CLOUDFLARE

UNIVERSITY OF WESTERN AUSTRALIA · CONFIDENTIAL

Cloudflare Security & Essential 8

How Cloudflare's layered security platform addresses E8 patch management requirements and provides auditable compensating controls

Jason Clarke
· Senior Solutions Engineer
Ian Hogben · Account Manager
April 2026

SECTION 1

The Problem

Why the 48-hour patch requirement cannot be met without a compensating control

Essential 8 ML1 — Patch Management Requirements

PATCH APPLICATIONS (E8.2)

48 hrs — critical/exploitable CVEs on internet-facing services

2 weeks — non-critical CVEs on internet-facing services

Daily vulnerability scanning of internet-facing services

PATCH OPERATING SYSTEMS (E8.3)

48 hrs — critical/exploitable CVEs on internet-facing servers

2 weeks — non-critical CVEs on internet-facing servers

Daily scanning for internet-facing server OS vulnerabilities

The E8 framework explicitly permits compensating controls where direct patching within the required window is not feasible — provided they are documented and approved.

Regulatory basis: ISO 27001 §12.6.1 names network-border access controls as acceptable compensating controls when patches cannot be deployed in time. The ASD ISM similarly accepts vendor mitigations as alternatives to direct patching for internet-facing systems.

Why the 48-Hour Requirement Cannot Be Met

Vendor validation cycles

1. Oracle (Callista) and other suppliers require third-party validation before UWA can deploy — routinely exceeds 48 hours.

Change management constraints

2. 28,000+ students, 3,990 staff. Production change windows, regression testing, and approvals cannot compress to 48 hours.

Semester availability constraints

3. Student portal, Callista, LMS, and research systems cannot be taken offline during teaching periods.

Legacy & end-of-life systems

4. Some internet-facing systems have no available patch, or require re-architecture rather than a simple update.

The result: a structural compliance gap that cannot be closed by patching alone — compensating controls are required.

SECTION 2

Cloudflare Application Services

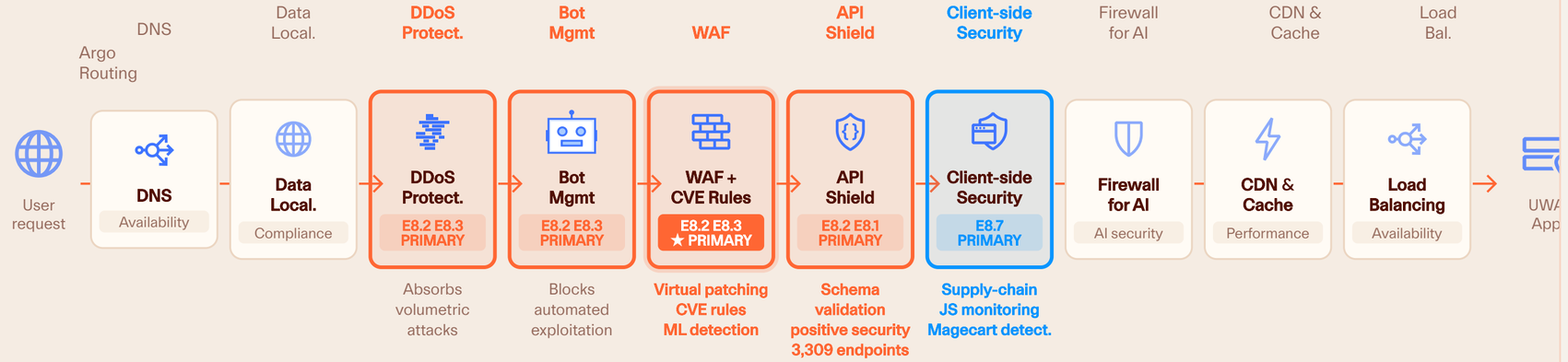
The security stack already active in UWA's environment

Cloudflare Application Services — E8 Capability Map

Each request passes through all services, close to the end user →

E8 Primary · E8 Supporting · Performance / availability

Cloudflare connectivity cloud · One control plane, accessible via API or UI



Cloudflare Access + Tunnel
MFA for legacy apps incl. Callista · **E8.6 MFA — Primary**

Cloudflare Gateway
DNS + HTTP filtering, outbound control · **E8.4 E8.5 — Supporting**

Leaked Credentials Detection
Blocks stolen credential auth · **E8.6 MFA — Supporting**

Cloudflare vs. All Essential 8 Controls

Primary Supporting Out of scope

PRIMARY

E8.2 Patch Applications

WAF virtual patching, OWASP + CF managed rules, ML Attack Score, API Shield schema validation

PRIMARY (HTTP)

E8.3 Patch OS

WAF managed rules for HTTP-exploitable OS CVEs (Apache, IIS, Nginx). Kernel/local exploits: out of scope.

PRIMARY

E8.6 MFA

Cloudflare Access enforces MFA for any HTTP/HTTPS app including legacy systems — no code changes needed

SUPPORTING

E8.4 Admin Privileges

Cloudflare Access RBAC + Gateway outbound filtering + full audit logging for privileged access

SUPPORTING

E8.1 App Control

API Shield schema validation (positive security model). WAF custom rules enforce allowlisted request types.

SUPPORTING

E8.5 Office Macros

Gateway HTTP filtering for file upload/download. Malicious Uploads Detection (Enterprise add-on).

PRIMARY (SUPPLY CHAIN)

E8.7 App Hardening

Client-side Security monitors all scripts in users' browsers. Blocks compromised 3rd-party scripts (Magecart).

OUT OF SCOPE

E8.8 Backups

Not an edge security function. Cloudflare provides availability resilience (DDoS, failover) but not backup infra.

E8.2 Patch Applications — Cloudflare Coverage

ML1 REQUIREMENTS

- Critical CVEs on internet-facing services within **48 hrs**
- Non-critical CVEs within **2 weeks**
- **Daily** vulnerability scanning
- EOL services removed

CLOUDFLARE COMPENSATING CONTROLS

- **WAF Managed Rules** — emergency CVE rules deployed within hours of disclosure
- **WAF Attack Score (ML)** — catches novel exploit variants with no rule needed
- **API Shield schema validation** — blocks structurally anomalous requests regardless of CVE
- **WAF Change Log** — timestamped audit evidence for compliance reporting

OWASP Core Ruleset

Scoring-based model for SQLi, XSS, RFI, LFI, RCE, command injection. Industry standard — regularly updated.

Cloudflare Managed Ruleset

Zero-day CVE rules, advanced attack techniques, stolen credentials. Weekly cycle + emergency out-of-band releases.

E8.3 Patch Operating Systems — Cloudflare Coverage

✓ **What Cloudflare covers**

- OS CVEs exploitable via HTTP/HTTPS
- Web server vulnerabilities — Apache, IIS, Nginx, Tomcat
- Application server CVEs — Oracle WebLogic, JBoss, Struts
- OS-level auth bypass delivered via web request
- EOL web server software — edge coverage while migration planned

✗ **Outside Cloudflare's scope**

- Kernel-level exploits (local access required)
- Memory corruption / local privilege escalation
- OS vulnerabilities with no HTTP attack vector
- Server-side processing after request passes the edge

Honest framing: Cloudflare is defence-in-depth — not a substitute for OS patching. Closes the exposure window for HTTP-delivered exploits while patches are validated and staged.

E8.6 Multi-Factor Authentication — Cloudflare Coverage

Cloudflare Access

Enforces MFA for **any HTTP/HTTPS application**, including legacy systems that cannot natively implement MFA. Works via Cloudflare Tunnel — no application changes required.

MFA for Callista & Legacy Systems

Cloudflare Access + Tunnel enforces MFA *at the edge* before requests reach Oracle Callista — enabling E8 MFA compliance without modifying the application or waiting for Oracle.

Leaked Credentials Detection

Scans authentication requests against Have I Been Pwned + Cloudflare breach data. When compromised credentials are detected: block, challenge, or flag the origin to trigger a password reset. **Directly relevant given UWA's August 2025 credential breach.**

Identity Provider Support

Cloudflare Access federates with SAML and OIDC IdPs. Works with UWA's existing identity infrastructure — enforces MFA at the edge regardless of whether the downstream app supports it.

E8.1 App Control & E8.7 User App Hardening

E8.1 APPLICATION CONTROL — SUPPORTING

API Shield — Positive Security Model

OpenAPI schema validation defines the *exact expected structure* of every API request. Any request that deviates — including zero-day exploits — is blocked. This is signature-independent application control for internet-facing APIs.

WAF Custom Rules

Organisation-specific allowlist rules — restrict which HTTP methods, headers, and parameters are permitted per application.

E8.7 USER APP HARDENING — PRIMARY (SUPPLY CHAIN)

Client-side Security (formerly Page Shield)

Monitors **every script** loading in UWA users' browsers — including Google Analytics/GTM, Facebook Pixel, TikTok Analytics, Microsoft Clarity, LinkedIn, Siteimprove, and others. If any vendor script is compromised (Magecart-style), Client-side Security detects it and can block via CSP. The trial is live and collecting data.

Critical gap this fills: A compromised third-party script exfiltrates data from the browser — no server-side WAF or network control detects it. Client-side Security is the only mechanism that catches this.

E8.4 Admin Privileges, E8.5 Macros & E8.8 Backups

E8.4 ADMIN PRIVILEGES · SUPPORTING

- **Cloudflare Access RBAC** — privileged routes locked to specific identity groups
- **Gateway outbound filtering** — restrict privileged users from internet/email access
- **Full audit logging** — every access event logged with user identity, device posture, timestamp

E8.5 OFFICE MACROS · SUPPORTING

- **Gateway HTTP filtering** — inspect and block Office document uploads/downloads from internet
- **Malicious Uploads Detection** — Enterprise add-on; scans files for malware including macro-embedded documents

Note: Endpoint-level macro control (Group Policy, Intune) remains the primary control. Cloudflare provides a complementary network layer.

E8.8 BACKUPS · OUT OF SCOPE

Backup infrastructure is not an edge security function. Cloudflare does not replace backup systems.

Availability: Cloudflare DDoS protection and anycast routing support availability requirements underpinning DR strategies.

SECTION 3

Virtual Patching in Detail

How Cloudflare closes the exposure window for UWA's internet-facing applications

How Virtual Patching Works

1

Detection

CVE disclosed. Cloudflare observes exploit traffic at scale across 20% of global internet — signals detected within minutes.

2

Rule Development

Security Research team writes a WAF rule matching the exploit's HTTP request pattern — payload, headers, parameters.

3

Testing

Rule tested in shadow mode against live traffic to verify false positive rates before deployment.

4

Global Deploy

Rule propagates globally. Every UWA request evaluated immediately. Application server sees only clean traffic.

Emergency releases (P1)

Triggered for critical/actively-exploited CVEs. Rules deployed out-of-band, outside the weekly cycle. Observed response: blocking rules live within hours of public disclosure. *Not a published contractual SLA — based on WAF changelog evidence.*

Standard releases

Monday weekly cycle. New rules deploy in Log mode for one week (false positive validation), then promote to Block. Provides layered protection during UWA's standard patch validation period.

Recent CVE Coverage — Confirmed from WAF Changelog

CVE	Vulnerability	CVSS	Cloudflare Response	Mode
CVE-2025-27636	Apache Camel — code injection, RCE	9.2	Emergency rule day of disclosure (11 Mar 2025)	**Block**
CVE-2025-29927	Next.js — auth bypass, unauthenticated route access	9.1	Emergency rule same day (22 Mar 2025). *Initially Disabled — must be enabled in UWA account.*	**Disabled***
CVE-2024-53677	Apache Struts — remote code execution	9.5	Weekly release (13 Jan 2025)	**Block**
CVE-2021-44228	Log4Shell — critical RCE in Log4j	10.0	Emergency rule within hours of disclosure (Dec 2021)	**Block**

Auditability: WAF Change Log at `developers.cloudflare.com/waf/change-log` — timestamped record of every rule with CVE references. Directly usable as E8 audit evidence.

***Disabled rules:** UWA should audit their account to confirm relevant CVE rules are enabled. Jason Clarke can assist in the PoC baseline phase.

Beyond Signatures — ML & Positive Security Model

WAF ATTACK SCORE — ML DETECTION

Every HTTP request scored **1–99** for likelihood of being SQLi, XSS, or RCE. Score is independent of any specific rule match — reflects structural/behavioural characteristics vs. observed attack traffic. *(Numeric score: Enterprise plan. Categorical: Business plan.)*

E8 implication: A novel zero-day with no existing Cloudflare rule may still be blocked if its request structure scores high. Protection exists *before* a specific rule is written.

API SHIELD — POSITIVE SECURITY MODEL

OpenAPI schema defines the exact expected structure of valid API requests. Any request that deviates — unexpected parameters, malformed payloads, wrong HTTP method — is blocked regardless of whether a CVE rule exists.

UWA trial finding:

3,309

API endpoints discovered in February 2026 — the highest monthly total on record. Many likely undocumented, outside any existing patch programme. Schema validation provides coverage from the moment schemas are applied.

Virtual Patching — Honest Coverage Scope

✓ Cloudflare covers

- HTTP/HTTPS-exploitable CVEs with distinguishable request pattern
- SQLi, XSS, RCE, LFI/RFI, command injection, SSRF, auth bypass via headers
- Zero-days in major frameworks — Apache, Next.js, Struts, IIS, Nginx, Oracle WebLogic
- Novel variants caught by ML Attack Score (no rule needed)
- API zero-days blocked structurally via schema validation
- Supply-chain JS compromise via Client-side Security
- EOL systems — edge coverage while decommission is planned

✗ Outside scope

- Kernel exploits, memory corruption, local privilege escalation
- Application logic flaws (IDOR) — WAF cannot distinguish intent where payload is valid
- Niche software not widespread enough for a managed rule
- CVEs older than ~3 years (out of managed rule scope)
- Server-side errors occurring post-edge

Correct framing: Defence-in-depth — not a substitute for patching. Closes the exposure window for the highest-risk HTTP-delivered vulnerability classes while patches are validated.

What Cloudflare Is Already Doing for UWA

August 2025 — the same month as UWA's credential breach — Cloudflare was simultaneously absorbing coordinated application-layer attacks:

54

Application-layer attacks mitigated in Aug 2025

33K

Requests/sec peak attack (17 Aug 2025)

11.9M

Malicious requests mitigated Aug 2025

34.5GB

Attack traffic absorbed in Aug 2025

Bot traffic growth

+300% over 11 months (15M → 60M req/month). 20M likely-automated requests in Feb 2026.

API exposure (trial)

3,309 API endpoints discovered in Feb 2026. 2,218 added to active management in March 2026.

Third-party script risk

Client-side Security trial monitoring Google, Facebook, TikTok, LinkedIn, and 6+ other vendor scripts across UWA properties.

SECTION 4

Callista PoC & Next Steps

Proposed implementation approach and compliance evidence framework

Why Callista as the Primary PoC

Crown jewel — high-value target

Manages sensitive student enrolment, results, and financial data.

Oracle dependency = exact E8 gap

Oracle patches require third-party validation. 48-hour E8 requirement is structurally unachievable without a compensating control.

Internet-facing — directly in scope

Publicly accessible web interfaces; directly subject to E8 Patch Applications requirements.

Representativeness

The constraints affecting Callista — vendor dependency, change management, semester availability — are **identical to those affecting the majority of UWA's internet-facing application estate.**

A successful Callista implementation establishes the **template, evidence framework, and operational process** that can be applied to all other crown jewel applications without starting from scratch.

Callista PoC — Four Phases to E8 ML1 Compliance

Phase 1

Baseline

Review WAF managed rule coverage for Callista. Identify active rules and gaps vs. Oracle/Callista CVE history. Confirm disabled-mode rules.

→ Documented coverage state

Phase 2

Monitor Mode

Deploy WAF rules in alert/log mode. Tune to eliminate false positives against legitimate Callista traffic. Establish FP baseline.

→ Validated rule set + FP baseline

Phase 3

Block Mode

Promote tuned rules to blocking. Establish monitoring and alerting. Confirm Leaked Credentials Detection configured to block.

→ Active compensating control

Phase 4

Evidence Package

Generate compliance report: active rules, CVE coverage, blocked attempt log, WAF Change Log entries for specific CVEs.

→ E8 ML1 audit evidence package

Compliance target
Nov 2025

Start
ASAP

First milestone
In-person workshop

E8 Compliance Evidence — What Cloudflare Produces

WAF Managed Rules Status

Dashboard → Security → WAF

Which rule sets are active on which UWA properties. Per-property configuration documented.

WAF Change Log (Timestamped)

developers.cloudflare.com/waf/change-log

Public record of every rule deployment with CVE references and dates. Proves compensating control was in place for specific CVEs during specific timeframes.

Security Events Log

Dashboard → Security Events

Which requests were blocked, by which rule, with timestamps. Shows the compensating control acting in real time.

API Shield Endpoint Inventory

API Shield → Endpoint Management

Complete API surface map with schema coverage status. Shows which endpoints are protected by positive security model.

This package produces documented, timestamped evidence that compensating controls were in place for specific CVEs during specific timeframes — directly meeting the E8 requirement to document exceptions and their associated compensating controls.

Next Steps & Decision Required

Decision required from Goran

In-principle approval of the compensating controls framework, so the Callista PoC can be scoped and commenced within the November 2025 compliance timeline. Jason Clarke will follow up within two business days to propose a working session date.

IMMEDIATE (WITHIN 2 WEEKS)

- **Trial readout document** — written summary of API Shield + Client-side Security findings; full API endpoint inventory and third-party script risk baseline.
- **WAF coverage mapping** — property-by-property map of active managed rules; identifies gaps including F5-fronted properties.
- **CVSS threshold documentation** — confirm score thresholds used for automatic rule application.

SHORT TERM (4–6 WEEKS)

- **Callista PoC in-person workshop** — whiteboard session to design and scope the phased WAF deployment.
- **SOC logging configuration** — work with Tony Zhao's team on log export to the new SOC provider.
- **E8 evidence package** — initial compliance documentation report from UWA's Cloudflare account.

CLOUDFLARE

Thank you

Jason Clarke
Senior Solutions Engineer
jason.clarke@cloudflare.com

Ian Hogben
Account Manager
ian.hogben@cloudflare.com

WAF Change Log (audit evidence): developers.cloudflare.com/waf/change-log
Full proposal document: Available as accompanying Google Doc