepts the limitations and risk of service degradation. The following aspects of the MDR service are unavailable to assets without the Insight Agent installed:

Detection Type	Limitation
Attacker Behavior Analytics	A significant portion of MDR's threat detection power lies in the ability to detect specific events (network connections, process start/stop) on each of the assets. This data can only be provided by the Insight Agent.
Manual Human Threat Hunting	The MDR threat hunts rely on the endpoint agent to collect the data in scope for threat hunts. Assets without the Insight Agent will be excluded from threat hunts.
Alert validation and IR Investigations	MDR's incident investigations rely on the Insight Agent to collect data for analysis. Assets without the Insight Agent will be out of scope for both the typical validation process conducted by the SOC team for an alert as well as any IR investigation.
Local Authentications and Group Membership Changes	The Insight Agent is required to identify authentications using local accounts, such as a local administrator account, and is required to identify local group membership changes (ex: user added to local administrators group). Assets without the Insight Agent will be excluded from local authentication and User behavior (UBA), where UBA is the act of tracking per-user and per-system actions to build statistical models of user activity and identify anomalies.

APPENDIX C

Managed Next-Generation Anti-Virus (NGAV) Technology and Service

Managed Next-Generation Antivirus Insight Agent add-on

Rapid7's Endpoint Prevention capabilities through the Next-Generation Antivirus (NGAV) add-on, offered as a service add-on, is a next-generation antivirus solution that monitors your assets for different kinds of threats and automatically responds according to a policy you've configured. These monitoring and response capabilities are delivered as part of the Insight Agent - the same software that runs silently on your assets and already powers several Rapid7 products like InsightIDR and InsightVM.

Endpoint Prevention add-ons implement their capabilities by way of configurable policies attached to exclusive prevention groups of all eligible agents in an organization. Each policy has a one-to-one relationship with the prevention group it's attached to and is composed of several prevention engines designed to detect specific types of threats. Your configuration of these policies determines what kind of behavior the Endpoint Prevention add-on will monitor, how it will respond when such behavior is detected, and how these events should be prioritized in InsightIDR.

Next-Generation Antivirus uses prevention engines, which are also leveraged in our Ransomware Prevention add-on. Ransomware Prevention acts as an additional layer of protection on your assets, designed to disrupt malicious actors and prevent ransomware attacks before they even start. This technology provides customers with dedicated ransomware prevention engines that reinforce at each stage of an attack to strengthen defenses and minimize exposure. The Next-Generation Antivirus add-on has an additional On-Access Scan (Antivirus) prevention engine compared to the Ransomware Prevention add-on, so runs as your complete antivirus, Endpoint Protection Platform (EPP), and EDR solution.

Note: The Insight Agent broadly supports installations on a range of Windows, macOS, and Linux operating systems. See the operating system support article for a list of Operating System versions eligible for Endpoint Prevention here. *Due to an Operating System requirement that only allows one antivirus solution to be running on the asset at a time, the Next-Generation Antivirus add-onn must be the only instance of antivirus running on your assets. If you have other antivirus software installed on these assets, that software must be uninstalled beforehand.*

Additional information about Rapid7's NGAV technology can be found in the product documentation here.

InsightIDR Next-Generation Antivirus Insight Agent Deployment

At the onset of deployment, the Rapid7 Security Consulting team collaborates with your teams to ensure seamless integration of the Insight Agent - to include the NGAV add-on - into your infrastructure and administration approach. A preliminary test is conducted on a subset of customer-approved endpoints in your environment, enabling the Security Consulting team to 1) equip your team with specific deployment recommendations; 2) educate your team on agent health KPIs; and 3) teach your team to configure policies, exclusions, and groups. The Security Consulting will also remain available throughout your full deployment to support you through any deployment issues you may encounter.

Your MDR Service

When a minimum of one (1) Insight Agent is deployed, the MDR team will conduct a service enablement session, verify agent deployment, NGAV health status and will then begin monitoring your environment. For 24x7x365

security monitoring of your NGAV alerts, your product health status is required to be “Good” (see Antivirus Health Status).

Exclusions

If you want Endpoint Prevention add-ons to ignore specific asset behavior that would otherwise trigger an Agent Action, you can configure and apply exclusions via InsightIDR. You can exclude some behaviors that you consider benign, are actually legitimate processes coming from other software you control, or are simply not relevant to your security concerns.

As part of your MDR service, a standard set of exclusions will be applied to your environment for common applications typically used by MDR customers. You can apply custom exclusions on an as-needed basis; however, exclusions for Endpoint Prevention add-ons should be approached with caution. At its strictest level, Endpoint Prevention is designed to intervene automatically when a threat is detected. Excluding certain behavior from this intervention may also mean increasing the risk of your assets. Ultimately, your business is in the best position to determine what level of risk is acceptable in your environment and what asset behaviors can be safely ignored and Rapid7 shall not be liable in connection therewith. If you have questions or would like consultation on implementing a custom exclusion, consult with your Cybersecurity Advisor.

More details on exclusions and exclusion types can be found in the product documentation here.

Prevention Group

Endpoint Prevention add-ons require all eligible Insight Agents to be associated with a Prevention Group. Prevention groups are the object to which you attach a prevention policy to, add and remove assets from, and apply exclusions to. For initial deployment, all your eligible assets are automatically placed in a default prevention group. This default group uses the immutable default prevention policy configured by Rapid7 to provide a baseline level of protection.

You can create your own custom prevention groups to configure Endpoint Prevention for your organization’s needs, but note that each prevention group has exclusive control of assets inside that prevention group. An asset can only be a member of one prevention group at a time, and associating an asset with a new prevention group will remove it from its existing group.

Note: MDR is not responsible for customer created exclusions and will not be monitoring the logic of these rules to ensure assets are included or excluded from MDR’s ability to monitor alerts from these assets. If a rule is created which excludes an asset or a prevention group from monitoring, these assets will fall outside of the MDR scope of service for 24x7x365 monitoring.

Prevention Policy

The configuration of each prevention engine, and the selection of the engines you decide to use overall, constitutes a prevention policy that you attach to a prevention group. A prevention policy exists solely within a prevention group and has a one-to-one relationship with that group. A group's policy defines what prevention engines should be actively monitoring the assets within that group for threats. You have full configuration control over the policies attached to your prevention groups.

Rule Priority

When a prevention engine responds to a detected threat with an Agent Action, it also tags the detection with a priority level you configure in your prevention policy. This designation is called Rule Priority. In the context of

InsightIDR, rule priority is used to inform your security practitioners of the urgency they should respond to investigations or alerts generated by the rule being triggered.

The Endpoint Prevention add-ons support these priority levels:

- **Low**
- **Medium**
- **High**

MDR will provide 24x7x365 security monitoring, investigation, and response for all “MDR Responsibility” Endpoint Prevention alerts at all priority levels.

Antivirus Health Statuses

There are four possible health statuses for your Insight Agents:

- **Good** - Antivirus is running successfully.
    - This is the desired status and indicates that the Endpoint Prevention add-on is operating on the Insight Agent as it should.
- **Poor** - Antivirus is running, but errors are present.
    - This status indicates that while the Endpoint Prevention add-on on the Insight Agent is functioning, the Insight Agent has encountered errors that may impact its performance.
- **Not Monitored** - Endpoint Prevention is installed on this Insight Agent, but its prevention policy does not have the On-Access Scanning (Antivirus) prevention engine enabled or the engine has encountered an internal error.
    - This status indicates that the asset on which the Insight Agent is installed has the Next-Generation Antivirus add-on, but threats are not being actively responded to.
- **N/A** - Antivirus is not installed due to an incompatible operating system or a connection issue. Check the requirements for antivirus eligibility details here.
    - Any Insight Agent installed on an operating system that's ineligible for the Next-Generation Antivirus add-on add-on will have this status. Insight Agents installed on assets running eligible operating systems can also have this status if a connectivity issue is preventing the Insight Agent from retrieving the Next-Generation Antivirus add-on from the Insight Platform.

Agent Actions

You can separately configure how the Insight Agent will respond to detected threats for each prevention engine in your policy. Overall, the Insight Agent is capable of these actions:

- **Block -** The Insight Agent will actively block any threat detected by the prevention engine and generate an alert in InsightIDR. Depending on the context of the threat, this could involve terminating malicious processes, denying access to files, and other active prevention methods.
- **Disinfect -** Specific to the On-Access Scanning (Antivirus) engine, the Insight Agent will attempt to remove the detected threat from affected files and generate an alert in InsightIDR.
- **Detection Only -** The Insight Agent will take no action other than generating an alert in InsightIDR.
    - This setting functionally disables Rapid7’s Endpoint Prevention technology's ability to play an active role in safeguarding your assets. You may determine that some asset behaviors do not warrant agent intervention beyond generating alerts in your environment, but be aware that you will need to be responsible for handling threats detected in these circumstances.

Activation Modes

Endpoint Prevention add-ons can operate in two modes. Like all settings in Agent Management, you configure this activation mode on a per-organization basis:

- **Monitor Only** - Your Insight Agents will not take any of the actions dictated by your prevention policies when threats are detected, but monitoring will continue nonetheless. When threats are detected, these events will be logged and alerts will still be generated.
    - This is the default mode for all Endpoint Prevention add-ons and allows you to complete all necessary configuration tasks before you're ready to switch to Active Prevention.
    - If you need to troubleshoot your Endpoint Prevention add-on, you can switch back to Monitor Only for this purpose.
- **Active Prevention** - Your Insight Agents will actively respond to detected threats with the actions dictated by your prevention policies. All such events will be logged and sent to InsightIDR for analysis and further action, if necessary. This mode should only be used once you have completed initial deployment and configuration.

Security Settings for Endpoint Prevention (Windows OS only)

The existence of an endpoint security solution can often lead to attackers attempting to tamper with the solution, so that they can freely perform malicious activities without being detected. The Tamper Protection engine is currently only available on Windows operating systems.

The **Tamper Protection** engine contains the required rules to protect the Endpoint Prevention add-on of the Insight Agent, therefore protecting your assets continuously.

When Tamper Protection is turned on, it prevents malware and bad actors from tampering with the files and functionality of Endpoint Prevention add-ons. It also offers the option of turning on **Password Protection**.

Using a one-time passcode (OTP) or a fixed password allows you to limit the users who can update, stop, or uninstall the Endpoint Prevention service. You can activate password protection at both the organizational level and for individual prevention groups that require extra security.
View more details about these security settings here.

Prevention Engine Details

The following prevention engines are available for use and configuration in your prevention policies. This section provides a high-level explanation of what each of these engines detect.

- **On Access-Scan (Antivirus)** - Available to Windows, Mac, and Linux operating systems, the On-Access Scanning prevention engine scans local and network files for viruses in real-time when a user accesses them, such as when a file is opened, moved, copied, or executed. When infected files are detected, you can decide the action you want to take on them. The engine can also update itself automatically, providing protection against the latest viruses and other types of malware.

The following engines are currently only available for Windows operating systems:

- **Memory Injection Attacks** - Malicious software can sometimes inject and hide itself in a legitimate process. The Memory Injection Attacks prevention engine stops fileless threats and blocks code execution from the file system, causing such malware to exit or crash.
- **Living-Off-the-Land Attacks** - Different from classic forms of malware, a Living-Off-the-Land attack attempts to cause damage by misusing tools that are built into the system. The Living-Off-the-Land Attacks prevention engine blocks the malicious software's ability to leverage such tools to infect an asset.
- **Malicious Document Attacks** - Malicious documents can sometimes misuse features such as macros, scripts, and built-in tools. The Malicious Document Attacks prevention engine disarms the malicious documents' attempts and allows applications to operate without being infected.
- **OS Credential Dumping Attacks** - Attackers or malware can sometimes attempt to harvest operating system credentials to gain access to an environment. The OS Credential Dumping Attacks prevention engine protects sensitive files, processes, and other key artifacts to prevent this type of threat.
- **File and Process Manipulation Attacks** - Malicious software can attempt to manipulate other software applications and processes to gain access to an asset's internal files. This prevention engine prevents malware from making deceptive modifications to files and processes.

Components of your NGAV Service Deliverables

Service reports listed below will include specifics about your Managed Next-Generation Antivirus add-on service. These include:

Deliverable	Description
Incident Response Reports	Details all analysis and incident management activities, key findings, the timeline of attacker activity, and recommended corrective actions to prevent the likelihood of recurrence and/or improve your ability to detect and respond to similar incidents in the future
Monthly Service Reports	Provides metrics and context about threat detection and incident response activities conducted in the previous month, along with information about the health of detection and response controls in your environment

InsightIDR NGAV Insight Agent Responsibilities Matrix

	Rapid7	Main POC	Security & IT	C-Suite
Deployment & Onboarding Phase				
Complete Technical Preparations *(see Endpoint Prevention Overview)*		✓		
Deployment Testing & Support	✓			
Customer Deployment			✓	

	Rapid7	Main POC	Security & IT	C-Suite
Service Delivery Phase				
Default Exclusion Policy Configuration	✓			
Custom Exclusion Policy Configuration		✓		

Default Prevention Group Configuration	✓	✓		
Custom Prevention Group Configuration		✓		
Default Prevention Policy	✓			
Custom Prevention Policy		✓		
Activation Mode Configuration		✓		
Real-time Security Monitoring				
Investigate alerts categorized as “Rapid7 Managed” as described in the 24x7x365 Security Monitoring	✓			
Request additional information (“RFIs”) from customers as needed to complete investigations resulting from alerts categorized as “Rapid7 Managed.”	✓			
Respond to RFIs from Rapid7 with the information requested to complete investigations resulting from alerts categorized as “Rapid7 Managed.”		✓		
- Investigate “Rapid7 Managed” Endpoint Prevention alerts - Customer to investigate Endpoint Prevention: on-access scanning (Antivirus) alerts	✓	✓		

APPENDIX D

Ransomware Prevention

Rapid7 Ransomware Prevention, offered as a service add-on, adds an additional layer of protection on the endpoint designed to disrupt malicious actors and prevent ransomware attacks before they even start. This technology provides customers with dedicated ransomware prevention engines that reinforce at each stage of an attack to strengthen defenses and minimize exposure. Ransomware prevention can also co-exist with Rapid7s existing NextGen AntiVirus (Endpoint Prevention) solution.

Endpoint Prevention implements its capabilities through configurable policies attached to exclusive groups of all eligible agents in an organization. Each policy has a one-to-one relationship with the group it's attached to and comprises several prevention engines designed to detect and prevent specific types of threats. Your configuration of these policies determines what kind of behavior Endpoint Prevention will monitor, how it will respond when such behavior is detected, and how these events should be prioritized in InsightIDR.

Your MDR Service

The Insight Agent serves as the vehicle through which the Endpoint Prevention feature and its capabilities are delivered. You need to have at least one (1) Insight Agent deployed before you can start utalizing Ransomware Prevention.

Exclusions

If you want Ransomware prevention to ignore specific asset behavior that would otherwise trigger an agent action, you can configure and apply exclusions via InsightIDR. You can exclude some behaviors that you consider benign, are actually legitimate processes coming from other software you control, or are simply not relevant to your security concerns.

You can apply custom exclusions on an as-needed basis; however, exclusions in Endpoint Prevention should be approached with caution. At its strictest level, Endpoint Prevention is designed to intervene automatically when a threat is detected. Excluding certain behavior from this intervention may also mean increasing the risk of your assets. Ultimately, your business is in the best position to determine what level of risk is acceptable in your environment and what asset behaviors can be safely ignored and Rapid7 shall not be liable in connection therewith. If you have questions or would like consultation on implementing a custom exclusion, consult with your Cybersecurity Advisor.

More details on exclusions and exclusion types can be found in the product documentation here.

Prevention Group

Ransomare Prevention requires that all eligible Insight Agents are associated with a prevention group. Prevention groups are the object to which you attach a prevention policy, configure agent membership, and apply exclusions. For initial deployment, all your eligible agents are automatically placed in a default prevention group. Ransomware Prevention will be provisioned remotely. Your organization's settings are set up as Monitor Only.

You are free (and encouraged) to create your own custom prevention groups to meet your Endpoint Prevention goals, but note that each group has exclusive control of agents inside that group. An agent can only be a member of one group at a time, and associating an agent with a new group means removing it from its existing group.

Note: MDR is not responsible for customer-created exclusion rules and will not be monitoring the logic of these rules to ensure agents are included or excluded from MDR's ability to monitor alerts from these agents. If a rule is created which excludes an agent or a prevention group from monitoring these agents such will fall outside of the MDR scope of service for 24x7x365 monitoring.

Prevention Policy

The configuration of each prevention engine and the selection of the engines you decide to use overall constitute a prevention policy that you attach to a prevention group. A prevention policy exists solely within a prevention group and has a one-to-one relationship with that group. A group's policy defines what prevention engines should actively monitor the agents within that group for threats. You have full configuration control over the policies attached to your prevention groups.

Rule Priority

When a prevention engine responds to a detected threat with an agent action, it tags the detection with a priority level you configure in your prevention policy. This designation is called rule priority. In the context of InsightIDR, rule priority is used to inform your security practitioners of the urgency with which they should respond to investigations or alerts generated by the rule being triggered.

Endpoint Prevention supports these priority levels:

- **Low**
- **Medium**
- **High**

MDR will provide 24x7x365 security monitoring, investigation, and response for all Ransomware alerts categorized as "MDR Responsibility" at all priority levels.

Agent Actions

You can separately configure how the Insight Agent will respond to detected threats for each prevention engine in your policy. Overall, the Insight Agent is capable of these actions:

- **Block -** The Insight Agent will actively block any threat detected by the prevention engine and generate an alert in InsightIDR. Depending on the context of the threat, this could involve terminating malicious processes, denying access to files, and other active prevention methods.
- **Detection Only -** The Insight Agent will take no action other than generating an alert in InsightIDR.
    - This setting functionally disables Endpoint Prevention's ability to play an active role in safeguarding your assets. You may determine that some asset behaviors do not warrant agent intervention beyond generating alerts in your environment, but be aware that you will need to be responsible for handling threats detected in these circumstances.

Endpoint Prevention Activation Modes

Endpoint Prevention can operate in two modes. Like all settings in Agent Management, you configure this activation mode on a per-organization basis:

- **Monitor Only** - Your Insight Agents will not take any of the actions dictated by your prevention policies when threats are detected, but monitoring will continue nonetheless. When threats are detected, these events will be logged, and alerts will still be generated.
    - This is the default mode for all Endpoint Prevention programs and allows you to complete all necessary configuration tasks before switching to Active Prevention.
    - If you need to troubleshoot your Endpoint Prevention configuration, you can switch back to Monitor Only for this purpose.
- **Active Prevention** - Your Insight Agents will actively respond to detected threats with the actions dictated by your prevention policies. If necessary, all such events will be logged and sent to InsightIDR for analysis and further action.

Security Settings for Endpoint Prevention

The existence of an endpoint security solution can often lead to attackers attempting to tamper with the solution, so that they can freely perform malicious activities without being detected.

The **Tamper Protection** engine contains the required rules to protect the Endpoint Prevention component of the Insight Agent, therefore protecting your assets continuously.

When Tamper Protection is turned on, it prevents malware and bad actors from tampering with the files and functionality of Endpoint Prevention. It also offers the option of turning on **Password Protection**.

Using a one-time passcode (OTP) or a fixed password allows you to limit the users who can update, stop, or uninstall the Endpoint Prevention service. You can activate password protection at both the organizational level and for individual prevention groups that require extra security.
View more details on Endpoint Prevention here.

Prevention Engine Details

The following prevention engines are available for use and configuration in your policies. This section provides a high-level explanation of what each of these engines detect.

- **Memory Injection Attacks** - Malicious software can sometimes inject and hide itself in a legitimate process. The Memory Injection Attacks prevention engine stops fileless threats and blocks code execution from the file system, causing such malware to exit or crash.
- **Living-Off-the-Land Attacks** - Different from classic forms of malware, a Living-Off-the-Land attack attempts to cause damage by misusing tools that are built into the system. The Living-Off-the-Land Attacks prevention engine blocks the malicious software's ability to leverage such tools to infect an asset.
- **Malicious Document Attacks** - Malicious documents can sometimes misuse features such as macros, scripts, and built-in tools. The Malicious Document Attacks prevention engine disarms the malicious documents' attempts and allows applications to operate without being infected.
- **OS Credential Dumping Attacks** - Attackers or malware can sometimes attempt to harvest operating system credentials to gain access to an environment. The OS Credential Dumping Attacks prevention engine protects sensitive files, processes, and other key artifacts to prevent this type of threat.
- **File and Process Manipulation Attacks** - Malicious software can attempt to manipulate other software applications and processes to gain access to an asset's internal files. This prevention engine prevents malware from making deceptive modifications to files and processes.

Components of your Ransomware Service Deliverables

Service reports listed below will include specifics about your Ransomware service. These include:

Deliverable	Description
Incident Response Reports	Details all analysis and incident management activities, key findings, the timeline of attacker activity, and recommended corrective actions to prevent the likelihood of recurrence and/or improve your ability to detect and respond to similar incidents in the future
Monthly Service Reports	Provides metrics and context about threat detection and incident response activities conducted in the previous month, along with information about the health of detection and response controls in your environment

InsightIDR Ransomware Agent Responsibilities Matrix

	Rapid7	Customer Main POC	Customer Security & IT	Customer C-Suite
Deployment & Onboarding Phase				
Customer Deployment		✓		

	Rapid7	Customer Main POC	Customer Security & IT	Customer C-Suite
Service Delivery Phase				
Default Exclusion Policy Configuration	✓			
Custom Exclusion Policy Configuration		✓		
Default Prevention Group Configuration	✓	✓		
Custom Prevention Group Configuration		✓		
Default Prevention Policy	✓			
Custom Prevention Policy		✓		
Activation Mode Configuration		✓		
Real-time Security Monitoring				
Investigate alerts categorized as “Rapid7 Managed” as described in the 24x7x365 Security Monitoring	✓			
Request additional information (“RFIs”) from customers as needed to complete investigations resulting from alerts categorized as “Rapid7 Managed.”	✓			
Respond to RFIs from Rapid7 with the information requested to complete investigations resulting from alerts categorized as “Rapid7 Managed.”		✓		
Investigate “Rapid7 Managed” Endpoint Prevention alerts	✓			

APPENDIX E

Penetration Testing

Many MDR customers perform penetration testing as an end-to-end assessment of their security controls - from prevention to detection and response. As a trusted partner responsible for detection and response to threats in your environment, Rapid7 will support these testing efforts as described in this section.

Planning for a Successful Penetration Test

Penetration tests can be planned and executed in many different ways, depending on your objectives and available testing resources. In some cases, a penetration test is only intended to validate the preventative controls of an organization, in which case testing scope may be limited to initial access and discovery activities. However, if you intend to also test the detection capabilities of your organization (and by extension Rapid7 MDR), please take the following into consideration:

- 'Assumed breaches' are less realistic and more difficult to detect. 'Assumed breach' is the practice of allowing the penetration tester initial access to your environment (for example, by connecting an unmanaged asset to your internal network). While Rapid7 may still detect this subsequent activity, many of our most effective detection techniques are focused on initial compromise activity originating from monitored customer assets.
- Your test should include as many of the steps in the 'kill chain' as possible - from initial access, to persistence, privilege escalation, and lateral movement. Performing isolated 'suspicious actions' is no substitute for a fully scoped penetration test.

If you have questions or concerns about whether your penetration test is correctly scoped to adequately test your detection and response controls, we encourage your team to work with your Cybersecurity Advisor in advance of the test. Your Cybersecurity Advisor can review your plans and provide feedback before the test begins.

In order to better coordinate resources and discern between pentest activity and real world threats, we ask that you inform your Cybersecurity Advisor in advance of conducting any scheduled penetration testing. This notification ensures that the MDR SOC is ready to promptly address any conflicts between testing activities and activities associated with potential malicious activity and that we can dedicate resources appropriately.

Please note that Rapid7 does not report on ongoing security testing that utilizes known-good testing frameworks. Rapid7 closes alerts generated by these frameworks as "Security Testing" for your review.

Initial Detection of Penetration Testing Activity

If the MDR SOC detects penetration test activity, we will follow the Incident Response process and escalate the activity to you as confirmed or suspected malicious activity. It's important for us to coordinate closely allowing our team to align with this activity so it is essential to inform Rapid7 immediately if the activity is related to a scheduled penetration test. This will ensure that the MDR SOC can 'de-conflict' testing activity from other potential attacks, as well as ensuring MDR SOC resources remain focused on detecting and responding to actual security incidents on behalf of all customers.

MDR analysts will continue to monitor for related testing activities and use additional context provided by your team (or determined through analysis), to differentiate between penetration test activity and potential attacker activity.

Subsequent Response to Penetration Testing Activity

Once a penetration test has been detected by Rapid7 and confirmed by you, the Rapid7 MDR team will ask you which engagement model you prefer:

- **No additional reporting** (default): Your team will not be alerted to further activity related to the penetration test, and a 'rollup report' of all related activity will not be provided at the conclusion of your test.
- **Rollup report**: The MDR team will identify any subsequent alerts related to this test and will deliver our findings as an aggregate 'roll-up' report which will list which alerts the SOC would have investigated had this been a real attack.

NOTE: MDR will *not* initiate full incident response activities (as described in the Incident Response section) in response to a penetration test, as these resources are reserved for response to actual security incidents on behalf of our customers. Furthermore, Rapid7 will not participate in your penetration test as the "blue team" for an undisclosed purple team.

Post-Test Reporting and Lessons Learned

Rollup Report

It is required that your team notifies your CA at the conclusion of the penetration test. Rapid7 will then provide a 'rollup report' of all alerts related to the penetration test. Upon review of this report, if you believe that Rapid7 may have missed specific penetration test activity, you may reach out to Rapid7 to review these potential detection gaps. Please note that Rapid7 is **not** responsible for performing this gap analysis on customer's penetration test reports. In order for Rapid7 to address potential detection gaps, your team **must** provide Rapid7 with specific examples of penetration test activity for which Rapid7 did not generate alerts. Rapid7 **requires** the following information for these specific examples**:**

- Description of the activity and/or tools used
- Timestamp(s) of the activity
- Associated asset name(s) and IP address(es)
- Associated account(s)

Missed Penetration Tests

If you performed a properly scoped penetration test (see 'Planning for a successful penetration test' above) and Rapid7 did not notify you of *any* activity related to the test, you may request an 'After Action Review' within **60 days** of the conclusion of the penetration test. In order for Rapid7 to perform this review, your team **must** provide Rapid7 with the full penetration test report provided to you by your penetration testing team, and enable Rapid7 to ask follow-up questions of your penetration testing team as needed.

Once these details are provided to Rapid7, we will perform a full review of the activity performed and to what extent this activity was logged and alerted on by InsightIDR, and how any resulting investigation(s) were handled by the Rapid7 MDR team. We will provide an After Action Report describing the results of this review, including 'lessons learned' and resulting 'corrective actions' that should be taken by either Rapid7 or the customer to improve the ability to detect similar activity in the future.

Please allow up to **30 days** from when all requested details are provided to Rapid7 for the final report to be delivered.

APPENDIX F

Rapid7 Managed Digital Risk Protection (MDRP)

Rapid7's MDRP is an add-on service offering for Managed Detection and Response ("MDR") and Managed Threat Complete customers that combines key components of our Threat Intelligence solution and expertise from MDR Analysts to protect your critical digital assets and data from external threats, to provide guidance and remediation where appropriate, and support rapid triage and investigation if active threats are identified in your environment.

The integration with our traditional MDR service allows you to have visibility across the clear, deep, and dark web to identify the earliest signals of an imminent attack or leaked data, stop threats earlier, and take action to protect your digital assets in the event of an active threat.

MDRP Team

In addition to the MDR/Managed Threat Complete team, you will be introduced to the following specialist roles involved in delivering your MDRP service: MDRP Onboarding Specialist, MDRP Analysts, Threat Intelligence Analysts, the 'Ask-an-Analyst' team, and the Remediation Service team that supports actions such as takedowns.

MDRP Onboarding Specialist

The MDRP Onboarding Specialist is responsible for helping you understand how the service and technology operate and how to get support and assistance when required. They will help you set up the required integrations with InsightIDR and start your service. Once the technology is operational and the required contextual information has been collated and integrated into your MDRP instance, you will be transitioned to your Cybersecurity Advisor.

MDRP Analyst

The primary function of the MDRP Analyst is to review and triage alerts in your platform to ensure the alerts you receive are as accurate as we can make them and are high fidelity. It is important to note that the accuracy of any threat/alert is heavily influenced by the uniqueness and clarity of your assets and the contextual information provided.

The MDRP Analyst will also leverage InsightIDR technology to validate that reported intelligence threats are not actively exploited in your environment. If we suspect that a reported intelligence threat, e.g., a lookalike website, is actively exploited by an attacker in your environment, the MDRP Analyst will escalate the incident to the MDR service team for investigation by the Rapid7 MDR SOC. If an active cyber threat is confirmed, your MDR team will notify you, as outlined in the MDR/Managed Threat Complete scope of service. The MDRP Analyst will monitor your alert queue during standard business hours (9 am to 5 pm, CET local time) Monday through Friday, excluding nationally observed holidays.

Threat Intelligence Analyst

Rapid7 Threat Intelligence Analysts are responsible for monitoring and examining internal and external cyber threats to assess risk on behalf of your organization. They will investigate trending global cyber events and emerging dark web content to identify threat actors' interests and motivations, highlight relevant information, and track down actors that potentially threaten your company. They spend most of their time analyzing ongoing attacks, such as phishing, DDoS, data leakage, ransomware, and more, to assess their origin, purpose, and potential impact on Rapid7's customers.

‘Ask an Analyst’ Team

Rapid7’s "Ask an Analyst" team provides guidance, additional context, remediation steps and recommendations, executing dark web purchases, and requesting threat actor engagement on existing alerts. They will respond to your requests for information via the Ask-an-Analyst chat box and investigate them using every tool and technique at our disposal to uncover new information.

You can also open a case via the customer portal to request information related to significant global cyber events, essential investigation of email addresses, dark web mentions on our database, or additional information on threat actors. The ‘Ask an Analyst’ service is available 24/7.

Remediation Service Team

The Remediation Service team engages external enforcement to take down campaigns that impersonate your brand, infringe on trademarks and copyrights, and threaten your organization's security. Rapid7’s in-house automated Remediation Services team can help you expedite takedowns of malicious and harmful web content targeting your brand.

Response Options	Quantity	Description
Remediation Requests	Limited to 50 requests per year **Additional bundles available*	Request that Rapid7 contact a content provider and act on your behalf to remove a threat from the Internet. The success of a remediation request is dependent on the proper preparation and submission of evidence. Rapid7 will help you collate and prepare the evidence to make a formal request.
Dark Web Purchases	Limited to 50 per year **Additional bundles available*	Rapid7 offers secure and anonymous clear and dark web purchases made on your behalf. To request a purchase, use the “Ask an Analyst” button in the dashboard.

Threat Intelligence Research Service Team

Rapid7 provides deep-dive investigation services and reports into external cyber threats, tactical attack or breach-related research, and strategic trend-based research. We offer an optional catalog that describes our standard menu of research offerings, how research is conducted, typical deliverables, and pricing should you require additional Threat Intelligence Research reports. Additional information can be provided through your Cybersecurity Advisor or the ‘Ask an Analyst’ team.

Cybersecurity Advisor Engagement

During your MDRP service, you will regularly engage with your Cybersecurity Advisor (CA). Your CA will be available to answer any questions and advise you on how to get the most from your MDRP service. They can offer guidance to best leverage the platform, when and how to engage with your Rapid7 teams, advise you when collecting evidence to support remediation actions, and how best to leverage dark web purchases. Your CA will also work with you to periodically review and tune noisy alerts created in the platform, configure and maintain appropriate notification settings, and help you understand how to schedule executive and technical reports via user dashboards.

Your CA will be available by phone and via the customer portal as outlined in the MDR/Managed Threat Complete scope of service.

In-Scope Service Components

MDRP is built around Rapid7's Digital Risk Protection platform, which delivers proactive defense by transforming threat intelligence into actionable insights.

Our platform leverages ground-breaking data-mining algorithms and unique cyber reconnaissance capabilities to continuously scan the clear, deep, and dark web to deliver actionable, contextual reconnaissance about potential threats to your organization, employees, executives, and board members. It integrates with our existing security solutions to highlight operational vulnerabilities, secure data, and protect your resources. This, combined with additional findings and expertise from the Threat Intelligence Analyst team, provides comprehensive protection for your organization.

MDRP incorporates the following components:

Modules Included	Description
Phishing Protection	
- Phishing Domains	Domains that may be used to launch future phishing attacks, typically against company employees or your customers. Alternatively, when a company website is copied or users are redirected to an illegitimate site to steal credentials or initiate malware attacks.
- Phishing Websites	Detected Phishing Websites impersonating the business or brand
Data Leakage	
- Leaked Ransomware Files	Internal or Company documents that are exposed publicly typically include user credential information or documents published following a ransomware incident.
- Credentials from Botnets	Employee/customer credentials found on Botnets
- Leaked User Credentials	Employee credentials found
Mobile Applications	
- Mobile Apps	Fake/suspicious/malicious mobile applications
Attack Indicators	
- Sectoral/Regional Alerts	Threat actors, campaigns, and malware targeting your sector/vertical
- Credit Cards for Sale	Company credit cards, bot-harvested credentials, or products sold on dark web black markets.
- InfoStealer Data for Sale	Data from information-stealing malware that is offered for sale on the Black Market
- Ransomware Live	Proactive scanning for mentions of customer assets within the list of ransomware victims from monitored blogs of active ransomware groups.
- Company Credentials/Botnets for Sale	Employee credentials that have been identified within a data dump or being sold on the dark web
- Attack Indication in Different Languages	Ability to translate information found in other languages back into English
Dark Web Monitoring	
- Dark Web Mentions	Black markets, cybercrime forums, etc.

Exploitable Data	
- SSL Issues	SSL/TLS handshake failed, TLS 1.0 enabled, vulnerabilities
- Open Environments	Internal environments/logins that are publicly facing
- Open Ports	Detection of open ports on external-facing IP addresses
- Email Security Validation	Missing DMARC/SPF records
- IP Reputation	Detection of external organization IP addresses that have been abused or reported to the IP blacklist provider
VIP Protection	
- SSN	Published Social Security numbers (for customers located in North America)
- Fake LinkedIn Profiles	Illegitimate LinkedIn Profiles Impersonating VIP's
Exposed FTP Login Pages	Exposed or unencrypted FTP Login pages
Social Media	*MDRP includes coverage of two social media sources. LinkedIn & Facebook are covered by default. Customers have the option to replace default sources from the list below.
- Linkedin	- Suspicious management/HR/executive position alerts - Suspicious VIP profile alerts - Suspicious company profile alerts
- Facebook	- Suspicious VIP profile alerts - Suspicious company page alerts
- Twitter	- Suspicious VIP profile alerts - Suspicious company profile alerts
- Instagram	- Suspicious VIP profile alerts - Suspicious company page alerts
- Youtube	- Suspicious channels
- Weibo	- Suspicious company page alerts

Service Reports

Bi-Weekly Threat Landscape Report

As an MDRP customer, you'll receive Rapid7's Bi-Weekly Threat Landscape Report sent directly to your preferred email. This report contains a general overview of the current threat landscape and features data curated from well-established cybersecurity newsletters and vendors.

Semi-Annual Industry Threat Landscape Report

The Industry Threat Landscape Report details the cyber threat landscape of a particular industry (for example, finance, telecommunications, energy, manufacturing, automotive, and retail). It provides an overview of each industry's various threats and cyber risks.

As part of your subscription, you will automatically receive a Semi-annual Industry Threat Landscape Report related to your industry. Reports will be provided in January and July of each calendar year and distributed to the email of your organization's designated admin user(s) defined in the platform.

Executive Summary Report

The Executive Summary report shows a high level breakdown of your alert types, remediation status as well as common sources of where your assets are being shown (pasted sites, black markets, etc). This report can be generated on custom timeframes depending on your team's needs (recommended monthly). All reports within Threat Command can be scheduled to run and be delivered to your email inbox, on a regular cadence of your choosing.

Return on Investment Report (ROI)

The ROI report outlines the overall risk and value your organization receives from the Threat Command platform. It provides your risk score and shows how your company compares to the industry benchmark. The report also highlights the Remediation & Takedown activity performed on behalf of your organization, an alert breakdown, and false positive rate determined by the MDRP analyst team. It helps identify opportunities to increase platform value and improve your overall security posture. All reports within Threat Command can be scheduled and delivered to your email inbox at a cadence of your choosing.

Service Deliverables

Monthly Service Review

Your CA will include a summary and overview of your MDRP service status during planned monthly meetings. The monthly meetings with your CA may include:

Deliverables	Description
Asset Review	Your assigned CA will work with your defined asset list and ensure all areas of your external environment are covered within the Threat Command Platform.
Remediation & Dark Web Purchase Review	Rapid7 will review remediations and dark web purchases on a monthly basis to confirm necessary actions took place, and to provide recommendations on how to protect against these threats further.
Alert review	Rapid7 will highlight any anomalies in alerting and go through discovery of particular domains or alerts of interest, and help update the alert profiler to reduce alert fatigue depending on each individual case.
Policy review	Rapid7 will assist with any automations within the Threat Command environment that could demonstrate value to your team and overall security posture.
Reporting	Rapid7 will ensure you are receiving the Executive Summary and ROI reports each month and review to help identify trends and show areas of improvement within your threat landscape.

Technology

The Rapid7 MDRP service is powered by Threat Command (Intel) and InsightIDR (XDR).

Threat Command Platform

Your subscription will include a single instance of Threat Command for your entire organization. Every security team user will be provided access to all data stored within this single instance. They will also be able to make requests to the 'Ask an Analyst' team, initiate remediations, approve dark web purchases, and access any other offering under this Scope of Service.

Threat Command monitors thousands of sources across the clear, deep, and dark web to identify threats targeting your unique digital footprint. It helps you make informed decisions and act quickly on critical threats posing the greatest risk to your business. Use cases supported include dark web monitoring, phishing protection, VIP protection, data/credential leakage, ransomware disclosure monitoring, fraud, and much more. User-based access controls are supported.

InsightIDR Instance

InsightIDR is Rapid7's cloud XDR solution which unifies Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Security Analytics technologies to provide comprehensive protection against intruders on your organization's internal network, devices, and cloud services. InsightIDR and the MDR delivery team leverage the Insight Agent and other event sources from your existing security infrastructure to ensure visibility into threats across your environment.

The offering requires the configuration and setup of the native InsightIDR to Threat Command integration to allow seamless investigation from the MDR SOC. Enabling integration will allow you to see all your MDRP alerts within InsightIDR.

Activating Your MDRP Service

Rapid7 has to populate your organization's assets into Threat Command before service can begin. You must add every asset that requires monitoring to an asset discovery sheet that will be shared by your Rapid7 account team as part of onboarding. If a POC is performed, asset collection is completed as part of that process.

Once assets are loaded, the platform automatically generates alerts and monitoring begins. If needed, you may schedule an MDRP overview session with your CA, to review your platform instance and answer any questions you may have.

MDRP Service Process

Rapid7's Threat Command platform monitors thousands of sources across the clear, deep, and dark web to deliver tailored threat intelligence alerts based on your organization's unique digital assets. In addition, Threat Intelligence Analysts work continuously to collate and research threat intelligence data related to your digital assets from areas of the Internet and dark web that are not open or capable of being automatically crawled, searched, or collated.

Between these intelligence data sources, the MDRP service offering aims to provide you with the most accurate, relevant, and up-to-date threat intelligence with actionable insights and recommendations.

However, not all intelligence sources are created equal, and not all digital assets are uniquely identifiable or contextually recognizable. There is always the risk of false positives and contextually incorrect alerts flowing into your view. These numbers can vary greatly depending on the use case, sources, and assets, creating the need for

customers to spend time triaging and validating alerts to ensure they represent risks with high confidence of accuracy.

Our service removes the need for you to manually review the output of your Threat Command platform to validate the accuracy of alerts if you lack the resources or inclination to do so yourself.

As part of your MDRP service, analysts will review any low-confidence alerts generated from the platform's in-scope modules each business day to remove false positives and ensure that any alerts reported to you have high confidence and validity.

In addition, your MDRP Analyst, where applicable, will pivot to InsightIDR to check for evidence of forensic artifacts that may indicate if an attacker is actively exploiting a reported risk. If suspicious activity is identified, the MDRP Analyst will escalate any potential or confirmed incident to the MDR SOC team for further investigation.

Remediation Services

Rapid7's Threat Intelligence remediation services include the following coverage areas:

Remediation Coverage
• Domains that were involved in phishing campaigns against our customers or their customers
• Phishing websites posing as a customer
• Fraudulent social media pages impersonating a customer, including fake job offers
• Fake and/or suspicious mobile applications posing as a legitimate customer application
• Pastes that contain sensitive data and/or any attack intention
• Suspicious email account posing as a customer
• Files or any malicious items involved in phishing or malware attacks against a customer
• Google search results leading to phishing websites and fraudulent activities
• Suspicious LinkedIn VIP profiles

This service is provided by contacting the source of fraudulent information to have the malicious item removed or suspended. The success rate is based on Rapid7's cooperation with the website owner or registrar and our ability to provide characteristics of suspicious content. Therefore, Rapid7 can't guarantee that remediations will be successful or completed within a certain timeframe. For social media sites, the fake profile must clearly resemble the customer's graphical content, logos, industry, etc., and present a security risk. For domains, evidence of malicious intent indicative of a security risk must be provided before removing it.

Remediation Requests

Rapid7 proactively identifies and alerts customers to thousands of instances of domain impersonation, exposed sensitive data, leaked customer details, and spoofed mobile applications. Our in-house remediation service acts as a force multiplier, operating as a direct extension of your SOC and security teams.

Rapid7 handles dozens of remediation requests daily, allowing customers to utilize our dedicated team of experts to gather prerequisites, accelerate requests, and streamline workflows so malicious content can be removed quickly.

You are entitled to 50 remediation requests annually. At the end of each contract year, your request allotment will be reset, any unused remediation requests are forfeited and will not be carried over to the following year.

Advanced Remediation

Mitigating risks posed by exposed threats often requires actively removing malicious or infringing content from various websites, platforms, app stores, and domain registrars. Rapid7 can attempt a takedown on behalf of your organization for sources that are supported as part of your service. For example, if there is an alert where the "Remediate" button does not exist, this indicates that the specific alert source cannot be taken down as part of the standard remediation services offering.

Rapid7 continually develops new partnerships with web registrars, app stores, and social media sites based on new attack vectors and hacker trends. Advanced remediation requests should be submitted as cases via the Rapid7 customer portal.

For more details about Rapid7's remediation services, please refer to the Remediation Services Overview.

Dark Web Purchases

Rapid7 offers secure and anonymous clear and dark web purchases made on your behalf. You are entitled to 50 dark web purchases annually. At the end of each contract year, your purchase allotment will be reset, and any unused purchases are forfeited and will not be carried over to the following year. While most requests typically require one credit, each situation is unique. The credits required for each request will be at the discretion of the Threat Intelligence team, depending on the effort involved and the type of purchase. Some scenarios may require two or more credits. Please contact the Threat Intelligence team via the Ask the Analyst chat for details of each request, and they will await your approval before processing any purchases on your behalf. Rapid7 offers additional packages in the event all credits are used before the end of your subscription.

Sometimes, it may need to be clarified whether or not to make a purchase on the dark web. Leverage your CA and the Threat Intelligence Analysts for guidance when making purchases as not everything being sold may be eligible to purchase. Rapid7 can provide recommendations based on our knowledge of the dark web and the reputation of threat actors.

Please note there is no way to know for certain if specific information purchased will be posted elsewhere. Rapid7 provides our best recommendations based on the information available at the time. In most cases, validating the information being sold before purchasing is beneficial. If found to be legitimate, your organization can take the appropriate action to mitigate the risk.

Dark web request services will include purchase items, subject to the fair use policy, directly related to an alert within the customer's account dashboard only. Each request comprises the basic item cost as presented in the source and the analyst labor costs associated with the transaction. For items with a base cost over $100, Rapid7 reserves the right to deny or approve the transaction individually. In these situations, additional credits may be required to initiate the transaction.

For more details about initiating this process, please refer to the Dark Web Purchase Guide.

APPENDIX G

Rapid7 MDR Custom Monitoring

MDR Custom Monitoring is an add-on to our MDR service that allows for the support of custom event sources beyond our standard supported integrations, enabling organizations to bring in unique or proprietary log data for security monitoring by our SOC who will monitor, triage, and respond to alerts generated from customer-defined sources.

Rapid7 MDR Custom Monitoring offering includes support for select non standard event sources, with tailored detection development and 24/7 SOC monitoring and triage into the workflow.

Rapid7 will work with the customer to understand their desired security use cases for alerting inclusive of SOC monitoring/triage. Once agreed by both parties, Rapid7 will configure the IDR platform to allow for event source ingestions and parsing, and relevant detections will be created. Alert tuning and thresholds will occur as part of our standard detection lifecycle process. Once configured, our SOC will treat alerts from these sources with the same triage and escalation process as standard sources.

Customer event sources must generate logs in a parsable format and can be onboarded through IDR's custom log ingestion pipeline.

MDR Custom Monitoring Deployment:

As part of the MDR Custom Monitoring service, tailored detection and monitoring capabilities are delivered through a collaborative process involving multiple specialized teams:

- Threat Intelligence and Detection Engineering (TIDE) team will lead the discussion with the customer on their desired security use cases and objectives to ensure actionable alerts are created that the SOC can triage.
- Professional Services (PS) is responsible for the one-time, initial configuration of the IDR platform for event source ingestion and parsing.
- Once the event source is integrated, the TIDE team develops custom detections. These detections are designed based on the customer's specific monitoring objectives and aligned with the visibility provided by the ingested log data.
- To ensure the SOC can effectively monitor and respond to these custom detections, they must undergo the standard TIDE detection development and operationalization process. This includes validation, tuning, deployment, and lifecycle management, consistent with the approach used for all first-party and third-party content in our existing detection library.

This structured process ensures custom detections are not only aligned with customer-specific needs but also meet the same quality, efficacy, and supportability standards as all MDR-managed content.