Deploying Darwinium via your CDN

A lightweight deployment that protects your entire customer journey in days, with virtually no engineering work on your side.

HOW IT WORKS

Darwinium connects directly to the CDN you already use (Cloudflare, CloudFront, or Akamai), the service that sits in front of your website and delivers content to your customers. Because Darwinium operates from that vantage point, it sees and protects every step of the customer journey, including web, mobile, APIs, and AI-agent traffic, without your developers changing a single line of your website or applications.

While most vendors will tell you their solution is easy to implement, they typically require adding a tracking script to every page and writing backend code for every decision point, which involves more heavy lifting from your side. A CDN-based solution is different.

AT A GLANCE: CDN DEPLOYMENT VS. TAGS + API

	Darwinium via your CDN	Typical tags + API approach
Time to go live	**Days.** Darwinium does the heavy lifting using infrastructure you already have.	**Months.** An engineering project to instrument every page and decision point.
Engineering work for your developers	**None.** No code changes to your website, apps, or backend.	Developers add script tags to every protected page and write backend code for every decision point, then maintain both.
Who is involved on your side	One IT/CDN administrator (about half a day), your fraud team, and one security review.	Frontend, backend, fraud, and security teams, coordinated across multiple release cycles.
Making changes after go-live	Your fraud team can self-serve. Changes can go live in minutes with no engineering tickets.	Each change to what is monitored waits on engineering backlogs and release schedules.
Where your data lives	Processed and stored within your own CDN infrastructure, supporting data-residency rules.	Typically sent to and processed in the vendor's cloud.

WHAT WE NEED FROM YOUR TEAM

ROLE	TIME COMMITMENT	WHAT THEY DO
IT / CDN administrator	About half a day	Grants Darwinium limited, documented access to your CDN account and completes a short, guided setup.
Fraud / risk team	A few working sessions	Decides which customer journeys to protect (e.g., account creation, login, payments) and where to look earlier in the journey for warning signs. Darwinium configures the starting rules and models with you.
Website / app developers	Not needed	No tags to add, no code to write, no release cycles to wait for.
Security / InfoSec	One review	Approves the limited access scope and confirms data handling. Darwinium never sees your customers' data in the clear: names, emails, and other identifiers are encrypted and hashed: only you hold the keys to this.

FROM ZERO TO LIVE WITH DARWINIUM

1. Darwinium provides ready-made journey templates: **account takeover, new-account fraud, payment fraud, scraping**, and more.
2. Our team builds and deploys everything to your CDN, and leaves any **existing CDN logic running untouched**.
3. We set up your **portal, dashboards, and data flows**, and tunes the initial risk strategy with your team.

AFTER GO-LIVE

Your fraud team makes rule, model, or journey changes in the Darwinium Portal and can deploy them in real time, responding to evolving threats as they happen, rather than after the fact, with no engineering tickets and no release-cycle dependency. Routine upkeep is light: occasional rotation of access credentials by IT (per your own security policy) and a periodic refresh, roughly every two months, that Darwinium guides.

LOWER FRAUD LOSSES

Respond as a new fraud or bot pattern appears, no waiting for the next development sprint.

LOWER OPERATING COST

Your fraud team can self-serve. Zero engineering tickets per rule, model, or journey change.

MORE AGILITY

Test, A/B, and roll back from the portal. Changes are live in minutes.

A technical deployment guide with full configuration detail is available for your engineering and security teams.