

## SOAR & Automation

# Automation with a person in the loop

Automate response with playbooks — and keep a person in the loop.



TotalHeal  
**ResponseFlow**

## Contents

---

|   |                        |    |                                    |
|---|------------------------|----|------------------------------------|
| 1 | Executive summary      | 6  | Security and data handling         |
| 2 | The challenge          | 7  | Where it fits                      |
| 3 | Architecture           | 8  | Deployment and system requirements |
| 4 | How it works           | 9  | Technical specifications           |
| 5 | Capabilities in detail | 10 | Getting started                    |

---

## 1 Executive summary

---

ResponseFlow takes alerts from its own signed webhook or from other TotalHeal products and runs playbooks on them. Every action follows your response policy and approvals, and every step is on a tamper-evident audit chain — automation that does not act behind your back.

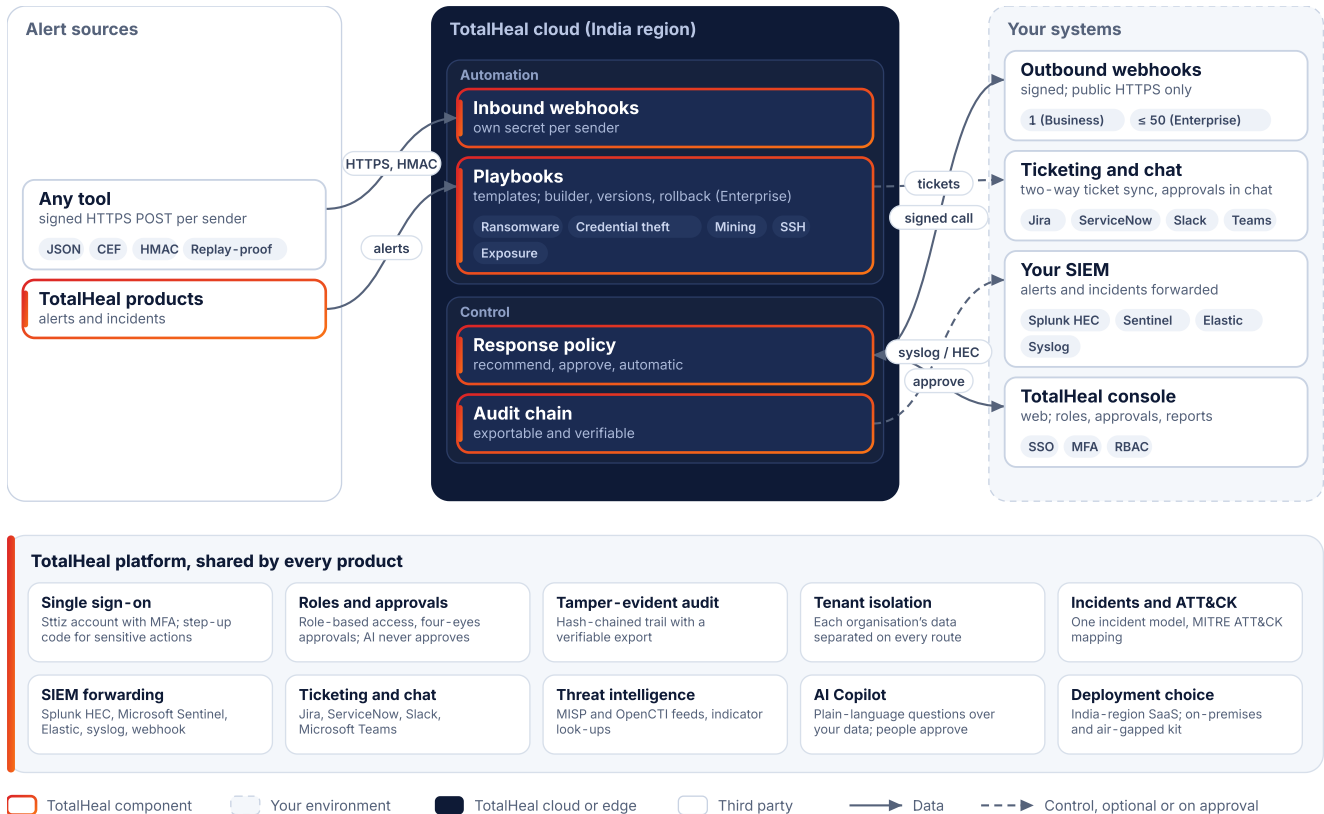
## 2 The challenge

---

Alerts from many tools arrive faster than a team can open tickets, enrich them and act, and automation that acts on its own is a risk of its own.

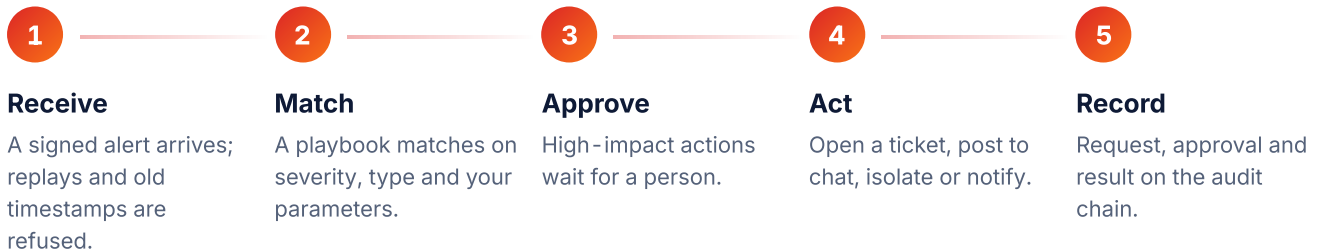
**The TotalHeal approach.** ResponseFlow takes alerts from its own signed webhook or from other TotalHeal products and runs playbooks on them. Every action goes through your response policy and its approvals, and every step is on a tamper-evident audit chain.

### 3 Architecture



Alerts arrive signed; playbooks act only through the response policy; outbound calls are signed and go only to public HTTPS addresses.

### 4 How it works



### 5 Capabilities in detail

- Its own alert source**  
 A signed inbound webhook per sending tool (JSON or CEF), each with its own secret; replays and old timestamps are refused. No SIEM or XDR licence is needed.
- Template playbooks**  
 Ready playbooks for third-party alerts, ransomware, credential theft, crypto-mining, SSH compromise and exposures. On Business you set their parameters — severities, risk threshold, messages, case titles and the webhook they call.
- Custom playbooks (Enterprise)**  
 Build your own playbooks with conditions, versions and rollback.
- A person approves**  
 Actions follow the response policy: recommend, approve or automatic; high-impact actions such as webhooks and isolation always wait for approval.



### Signed outbound webhooks

Calls to your ticketing or chat tool are signed and leave only to public HTTPS addresses. Business includes one endpoint; Enterprise up to 50.



### Audit you can verify

Every request, approval and result is on a hash-chained audit log that can be exported and verified.

## 6 Security and data handling

### Signed in, signed out

Inbound webhooks are signed per sender; outbound calls are signed.

### No private-network calls

Outbound calls go only to public HTTPS addresses.

### People decide impact

Isolation and webhooks always wait for approval.

## 7 Where it fits

### Ticket every high alert

Create and enrich a ticket automatically.

### Ransomware first steps

Template playbook with isolation waiting for approval.

### Chat-ops

Post incidents to your team chat with a link back.

## 8 Deployment and system requirements



### Cloud (SaaS)

Available

Single-region service.



### On-premises

Available

Delivered with our team from the on-premises kit.



### Air-gapped

Available

Offline kit, offline licence file and offline update bundles.

### Protected platforms



Any HTTPS sender  
HMAC-signed

### Works with



Jira



ServiceNow



Slack



Microsoft Teams

### On-premises server

Operating system

RHEL, Rocky Linux or AlmaLinux 8 / 9; Ubuntu 20.04, 22.04 or 24.04; Debian 11 / 12

Processor

4 vCPU (tested configuration)

Memory

8 GB recommended (6 GB minimum)

Disk

10 GB free for software, releases and backups, plus data

Sign-in

Active Directory / LDAP, SAML 2.0 or OpenID Connect

Software

### Network and access

- An alert source: a tool that can send signed HTTPS requests, or other TotalHeal products

### Alerts and tickets to

splunk>

Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

Nothing to pre-install: no  
container runtime, database, web  
server or Java



## 9 Technical specifications

| Features                                                                     |                                                                            | Included           |
|------------------------------------------------------------------------------|----------------------------------------------------------------------------|--------------------|
| Its own alert source                                                         | ✓                                                                          | Included           |
| Template playbooks                                                           | ✓                                                                          | Included           |
| Custom playbooks (Enterprise)                                                | ✓                                                                          | Included           |
| A person approves                                                            | ✓                                                                          | Included           |
| Signed outbound webhooks                                                     | ✓                                                                          | Included           |
| Audit you can verify                                                         | ✓                                                                          | Included           |
| Availability by edition                                                      |                                                                            | BusinessEnterprise |
| Inbound alert webhooks, template playbooks with parameters, approvals, audit | ✓                                                                          | IncludedIncluded   |
| Outbound webhook endpoints                                                   | 1                                                                          | Up to 50           |
| Custom playbooks, builder, versions and rollback                             | —                                                                          | ✓ Included         |
| Platforms and coverage                                                       |                                                                            |                    |
| Senders                                                                      | Any tool that can send an HTTPS POST with an HMAC signature                |                    |
| Console                                                                      | TotalHeal web console                                                      |                    |
| Deployment options                                                           |                                                                            |                    |
| SaaS (India region)                                                          | Available<br>Single-region service.                                        |                    |
| On-premises control plane                                                    | Available<br>Delivered with our team from the on-premises kit.             |                    |
| Air-gapped                                                                   | Available<br>Offline kit, offline licence file and offline update bundles. |                    |
| Licensing                                                                    |                                                                            |                    |
| Priced per                                                                   | Analyst per year                                                           |                    |
| Counted                                                                      | People who run or approve playbooks                                        |                    |
| Trial                                                                        | 30 days                                                                    |                    |

|                            |                                                                                                                                                                                                                                                                                                                       |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Government profile</b>  | Government is a profile, not a separate tier or price list: the Enterprise tier with Government defaults switched on — data residency in India, four-eyes approval of policy changes, a distinct approver for every approval-level action, retention of at least 180 days, and the CERT-In and DPDP reporting clocks. |
| <b>Procurement dossier</b> | Compliance matrix, bill of materials, architecture and hardening, SLA and OEM authorisation letter, on request                                                                                                                                                                                                        |
| <b>On-premises server</b>  |                                                                                                                                                                                                                                                                                                                       |
| <b>Operating system</b>    | RHEL, Rocky Linux or AlmaLinux 8 / 9; Ubuntu 20.04, 22.04 or 24.04; Debian 11 / 12                                                                                                                                                                                                                                    |
| <b>Processor</b>           | 4 vCPU (tested configuration)                                                                                                                                                                                                                                                                                         |
| <b>Memory</b>              | 8 GB recommended (6 GB minimum)                                                                                                                                                                                                                                                                                       |
| <b>Disk</b>                | 10 GB free for software, releases and backups, plus data                                                                                                                                                                                                                                                              |
| <b>Sign-in</b>             | Active Directory / LDAP, SAML 2.0 or OpenID Connect                                                                                                                                                                                                                                                                   |
| <b>Software</b>            | Nothing to pre-install: no container runtime, database, web server or Java                                                                                                                                                                                                                                            |
| <b>Requirements</b>        |                                                                                                                                                                                                                                                                                                                       |
| <b>Requirement 1</b>       | An alert source: a tool that can send signed HTTPS requests, or other TotalHeal products                                                                                                                                                                                                                              |

## 10 Getting started

- An alert source: a tool that can send signed HTTPS requests, or other TotalHeal products

Start a 30 days trial in the TotalHeal console with a Sttiz account. For a quote, an on-premises installation or the procurement dossier (compliance matrix, bill of materials, architecture and hardening, SLA, OEM authorisation letter), write to [business@totalhealsecurity.com](mailto:business@totalhealsecurity.com).

### About TotalHeal

TotalHeal is a security platform from Freaquer Corporation Pvt Ltd: endpoint, network, application, cloud, security-operations and backup products, each sold on its own and run from one console.

### Datasheet

[totalhealsecurity.com/datasheet/soar](https://totalhealsecurity.com/datasheet/soar)

No third-party certification is claimed. Figures are from our own tests where stated, with their dates. Specifications can change; this whitepaper is dated 27 October 2026.