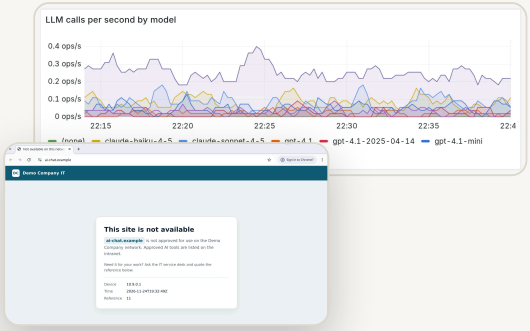
See and control how AI is used on your network.

titer shows your IT and security team which AI services, models and agents your people and systems use, and enforces your policy on them, together with web filtering, on infrastructure you run yourself.



01 SEE

Know what is used, by whom

- ✓ AI services, models and agent tools per device and network
- ✓ Token counts where the service reports them
- ✓ The site name of every connection, without decryption

02 CONTROL

Enforce the policy you have

- ✓ Approved AI services and models only, per team, network or time
- ✓ Single agent tools blocked where titer reads the traffic
- ✓ Web filtering with block pages people understand

03 PROVE

Have the record when asked

- ✓ Optional AI conversation record for your SIEM
- ✓ Credentials in request headers never written
- ✓ Grafana dashboard, Prometheus alerts, block events

AI-NATIVE OPERATIONS

Built for the AI era, both ways.

titer governs your organisation's AI traffic, and your own AI agents and assistants can operate titer through its built-in Model Context Protocol (MCP) interface, with guardrails, apart from the agent traffic it inspects.

- ✓ **Read** status, statistics and logs
- ✓ **Change policy live** if allowed: new connections follow at once, traffic keeps flowing
- ✓ **A token per agent** with three levels: read-only, policy changes, full
- ✓ **Every change logged** with the token's name and the client's address
- ✓ **Configuration changes checked** first and rolled back if the reload fails

Speaks the languages of AI

OpenAI · OpenAI-compatible servers · Anthropic · Google Gemini API · Ollama · vLLM · MCP

titer-extra; on traffic titer reads: to your own AI services, or decrypted where you decide. Names are trademarks of their owners.

Request a demo

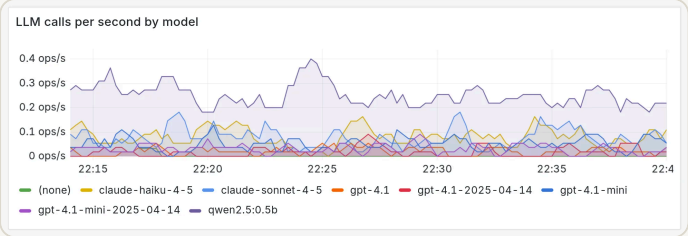
Demos, licensing and the free edition. General questions: hello@titer.network

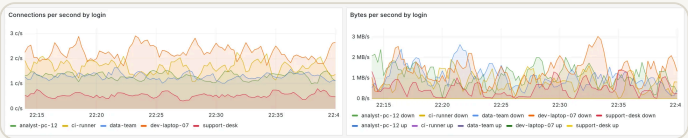
sales@titer.network

01 SEE

See which AI tools your team uses.

Services, models and agent tools per login, device and network, in the Grafana dashboard that ships with titer. Recognised by what they send, on any address or port.



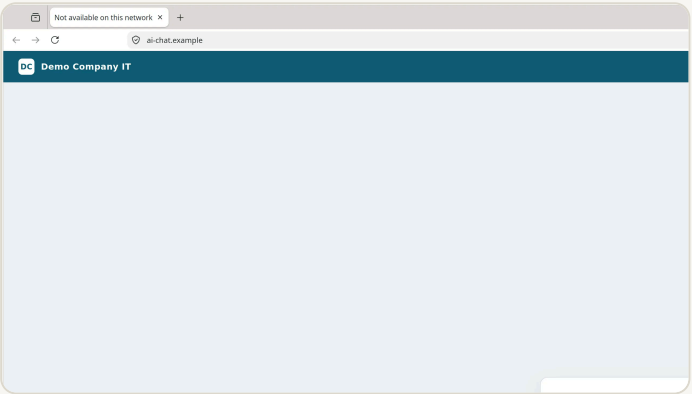


AI calls per second by model; activity per login.

02 CONTROL

Stop data going to unapproved AI.

Approved services and models only, per team, network or time of day, and a block page in your wording, also as a secure page on encrypted sites.



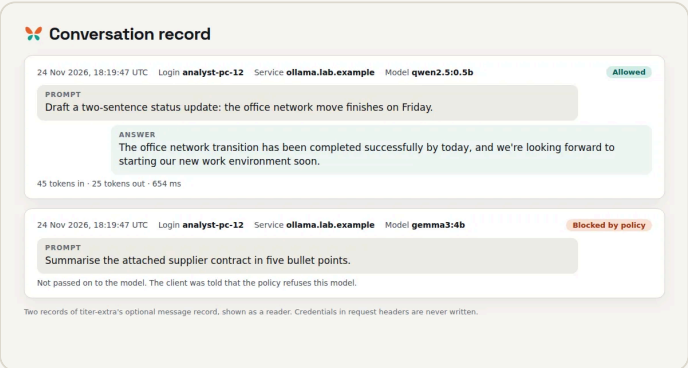
A branded block page in Firefox on an encrypted site.



03 GOVERN AGENTS

Put AI agents on a leash.

Single agent tools and unapproved models refused, with an error the tool can report; the agent goes on with the tools it may use. An optional conversation record for your SIEM.



The official OpenAI and MCP Python SDKs through titer-extra; two entries of the conversation record.

Two editions

titer: free edition

Web filtering, policy, routing and monitoring for any Linux network, free of charge for any use on your own networks. Binary packages are available on request now; public downloads are coming.

titer-extra: on request

Everything in titer, plus recognition and control of AI and agent traffic, selective decryption with your own certificate authority, the AI conversation record and operation by your AI agents. Licensing on request.

Capability	titer	titer-extra
WEB		
Filtering by name, blocklists, schedules, device groups	✓	✓
Block pages; clear refusals for encrypted sites	✓	✓
Secure block page for encrypted sites	–	✓
DNS filtering and HTTP/3 coverage	✓	✓
AI AND AGENTS		
AI services by name: allow or block	✓	✓
AI services, models and agent tools recognised by content	–	✓
AI usage policy per model, service, agent tool, team or time	–	✓
AI conversation record for your SIEM (optional)	–	✓
Operation by your AI agents, with per-agent permissions	–	✓
ENCRYPTED TRAFFIC AND OPERATIONS		
Policy without decryption	✓	✓
Selective decryption with your own certificate authority	–	✓
Live changes, central policy for many sites, metrics and dashboards	✓	✓

Where it runs

- ✓ On the gateway or router, with no device settings
- ✓ As a proxy or DNS filter, in containers and Kubernetes
- ✓ Linux distributions, OpenWrt, containers; x86, ARM and MIPS; both editions

Security and privacy

- ✓ Self-hosted; no telemetry: nothing is sent to the vendor
- ✓ By default only names, models and counts are recorded
- ✓ Decryption only for the services your policy names

2,539 B
of titer's memory per open relayed connection

46.7 Gbit/s
through a single relayed connection

~0.2 s
for a changed policy file to apply

0.55 MB
the free edition's program, x86-64

Measured: memory 24 Nov 2026, 10,000 relayed connections held open, 24-CPU x86-64 Linux; throughput 16 Nov 2026, loopback, Core i9-12900K, reload as tested, program built from the 1.0.0 source, stripped. Charts and conditions: titer.network/performance/

All 91 features

Every item is in both editions unless marked extra (titer-extra only).

TRAFFIC MODES AND DEPLOYMENT

- Transparent gateway
- HTTP proxy
- SOCKS5, SOCKS 4 and 4a, with UDP
- Proxy logins
- Name-based gateway
- Reverse proxy by name
- HTTP/3 (QUIC)
- IPv4 and IPv6
- PROXY protocol, in and out
- Any TCP protocol, unchanged

POLICY

- By site name and domain
- By device, network and entry point
- By destination address
- Schedules
- By encryption properties
- Predictable decisions
- Checked before it applies
- Decision logging per policy entry
- Custom decision logic extra

BLOCKLISTS AND CENTRAL POLICY

- Public blocklists
- Lists that follow their files
- Central policy and lists in Redis
- Central policy and lists in Riak
- Safe when the store is down
- Instant blocks

BLOCK PAGES AND ANSWERS

- Branded block page
- Branded error page
- Clear refusals for encrypted sites
- Choice of refusal
- Secure block and error pages for HTTPS extra

DNS

- DNS filtering
- Forwarding with failover
- A record of every query answered

TLS AND ENCRYPTED TRAFFIC

- Policy without decryption
- Selective decryption extra
- Your own certificate authority extra
- Real servers always verified extra
- Your choice for what cannot be decrypted extra
- Certificate rollout tools extra

AI AND AGENT TRAFFIC

- The well-known AI APIs extra
- MCP agent traffic extra
- Streamed, compressed and live connections extra
- AI usage policy extra
- Fail-closed by default extra
- Checked with real clients extra
- New AI APIs without a release extra
- Sandboxed extensions extra

MCP CONTROL AND AUTOMATION

- Built-in MCP interface extra
- A token per agent, three levels extra
- Live changes while traffic flows extra
- Safe configuration changes extra
- Recent logs for agents extra
- Command-line control

LOGGING, RECORDS AND SIEM

- A record per connection
- Block events
- AI conversation record extra
- Remote record destinations extra
- Privacy in records

MONITORING AND ALERTING

- Prometheus metrics
- Status as JSON
- Traffic per site and per client
- Grafana dashboard and alerts

ROUTING AND LOAD BALANCING

- Split routing
- Through other proxies
- Chosen servers
- Load balancing
- Health checks
- External decision service
- Bandwidth limits
- Header privacy

OPERATIONS

- Changes in about 0.2 seconds
- Faulty changes rejected
- Kubernetes ConfigMaps
- Log rotation
- Upgrades without dropped connections
- Graceful drain and shutdown
- Limits and timeouts
- Efficient at rest and under load
- Loop protection
- systemd and OpenRC

SECURITY HARDENING

- Runs unprivileged
- System call filter
- File access restricted
- Strict reading of untrusted traffic

PLATFORMS AND PACKAGES

- Linux packages
- Switch editions in place extra
- Container images
- Static binaries
- OpenWrt packages
- Builds sized to the device
- Handbook and tested examples

Integrations: Redis, Riak, Prometheus, Grafana, Syslog and the systemd journal, HTTP and TCP collectors, Vector and SIEM platforms, Kubernetes, systemd and OpenRC, OpenWrt, Model Context Protocol (MCP), PROXY protocol, AI providers and servers, Windows group policy.

Product names are trademarks of their owners.