

ONE CHECKBOX, TWO DECISIONS

What the CloudFront outage revealed about bundled
architecture tradeoffs

YOU WANTED TO HIDE THE ORIGIN

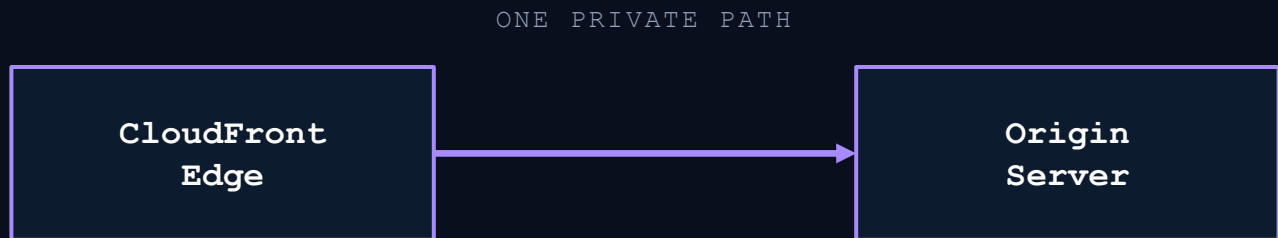


SECURITY OBJECTIVE

A public origin server is reachable by anyone who finds it —
CDN or no CDN. Removing that public IP closes a real,
findable attack surface.

This part of the decision is correct, and reviewed.

THE ORIGIN WENT PRIVATE. SO DID YOUR OPTIONS.



There is no longer a public IP to fall back to. Every request — and every recovery attempt — now runs through exactly one route.

THE EMERGENCY EXIT DISAPPEARED



A public-origin setup keeps a manual fallback — a public IP an operator can reroute to under pressure. VPC Origins doesn't degrade that option. It removes it.

ONE PATH IS NOW DOING THE WORK OF TWO

VPC ORIGINS
CONTROL PLANE

Origin availability and CloudFront's own control-plane availability are no longer two separate questions. They're the same question, answered once.

Nobody signed off on that merge. It happened by default.

ONE AZ. ONE CAPACITY LIMIT. GLOBAL REACH.

JULY 16 · 07:45 UTC

A capacity limit in a single Frankfurt availability zone (euc1-az2) — not a full CloudFront failure, not a weather event.

The edge processors kept running. They just stopped receiving valid routing instructions for VPC Origins traffic — everywhere, at once.

HUGGING FACE. NATIONAL LOTTERY. HUNDREDS OF UNIVERSITIES.

Hugging Face

UK National Lottery

Canvas + Blackboard

Tailscale · Ubiquiti

None of them chose CloudFront for reliability. They inherited it through a security decision.

WHAT ALTERNATIVE DISAPPEARED WHEN YOU CHECKED THAT BOX?

Every review asks what a feature adds.
Few ask what it quietly takes away.