Turning
Chaos into Control
with Cloudflare

John Adib

Organized By

Hosted By
CLOUDFLARE

24 | September | 2025

Cloudflare, 6th Floor, The County Hall,
Belvedere Rd, London SE1 7PB

When Reality Hit

Marks & Spencer - April 2025

OUR DIGITAL CLICK
& COLLECT SERVICE
IS TEMPORARILY
UNAVAILABLE

We're experiencing technical issues
with digital collection and returns.

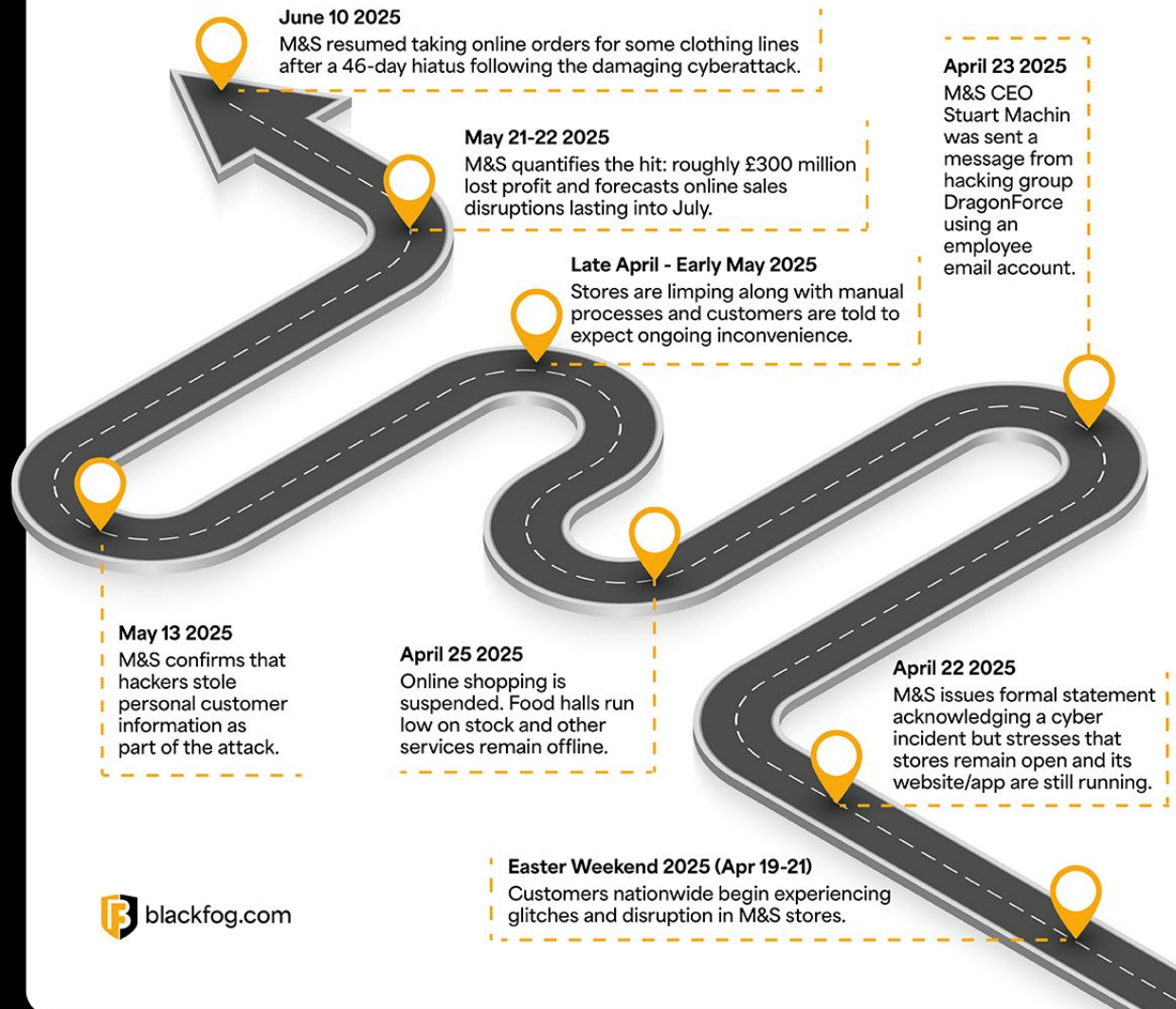Please speak to a colleague
if you need assistance.

M&S

The Scale of Damage

46 days of disruption

£300m loss

June 10 2025
M&S resumed taking online orders for some clothing lines after a 46-day hiatus following the damaging cyberattack.

May 21-22 2025
M&S quantifies the hit: roughly £300 million lost profit and forecasts online sales disruptions lasting into July.

April 23 2025
M&S CEO Stuart Machin was sent a message from hacking group DragonForce using an employee email account.

Late April - Early May 2025
Stores are limping along with manual processes and customers are told to expect ongoing inconvenience.

May 13 2025
M&S confirms that hackers stole personal customer information as part of the attack.

April 25 2025
Online shopping is suspended. Food halls run low on stock and other services remain offline.

April 22 2025
M&S issues formal statement acknowledging a cyber incident but stresses that stores remain open and its website/app are still running.

Easter Weekend 2025 (Apr 19-21)
Customers nationwide begin experiencing glitches and disruption in M&S stores.

blackfog.com

TURNING CHAOS INTO CONTROL
WITH CLOUDFLARE

24 SEPTEMBER 2025

JOHN ADIB

Not Just Node.js

Node.js everywhere, plus some Python

Too Many Deployment Models

Cloud Functions. Cloud Run. Kubernetes. Firebase.

Scattered URLs

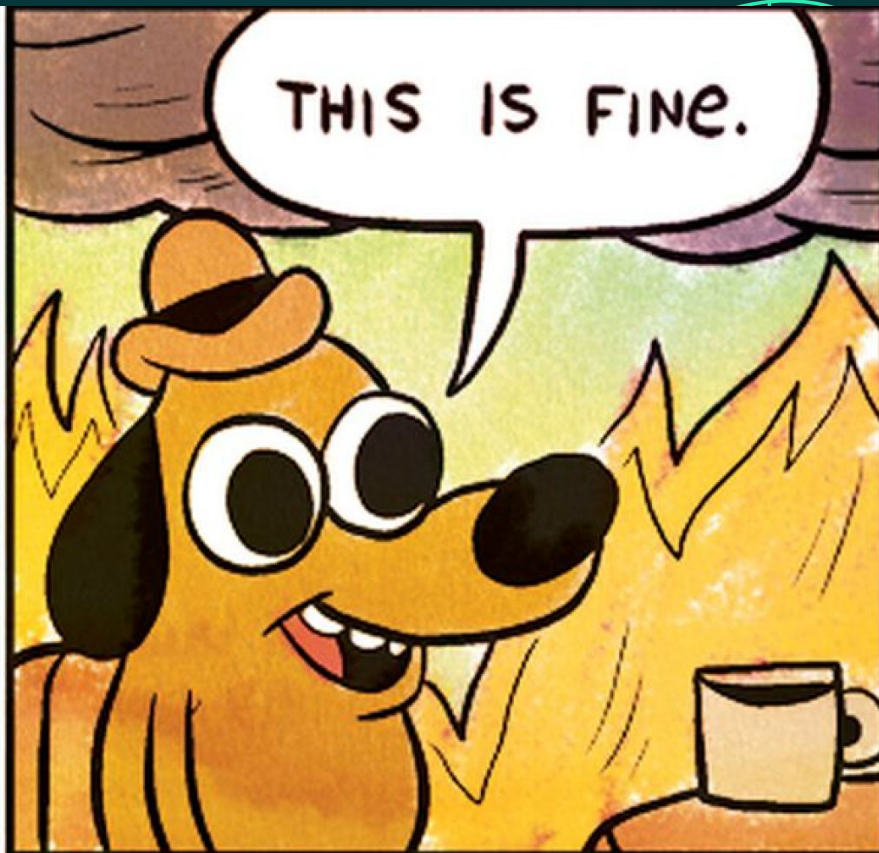Multiple domains. Cloud Run URLs. No single entry point.

Security Gaps

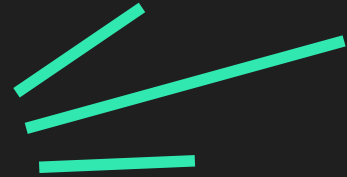Public endpoints. Direct DB access. No Zero Trust model.

High Business Stakes

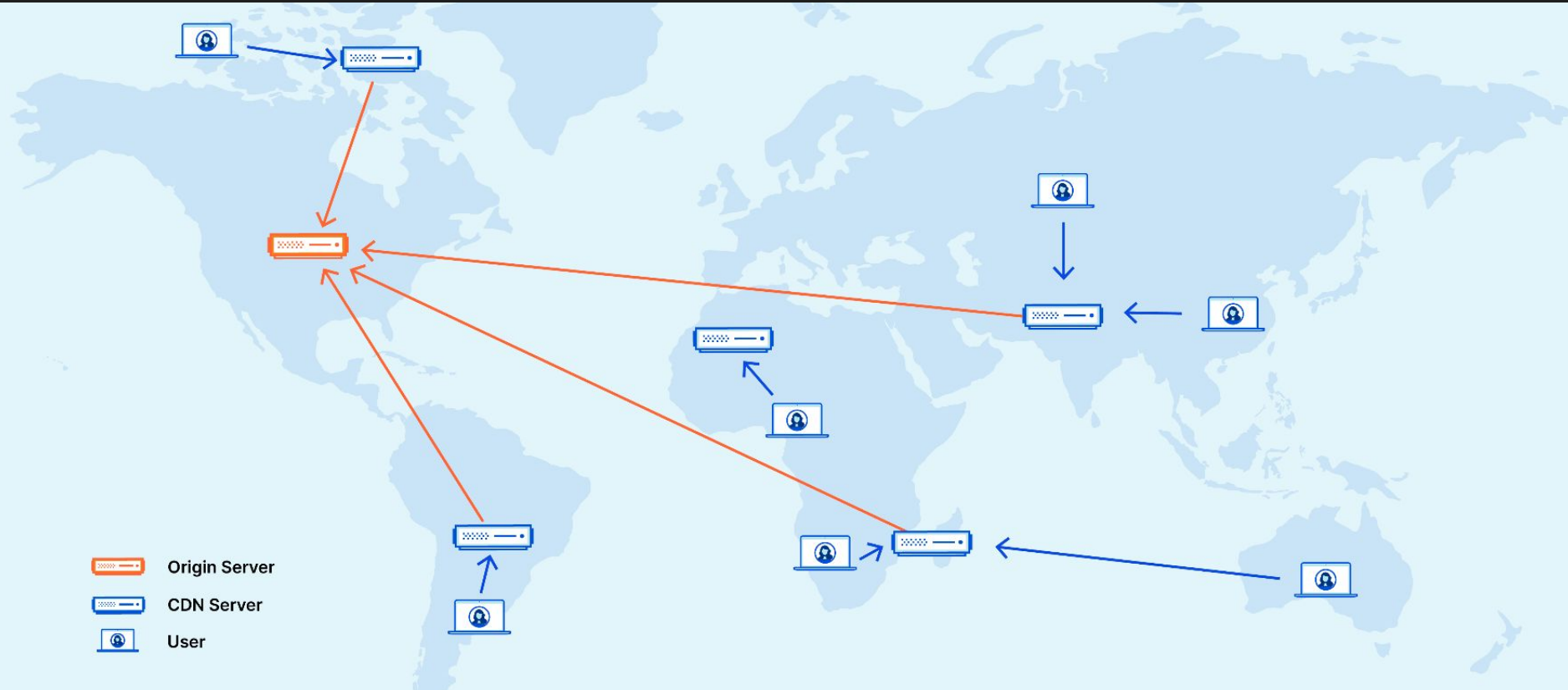Thousands of orders. Millions of requests. Security matters.
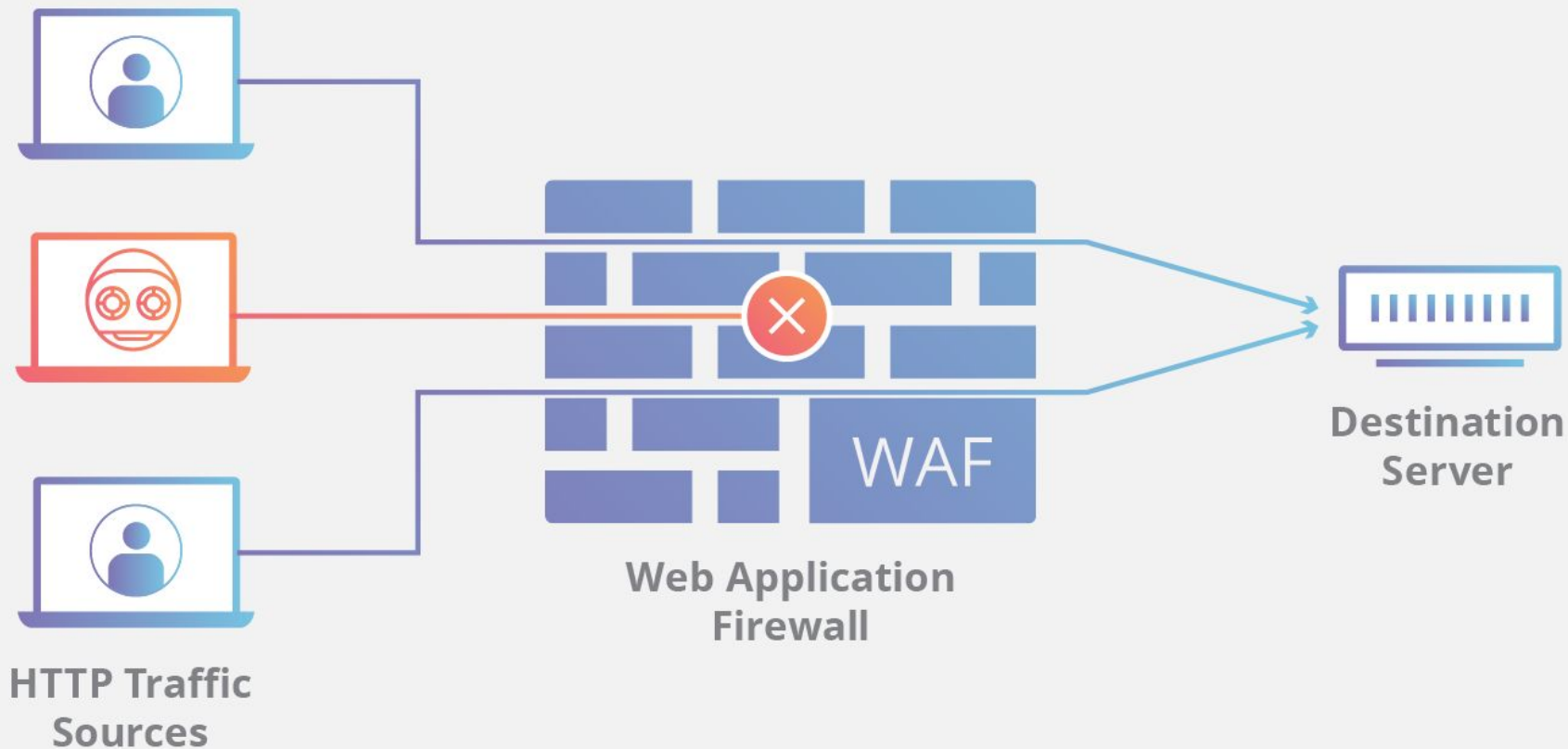
Foundation of the Solution

CDN - Content Delivery Network

Origin Server

CDN Server

User

WAF - Web Application Firewall

HTTP Traffic Sources

Web Application Firewall

Destination Server

WAF

Authentication

Who you are

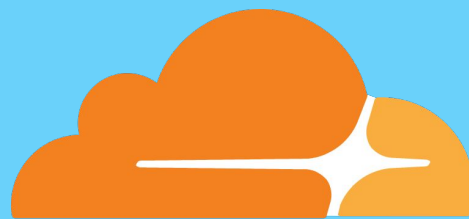# Authorization

What you can do after login

Single Sign-On (SSO)

One login for everything

Zero Trust

Never trust, always verify

One Domain for All

One front door instead of many URLs

Protecting Everything

APIs, events, and UI all behind Cloudflare

Customer-Facing website

Better experience for end users

Cloudflare Zero Trust

From dev to prod, every request checked by policy

Reality Check

One-Time PIN Issues

OTP delays → moved to Google Login

CF Zero Trust Pricing

50-user limit

Pay-as-you-go £7 per user

GCP Cloud Run

No custom domain support for servers in London (eu-west-2)

GCP Load Balancer + Cloud Armor

Extra Layers We Didn't Plan For

E2E Testing

E2E tests need headers to bypass Zero Trust

QA

Are we happy with the result?

Yes!

Did we face any surprises?

Yes!

Was that the best solution?

Yes!

All your cyber security efforts

That one employee clicking on a phishing link

Thank you, Let's connect!

MrAdib.com