# Amazon CloudFront Service

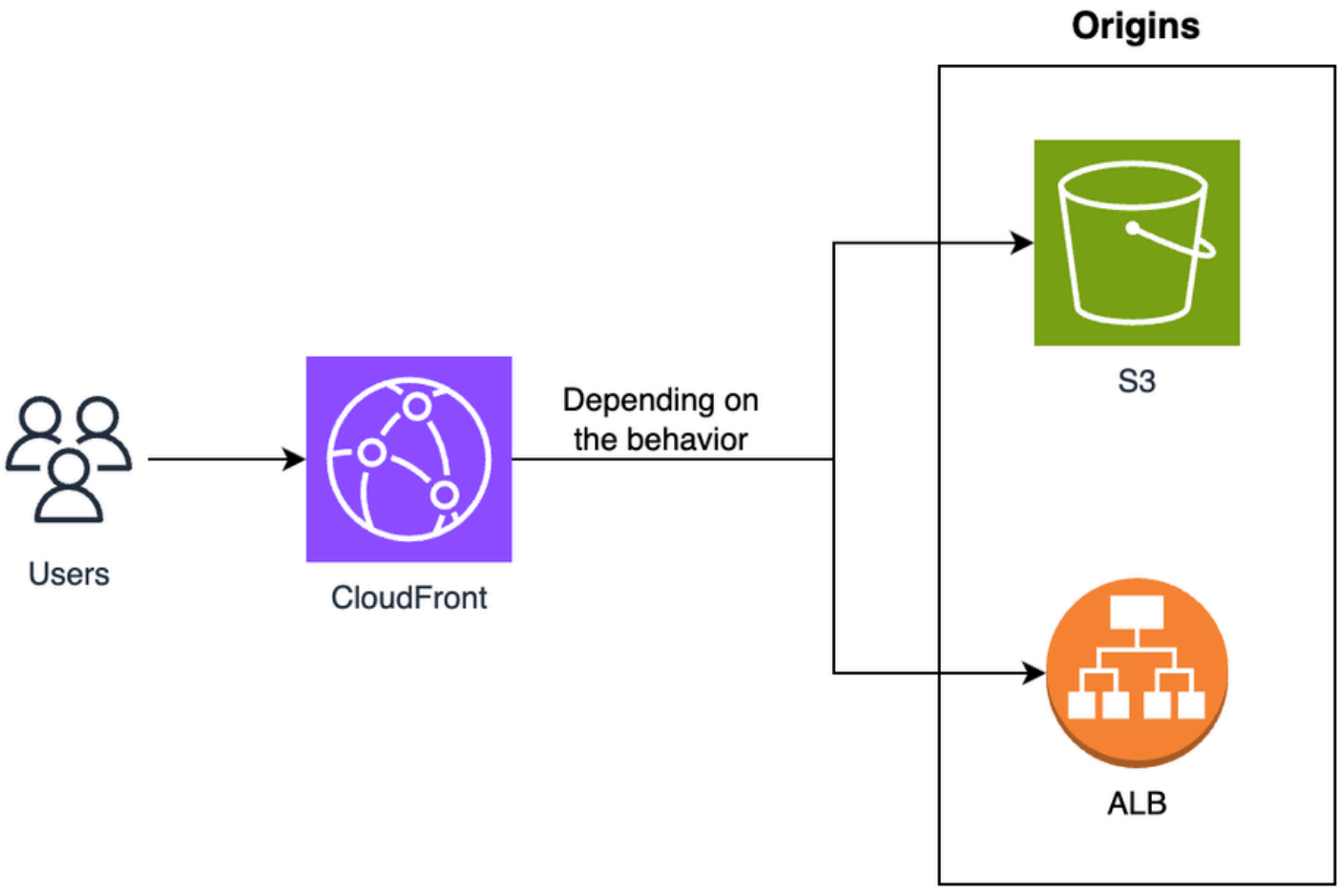
Amazon CloudFront is a **content delivery network (CDN)** service that securely delivers data, videos, applications, and APIs with **low latency, high transfer speeds, and global reach**. It integrates with AWS services like **S3, EC2, Elastic Load Balancer (ELB), Route 53**, and **AWS Shield** to optimize content delivery and security.

## How CloudFront Works

CloudFront accelerates content delivery by caching copies of content in a network of **global edge locations**. When a user requests content, CloudFront serves it from the nearest edge location, reducing latency and improving performance.

### Workflow:

1. **User Requests Content** → DNS routes the request to the nearest CloudFront edge location.
2. **Edge Cache Check** → If content is cached, it is served immediately.
3. **Fetch from Origin (if needed)** → If not cached, CloudFront retrieves it from the **origin server** (S3, EC2, or custom origin).
4. **Deliver & Cache** → The content is **cached** at the edge for future requests.



# Key Components of CloudFront

### 1. Distributions

A CloudFront distribution manages how content is delivered and cached.

- **Web Distribution** – Used for websites, APIs, and dynamic content.
- **RTMP Distribution (Deprecated)** – Previously used for streaming media over RTMP.

### 2. Origin

Defines where CloudFront fetches content from:

- **Amazon S3 Bucket** – To distribute static content like images, videos, and HTML.
- **EC2 Instances or Load Balancers** – To serve dynamic content.
- **Custom Origin (Non-AWS)** – Any web server outside AWS.

### 3. Edge Locations

- Global **Points of Presence (PoPs)** where CloudFront caches content.
- Reduces latency by serving users from nearby locations.

### 4. Cache Behavior

- Defines how CloudFront handles requests, caching, and forwarding.
- Can customize cache TTL (Time-to-Live) settings.

### 5. CloudFront Security

- **AWS Shield & AWS WAF** – Protects against DDoS attacks and malicious traffic.
- **Origin Access Control (OAC)** – Ensures only CloudFront can access S3 content.
- **SSL/TLS Encryption** – Ensures secure HTTPS connections.

### Real-Time Analytics

- CloudFront offers real-time analytics and reporting to monitor the performance and usage of your content.

## Mini Project

*Accelerating Web Content Delivery with CloudFront*

**Project Objective**

Accelerate the delivery of your web application's content by configuring CloudFront to cache and distribute it globally.

**Steps**

1. Access AWS CloudFront Dashboard

- Sign in to your AWS Management Console.
- Navigate to the AWS CloudFront service.

2. Create a Distribution

- Create a new CloudFront distribution.
- Choose the type of content you want to distribute (web, RTMP, or custom).

3. Configure Origins

- Specify the origin from which CloudFront retrieves the content.
- Choose an Amazon S3 bucket, an HTTP/HTTPS server, or other AWS resources as the origin.

4. Set Caching Behavior

- Define caching behavior for different types of content.
- Configure cache settings, including time-to-live (TTL) values.

5. Configure Security (Optional)

- If needed, configure security features like AWS WAF to protect your application from web threats.

6. Distribution Settings:

- Define settings such as domain names (CNAMEs), SSL/TLS certificates, and compression.

## Use Cases of CloudFront

### 1. Website Acceleration

- Reduces latency and improves speed for global users.
- Ideal for e-commerce, news sites, and blogs.

### 2. API & Web Application Acceleration

- Enhances API response times by caching GET/POST requests.
- Reduces backend load on EC2 or containers.

### 3. Live & On-Demand Video Streaming

- Uses **HLS, MPEG-DASH, or CMAF** formats for streaming.
- Ensures smooth playback with low latency.

### 4. Security & DDoS Protection

- Works with AWS Shield and WAF for enhanced security.
- Encrypts sensitive data at transit and at rest.

### 5. CloudFront Pricing

CloudFront charges are based on:

- **Data Transfer Out** – Costs depend on edge location.
- **HTTP/HTTPS Requests** – Pricing based on request types.
- **Invalidation Requests** – Clearing cache beyond free limit is chargeable.
- **Lambda@Edge Execution** – Charged per invocation.

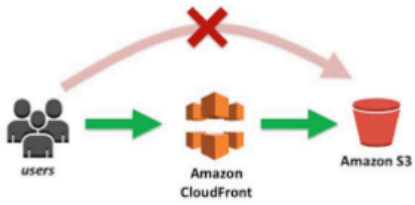
---

**CASE STUDIES:**

**1. Large State Agency**

**Challenge**
Client wanted to migrate their royalty and compliance application from an on-premises solution to the cloud and ensure a good user experience. The customer also had a need to retain and protect files uploaded by its users as well as meet NIST-compliance high availability and security standards.

**Solution**
Application is static JavaScript-based is deployed on AWS S3 with web hosting enabled. This is fronted by CloudFront which adds additional level of security by using Origin Access Identity (OAI) to restrict access to content that is serve from Amazon S3 buckets (static JavaScript application). Further, CloudFront, in conjunction with WAF, protects the application from malicious access including cross-site scripting and SQL injection attacks.




**Outcome**

1. Improved user experience
2. Highly scalable solution
3. Improved application security

## 8. CloudFront vs Other CDNs

| Feature | AWS CloudFront | Akamai | Cloudflare |
|---|---|---|---|
| AWS Integration | ✅ Best for AWS | ❌ | ❌ |
| DDoS Protection | ✅ AWS Shield | ✅ | ✅ |
| Dynamic Content Caching | ✅ | ✅ | ✅ |
| Serverless at Edge | ✅ Lambda@Edge | ❌ | ✅ Cloudflare Workers |
| Pricing | **Pay-as-you-go** | Expensive | Free & paid plans |

---

## Conclusion

Amazon CloudFront is a **powerful CDN** that enhances **speed, security, and scalability** for content delivery. It integrates seamlessly with AWS services, making it the best choice for

**AWS users** looking to optimize website performance, API responses, and media streaming.