

SIEM & Log Management

A SIEM that never drops your logs because of the licence

Collect, search and alert on logs from firewalls, DNS servers, servers and identity providers.



TotalHeal
LogIntelligence

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

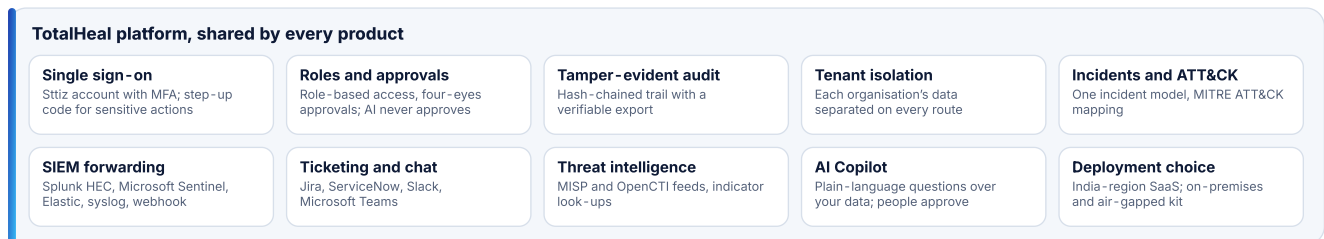
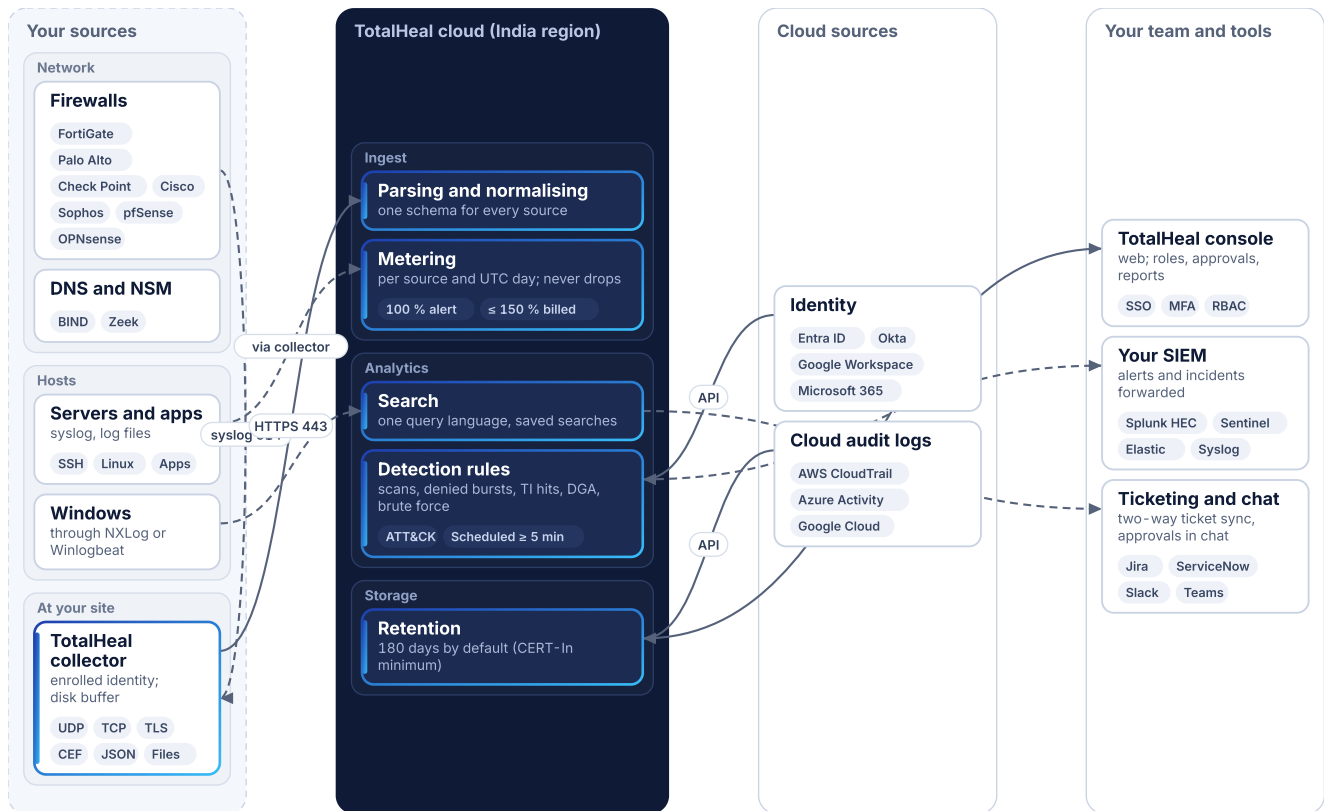
LogIntelligence collects syslog, CEF, JSON and log files through a collector at your site, parses common firewalls, DNS, identity and cloud sources, and alerts on built-in detection rules. Ingest is metered per day; above the licence you are alerted and billed, never silently dropped.

2 The challenge

Firewalls, DNS servers and servers write the evidence of most attacks into logs nobody reads until after an incident — and SIEM licences often punish you for sending more of them.

The TotalHeal approach. A collector at your site sends syslog, CEF and log files to TotalHeal, where they are parsed, searched and checked by built-in detection rules. Ingest is metered per day, and nothing is ever dropped because of the licence.

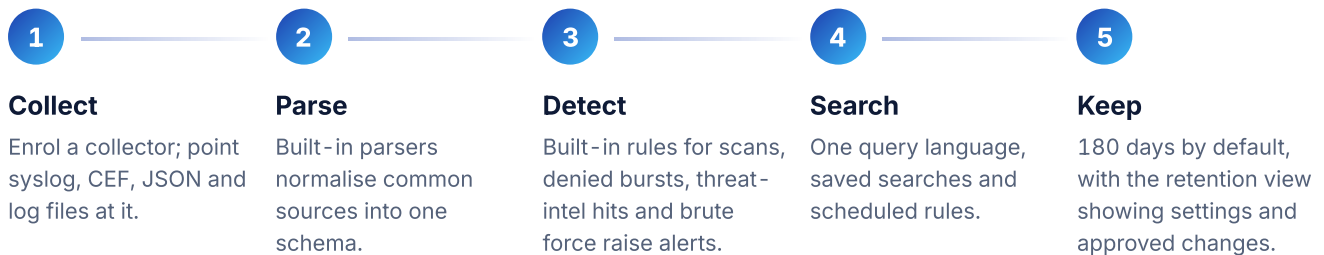
3 Architecture



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

Sources send to the collector at your site, which buffers on disk and forwards over HTTPS; cloud sources arrive through API connectors.

4 How it works



5

Capabilities in detail



Collector at your site

Syslog over UDP, TCP or TLS, CEF, JSON and log files, from one enrolled collector with its own device identity. If the cloud is unreachable it keeps the events on disk and sends them later.



Detection rules for network logs

Port scans and host sweeps, bursts of denied connections, allowed connections to threat-intelligence addresses, DNS queries for threat-intelligence domains, newly seen algorithm-like domains and login brute force from one address — each mapped to MITRE ATT&CK.



Metered ingest that never drops data

Accepted volume is measured per source and day. At 100 % of your licence you are alerted; up to 150 % the extra is billed; above that only sources that were not sending yet wait in their collector — existing sources keep sending.



Measured on our test system

In our 25 Oct 2026 run, one collector took 30,000 FortiGate traffic lines over syslog/TCP into a test service on a development machine in 23 seconds (about 1,300 events a second), metered at 670 bytes per event, so 1 GB a day is about 1.5 million such lines; a search over them answered in 124–145 ms. The port scan and the burst of denied connections in the replay each raised one alert.



Parsers for common sources

FortiGate, pfSense / OPNsense, CEF firewalls (Check Point, Palo Alto), BIND and Zeek DNS logs, SSH logs, Microsoft Entra ID, Okta, Google Workspace, Microsoft 365, AWS CloudTrail, Azure Activity and Google Cloud audit logs.



Search, saved searches and scheduled rules

One query language over every source; save searches and schedule them as rules that raise alerts. Business includes up to 10 scheduled rules, each run at most every 15 minutes.



Retention you can see

Events are kept 180 days by default, the CERT-In minimum; the retention view shows the setting, the floor and any approved change.

6

Security and data handling

Nothing dropped for the licence

At 100 % you are alerted; up to 150 % is billed; existing sources keep sending.

Its own identity

Each collector is an enrolled device with its own identity.

Survives outages

The collector keeps events on disk and sends them later.

7 Where it fits

CERT-In log retention

Firewall and server logs kept 180 days, searchable.

Firewall monitoring

Scans and threat-intel hits from FortiGate or pfSense raised as alerts.

Identity and cloud audit

Sign-in and cloud audit logs searchable next to network logs.

8 Deployment and system requirements



Cloud (SaaS)

Available

Single-region service; no archive tier yet.



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



Collector

x86_64,
aarch64,
systemd



FortiGate



Palo Alto
Networks



Check
Point



Cisco



Sophos



pfSense /
OPNsense



Zeek / BIND

Works with



Microsoft
Entra ID



Okta



Google
Workspace



Microsoft
365



AWS



Microsoft
Azure



Google
Cloud

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 Linux host at your site for the collector, reachable by your log sources
- Outbound HTTPS from the collector to TotalHeal

Alerts and tickets to

splunk>

Splunk



Microsoft
Sentinel



Elastic



Syslog /
CEF



Jira



ServiceNow



Slack



Microsoft
Teams

9 Technical specifications

Features	Included	
Collector at your site	✓ Included	
Parsers for common sources	✓ Included	

Detection rules for network logs	✔ Included	
Search, saved searches and scheduled rules	✔ Included	
Metered ingest that never drops data	✔ Included	
Retention you can see	✔ Included	
Measured on our test system	✔ Included	
Availability by edition		
	Business	Enterprise
Collector, parsers, search, saved searches, retention view	✔ Included	✔ Included
Built-in detection rules for firewall and DNS logs	✔ Included	✔ Included
Scheduled rules	Up to 10, every 15 min or more	Unlimited, every 5 min or more
Hunt packs, correlation studio, detection engineering	—	✔ Included
Platforms and coverage		
Collector	Linux with systemd, x86_64 or aarch64 (.deb / .rpm packages through our team until the public package repository opens)	
Sources	Anything that sends syslog, CEF or JSON, or writes log files; Windows events through NXLog or Winlogbeat	
Console	TotalHeal web console	
Deployment options		
SaaS (India region) with a collector at your site	✔ Available Single-region service; no archive tier yet.	
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	GB of log ingest per day	
Counted	Accepted bytes per UTC day (normalised events)	
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 Linux host at your site for the collector, reachable by your log sources
Requirement 2	Outbound HTTPS from the collector to TotalHeal

10 Getting started

- A Linux host at your site for the collector, reachable by your log sources
- Outbound HTTPS from the collector to TotalHeal

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/siem

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.