

# Scope of Service

## Rapid7 Managed Threat Complete (MTC) Essential

Rapid7's MTC is a single, integrated service that allows you to prepare for, detect, and respond to threats in your environment. MTC is delivered as a collaboration between Rapid7 and your team ("you", "customer", "your organization", "your environment") to accelerate your proactive, responsive, and strategic security maturity and extend your security operations by providing customized security guidance and hands-on 24x7x365 monitoring, threat hunting, incident response, and exposure management.

This Scope of Service will define the service delivery experience for MTC Essential.

## MTC Team

The MTC team is composed of a Customer Advisor, a Security Operations Center ("SOC") Tactical Operations team, SOC Pod, the Rapid7 Incident Response team, a Product Security Consultant, and an Advisory Security Consultant.

### Customer Advisor

As an MTC Essential customer you will be assigned a resource from a pool of Customer Advisors ("CA"). These resources will work with your team as a strategic security partner—from initial technology deployment through incident response and ongoing security consultation—to shepherd your organization's security maturity. For any Vulnerability or InsightConnect questions, your CA team would direct you to opening a support ticket. You will interface with the MTC delivery team through the Customer Portal.

Throughout your MTC service term, a 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, a CA will work closely with Rapid7's MDR SOC team to understand and convey information relevant to any investigations and incidents.

### 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 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.

### Product Security Consultant

Rapid7's Product Security Consultants are field experts with years of security experience, helping you extract the maximum value from your MTC solutions. Our deployment services are tailored by the Product Security Consultant to operationalize your security program, augmenting your deployment with product configurations, process automation, and reporting workflows. Working directly with your team and your current tools, we help you align Rapid7 products with industry best practices.

## Advisory Security Consultant

Rapid7's Advisory Security Consultants have the experience to assist you in making your security programs relevant, actionable, and sustainable specific to your organization's incident detection & response and vulnerability management processes. During the onboarding phase, Rapid7 Advisory Security Consultants will quickly assess what's working, what isn't, and what can be improved. We help you optimize and get the most out of your existing security investments, maximizing the impact of your people, processes, and technology. You'll have prioritized, actionable, and data-driven insights, with a step-by-step guide to strengthen your security posture.

## Customer Advisor Engagement

A CA team will be available to answer any questions about your MDR service, and advise you toward advancing your security maturity. They 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.

As an MTC Essential customer you are able to request ad-hoc meetings with a CA virtually. This is done via the Customer Portal.

## Inquiry Response Times

Below are response times to inquiries from your team:

Response Trigger	Time to Action	Action
<b>Inbound Urgent Request</b>	2 hours	Acknowledge an urgent request from the customer's team made via the Customer Portal or Customer Advisor Hotline. Urgency is based on the discretion of the MTC delivery team. If an incident reported by you is confirmed by Rapid7, the incident response process will be initiated (see <a href="#">Incident Response</a> ).
<b>Inbound Non-urgent Request</b>	24 hours	Respond to a non-urgent request from the customer's team made via the Customer Portal. Urgency is based on the discretion of the MTC delivery team.

## Service Deliverables

MTC service reports and deliverables are provided to customers during their MTC service. These include:

Deliverable	Description
<b>IR Planning Workshop</b>	During onboarding, you will attend an on demand webinar that will help your team to build an Incident Response Plan and Runbook for engaging with the Rapid7 MTC service. This will provide you with the foundational tools and framework to appropriately respond in the event an incident was discovered and addressed by Rapid7's MTC team.
<b>Security Posture Assessment Report</b>	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 <a href="#">Incident Response</a> for additional details).
<b>Incident Response Reports</b>	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.

<b>Monthly MTC Service Reports</b>	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
------------------------------------	--

You may access additional reports in the VM console. Rapid7 continuously updates these reports to match the cadence of the evolving threat landscape.

## Technology Instance Set-Up

### InsightIDR Instance

Your MTC service includes a single instance of InsightIDR (IDR) for your entire organization. IDR is the primary solution used by Rapid7's team to perform Managed Detection and Response (MDR). All log sources will be ingested into this single instance. All of your security team 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 MTC to multiple internal organizations as separate instances to provide separate visibility and reporting across these logically separated organizations or business units. Details and costs regarding the service delivery options for additional organizations can be discussed with your account team.

### InsightVM Instance

Your MTC service includes a single instance of InsightVM (IVM) deployed and available for use by your entire organization. Rapid7 will host a console enabling your team to use all generally available features and functionalities of the instance available through the User Interface (UI) such as: dashboards, scan scheduling, and reporting.

### InsightConnect Instance

Your MTC service includes InsightConnect (ICON) to enable the integrations and automations necessary to deliver the Active Response related services via Response Actions. This includes standing up an Orchestrator, as well as configuring and deploying select Response Action snippets.

Customers are entitled to unlimited use of InsightConnect for its broader automation capabilities, such as automating responses and handling alerts triggered from IDR, as well as automations to address IVM discovered vulnerabilities. This further usage, is outside the scope of the MTC onboarding but included in the MTC subscription.

## Managed Detection and Response (MDR) In-Scope Environment

The 'in-scope environment' refers to the assets (and supporting infrastructure) you have licensed for the MDR element of your MTC service. 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.

## InsightIDR 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 UBA 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 UBA 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 UBA and 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.

Rapid7 MDR leverages InsightIDR event sources as described below:

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

### 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.

### Detection Rules

InsightIDR detection rules generate investigations 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

<sup>1</sup> Alerts generated by these event sources are reviewed by either your organization or the MDR SOC, per the 'responsibility' guidelines described in the 'Detection Rules' section below.  
v04102024

of a non-customer authored detection including, but not limited to responsibility, 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	Responsibility
<b>User Behavior Analytics (UBA)</b>	A detection library that includes: <ul style="list-style-type: none"> <li>• UBA activity: InsightIDR creates a baseline of normal user activity within your environment and generates investigations when there is a deviation.</li> <li>• Custom Alerts: Detection rules written by your organization.</li> <li>• Community Threats: Detection rules powered by community-managed threat intelligence feeds.</li> <li>• Third Party Alerts: Alerts generated by third-party security vendors.</li> </ul>	Your organization is responsible for configuring and tuning these detection rules, and for handling any resulting investigations. <b>Should you identify activity in these investigations that you believe is suspicious, 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 <a href="#">Incident Response</a> section.</b>
<b>Attacker Behavior Analytics (ABA)</b>	InsightIDR applies behavioral analytics and curated threat intelligence to generate investigations, built from our experience and understanding of attacker tools, tactics, procedures, and methodologies.	Each ABA detection rule has a 'responsibility' attribute which determines whether the detection rule (and resulting investigations) are the responsibility of your organization or Rapid7 MDR.  Rapid7 is responsible for configuring, tuning, and handling any resulting investigations for detection rules marked as 'Rapid7 Managed'. See <a href="#">24x7x365 Security Monitoring</a> for details on how Rapid7 handles these alerts.  Your organization is responsible for configuring, tuning, and handling any resulting investigations for detection rules marked as 'Your Organization' <sup>3</sup> .

### Managed Cyber Risk In-Scope Environment

Routine vulnerability scanning and reporting will be conducted by Rapid7 and reports will be made available as part of MTC. The primary in-scope environment is the same as the above-described MTC Managed Detection & Response in-scope environment. In addition to the managed scanning & reporting, you are permitted to use the solution to perform unlimited vulnerability scanning on all assets owned by your organization.

You have access to unlimited scanning of all assets owned by your organization, including those that are out of scope for MDR. Additional internal scan engines are available for your team to deploy in order to include scanning of your internal, out-of-scope devices.

## Technology Deployment Overview

Deployment is designed to accelerate the technical implementation of MTC in your environment. For existing customers with some or all of the MTC components already implemented, Rapid7 will review all current technology deployments with the goal of ensuring the health of the implementation and suitability of the implementation to support the managed service.

### Foundational Configuration

MTC deployment includes an overview of the Insight Platform and configuration in line with Rapid7 best practices.

Foundational Configuration includes:

- Review and implementation of recommended Multi-Factor Authentication (MFA) and Single Sign-On (SSO) configuration (as applicable)
- Review of Insight Platform best practices for administration and auditing
- Establishing InsightAgent deployment strategy
- Establishing Platform authentication for the hosted InsightVM console

### Component Configuration

MTC deployment services consist of initial configuration of IDR to support the MDR service elements, establishing on-prem network scan infrastructure for IVM, and deploying the on-prem component of ICON. Together, these components enable your security team to leverage the MTC suite of services.

Some configuration activities are largely administrative; therefore they take place in partnership with your security team to enable them to confidently replicate the configurations across your organization. This also ensures your team is empowered to expand coverage of the MTC components beyond the baseline required for delivery of the MDR and InsightVM services.

As part of the MTC deployment, the Rapid7 deployment team will review any existing InsightIDR, InsightVM, and InsightConnect configurations or help deploy any absent technology components to ensure they are prepared to support the MTC services.

Specific Activities during MTC Component Deployment:

- Overview of the MDR service including Rapid7 and customer responsibilities
- Tuning MDR alerting and configurations
- Discuss placement of InsightIDR Collectors and InsightVM Scan Engines
- Discuss InsightAgent's role in InsightIDR, InsightVM, and InsightConnect
- Deploy initial InsightIDR Collector
- Discuss recommended IDR event sources and determine collection mechanisms
- Establish ingestion of foundational event sources
- Discuss and establish additional event sources leveraged by MDR
- Review network sensor and deception technologies
- Review MDR settings, customization, and operational best practices
- Review MDR best-practice workflows and investigation tooling
- Deploy the InsightConnect Orchestrator
- Establish baseline InsightVM configuration supporting managed service reporting

The deployment services team will provide advice on but will not directly configure or guarantee the following:

- Organization-wide deployment of the InsightAgent
- SSO if the SSO administrator is not present on the deployment call with all change management steps completed
- Configuration of non-Rapid7 appliances and tools including security controls

- Configuration of unsupported event sources
- Custom event sources
- Configuration of more than three instances of the same event source
- Custom integrations and automation workflows
- Debugging of network connectivity when using InsightVM scan engines across network segment boundaries
- Customized reporting, asset group, and tag configurations within InsightVM

## Activating Your MDR Service

Rapid7 can begin monitoring your environment (See [24x7x365 Security Monitoring](#) below) as soon as your engagement begins. When a minimum of one (1) Insight Agent is deployed, the MDR team will conduct a service enablement session, verify agent deployment, and will then begin monitoring your environment.

## MTC Customer Expectations

All deployment activities are dependent on Customer completion of all prerequisite steps prior to the deployment engagement. Some configuration items with missing prerequisites will be covered on a theoretical basis only and self-service resources for implementation will be provided.

**Note:** Deployment is limited to the installation of Rapid7 products and does not include prerequisites such as provisioning physical or virtual resources/servers.

## D&R Program Advisory

### IR Planning Workshop

All MTC customers are invited to join an on demand Customer Advisor-led webinar workshop. The workshop is intended to assist in the ideation and review of IR Plan and Runbook documents provided at the onset of the service initiation. The goal of the workshop is to educate and ideate on improvements that customers in general can make over the course of 6-12 months within their IR Programs.

The scope of the workshop includes:

- Review of the provided IR Planning and Runbook documents
- Advisory Security Consulting led session on each area, the importance of each section, and how it governs Incident Response elements
- How to continue to evolve general Incident Response process

Outcomes of the workshop include:

- A framework for IR governance
- A framework to define formal IR processes
- A roadmap of activities to self evolve people & process internally
- A better understanding of how to integrate and action MDR notifications and incident reports

## Threat Detection

Rapid7 leverages compromise 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).

In addition, you will receive a compromise assessment report as described in [Service Deliverables](#).

### 24x7x365 Security Monitoring

InsightIDR investigations are created when a detection rule is triggered based on activity in your environment. The 'responsibility' attribute of an investigation is determined based on the 'responsibility' attribute of the detection rule that generated the investigation (see [Detection Rules](#) for details).

Rapid7 will fully investigate all InsightIDR investigations with the responsibility of '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 investigations 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:

Investigation Priority	Time to Begin Investigation
Critical	15 minutes
High	1 hour
Medium	12 hours
Low	48 hours

## 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.

## 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](#)).

## Incident Response

If an eligible incident is discovered by you or Rapid7 within your in-scope environment at any time during your MTC 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

Rapid7 determines the severity of an incident based on 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 and criticality 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 criticality of in-scope assets or users, evidence of data exfiltration, etc.

Incident Severity	Incident Definition	Example Incident(s)
Low	A non-targeted, low-impact threat involving a small number of systems or users which is already contained.	A non-targeted phishing attack with evidence that the recipient(s) provided credentials.
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 only partially 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.

Rapid7 MDR reserves the right to lead all high severity incident investigations. Should Customer contract a third party for digital forensics and incident response support during a high severity incident, Rapid7 will facilitate a handover meeting with the third party and the customer. The handover process will include providing the third party with the complete findings from Rapid7's investigation, acquired forensic artifacts, all written status updates, and provisioning their access to the Insight platform. At the conclusion of the handover, Rapid7's MDR service will transition back into standard monitoring and Rapid7 will no longer be facilitating the investigation for the applicable high severity incident investigation.

## 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.



Phase	Activity	Definition	Severity
<b>Incident Notification</b>	<b>Incident Notification - Email</b>	Initial notification immediately via a Customer Portal case and e-mail notification to your designated contacts.	All
	<b>Incident Notification - Phone Call</b>	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, High
	<b>Incident Kickoff Call</b>	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
<b>Incident Investigation</b>	<b>Forensic Analysis</b>	Investigation of incident scope, impact, and root cause using data sent to InsightIDR, data generated by the	All

<b>and Analysis</b>		Insight Agent, and other forensic analysis techniques will begin immediately.	
	<b>Incident Updates</b>	For incidents that are in progress for more 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.	High
<b>Incident Remediation</b>	<b>Containment and Eradication</b>	During incident response, Rapid7 will communicate recommended remediation actions to contain and eradicate the threat in your environment. Rapid7's approach includes: <ul style="list-style-type: none"> <li>Fully scoping the incident before recommending remediation activities</li> <li>Recommendations for removing all attacker remote access capabilities, restoring prioritized business processes, and securing compromised user accounts</li> </ul> <p>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 <a href="#">Active Response section</a>.</p>	All
<b>Post-Incident Activities</b>	<b>Incident Response Report</b>	An Incident report as described in <a href="#">Service Deliverables</a> . This report will be delivered to you within 10 business days of the conclusion of the incident investigation.	All
	<b>Incident Debrief</b>	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
	<b>Corrective Action Tracking</b>	Your Customer 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

**Customer Advisor:** A Customer Advisor (or another member of Rapid7's Customer 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 you are 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.

## Cyber Risk Management

Rapid7's Cyber Risk Management service leverages our InsightVM technology and our security expertise to programmatically deliver the people and processes our customers need to effectively and rapidly manage and reduce their security risk.

The service provides a managed, scalable, and efficient way to collect your vulnerability data, turn it into answers, and minimize risk. The platform incorporates the latest analytics and endpoint technology to discover vulnerabilities in a real-time view, pinpoint their location, prioritize them for your business, facilitate collaboration with other teams, and confirm your exposure has been reduced.

The Rapid7 InsightAgent, deployed and configured in the customer's environment during the Onboarding stage, in collaboration with your deployment team, automatically collects data from all your in-scope endpoints, including those from remote workers and sensitive assets that cannot be actively scanned, or that rarely join the corporate network. Rapid7 updates the capability and content of the Insight Agent frequently, as necessary, to enable identification of emerging vulnerabilities. Updates may occur as frequently as daily. Updates to the InsightAgent take place in the background with no customer intervention needed.

Scanning of in-scope customer assets runs continuously and is also triggered by changes detected on the asset via the InsightAgent. This means you are continuously updated to evolving vulnerabilities and fresh data.

Scanning of additional, internal, out-of-scope, assets is accomplished via customer-deployed Rapid7's InsightVM scan engines and customer-directed scan scheduling.

Scanning of external assets is accomplished via Rapid7's hosted external scan engines and is inclusive of both those that are in-scope and out-of-scope.

All scan scheduling is customer-directed.

Customers are at liberty to deploy additional internal scan engines as needed and will be responsible to pair those engines to their existing hosted console via opening a support ticket with Rapid7.

Customers view and interact with fresh vulnerability data through the InsightVM hosted console. Rapid7 hosts and manages the console functionality on behalf of the customer. The console provides the customer with frequently updated data and is interactive by nature. You can easily create custom, tailored cards and full views for anyone—from sysadmins to CISOs—and query each card with simple language to track progress of your security program.

Via the console, the granular, 1-1000 Real Risk score takes into account CVSS scores, malware exposure, exploit exposure and ease of use, and vulnerability age. This makes it simpler—and more precise than CVSS alone—to prioritize vulnerabilities for remediation. Rapid7 Project Sonar data and threat feeds translate to dashboards within the console, so you can understand which external network doors you're missing and which vulnerabilities attackers are actively exploiting. In addition, Rapid7's Emergent Threat Response team continuously monitors for emerging threats and tags affected customer endpoints for prioritized visibility.

The Rapid7 hosted console allows for the following customer technology integrations: Azure, AWS, DHCP, ServiceNow & JIRA.

Once the most critical vulnerabilities are brought to the surface, you can assign and track remediation duties in real time with remediation workflows and IT ticketing integrations with solutions like Atlassian's JIRA and ServiceNow.

MTC customers are entitled to leverage the included InsightConnect functionality to design and automate vulnerability remediation workflows.

Customers will have access to several reports via the VMconsole. Rapid7 will configure and schedule the reports to automatically generate, including by not limited to:

- Top 10 Assets by Vulnerability Risk
- Top 25 Remediations by Risk
- Vulnerability Risk Scorecard

The VM Platform Report

- Executive Summary Report

Customers will also have direct access to the full report library and the ability to create sql queries based on the data model.

## Customer Responsibilities

Ensure continuous network connectivity between the on-premises Rapid7 technology and the Rapid7 hosted platform.

Deploy InsightAgent (included) and scan engines (optional) and remedy customer-environment dependencies to enable scanning operations and communication.

Ensure ongoing availability of customer-site deployed technology including Insight Collector (optional), scan engines (optional), including the continuous ability to report to Rapid7 infrastructure.

## Joint Requirements For Ensuring Success

To ensure your organization realizes the full value of Rapid7 MTC, 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 MTC technology stack (InsightIDR, Insight Agent) and in conjunction with the event sources configured in InsightIDR from your environment
2	Provide a deployment team to proactively guide you through the steps to get set up, including product deployments and service launch
3	Provide access to a security advisor (“Customer 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 Customer 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. The Insight Agent deployment for InsightVM is limited to MTC licensed assets.
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)
3c	Complete & return prerequisite data gathering questionnaires and materials in a timely manner
4	Deploy Insight Agents to all workstation, desktop, and server assets in the in-scope environment(s) and connect all Insight Agents to InsightIDR <ul style="list-style-type: none"><li>Assets without the Insight Agent deployed will not be fully supported by the MDR service</li><li>You must deploy Insight Agents to at least 80% of existing assets in the in-scope environment in order for Rapid7 to perform Security Posture Assessment</li></ul>
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: <ul style="list-style-type: none"><li>Collect the event sources described in 6 and 7</li><li>Proxy connections from ‘on premise’ Insight Agents to the Insight Platform</li></ul>
6	Connect all available recommended data sources to InsightIDR (see <a href="#">Event Sources</a> ) for each in-scope environment and ensure availability and connectivity to Rapid7 infrastructure for all MDR technology and

	event sources
<b>6a</b>	Deploy Insight network sensors in your environment to analyze and log network traffic data
<b>6b</b>	Set up honey users, honey files and honeypots
<b>7</b>	Connect any other security-relevant event sources to InsightIDR <i>Note: All connected event sources may be leveraged for investigation, threat hunting and incident response purposes.</i>
<b>8</b>	Notify Rapid7 of any personnel, technology, event source, or point of contact changes or modifications
<b>9</b>	Configure the InsightIDR instance in accordance with the recommendations from your deployment team and Customer Advisor
<b>10</b>	Review investigations that are not in-scope for the MDR service as these investigations will not be reviewed by the MDR service. See the <a href="#">Detection Rules</a> section for details on investigation responsibility.
<b>11</b>	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.
<b>12</b>	Partner with Rapid7 during and after an incident response engagement, as described in the incident response <a href="#">Customer Responsibilities</a> 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 Customer 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 Requirements](#)

### Other Supported Agents (CrowdStrike Falcon, SentinelOne, Carbon Black Cloud, Microsoft Defender) –

- 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, the customer is 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 the customer's security credentials between third party apps:
3a	If using <b>LDAP &amp; Active Directory</b> for Active Response user containment, connect it to InsightConnect as described <a href="#">here</a> .
3b	If using <b>Carbon Black Cloud</b> for Active Response asset containment, connect it to InsightConnect as described on the documentation tab <a href="#">here</a> . Note: multi-domain is not supported for Carbon Black Cloud.
3c	If using <b>Microsoft Defender</b> for Active Response asset containment, connect it to InsightConnect as described on the documentation tab <a href="#">here</a> or using the setup guide <a href="#">here</a> .
3c	If using <b>SentinelOne</b> for Active Response asset containment, connect it to InsightConnect as described on the documentation tab <a href="#">here</a> .
3d	If using <b>CrowdStrike Falcon</b> for Active Response asset containment, connect it to InsightConnect as described on the documentation tab <a href="#">here</a> .
4	If using the Insight Agent for Active Response, enable <b>Windows Firewall</b> on all endpoints in accordance with the <a href="#">Insight Agent Requirements</a>
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 the customer.
6	All unquarantine actions must be completed by the customer.

## Active Response Service Responsibilities

Active Response service will be responsible for the following:

Responsibilities and Requirements	
1	Deliver a 24x7 response service.
2	Provide the customer with a license of InsightConnect for the sole purpose of enabling the Active Response service. Note: with MTC the customer also receives a license for InsightConnect Insight Automation that can be used by the customer to enable security automations that leverage InsightIDR or InsightVM.
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 the customer with requests, and continuously notify the customer, for any proposed action or change in response status.
6	Active Response service will update the customer to status changes via the InsightIDR Investigation Timeline and Audit Log.
7	All Active Response actions will be taken immediately.
8	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 the customer's 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 the customer's 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 the customer's 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 Rapid7SOC 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

- 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.
- MDR Elite customers agree not to install any additional workflows from the InsightConnect Extensions Library. Unless the customer has a separate InsightConnect license.
- If a customer 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. The customer (of MTC) has the option to leverage the InsightConnect Insight Automation license to set up their own workflows to extend their own capabilities of response using it as a general purpose Security Orchestration Automation and Response (SOAR) solution.

## 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.

## Additional Terms

This Scope of Services is governed by the Rapid7 terms available at <https://www.rapid7.com/legal/terms> unless the parties have a fully executed 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 Managed Threat Complete (MTC) Essential 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.

# APPENDIX A

## MTC Responsibilities Matrix

	Rapid7	Main POC	Security & IT	C-Suite
<b>Initiation Phase</b>				
Complete Solution Alignment Survey		✓	✓	
Define internal remediation escalation path(s) for MDR reporting		✓		
Set up customer in InsightIDR	✓	✓		
Set up customer in InsightVM	✓	✓		
Set up customer with Active Response (InsightConnect)	✓	✓		
Enable customer in customer's services portal	✓			
<b>Deployment &amp; Onboarding Phase</b>				
Onboarding Kick Off Video	✓	✓		
Download and install Collectors		✓		
Deploy Insight Agent to all servers and workstations		✓	✓	
Deploy Insight Network Sensor(s)		✓	✓	
Install Orchestrator and Active Response workflows	✓	✓	✓	
Configure event sources	✓	✓		
Ensure collector/agent network connectivity to InsightPlatform		✓		
Deploy InsightVM Scan Engine(s)	✓	✓		
Deploy and Manage InsightVM Console	✓			
IR Planning Workshop	✓	✓	✓	
InsightIDR walkthrough	✓	✓		
<b>Service Delivery Phase</b>				
Service Delivery Kickoff call	✓	✓		
Security Posture Assessment	✓			
<b>Real-time Security Monitoring</b>				
Investigate "Rapid7 Managed" responsibility investigations as described in the <a href="#">24x7x365 Security Monitoring</a> .	✓			
Request additional information ("RFIs") from customers as needed to complete "Rapid7 Managed" responsibility investigations.	✓			
Respond to RFIs from Rapid7 with the information requested to complete "Rapid7 Managed" responsibility investigations.		✓		

Investigate "Customer" responsibility investigations		✓	✓	
Notify Rapid7 of any "Customer" responsibility investigations that may be indicative of malicious activity so that Rapid7 can initiate incident response.		✓		
Detection Rule Tuning ("Rapid7 Managed" responsibility detection rules)	✓			
Detection Rule Tuning ("Customer" responsibility detection rules)		✓		
<b>Threat Hunting</b>				
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	✓			
<b>Threat Intelligence</b>				
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	✓			
<b>Incident Response</b>				
Incident identification and notification	✓			
Incident investigation	✓	✓		
Recommend remediation actions (containment and eradication)	✓			
Perform containment actions (assets and users)				
<i>Without Active Response set up</i>		✓	✓	
<i>With Active Response set up</i>	✓			
Perform containment actions (other)		✓	✓	
Perform eradication and recovery actions		✓	✓	
Incident report creation and delivery	✓			
Recommend corrective actions	✓			
Perform corrective actions		✓	✓	
<b>Risk Management</b>				
InsightVM console deployment and maintenance	✓			
Configure sites	✓	✓	✓	
Initial scheduled scans	✓			
Scan	✓	✓	✓	
Monitor stability	✓			
Run reports	✓	✓	✓	

## APPENDIX B

### Technology-Dependent Service Limitations

Some aspects of the Rapid7 MTC 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
<b>Attacker Behavior Analytics</b>	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.
<b>Manual Human Threat Hunting</b>	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.
<b>Alert validation and IR Investigations</b>	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.
<b>Local Authentications and Group Membership Changes</b>	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 NGAV Agent Technology

Rapid7's Endpoint Prevention with NGAV as an 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 InsightAgent - the same software that runs silently on your assets and already powers several Rapid7 products like InsightIDR and InsightVM.

Endpoint Prevention implements its capabilities by way of 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 is composed of several prevention engines designed to detect 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.

**Note:** While the Insight Agent broadly supports installations on a range of Windows, macOS, and Linux operating systems, only select Windows operating systems are eligible for use with Endpoint Prevention. See the operating system support article for a list of Windows versions that are eligible for Endpoint Prevention [here](#). Due to a Windows requirement that only allows one antivirus solution to be running on the asset at a time, Endpoint Prevention

*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 NGAV Agent Technology 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 component - 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](#)) and endpoints must be included in the "Default" group (see [Prevention Groups](#)).

## Exclusions

If you want Endpoint Prevention to ignore certain 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 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 also means 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. If you have questions or would like consultation on implementing a custom exclusion, consult with your Customer Advisor.

More details on exclusions and exclusion types can be found in the product documentation [here](#).

## Prevention Group

Endpoint 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. This group uses the immutable default prevention policy configured by Rapid7 to provide a baseline level of protection.

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 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 agents within that group for threats.

You have full configuration control over the policies attached to your custom prevention groups. An exception to this is the default prevention group and the default prevention policy attached to it. This policy is immutable and its configuration is maintained solely by Rapid7.

## 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.

Endpoint Prevention supports these priority levels:

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

MDR will provide [24x7x365 security monitoring](#), investigation, response for all "MDR Responsibility" NGAV alerts at all priority levels within the default prevention group.

## Antivirus Health Statuses

There are 4 possible health statuses for your Insight Agents:

- **Good** - Antivirus is running successfully.
  - This is the desired status and indicates that the Endpoint Prevention component 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 component on the Insight Agent is functioning, the agent has encountered errors that may impact its performance.
- **Not Monitored** - Endpoint Prevention is installed on this agent, but its prevention policy does not have the On-Access Scanning 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 Endpoint Prevention component, 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 Endpoint Prevention will have this status. Agents on assets running eligible operating systems can also have this status if a connectivity issue is preventing the Insight Agent from retrieving the Endpoint Prevention component 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 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 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 you're ready to switch 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. All such events will be logged and sent to InsightIDR for analysis and further action, if necessary.

## 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](#).

## Managed NGAV Service Deliverables

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

Deliverable	Description
<b>Incident Response Reports</b>	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
<b>Monthly Service Reports</b>	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 Agent Responsibilities Matrix

	Rapid7	Main POC	Security & IT	C-Suite
<b>Deployment &amp; Onboarding Phase</b>				
<b>Complete Technical Preparations</b> (see <a href="#">"Managed NGAV" Deployment Handbook</a> )		✓		
<b>Deployment Testing &amp; Support</b>	✓			
<b>Customer Deployment</b>			✓	
<b>Service Delivery Phase</b>				
<b>Default Exclusion Policy Configuration</b>	✓			
<b>Custom Exclusion Policy Configuration</b>		✓		
<b>Default Prevention Group Configuration</b>	✓	✓		
<b>Custom Prevention Group Configuration</b>		✓		
<b>Default Prevention Policy</b>	✓			
<b>Custom Prevention Policy</b>		✓		
<b>Activation Mode Configuration</b>		✓		
<b>Real-time Security Monitoring</b>				
Investigate "Rapid7 Managed" responsibility alerts as described in the <a href="#">24x7x365 Security Monitoring</a>	✓			
Request additional information ("RFIs") from customers as needed to complete "Rapid7 Managed" responsibility investigations.	✓			
Respond to RFIs from Rapid7 with the information requested to complete "Rapid7 Managed" responsibility investigations.		✓		

## APPENDIX D

### 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 Customer Advisor in advance of the test. Your Customer 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 Customer 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 E**

### **Rapid7 Managed Digital Risk Protection (MDRP)**

Rapid7's MDRP is an add-on service offering for MDR/MTC customers that combines key components of our Threat Command platform and expertise from both our Threat Command and Managed Detection & Response Analysts to protect your critical digital assets and data from external threats, 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.

This Scope of Service will define the service delivery experience for MDRP.

#### **MDRP Team**

In addition to the MDR/MTC team, you will be introduced to the following specialist roles involved in the delivery of your MDRP service, namely: MDRP Onboarding Specialist, Managed Digital Risk Protection Analysts, Threat Command Analysts, the 'Ask-an-Analyst' team, plus our Response team that supports remediation actions such as takedowns and dark web purchases.

#### **MDRP Onboarding Specialist**

The MDRP Onboarding Specialist is responsible for enabling you to understand how the service operates, become familiar with the Threat Command technology, and how to get support and assistance when required. They will perform a basic tuning, help you set up the required integrations with InsightIDR, and start your service. Once the technology is operational and all your initial contextual information has been collated and integrated into your Threat Command instance, you will be transitioned to the Customer Advisor resource pool.

#### **MDRP Analyst**

The primary function of the MDRP Analyst is to review and triage alerts in your Threat Command instance to ensure the alerts you receive are as accurate as we can make them and contain the minimum amount of noise, e.g., false positives. It is important to note that the accuracy of any threat/alert is heavily influenced by the uniqueness and clarity of your brands and the contextual information you provide, so some level of regular tuning and review will be required.

The MDRP Analyst will also leverage your 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. lookalike website, is actively being exploited by an attacker in your environment, the MDRP Analyst will escalate the incident to your MDR/MTC service team for investigation by the Rapid7 MDR SOC. If an active cyber threat is confirmed, you will be notified by your MDR team, as outlined in your MDR/MTC scope of service. The MDRP Analyst will monitor the Threat Command alert queue during standard business hours (CET local time) Monday through Friday, excluding nationally observed holidays.

#### **Threat Command Analyst**

Behind the scenes, Rapid7 Threat Command Analysts are responsible for monitoring and analyzing external and internal 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 pieces

of information, and track down actors that potentially pose a threat to 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 impact on our customers.

**‘Ask an Analyst’ Service Team**

Rapid7’s Threat Command "Ask an Analyst" Service is the primary engagement resource responsible for providing guidance, additional details, and context, recommending remediation steps, executing dark web purchases, or 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 our 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.

Response Trigger	Time to Action	Action
<b>Urgent Intel Request</b>	2 hours	To provide an initial response to an urgent request from the customer’s team made via the Threat Command - ‘Ask an Analyst’ chat or customer portal.
<b>Non-urgent Intel Request</b>	6 hours	To provide an initial response to a non-urgent request from the customer’s team made via the Threat Command - ‘Ask an Analyst’ chat or customer portal.

**Remediation Service Team**

As organizations adopt new digital channels to reach customers, cybercriminals follow suit by impersonating popular brands, promoting scam campaigns, and profiting from unknowing consumers. Our remediation team services external enforcement to take down campaigns that impersonate your brand, infringe on trademarks and copyrights, and threaten customers. Threat Command’s in-house automated Remediation Services can help you expedite takedowns of malicious and harmful web content targeting your brand.

Response Options	Quantity	Description
<b>Takedown Requests</b>	Limited to 20 requests per year	Request that Rapid7 contact a content provider and act on your behalf to remove a threat from the Internet. There are two options available to you: <ul style="list-style-type: none"> <li>- <b>Malicious Domain</b> - we will contact the Domain registrar to request the domain be removed from the web.</li> <li>- <b>Malicious Website</b> - we will contact the hosting provider to request the website be removed from the web.</li> </ul> <p>The success of a takedown 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.</p>
<b>Dark Web Purchases</b>	Limited to 50 per year (not exceeding \$100 each)	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 Command Research Service Team

Rapid7 provides deep-dive investigation services and reports into external cyber threats, including incident response research, 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 Command Research products. Submit an 'Ask an Analyst' ticket if you should require additional work.

## In-Scope Service Components

MDRP is built around our Threat Command platform, which delivers proactive defense by transforming threat intelligence into security actions and actionable alerts.

Threat Command leverages ground-breaking data-mining algorithms and unique cyber reconnaissance capabilities to continuously scan the surface, 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.

MDRP incorporates the following components of Threat Command.

Modules Included	Description
<b>Phishing Protection</b>	
- 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	
<b>Data Leakage</b>	
- Leaked Ransomware Files	Internal or company confidential documents that are exposed publicly typically include users' credential information or company documents that have been published following a ransomware incident.
- Credentials from Botnets	
- Leaked User Credentials	
<b>Attack Indication</b>	
- Credit Cards for Sale	Company credit cards, bot-harvested credentials, or products sold on dark web black markets.
- InfoStealer Data for Sale	

## Service Deliverables

### Monthly Service Review

In line with your existing MDR deliverables, your Customer Advisor will include a summary and overview of your MDRP service status in your planned monthly meeting.

## Technology

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

## Threat Command Instance

Your MDRP subscription will include a single instance of Threat Command for your entire organization. All of your security team users will be assigned to and will have access to all data stored within this single instance, be able to access our expansive Threat Library, make requests to our 'Ask an Analyst' team, initiate takedowns, approve Dark Web purchases, and access any other offering under this Appendix.

Threat Command is Rapid7's Intel solution and monitors thousands of sources across the clear, deep, and dark web to identify threats directly targeting your unique digital footprint, helping you make informed decisions and act quickly on critical threats posing the greatest risk to your business. Use cases supported include dark web monitoring, threat hunting, phishing protection, data/credential leakage, ransomware disclosure monitoring, fraud, and malware detection.

Threat Command supports user-based access controls, so each feature can be restricted per user as required.

## 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.

MDRP leverages both technology platforms to provide your full MDRP services, but you should expect to receive most of your Intelligence reporting, alerts, and guidance within the Threat Command platform. This platform should also be your first choice when you wish to interact with our Threat Command teams, such as making requests to our 'Ask an Analyst' team, submitting a 'Takedown' request, or approving a Dark Web purchase. The 'Ask an Analyst' team can also provide additional guidance and support on getting the most out of your MDRP service and how to best leverage the Threat Command platform.

The MDRP offering does require the configuration and setup of the native InsightIDR to Threat Command integration to allow seamless investigation from the MDR SOC. Enabling integration will also allow you to see all your Threat Command alerts within InsightIDR if you wish. Collaboration with Rapid7's Threat Command teams will remain in the Threat Command platform.

## APPENDIX F

### MTC Essential, Advanced & Ultimate Comparison

MTC customers have the option to purchase MTC Essential, MTC Advanced or MTC Ultimate with the technology, services, and deliverables annotated in the chart below.

	ESSENTIAL	ADVANCED	ULTIMATE
<b>Threat Detection and Response</b>			
<b>24x7x365 SOC Monitoring</b>	✓	✓	✓
<b>SOC and Incident Response (IR) Experts</b>	✓	✓	✓
<b>Forensic Investigations and Incident Reports</b>	✓	✓	✓



Unlimited Incident and Breach Response	✓	✓	✓
Proactive Threat Hunting	✓	✓	✓
Active Response for Remote Containment	✓	✓	✓
Endpoint Detection and Response (EDR)	✓	✓	✓
Network Traffic Detection and Response (NDR)	✓	✓	✓
Deployment and Onboarding Assistance	✓	✓	✓
Complete XDR Detection Coverage	✓	✓	✓
3rd Party Cloud Alert Triage		✓	✓
Next-Gen Antivirus	Add-On	Add-On	Add-On
<b>Ransomware</b>			
Hosted DFIR Framework, Velociraptor			✓
Ransomware Prevention			Coming Soon
<b>Exposure Management</b>			
Unlimited Risk Scanning of Internal and External Networks	✓	✓	✓
Vulnerability Assessment Reports and Scorecards	✓	✓	✓
Targeted Remediation Reports	✓	✓	✓
Scan Configuration and Scheduling Operations			✓
Vulnerability Remediation Prioritization and Guidance			✓
Managed Infrastructure Management	✓	✓	✓
Phishing Protection	Managed DRP Add-On	Managed DRP Add-On	✓
Data and Credential Leakage	Managed DRP Add-On	Managed DRP Add-On	✓
Dark Web Monitoring	Managed DRP Add-On	Managed DRP Add-On	✓
Takedowns and Dark Web Purchases	Managed DRP Add-On	Managed DRP Add-On	✓
<b>Cybersecurity Program Growth</b>			
IR Planning Assistance and Runbooks	✓	✓	✓
Security Posture Assessment	✓	✓	✓
Access to Rapid7 MTC Peer Network	✓	✓	✓
Assigned Customer Advisor		✓	✓
Monthly Security Posture Review Meetings		✓	✓

<b>Executive Trend Report and Readout</b>		✓	✓
<b>Critical Security Controls Assessment</b>		✓	✓
<b>D&amp;R Readiness Assessment</b>		✓	✓
<b>Proactive Remediation Coaching</b>			✓
<b>Data and Technology</b>			
<b>Full Access to the Underlying XDR Platform</b>	✓	✓	✓
<b>Unlimited VRM Tooling, InsightVM</b>	✓	✓	✓
<b>Unlimited SOAR</b>	✓	✓	✓
<b>Unlimited Data Ingestion</b>	✓	✓	✓
<b>13 Months Data Retention</b>	✓	✓	✓