

## FASTNETMON COMMUNITY EDITION

### PRIVACY NOTICE

#### **ABOUT THIS NOTICE**

FastNetMon Ltd is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you in accordance with data protection law in relation to our product "FastNetMon Community Edition". Please read it carefully.

For information about how we use your data in relation to our other products, or otherwise, please see the privacy policy on our website at <https://fastnetmon.com/privacy-policy/>

Data protection law says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

If you have any questions about this notice or how we collect and use personal information about you in relation to FastNetMon Community Edition please contact us.

#### **1. INFORMATION ABOUT US**

- 1.1 We are FastNetMon Ltd. Our registered office is at 20-22 Wenlock Road, London, England, N1 7GU and our registered company number is 10667417.
- 1.2 If you have any questions, you can contact us using the details at <https://fastnetmon.com/contact/>

#### **2. INSTALLATION INFORMATION AND OTHER CORRESPONDENCE**

- 2.1 **FastNetMon Community Edition is only intended for corporate customers.** Individuals (including individuals acting for business purposes) are not permitted to use FastNetMon Community Edition. On that basis, we are entitled to assume that information we collect or receive about FastNetMon Community Edition users is about corporate entities, not individuals acting on their own behalf. On that basis, many of the types of information set out in this privacy notice may not be personal data, but we have included and described them here for clarity. Just because a type of information is described in this privacy notice, that does not mean it will constitute personal data.

2.2 **Installation data.** When you download and install FastNetMon Community Edition we will collect certain information such as:

- 2.2.1 An email address for the installer of our product
- 2.2.2 IPv4 and IPv6 address of the server where installation happens
- 2.2.3 Operating system name
- 2.2.4 Operation system version

2.3 We need certain information to allow you to download and use FastNetMon Community Edition and you must provide this, if you do not, you will not be allowed to download or use the software.

2.4 We will keep and use that information to comply with any legal requirements for us to maintain certain records or carry out certain verifications and/or for our legitimate interests in preventing fraud, dealing with a complaint or enquiry and administering your (or your organisation's) account and any services we offer, as well as to review and improve our offerings, including troubleshooting, data analysis, testing, research, statistical and survey purposes.

2.5 This information is kept indefinitely for the purposes above and in particular as it will contain minimal personal data or no personal data at all. Keeping this information also allows us to deal with any after future enquiries or claims and keep accurate records of our existing installations.

2.6 **Error tracking data.** We may also collect error tracking information, which includes information about the server environment on which our software is installed, and the behaviour of our software. Options for the collection of error tracking information can be disabled through tool settings. We use this information as necessary for our legitimate interests in investigating and correcting malfunctions and issues in our software. We use Sentry (sentry.io) for these purposes, but may replace this or use other tracking tools at our discretion. This information is kept indefinitely to enable us to track our error issues and maintain accurate records of our error corrections and development.

2.7 **Correspondence** (for example by email or via our website) between you and us, will include personal information (such as names and contact details) in that correspondence. This may include enquiries, reviews, follow-up comments or complaints lodged by or against you and disputes with you or your organisation.

2.8 **Social media.** If we engage with you on social media, we may use information you share with us (including your social media handle or profile) or which is available from your account to inform our correspondence with you.

2.9 We will keep and use that information for our legitimate interests in dealing with a complaint or enquiry, as well as to review and improve our offerings, including troubleshooting, data analysis, testing, research, statistical and survey purposes.

2.10 If your information is on social media, it will be retained in accordance with the relevant social media platform's policies. Any other information set out above such as initial enquiries or correspondence which doesn't relate to a customer is kept for up to 10 years after our last contact with you.

### 3. MARKETING AND UPDATES

3.1 We may collect your name and email address in order to send you information about our products and services which you might be interested in. To do this we use the contact details you have provided us (which we may also combine with information we have received about your usage or installation of our software) as necessary for our legitimate interests in marketing to you (by various channels) and maintaining a list of potential customers.

3.2 **You always have the right to "opt out" of receiving our marketing.** You can exercise the right at any time by contacting us. If we send you any marketing emails, we will always provide an unsubscribe option to allow you to opt out of any further marketing emails. If you "opt-out" of our marketing materials you will be added to our suppression list to ensure we do not accidentally send you further marketing. We may still need to contact you for administrative or operational purposes, but we will make sure that those communications don't include direct marketing.

3.3 We never share your name or contact details with third parties for marketing purposes. We may use third party service providers to send out our marketing, but we only allow them to use that information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

3.4 **We retain your details on our marketing list until you "opt-out" at which point we add you to our suppression list.** We keep that suppression list indefinitely to comply with our legal obligations to ensure we don't accidentally send you any more marketing.

### 4. USAGE INFORMATION

4.1 **We may collect information about your use and installation of FastNetMon Community Edition in addition to the "Installation data" set out above.** This option can be turned off upon the installation of the software or by authorised users at any time. While the information we collect is not directly connected to any contact information you may have provided, it is associated with a random unique identifier which is allocated to each installation which we may use in connection with other information to identify the individual installing the software. The information collected generally relates to the configuration of the software you are using, the ways in which you use it, and the system which you are using it on. We use this as necessary for our legitimate interests in administering and improving our software, to ensure it operates effectively and securely, to develop our business and inform our development strategy, and for other administrative purposes. We may also create aggregate statistical data from that information which is not personal information about you.

4.2 Usage data will include the following types of information (although these may be updated from time to time):

- 4.2.1 Instance ID random identifier allocated during installation
- 4.2.2 Current incoming and outgoing bandwidth for IPv4, IPv6 and IPv4+IPv6 traffic
- 4.2.3 Total number of hosts in IPv4 network
- 4.2.4 Number of active IPv4 and IPv6 hosts
- 4.2.5 External IPv4 and IPv6 addresses of machines where FastNetMon is installed
- 4.2.6 Number of observed Netflow/IPFIX flows per second

- 4.2.7 Number of observed sFlow headers per second
- 4.2.8 Version of FastNetMon
- 4.2.9 Enabled plugins (af\_packet, sflow, netflow, xdp)
- 4.2.10 Virtualisation technology
- 4.2.11 Time required for speed calculation
- 4.2.12 Linux kernel version
- 4.2.13 Linux distribution name
- 4.2.14 Linux distribution version
- 4.2.15 CPU flags
- 4.2.16 Feature flags (enabled or disabled) for following features: BGP, InfluxDB, Prometheus

4.3 We keep this usage data indefinitely for the purposes above however in most cases this data will contain minimal personal data or no personal data at all. Keeping this information also allows us to deal with any after future enquiries or claims and keep accurate records of our existing installations.

## 5. ATTACK ANALYTICS INFORMATION

- 5.1 FastNetMon Community Edition allows for copies of attack reports for installations of the software to be sent automatically to us. This option can be turned off after the installation of the software by authorised users through tool settings.
- 5.2 Attack reports include IP addresses of the server where the software is installed, the customer operated IP addresses from which any attack originated for outgoing attacks and the customer operated IP addresses which were targets of incoming attack. They also include the traffic which was used in the attack and other details regarding the attack and the way in which it took place. In particular, this will include the following types of information (although these may be updated from time to time):
  - 5.2.1 Direction of attack (incoming or outgoing)
  - 5.2.2 Amount of packets per second, bits per second and flow per second for all most used protocol types during attack.
  - 5.2.3 IP which is under attack (for incoming attack) or IP which is source of attack (outgoing attacks)
  - 5.2.4 Duration of attack
  - 5.2.5 Traffic sample information
  - 5.2.6 External IPv4 and IPv6 addresses of machine where FastNetMon is installed
  - 5.2.7 The Instance ID random identifier allocated during installation

5.3 Traffic sample information includes the following fields extracted from network traffic before, during and after DDoS attack for the purposes of collecting information which may assist the investigation of such attacks (although these may be updated from time to time):

- 5.3.1 Source and destination MAC addresses
- 5.3.2 Source and destination IPv4 or IPv6 addresses
- 5.3.3 Source and destination ports (UDP, TCP)
- 5.3.4 IP protocol type
- 5.3.5 Packet or flow length
- 5.3.6 Number of packets in flow
- 5.3.7 IP TTL field
- 5.3.8 Sampling rate
- 5.3.9 Source and destination autonomous system numbers
- 5.3.10 Timestamp
- 5.3.11 TCP flags
- 5.3.12 Source and destination interface IDs
- 5.3.13 IP protocol fragmentation flags
- 5.3.14 Network device IP address

5.4 The exact information we receive will depend on the configuration used by the network which has installed our software. It may include information which has been inputted to an internet service by third party users (including form details and free text) including information provided by:

- 5.4.1 your direct customers; and/or
- 5.4.2 remote users who have provided information accessible by us pursuant to this clause, whether directly to you, to your customers, or to any other party.

We are not in control of the information which is received by us. However, we take reasonable steps to filter out any data which is not relevant to analysing the attack, and include in our licences to users of the software obligations for them to correctly configure their installations.

5.5 We use this information as necessary for our legitimate interests in preventing cyber-attacks and fraud, improving, and developing our products and services, and for other administrative purposes.

5.6 In particular, if an IP address is used as part of an attack on a website or network which provides attack or traffic data to us, that IP address may be added to a “blocklist” which we include within our products to more effectively prevent attacks. This may mean that an IP address is blocked from visiting certain websites or networks. If you believe your IP address has been added to a blocklist in error, please contact us.

- 5.7 We may make the aggregated statistical data, information regarding specific attacks, or IP address blocklists available to third parties as part of our business, whether that is directly to users of our software, or other security service providers. We will do this as necessary for our and their legitimate interests in preventing cyber-attacks and fraud and providing our products and services.
- 5.8 We keep these attack reports indefinitely for the purposes above however in most cases this data will contain minimal personal data or no personal data at all. Keeping this information also allows us to deal with any after future enquiries or claims and keep accurate records of our existing installations.

## 6. PROFESSIONAL INFORMATION

- 6.1 If you work for one of our customers or business partners, the information we collect about you may include your contact information, details of your employment and our relationship with you. This information may be collected directly from you, or provided by your organisation. Your organisation should have informed you that your information would be provided to us, and directed you to this policy. We use this as necessary for our legitimate interests in managing our relationship with your organisation. If we have a business relationship with you or your organisation, we may receive information about you from your organisation.
- 6.2 We keep this information for up to seven years after the end of our relationship with your organisation.

## 7. LEGAL CLAIMS

Where we consider there to be a risk that we may need to defend or bring legal claims, we may retain your personal information as necessary for our legitimate interests in ensuring that we can properly bring or defend legal claims. We may also need to share this information with our insurers or legal advisers. How long we keep this information for will depend on the nature of the claim and how long we consider there to be a risk that we will need to defend or bring a claim.

## 8. WHY ELSE DO WE USE YOUR INFORMATION?

- 8.1 **Common uses of your information.** We will only use your personal information when the law allows us to do so. Although in limited circumstances we may use your information because you have specifically consented to it, we generally use your information in the ways set out in this notice because:
  - 8.1.1 we need to perform a contract we have entered into with you.
  - 8.1.2 we need to comply with a legal obligation.
  - 8.1.3 it is necessary for our legitimate interests (or those of a third party) and your interests and rights do not override those interests.
  - 8.1.4 we need to protect your interests (or someone else's interests) or where it is needed in the public interest (although these circumstances are likely to be rare).
- 8.2 **Change of purpose.** We will only use your personal information for the purposes for which we collected it as set out in this notice, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to

use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

## 9. SHARING YOUR INFORMATION

- 9.1 **Attack reports and attack traffic sample.** As noted above, we may make the aggregated statistical data, information regarding specific attacks, or IP address blocklists available to third parties as part of our business. We may be remunerated for this.
- 9.2 **We never sell your data to third parties** other than as set out above. But we may need to share your information with third parties, including third-party service providers and other entities in our group. Third parties are required to respect the security of your personal information and to treat it in accordance with the law.
- 9.3 **Why might we share your personal information with third parties?** We may share your personal information with third parties if we are under a duty to disclose or share your personal information in order to comply with any legal obligation, or in order to enforce or apply our agreements with you, or to protect the rights, property, or safety of us, our customers, or others or where we have another legitimate interest in doing so. This may include exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.
- 9.4 **What about other third parties?** We may share your personal information with other third parties, for example with potential buyers and professional advisers in the context of the possible sale or restructuring of the business where necessary in connection with the purposes which your information was collected for. We may also need to share your personal information with a regulator or to otherwise comply with the law.

## 10. WHERE WE STORE YOUR INFORMATION

- 10.1 We are established in the UK. However, where required to perform our contract with you or for our wider business purposes, the information that we hold about you may be transferred to, and stored at, a destination outside the UK and the EU, including to suppliers based in the United States. It may also be processed by staff operating outside the UK and EU who work for us or for one of our service providers.
- 10.2 We will take all steps reasonably necessary to ensure that your personal information is treated securely and in accordance with this privacy notice.
- 10.3 Some countries or organisations outside of the UK and the EU which we may transfer your information to will have an "adequacy decision" in place, meaning the EU considers them to have an adequate data protection regime in place. These are set out on the European Commission website: [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en).
- 10.4 If we transfer data to countries or organisations outside of the UK and the EU which the EU does not consider to have an adequate data protection regime in place, we will ensure that appropriate safeguards (for example, model clauses approved by the EU or a data protection authority) are put in place where required. To obtain more details of these safeguards, please contact us.

## 11. DATA SECURITY

- 11.1 As well as the measures set out above in relation to sharing of your information, we have put in place appropriate internal security measures to prevent your personal information

from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

11.2 We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where necessary.

## 12. HOW LONG WILL WE KEEP YOUR INFORMATION FOR?

12.1 We have set out above indications of how long we generally keep your information. In some circumstances, it may be necessary to keep your information for longer than that in order to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

12.2 To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

12.3 In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

## 13. YOUR RIGHTS

13.1 Data protection law gives you a number of rights when it comes to personal information we hold about you. The key rights are set out below. More information about your rights can be obtained from the Information Commissioner's Office (ICO). Under certain circumstances, by law you have the right to:

13.1.1 **Be informed** in a clear, transparent and easily understandable way about how we use your personal information and about your rights. This is why we are providing you with the information in this notice. If you require any further information about how we use your personal information, please let us know.

13.1.2 **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

13.1.3 **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

13.1.4 **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it (for instance, we may need to continue using your personal data to comply with our legal obligations). You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

13.1.5 **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your

particular situation which makes you want to object to us using your information on this basis and we do not have a compelling legitimate basis for doing so which overrides your rights, interests and freedoms (for instance, we may need it to defend a legal claim). You also have the right to object where we are processing your personal information for direct marketing purposes.

- 13.1.6 **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- 13.1.7 **Request the transfer** of your personal information to another party where you provided it to us and we are using it based on your consent, or to carry out a contract with you, and we process it using automated means.
- 13.1.8 **Withdraw consent.** In the limited circumstances where we are relying on your consent (as opposed to the other bases set out above) to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another compelling legitimate interest in doing so.
- 13.1.9 **Lodge a complaint.** If you think that we are using your information in a way which breaches data protection law, you have the right to lodge a complaint with your national data protection supervisory authority (if you are in the UK, this will be the ICO).

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal information, withdraw your consent to the processing of your personal information or request that we transfer a copy of your personal information to another party, please contact us.

- 13.2 **No fee usually required.** You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- 13.3 **What we may need from you.** We may need to request specific information from you to help us understand the nature of your request, to confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it. If we request any identification from you for this purpose, it is on the basis that it is necessary to comply with our legal obligations, and we will only keep and use this until your identity has been verified.
- 13.4 **Timescale.** Please consider your request responsibly before submitting it. We will respond to your request as soon as we can. Generally, this will be within one month from when we receive your request but, if the request is going to take longer to deal with, we will let you know.

#### **14. CHANGES TO THIS PRIVACY NOTICE**

Any changes we make to our privacy notice in the future will be posted on this page and may be, where appropriate, notified to you by e-mail or otherwise. Please check back frequently to see any updates or changes to our privacy notice.