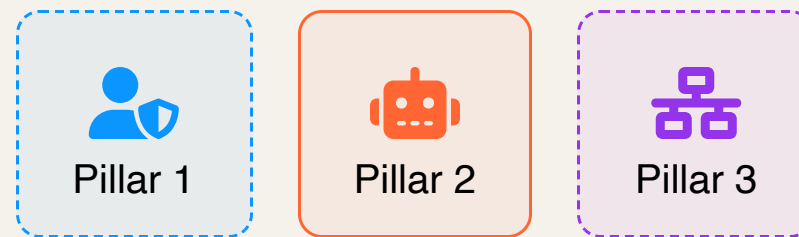


AI Security

Bill of Materials

Product requirements for each pillar and complete solution



Overall BOM — All Three Pillars

Product / SKU	Description	Required For	Notes
Cloudflare One (Internal)	Zero Trust platform — Gateway, Access, WARP	Pillar 1, Pillar 3	Seats-based. Advantage tier recommended
DLP	Data Loss Prevention profiles & scanning	Pillar 1, 2, 3	Included in all Internal tiers
Browser Isolation	Remote browser rendering on Cloudflare edge	Pillar 1	Included in Advantage/Premier
AI Gateway	LLM API proxy with observability, caching, rate limiting	Pillar 2	Core features free. Advanced features paid
Enterprise WAF	Web Application Firewall foundation	Pillar 3	Required for AI Security for Apps
AI Security for Apps	Prompt injection scoring, PII detection, unsafe topics	Pillar 3	Requires WAF or AI Gateway. Separately licensed
MCP Server Portal Open Beta	Zero Trust gateway for MCP servers	Pillar 3	Built on Access infrastructure

Pillar 1 BOM: End-User Protection

Employees using ChatGPT, Claude, Copilot, Gemini via browser

Product / SKU	Purpose	Required?	Notes
Cloudflare One (Interna)	Gateway + Access + WARP client deployment	Required	Minimum: Essentials tier
DLP	Scan prompts for PII, secrets, sensitive data	Required	Included in all Interna tiers
Browser Isolation	Block copy/paste, disable uploads to AI tools	Recommended	Included in Advantage/Premier
CASB	Discover shadow AI usage across organisation	Recommended	SaaS apps only
Log Explorer	Retain and search AI interaction logs	Optional	Add-on for all tiers

Minimum Pillar 1
Interna Essentials (DLP included)

Recommended Pillar 1
Interna Advantage (adds Browser Isolation, File Sandboxing)

Pillar 2 BOM: App & API Security

Applications and agents calling LLM APIs programmatically (OpenAI, Anthropic, etc.)

Product / SKU	Purpose	Required?	Notes
AI Gateway	Unified endpoint, caching, rate limiting, observability	Required	Core features free on all plans
DLP (via AI Gateway)	Scan prompts AND responses for sensitive data	Required	Free on all plans. Native to AI Gateway

Key Commercial Note

AI Gateway **core features are free** on all plans (caching, rate limiting, observability, DLP). Advanced features require paid tier. Not included in Cloudflare One subscriptions.

Minimum Pillar 2
AI Gateway

Pillar 2 is standalone
Does not require Interneta/Cloudflare One

Pillar 3 BOM: Agentic & MCP Security

AI agents using MCP to access tools, databases, APIs — both outbound (tool calls) and inbound (public MCP servers)

Product / SKU	Purpose	Required?	Notes
MCP Server Portal Beta	Zero Trust gateway for MCP servers	Required	Open Beta. Built on Access
Cloudflare One (Internal)	Access policies for MCP Portal auth	Required	Identity-based access control
DLP	Scan tool outputs for sensitive data	Required	Included in all Internal tiers
WAF or AI Gateway	Foundation for AI Security rules	Required	Either product enables AI Security for Apps
AI Security for Apps	Prompt injection scoring, PII detection	Required	Requires WAF or AI Gateway. Separately licensed
AI Gateway	Observability on LLM calls from agents	Recommended	For the LLM leg of agent traffic

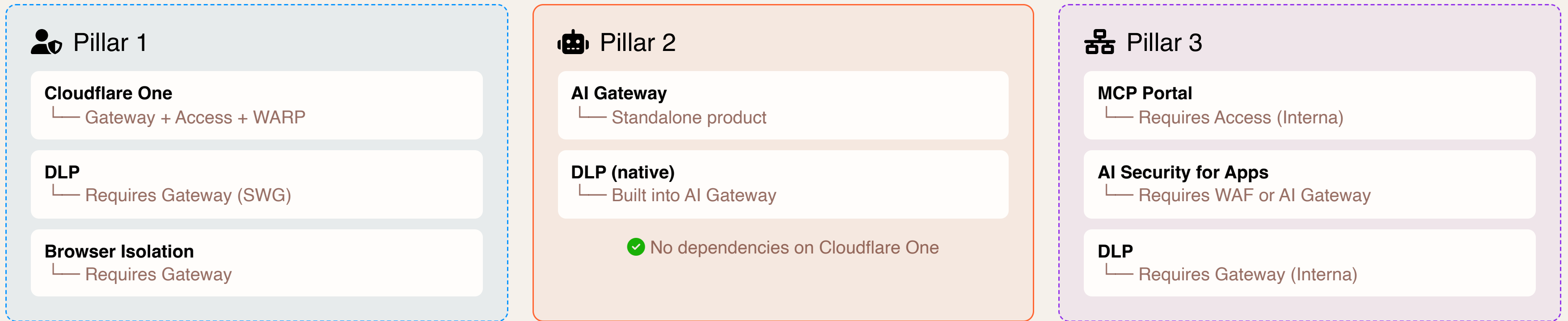
BOM by Scenario

Scenario	Products Required
<p>Pillar 1 Only</p> <p>End-User Protection</p>	Interna Essentials (DLP included). Advantage adds Browser Isolation
<p>Pillar 2 Only</p> <p>App & API Security</p>	AI Gateway
<p>Pillar 3 Only</p> <p>Agentic & MCP</p>	Interna + (WAF or AI Gateway) + AI Security for Apps + MCP Portal
<p>All 3 Pillars</p> <p>Complete AI Security</p>	Interna + AI Gateway + AI Security for Apps + MCP Portal

⚠️ Key Commercial Notes

- **AI Gateway** — core features free, advanced features paid
- **AI Security for Apps** — requires WAF or AI Gateway, separately licensed
- **MCP Server Portal** — Open Beta (since Aug 2025)
- **DLP** — included in all Interna tiers (Essentials, Advantage, Premier)

Product Dependencies



Pillar 3 has the most dependencies – requires Interna (Zero Trust) plus WAF or AI Gateway

Scope note: AI Security for Apps protects AI endpoints you run. It does NOT protect employees using third-party AI (ChatGPT, Claude) – that's Pillar 1's job.