# Scope of Service

## Rapid7 Managed Digital Risk Protection (MDRP)

Rapid7's MDRP is our Threat Intelligence solution and expertise. It protects your critical digital assets and data from external threats and provides guidance and remediation where appropriate.

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

## MDRP Delivery

The MDRP service provides actionable threat intelligence expertise and response support to reduce your digital risk. By focusing on delivering timely insights and effective guidance, the service helps you proactively manage and mitigate external threats targeting your organization.

Key outcomes of the MDRP service include:

- Ongoing validation and triage of alerts
- Contextual threat analysis across the clear, deep, and dark web
- Access to remediation support for impersonation, phishing, and leaked data
- Guidance on using the platform to manage alerts, tune the signal to noise, and generate executive or technical reporting
- Expert-backed recommendations for interpreting threat activity and taking the appropriate action

Rapid7 maintains regular engagement with you to review service activity, deliver key findings, and ensure the MDRP platform is aligned to your organization's digital risk profile.

The MDRP service experience is powered by built-in expertise that delivers continuous threat monitoring, actionable insights, and tailored response guidance.

### MDRP Analysts

The MDRP Analyst plays a key role in maintaining the quality and relevance of alerts within your platform. Their primary responsibility is to review and triage incoming alerts to ensure that what reaches you is as accurate and high-fidelity as possible. It is important to note that the accuracy of any threat/alert is heavily influenced by the uniqueness and clarity of your assets and the contextual information provided. The MDRP Analyst will monitor your alert queue during standard business hours.

### Threat Intelligence Analysts

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

## ‘Ask an Analyst’

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

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

## Remediation Service

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

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

## Threat Intelligence Research

Rapid7 provides deep-dive investigation services and reports into external cyber threats, tactical attack or breach-related research, and strategic trend-based research. We offer an optional catalog that describes our standard menu of research offerings, how research is conducted, typical deliverables, and pricing should you require additional Threat Intelligence Research reports. Additional information can be provided through your MDRP Services Team or ‘Ask an Analyst.’ Customers can purchase additional research reports at an extra cost. When redeeming report credits, customers can choose the type of reports to be redeemed. For more details about Rapid7’s report types, please refer to the Threat Intelligence Research Catalog. For more information on the bundle options, please contact your MDRP services team.

# MDRP Delivery Engagement

Throughout your MDRP service, you will benefit from ongoing engagement designed to help you maximize the value of the platform and stay ahead of emerging threats. Rapid7 offers guidance on how to best leverage the platform, including when and how to escalate issues, gather supporting evidence for remediation, and utilize intelligence related to dark web activity and purchases.

You'll also receive support to optimize alert fidelity by reviewing and tuning noisy alerts, configuring effective notification settings, and scheduling executive and technical reports via user dashboards.

## In-Scope Service Components

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

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

MDRP incorporates the following components:

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

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

# Service Reports

## Bi-Weekly Threat Landscape Report

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

## Semi-Annual Industry Threat Landscape Report

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

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

## Technology

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

### Threat Command Platform

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

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

### Activating Your MDRP Service

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

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

## MDRP Service Process

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

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

However, not all intelligence sources are created equal, and not all digital assets are uniquely identifiable or contextually recognizable. There is always the risk of false positives and contextually incorrect alerts flowing into your view. These numbers can vary greatly depending on the use case, sources, and assets, creating the need for customers to spend time triaging and validating alerts to ensure they represent risks with high confidence of accuracy.

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

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

## Remediation Services

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

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

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

### Remediation Requests

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

Rapid7 handles dozens of remediation requests daily, allowing customers to utilize our dedicated team of experts to gather prerequisites, accelerate requests, and streamline workflows so malicious content can be removed quickly. You are entitled to 50 remediation requests annually. At the end of each contract year, your request allotment will be reset, any unused remediation requests are forfeited and will not be carried over to the following year.

### Advanced Remediation

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

Rapid7 continually develops new partnerships with web registrars, app stores, and social media sites based on new attack vectors, hacker trends, and popular customer requests. If a specific alert source cannot be taken down under a standard remediation request, we may be able to support this as an 'ad-hoc' or 'Advanced Remediation' request, or advise you why it is not possible to remediate. Advanced remediation requests should be submitted as cases via the Rapid7 customer portal. It may cost additional credits to support complex remediation requests, in these cases we will notify you of any additional cost and seek your approval before we proceed.

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

## Dark Web Purchases

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

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

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

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

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

## 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) Ultimate 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.