EDITH COWAN UNIVERSITY · WESTERN AUSTRALIA

Securing ECU's University of the Future

How Cloudflare can protect and connect ECU's people, research and digital infrastructure across every campus.

Prepared by

Jason Clarke

Senior Solutions Engineer, Cloudflare

Date

May 2026

ECU TODAY

A university in the middle of its most ambitious transformation

ECU's Strategic Plan 2022–2026 — Towards the University of the Future — sets a clear direction: lead the sector in educational experience, research with impact, and positive contributions to industry and communities.

ECU City opened at Perth City Link — at 500 Wellington Street in the CBD, bound by Roe, Wellington and Queen streets and directly interfacing with Yagan Square. It brings technology, industry and creativity together in the heart of Perth. This is not a minor upgrade. It is a structural shift in how ECU operates.

30,000+
Students and staff across WA campuses

4
Campuses: Joondalup, City, South West, Sri Lanka

2026
ECU City opens — Perth CBD, 11 levels

Cyber CRC
ECU is a founding participant — national security research

The strategic commitment: ECU will "secure our future through innovation and leadership" and "create partnerships for economic and social well-being." Technology infrastructure is not a support function — it is the foundation every one of these goals rests on.

THE THREAT CONTEXT

Education is one of the most targeted sectors in Australia

The Australian Signals Directorate's 2023–24 Cyber Threat Report identified education as a high-priority target sector. Universities hold research data, student PII, health records, and increasingly — defence-sensitive research.

Research data is a nation-state target

ECU's Cyber Security CRC and Defence Research programs handle sensitive IP. A breach is not just an IT incident — it is a national security event.

Open networks are the attack surface

Universities must provide open, accessible networks for learning. That openness is exactly what attackers exploit — phishing, credential theft, ransomware.

Multi-campus complexity multiplies risk

Joondalup, City, South West, Sri Lanka — each campus is a potential entry point. Inconsistent policy enforcement across sites creates gaps.

ASD CYBER THREAT REPORT 2023–24

87,400

Cybercrime reports received by ASD in FY2023–24 — one every 6 minutes

AVERAGE COST PER INCIDENT

$62,800

Average self-reported cost per cybercrime report for medium organisations (ASD Annual Cyber Threat Report 2023–24)

CLOUDFLARE GLOBAL THREAT INTELLIGENCE

215B

Cyber threats blocked per day on average in Q4 2025 — across all

PART ONE

Where ECU's infrastructure creates friction

Three structural challenges that grow harder to manage as ECU scales

THE CHALLENGE

Three structural challenges that grow with ECU's ambition

Multi-campus connectivity

Joondalup, City, South West and Sri Lanka each need consistent, secure access to shared systems. Traditional hub-and-spoke WAN architectures backhaul traffic through a central point — adding latency and creating a single point of failure.

The impact: Staff and students at ECU City or South West experience slower access to Joondalup-hosted systems. IT teams manage multiple site configurations.

SaaS sprawl and identity risk

Microsoft 365, research collaboration platforms, student portals, HR systems — ECU's application estate spans dozens of SaaS tools. Each is a potential credential theft vector. Without consistent Zero Trust enforcement, a compromised student account can pivot laterally.

The impact: IT security teams spend disproportionate time on access policy management across fragmented tools.

Research data and application exposure

ECU's Cyber Security CRC and Defence Research programs handle sensitive IP. Public-facing research portals, collaboration tools and APIs are exposed to the internet. DDoS attacks on university infrastructure are increasing in frequency and scale globally.

The impact: A successful attack on research infrastructure damages ECU's reputation as a trusted defence and industry partner.

THE HIDDEN COST

The status quo has a compounding cost that rarely appears on a single line item

Most universities don't have a single "security problem." They have a collection of point solutions — each solving one problem, each requiring its own management overhead, each creating gaps at the boundaries.

> *"Cyber security is a strategic priority for Australia's national security, includi for its critical infrastructure."*
>
> — David Irvine, former Chair, Cyber Security Cooperative Research Centre

As ECU adds ECU City and grows its international footprint, the complexity of managing disparate tools scales faster than headcount. The question is not whether to invest in security — it is whether to invest in consolidation or fragmentation.

IT ops time on policy management

Organisations consolidating to Cloudflare Zero Trust report a 35% reduction in IT operations time — time that can be redirected to ECU's digital transformation priorities. *(Forrester TEI, Jan 2026)*

Licensing consolidation

The same Forrester study found a 20% reduction in security licensing costs when consolidating to a single platform — relevant for ECU's AUD budget environment.

Essential Eight alignment

As a WA public university, ECU operates under ASD's Essential Eight framework. Cloudflare addresses multiple Essential Eight strategies — application control, patching, MFA, restricting admin privileges — from a single platform.

Sustainability

Replacing on-premises appliances with Cloudflare's network reduces carbon footprint by 78–96% vs. on-premises infrastructure. *(Analysys Mason, 2023)*

PART TWO

A different approach

One platform. Three outcomes. Built for how ECU actually works.

CLOUDFLARE FOR ECU

One platform. Three outcomes. No added complexity.

Zero Trust Access

- Replace VPN with identity-aware access
- Every user, every device, every campus verified
- Works alongside Microsoft Entra ID
- Consistent policy across all 4 campuses

Application & Research Protection

- WAF protecting student portals and research APIs
- Automatic DDoS — 31.4 Tbps mitigated (Nov 2025)
- Bot management for credential stuffing
- DNS filtering at the resolver level

Network Modernisation

- Cloudflare WAN replacing legacy MPLS
- Traffic inspected at nearest PoP — Perth local, not Sydney backhaul
- No backhaul to a central gateway
- Sri Lanka on the same policy plane

Cloudflare's network spans **330+ cities in 125+ countries**, with **500 Tbps of provisioned capacity** and interconnects with ~13,000 networks globally. Cloudflare protects approximately 20% of the web — giving ECU access to threat intelligence at a scale no single university could replicate independently.

ZERO TRUST · CLOUDFLARE ACCESS + GATEWAY

Securing ECU's people and devices — without slowing them down

ECU's 30,000+ students and staff access systems from Joondalup, the new City Campus, South West, Sri Lanka, and remotely. A traditional VPN creates a bottleneck and treats every authenticated user as trusted — regardless of device health or behaviour.

Cloudflare Access replaces VPN with identity-aware, per-application access. Cloudflare Gateway provides DNS and HTTP filtering for every device — on or off campus — without requiring traffic to backhaul through Joondalup.

Works with what ECU already has: Cloudflare sits in front of your Microsoft 365 and Entra ID estate — it is the network-level enforcement layer that makes your existing identity investments more effective, not a replacement for them.

Cloudflare Access

Zero Trust application access — replaces VPN. Staff access HR, research systems and admin tools with identity + device posture checks. No inbound firewall rules required.

Cloudflare Gateway

DNS and HTTP filtering for all ECU devices. Blocks phishing, malware C2, and inappropriate content. Applies consistently whether a student is on campus Wi-Fi or at home.

WARP Client

Lightweight agent for staff and managed devices. Routes traffic through Cloudflare's network for inspection — no performance penalty, no VPN client complexity.

Browser Isolation

For high-risk browsing — research staff accessing external collaboration portals, or contractors accessing internal tools — execute browser sessions in Cloudflare's network, not on the endpoint.

APPLICATION SECURITY · WAF + DDOS + DNS

Protecting ECU's research, portals and APIs from the internet

ECU's participation in the national Cyber Security CRC and its Defence Research programs mean ECU handles sensitive IP that is a target for nation-state actors. Public-facing research portals, student enrolment systems and APIs need protection that operates at internet scale.

CLOUDFLARE WAF

Protects web applications from OWASP Top 10, zero-day exploits and credential stuffing. Rules updated continuously from threat intelligence across 20%+ of web traffic. No appliance to patch.

DDOS PROTECTION

Unmetered, automatic DDoS mitigation. Cloudflare automatically mitigated the world's largest recorded DDoS attack — 31.4 Tbps — in November 2025. ECU's research portals and student systems stay online regardless of attack volume.

DNS SECURITY

Cloudflare processes ~85 million DNS queries per second globally. ECU's DNS infrastructure benefits from this scale — fast, resilient, and with built-in threat filtering at the resolver level.

WHY THIS MATTERS FOR ECU SPECIFICALLY

- **Cyber CRC credibility:** ECU is a founding participant in Australia's national Cyber Security CRC. Its own infrastructure must demonstrate the security posture it researches and teaches.
- **Defence research obligations:** ECU's Defence Research and Engagement programs — covering cyber security, information warfare and engineering — require a security posture consistent with government partner expectations.
- **Student portal availability:** Enrolment, results and student services must be available 24/7. A DDoS attack during census date or exam results release is a reputational and operational crisis.

Cloudflare blocked 230 billion threats per day on average across 2025 — a 21% increase in threats blocked per day year-on-year. ECU's applications benefit from this threat intelligence the moment they are onboarded.

NETWORK · MAGIC WAN + CLOUDFLARE TUNNEL

Connecting ECU's campuses without the complexity of legacy WAN

ECU's new City Campus, combined with Joondalup, South West and Sri Lanka, creates a genuinely distributed university. Legacy MPLS or site-to-site VPN architectures were not designed for this model — they backhaul traffic through a central point, adding latency and cost.

1. **Replace site-to-site VPN with Cloudflare Tunnel**

   Each campus connects outbound to Cloudflare's network via a lightweight tunnel. No inbound firewall rules. No exposed public IPs. Traffic is inspected at the nearest PoP — for Perth campuses, that means local inspection, not Sydney backhaul.

2. **Unified policy across all sites**

   Security policy is defined once in Cloudflare's dashboard and applied consistently across Joondalup, City, South West and Sri Lanka. A new campus is onboarded in hours, not weeks.

3. **Cloudflare WAN for branch connectivity**

   For sites requiring dedicated connectivity, Cloudflare WAN replaces MPLS with Cloudflare's private backbone — connecting to 330+ cities, with built-in redundancy and no hardware refresh cycles.

BEFORE VS. AFTER

TODAY	WITH CLOUDFLARE
• Traffic backhauled to central gateway	• Traffic inspected at nearest PoP
• Per-site VPN configuration	• Single dashboard for all sites
• Hardware appliances at each site	• No hardware — software-defined
• Inconsistent policy enforcement	• Consistent policy everywhere
• Sri Lanka on separate management plane	• Sri Lanka on same policy plane

PROOF POINTS

What peer institutions and independent research show

FORRESTER TOTAL ECONOMIC IMPACT — JANUARY 2026

227%
ROI over 3 years

<6mo
Payback period

35%
IT ops time reduction

Forrester interviewed Cloudflare customers across multiple sectors and found consistent, measurable returns from consolidating to Cloudflare's platform. Full report: tei.forrester.com/go/cloudflare/cloudflaretei/

ANALYSYS MASON — CARBON REDUCTION (2023)

78–96%

Carbon reduction vs. on-premises infrastructure. Relevant to ECU's sustainability commitments and WA government reporting requirements.

EDUCATION SECTOR — CLOUDFLARE CUSTOMERS

Cloudflare protects universities and research institutions globally, including institutions with similar profiles to ECU — multi-campus, research-intensive, with international student populations and defence/government research obligations.

Common use cases in higher education: Zero Trust replacing VPN for staff and researchers, WAF protecting student portals, DDoS protection for enrolment and exam systems, and Cloudflare WAN connecting distributed campuses.

CLOUDFLARE NETWORK SCALE

330+
Cities in 125+ countries

500 Tbps
Network capacity (April 2026)

20%+
Of all web traffic

~13,000
Network interconnects globally

PROPOSED NEXT STEP

A focused 60-minute discovery session — no commitment required

ECU is at an inflection point. The opening of ECU City, the growth of the Cyber Security CRC, and the expansion of Defence Research programs all create new infrastructure requirements — and new risk exposure.

The most useful next step is a structured conversation with ECU's IT and security leadership to understand your current architecture, your priorities for 2026–27, and where Cloudflare can deliver the most immediate value.

Jason Clarke
Senior Solutions Engineer — Western Australia
jclarke@cloudflare.com

What we'd cover in 60 minutes:

- Current WAN and security architecture across all campuses
- Priority use cases: Zero Trust, application protection, or network modernisation
- Essential Eight maturity and any compliance obligations
- Existing vendor relationships and what's working vs. what isn't
- Timeline and budget cycle for 2026–27

SUGGESTED PHASED APPROACH

Three phases — each delivering value before the next begins

1

Application Protection

30 DAYS · QUICK WIN

Onboard ECU's public-facing student portal and research APIs behind Cloudflare WAF and DDoS protection.

Outcome: Immediate risk reduction. No infrastructure change required. Research portals and student systems protected from day one.

2

Zero Trust Pilot

60–90 DAYS · STAFF ACCESS

Replace VPN for a defined group — IT staff or research team — with Cloudflare Access. Measure the experience difference before broader rollout.

Outcome: Validated Zero Trust model. Reduced VPN complexity. Consistent access policy for Joondalup and City Campus staff.

3

Network Modernisation

FY2026–27 · ECU CITY + WAN

As ECU City reaches full operational capacity, connect it to Cloudflare's network alongside Joondalup — establishing a consistent, software-defined WAN for all WA campuses.

Outcome: No backhaul. Unified policy. Sri Lanka on the same management plane. Hardware refresh cycle eliminated.

Each phase is independently valuable. ECU can start with Phase 1 and evaluate before committing to subsequent phases. Cloudflare's per-seat licensing model means costs scale with ECU's actual usage — not with hardware or site count.