



Rapid7 Privacy Policy

Last Updated: November 10, 2023

Our quest to accelerate insight for security and technology practitioners requires collecting and processing a significant amount of data. Ensuring your data is used only in a manner consistent with your expectations is a responsibility we take very seriously, and we back the privacy statements below with layers of security to safeguard your data.

Rapid7, we, and us refers to Rapid7, Inc., Rapid7 LLC and any of our corporate affiliates.

This Privacy Policy describes how we collect, use, and disclose information you provide to us, including personal information, by which we mean information that would allow us to determine your identity when you engage with us. For example, we may receive your information when you use our solutions or services or otherwise interact with us (for example, by using our websites or attending our events). In addition, this Privacy Policy covers the information we may collect through our research initiatives.

This Privacy Policy also describes the choices available to you regarding our use of your personal information and how you can access and update this information. We encourage you to read this Privacy Policy carefully when using or providing information to us through our sites, solutions, and services. You understand that by using our sites, solutions, and services, you are accepting our practices as described in this Privacy Policy.

What kinds of information do we collect?

Information you provide directly to us

For example, we collect information you provide in order to access our solutions, use our sites, subscribe to our content, or register for an activity associated with Rapid7. This may include, but is not limited to, your name, email address, telephone number, and mailing address.

If you make a purchase from Rapid7, become one of our vendors, or otherwise establish a relationship with us that involves financial transactions, we collect information about those transactions. This may include, but is not limited to, your credit or debit card information, account and authentication information, tax identifiers, and other billing, delivery, and contact details.

Information we collect to deliver and improve our solutions and services

In order to provide our solutions and services, we must necessarily collect certain information automatically. This also helps us to ensure that our solutions and services are operating correctly. The types of information we collect include:

- Device and network data
- User and system behavior
- Application logs



- Organizational information
- Other relevant machine data

We also collect information about the services and solutions that you use and how you use them, such as how often you access our products and which features you use most frequently. We collect this information to improve our services and solutions and your experience with them. For example, we may use this information to reach out to you if you seem “stuck” on a certain process within the solution, to make our solutions more intuitive, or to enhance the solution’s most popular features.

On our sites, Rapid7 and our third-party partners collect information using cookies and other tracking technologies. Please see [What are cookies and how does Rapid7 use them?](#) below for more information.

Information from third-parties

We receive various types of information from third-parties on some occasions, such as when we jointly offer services or sponsor events. We also collect data from third party security providers and online databases in connection with our research activities that relate to active or historic threats, vulnerabilities, and risks around the world. This can include data like domain names, IP addresses, email accounts, and usernames that are associated with security risks (for example, known compromised accounts and usernames), and we use this information to enhance the security services and solutions we provide to you. Additionally, we also collect certain information from publicly available third party sources, including the dark web, in connection with our research activities, solutions, and services, in particular to identify and help our customers protect against the likes of historic and/or future security threats, vulnerabilities, and risks. This information can include the likes of domain names, IP addresses, email addresses, and usernames and any other data that might be associated with the applicable security risks of issues identified (for example, known compromised accounts and usernames).

How do we use this information?

To deliver, improve, and develop our offerings

We are able to deliver our solutions and services, understand the behavior of attackers, and better help our customers keep their environments safe by using the information we collect above.

In general, we only process our customers' information to deliver our offerings on their behalf. Although we may collect the information listed above, we do not access information that we process on our customer’s behalf, such as user, network, vulnerability, incident, or asset information, unless our customers have requested we do so to investigate issues with our solution or carry out a service.



To communicate with you

We use your information to communicate with you about our solutions, services, features, surveys, newsletters, offers, promotions, and events, and to provide other news or information about Rapid7 and our partners, in accordance with your communications preferences.

We will also use your information to respond to you when you contact us.

To conduct research initiatives

The vast majority of the data we collect through our research initiatives is data that's publicly available. It is collected to educate and enrich the security community, and foster secure adoption of technology. For example, one of our research initiatives uses the metadata from publicly exposed services to identify large-scale misconfigurations and vulnerabilities in consumer, enterprise, and critical infrastructure systems.

How is this information shared?

With our customers and organizations participating in or promoting research

We will share information that we identify about security risks and/or incidents that affect or relate to our customers with those customers. Additionally, information related to the research we conduct may be shared with various research and security organizations, including academic institutions or publications, but only when this information is already freely publicly available and/or non-identifiable. We may also publish this research online on our website or through third party social media sites.

With third-party vendors, consultants, service providers, or other business partners

Some third parties provide services on our behalf and may require access to your information to carry out that work, including billing, customer support, etc. These service providers are authorized to use your information only as necessary to provide the services and solutions in scope and are subject to strict contractual controls to protect the confidentiality and security of your information. If you're a customer of our products or services, our list of subprocessors is available [here](#).

In the case of a merger, sale, financing, or acquisition

We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company. You will subsequently be notified via email and/or via a prominent notice on our sites of any change in ownership or uses of your personal information, as well as any choices you may have regarding your personal information. The recipient of your information will be informed of the need to protect your personal information in accordance with this Privacy Policy.



California Consumer Privacy Act

We do not sell our customers' personal information (as that term is defined in the California Consumer Privacy Act) and we will not sell such personal information without providing any required notice and/or right to opt-out of such sale.

What are cookies and does Rapid7 use them?

What are cookies?

Cookies are small data files that are placed on your computer or mobile device when you visit a website. Cookies are widely used by website owners in order to make their websites work, or to work more efficiently, as well as to provide reporting information.

Cookies set by the website owner (in this case, Rapid7) are called "first party cookies". Cookies set by parties other than the website owner are called "third party cookies". Third party cookies enable third party features or functionality to be provided on or through the website (e.g. like advertising, interactive content and analytics). The parties that set these third party cookies can recognize your computer both when it visits the website in question and also when it visits certain other websites.

How does Rapid7 use them?

We use first party and third party cookies for several reasons. Some cookies are required for technical reasons in order for our Websites to operate, and we refer to these as "strictly necessary" cookies. Other cookies also enable us to track and target the interests of our users to enhance the experience on our Websites. Third parties serve cookies through our Websites for advertising, analytics and other purposes. This is described in more detail below.

To view and control the specific types of first and third party cookies we serve, please visit our [Cookie Preference Centre](#).

How do we respond to legal requests?

We may share personal information with companies, organizations, or individuals outside of Rapid7 if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Protect against harm to the rights, property, or safety of Rapid7, our customers or the public.
- Meet any applicable law, regulation, legal process, or enforceable governmental request.
- Detect, prevent, or otherwise address fraud, security, or technical issues.



If we receive a government or law enforcement request for customer data, we will promptly notify the customer and provide them with a copy of the request, unless we are legally prohibited from doing so. Further, we may challenge government or law enforcement requests for customer data that we consider to be overly broad or unlawful.

How do we operate our global services and solutions?

Rapid7 may share information internally across our parent, subsidiary, and affiliate companies or with third parties for the purposes defined in this policy. Information collected within the European Economic Area (“EEA”) and the UK may, for example, be transferred to countries outside of the EEA and the UK (including the United States of America) for the purposes described in this policy.

When we transfer EEA, Swiss and UK personal information to non-EEA/non-Swiss/non-UK countries, we will implement appropriate safeguards to protect this information. This may include implementing Standard Contractual Clauses (available [here](#) and [here](#)) with our customers when we process personal information on their behalf.

For transfers from the EU, UK and Switzerland to the United States, Rapid7 complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)] as set forth by the U.S. Department of Commerce. For further information, please see our “Data Privacy Framework Self-Certification Notice”

How will we notify you of changes to this policy?

We may update the Rapid7 Privacy Policy to reflect changes to our information practices. If we make any change in how we use your personal information we will take steps to notify you, which may include notifying you by email (sent to the email address specified in your account) or by means of a notice on this site prior to the change becoming effective. If required by applicable data protection laws, we will seek your consent to any material change in how we use your personal information before that change takes effect.

We encourage you to periodically review this page for the latest information on our privacy practices.

How can you manage or delete information about your organization?

Correcting and updating your information

Upon request, Rapid7 will provide you with information about whether we hold any of your personal information. You may access, correct, update or request deletion of your personal



information by emailing us at privacy@rapid7.com. We will respond to your request within a reasonable timeframe and in accordance with applicable data protection laws.

Communications opt-out

We may use your information to send you a newsletter or other marketing communications in accordance with your communication preferences. You may choose to stop receiving our newsletter or marketing communications at any time by following the unsubscribe instructions included in the newsletters or communications. Alternatively, you can opt-out of receiving such newsletters and communications by contacting us at privacy@rapid7.com.

Customer data

If you opt to end your engagement with Rapid7, you have the opportunity to collect and transfer any data that is possible to export. If you request that Rapid7 delete your data, the request will be processed in accordance with applicable law and regulation.

How secure is my data?

We're a security company, so naturally we take data security very seriously. We use appropriate technical and organizational security measures to protect your data against any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the information we process.

How long do you keep data for?

If you are a customer, we will retain your information for as long as your account is active, or as needed to provide you products and/or services. If you wish to cancel your account or request that we no longer use your information to provide our offerings, contact us at privacy@rapid7.com.

In all other cases, we will retain and use your information as necessary for legitimate business reasons, including as needed to comply with our legal obligations, to resolve disputes, and to enforce our agreements. When we have no ongoing legitimate business reason to process your information, we will either delete or anonymise it or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your information and isolate it from any further processing until deletion is possible.

I'm from the European Economic Area/the UK – is there anything else I should know?

Legal basis for processing personal information



If you are an individual in the European Economic Area or the UK, our legal basis for collecting and using your information will depend on the information concerned and the specific context in which we collect it.

However, we will normally collect information from you only where we have your consent to do so, where we need the information to perform a contract with you, or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms. Where we collect and use your information in reliance on our legitimate interests (or those of any third party), it will normally be obvious from the context what those legitimate interests are. For example, in relation to personal data processed in connection with our provision of services and/or research activities, it is in the legitimate interests of Rapid7 and our customers to detect, remediate and protect against a broad variety of cyber threats.

If we are processing information about you on behalf of a customer in the course of providing our services and solutions to them (i.e. as a data processor), then it is our customer's responsibility to determine the legal basis for the processing we conduct on their behalf. If you ask us about information we are processing on behalf of a customer, we will direct you to speak with the relevant customer.

If you have questions about or need further information concerning the legal basis on which we collect and use your information, please contact us using the contact details provided below.

Additional data protection rights

In addition to your rights to access, correct, update and delete your information described above, and your right to opt-out of communications also explained above, you also have the right to object to processing of your information, ask us to restrict processing of your information or to request portability of your information. You can exercise these rights by contacting us using the contact details provided below.

If we have collected and process your information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your information conducted in reliance on lawful processing grounds other than consent.

If you are unhappy with the way we have processed your information, you have the right to complain to a data protection authority. For more information, please contact your local data protection authority. (Contact details for data protection authorities in the European Economic Area are available here.)

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

Data Protection Officer

To contact our Data Protection Officer, please e-mail privacy@rapid7.com.

UK representative



Our representative in the UK is Rapid7 International Limited with a registered office at Riverbank House, 2 Swan Lane, London, England, EC4R 3TT.

EU representative

Our representative in the European Union is Rapid7 Ireland Limited with a registered office at 70 Sir John Rogerson's Quay, Dublin 2, Ireland.

How can you contact Rapid7 with questions or concerns?

Mailing Address:

Rapid7, 120 Causeway Street, Suite 400, Boston, MA 02114

Phone:

1.617.247.1717

Email:

privacy@rapid7.com
