

Security Awareness Training

Training every employee — with evidence an auditor accepts

Short security courses for every employee, with signed certificates and reports for auditors. Phishing simulation coming.



TotalHeal
CyberAware

Contents

1 Executive summary

2 The challenge

3 Architecture

4 How it works

5 Capabilities in detail

6 Security and data handling

7 Where it fits

8 Deployment and system requirements

9 Technical specifications

10 Getting started

1 Executive summary

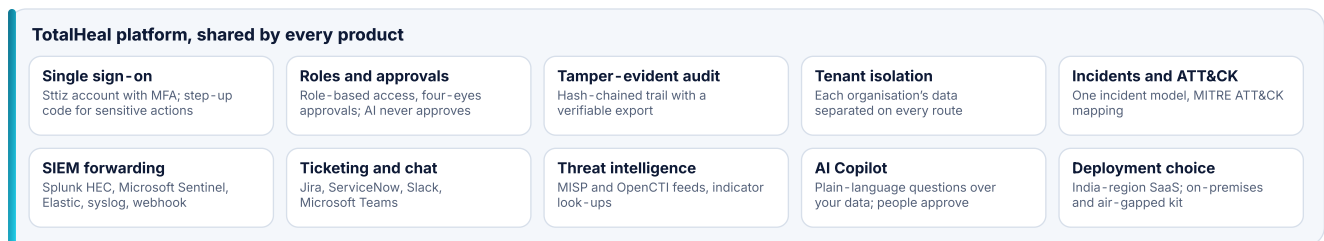
CyberAware gives every employee short courses that work on a phone, assigned by department with due dates and reminders, and keeps signed certificates and a compliance report as evidence. E-mail goes only to domains you have proved you own.

2 The challenge

Most incidents involve a person: a shared OTP, a reused password, a UPI collect request approved by mistake, a lost phone reported days late. Auditors expect organisations to train staff and keep evidence of it.

The TotalHeal approach. Courses of 5 to 10 minutes that work on a phone, assigned by department with due dates and reminders, with signed certificates and a compliance report. Training only in this release.

3 Architecture



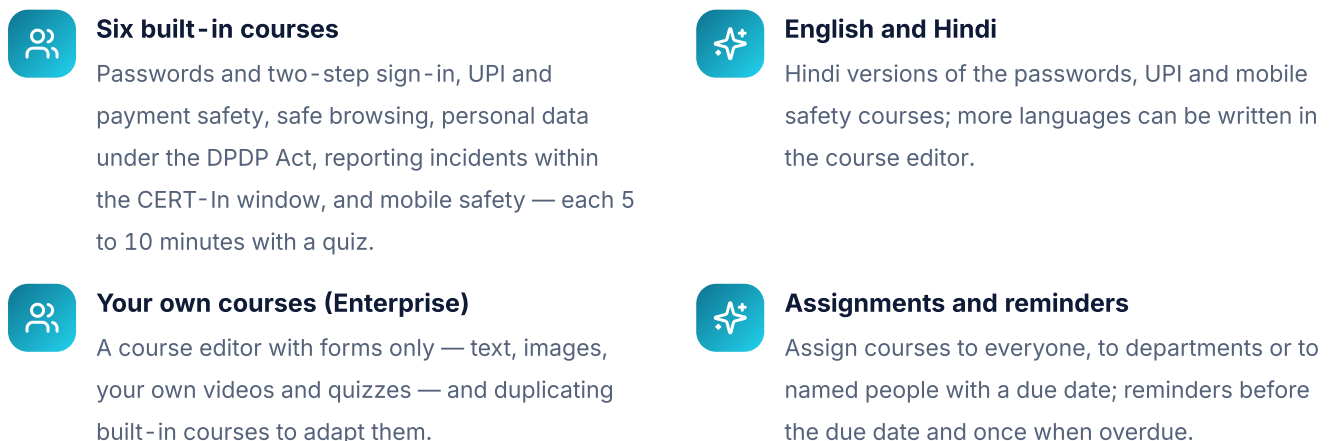
TotalHeal component
Your environment
TotalHeal cloud or edge
Third party
→ Data
 - - - → Control, optional or on approval

Employees open courses from an e-mail link on any device; mail goes only to verified domains; certificates verify on a public page.

4 How it works



5 Capabilities in detail





E-mail only to your verified domains

Sign-in links and reminders go only to your employees at domains you have proved you own with a DNS record. Nothing is sent anywhere else.



Learner portal

Employees open their courses from an e-mail link — no account or password — on a phone or computer, in light or dark.



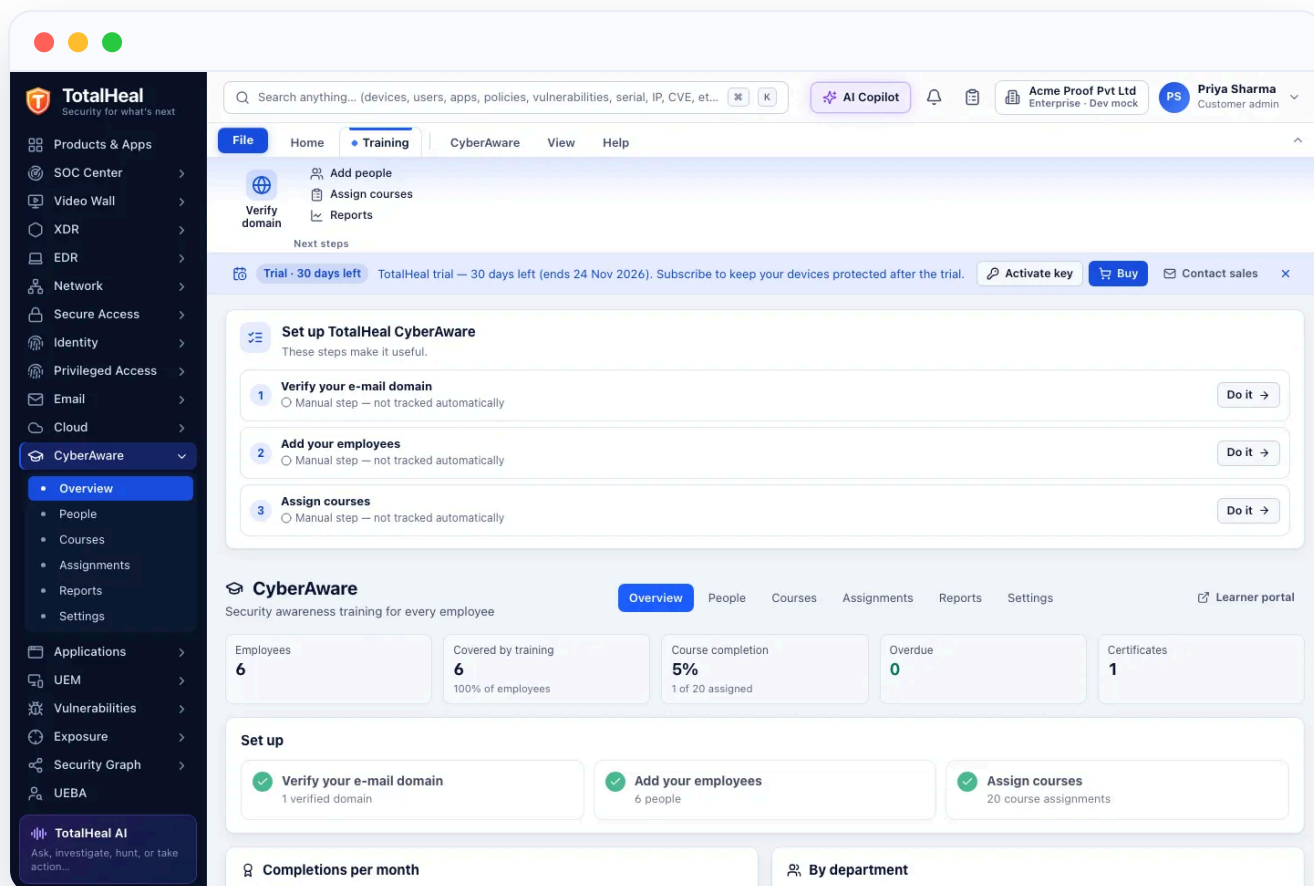
Signed certificates

A certificate of completion for every finished course, signed by TotalHeal CyberAware, with a public page to check that it is genuine.



Reports for auditors

Completion by department, course and person, a monthly trend and a downloadable compliance report listing the training evidence auditors commonly ask for. No official logos are used.



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

6 Security and data handling

Mail only to verified domains

Links and reminders go only to domains you own.

Evidence, not certification

The report is evidence of training, not a certification.

Certificates that verify

Each certificate is signed and has a public check page.

7 Where it fits

Annual training

Every employee trained with certificates on file.

DPDP and CERT-In awareness

Personal data and incident-reporting courses built in.

Hindi-speaking staff

Hindi versions of the passwords, UPI and mobile courses.

8 Deployment and system requirements



Cloud (SaaS)

Available

Training only; phishing simulation is not included yet.



On-premises

Available

With your own mail and DNS servers.



Air-gapped

Available

With your own mail and DNS servers.

Protected platforms



Any browser



Android 8.0 and later



iPhone, iPad
Apple MDM



Windows 10 / 11 (x64)



macOS 11 and later

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

- A DNS TXT record for each e-mail domain of your employees
- A list of employees (CSV with e-mail, name and department)

Alerts and tickets to

splunk> Splunk

Microsoft Sentinel

Elastic

Syslog / CEF

Jira

ServiceNow

Slack

Microsoft Teams

9 Technical specifications

Features	Included	
Six built-in courses	✓ Included	
English and Hindi	✓ Included	
Your own courses (Enterprise)	✓ Included	

Assignments and reminders	✔ Included	
E-mail only to your verified domains	✔ Included	
Learner portal	✔ Included	
Signed certificates	✔ Included	
Reports for auditors	✔ Included	
Availability by edition		
	Business	Enterprise
Built-in courses, assignments, reminders, learner portal, certificates, reports and compliance report	✔ Included	✔ Included
Your own courses (images, video, quizzes), duplicating built-in courses	—	✔ Included
API access with service accounts	—	✔ Included
Phishing simulation	Roadmap	Roadmap
Platforms and coverage		
Learner portal	Any modern browser on a phone or computer	
Console	TotalHeal web console	
Deployment options		
SaaS (India)	✔ Available Training only; phishing simulation is not included yet.	
On-premises / air-gapped	✔ Available With your own mail and DNS servers.	
Licensing		
Priced per	Employee per year	
Counted	Active employees in the training programme	
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	A DNS TXT record for each e-mail domain of your employees
Requirement 2	A list of employees (CSV with e-mail, name and department)

10 Getting started

- A DNS TXT record for each e-mail domain of your employees
- A list of employees (CSV with e-mail, name and department)

Start a 30 days 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/security-awareness

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.