

Web Application Firewall (WAF)

A web application firewall you can tune without breaking real users

A web application firewall in front of your portals, tuned without breaking real users.



TotalHeal
WebShield

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

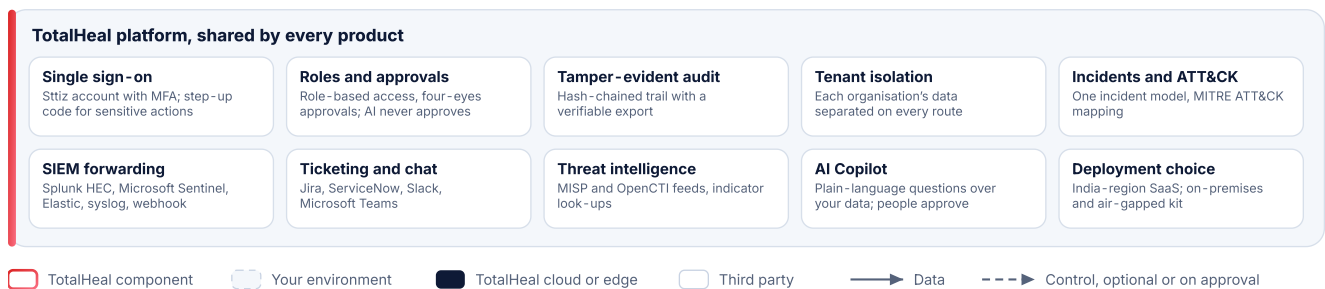
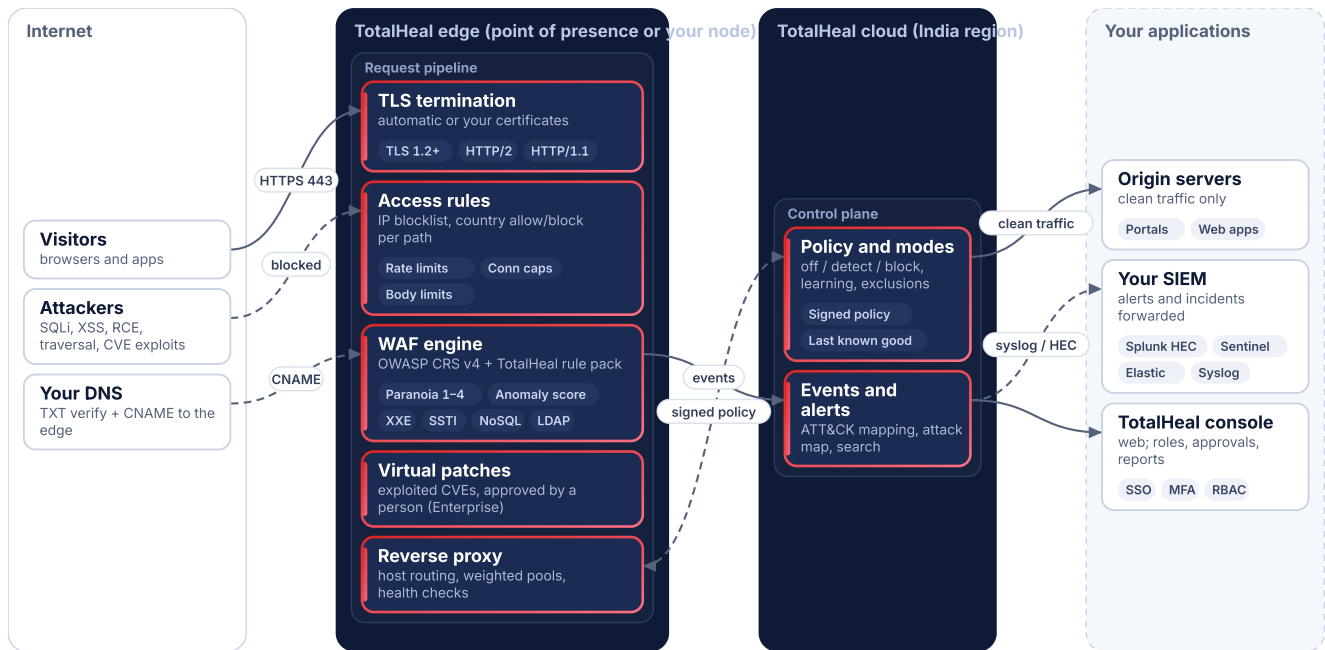
WebShield sits in front of your portals and applications at the TotalHeal edge, runs the OWASP Core Rule Set plus TotalHeal rules, learns before it blocks and reports attacks next to your endpoint and identity alerts. In our 8 Oct 2026 GoTestWAF run at paranoia level 1 every attack payload was blocked and no legitimate request was.

2 The challenge

Public web applications and portals are attacked constantly: SQL injection, cross-site scripting, remote code execution, path traversal and exploits for known CVEs. Most organisations cannot patch every application quickly.

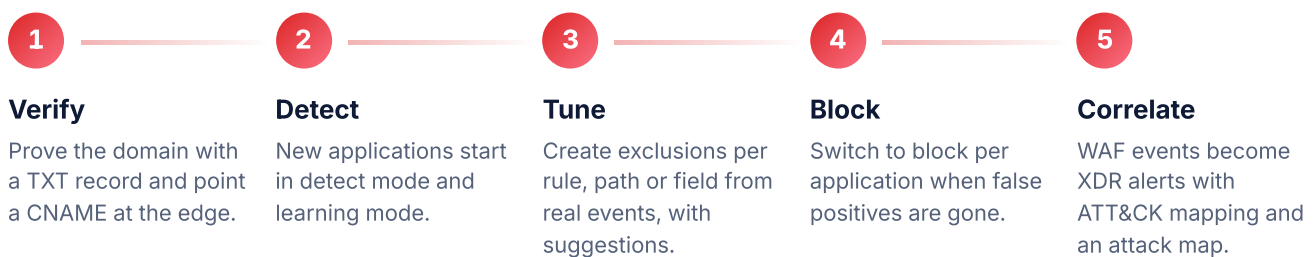
The TotalHeal approach. A filter in front of the application that blocks attacks, can be tuned without breaking real users, and reports attacks to the security team next to endpoint and identity alerts.

3 Architecture



Visitors reach the TotalHeal edge by CNAME; only clean traffic reaches your origin. Policy arrives signed with a last-known-good fallback.

4 How it works



5 Capabilities in detail

Reverse proxy per application

Host routing, weighted upstream pools and active health checks; unknown hosts are never proxied.

TLS done for you

Automatic certificates or your own; TLS 1.2 minimum; HTTP/2 and HTTP/1.1.



OWASP Core Rule Set

OWASP CRS v4 with off, detect or block per app, paranoia level 1–4 and an anomaly threshold, plus the TotalHeal rule pack (XXE, SSTI, NoSQL, LDAP and more).



False-positive control

New apps start in detect mode; learning mode; rule exclusions per rule, path and field, created from an event, with suggestions.



Virtual patches (Professional and Elite)

A curated library of virtual patches for exploited CVEs, suggested from your vulnerability findings; a person approves.



Country access control

Allow or block visitors by country for a whole application or for one path (for example only India on /admin), from an offline IP-location database. Detect mode reports what would be refused before you block.



Measured detection quality

In our 8 Oct 2026 run of the open-source GoTestWAF tool at paranoia level 1, all attack payloads were blocked and no legitimate requests were blocked; the OWASP CRS regression suite passed 99.6 %.



Rate limits and blocklists

Per-IP and per-path rate limits, connection caps, body limits, and an IP blocklist from your threat intel with expiry and rollback.



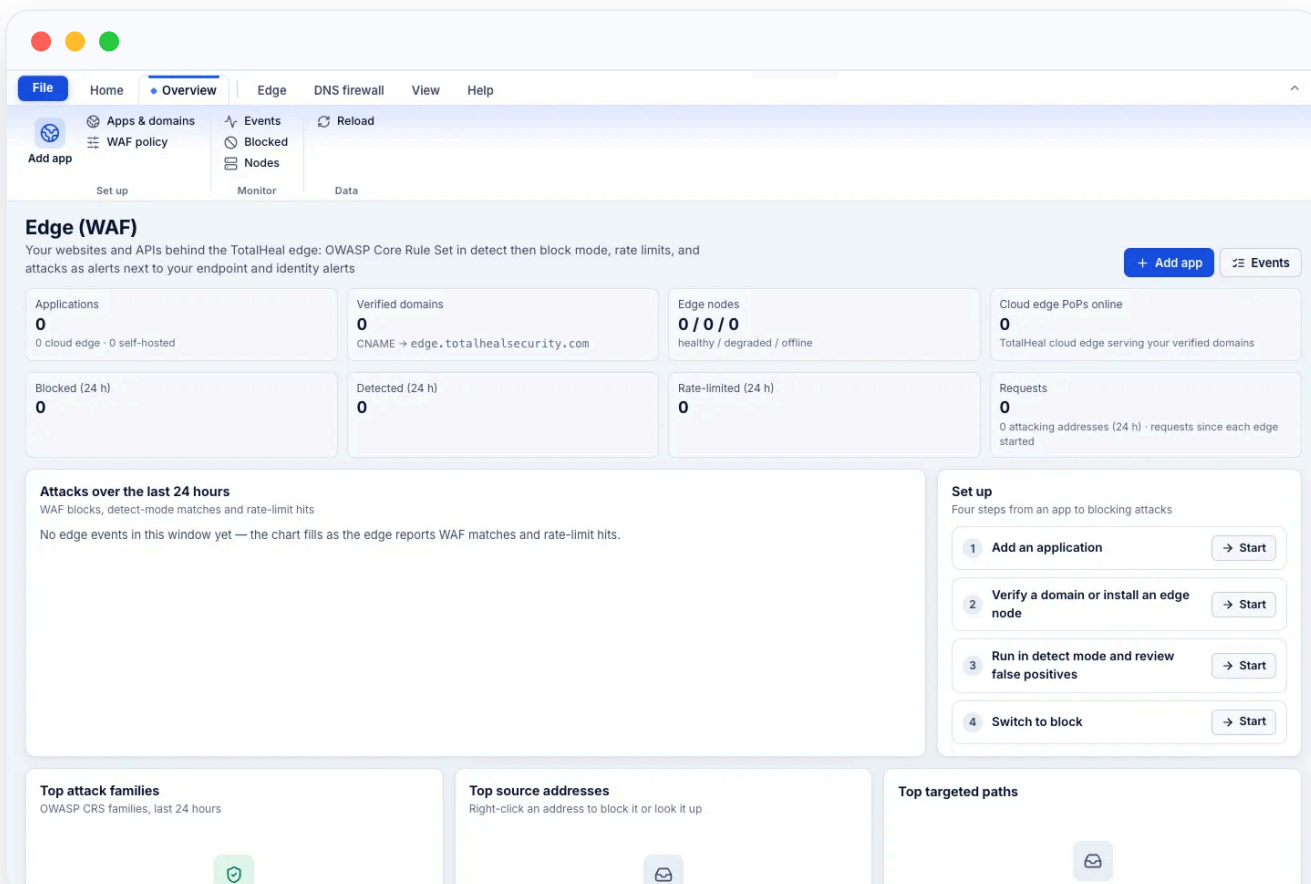
Signed policy with last-known-good

Policy bundles are signed and rollback-protected; the edge falls back to the last known good policy.



Alerts next to your other alerts

WAF events become XDR alerts with ATT&CK mapping, an attack map and search. Every mode change and exclusion is audited.



The WebShield WAF overview in the TotalHeal console (demo organisation, no traffic yet). Real screenshot, demo data.

6 Security and data handling

Unknown hosts never proxied

Only verified domains are served by the edge.

Signed policy, last known good

Policy bundles are signed and rollback-protected; the edge keeps the last good policy.

Every change audited

Mode changes and exclusions are recorded with who and why.

7 Where it fits

Citizen and customer portals

Protect public portals that cannot be patched quickly.

Virtual patching (Enterprise)

Shield exploited CVEs from your vulnerability findings, approved by a person.

Admin paths by country

Allow /admin only from India while the public site stays open.

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

Network and access

- SaaS: a DNS TXT record and a CNAME for each protected domain; the origin reachable from the TotalHeal edge
- Self-hosted node: a Linux VM with systemd, outbound HTTPS, inbound 80/443

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		
Reverse proxy per application	✓ Included		
TLS done for you	✓ Included		
OWASP Core Rule Set	✓ Included		
Measured detection quality	✓ Included		
False-positive control	✓ Included		
Rate limits and blocklists	✓ Included		
Virtual patches (Professional and Elite)	✓ Included		
Signed policy with last-known-good	✓ Included		
Country access control	✓ Included		
Alerts next to your other alerts	✓ Included		
Availability by tier	Essential	Professional	Elite
Delivery from TotalHeal points of presence, OWASP CRS WAF, detect then block, paranoia levels, learning mode, exclusions, false-positive review	✓ Included	✓ Included	✓ Included
Rate limits, connection caps, IP blocklist, country allow and block per app and path, events, attack map, alerts in the incident queue	✓ Included	✓ Included	✓ Included
Self-hosted edge nodes in your data centre	—	✓ Included	✓ Included
Virtual patches from VulnSight findings and the CISA KEV catalogue, approved by you	—	✓ Included	✓ Included
Threat-actor and campaign intelligence on attackers	—	—	✓ Included

List price per application per year	US\$1,200 · ₹1,14,190	US\$3,600 · ₹3,42,580	US\$9,600 · ₹9,13,540
Platforms and coverage			
SaaS	Any web application over HTTP(S): verify the domain, point a CNAME at the TotalHeal 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, with a monthly request allowance		
Counted	Applications configured; requests per month		
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	SaaS: a DNS TXT record and a CNAME for each protected domain; the origin reachable from the TotalHeal edge		

10 Getting started

- SaaS: a DNS TXT record and a CNAME for each protected domain; the origin reachable from the TotalHeal edge
- Self-hosted node: a Linux VM with systemd, outbound HTTPS, inbound 80/443

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/edge-waf

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.