CLOUDFLARE

Fortescue
L7 DDoS Protection

Unsolicited Opportunity Brief – April 2026

New Logo Enterprise UNPROTECTED ORIGIN

Customer Profile

Who is Fortescue?

ABOUT

Industry
Iron ore mining, green energy & technology. One of the world's largest iron ore producers.

Listed
ASX: FMG — A$18.5B FY25 revenue. A$45B+ in dividends paid over 20 years.

Operations
Pilbara, WA. Global green energy projects across Americas, Europe & Middle East.

Headcount
~13,000 employees globally across mining, energy and technology divisions.

A$25.9B
Total global economic contribution (FY25)

2.5B t
Iron ore shipped since 2008

330+
Cities Cloudflare network spans

2030
Real Zero (Scope 1&2) emissions target

Key web properties: fortescue.com · investors.fortescue.com · zero.fortescue.com · capital.fortescue.com

Why Fortescue is a DDoS Target

ASX-Listed

Investor relations site down during an earnings release or trading update is a market-sensitive event. IR site outage = regulatory exposure.

Geopolitical Exposure

Iron ore trade with China creates visibility with state-affiliated threat actors. Critical infrastructure profile per ASD/CISA advisories.

High-Profile Brand

Fortescue's green energy ambitions and media presence make them a hacktivist target. Andrew Forrest's public profile adds personal exposure.

Major Announcements

Acquisitions, ASX announcements and investor days create predictable high-traffic windows — ideal timing for a DDoS attack.

Critical Infrastructure

Major iron ore and green energy operations. Web presence supports supplier, investor, and partner-facing workflows.

Cost of Downtime

A$18.5B annual revenue. A single day of IR/comms downtime during a material event vastly exceeds the full annual cost of enterprise DDoS protection.

Current State

Infrastructure Recon Findings

> *"Your sites already sit on Cloudflare's network. You just don't own any of it."*

Property	IP / Provider	CF Proxy?	Fortescue Controls It?
`fortescue.com`	64.239.109.1 — **Vercel**	⚠ Via Vercel's CF account	✗ No
`investors.fortescue.com`	Vercel (same infra)	⚠ Via Vercel's CF account	✗ No
`zero.fortescue.com`	Vercel (same infra)	⚠ Via Vercel's CF account	✗ No
`capital.fortescue.com`	Vercel (same infra)	⚠ Via Vercel's CF account	✗ No
`content.fortescue.com`	172.64.x.x — **Cloudflare**	✓ **Via Sitecore's CF account**	✗ No
`vault.fortescue.com`	104.18.x.x — **Cloudflare**	✓ **Via Sitecore's CF account**	✗ No

DNS managed by CSD DNS (cscdns.net). Email via Proofpoint. Live recon: April 2026.

The Vercel DDoS Gap

WHAT VERCEL PROVIDES

- L3/L4/L7 DDoS mitigation — automatic, all plans
- WAF with basic custom rules (Pro/Enterprise)
- Attack Challenge Mode (blanket CAPTCHA)
- Alerts at >100K requests per 10 minutes

WHAT FORTESCUE DOESN'T GET

- **Zero visibility** — no Security Events, no Logpush, no analytics dashboard
- **Zero tuning** — cannot adjust DDoS sensitivity thresholds
- **No adaptive protection** — no traffic baseline profiling, no ML scoring
- **No enterprise SLA** — Vercel's DDoS is best-effort, no uptime guarantee for security
- **Opaque and vendor-controlled** — Vercel can change, pause, or modify protection at any time

Recommended Solution

Proposed Architecture

BEFORE – CURRENT STATE

Internet / Attacker

Unfiltered traffic

Vercel Edge

fortescue.com (64.239.109.1)
Basic DDoS — not configurable

Vercel Origin / Functions

Next.js SSR

⚠ Vercel IP publicly exposed · No Fortescue visibility · Vercel-controlled protection

AFTER – CLOUDFLARE ENTERPRISE

Internet / Attacker

Attack traffic

Cloudflare Enterprise Edge

L7 DDoS scrubbing · WAF · Adaptive Protection
330+ PoPs · Fortescue controls all rules

Vercel Edge (Origin)

Clean traffic only · IP allowlisted to CF ranges

Vercel Origin / Functions

Next.js SSR — unchanged

Onboarding: CNAME setup — Fortescue keeps CSD DNS, adds CNAME records pointing to Cloudflare. No origin infrastructure changes required.

Cloudflare Enterprise + Advanced DDoS

ENTERPRISE WAF/CDN (BASE)

- **Always-on HTTP DDoS managed ruleset** — zero config, auto-blocks known attack patterns
- **Unmetered DDoS** — no per-Gbps billing during attacks
- **WAF managed rules** — Cloudflare Managed + OWASP rulesets
- **Proactive false positive detection** for new rules before deployment
- **100% uptime SLA** · 24/7 phone & email support

+ ADVANCED DDOS PROTECTION (RECOMMENDED)

- **Full Adaptive DDoS** — For Origins, User-Agents & Locations (geo-profiling)
- **ML-score profiling** — client country, user agent, query string signals
- **10 custom ruleset overrides** with expression filtering (vs 1 on base plan)
- **Advanced alerts** with filtering — PagerDuty, webhook, email
- **7-day traffic profiling** — system learns Fortescue's baseline before enabling block mode

Externa Package — Bundle as an **Externa package** — no attack traffic tax, simple value-driven pricing, includes **50 Interna (SASE) seats** as a Zero Trust on-ramp.

Key Technical Considerations

01 – SSL/TLS

Set CF SSL mode to **Full (Strict)**. CF terminates TLS at the edge, then opens a new validated connection to Vercel's origin cert. Do not use Flexible mode.

02 – Real IP Passthrough

Without configuration, Vercel sees CF's edge IP, not the real visitor. CF adds `CF-Connecting-IP` header — Vercel Enterprise must be configured to trust CF as a proxy for accurate analytics and IP-based rules.

03 – Origin Lockdown (Critical)

After orange clouding, Vercel's backend IP remains publicly known (shared Vercel infra). An attacker could bypass CF entirely. **Lock Vercel to accept traffic only from Cloudflare's IP ranges** using Vercel's trusted IP allowlist. This closes the bypass gap.

04 – Caching & Performance

CF caches static assets at its edge — Vercel is not hit for cached content (**faster, lower Vercel costs**). Dynamic/SSR content adds ~10–30ms hop but both CF and Vercel have Sydney PoPs, minimising AU latency impact.

✓ **Double protection benefit:** Vercel's platform-level DDoS stays active underneath Cloudflare. Attack traffic stopped by CF never reaches Vercel. Anything that slips through CF hits Vercel's protection as a second layer.

Business Value

Why Cloudflare — and Why Now

No Attack Traffic Tax

Only pay for clean traffic. Unlike Akamai Prolexic and Imperva, Cloudflare does not charge per-Gbps during an active DDoS attack.

Unmetered DDoS

No matter the scale of attack, Cloudflare absorbs it at the network layer. 321 Tbps network capacity — the largest in the industry.

Full Control

Fortescue owns their security posture. Tune DDoS sensitivity, write custom WAF rules, monitor every event in real time — not possible with Vercel.

Global Edge Scrubbing

Attack traffic is scrubbed closest to the attacker — not at Fortescue's origin. 330+ PoPs, ~50ms from 95% of the internet.

Enterprise Visibility

Security Events dashboard, Logpush to SIEM, real-time attack analytics, and advanced alerting. Full audit trail for incident response.

SASE On-Ramp

Externa package includes 50 Interna (SASE) seats. Natural expansion into Zero Trust for Fortescue's 13,000-person workforce — one platform, one vendor.

Cost-to-risk framing: Fortescue's IR site down during an ASX announcement or investor day is a material market event. Annual DDoS protection cost (~$70–120K USD) is a fraction of a single day's revenue (A$18.5B / 365 ≈ A$50M/day).

Cloudflare & Australian Cyber Defence

ASD's ACSC Annual Cyber Threat Report 2024–25

Australia's Government technical authority on cyber security

280%

Increase in DDoS incidents in Australia — year on year

ASD's ACSC responded to **more than 200 incidents** involving DoS or DDoS attacks. The rise of DDoS attacks against Australian organisations has the potential to cause significant disruptions across the Australian economy.

55% Increase in DDoS attacks globally year on year — Cloudflare threat intelligence

GOVERNMENT PARTNERSHIP

- **March 2025:** ASD's ACSC co-published official DDoS guidance with **Cloudflare Pty Ltd**
- **Malicious website programme:** ASD's ACSC uses Cloudflare's API-based abuse reporting to programmatically identify and act on malicious Australian websites

CLOUDFLARE NETWORK SCALE

477 Tbps Network capacity (and growing)	**215B** Cyber threats blocked every day
22M+ Peak monthly threats blocked (AU customers)	**10×** Increase in WAF & Firewall events (AU)

Source: ASD's ACSC Annual Cyber Threat Report 2024–25 · cyber.gov.au · Cloudflare threat intelligence (slides provided by Cloudflare AU team)

Traffic Profile & Pricing

Traffic Profile — Fortescue.com

SEMRUSH DATA – MARCH 2026

121K
Visits/month
+14% MoM

450K
Page views/month
(3.71 pages/visit)

9:01
Avg session duration

50%
Bounce rate

Geographic distribution

Australia	52% – 63K visits
United Kingdom	21% – 26K visits
Canada	11% – 14K visits
United States	4% – 4.7K visits

HTTP REQUEST VOLUME ESTIMATE

Used for Cloudflare quote sizing

450K page views × ~30 sub-requests (Next.js SPA)

≈ 13.5M requests/month — fortescue.com

≈ 30–45M requests/month — all 4 zones combined

Page response sizes (measured)

`fortescue.com/en/`	~402 KB
`investors.fortescue.com/en/`	~285 KB
`zero.fortescue.com/en/`	~182 KB

ℹ For deal desk: Low-to-mid volume enterprise profile. Pricing argument is risk-adjusted value, not traffic cost savings.

Indicative Cost Estimate

ANNUAL COST BREAKDOWN (USD)

Enterprise WAF/CDN 4 zones: fortescue.com, investors, zero, capital	$50–80K
Advanced DDoS Protection Adaptive profiling, ML scoring, 10 overrides	$20–40K
50 × Interna Essentials Seats Included with Externa package	Included
Total estimated annual	$70–120K USD

Important notes

Cloudflare Enterprise has no public rate card — all pricing is negotiated via deal desk (SFDC CPQ).

3-year contract preferred for best discount. 1-year available.

Traffic volume is low-to-mid enterprise — pricing argument is **risk value**, not cost savings.

Cost vs. risk

Fortescue FY25 revenue: **A$18.5B**
Revenue per day: **≈ A$50M**

One day of IR/comms downtime during an ASX material event exceeds the entire annual contract value by **300–500×**.

Competitor comparison: Akamai Prolexic and Imperva charge per-Gbps during attack events. During a large attack this can cost $50–200K in a single incident. Cloudflare's unmetered model eliminates this entirely.

Recommended Next Steps

1 Qualify the Opportunity

Identify the CISO/CTO contact at Fortescue. Research procurement cycle — FMG financial year ends June 30, so H2 budget planning starts now.

2 Outreach — Lead with Recon

Share the infrastructure findings: "Your sites sit on Cloudflare but you don't control the DDoS configuration." This is a compelling, provable opener for an unsolicited approach.

3 Propose a Free Trial / PoV

Offer a 30-day Enterprise trial on fortescue.com — CNAME setup, log-mode only, zero risk. Shows them their attack surface in real time before they commit.

4 Generate Indicative Quote

Work with deal desk via SFDC CPQ. Scope: 4 zones, Enterprise WAF/CDN + Advanced DDoS add-on, 3-year term. Target: $70–120K USD/year.

5 Expand Conversation to SASE

Fortescue's Zero/Capital/Elysia divisions and remote Pilbara workforce are natural Zero Trust candidates. DDoS entry → Interna (SASE) expansion story.

Account Summary

New logo · No CF presence · 4 unprotected zones · ~$70–120K USD opportunity · Strong SASE expansion path · ASX-listed risk profile justifies urgent outreach.

APPENDIX

Vercel vs Cloudflare DDoS Battlecard

A technical and commercial comparison for sales conversations

Architecture & Detection Model

Vercel

126 PoPs — L3/L4 only

TCP termination and basic volumetric drop. No WAF, no TLS, no L7 inspection at this layer.

↓ private network hop

20 Compute Regions — L7 firewall

TLS terminates here. WAF, challenge, JA3/JA4, DDoS rules all evaluated here — not at the edge. Attack traffic must reach a compute region to be assessed.

⚠ Sophisticated L7 floods reach the compute region before being assessed. No adaptive profiling. No ML scoring. Detection is static fingerprinting only.

Cloudflare Enterprise

330+ PoPs — Full stack at every city

TCP termination, TLS termination, HTTP DDoS managed ruleset, WAF, rate limiting and adaptive DDoS all fire at the ingress PoP. No extra hop required.

Adaptive DDoS — 7-day traffic baseline

Learns Fortescue's traffic profile. Detects deviation by geo, user agent, query string, and ML score. Escalates from Log → Block automatically — no human required.

✓ 477 Tbps network capacity (published). Attack traffic scrubbed closest to the attacker, not at a centralised compute region.

Billing & Availability During an Attack

VERCEL – WHAT HAPPENS

Attack traffic is billed

Requests served before mitigation kicks in incur Function invocation, Fast Data Transfer, and Edge Request charges. A 100K req/min L7 flood = millions of billable invocations per hour.

Spend limit hit → all 4 sites auto-pause

If Spend Management is configured, all projects return `503 DEPLOYMENT_PAUSED` to every visitor. Fortescue effectively DDoS's themselves. Manual per-project recovery required.

Attack Challenge Mode = blanket JS challenge

Only manual defence available. All visitors — investors, media, suppliers — see "Vercel Security Checkpoint." Cannot be scoped to suspicious traffic only.

Alert fires at >100K req / 10 minutes

Notification only — no automated escalation. Fortescue must manually respond during a live attack with no real-time traffic analytics.

CLOUDFLARE ENTERPRISE – WHAT HAPPENS

Zero billing for attack traffic

Cloudflare's unmetered DDoS model means attack traffic is absorbed at the network layer with no per-request, per-Gbps, or per-invocation charges. Predictable costs during any attack.

Sites stay online — always

100% uptime SLA. Legitimate traffic continues to be served while attack traffic is blocked. No self-pausing, no 503s for investors.

Managed Challenge — surgical, not nuclear

Challenge can be scoped to suspicious IPs, geos, or user agents. Legitimate investors browsing from known locations are never challenged.

Automated escalation — no human required

Adaptive DDoS moves from Log to Block automatically. Advanced alerts with filtering sent to SIEM/PagerDuty. Full Security Events audit trail available in real time.

Feature Comparison — Vercel vs Cloudflare Enterprise

Capability	Vercel (current state)	Cloudflare Enterprise + Advanced DDoS
L3/L4 DDoS mitigation	⚠ At 126 PoPs. Unpublished capacity limit.	**✓ All 330+ cities. 477 Tbps published capacity.**
L7 DDoS inspection location	✗ 20 compute regions only (extra hop)	**✓ All 330+ PoPs at ingress — no extra hop**
Adaptive / ML-based detection	✗ Not available	**✓ 7-day traffic profiling, geo/UA/ML scoring**
Attack traffic billing	✗ Billed until mitigation activates	**✓ Zero — no attack traffic tax ever**
Site availability during attack	✗ Risk of self-pause (503) if spend limit hit	**✓ 100% uptime SLA — never self-pauses**
Post-attack recovery	✗ Manual per-project unpausing	**✓ Automatic — no action required**
Fortescue visibility	✗ None — no logs, no dashboards	**✓ Security Events, Logpush to SIEM, real-time analytics**