

TotalHeal SurfGuard

Secure Web Gateway (SWG)

Every web request your people make, checked against their own policy — malware, phishing, your threat intelligence and about 57 content categories — in the TotalHeal cloud or on a proxy in your office.



Cloud (SaaS)

On-premises

Air-gapped

The challenge

Most attacks still start with a click: a phishing page that looks like the bank, a download from a look-alike site, a link in an SMS. DNS filtering stops many of them but sees only the name, not the person or the file, and gives the user no explanation. Content rules differ by team — the newsroom needs social networks, accounts does not — and when a site is blocked by mistake there is no simple way to ask for it.

The answer

SurfGuard is a secure web gateway. Browsers send their web traffic to it — the TotalHeal cloud proxy or a proxy in your office — and each person signs in with their e-mail and a proxy token. Every request is checked against that person's policy: the security checks of DNSGuard first, then content categories, then your own lists. A blocked or warned site shows a page that says why, with a button to request access.

Status	Available
Deploys as	Cloud (SaaS) · On-premises · Air-gapped
Runs on	Browsers; Self-hosted proxy; Category data
Priced per	user per year
Trial	30 days, up to 25 people
Licence	Sold on its own; one TotalHeal console

Supported platforms



Any browser with a PAC file or proxy setting

Windows, macOS, Linux, ChromeOS, Android, iOS



Self-hosted proxy

Linux x86-64 / arm64

How it works

1

Connect

Browsers take the PAC file; people sign in with their e-mail and a proxy token.

2

Decide

Security checks, content categories and your lists decide each request for that person's policy.

3

Explain

Blocked and warned sites show the reason; a warning can be continued for an hour.

4

Ask

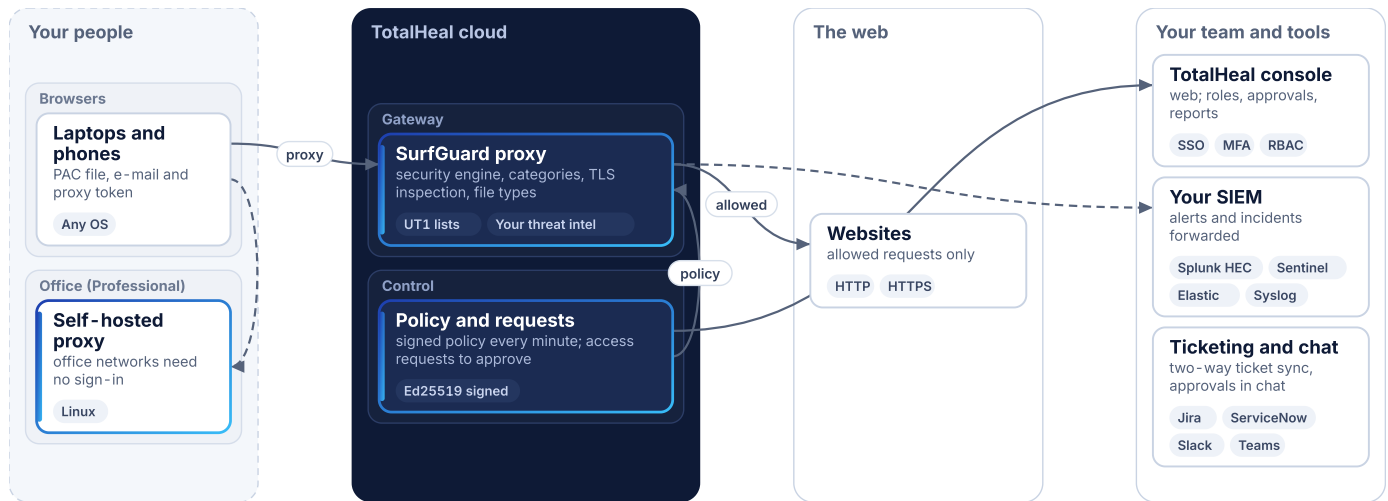
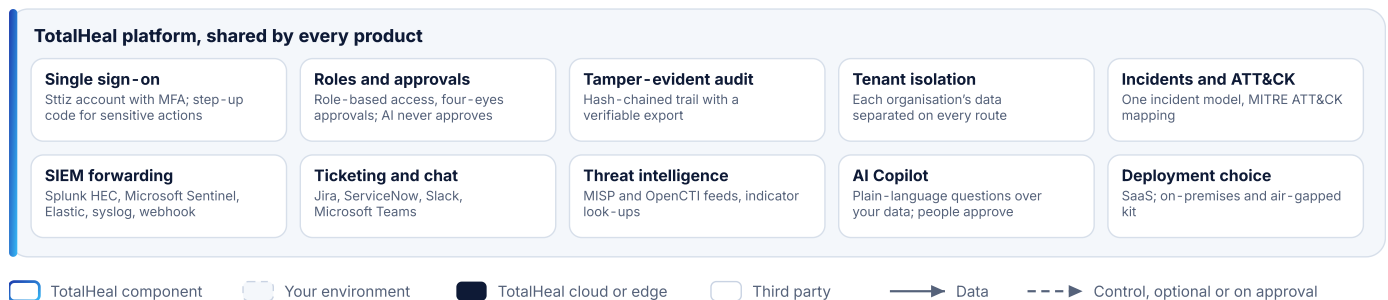
People request access from the page; an administrator approves for them or for the policy.

5

Record

Every block is logged and security blocks raise alerts in the incident queue.

Reference architecture



Browsers use the PAC file and sign in to SurfGuard; the proxy decides each request from the signed policy and the category database, and reports every block.

Key capabilities

- A policy per person**

Each person gets their own policy, the policy of the first group rule that matches, or the default. Allow, warn or block each content category; add sites to always allow or always block; turn on safe search for Google, Bing, YouTube and DuckDuckGo.

57 content categories

Adult, gambling, piracy, proxies and anonymisers, social networks, streaming, shopping, games, webmail and more — about 5 million domains from the Université Toulouse Capitole (UT1) lists, rebuilt daily. A site in several categories is decided by all of them.

Access requests

Requests arrive in the console with the site, its categories and the reason. Approve for that person only, or add the site to their policy's allow list for everyone; the proxies have it within a minute.

Security first

Malware and phishing hosts (URLhaus), your own threat intelligence, analyst blocks from incident response and look-alike domains of your brands and Indian banks are decided by the same engine as DNSGuard, before any category. Security blocks raise alerts in the incident queue with MITRE ATT&CK.

Pages that explain

Blocked and warned sites show a page with the reason — on HTTPS too, when devices trust the organisation's SurfGuard root. A warning lets the person continue for an hour; a block lets them request access with a reason.

TLS inspection

On the Professional tier, allowed HTTPS sites can be decrypted with the organisation's root, except the categories and sites you exempt (online banking and finance by default), so the activity shows full addresses and downloads can be checked.



File types

On the Professional tier, downloads of chosen file types — exe, msi, apk, iso — are blocked, by name and by the file name the server sends.



Cloud or office

The TotalHeal cloud proxy serves people anywhere; on the Professional tier a self-hosted proxy runs in the office, where listed office networks need no sign-in. Both take the same signed policy and keep working on the last good one if the cloud cannot be reached.



Work hours

On the Elite tier, categories can be blocked only inside work hours — for example streaming and games from 09:30 to 18:30 on weekdays, in your time zone.

In the console

When	Person	Site	Outcome	Why	Categories	HTTPS
just now	meera@pragati-media.example	www.amazon.in https://www.amazon.in/deals	continued	continued after a warning (Shopping)	Shopping	inspected
just now	meera@pragati-media.example	www.amazon.in	continued	continued after a warning (Shopping)	Shopping	—
just now	neha@pragati-media.example	www.flipkart.com https://www.flipkart.com/	allowed	allowed	—	inspected
just now	neha@pragati-media.example	www.pornhub.com https://www.pornhub.com/	blocked	Adult is blocked by policy Default	Adult	inspected
just now	joseph@pragati-media.example	www.netflix.com https://www.netflix.com/browse	allowed	allowed	Audio and video streaming	inspected
just now	joseph@pragati-media.example	wetransfer-share.example https://wetransfer-share.example/d/9F2K	blocked	on the policy's block list (wetransfer-share.example)	—	inspected
just now	joseph@pragati-media.example	downloads.fontshare-mirror.example http://downloads.fontshare-mirror.example/installer/setup.exe	blocked	.exe downloads are blocked by policy Default	—	—
just now	meera@pragati-media.example	medium.com https://medium.com/@editor/how-we-cover-elections	allowed	allowed	—	inspected
just now	meera@pragati-media.example	www.google.com https://www.google.com/search?q=quarterly+ad+rates	safe search	safe search	—	inspected

SurfGuard activity for a demo media company browsing through the cloud proxy. Real screenshot, demo data.

Deployment options



Cloud (SaaS)

Available

The cloud proxy runs in the TotalHeal cloud; a self-hosted proxy runs in your office (Professional).



On-premises

Available

Delivered with our team from the on-premises kit.



Air-gapped

Available

Offline kit, offline licence file and offline update bundles.

System requirements

Protected platforms



Any browser with a PAC file or proxy setting
Windows, macOS, Linux, ChromeOS, Android, iOS



Self-hosted proxy
Linux x86-64 / 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

- Browsers set to the SurfGuard PAC file (by Group Policy, MDM or TotalHeal UEM)
- The SurfGuard root trusted on devices for pages on HTTPS and for inspection

Alerts and tickets to

 **Splunk**

 **Microsoft Sentinel**

 **Elastic**

 **Syslog / CEF**

 **Jira**

 **ServiceNow**

 **Slack**

 **Microsoft Teams**

Technical specifications

Features	Included		
A policy per person	✓ Included		
Security first	✓ Included		
57 content categories	✓ Included		
Pages that explain	✓ Included		
Access requests	✓ Included		
TLS inspection	✓ Included		
File types	✓ Included		
Cloud or office	✓ Included		
Work hours	✓ Included		
Availability by tier	Essential	Professional	Elite
Cloud proxy with a PAC file; each person signs in with their e-mail and a proxy token; policy by person, group rule or default	✓ Included	✓ Included	✓ Included
Malware, phishing, your threat intelligence, analyst blocks and typo-squats (the DNSGuard engine); your allow and block lists; safe search	✓ Included	✓ Included	✓ Included
About 57 content categories from the UT1 lists (5 million domains, updated daily): allow, warn or block each	✓ Included	✓ Included	✓ Included
Block and warning pages on HTTP and HTTPS (with the SurfGuard root trusted), continue for an hour, request access; approve for a person or a policy	✓ Included	✓ Included	✓ Included
Alerts from security blocks in the incident queue; activity search	✓ Included	✓ Included	✓ Included
TLS inspection with exempt categories and sites; full addresses in the activity	—	✓ Included	✓ Included
File - type blocking of downloads (exe, msi, apk ...)	—	✓ Included	✓ Included

Self-hosted proxies in your office; office networks that need no sign-in	—	✓ Included	✓ Included
Work-hours rules: categories blocked only inside the hours, in your time zone	—	—	✓ Included
Activity kept 30 days (Essential), 90 days (Professional), one year (Elite)	✓ Included	✓ Included	✓ Included
List price per user per year	US\$30 · ₹2,850	US\$54 · ₹5,140	US\$78 · ₹7,420

Platforms and coverage

Browsers	Any browser that takes a PAC file or a proxy setting (Windows, macOS, Linux, ChromeOS, Android, iOS)
Self-hosted proxy	Linux x86-64 or arm64 with systemd (Professional)
Category data	Université Toulouse Capitole blacklists (UT1), CC BY-SA 4.0, rebuilt daily
Console	TotalHeal web console

Deployment options

SaaS	Available The cloud proxy runs in the TotalHeal cloud; a self-hosted proxy runs in your office (Professional).
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	user per year
Counted	People who sign in to SurfGuard
Trial	30 days, up to 25 people
Editions	SurfGuard is sold on its own, outside the editions.
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	Browsers set to the SurfGuard PAC file (by Group Policy, MDM or TotalHeal UEM)
Requirement 2	The SurfGuard root trusted on devices for pages on HTTPS and for inspection

Get started

30 days, up to 25 people trial in the TotalHeal console. Quotes and the procurement dossier (compliance matrix, bill of materials, architecture and hardening, SLA, OEM authorisation letter): business@totalhealsecurity.com

Freaquer Corporation Pvt Ltd

totalhealsecurity.com/products/surfguard · [whitepaper: totalhealsecurity.com/datasheets/totalheal-surfguard-whitepaper.pdf?v=2a55b7551d](https://totalhealsecurity.com/datasheets/totalheal-surfguard-whitepaper.pdf?v=2a55b7551d)

Figures are from our own tests where stated, with their dates. Specifications can change; this datasheet is dated 27 October 2026.