

SaaS Security Posture Management (SSPM)

Your Microsoft 365 and Google Workspace settings, checked every few hours — and fixed with two people agreeing

Checks the security settings of your Microsoft 365 and Google Workspace tenants continuously — MFA, administrators, app consent, sharing, third-party apps — and fixes them with a second person's approval.



TotalHeal
SaaSPosture

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

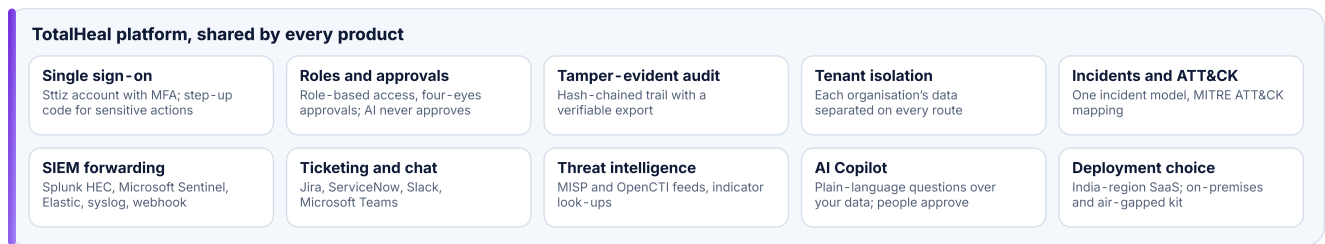
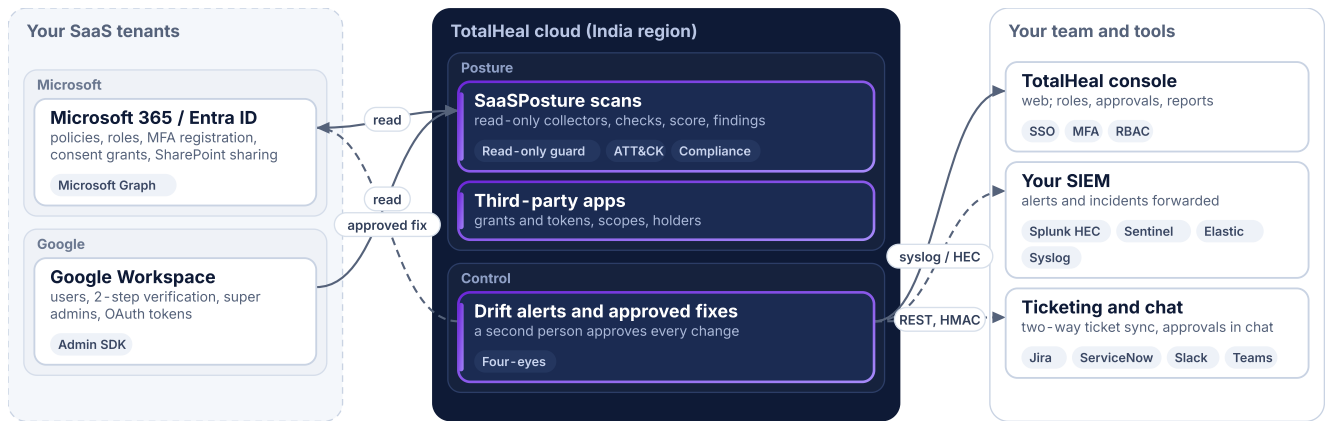
SaaSPosture reads the security settings of your Microsoft 365 / Entra ID and Google Workspace tenants with read-only access and checks them continuously: MFA, administrators, legacy authentication, app consent, guests, sharing and third-party apps. Every failing setting comes with the fix; drift raises an alert; and fixes TotalHeal applies need a second person's approval.

2 The challenge

Most breaches of Microsoft 365 and Google Workspace come from settings, not exploits: MFA that is registered but not required, legacy protocols that skip it, an administrator nobody uses, people allowed to grant any app access to their mailbox, files shared with links anyone can open. Settings drift as admins change them, and nobody notices until an attacker does.

The TotalHeal approach. SaaSPosture reads the settings of your Microsoft 365 / Entra ID and Google Workspace tenants through the connectors you already have, with read-only access, and checks them continuously. Each failing setting is a finding with the fix, its MITRE ATT&CK techniques and the compliance controls it maps to. The Professional tier adds the third-party app inventory and drift alerts; the Elite tier applies fixes after a second person approves.

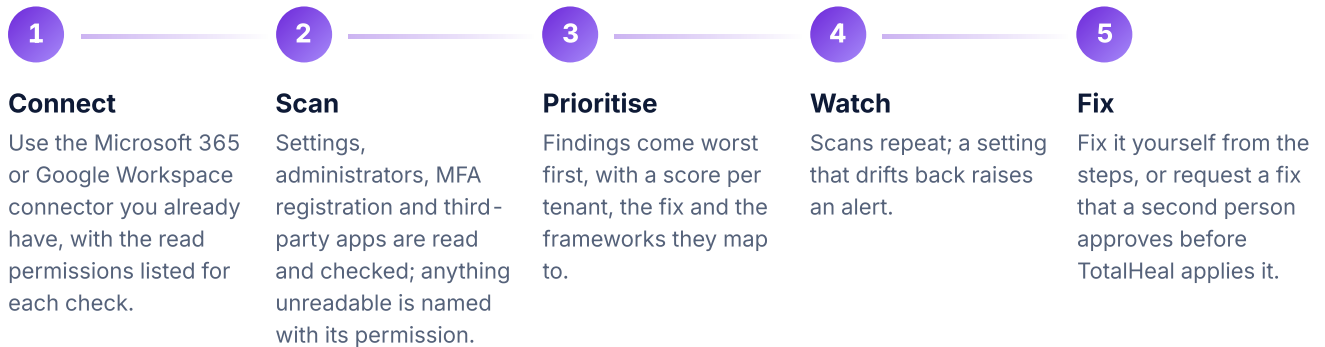
3 Architecture



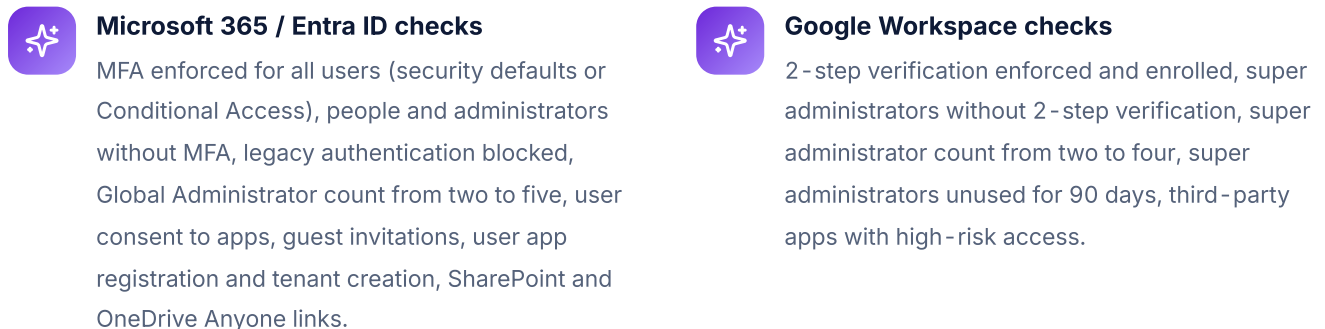
TotalHeal component
Your environment
TotalHeal cloud or edge
Third party
 Data
 Control, optional or on approval

Scans read each tenant's settings, administrators and app grants through the providers' APIs with read permissions only; fixes go out only after a second person approves.

4 How it works



5 Capabilities in detail





Read-only by design

Scans use read permissions only, and every scan request is checked before it leaves TotalHeal: anything that is not a read is refused. A setting the connector may not read is reported as not evaluated with the permission it needs — never guessed.



Mapped to frameworks

Each check maps to MITRE ATT&CK techniques and to controls of NIST 800-53, NIST CSF, ISO 27001, SOC 2, PCI DSS, CIS v8, DPDP and other packs in TotalHeal Compliance.



Drift alerts

After a clean scan, a critical or high setting that starts failing raises an alert in the same incident queue as endpoint, identity and cloud alerts, and goes on to your SIEM, ticketing and playbooks.



A score and a fix for every finding

A severity-weighted score per tenant and overall, findings worst first, the steps to fix each one in the admin centre, and a trend. Accept a risk with a reason and an optional end date; it reopens by itself.



Third-party app inventory

Every app people granted delegated access (Microsoft 365) or OAuth tokens (Google Workspace): its publisher and whether it is verified, its scopes in plain words, and how many people — or everyone, by administrator consent — granted it. Apps that can read or send mail, read or change every file, or change the directory come first.



Fixes with four-eyes approval

Request a fix — stop users consenting to apps, allow only administrators and Guest Inviters to invite guests, revoke an app's access — and a different person approves it before TotalHeal makes the change with the connector's credentials. Both decisions are kept in the audit log, and the tenant is scanned again.

Check	Resource	Account	Severity	ATT&CK	Status	First seen	Last seen
Administrator without MFA Microsoft Entra ID - Identity	admin1@contoso.example entra.user	Contoso Demo	Critical	T1078.004 T1110	Open	2m ago	1m ago
App from an unverified publisher holds high-risk access Microsoft Entra ID - Third-party apps	PDF Helper Free entra.app	Contoso Demo	Critical	T1528	Open	2m ago	1m ago
Super administrator without 2-step verification Google Workspace - Identity	old-admin@acme-gws.example gws.admin	acme-gws.example	Critical	T1078.004	Open	2m ago	2m ago
Users can consent to any app Microsoft Entra ID - Third-party apps	Contoso Demo entra.account	Contoso Demo	High	T1528 T1566.002	Open	2m ago	1m ago
Third-party app with high-risk access Microsoft Entra ID - Third-party apps	MailSync Pro entra.app	Contoso Demo	High	T1528 T1558.001	Open	2m ago	1m ago
Third-party app with high-risk access Microsoft Entra ID - Third-party apps	PDF Helper Free entra.app	Contoso Demo	High	T1528 T1550.001	Open	2m ago	1m ago
Legacy authentication is not blocked Microsoft Entra ID - Identity	Contoso Demo entra.account	Contoso Demo	High	T1110.003 T1078.004	Open	2m ago	1m ago
Users without MFA Microsoft Entra ID - Identity	Contoso Demo entra.account	Contoso Demo	High	T1078.004 T1110	Open	2m ago	1m ago

SaaSPosture findings for a demo organisation's Microsoft 365 and Google Workspace tenants. Real screenshot, demo data.

6 Security and data handling

Read-only scans

Every scan request is a read; anything else is refused before it leaves TotalHeal.

Nothing guessed

A setting that cannot be read is reported as not evaluated, with the permission it needs.

Two people for every change

A fix runs only after someone other than the requester approves it, and both are audited.

Your tenants only

Each organisation's findings, apps and fixes are visible to it alone.

7 Where it fits

MFA everyone thought was on

Find the users and administrators without MFA and the legacy protocols that bypass it.

Consent phishing

See which apps hold mail and file access for everyone, and revoke the unknown ones with approval.

Audit evidence

Show auditors the checks, their results over time and the controls they map to.

8 Deployment and system requirements



Cloud (SaaS)

Available

Scans run from the TotalHeal cloud against the providers' APIs.



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



Microsoft
365 / Entra
ID



Google
Workspace

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

Network and access

- A Microsoft Entra ID / Microsoft 365 or Google Workspace connector in TotalHeal with the read permissions above
- For fixes (Elite): the write permissions above, granted to the same app registration or service account

Alerts and tickets to

splunk>

Splunk



Microsoft
Sentinel



Elastic



Syslog /
CEF



Jira



ServiceNow



Slack



Microsoft
Teams

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



9 Technical specifications

Features	Included		
Microsoft 365 / Entra ID checks	✓ Included		
Google Workspace checks	✓ Included		
Read - only by design	✓ Included		
A score and a fix for every finding	✓ Included		
Mapped to frameworks	✓ Included		
Third - party app inventory	✓ Included		
Drift alerts	✓ Included		
Fixes with four - eyes approval	✓ Included		
Availability by tier	Essential	Professional	Elite
Microsoft 365 / Entra ID and Google Workspace checks, read - only: MFA and 2 - step verification, administrators, legacy authentication, consent, guests, tenant creation, SharePoint and OneDrive sharing	✓ Included	✓ Included	✓ Included
Score per tenant, findings with the fix, MITRE ATT&CK and compliance controls; accept a risk with a reason and an end date	✓ Included	✓ Included	✓ Included
Third - party app inventory: apps people granted access, their scopes, who holds them, high - risk access flagged	—	✓ Included	✓ Included
Drift alerts: a critical or high setting that starts failing raises an alert in the incident queue	—	✓ Included	✓ Included

Fixes TotalHeal applies after a second person approves: stop user consent, restrict guest invitations, revoke an app	—	—	 Included
List price per user per year	US\$12 · ₹1,140	US\$24 · ₹2,280	US\$36 · ₹3,430
Platforms and coverage			
Microsoft 365 / Entra ID	App registration with Microsoft Graph application permissions AuditLog.Read.All, Directory.Read.All, Policy.Read.All; SharePointTenantSettings.Read.All, DelegatedPermissionGrant.Read.All and Application.Read.All for sharing and apps		
Google Workspace	Service account with domain - wide delegation for admin.directory.user.readonly and admin.directory.user.security		
Fixes (Elite)	Policy.ReadWrite.Authorization and DelegatedPermissionGrant.ReadWrite.All (Microsoft 365); admin.directory.user.security (Google Workspace)		
Console	TotalHeal web console		
Deployment options			
SaaS (India region)	Available Scans run from the TotalHeal cloud against the providers' APIs.		
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	Member users of the connected Microsoft 365 and Google Workspace tenants		
Trial	30 days, up to 50 users		
Editions	SaaSPosture 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	A Microsoft Entra ID / Microsoft 365 or Google Workspace connector in TotalHeal with the read permissions above
Requirement 2	For fixes (Elite): the write permissions above, granted to the same app registration or service account

10 Getting started

- A Microsoft Entra ID / Microsoft 365 or Google Workspace connector in TotalHeal with the read permissions above
- For fixes (Elite): the write permissions above, granted to the same app registration or service account

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/saasposture

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.