

Secure AI · Cloudflare, managed by FirstNet

Say yes to AI. Keep your data.

Your people already use ChatGPT, Claude and Gemini, often without IT knowing. Cloudflare shows you which AI tools are in use and puts guardrails around them. FirstNet designs, deploys and runs it for you.

Shadow AI

see which AI tools are in use, and by whom

By identity

allow, block, isolate or redirect each AI app

Every prompt

checked in real time for sensitive data

1 provider

one FirstNet contract and one escalation path

Sound familiar?

- Staff paste customer data or source code into public AI tools
- You don't know which AI apps are in use, or by whom
- Blocking AI outright pushes people onto personal devices
- Approved AI platforms were set up quickly and never reviewed
- Auditors ask how AI use fits your POPIA and ISO controls

Guardrails, not a ban. Steer people to approved AI tools and stop sensitive data at the prompt, so work keeps moving.

One platform, three ways to govern AI use

See AI use

Find sanctioned, unsanctioned and in-review AI apps, who uses them and how usage is trending.

Gateway (SWG) · CASB · Shadow AI reporting

Control access

Allow, block, isolate or redirect AI apps by user, group and device, wherever people work.

Access policies · Browser Isolation · Entra ID, Okta, Google

Protect your data

Inspect prompts and uploads to stop personal information, source code and regulated data, and flag jailbreak attempts.

Prompt inspection · DLP · AI security posture management

Start where it hurts, then expand. Most organisations begin with shadow AI discovery, then add prompt and data controls.

What FirstNet does for you

1

Discover

Find the AI tools in use and the data at risk.

2

Design

Agree which tools to allow and what data stays in.

3

Deploy

Identity-based policies, logging first, then blocking.

4

Tune

Refine prompt and DLP rules with your team.

5

Manage

Reporting, policy changes and escalation into Cloudflare.

Why FirstNet

- ✓ **One accountable provider** for connectivity, cloud, security and voice, with one Rapid Response entry point.
- ✓ **Joined up with your network.** AI controls on FirstNet SD-WAN and internet, and Sovereign AI when prompts must stay in South Africa.
- ✓ **Local engineers** aligned to your change windows and South African working hours.
- ✓ **Cloudflare MSSP partner**, ICASA-licensed group, ISO 27001:2022 and ISO 9001.

Getting started

1

AI security assessment. Which AI tools are in use, what data is at risk and where the gaps are.

2

Policy design. We agree approved tools, guardrails and data rules with your team.

3

Scoped pilot. Prove it with one team before a wider rollout.

What we will need from you: your identity provider details, your approved AI tools (if any) and a named technical contact.

Let's elevate your AI security.

Book an AI security assessment with your FirstNet account team.

firstnet.co.za →

0861 989 896 · sales@firstnet.co.za

Cloudflare is a cloud platform and is not a managed SOC or MDR service. Features, availability and outcomes depend on solution design, scope and the signed customer agreement. These controls support, but do not guarantee, compliance with POPIA or ISO standards; compliance remains a shared responsibility. Some controls need the Cloudflare WARP client on managed devices. Cloudflare and the Cloudflare logo are trademarks of Cloudflare, Inc. All other names belong to their respective owners.