

Bot management & L7 DDoS

Telling people from scripts, and staying up through Layer 7 floods

Keep bots, credential stuffing and application-layer (Layer 7) floods off your sites.



TotalHeal
TrafficShield

Contents

1 Executive summary

2 The challenge

3 Architecture

4 How it works

5 Capabilities in detail

6 Security and data handling

7 Where it fits

8 Deployment and system requirements

9 Technical specifications

10 Getting started

1 Executive summary

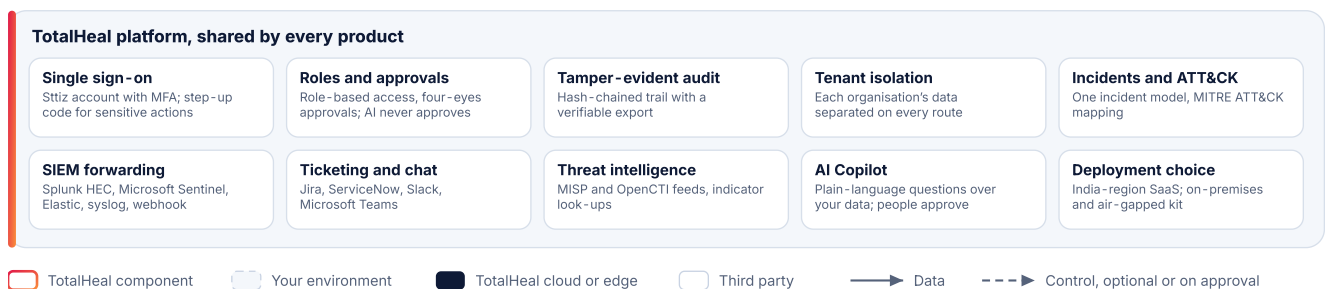
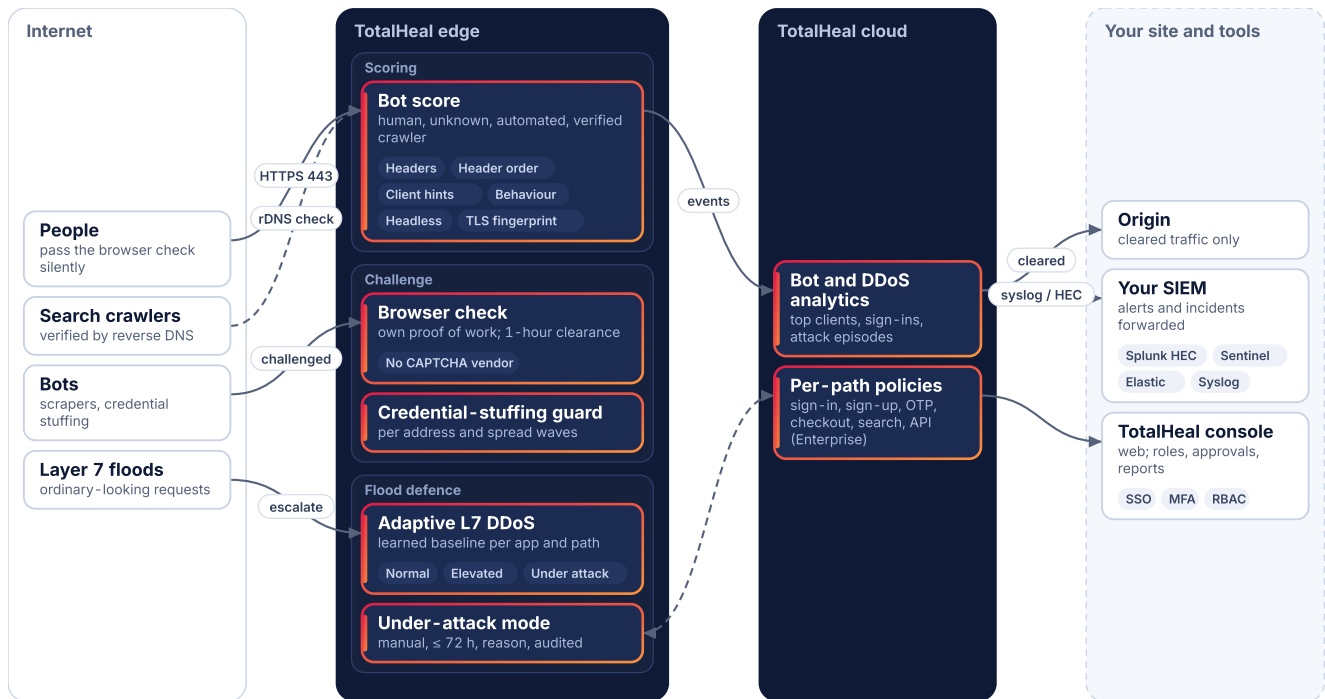
TrafficShield scores every request at the TotalHeal edge, protects sign-in pages from credential stuffing and escalates on its own during an application-layer flood — with its own browser check and no CAPTCHA vendor. In our 25 Oct 2026 test a page flood was challenged 21.6 seconds after it began and none of it reached the site afterwards.

2 The challenge

Public sites and sign-in pages are hit by automated clients: scrapers, credential-stuffing tools and application-layer floods that send ordinary-looking requests until the site slows down or falls over.

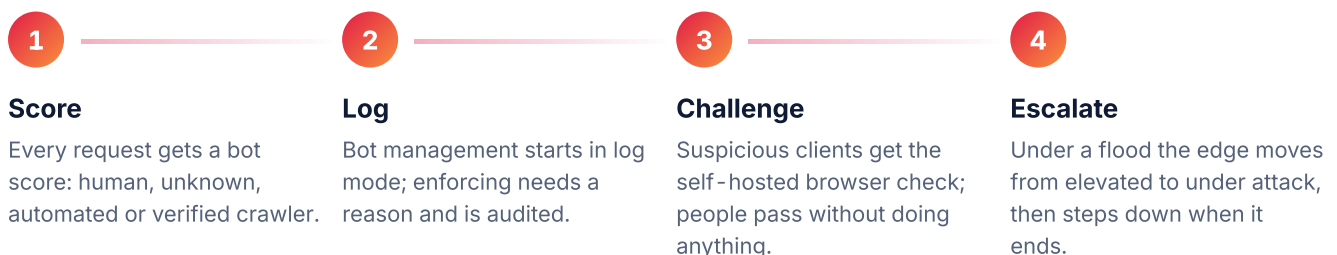
The TotalHeal approach. The TotalHeal edge tells people from scripts, protects sign-in pages from credential stuffing and escalates by itself during a Layer 7 flood — with its own browser check, no CAPTCHA vendor in the path.

3 Architecture

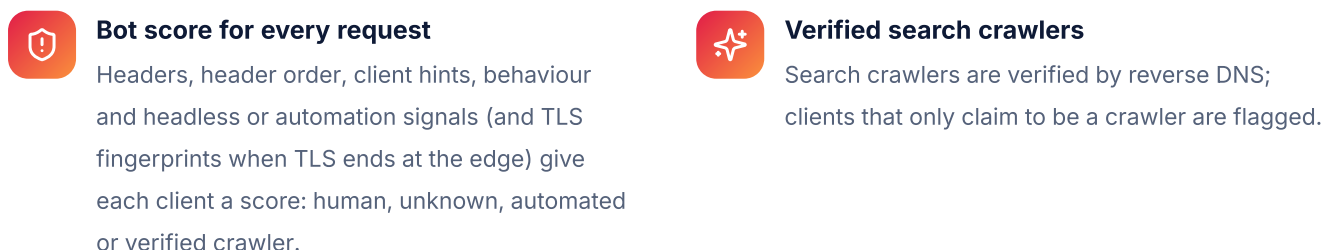


The edge scores, challenges and escalates on its own; only cleared traffic reaches your site. Layer 3/4 floods are out of scope.

4 How it works



5 Capabilities in detail





Own browser check, no CAPTCHA

A self-hosted browser check and proof-of-work challenge with no third-party script; a person passes it without doing anything and gets a clearance for an hour.



Credential-stuffing protection

One address trying many user names with many failures on a sign-in page — or a wave spread across addresses — is detected, then challenged or blocked.



Under-attack mode

Turn on under-attack mode by hand for up to 72 hours, with a reason; it is audited.



Alerts next to your other alerts

Bot, credential-stuffing and flood detections become alerts with MITRE ATT&CK mapping, with bot traffic, top clients, sign-in attempts and attack episodes in the console.



Log first, enforce when ready

Bot management starts by scoring and reporting only; switching an app to enforce needs a reason and is audited.



Adaptive Layer 7 DDoS

A learned traffic baseline per app and path; under a flood the edge escalates by itself from elevated to under attack (every client without clearance is checked), and steps down when the flood is over.



Measured on our test edge

In our 25 Oct 2026 run, a 70-requests-a-second page flood was challenged 21.6 seconds after it started and none of it reached the site after that; every real browser that was checked during the attack passed on its own; a credential-stuffing replay was flagged after 8 failed sign-ins.

6

Security and data handling

No third-party script

The browser check is TotalHeal's own; no CAPTCHA vendor sees your visitors.

Crawlers verified

Search crawlers are verified by reverse DNS; impostors are flagged.

Changes audited

Under-attack mode and enforcement changes need a reason and are audited.

7

Where it fits

Sign-in pages

Credential stuffing detected and challenged, from one address or spread across many.

Public sites under flood

Automatic escalation keeps the site serving real users.

Scraping

Automated clients scored and reported, then blocked by policy.

8 Deployment and system requirements



Cloud (SaaS)

Available

No production point of presence with high availability yet.



Hybrid

Available

The installer stays locked until the release key is published.



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 HTTP(S) application



Edge node
x86_64,
aarch64,
systemd

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

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



Network and access

- The TotalHeal edge in front of your site (TotalHeal point of presence, or a self-hosted edge node on Professional and Elite)
- SaaS: a DNS TXT record and a CNAME for each protected domain; the origin reachable from the TotalHeal edge

Alerts and tickets to



Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

9 Technical specifications

Features	Included
Bot score for every request	✓ Included
Verified search crawlers	✓ Included
Own browser check, no CAPTCHA	✓ Included
Log first, enforce when ready	✓ Included
Credential-stuffing protection	✓ Included
Adaptive Layer 7 DDoS	✓ Included

Under - attack mode	✔ Included		
Measured on our test edge	✔ Included		
Alerts next to your other alerts	✔ Included		
Availability by tier	Essential	Professional	Elite
Bot score, verified crawlers, log or enforce, browser and proof-of-work checks	✔ Included	✔ Included	✔ Included
Credential-stuffing protection on sign-in pages	✔ Included	✔ Included	✔ Included
Adaptive Layer 7 DDoS protection, under-attack mode, attack episodes and history, alerts	✔ Included	✔ Included	✔ Included
Per-path bot policies (sign-in, sign-up, OTP, checkout, search, API)	—	✔ Included	✔ Included
Self-hosted edge nodes in your data centre	—	✔ Included	✔ Included
Threat-actor and campaign intelligence on attacking addresses	—	—	✔ Included
List price per application per year	US\$2,400 · ₹2,28,380	US\$7,200 · ₹6,85,150	US\$18,000 · ₹17,12,880
Platforms and coverage			
SaaS	Any web application over HTTP(S) behind the TotalHeal edge: verify the domain, point a CNAME at the edge		
Self-hosted edge node	Linux with systemd, x86_64 or aarch64 (Professional and Elite)		
Console	TotalHeal web console		
Deployment options			
SaaS (CNAME to the TotalHeal edge, India)	Available No production point of presence with high availability yet.		
Hybrid (self-hosted Linux edge node)	Available The installer stays locked until the release key is published.		
On-premises control plane	Available Delivered with our team from the on-premises kit.		
Air-gapped	Available Offline kit, offline licence file and offline update bundles.		
Licensing			

Priced per	Protected application (FQDN) per year
Counted	Applications configured
Trial	30 days
Government profile	Government is a profile, not a separate tier or price list: the Elite 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.
Procurement dossier	Compliance matrix, bill of materials, architecture and hardening, SLA and OEM authorisation letter, on request
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	Nothing to pre-install: no container runtime, database, web server or Java
Requirements	
Requirement 1	The TotalHeal edge in front of your site (TotalHeal point of presence, or a self-hosted edge node on Professional and Elite)
Requirement 2	SaaS: a DNS TXT record and a CNAME for each protected domain; the origin reachable from the TotalHeal edge

10 Getting started

- The TotalHeal edge in front of your site (TotalHeal point of presence, or a self-hosted edge node on Professional and Elite)
- SaaS: a DNS TXT record and a CNAME for each protected domain; the origin reachable from the TotalHeal edge

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.

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/bot-ddos

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.