PARTNER TECHNICAL BRIEFING · CONFIDENTIAL

Cloudflare for Cythera

Platform Architecture & AI Security
A technical briefing for security architects

Part 1 — Cloudflare Platform

Part 2 — AI Security

Jason Clarke · Senior Solutions Engineer · Cloudflare APAC

PART 1

The Cloudflare Platform

Network scale · Security architecture · Technical capabilities

The Network Underneath Everything

Every Cloudflare product runs on the same global network — not a collection of regional gateways. This is the architectural difference that matters for latency-sensitive markets like Western Australia.

330+
Cities in 125+ countries

500
Tbps network capacity (April 2026)

13,000+
Network interconnects globally

95%
Of Internet population within 50ms

THREAT INTELLIGENCE SCALE

215 billion cyber threats blocked per day (Q4 2025 average)

Largest DDoS ever mitigated: **31.4 Tbps** (Q4 2025) — automatically, without human intervention

WHY ANYCAST MATTERS FOR PERTH

Traffic inspected at the **nearest PoP** — not backhauled to a regional gateway in Sydney or Singapore

For Cythera's WA clients: measurably lower latency for Zero Trust, SWG, and DDoS mitigation

One Platform, Four Capability Pillars

Cloudflare is not a point product. Every capability runs on the same network, managed from a single control plane — no separate management consoles, no per-site appliances.

Application Security

WAF · DDoS mitigation · Bot management · API security · Page Shield · Rate limiting · SSL/TLS. Protects web properties and APIs from the edge — no traffic backhauling required.

Zero Trust & SASE

Cloudflare One: Access (ZTNA) · Gateway (SWG) · WARP (device agent) · DLP · CASB · Browser Isolation · Magic WAN. Replace legacy VPN and perimeter security with identity-enforced access.

Network Services

Magic Transit (DDoS for IP ranges) · Magic WAN (SD-WAN replacement) · Magic Firewall · Spectrum (TCP/UDP proxy) · Cloudflare Tunnel. Extend Cloudflare's network to replace physical infrastructure.

Developer Platform

Workers (serverless compute at edge) · Workers AI · AI Gateway · D1 (SQLite at edge) · R2 (object storage) · Durable Objects. Build and deploy applications globally without managing infrastructure.

Application Security — Technical Architecture

HOW IT WORKS

Traffic is proxied through Cloudflare's Anycast network. Every request is inspected at the nearest PoP before reaching the origin — no latency penalty for inspection.

Relevant for Cythera's clients

WAF + DDoS + Bot as a managed service layer — Cythera can deliver this to 400+ clients without per-client hardware

WAF

OWASP Top 10 · Custom rules · Managed rulesets · Rate limiting. 2025 Forrester Wave: Leader. Inspects HTTP/S at L7 — no TLS break-and-inspect required.

DDoS Mitigation

Always-on, unmetered, automatic. L3/4/7 protection. Largest attack mitigated: 31.4 Tbps. No traffic scrubbing centres — mitigation happens at every PoP simultaneously.

Bot Management

ML-based bot scoring on every request. Distinguishes good bots (search crawlers) from bad (scrapers, credential stuffers). Turnstile as CAPTCHA replacement.

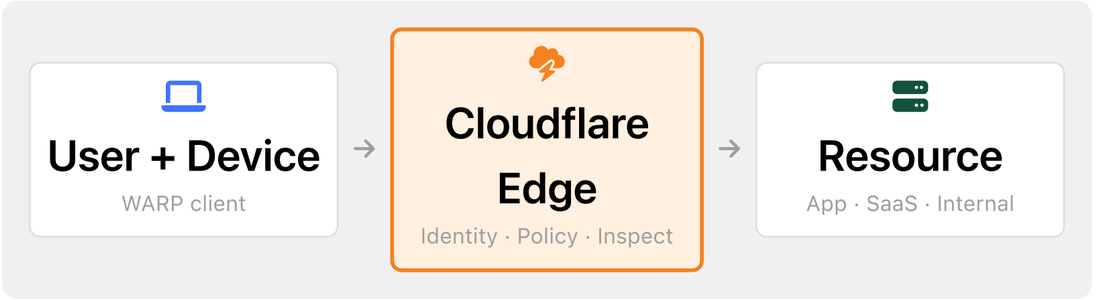
API Security

API Discovery (auto-detect endpoints) · Schema validation · Sequence mitigation · JWT validation. Protects REST, GraphQL, and gRPC APIs without code changes.

Zero Trust & SASE — Cloudflare One

ARCHITECTURE PRINCIPLE

Replace the implicit trust of VPN and perimeter firewalls with explicit, identity-enforced access decisions made at the nearest Cloudflare PoP — not at a centralised gateway.



Access (ZTNA)

Identity-aware proxy for internal apps. Integrates with any IdP (Entra, Okta, Google). Replaces VPN for application access. Short-lived certificates, no persistent tunnels.

Gateway (SWG)

DNS + HTTP filtering for outbound traffic. 42+ AI app controls. DLP scanning. Threat intelligence from 20%+ of web traffic. No hardware required — WARP routes traffic to the nearest PoP.

DLP + CASB

700+ built-in data detectors. Exact Data Match for sensitive lists. CASB discovers shadow SaaS and misconfigured cloud apps. Inline inspection without TLS break-and-inspect complexity.

Browser Isolation

Render web content on Cloudflare's edge — only a visual stream reaches the endpoint. Blocks malware downloads, prevents data exfiltration via clipboard/print, protects unmanaged devices.

Network Services — Magic Transit & Magic WAN

MAGIC TRANSIT — DDOS FOR IP INFRASTRUCTURE

Advertise your IP prefixes via BGP to Cloudflare. All traffic is absorbed and scrubbed at the nearest PoP before being forwarded to your network via GRE or CNI tunnels.

No scrubbing centre latency — mitigation at every PoP simultaneously

Magic Firewall — L3/4 stateless firewall rules applied at the edge

Relevant for — Cythera clients with on-prem infrastructure, ISPs, government networks

MAGIC WAN — SD-WAN REPLACEMENT

Connect branch offices, data centres, and cloud environments to Cloudflare's network via IPsec or GRE tunnels. Replace MPLS and SD-WAN hardware with Cloudflare as the WAN fabric.

Architecture comparison

Legacy SD-WAN	Magic WAN
Per-site appliances · Hardware refresh cycles · Separate security stack · Complex management	Software-defined · No per-site hardware · Security built-in · Single dashboard

Cloudflare + Cythera — The Partner Opportunity

WHY CLOUDFLARE COMPLEMENTS CYTHERA'S STACK

Cythera already delivers MDR, DFIR, and MSSP services across 400+ clients. Cloudflare adds the network-layer enforcement that makes those services more effective — and creates new managed service revenue lines.

Managed SASE / Zero Trust

Deliver Cloudflare One as a managed service to your 400+ clients — per-seat licensing, no hardware, single pane of glass

Managed Application Security

WAF + DDoS + Bot as a managed overlay — no per-client infrastructure, scales across your entire client base

AI Security Practice

Cloudflare's AI Gateway + MCP Portal + WAF AI Security — a differentiated service line your competitors cannot yet match

EXISTING VENDOR ALIGNMENT

Cloudflare is **complementary** to Cythera's existing vendor ecosystem — not a replacement.

- CrowdStrike
- Netskope
- Wiz
- Cato Networks

Cloudflare sits in front of your entire stack — network-level enforcement that makes CrowdStrike telemetry richer, Netskope policies more effective, and Wiz findings more actionable.

Forrester TEI (January 2026): **227% ROI**, payback <6 months, 35% reduction in IT ops time — tei.forrester.com

Essential Eight Alignment

Cloudflare addresses multiple Essential Eight strategies out of the box — relevant for Cythera's government and regulated-industry clients across Australia.

Application Control

Gateway blocks unauthorised applications and SaaS tools. CASB discovers shadow IT. Browser Isolation prevents unapproved code execution.

Restrict Admin Privileges

Access enforces least-privilege with MFA and device posture checks before any privileged session. Short-lived credentials, full audit trail.

Multi-Factor Authentication

Access integrates with any IdP for MFA enforcement. Hardware key support (FIDO2/WebAuthn). Phishing-resistant authentication for all internal apps.

User Application Hardening

Browser Isolation renders web content remotely — malicious scripts never execute on the endpoint. Blocks file downloads, clipboard exfiltration, and macro execution.

Patch Applications

Virtual patching via WAF rules — mitigate known CVEs at the edge before patches are deployed to origin servers

Regular Backups / Data Protection

DLP prevents sensitive data exfiltration via web, email, and AI tools. CASB monitors cloud storage for misconfigured sharing

PART 2

Cloudflare AI Security

Three Pillars of Protection for the AI Era

THE CHALLENGE

AI Adoption Is Outpacing Security

Three distinct threat surfaces have emerged — each requiring a different response. Most organisations are exposed on all three simultaneously.

Your People

Employees are using ChatGPT, Copilot, and Claude every day — often without IT visibility. Corporate data, customer PII, and source code are leaving the organisation in prompts.

Your Applications

Development teams are building AI-powered products that call LLM APIs directly. Without a control layer, there is no visibility into cost, data exposure, or what happens when a provider goes down.

Your AI Agents

AI agents now take actions — reading files, sending emails, querying databases. Without governance, a single compromised agent can exfiltrate data or execute unauthorised actions at machine speed.

The common thread: Traditional perimeter security was not designed for AI. Cloudflare addresses all three surfaces from a single platform — without adding new vendors or complexity.

CLOUDFLARE AI SECURITY

Three Pillars. One Platform. One Dashboard.

PILLAR 1

End-User Protection

Employees using AI tools in their browser

Products:

Cloudflare One · Gateway · DLP · Browser Isolation · CASB

Outcome: Shadow AI visibility + data loss prevention

PILLAR 2

App & API Security

Applications calling LLM APIs programmatically

Products:

AI Gateway · DLP on prompts & responses · Rate limiting · Observability

Outcome: Cost control + resilience + full audit trail

PILLAR 3

Agentic & MCP Security

AI agents accessing tools, APIs, and data

Products:

MCP Portal (open beta) · AI Gateway · AI Security for Apps · Gateway

Outcome: Zero Trust governance for every agent action

PILLAR 1 — END-USER PROTECTION

Let Your People Use AI. Safely.

The Business Risk Today

When employees use AI tools without IT oversight:

- Customer PII enters third-party AI systems
- Source code and IP shared in prompts
- No audit trail for compliance or breach response
- No way to enforce policy across 40+ AI applications

75% of employees use AI tools at work. **60%** do so without IT approval.

Industry surveys, 2024

What Cloudflare Delivers

Complete Visibility

See every AI tool in use across your organisation — including tools IT didn't approve

Data Loss Prevention

Scan prompts and file uploads for PII, credentials, and proprietary data before they reach any AI provider

Granular Policy

Allow, block, or restrict AI tools by user, group, device, or application — without blocking productivity

Compliance Audit Trail

Full conversation logging with user attribution — supports Privacy Act NDB obligations and internal investigations

PILLAR 2 — APP & API SECURITY

Control Every LLM Call Your Applications Make

⚠ The Business Risk Today

When applications call LLM APIs without a control layer:

- A single runaway agent loop can cost $10,000+ in minutes
- No visibility into what data is being sent to which model
- Single provider dependency — one outage breaks your product
- Prompt injection attacks can hijack application behaviour

AI Gateway core features are free — observability, caching, and rate limiting at no additional cost on any Cloudflare plan.

✓ What Cloudflare Delivers

Cost Control

Rate limits and budget caps per model, per user, or per application. Semantic caching reduces repeat API costs.

Resilience

Automatic failover across 20+ LLM providers. If OpenAI is down, route to Anthropic or Workers AI — your application keeps running

Full Observability

Every prompt and response logged — token counts, latency, cost per request, and guardrail triggers. No more black-box AI spend

DLP on Both Directions

Scan prompts before they reach the LLM and responses before they reach your users — no TLS interception required

PILLAR 3 — AGENTIC & MCP SECURITY

AI Agents Take Actions. Govern Them.

⚠ The Business Risk Today

AI agents connected to your systems via MCP can:

- Access tools and data beyond their intended scope
- Be hijacked by malicious data returned from a tool call
- Connect to unvetted third-party MCP servers
- Exfiltrate sensitive data at machine speed, without human review

MCP (Model Context Protocol) is the emerging standard for connecting AI agents to external tools. Adoption is accelerating — governance frameworks are not keeping pace.

✓ What Cloudflare Delivers

Governed Tool Access

MCP Portal (open beta) gives agents a single, identity-enforced gateway to approved tools — only vetted servers are accessible

Shadow MCP Detection

Cloudflare Gateway detects and blocks employees connecting AI clients to unauthorised MCP servers outside the approved portal

Inbound App Protection

WAF-based AI Security scores every inbound prompt for injection risk and PII — protecting your public-facing AI applications

Complete Audit Trail

Every tool call and every LLM call logged centrally — who did what, when, with which agent. Supports board-level accountability requirements

WHY CLOUDFLARE

One Platform. Proven at Scale. Ready Now.

227%
ROI over 3 years
Forrester TEI, Jan 2026

<6 mo
Payback period
Forrester TEI, Jan 2026

35%
Reduction in IT ops time
Forrester TEI, Jan 2026

38%
of Fortune 500 are
Cloudflare customers

Single dashboard. Zero Trust, AI Gateway, and WAF are managed from one place — no separate consoles, no separate vendors, no integration projects.

→ Suggested Next Steps for Cythera

1. **Technical Workshop (1 hr)**
   Map Cythera's current AI tool usage, application LLM calls, and agentic workflows — identify which pillar is most urgent for your clients

2. **Proof of Concept (2–4 weeks)**
   Deploy the highest-priority pillar in Cythera's own environment — measure shadow AI discovery, cost reduction, or agent governance against your current baseline

3. **MSSP Partner Programme**
   Explore reselling Cloudflare AI Security to your 400+ clients — per-seat licensing, managed from a single dashboard, with dedicated Cloudflare partner support

Cloudflare

Thank You

Cloudflare + Cythera — protecting Australia's organisations at network speed

Jason Clarke · jason.clarke@cloudflare.com

cloudflare.com/partners

Forrester TEI (Jan 2026): 227% ROI · tei.forrester.com/go/cloudflare/cloudflaretei/