CONFIDENTIAL – FOR FORTESCUE USE ONLY

# Fortescue

## Security Threats seen in WA

April 2026

# Security at a Glance

Over the past 12 months, Cloudflare has protected ACME's global web presence — blocking attacks, managing automated traffic, and securing 300M+ DNS queries every month across 6 domains.

**22.7M**

Peak monthly threats blocked

Aug 2025

**~65%**

Traffic to acme.com is automated/bot

Monthly avg

**300M+**

DNS queries protected / month

6 domains

**89%**

Support tickets resolved / closed

19 total tickets

**WAF & Firewall**
10× growth in events since May 2025

**Bot Activity**
Two major attack waves identified

**Multi-Layer Defence**
CDN, DNS, Spectrum, API Shield active

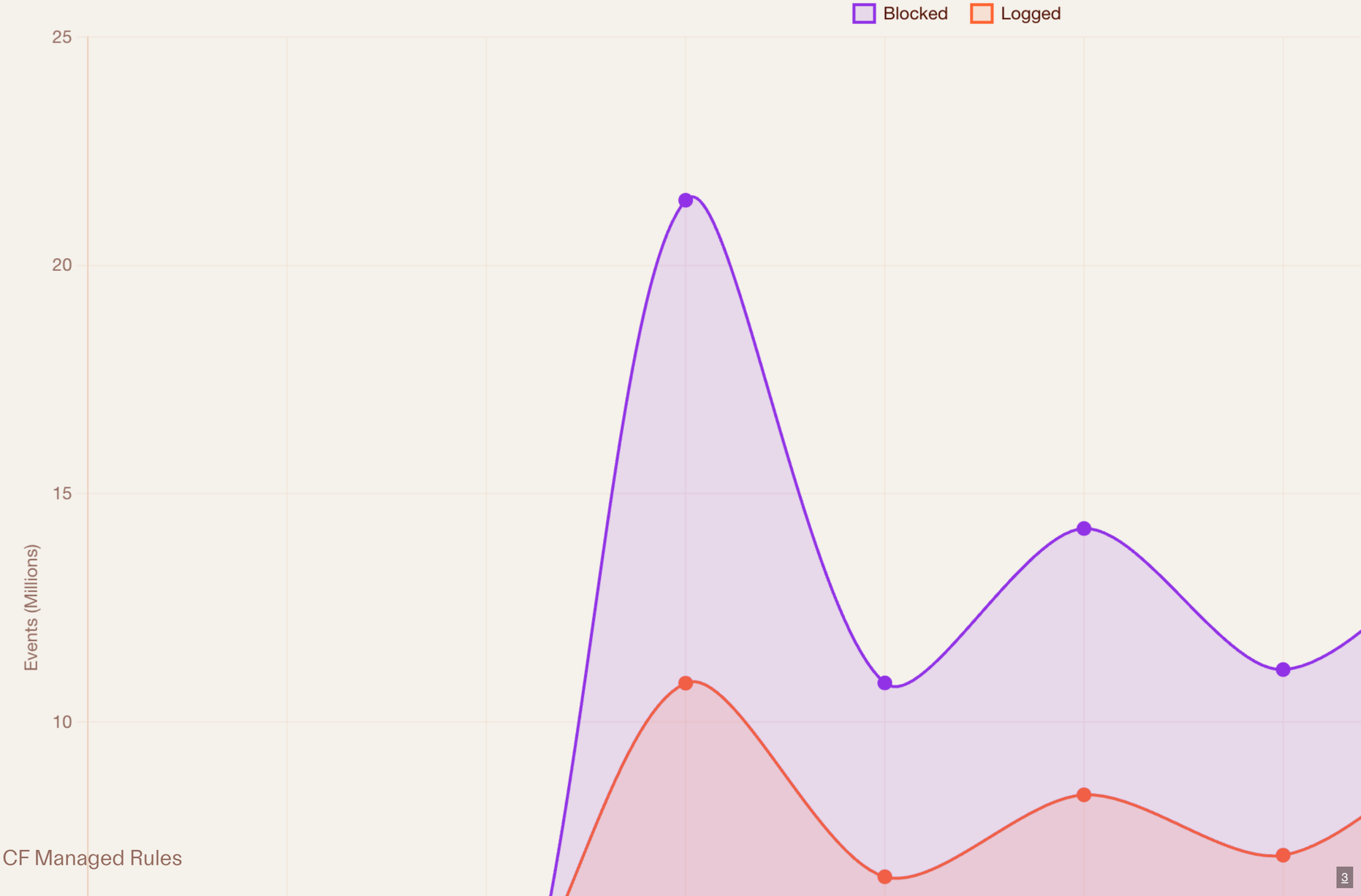
Download Slides

# WAF & Firewall — CF Managed Rules

**22.68M**
Peak blocks
Aug 2025

**22.18M**
Second wave
Jan 2026

**10×**
Growth since
May 2025




acme.com zone · May 2025 – February 2026 · CF Managed Rules

Download Slides

# Recommendations & Next Steps



1

## Deploy Bot Management

Challenge suspicious bots, protect logins, and reduce WAF noise. ~65% of acme.com traffic is non-human — Bot Management provides granular control beyond classification.

2

## WAF Rules Audit & Consolidation

6+ years of legacy rules need rationalisation. Joint SE review + App Security Reports (now GA) to retire duplicates, reduce false positives, and modernise to WAF 2.0.

3

## Expand API Shield Coverage

Actual API traffic (550M/month) is 3.7× the contracted allowance. Run API Discovery to surface shadow endpoints — ACME's security team is already a strong internal champion.

4

## AI Gateway & AI Security

Govern AI developers with visibility into LLM API usage. Firewall for AI protects AI-enabled apps. Addresses ACME's data leakage concerns without blocking innovation.

5

## Zero Trust Access — Developer SSO

Complete Entra ID + group RBAC integration. This is the blocker for the developer platform and expanding Zero Trust coverage beyond the current pilot.

6

## Cache Rules — Reduce Origin Load 40–60%

ACME's current cache hit rate is 0.09%. Adding Cache Rules for images, JS, CSS & fonts could serve the majority of static traffic from Cloudflare's edge — cutting origin costs and improving global load time.

# 29.43M Requests — Here's What They Were

**14.86M**
50.5%
LIKELY HUMAN

**6.42M**
21.8%
VERIFIED BOT

**2.2M**
7.5%
LIKELY AUTOMATED

**5.94M**
20.2%
AUTOMATED (SCORE 1)

**8.14 million unverified automated requests in 7 days**

Nearly **1 in 3 requests** to ACME's estate is unverified bot traffic — all detected and scored by your Bot Management subscription.

# Bot Score Distribution & Detection Sources

SCORE 1 = DEFINITELY AUTOMATED | SCORE 99 = DEFINITELY HUMAN


DETECTION ENGINE

**Machine Learning**

**16.71M**

Scores every request 1–99 — catches spoofed bots that look human at the network layer

**Heuristics**

**6.29M**

Pattern-matched known malicious fingerprints — instant score of 1

**Verified Bot**

**6.42M**

Legitimate crawlers — Google, Bing — identified and allowlisted

Download Slides

# Bot Detection Tags — 5 Categories Hitting ACME

**ai_bot**

AI crawler agents — GPTBot, CCBot, Bytespider — systematically harvesting ACME's content, documentation, and proprietary data to train commercial LLMs without permission.

**2.85M**

**empty_ua**

Automated scripts with no user agent set. No legitimate browser ever does this — these are scrapers and attack tooling running in bare HTTP clients.

**1.67M**

**spoofed_bot**

Bots deliberately impersonating legitimate browsers. Faking user agents, mimicking human HTTP behaviour. A firewall rule or rate limit won't catch these — only ML behavioural analysis does.

**1.61M**

**sneakerbot**

Automated form-submission and account automation tools. In an enterprise context: automated attempts against account portals, registration systems, and login endpoints.

**1.55M**

**java**

Java-based HTTP clients — typically bulk data extraction pipelines and enterprise scraping tools. Not a browser, not a user.

**1.24M**

# What's Being Targeted

## TOP HOSTS BY REQUEST VOLUME

| | |
|---|---|
| www.acme.com | 10.81M |
| cdn.acme.com | 5.76M |
| hr.acme.com<br>HR / Payroll System | 1.53M |
| hr2.acme.com<br>HR / Payroll System | 1.39M |

⚠ 2.92M automated requests hit ACME's HR & payroll platform in 7 days. This system holds staff contracts, salary, and personal data.

## TOP PATHS BY REQUEST VOLUME

| | |
|---|---|
| /api/v/<br>REST API — Internal Systems | 1.63M |
| / | 807K |
| /repo/browse<br>Content Repository | 590K |
| /home | 336K |
| /api/ws/<br>REST API — Internal Systems | 322K |

🤖 2.85M ai_bot requests cross-referenced with /repo/browse — ACME's content repository is being systematically harvested.

Download Slides

# Where the Bots Are Coming From

## TOP SOURCE ASNS

**4.94M**

AS8075 — MICROSOFT AZURE

**2.69M**

AS16509 — AMAZON AWS

**7.63M requests from cloud infrastructure**

Attackers and AI crawlers run from cloud providers — cheap, scalable, and clean IP ranges that basic IP blocklists miss entirely. Only ML fingerprinting catches these reliably.

## TOP SOURCE COUNTRIES

| | |
|---|---|
| Australia | 11.64M |
| United States | 4.78M |
| Singapore | 1.80M |
| Canada | 1.27M |
| China | 1.09M |

ACME's user base is predominantly Australian — yet **more than one third of all traffic originates overseas**. The US alone (4.78M) nearly matches Australia's bot contribution, driven by cloud-hosted automation.

Download Slides