

Identity Threat Detection & Response (ITDR)

Catching the attack that starts with a valid sign-in

Spot identity attacks in your sign-in data and act on them.



TotalHeal
IdentityWatch

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

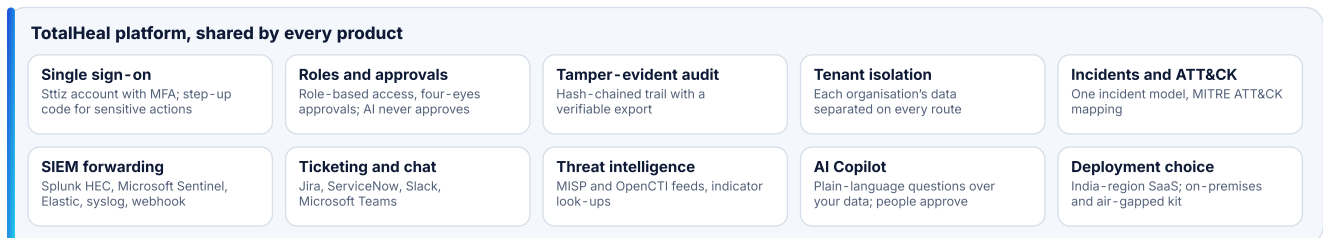
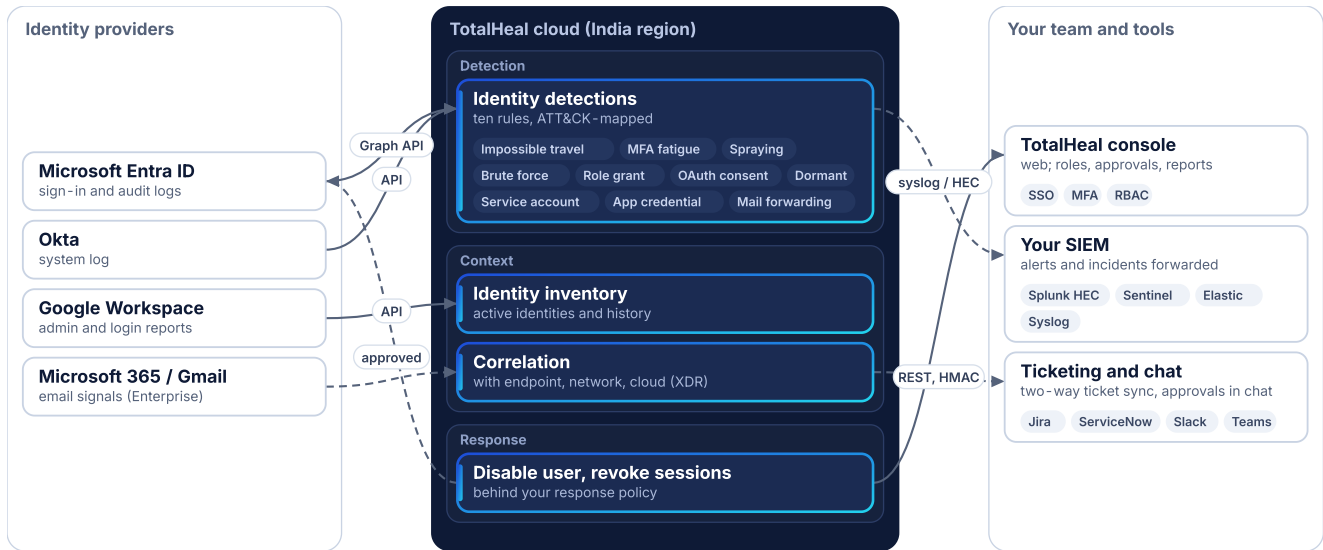
IdentityWatch reads your identity provider's sign-in and audit logs, detects ten identity attack patterns — from password spraying to malicious OAuth consent — and lets you disable a user or revoke sessions from the incident.

2 The challenge

Most intrusions now start with a valid sign-in: a sprayed password, a tired user approving the tenth MFA push, a malicious app granted access to mail. Identity providers record all of it, but few teams watch it.

The TotalHeal approach. IdentityWatch connects to your identity provider, keeps an inventory of active identities, detects identity attacks in the sign-in and audit data, and lets you disable a user or revoke sessions from the incident.

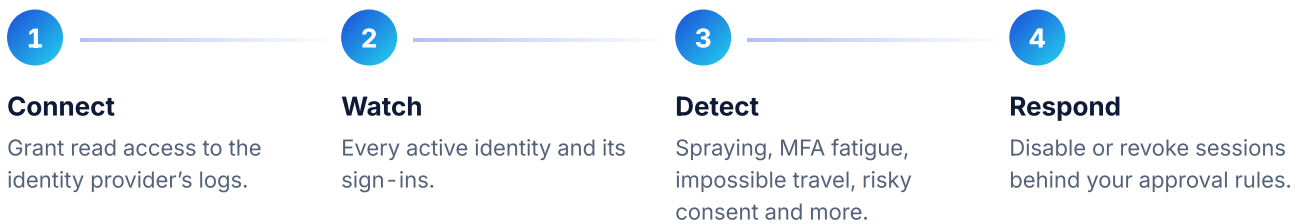
3 Architecture



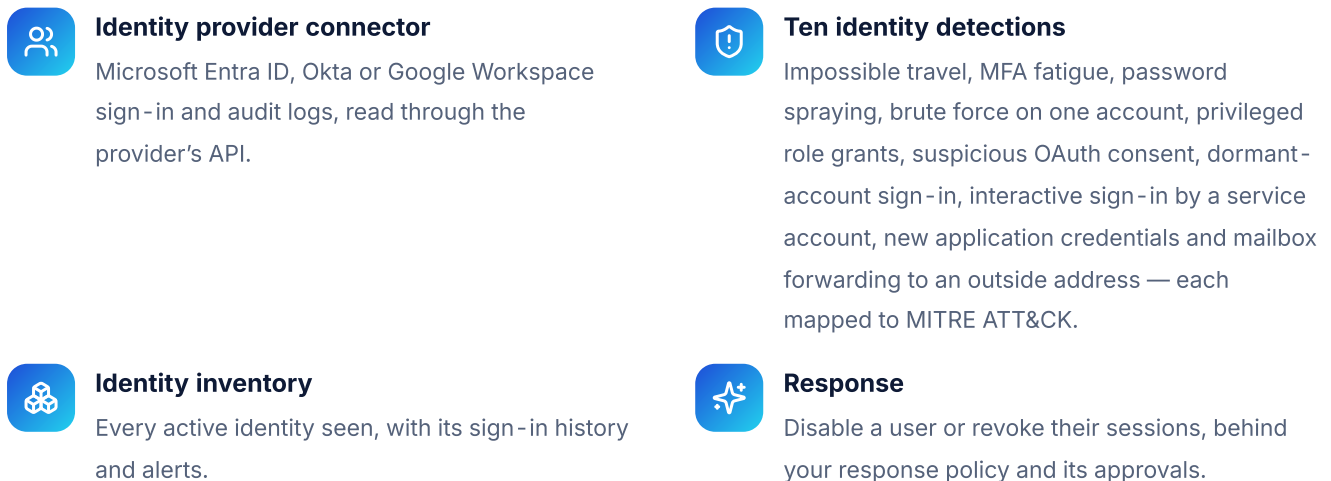
TotalHeal component
Your environment
TotalHeal cloud or edge
Third party
 Data
 Control, optional or on approval

TotalHeal reads sign-in and audit data through each provider's API; response goes back through the same API, behind approval.

4 How it works



5 Capabilities in detail





One incident

Identity alerts join the same incidents as endpoint, network and cloud alerts when ThreatFusion XDR is present.



Email signals (Enterprise)

Microsoft 365 and Google Workspace email signals for your users — the providers' own verdicts.

6 Security and data handling

Read-only by default

Detections need only read access.

Audit

Every action recorded and verifiable.

Approval for impact

Disabling users follows your response policy.

7 Where it fits

Microsoft 365 tenants

MFA fatigue and mailbox forwarding caught early.

Okta organisations

Password spraying across many accounts.

App consent abuse

Risky OAuth grants flagged.

8 Deployment and system requirements



Cloud (SaaS)

Available

Single-region service.



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
Entra ID



Okta



Google
Workspace



Microsoft
365

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

Network and access

- An administrator who can grant TotalHeal read access to the identity provider's logs

Alerts and tickets to

splunk>

Splunk



Microsoft
Sentinel



Elastic



Syslog /
CEF



Jira



ServiceNow



Slack



Microsoft
Teams



9 Technical specifications

Features	Included	
Identity provider connector	✔ Included	
Ten identity detections	✔ Included	
Identity inventory	✔ Included	
Response	✔ Included	
One incident	✔ Included	
Email signals (Enterprise)	✔ Included	
Availability by edition	Business	Enterprise
Connector, identity detections, inventory, response	✔ Included	✔ Included
Microsoft 365 and Google Workspace email signals	—	✔ Included
Platforms and coverage		
Identity providers	Microsoft Entra ID, Okta, Google Workspace	
Console	TotalHeal web console	
Deployment options		
SaaS (India region)	✔ Available Single-region service.	
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	Identity per year	
Counted	Active identities seen through the connector	
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	An administrator who can grant TotalHeal read access to the identity provider's logs

10 Getting started

- An administrator who can grant TotalHeal read access to the identity provider's logs

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/identity-security

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.