

DNS Firewall & Security

Stopping attacks at the DNS lookup, before any connection is made

Stop malware, phishing and DNS tunnelling at the lookup — for every device, on site or on the road.



TotalHeal
DNSGuard

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

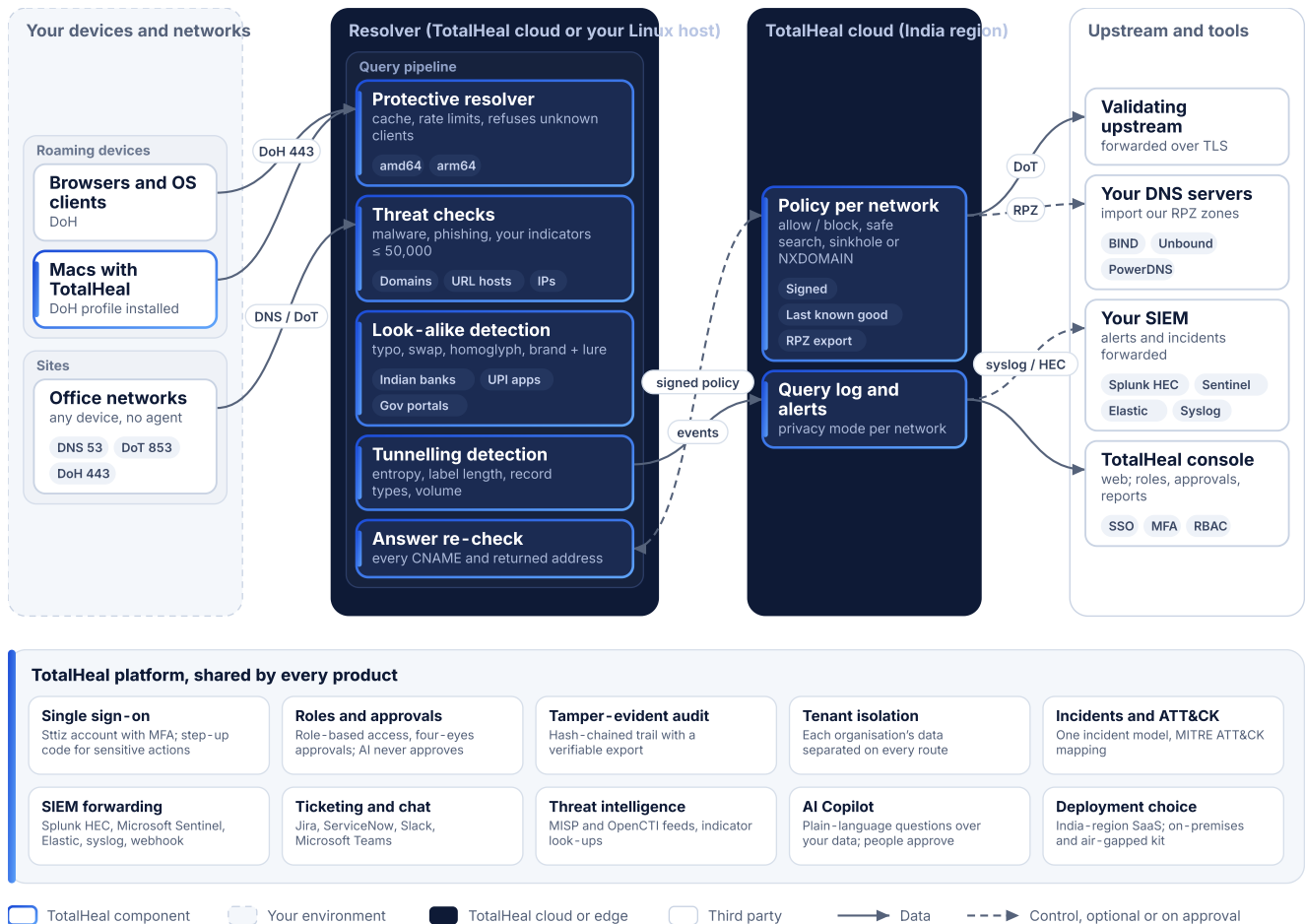
DNSGuard is a protective resolver, in the TotalHeal cloud or on your own Linux hosts. It blocks malware, phishing and look-alike domains, detects DNS tunnelling, re-checks every answer and lands its detections next to your endpoint alerts — without an agent on every device.

2 The challenge

Most malware, phishing and data-theft traffic starts with a DNS lookup. A protective resolver stops the lookup before a connection is made, for every device on a site or on the road, without an agent on every device.

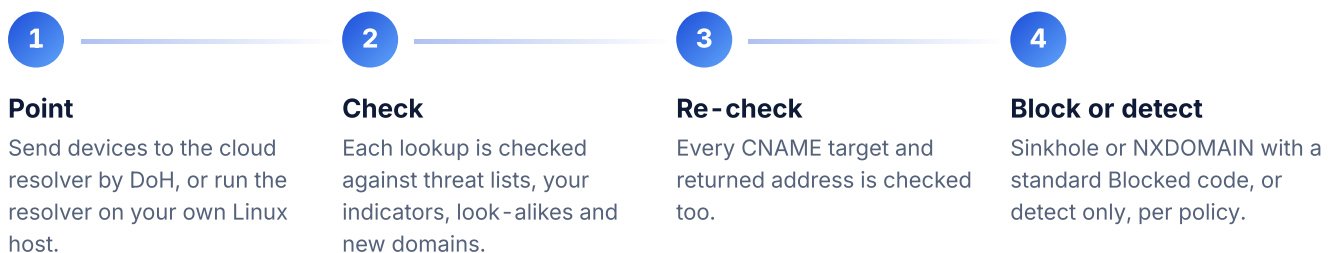
The TotalHeal approach. Threat-blocking protective DNS from the TotalHeal cloud or your own resolver, with blocks and detections landing next to your endpoint alerts. No content-category filtering.

3 Architecture

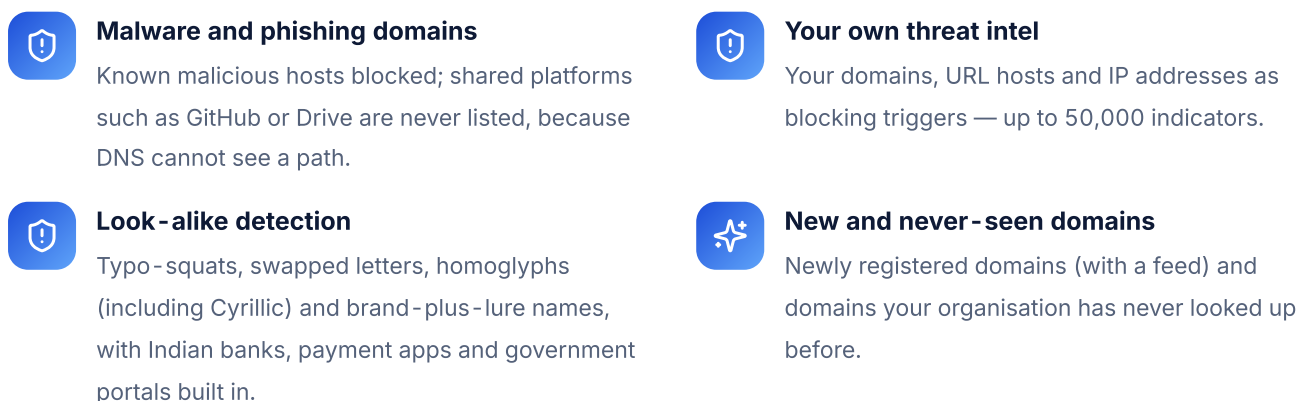


Clients query over DoH (cloud) or DNS, DoT and DoH (your resolver); every answer is re-checked; policy arrives signed; the resolver never fails open.

4 How it works



5 Capabilities in detail





DNS tunnelling and exfiltration

Detected from entropy, label length, record types and volume; detect or block per policy.



Policies per network

Allow and block lists, safe search for Google, Bing, DuckDuckGo and YouTube, sinkhole or NXDOMAIN, with a standard "Blocked" error code.



Never an open resolver, never fails open

Unknown clients refused, rate limits, zone transfers refused; signed policy bundles with last-known-good. Privacy modes per network; BYOD networks never log allowed queries.



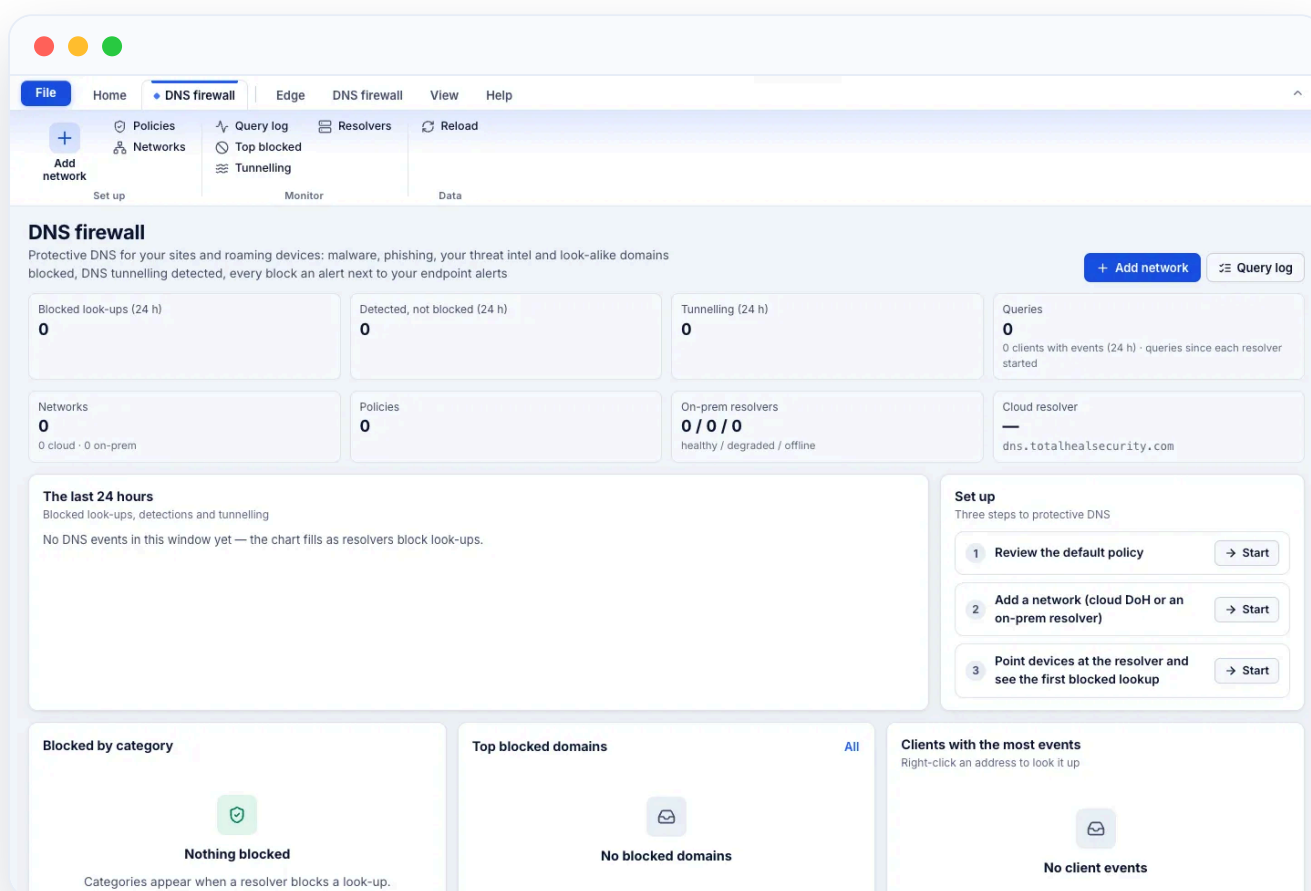
Answers are checked too

Every CNAME target and returned address is re-checked.



Standard formats

Every list is a standard RPZ zone you can export for BIND, Unbound or PowerDNS. DoH in the cloud; DNS, DoT and DoH on your own resolver.



The DNS Firewall overview in the TotalHeal console (demo organisation, no queries yet). Real screenshot, demo data.

6 Security and data handling

Never an open resolver

Unknown clients are refused, rate limits apply and zone transfers are refused.

Privacy by network

BYOD networks never log allowed queries.

Never fails open

Signed policy bundles with last known good.

7 Where it fits

Branch offices

Protect every device on a site without installing anything on them.

Phishing look-alikes

Indian banks, payment apps and government portals protected from typo-squats.

Exfiltration

DNS tunnelling detected or blocked.

8 Deployment and system requirements



Cloud (SaaS)

Available

Runs as a test deployment for listed organisations.



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



Browsers
DoH



macOS
11 and later



iPhone, iPad
DoH profile



Android
DoT



Resolver node
amd64, arm64

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

- Cloud: a client that speaks DoH
- On-premises: a Linux host with systemd, outbound HTTPS, a TLS certificate for DoT/DoH, a Professional or Elite licence

Alerts and tickets to

splunk>

Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

9 Technical specifications

Features	Included
Malware and phishing domains	✓ Included
Your own threat intel	✓ Included

Look-alike detection	✔ Included		
New and never-seen domains	✔ Included		
DNS tunnelling and exfiltration	✔ Included		
Answers are checked too	✔ Included		
Policies per network	✔ Included		
Standard formats	✔ Included		
Never an open resolver, never fails open	✔ Included		
Availability by tier			
	Essential	Professional	Elite
Cloud DoH resolver, threat categories, safe search, allow and block lists, tunnelling detection, query log, alerts, RPZ export	✔ Included	✔ Included	✔ Included
Secure DNS on TotalHeal desktop agents	✔ Included	✔ Included	✔ Included
On-premises resolvers (DNS, DoT, DoH, block page)	—	✔ Included	✔ Included
Threat-actor and campaign intelligence	—	—	✔ Included
List price per user per year	US\$18 · ₹1,710	US\$36 · ₹3,430	US\$54 · ₹5,140
Platforms and coverage			
Cloud resolver (DoH)	Any client that speaks DoH: browsers, macOS/iOS by profile; the TotalHeal app on macOS installs the profile		
On-premises resolver node	Linux amd64/arm64 with systemd (Professional and Elite)		
Deployment options			
SaaS (cloud DoH resolver, India)	Available Runs as a test deployment for listed organisations.		
Hybrid (your resolver, TotalHeal console)	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 user per year
Counted	Distinct users or devices seen by the resolver
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	Cloud: a client that speaks DoH
Requirement 2	On-premises: a Linux host with systemd, outbound HTTPS, a TLS certificate for DoT/DoH, a Professional or Elite licence

10 Getting started

- Cloud: a client that speaks DoH
- On-premises: a Linux host with systemd, outbound HTTPS, a TLS certificate for DoT/DoH, a Professional or Elite licence

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/dns-firewall

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.