CLOUDFLARE ONE · CITY OF PERTH

Simplifying Your Network. One Platform. Zero Complexity.

A path to consolidating DNS, remote access, and application delivery onto Cloudflare One — removing vendor sprawl and strengthening security posture.

Cloudflare One Prepared for City of Perth · May 2026

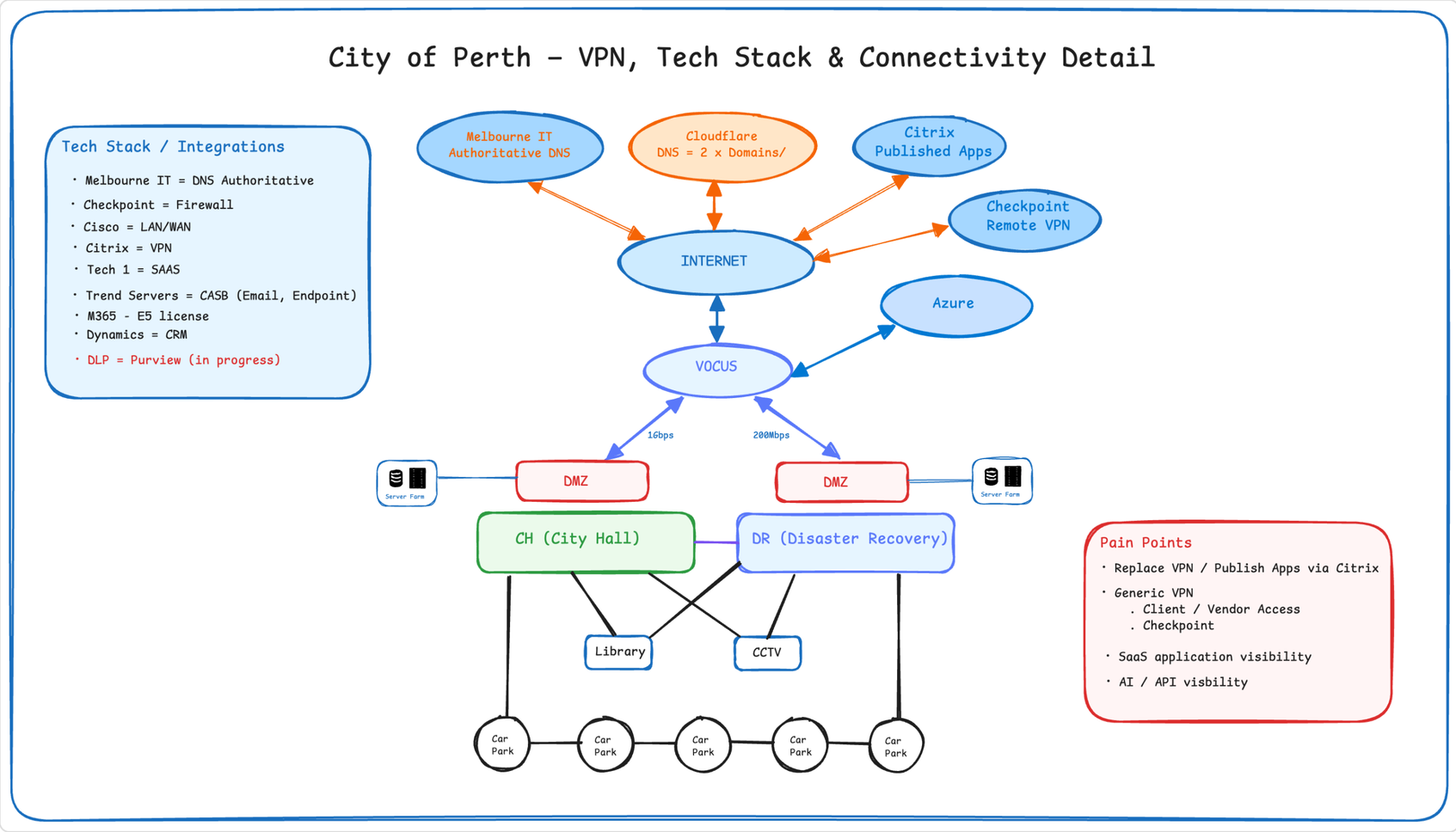
SECTION 1

Where You Are Today

Current architecture, vendor landscape, and the pain points driving change.

CURRENT STATE

City of Perth — Today's Architecture



CURRENT CHALLENGES

Four Pain Points Driving This Conversation

VPN & REMOTE ACCESS

Checkpoint VPN is a single point of failure

Corporate users, BYOD, and third-party vendors all share the same generic VPN — no device posture, no per-app controls, no audit trail.

PUBLISHED APPLICATIONS VIA CITRIX

Citrix adds cost and complexity without Zero Trust

Applications published through Citrix require VDI infrastructure, ongoing licensing, and provide no identity-aware access controls at the network layer.

DNS SPLIT ACROSS VENDORS

Melbourne IT holds authoritative DNS; Cloudflare holds 2 domains

Split DNS management creates operational overhead, inconsistent security policies, and limits visibility into DNS-based threats across all City domains.

SAAS & AI/API VISIBILITY

No visibility into SaaS usage or AI/API traffic

With M365 E5, Dynamics, and Trend Servers in use, there is no unified view of what SaaS applications staff are accessing or what data is leaving the organisation.

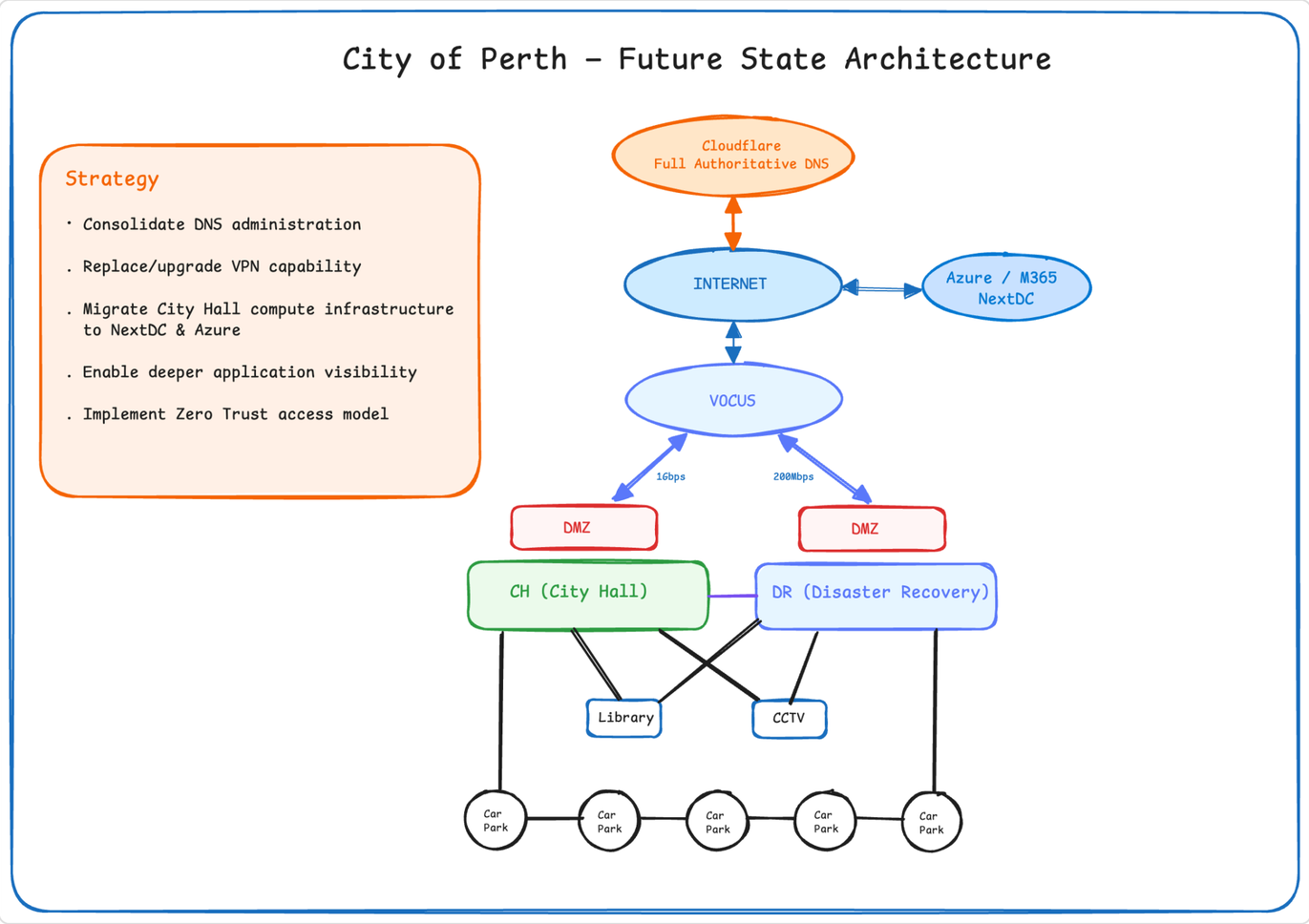
SECTION 2

The Consolidated Future State

One platform replacing four discrete vendor solutions — DNS, VPN, application access, and security in a single control plane.

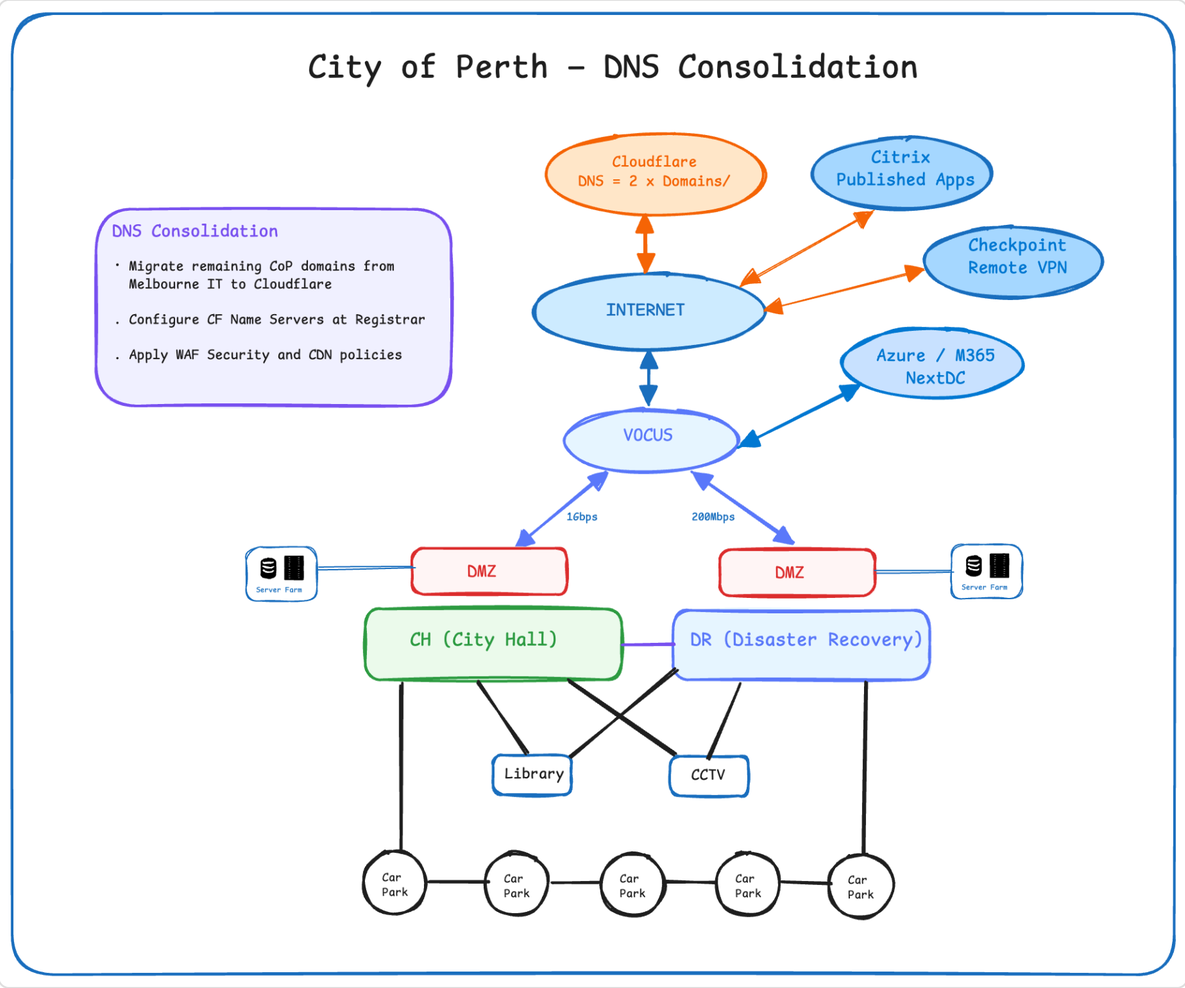
FUTURE STATE ARCHITECTURE

City of Perth — Cloudflare One Platform



WORKSTREAM 1 · DNS

DNS Consolidation



WORKSTREAM 1 · DNS

DNS Consolidation — What Changes & What You Gain

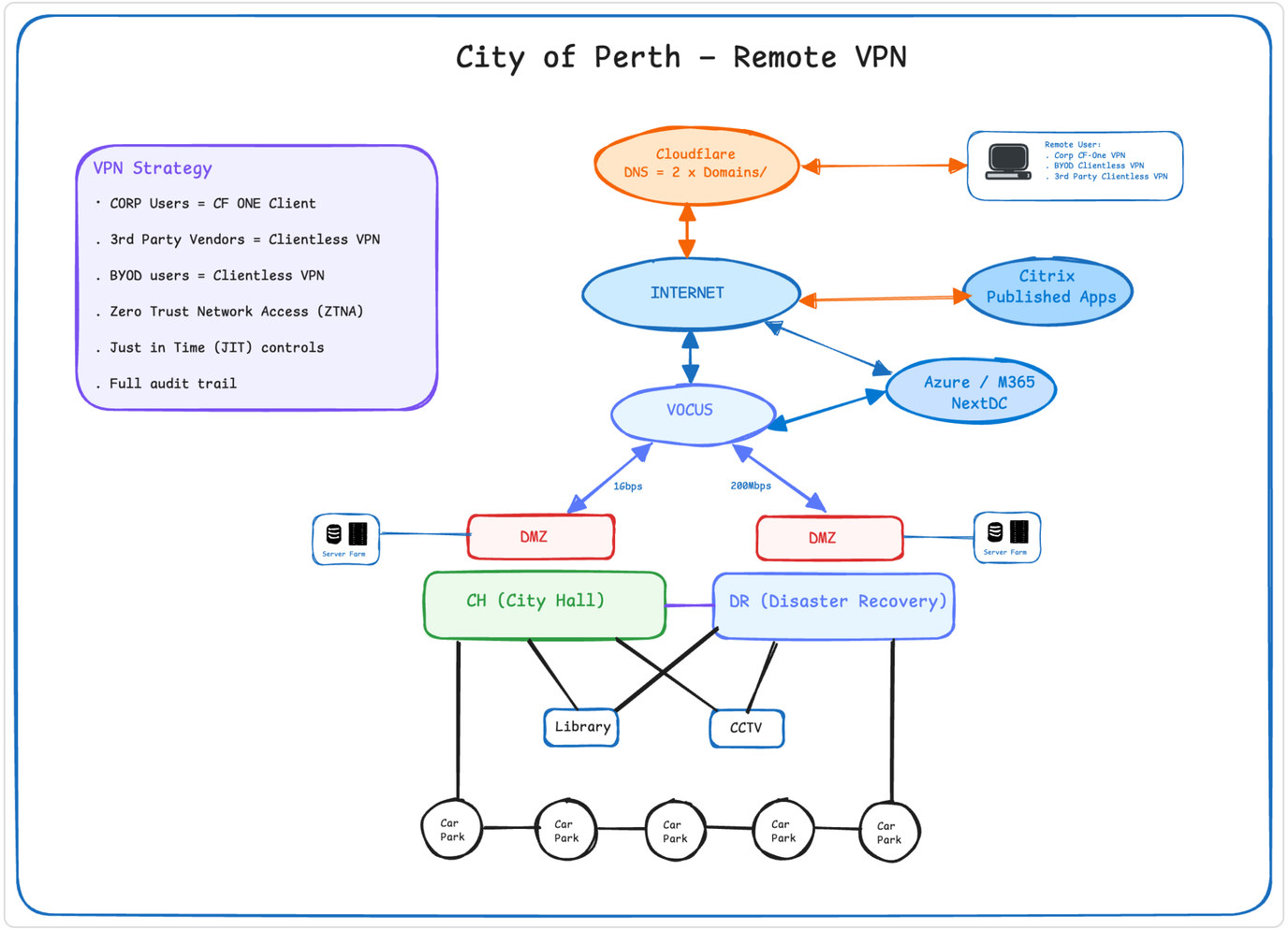
What changes

- Migrate remaining City of Perth domains from Melbourne IT to Cloudflare
- Configure Cloudflare Name Servers at the registrar
- Apply WAF security and CDN policies across all domains

What you gain

- Single pane of glass for all DNS records
- DNS-layer threat blocking — malware, phishing, C2 domains
- Anycast DNS resolves from the nearest of 330+ cities globally
- Eliminates Melbourne IT dependency and management overhead

Replacing Checkpoint VPN with Zero Trust Network Access



WORKSTREAM 2 · REMOTE ACCESS

Three Access Tiers. One Platform. Full Audit Trail.

Three access tiers — one platform

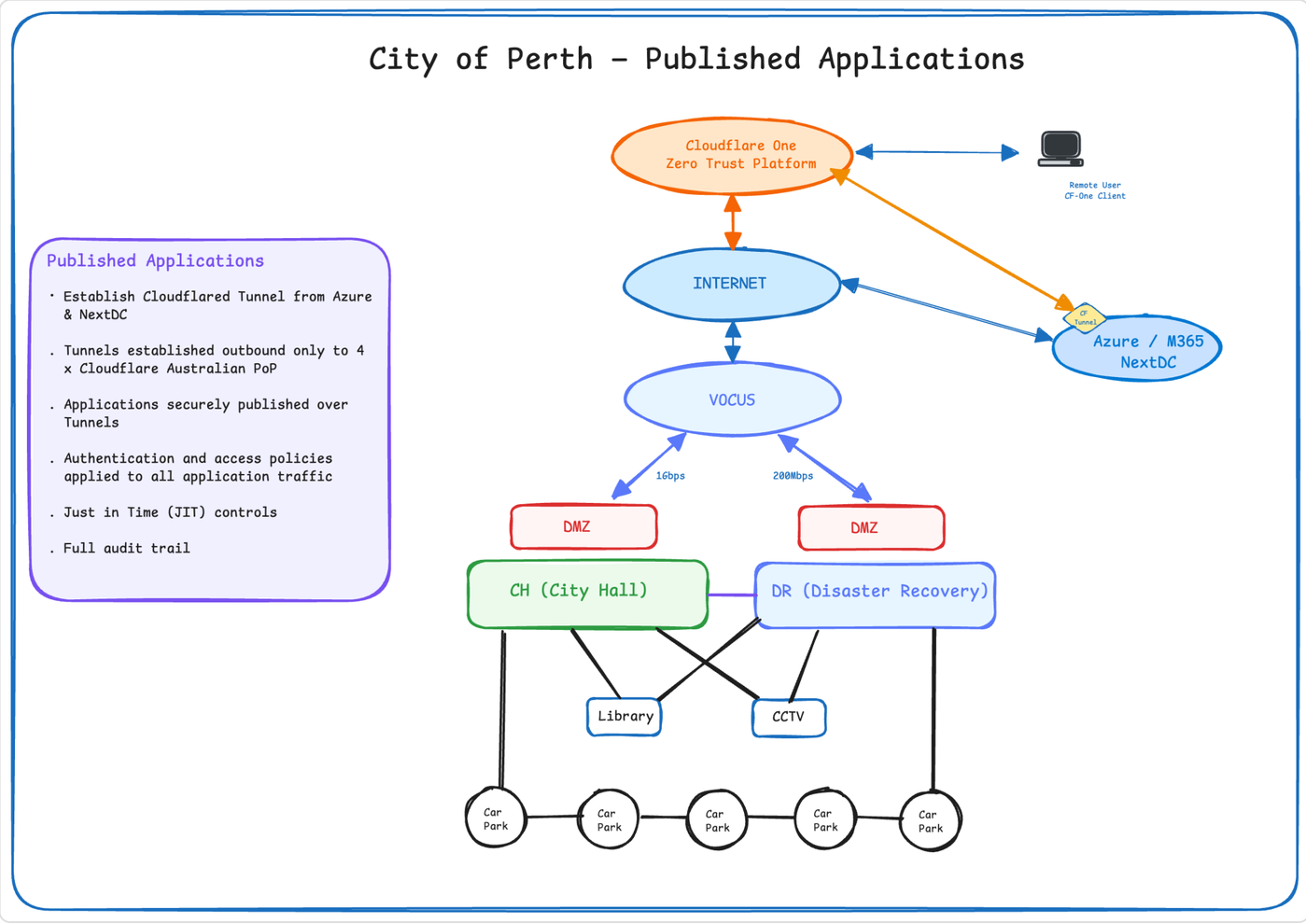
- **Corporate users** — CF One Client with device posture (OS version, disk encryption, serial number)
- **BYOD users** — Clientless browser-based VPN, no agent required
- **3rd party vendors** — Clientless VPN with JIT access controls and full audit trail

Security improvements over Checkpoint

- Zero Trust Network Access — no implicit trust, every session verified
- Entra ID integration — revoked accounts blocked at next authentication check
- Every access event logged — full audit trail for compliance
- Supports Essential Eight — MFA and Restrict Admin Privileges

WORKSTREAM 3 · APPLICATION ACCESS

Replacing Citrix with Cloudflare Tunnels & Access



WORKSTREAM 3 · APPLICATION ACCESS

How Cloudflare Tunnels Replace Citrix

How it works

- Cloudflare Tunnel established outbound-only from Azure & NextDC — no inbound firewall rules required
- Tunnels connect to Australian Cloudflare PoPs (Sydney, Melbourne, Brisbane, Perth)
- Applications published securely over Tunnels — users never touch the network directly
- Authentication and access policies applied to every request

What replaces Citrix

- No VDI infrastructure required — apps delivered natively via browser
- JIT access controls — access granted per session, not standing
- Full audit trail of every application access event
- Entra ID integration — revoked accounts blocked at next authentication check

SECTION 3

Why Consolidation Matters

The security and operational case for removing discrete vendor solutions.

OPERATIONAL BENEFITS

From Vendor Sprawl to a Single Control Plane

REPLACED	CONSOLIDATED ONTO CLOUDFLARE ONE
✕ **Checkpoint** — Remote VPN	✓ **ZTNA** — CF One Client + Clientless VPN
✕ **Citrix** — Published applications & VDI	✓ **Cloudflare Access + Tunnels** — App publishing
✕ **Melbourne IT** — Authoritative DNS	✓ **Cloudflare DNS** — Full authoritative DNS
✕ **Cisco LAN/WAN** — Network management complexity	✓ **Single dashboard** — One policy engine for all traffic

> *Organisations consolidating onto Cloudflare One report a **35% reduction in IT operations time** and **20% reduction in licensing costs** — Forrester TEI, January 2026.*
>
> Source: Forrester Total Economic Impact™ Study

SECURITY BENEFITS

Stronger Security Posture Across Every Layer

Zero Trust Access

- Every user and device verified before access
- Device posture enforced at connection time
- Entra ID integration — revoked accounts blocked at next authentication check
- **Essential Eight:** Restrict Admin Privileges & MFA

DNS & Network Security

- DNS-layer threat blocking — malware, phishing, C2
- WAF and CDN policies across all public domains
- ~85 million DNS queries/second threat intelligence
- **Essential Eight:** User Application Hardening

Application & API Visibility

- Full audit trail for every application access event
- SaaS visibility — M365, Dynamics, Shadow IT
- AI/API traffic visibility across all outbound connections
- Complements Purview DLP already in progress

NEXT STEPS

Proposed Path Forward

1

DNS Migration PoC

Migrate one domain from Melbourne IT to Cloudflare. Validate DNS resolution, WAF policies, and CDN performance. Low risk, high visibility win.

2

ZTNA Pilot

Deploy CF One Client to a pilot group of corporate users. Validate device posture, Entra ID integration, and access policies against one internal application.

3

Application Publishing PoC

Establish a Cloudflare Tunnel from Azure/NextDC and publish one Citrix-hosted application via Cloudflare Access. Demonstrate the Citrix replacement path.

Ready to start? Let's align on a PoC scope and timeline — **Jason Clarke** · jclarke@cloudflare.com