

Email Security (Microsoft 365 and Google Workspace)

The phishing your mail filter lets through, caught and pulled out of the inbox

Catches phishing, malware and business email compromise in Microsoft 365 and Google Workspace mailboxes, and pulls malicious mail out of the inbox automatically — no MX record change.



TotalHeal
MailShield

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

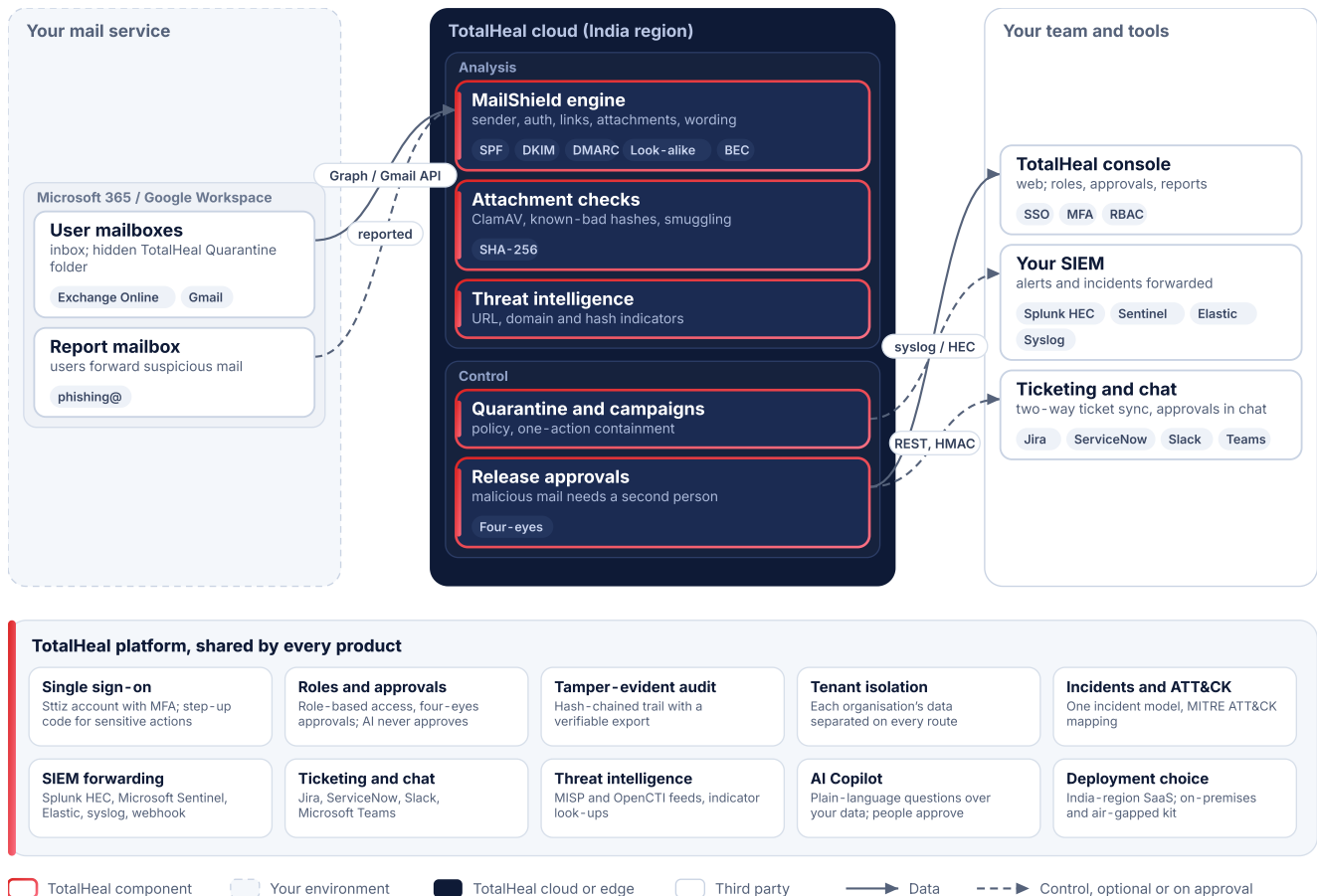
MailShield analyses every new message in Microsoft 365 and Google Workspace through their APIs — sender, authentication, links, attachments and wording — explains each verdict reason by reason, quarantines malicious mail automatically, groups campaigns across mailboxes, and lets a malicious message out only when a second person agrees.

2 The challenge

Most attacks still start in an inbox: a look-alike DocuSign or Microsoft sign-in page, an invoice that builds malware in the browser, a message from the managing director asking for an urgent transfer, a supplier whose bank details suddenly change. Built-in filters let these through because they come from clean, authenticated domains with no attachment to scan.

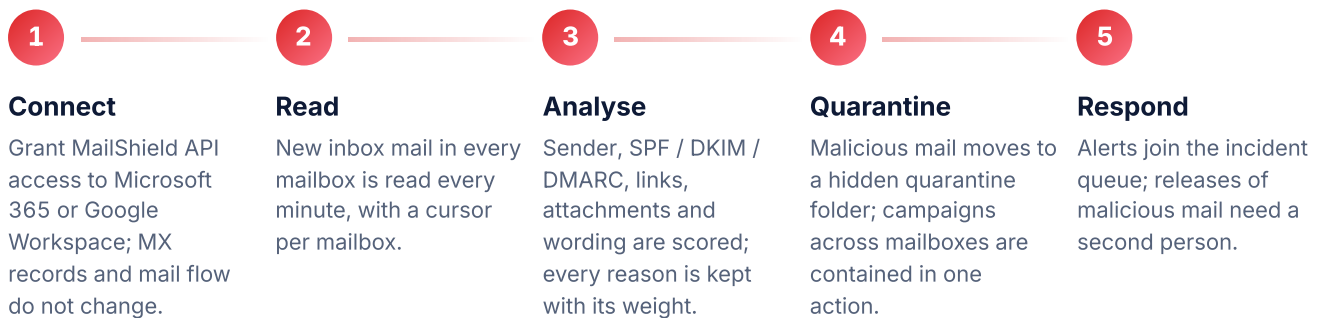
The TotalHeal approach. MailShield reads every new inbox message through the Microsoft 365 and Google Workspace APIs, analyses the sender, its authentication, every link, every attachment and the words of the message, explains each verdict reason by reason, and moves malicious mail to a hidden quarantine before the user acts on it.

3 Architecture



MailShield reads mail through the providers' APIs over HTTPS and moves malicious mail to a hidden folder; mail flow and MX records never change, and bodies are never stored.

4 How it works



5 Capabilities in detail

- API-based, no MX change**
 Connects to Microsoft 365 through Microsoft Graph (an app with Mail.ReadWrite and User.Read.All, or keyless with a federated credential) and to Google Workspace through a service account with domain-wide delegation. Mail flow and MX records stay exactly as they are.
- Every mailbox, every minute**
 Every user mailbox of the connection is listed automatically and new inbox mail is read every minute, round robin, with a cursor per mailbox so nothing is analysed twice or skipped.



Sender impersonation

Look-alike sender domains of your own domains, your suppliers and more than 40 global and Indian brands (typos, homoglyphs, extra words: micros0ft-support.com, tata-steel.com, docuSign-notice.net); a brand or one of your executives named in the display name of outside mail; a Reply-To or Return-Path that differs from the sender; a display name that shows a different address; a sender writing to your organisation for the first time.



Links

Every link checked against TotalHeal threat intelligence and your own indicator feeds (URL and domain); links whose text shows one site but go to another; look-alike, punycode, raw IP-address and URL-shortener links.



Business email compromise

Requests to change bank or payment details, urgent payment and transfer requests, gift-card requests and credential requests ("your password will expire", "verify your mailbox", KYC and PAN updates), in English and Indian business phrasing.



Automatic quarantine

Malicious mail (or suspicious mail too, if you choose) is moved to a hidden TotalHeal Quarantine folder or label; detect-only mode alerts without moving anything.



Campaigns

The same message from one sending domain reaching several mailboxes is grouped as a campaign, alerted once it reaches three mailboxes in a day, and quarantined everywhere in one action.



Authentication

SPF, DKIM and DMARC results as your mail service recorded them; mail that claims your own domain but fails authentication is flagged as spoofed.



Attachments

ClamAV scanning when a ClamAV server is configured; SHA-256 of every attachment checked against known-malicious hashes; HTML smuggling (a page that builds a file in the browser); HTML sign-in forms that post to another site; executables, scripts, disk images and shortcuts from outside; a document extension hiding an executable (invoice.pdf.exe); password-protected archives that cannot be scanned.



A score with every reason

Each message gets a score from 0 to 100 and a verdict — clean, suspicious or malicious — with a category (phishing, malware, business email compromise, impersonation) and every reason listed with its weight.



Release with four-eyes

Suspicious mail can be released by one person with a reason; releasing malicious mail needs a second person — never the requester, never a service account.



User-reported phishing

Employees forward suspicious mail to your report mailbox; MailShield analyses the original message inside the forward and always sends it to your SOC.



Your policy

Your domains, the executives attackers impersonate, your supplier and partner domains, allow and block lists. Malware is caught even from allowed senders.



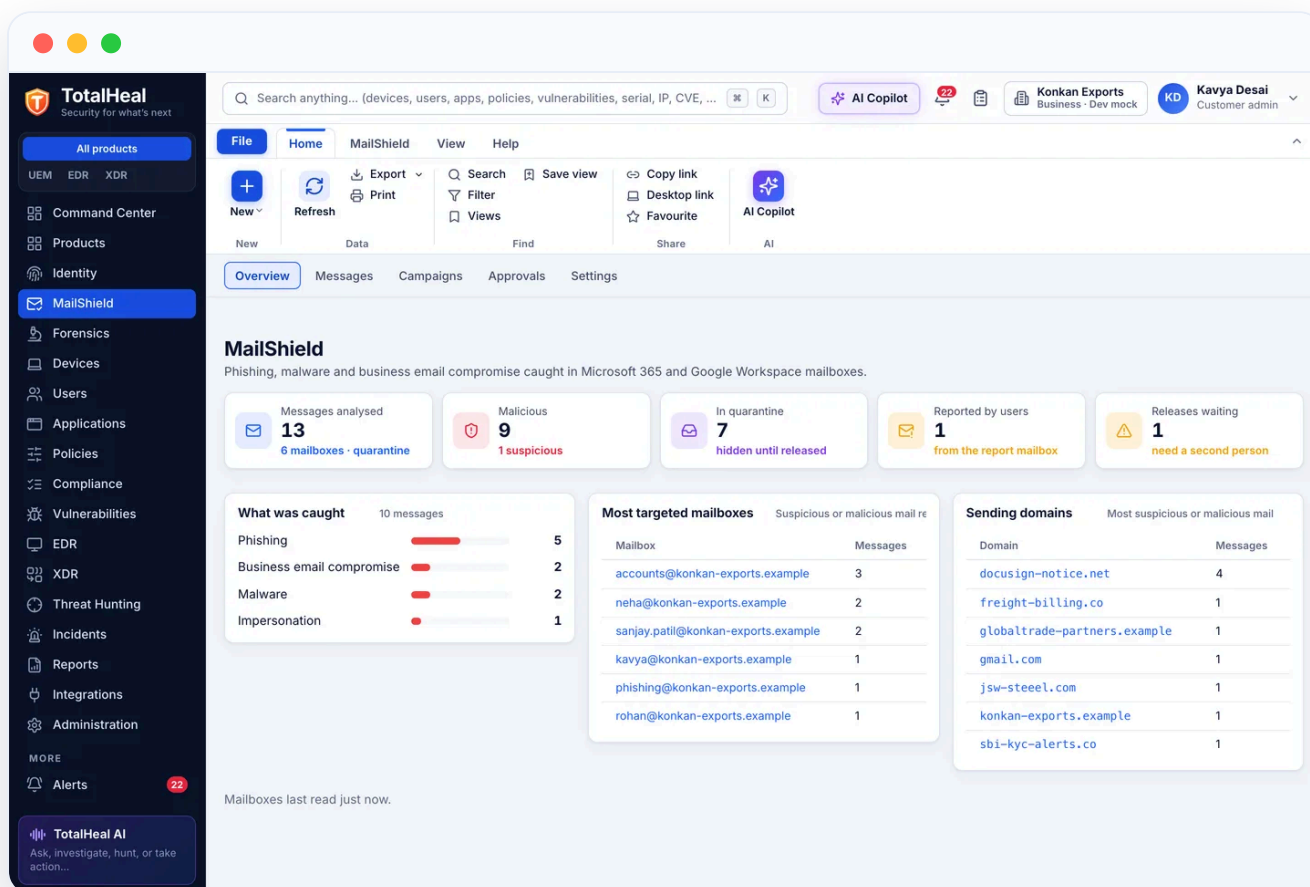
Alerts in the same incident queue

Every finding is an alert mapped to MITRE ATT&CK (T1566 phishing, T1684.001 impersonation, T1684.002 email spoofing), correlated with endpoint, identity and cloud alerts, and sent on to your SIEM, ticketing and playbooks.



Privacy by design

Message bodies and attachments are analysed in memory and never stored: MailShield keeps the headers, link hosts, attachment names and hashes, and the verdict. Credentials are sealed per organisation and never shown again.



The MailShield overview in the TotalHeal console (demo organisation). Real screenshot, demo data.

6 Security and data handling

Bodies are never stored

Messages and attachments are analysed in memory; only headers, link hosts, attachment hashes and the verdict are kept.

No mail-flow change

Nothing is routed through TotalHeal; if MailShield stops, mail keeps flowing.

Two people to release malware

A malicious message reaches the inbox only when a second person approves — never the requester, never a service account.

Every verdict explained

Each reason is shown with its weight, so analysts and users see why a message was stopped.

7 Where it fits

Payment fraud

Stop the “urgent transfer” from a managing director’s look-alike and the supplier whose bank details changed.

Credential phishing

Pull the DocuSign or Microsoft 365 sign-in look-alike out of every mailbox it reached.

User reports that reach the SOC

Every forwarded suspicious message is analysed and becomes an alert.

8 Deployment and system requirements



Cloud (SaaS)

Available

Single-region service.



On-premises

Available

Needs outbound HTTPS to Microsoft Graph or the Gmail API.



Air-gapped

Not applicable

Microsoft 365 and Google Workspace are cloud mail services.

Protected platforms



Microsoft 365



Google Workspace



Gmail

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

- Microsoft 365: an Entra ID app with Mail.ReadWrite and User.Read.All (admin consent), or a federated credential trusting TotalHeal
- Google Workspace: a service account with domain-wide delegation for gmail.modify and admin.directory.user.readonly
- Optional: a ClamAV server (clamd) for attachment scanning

Alerts and tickets to

splunk> Splunk



Microsoft Sentinel



Elastic



Syslog / CEF



Jira



ServiceNow



Slack



Microsoft Teams

9 Technical specifications

Features	Included	
API-based, no MX change	✓ Included	
Every mailbox, every minute	✓ Included	

Sender impersonation	✔ Included	
Authentication	✔ Included	
Links	✔ Included	
Attachments	✔ Included	
Business email compromise	✔ Included	
A score with every reason	✔ Included	
Automatic quarantine	✔ Included	
Release with four-eyes	✔ Included	
Campaigns	✔ Included	
User-reported phishing	✔ Included	
Your policy	✔ Included	
Alerts in the same incident queue	✔ Included	
Privacy by design	✔ Included	
Availability by edition		
	Business	Enterprise
Analysis, automatic quarantine, campaigns, four-eyes release, user reports, policy, alerts	✔ Included	✔ Included
Platforms and coverage		
Microsoft 365 (Exchange Online)	Microsoft Graph — app permissions Mail.ReadWrite, User.Read.All; or keyless (federated credential)	
Google Workspace (Gmail)	Gmail API and Admin SDK — service account with domain-wide delegation	
Attachment scanning	ClamAV (clamd) on your TotalHeal installation, plus known-bad hashes from threat intelligence	
Console	TotalHeal web console	
Deployment options		
SaaS (India region)	✔ Available Single-region service.	
On-premises control plane	✔ Available Needs outbound HTTPS to Microsoft Graph or the Gmail API.	
Air-gapped	✖ Not applicable Microsoft 365 and Google Workspace are cloud mail services.	
Licensing		
Priced per	Mailbox per year	

Counted	User mailboxes of the connected tenants
Trial	30 days, up to 25 mailboxes
Editions	MailShield is sold on its own, outside the editions.
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	Microsoft 365: an Entra ID app with Mail.ReadWrite and User.Read.All (admin consent), or a federated credential trusting TotalHeal
Requirement 2	Google Workspace: a service account with domain-wide delegation for gmail.modify and admin.directory.user.readonly
Requirement 3	Optional: a ClamAV server (clamd) for attachment scanning

10 Getting started

- Microsoft 365: an Entra ID app with Mail.ReadWrite and User.Read.All (admin consent), or a federated credential trusting TotalHeal
- Google Workspace: a service account with domain-wide delegation for gmail.modify and admin.directory.user.readonly
- Optional: a ClamAV server (clamd) for attachment scanning

Start a 30 days, up to 25 mailboxes 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/mailshield

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.