

Cloud app discovery and control (CASB)

Know every cloud app your people use — and decide about each one

Shows which cloud apps your people use — generative AI, file transfer, remote access and 100 more — how risky each is, and blocks the ones you decide against through DNSGuard.



TotalHeal
SaaSGuard

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

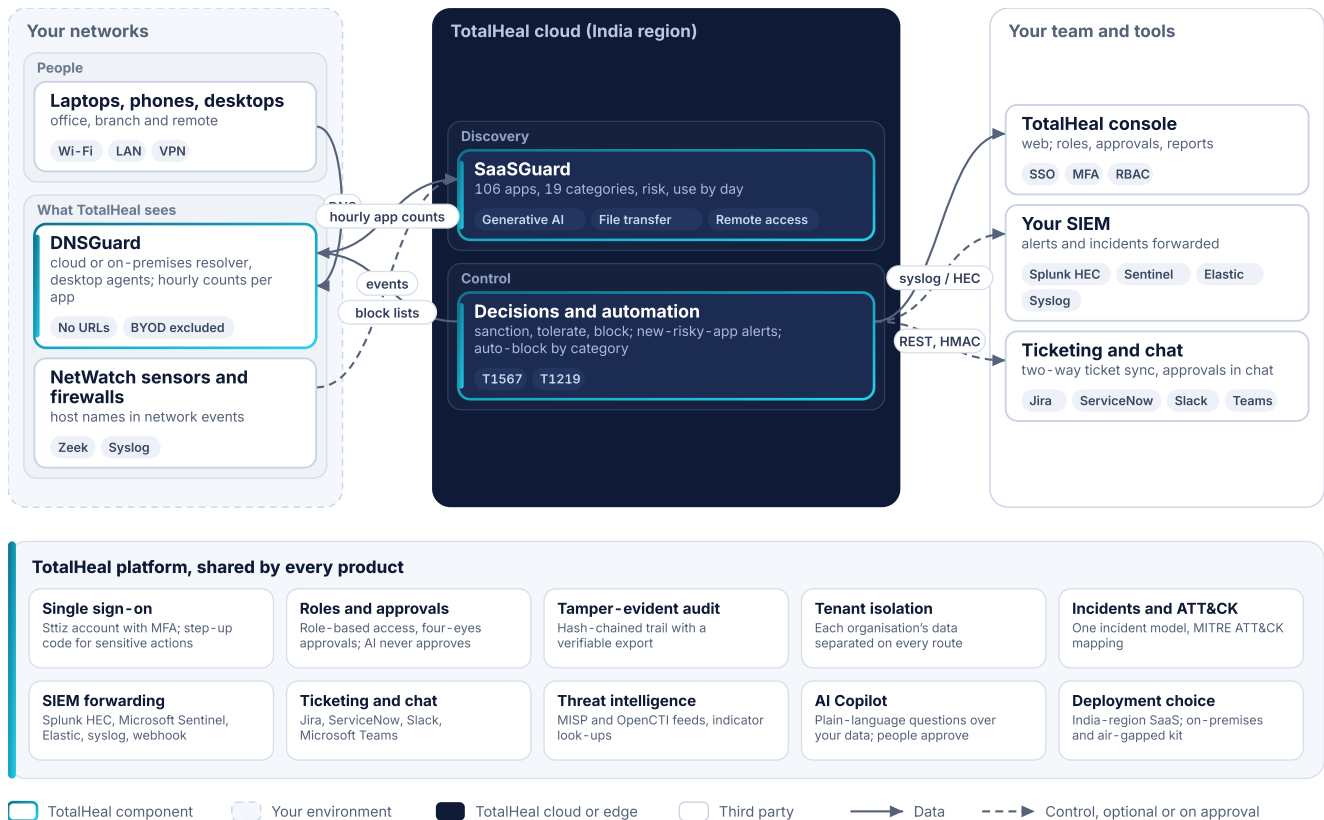
SaaSGuard turns what TotalHeal already sees — DNSGuard's hourly count per app and the host names in sensor and firewall events — into an inventory of the cloud apps in use, each with a risk. Mark each one sanctioned, tolerated or blocked; blocking goes through DNSGuard on every network straight away, and new high-risk apps raise an alert or are blocked automatically.

2 The challenge

People sign up for whatever gets the job done: a free AI assistant for a contract, a file-transfer site for a large export, a remote-desktop tool for a vendor, a PDF converter for a payslip. None of it is on an approved list, and nobody can say which apps hold company data, who uses them, or whether the one that was banned last quarter is still in use.

The TotalHeal approach. SaaSGuard learns which cloud apps are used from what TotalHeal already sees — DNSGuard's hourly count per app, DNS logs and the host names in network-sensor and firewall events — and matches it against a catalogue of 106 applications in 19 categories. Each app gets a risk and a decision: sanctioned, tolerated or blocked. Blocking goes through DNSGuard on every network straight away.

3 Architecture

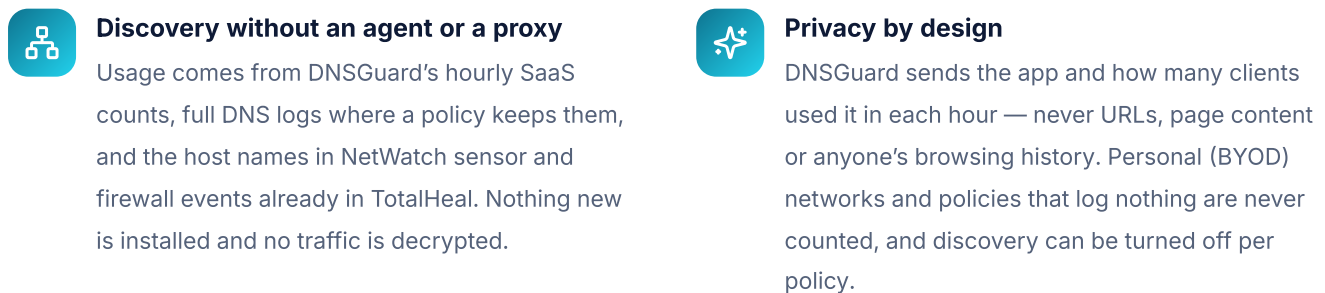


DNSGuard counts look-ups for catalogued apps every hour and sends only the app and the number of clients; SaaSGuard adds what sensors and firewalls saw, scores each app, and blocks the apps you decide against through DNSGuard.

4 How it works



5 Capabilities in detail





A catalogue of 106 cloud apps

Office suites, storage, file transfer, messaging, video meetings, generative AI, collaboration, document tools, translation, e-signature, development, cloud consoles, paste sites and tunnels, remote access, CRM, marketing, web mail, social media and streaming — matched by their domains, the most specific first.



What each app is used for

Look-ups, refused look-ups, users, networks, sources, first and last seen, and use by day over up to 90 days, for every app seen or decided.



New risky apps raise an alert

Every hour SaaSGuard checks for apps used for the first time; a high-risk one nobody has reviewed raises an alert mapped to MITRE ATT&CK (T1567 exfiltration over web services, T1219 remote access software) in the same incident queue as endpoint and identity alerts.



Generative AI in view

ChatGPT, Claude, Gemini, Copilot, DeepSeek, Perplexity and other AI assistants are their own category, so you can see who uses them and sanction the one the company pays for.



Risk for every app

Each category has a base risk from what it lets data do (file transfer, paste sites and tunnels: very high; generative AI, remote access, document tools: high); wide use raises it, and a sanctioned app is lowest.



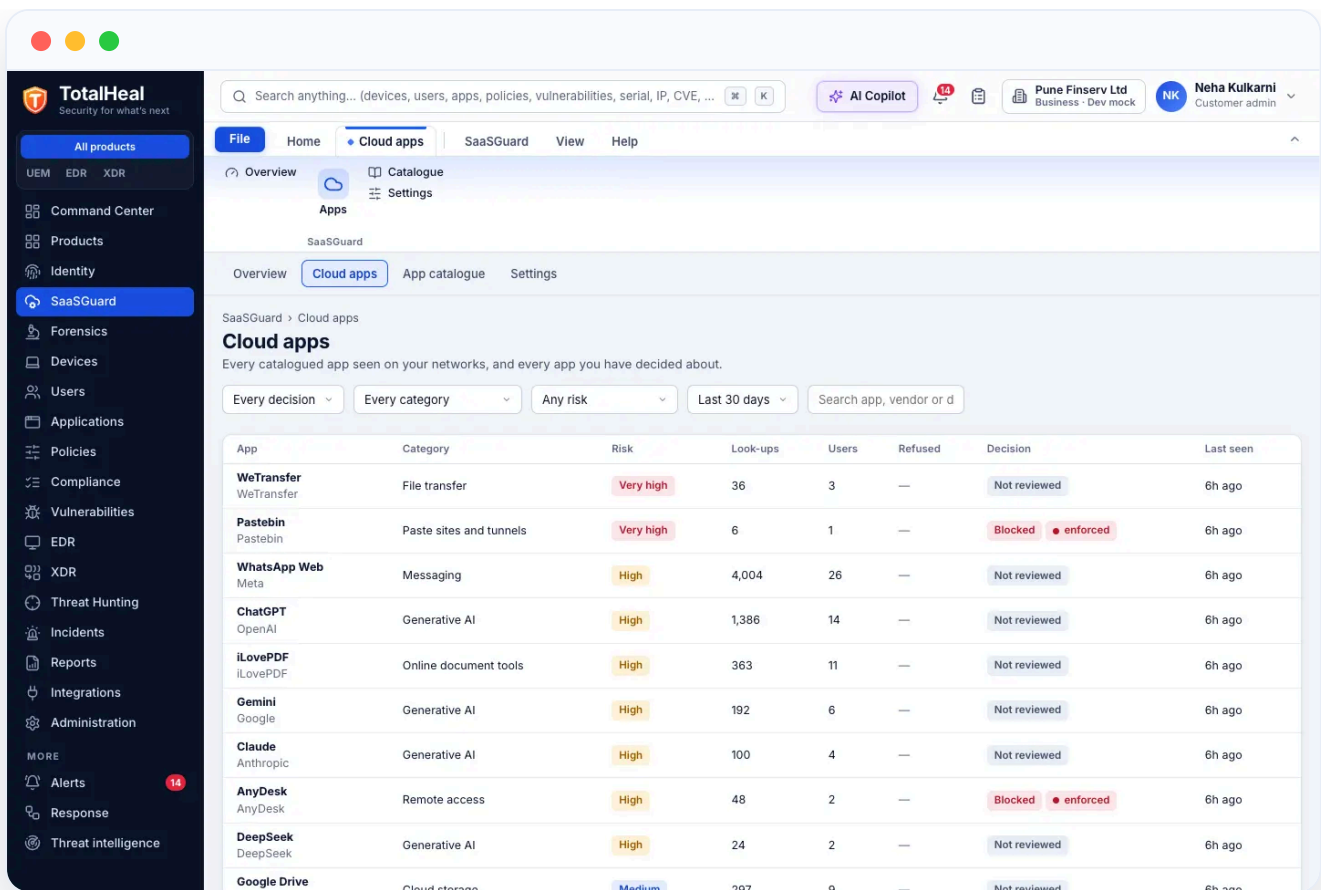
Sanction, tolerate or block

Every decision carries a note and is kept in the audit trail. Blocking puts the app's domains on the deny list of every DNSGuard policy straight away; unblocking or sanctioning removes exactly the domains SaaSGuard added and nothing an administrator put there.



Block new apps automatically

Choose categories — paste sites and tunnels, file transfer, remote access — and a new app in them is blocked the first time it is seen. Apps you already decided about are never changed.



Cloud apps in SaaSGuard, from a demo office's look-ups through the DNSGuard resolver. Real screenshot, demo data.

6 Security and data handling

Apps, not browsing history

DNSGuard sends the app and the number of clients each hour, never URLs or page content.

Blocking you can undo exactly

Unblocking removes only the domains SaaSGuard added, never an administrator's own entries.

Personal networks left alone

BYOD networks and policies that log nothing are never counted; discovery can be turned off per policy.

Every decision recorded

Who decided, when and why, in the audit trail.

7 Where it fits

Generative AI

See who uses which AI assistant, sanction the one the company licenses and block the rest.

Data leaving by file transfer

WeTransfer, paste sites and tunnels flagged as very high risk and blocked automatically when new ones appear.

Unapproved remote access

AnyDesk, TeamViewer and similar tools seen and blocked so vendors use the approved route.

8 Deployment and system requirements



Cloud (SaaS)

Available

Discovery and decisions in the cloud; blocking in DNSGuard wherever it resolves.



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



DNSGuard networks and desktop agents



NetWatch sensors



Firewall logs sent to TotalHeal

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

- DNSGuard on your networks or desktop agents, a NetWatch sensor, or firewall logs sent to TotalHeal
- For blocking: DNSGuard with at least one policy

Alerts and tickets to

splunk>

Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

9 Technical specifications

Features	Included
Discovery without an agent or a proxy	✓ Included
Privacy by design	✓ Included
A catalogue of 106 cloud apps	✓ Included
Risk for every app	✓ Included
What each app is used for	✓ Included
Sanction, tolerate or block	✓ Included

New risky apps raise an alert	✔ Included		
Block new apps automatically	✔ Included		
Generative AI in view	✔ Included		
Availability by tier	Essential	Professional	Elite
Discovery from DNSGuard hourly counts, DNS logs and network-sensor and firewall events: 106 cloud apps in 19 categories, risk, users, look-ups, networks, use by day	✔ Included	✔ Included	✔ Included
Decisions per app — sanctioned, tolerated, not reviewed — with a note and an audit trail; app catalogue	✔ Included	✔ Included	✔ Included
Alert in the incident queue when a new high-risk app is used for the first time	✔ Included	✔ Included	✔ Included
Block an app: its domains go on every DNSGuard policy, and unblocking removes exactly what SaaSGuard added	—	✔ Included	✔ Included
Block new apps automatically in the categories you choose	—	—	✔ Included
List price per user per year	US\$12 · ₹1,140	US\$24 · ₹2,280	US\$36 · ₹3,430
Platforms and coverage			
Sources	DNSGuard (cloud resolver, on-premises resolver or desktop agents); NetWatch sensors; firewall and proxy logs sent to TotalHeal		
Blocking	Through DNSGuard policies, on every network and desktop that uses them		
Console	TotalHeal web console		
Deployment options			
SaaS (India region)	Available Discovery and decisions in the cloud; blocking in DNSGuard wherever it resolves.		
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 in the organisation whose traffic SaaSGuard covers
Trial	30 days, up to 50 users
Editions	SaaSGuard is sold on its own, outside the editions; blocking needs DNSGuard.
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	DNSGuard on your networks or desktop agents, a NetWatch sensor, or firewall logs sent to TotalHeal
Requirement 2	For blocking: DNSGuard with at least one policy

10 Getting started

- DNSGuard on your networks or desktop agents, a NetWatch sensor, or firewall logs sent to TotalHeal
- For blocking: DNSGuard with at least one policy

Start a 30 days, up to 50 users 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/saasguard

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.