

API Security

Knowing every API you expose, and enforcing what it should accept

Protect API hosts at the same edge that runs WebShield: discovery, schema enforcement and API abuse findings.



TotalHeal
APIShield

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

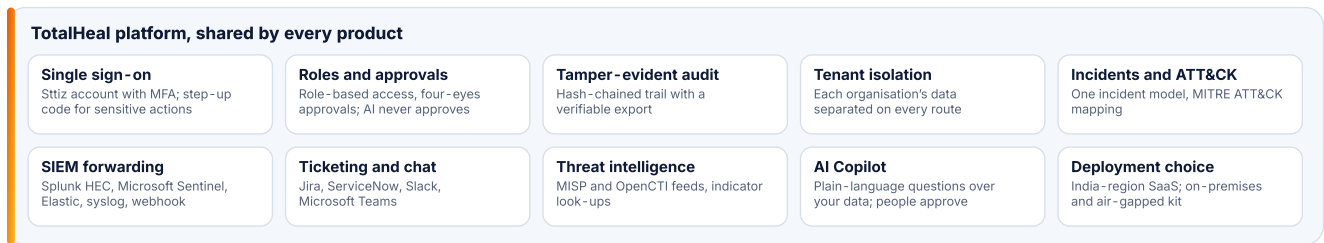
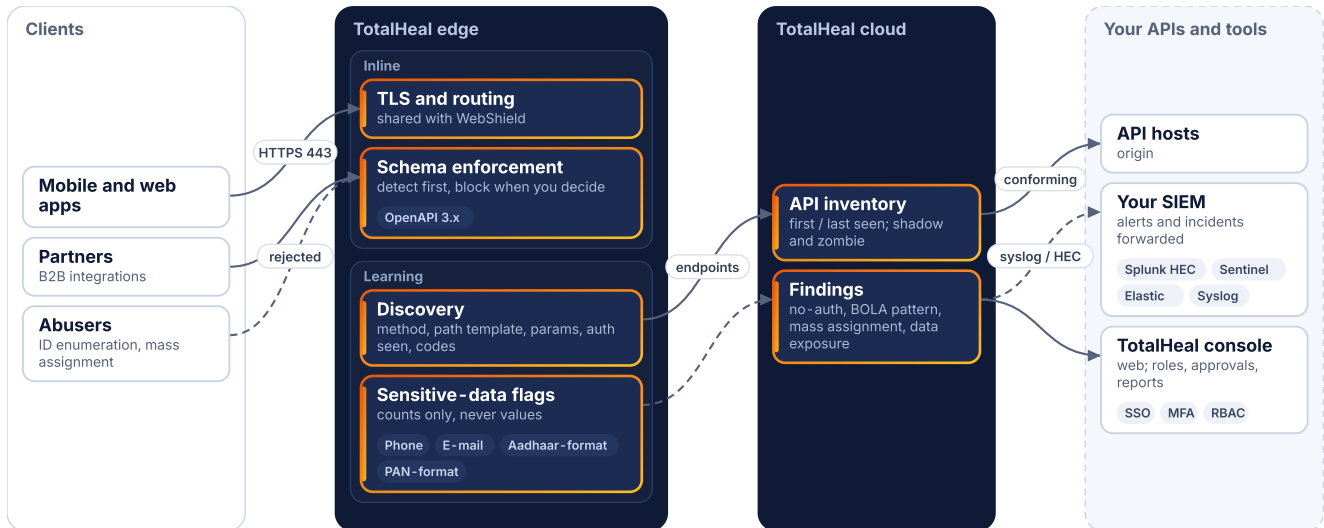
APIShield runs at the TotalHeal edge in front of your API hosts: it learns endpoints from traffic, imports your OpenAPI description, enforces the schema when you are ready and reports API abuse — enumeration, mass assignment, missing authentication — as findings.

2 The challenge

APIs now carry most application traffic, and the classic attacks on them — reading other customers' records by changing an ID, sending fields the client should not set, calling forgotten endpoints — look like ordinary requests to a web firewall.

The TotalHeal approach. APIShield runs at the TotalHeal edge in front of your API hosts. It learns the endpoints from traffic, imports your OpenAPI description, enforces the schema when you are ready and reports API abuse patterns as findings.

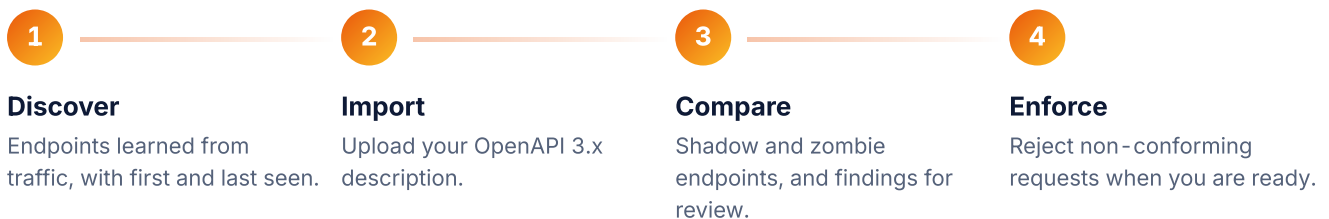
3 Architecture



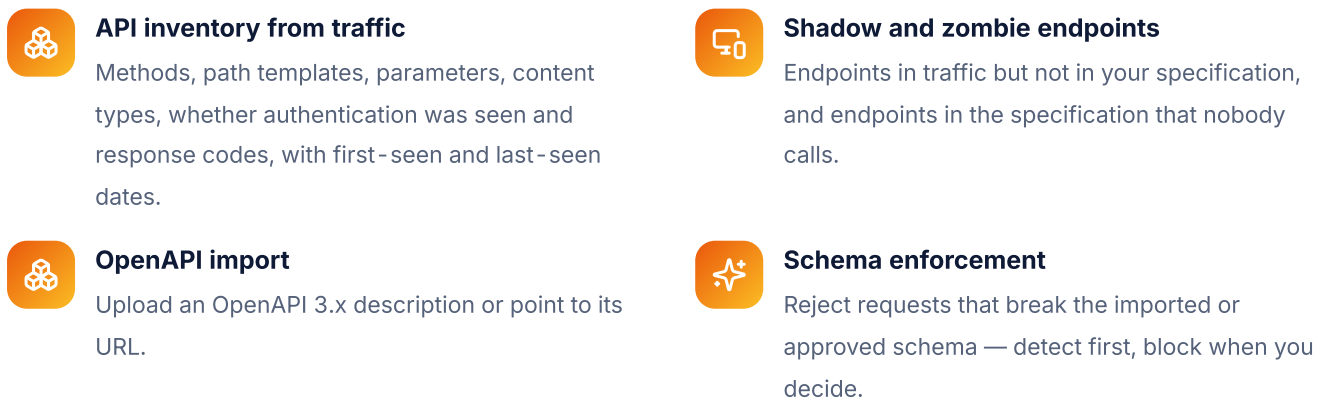
■ TotalHeal component
 ■ Your environment
 ■ TotalHeal cloud or edge
 ■ Third party
 → Data
 - - - Control, optional or on approval

API clients reach the TotalHeal edge; APIShield learns endpoints, checks requests against the schema and forwards conforming traffic to your hosts.

4 How it works



5 Capabilities in detail





Abuse findings

Unauthenticated access to endpoints that usually carry authentication, object-ID enumeration from one client, unexpected body fields (mass assignment) and excessive data in responses — shown as findings, not automatic blocks.



Sensitive data, counted not stored

Responses are flagged for personal-data patterns such as phone, e-mail, Aadhaar-format and PAN-format values; only counts are kept, never the values.

6 Security and data handling

Detect first

Enforcement is switched on by you, never by default.

Findings, not surprises

Heuristics never block on their own.

Counts, not values

Sensitive-data flags keep counts only.

7 Where it fits

Mobile app backends

See every endpoint the app really calls.

Partner APIs

Enforce the agreed schema at the edge.

Data exposure

Find endpoints returning personal data.

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)
API
OpenAPI 3.x



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

Network and access

- The TotalHeal edge in front of your API host (TotalHeal point of presence or a self-hosted edge node)

Alerts and tickets to

splunk> Splunk



Microsoft
Sentinel



Elastic



Syslog /
CEF



Jira



ServiceNow



Slack



Microsoft
Teams

Software

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



9 Technical specifications

Features	Included		
API inventory from traffic	✓ Included		
Shadow and zombie endpoints	✓ Included		
OpenAPI import	✓ Included		
Schema enforcement	✓ Included		
Abuse findings	✓ Included		
Sensitive data, counted not stored	✓ Included		
Availability by tier	Essential	Professional	Elite
API inventory from traffic: methods, path templates, parameters, content types, authentication seen, response codes; OpenAPI export	✓ Included	✓ Included	✓ Included
Sensitive data in responses counted, never stored (phone, e-mail, Aadhaar and PAN formats)	✓ Included	✓ Included	✓ Included
OpenAPI 3.x import, shadow and zombie endpoints, endpoint review	—	✓ Included	✓ Included
Schema enforcement — detect first, block when you decide	—	✓ Included	✓ Included
Self-hosted edge nodes in your data centre	—	✓ Included	✓ Included
Abuse findings: unauthenticated access to endpoints that usually carry it, object-ID enumeration from one client; accept or reopen	—	—	✓ Included
List price per API host per year	US\$2,400 · ₹2,28,380	US\$6,000 · ₹5,70,960	US\$12,000 · ₹11,41,920

Platforms and coverage	
SaaS	Any API 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
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	API host per year
Counted	API hosts configured at the edge
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 API host (TotalHeal point of presence or a self-hosted edge node)

10 Getting started

- The TotalHeal edge in front of your API host (TotalHeal point of presence or a self-hosted edge node)

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/api-security

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.