

Business Antivirus (NGAV / Endpoint Protection)

Business antivirus that stops malware without stopping the business

Business antivirus on the TotalHeal agent: stop known malware without quarantining legitimate work.



TotalHeal
ThreatGuard

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

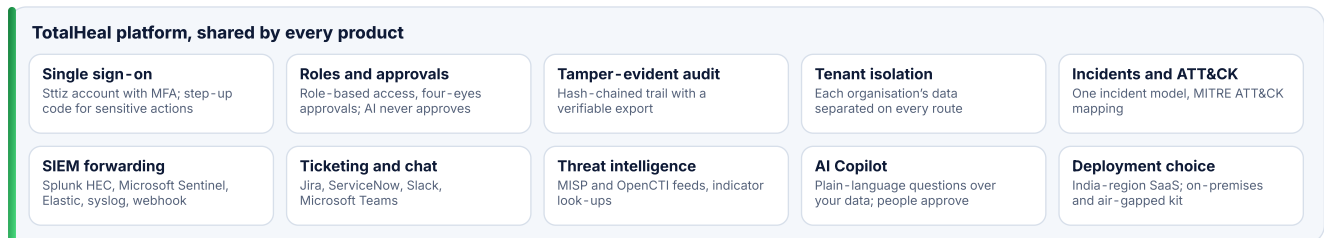
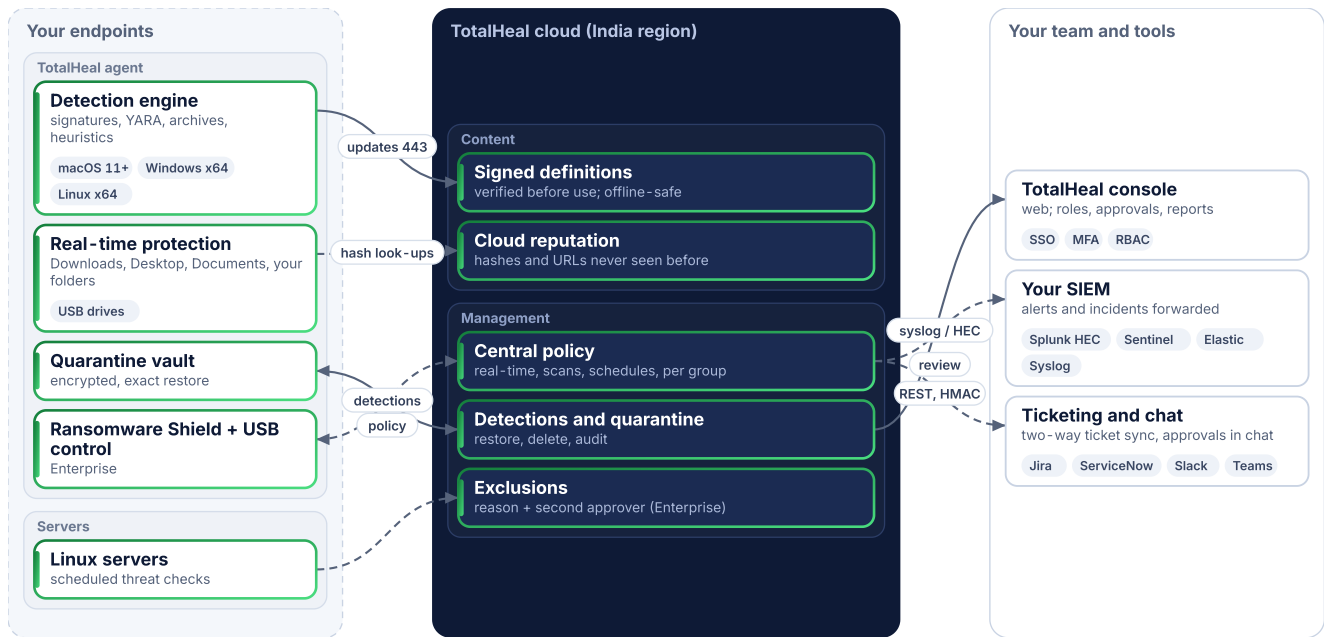
ThreatGuard runs on the same TotalHeal agent as your other products. It blocks known malware with layered detection, quarantines only confident verdicts automatically and puts every quarantine, restore and exclusion on record — because an antivirus that quarantines legitimate work soon gets switched off.

2 The challenge

Every organisation still has to stop known malware on its laptops and desktops, and tenders buy antivirus as its own line. An antivirus that quarantines developers' projects or business files soon gets switched off.

The TotalHeal approach. Endpoint protection on the same TotalHeal agent as your other products, steered from the console, with every quarantine, restore and exclusion on record.

3 Architecture



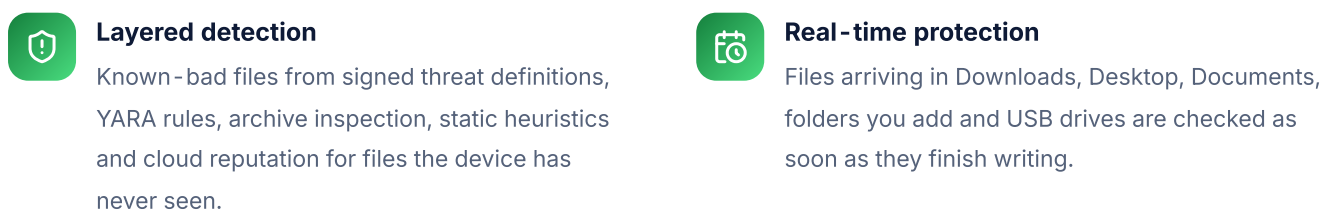
■ TotalHeal component
 ■ Your environment
 ■ TotalHeal cloud or edge
 ■ Third party
 → Data
 - - - → Control, optional or on approval

Detection runs on the device and keeps working offline; the cloud supplies signed definitions, reputation and central policy.

4 How it works



5 Capabilities in detail





Built against false positives

Only confident verdicts are quarantined automatically; heuristic findings wait for a person. Rules only count on the kind of file they were written for, and common developer folders are excluded by default — visibly, and removable.



Safe quarantine and restore

Quarantined files are kept encrypted and can be put back exactly as they were. A restore never overwrites a newer file.



Central policy

Real-time protection on or off, quarantine or report on detection, and scheduled scans — set once for the organisation.



USB control and Ransomware Shield (Enterprise)

Scan drives on insert and eject untrusted ones; ransomware activity in protected folders is detected and raised as an alert.



Its own licence

An expired ThreatGuard licence pauses only antivirus, with a clear message on the device; other TotalHeal products keep running and restores always work.



Quick, full and custom scans

On the device or sent from the console, with pause, resume and cancel.



Works offline

Protection keeps running with the last installed definitions when the device is offline; definitions are verified before they are used.



Central quarantine and detections

Every detection across devices in one list; restore or delete quarantined files from the console, with an audit trail.



Approved exclusions and per-group policy (Enterprise)

Every exclusion carries a reason and a second person's approval; different policies and scan schedules per device group.

6 Security and data handling

Restores are exact

Quarantined files are kept encrypted and put back exactly as they were; a restore never overwrites a newer file.

Definitions are verified

Definitions are signed and checked before use; protection keeps working offline.

Exclusions are approved

Each exclusion carries a reason and, on Enterprise, a second person's approval.

7 Where it fits

Antivirus line in a tender

A business antivirus sold as its own line, on the same agent as UEM and patching.

Developer machines

Common developer folders excluded visibly by default, so builds are not quarantined.

USB control (Enterprise)

Drives scanned on insert and untrusted ones ejected.

8 Deployment and system requirements



Cloud (SaaS)

Partial

In development: the console side is built; company computers apply the policy from desktop 0.3.10, not released yet.



On-premises

Available

Delivered with our team from the on-premises kit.



Air-gapped

Roadmap

No offline definitions package yet.

Protected platforms



macOS
11 and later



Windows
x64



Linux desktop
x64



Linux servers
scheduled checks

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

- TotalHeal desktop agent enrolled to your organisation on each endpoint
- macOS: Full Disk Access for TotalHeal (by the person or your MDM)
- Outbound HTTPS to the TotalHeal cloud for definitions, reputation and policy

Alerts and tickets to

splunk> **Splunk**



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

9 Technical specifications

Features	Included	
Layered detection	✓ Included	
Real-time protection	✓ Included	
Built against false positives	✓ Included	
Quick, full and custom scans	✓ Included	
Safe quarantine and restore	✓ Included	
Works offline	✓ Included	

Central policy	✔ Included	
Central quarantine and detections	✔ Included	
USB control and Ransomware Shield (Enterprise)	✔ Included	
Approved exclusions and per-group policy (Enterprise)	✔ Included	
Its own licence	✔ Included	
Availability by edition		
	Business	Enterprise
Detection engine, real-time protection, quarantine, offline protection	✔ Included	✔ Included
Central policy, scheduled scans, quick and full scans from the console	✔ Included	✔ Included
Central quarantine (restore, delete, audit) and detections list	✔ Included	✔ Included
USB control and Ransomware Shield policy	—	✔ Included
Exclusions with reason and second-person approval	—	✔ Included
Per-group policies and scan schedules	—	✔ Included
Platforms and coverage		
macOS 11 or later	TotalHeal desktop agent (Full Disk Access needed for real-time protection)	
Windows (x64)	TotalHeal desktop agent	
Linux desktops (x64)	TotalHeal desktop agent	
Linux servers	Threat checks by the TotalHeal server agent: scheduled, not real-time	
Deployment options		
SaaS (TotalHeal cloud, India region)	Partial In development: the console side is built; company computers apply the policy from desktop 0.3.10, not released yet.	
On-premises	Available Delivered with our team from the on-premises kit.	
Air-gapped	Roadmap No offline definitions package yet.	
Licensing		

Priced per	Endpoint per year
Counted	Devices with endpoint protection switched on
Trial	30 days
Government profile	Government is a profile, not a separate tier or price list: the Enterprise 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	TotalHeal desktop agent enrolled to your organisation on each endpoint
Requirement 2	macOS: Full Disk Access for TotalHeal (by the person or your MDM)
Requirement 3	Outbound HTTPS to the TotalHeal cloud for definitions, reputation and policy

10 Getting started

- TotalHeal desktop agent enrolled to your organisation on each endpoint
- macOS: Full Disk Access for TotalHeal (by the person or your MDM)
- Outbound HTTPS to the TotalHeal cloud for definitions, reputation and policy

Start a 30 days trial in the TotalHeal console with a Sttizi 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/threatguard

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.