



LEGAL · VERSION 1

Security Overview

How Frabs protects the service and its customers' data, in plain language.

VERSION

FRABS_SO_V.1
OCTOBER 2026

APPLIES TO

Customers and their
security teams

GOVERNING LAW

England and Wales

CONTACT

frabs.net
info@frabs.net
support@frabs.net

1. ABOUT THIS DOCUMENT

- 1.1 This document explains in plain language how Frabs protects the Service and its customers' data. It is written to help customers with their own security reviews.
- 1.2 It describes what is in place at the date shown on the cover. The commitments that Frabs gives to customers are in clause 12 of the Frabs Terms and Conditions and in the Frabs Data Processing Agreement.
- 1.3 In this document, "Frabs", "we" and "us" mean the business that operates frabs.net. Words that start with a capital letter have the meaning they have in the Terms.

2. HOW THE SERVICE IS BUILT

- 2.1 The Sensor works at the hypervisor level. Nothing is installed inside an End Customer's virtual server, so the Service cannot be seen, changed or switched off by the End Customer.
- 2.2 The Sensor looks at network flow metadata and abuse indicators, such as addresses, ports, protocols, volumes and timings. It is designed not to collect the content of traffic.
- 2.3 The Service runs on separate servers for separate jobs: the website and Panel, the API, the database, the mail system and a management server. A problem on one does not give direct access to the others.
- 2.4 The database cannot be reached from the public internet. It is reachable only through an encrypted private tunnel from the other Frabs servers.
- 2.5 There is one way in for administration, a management server that is reached over an encrypted private tunnel. The operations console runs only on that private network.

3. ACCESS AND SIGN-IN

- 3.1 Every Authorised User signs in with multi-factor authentication. This is not optional.
- 3.2 Each Authorised User has a role: owner, admin, analyst or a read-only role. Roles decide who can change settings, approve actions, raise support tickets or only look.
- 3.3 Frabs operators sign in to the operations console with passkeys, on a separate sign-in system from the one that customers use.
- 3.4 When a member of staff needs to look at a customer's Account to give support, they use a read-only view. They must record a reason, the view lasts for 30 minutes, and each view is shown in the customer's own audit log.
- 3.5 Actions on our hosting provider's systems, such as restarting a server, need a typed confirmation and are logged.

4. PROTECTING CUSTOMER DATA

- 4.1 Each customer's data is kept separate from other customers' data. The separation is enforced by the database itself, not only by the application.
- 4.2 Data is encrypted in transit. Traffic between users and Frabs uses TLS. Traffic between Frabs servers goes through encrypted private tunnels.
- 4.3 Secrets such as keys and tokens are stored in protected form and are not shown in full after they are created.
- 4.4 Backups of the database are taken regularly and are kept separately from the live system.
- 4.5 When an Account ends, the customer has 30 days to export its Incident records and audit log, and the data is deleted within a further 30 days.

5. SAFE REMEDIATION

- 5.1 Frabs takes a Remediation Action only after an Authorised User has approved it, or under an automation rule that an owner or admin has switched on.
- 5.2 Every Incident, approval, rule and action is recorded in the customer's audit log with the time and the person or rule responsible.
- 5.3 The customer can reverse an action in the Panel.

6. LOGGING AND MONITORING

- 6.1 Staff actions in the operations console are written to an audit log that is tamper-evident, so that any change to an earlier entry can be detected.
- 6.2 Servers are monitored for health and unusual activity, and logs are collected in one place so that problems can be found and investigated.
- 6.3 Sign-in activity is logged. A customer is told by email when a new device signs in to their Account.

7. EMAIL SECURITY

- 7.1 Emails from frabs.net are authenticated using SPF, DKIM and DMARC, so that others can check they are genuine.
- 7.2 Our emails do not use tracking pixels or link tracking. Emails about support tickets never contain the text of the ticket.
- 7.3 Frabs will never ask for a password, a passkey or a sign-in code by email. The only place to sign in is panel.frabs.net.

8. IF SOMETHING GOES WRONG

- 8.1 Frabs investigates security incidents, takes steps to contain them and keeps a record of what happened and what was done.
- 8.2 If a breach of security affects a customer's personal data, Frabs will tell the customer without undue delay and within 48 hours of becoming aware of it, and will help the customer to meet its own duties.

9. WHAT CUSTOMERS DO

- 9.1 Security is shared. Customers help to keep their data safe by:
 - (a) keeping the Sensor up to date on their Nodes;
 - (b) securing their Nodes and their own systems;
 - (c) giving each Authorised User the lowest role they need, and removing people who leave;
 - (d) protecting passkeys and devices used to sign in; and
 - (e) reviewing approval requests carefully before they approve them.

10. REPORTING A VULNERABILITY

- 10.1 If you think you have found a security problem in Frabs, please email info@frabs.net with "Security" in the subject line. Give enough detail for us to reproduce it.
- 10.2 We will acknowledge your report, keep you informed and fix real problems as quickly as we can. We will not take legal action against anyone who reports a problem in good faith, who does not access or change data that is not their own, and who gives us a reasonable time to fix it before telling others.

11. QUESTIONS FROM CUSTOMERS

- 11.1 If your security team has questions or needs a questionnaire completed, email info@frabs.net. Customers can also raise a ticket in the Panel.