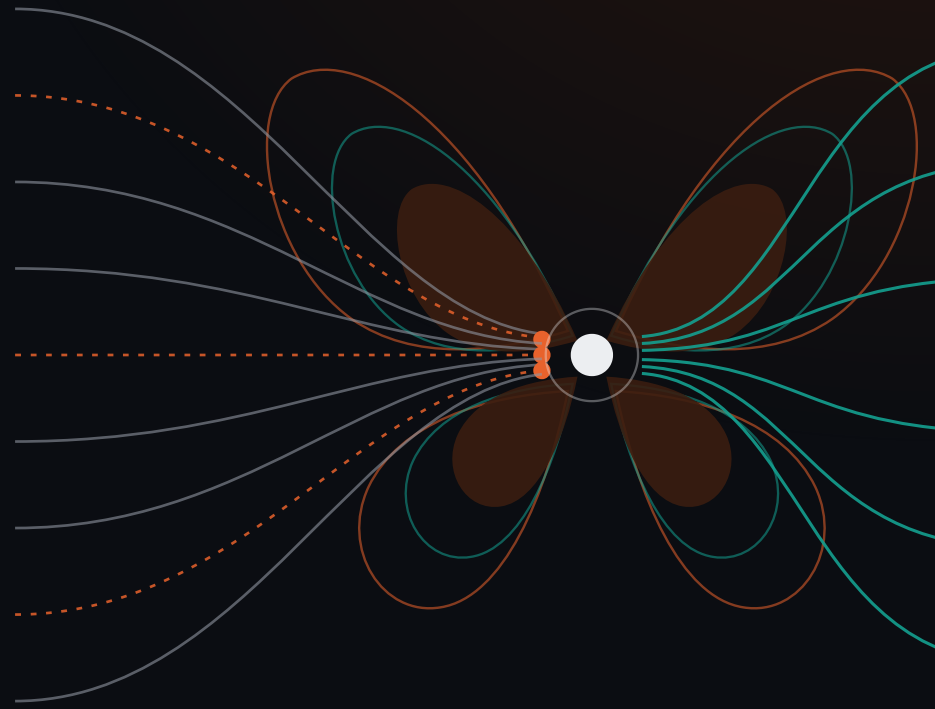
AI AND WEB TRAFFIC CONTROL

See and control how AI is used on your network.

titer shows which AI services, models and agents are used, and enforces your policy on them, together with web filtering, on infrastructure you run yourself.

Self-hosted. No telemetry. A free edition to start with.



THE PROBLEM

AI arrived on the network before the policy did.

Shadow AI

New AI tools appear every week. Nobody knows which services, models and agents are in use, or by whom.

Data leaving to AI services

Prompts carry source code, customer records and credentials. Once sent, they are outside your control.

Agents that act

Agents call tools that read, write and delete. A policy is needed for what they may do.

ONE CONTROL POINT

Web and AI traffic, decided where it leaves your network.

01 SEE

Know what is used

- ✓ AI services, models and agent tools per device
- ✓ Token counts where the service reports them
- ✓ The site name of every connection

02 CONTROL

Enforce the policy

- ✓ Approved AI services and models only
- ✓ Single agent tools blocked
- ✓ Web filtering with clear block pages

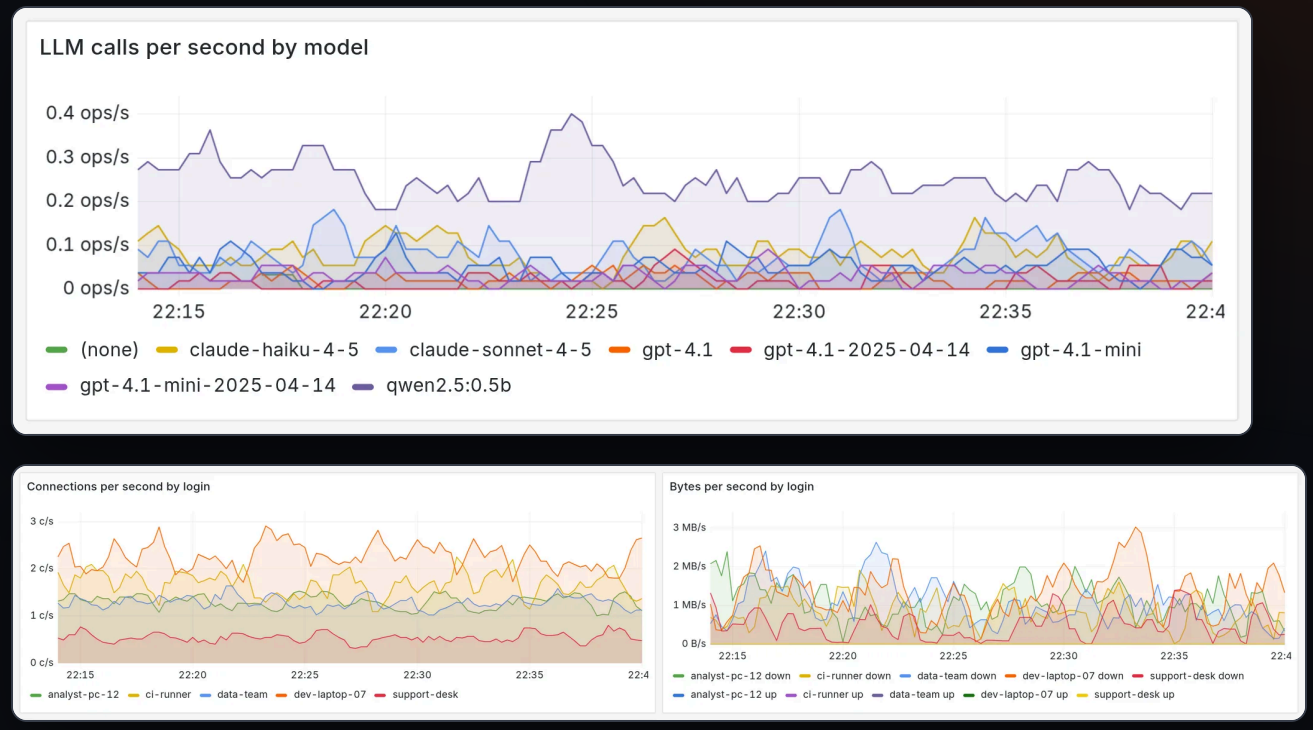
03 PROVE

Keep the record

- ✓ Optional AI conversation record
- ✓ Dashboards, alerts, block events
- ✓ On your own systems

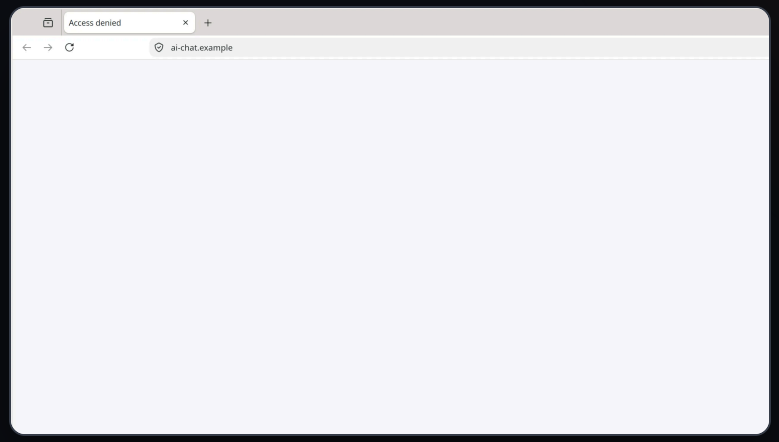
See which AI tools your team uses.

- **Services, models and agent tools** per login, device and network
- **Calls and tokens per model,** where the service reports them
- **In your own Grafana,** with the dashboard that ships with titer



Stop data going to unapproved AI.

- **Approved services and models only,** per team, network or time
- **A block page people understand,** in your wording
- **Secure on encrypted sites,** on devices that trust your CA

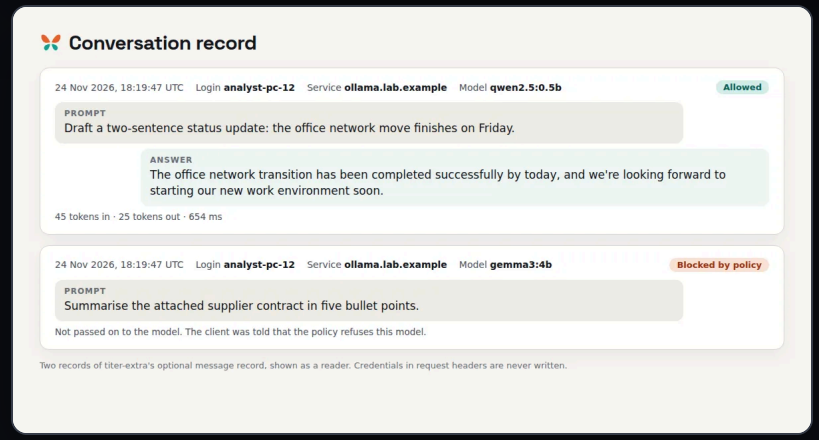


The built-in block page in Firefox, shown as secure.

Put AI agents on a leash.

- **Single agent tools refused,** such as anything that deletes
- **An error the tool can report,** not a hanging request
- **An optional conversation record** for your SIEM

```
analyst@pc-12:~/work$ python3 ask.py qwen2.5:0.5b "Say hello in five words."
Hello! How can I help you today?
analyst@pc-12:~/work$ python3 ask.py gemma3:4b "Summarise the attached contract."
PermissionDeniedError: Error code: 403 - denied by titer rule 2
analyst@pc-12:~/work$ python3 cleanup_agent.py
connected to files-server 2.0.1
tools: delete_dir, delete_file, list_files, read_file, write_file
list_files -> /docs/plan.txt  /docs/readme.txt  /tmp/scratch.txt
read_file /docs/plan.txt -> Step one.
delete_file /docs/plan.txt -> MCPError: denied by titer rule 6 (code -32001)
list_files -> /docs/plan.txt  /docs/readme.txt  /tmp/scratch.txt
analyst@pc-12:~/work$
```



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

AI USAGE CONTROL · TITER-EXTRA

Say yes to AI, on your terms.

- **Recognised by what they send,** not by a list of addresses: self-hosted models and new providers that speak a supported API
- **Allow approved services and models,** per team, network or time of day
- **Block single agent tools,** prompts or resources where titer reads the traffic; the agent goes on with the others
- **Clear permission errors** for blocked requests, no hanging tools
- **Fail-closed by default:** unreadable AI traffic is not waved through where a policy blocks

Coverage

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

Checked with real clients, among them the official OpenAI, Anthropic, Ollama and MCP SDKs, Claude Code, Codex and Gemini CLI. Product names are trademarks of their owners.

AI-NATIVE OPERATIONS · TITER-EXTRA

Built for the AI era, both ways.

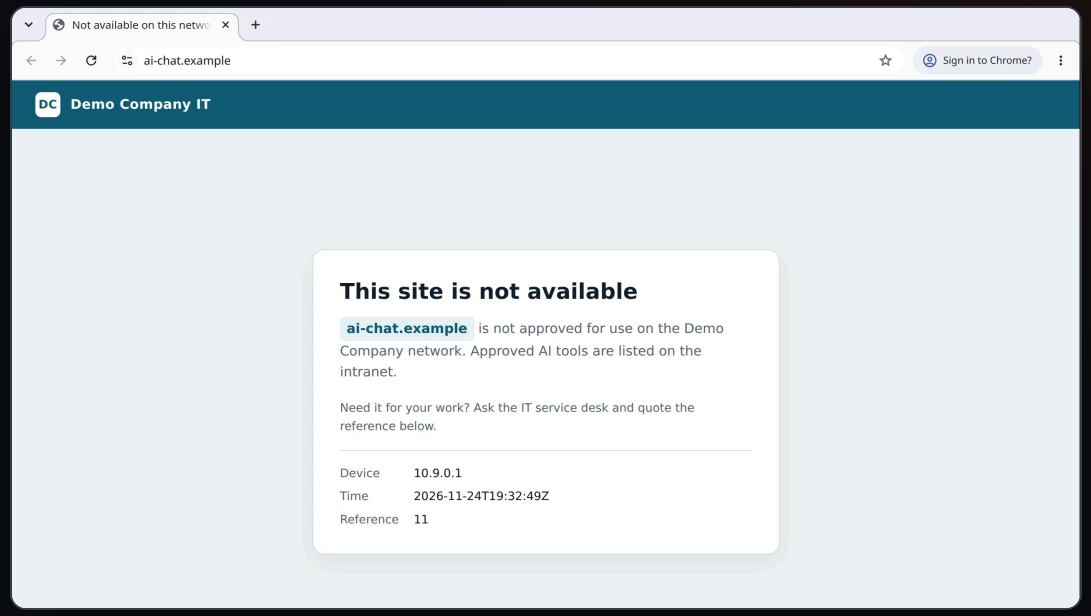
titer governs your organisation's AI traffic, and your own AI agents and assistants can operate titer through its built-in Model Context Protocol (MCP) interface, with guardrails. It is titer's own control interface, separate from the agent traffic titer inspects.

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

WEB FILTERING · BOTH EDITIONS

When the policy says no, people see why.

- Sites, domains and public blocklists
- Schedules, device groups and networks
- Web traffic, DNS and HTTP/3 under one policy
- Block pages in your wording, with a reference for the helpdesk
- A refusal the browser names for encrypted sites; a secure block page with titer-extra



A branded block page in Chrome on an encrypted site.

ENCRYPTED TRAFFIC

See into encrypted traffic only where you decide to.

Without decryption · both editions

Filtering, routing and records by destination name. Prompts, models and tool calls stay unseen. The free edition never decrypts.

Selective decryption · titer-extra

Only the services your policy names, on devices that trust your own certificate authority. The real server is always verified first; everything else passes untouched. Apps that pin their certificates cannot be decrypted.

DEPLOYMENT

Runs where your traffic already passes.

Gateway or router

No settings on the devices.

Proxy or DNS filter

For browsers, AI tools and SDKs, with logins if needed.

Containers and fleets

Kubernetes, and many sites under one policy.

Both editions: Debian, Ubuntu, Fedora, RHEL, CentOS Stream and Alpine packages, OpenWrt packages, a container image and static binaries; x86-64, ARM and MIPS. Linux only; Windows, Linux and Android devices checked as clients.

SECURITY AND PRIVACY

Your traffic, your records, your infrastructure.

- **Self-hosted, no telemetry:** nothing is sent to the vendor
- **Little by default:** names, models and counts
- **Conversation record** only when switched on
- **No credentials** from request headers in any record
- **Hardened:** unprivileged, confined by the kernel's sandboxing where available

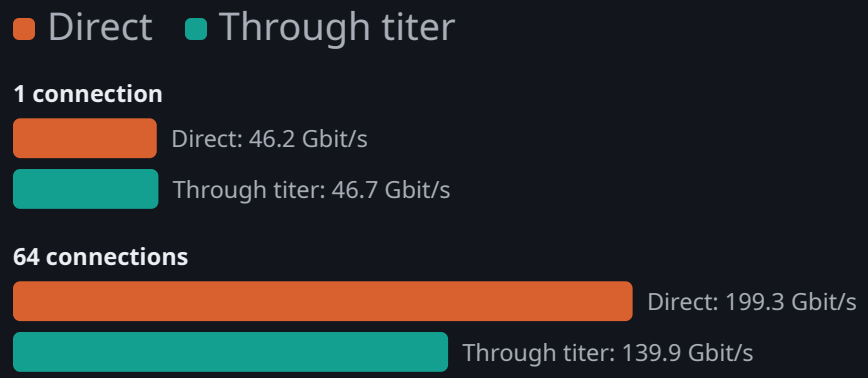


An alert firing in Grafana.

MEASURED

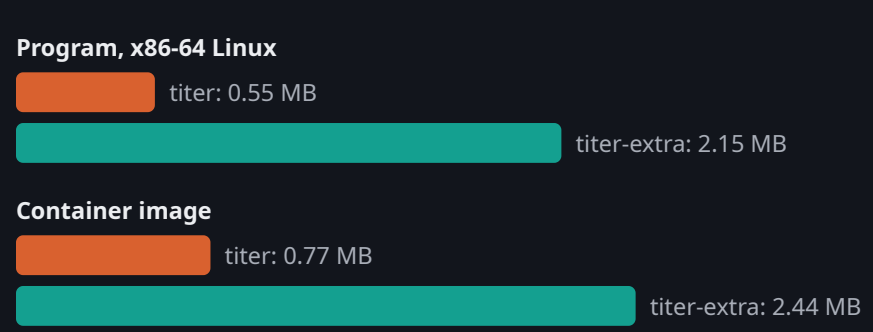
Light enough for a router, ready for a data centre.

Throughput through titer, compared with a direct connection



Measured 16 November 2026: Intel Core i9-12900K (24 CPUs), Linux 7.0, loopback interface, the free edition with 8 workers on 8 CPUs, the load generator and the servers on other CPUs, 10 s per test. Repeated runs vary by about 10 %, the 64-connection test more. Results depend on hardware and traffic.

Size of each edition



Version 1.0.0, read 24 November 2026: the program built from the release source for x86-64 Linux (GCC 13.3, stripped); the container images titer:1.0.0 and titer-extra:1.0.0 as the container engine reports them. titer-extra holds the AI decoding, decryption and agent control the free edition does not have.

ALL FEATURES · 1 OF 2

Everything titer and titer-extra do.

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

Unmarked: both editions. extra : titer-extra only.

ALL FEATURES · 2 OF 2

Everything titer and titer-extra do.

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

Unmarked: both editions. extra : titer-extra only.

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.

EDITIONS AND LICENSING

No cost to start. AI control when you need it.

Capability	titer	titer-extra
Web filtering, block pages, DNS and HTTP/3	✓	✓
Live changes, central policy, metrics and dashboards	✓	✓
AI services, models and agent tools: recognised and controlled	–	✓
Selective decryption with your own CA	–	✓
AI conversation record for your SIEM	–	✓
Operation by your AI agents (MCP), per-agent permissions	–	✓

titer: free of charge for any personal or business use on your own networks and systems; a licence is needed to offer it as a service or to bundle it into a product or device; copies only from the official source; packages on request now. titer-extra: separate licence agreement, on request.

NEXT STEP

See titer on your own traffic.

Request a demo, or talk to us about licensing for your organisation, your customers or your devices.

sales@titer.network

titer.network · general questions: hello@titer.network

