

How CDN Service Outages Caused Repeated Revenue Losses for a UK Digital Dependent Services Operator

CUSTOMER OVERVIEW

- **Industry:** Short term real estate and location based services
- **Geography:** United Kingdom
- **Scale:** Hundreds of distributed physical locations
- **Annual Transaction Revenue:** ~£200M
- **Operational Dependency:** Centralized digital platforms supporting access control, payment processing, and automated detection systems

This organization operates revenue generating physical assets that are entirely dependent on continuous digital service availability to function.



Business Challenge

To safeguard its internet-facing systems, the organization utilized a global CDN platform configured in “always on” mode for enhanced availability and DDoS protection.

The company encountered multiple significant service disruptions attributed to availability issues within the CDN provider’s platform, rather than successful cyberattacks.

Public reporting and statements from the customer’s IT leadership characterized these incidents as costly and highly disruptive. Individual outages were estimated to result in £500K–£2M in lost revenue, primarily due to the inability to deliver core digital services during the outages.

What Actually Happened

CDN service outages became a single point of failure. During multiple incidents, the CDN provider experienced service level outages that prevented legitimate customer traffic from being delivered.

Due to the CDN’s “always-on” architectural design, the following occurred:

- All external access was routed through the CDN.
- Core applications were reachable only via that platform.
- No local or alternate access path was available.

When the CDN service became unavailable, legitimate traffic could not reach business critical systems, despite those systems themselves remaining operational.

These outages were not related to traffic blackholing, mis triggered mitigation, or attack spillover, but rather to availability failures within the CDN service layer.

Operational Impact

Because the organization's business model depended on always on digital access to centralized systems, CDN outages immediately resulted in:

- Inability to authenticate or validate users and assets.
- Failure of automated detection and validation systems.
- Disruption of payment and transaction processing.
- Temporary halt of revenue generating operations at affected locations.

Unlike traditional web or e-commerce downtime, these outages had direct physical world consequences, preventing the organization from delivering or monetizing its services for the duration of each incident.

Why CDN Only Architecture Exposed the Risk

This case highlighted a broader architectural risk increasingly seen in organizations that rely on external platforms for critical availability functions:

1. External platform availability becomes business availability

When all access paths depend on a single upstream service, any provider outage immediately affects core operations, regardless of whether an attack is occurring.

2. CDNs are optimized for web delivery, not operational continuity

CDN platforms are designed primarily for performance and edge protection of web traffic—not for sustaining operational systems that lack local autonomy when cloud connectivity is lost.

3. Lack of architectural independence

With no local, on-path, or near-edge control plane, the organization had no ability to selectively fail open, bypass, or locally preserve service availability during third-party service outages.

Architectural Lesson Learned

The key lesson from this experience was not that CDN services lack value—but that they cannot be the sole dependency for availability in revenue-critical, operational environments.

For this class of organization:

- Availability risks include provider outages, not just cyber threats.
- Protection architectures must avoid introducing new single points of failure.
- Digital services that underpin physical operations require layered and independent availability controls.

This has driven increased emphasis on hybrid, multi-layer availability architectures, where upstream platforms are complemented by localized protection, visibility, and control, ensuring that external service failures do not fully incapacitate the business.

Key Takeaway

This case demonstrates a critical but often overlooked reality:

Availability risk is not limited to attacks—it also includes dependency on upstream service providers.

Organizations whose physical operations depend on digital systems must design for provider failure scenarios, not just attacker behavior, and avoid architectures in which a single external platform outage can halt core business functions.

Public reporting and statements from the customer's IT leadership characterized these incidents as costly and highly disruptive.

The Solution

The Right Architecture: Designing for Attacks and Provider Failures

This experience underscored that protecting availability for digitally dependent operations requires architectural resilience, not just outsourced protection.

The proper model is a layered, hybrid availability architecture that removes any single external platform as a hard dependency for business continuity.

Principles of a Resilient Availability Architecture

A resilient design for revenue-critical digital services should include:

1. Multiple layers of protection

- Upstream, cloud-based services to absorb large-scale volumetric events.
- Local or near-edge controls to preserve availability when upstream services fail or become unavailable.

2. Operational independence

- The ability for core services to remain reachable and controllable even during third-party service outages.
- Avoiding “all traffic must pass here” choke points.

3. Visibility before control

- Continuous insight into traffic behavior and service health.
- Early detection of anomalies that impact availability—whether caused by attacks or provider degradation.

4. Surgical, not blunt, mitigation

- Precision controls that address malicious or disruptive traffic without interrupting legitimate service flows.

How NETSCOUT Enables This Architecture

NETSCOUT's DDoS and availability solutions are designed specifically to support this defense in depth model, complementing—not replacing—upstream CDN services.

Key Capabilities:

Upstream Protection and Scale (Arbor Cloud)

- Provides cloud based DDoS protection to absorb and mitigate large scale volumetric attacks before they reach the organization's infrastructure.
- Offers a second layer of defense without requiring all traffic to be routed through a single network operator.

On Path, Local Protection (Arbor Edge Defense)

- Delivers always on, inline protection deployed close to applications and critical services.
- Preserves service availability during upstream provider outages by enabling local enforcement and control.
- Protects non web, application layer, and protocol specific traffic that CDN platforms are not designed to handle.

Global Threat Intelligence (ATLAS Intelligence Feed)

- Enhances detection accuracy using real world DDoS intelligence observed across a large portion of global internet traffic.
- Helps distinguish between malicious activity, legitimate demand surges, and provider related availability anomalies.

The Results:

The Resulting Architecture

When combined, this approach delivers:

- No single point of failure for availability.
- Resilience to both cyberattacks and provider outages.
- Operational continuity for digital systems underpinning physical services.
- Greater visibility and control for IT and infrastructure teams.

Rather than treating DDoS protection as a CDN add-on, the organization gains an availability architecture—one that ensures upstream platforms enhance resilience without becoming critical dependencies.

Final Takeaway

This case reinforces a broader industry lesson:

True availability protection means designing for failure—attacker failure and provider failure.

By adopting a layered architecture that combines Arbor Cloud for scale with Arbor Edge Defense for local control and resilience, organizations can protect revenue critical services without introducing new systemic availability risks.

LEARN MORE

For more information about NETSCOUT solutions visit:

www.netscout.com



Corporate Headquarters

NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information

Toll Free US: 800-309-4804
(International numbers below)

Product Support

Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us