Amazon CloudFront for Federal Agencies

Cost-Efficient Migration to a Next-Generation Content Delivery Network (CDN)

AUSTIN O'DONOGHUE
VP of Cloud and Infrastructure

JULY 2024

Delivering robust content to a global audience on federal websites and applications poses unique challenges for architects and platform operators. Federal agencies must ensure the highest-quality experience for end users, with reliable delivery, low startup latency, and a diverse range of content. Meeting these expectations often requires a cost-effective content delivery service that simultaneously addresses performance and security needs while exceeding user demands.

Amazon Web Services (AWS) CloudFront is an ideal solution for these challenges. CloudFront is a Content Delivery Network (CDN) platform that securely delivers video, data, applications, and API operations to customers worldwide with low latency, high transfer speeds, and a developer-friendly environment. As part of AWS FedRAMP services, CloudFront has physical locations directly connected to the AWS Global Infrastructure, ensuring high reliability and performance. Compared to other CDN providers, CloudFront offers a more cost-effective option. The CloudFront security savings bundle can save agencies between 30-60% and includes credits for AWS Web Application Firewall (WAF), a web application firewall that protects against common web exploits, adding an extra layer of security to the CDN.

With over 410 Points of Presence, including CloudFront Edge locations and 13 regional mid-tier caches in more than 90 cities across 48 countries, CloudFront ensures low-latency content delivery regardless of the end user's location. This extensive global network allows for secure and efficient content distribution, meeting the high standards expected by federal agencies while optimizing costs and enhancing security.

Austin O'Donoghue
VP of Cloud and Infrastructure
aodonoghue@rivasolutionsinc.com

Common Pitfalls

Misconfiguration Related Outages

Outages have a propagating effect on both customer satisfaction and internal IT teams, as addressing the outage and its aftermath requires a significant amount of time on documentation and lessons learned, rather than focusing on customer needs.

Infrastructure Dependencies

Other CDNs may depend on an external CDN provider that may not have robust infrastructure or control of the infrastructure they are using to deliver content. Amazon CloudFront pairs with thousands of Tier 1/2/3 telecom carriers globally and is well-connected with all major access networks for optimal performance with hundreds of terabits of capacity.

Overpaying for Services

Federal agencies often overpay for CDN services, including paying for unnecessary add-ons. CloudFront pricing allows agencies to consolidate contracts by purchasing CDN with other AWS services, improving procurement processes and timelines.

Improved Security Posture

Many agencies that distribute content over the internet want to restrict access to documents, business data, media streams, or content intended for a subset of users. To securely serve this content using Amazon CloudFront, you can do one or more of the following using easy-to-use configuration interfaces:

Use Signed URLs or Cookies

You can restrict access to content intended for selected users—for example, users who have paid a fee—by serving this private content through CloudFront using signed URLs or signed cookies.

Deny by Default

If you restrict access to CloudFront signed URLs or signed cookies, you also won't want people to view files using the direct URL. Instead, access files only by using the CloudFront URL with a "Deny by Default" policy for protected content.

Utilize an Application Load Balancer

When you use CloudFront with an Application Load Balancer in Elastic Load Balancing as the origin, you can configure CloudFront to prevent users from directly accessing the Application Load Balancer. This allows users to access the Application Load Balancer only through CloudFront, ensuring that you get the benefits of using CloudFront.

Use AWS WAF Web ACLs

You can use AWS WAF, a web application firewall service, to create or utilize an extant web access control list (web ACL) to restrict access to your content. AWS WAF offers managed ACLs such as the AWS WAF Bot Control group. Based on specified conditions, such as the IP addresses that requests originate from or the values of query strings, CloudFront responds to requests either with the requested content or WAF filters the request and returns the appropriate status code.

Steps to Successful Implementation

1

Perform Thorough Discovery

Thorough discovery of all origins and endpoints during the planning phase of a content delivery network migration is crucial to ensure seamless data flow and minimize downtime. It allows for accurate mapping of current infrastructure, enabling precise replication and optimization in the new network. Identifying all dependencies and potential bottlenecks helps in proactive troubleshooting, ensuring a smooth and efficient migration process.

2

Utilize Infrastructure as Code

Infrastructure as Code (IaC) tools like AWS CloudFormation Templates, Hashicorp Terraform, and Gruntwork.io's Terragrunt enhance the provisioning of cloud resources by allowing configurations to be parameterized, ensuring consistency and reducing manual errors. They enable repeatable deployments, making it easy to replicate environments across multiple stages, from development to production. These tools provide traceability and auditability, as all changes are version-controlled, facilitating compliance and accountability.

3

Optimize Service for Your Customers While Controlling Costs

Using AWS's CloudFront CDN distribution options to limit edge locations to specific geographic regions allows customers to target their audience effectively while controlling costs. By restricting edge locations, customers can optimize content delivery for regions of interest, ensuring lower latency and improved performance for end users in those areas. This selective approach also reduces unnecessary data transfer and storage costs associated with serving content globally, making it a cost-effective solution.

4

Pair Your CDN with a Web Application Firewall

Pairing your content delivery network migration with a serverless WAF like AWS WAF provides enhanced security and scalability without the need for dedicated infrastructure. AWS WAF offers real-time protection against common web threats such as SQL injection and cross-site scripting, ensuring robust security for your applications. Its serverless nature allows for seamless integration and automatic scaling to handle varying traffic loads, ensuring consistent performance and protection.

5

Use AWS Native Tools

Using AWS native tools like the AWS S3 CLI to migrate binaries streamlines the migration process by automating file transfers, significantly reducing the risk of user error associated with manual downloading and uploading. These tools provide efficient and reliable command-line operations for large-scale data migration, ensuring data integrity and consistency throughout the process. AWS S3 CLI supports advanced features such as parallel uploads and data encryption, enhancing both the speed and security of the migration.

6

Deploy Lambda@Edge

Using AWS Lambda@Edge to create redirect behaviors and modify HTTP requests and responses offers several advantages, including enhanced flexibility and reduced latency. By running code at AWS edge locations, Lambda@Edge allows for real-time, low-latency customizations that improve user experience by dynamically modifying content delivery based on user location, device type, or other factors. It eliminates the need for origin server modifications, streamlining deployment, and reducing infrastructure complexity while enabling sophisticated traffic management and security enhancements.

Case Study

On a $36M Web Modernization contract, team RIVA led AWS CloudFront strategy to migrate the legacy CDN architecture to a cloud-native serverless architecture. This project entailed planning, migration, and post-migration monitoring of the complete set of web properties operated by the federal agency to the AWS CloudFront CDN, protected by AWS WAF. The objectives for the agencies' CDN usage were cost reduction, operational resiliency, and web redirects (previously managed in the legacy console).

Through the combination of CloudFront and WAF, RIVA upgraded the services received from the legacy provider. Team RIVA ensured there were no service interruptions or site downtime during the migration through deploying infrastructure in parallel and utilizing a blue-green deployment model accomplished through DNS routing. The migration advantages included cost savings, consolidation to one platform, and flexibility to scale based on usage to expanding into new services AWS CloudFront has available to offer.

This included the following:

- Consolidation of services in AWS Cloud
- Integration into existing AWS landscape for web services and security
- Improved scalability and availability at a reduced cost
- Improved developer experience interacting with AWS Edge Services

We compared key metrics related to Performance, Scalability, Security, and Cost below:

30%
Improvement in Application Performance

Performance

CloudFront helps improve application performance. For static content, the CDN can store (cache) content closer to the end user. For dynamic content or APIs, our global private network helps accelerate delivery.

400+
Points of Presence

Scalability/Availability

With over 400 Points of Presence, CloudFront allows customers to serve content locally without having to replicate origin services. This also ensures the availability of their application by serving content even when the origin server might be unresponsive. 13 regional mid-tier caches in 90+ cities across 47 countries.

24/7
DDOS Protection

Security

CloudFront provides several native security controls such as SSL/TLS Encryption, Geo-Restriction, Signed URLs/Cookies, and protection against network layer DDoS attacks. CloudFront integrates seamlessly with AWS WAF and AWS Shield to provide advanced protection against hackers, bots, and volumetric cyberattacks. RIVA helps bolster security posture to ensure content is protected through signed URLs and cookies.

30%
Cost Savings

Cost

CloudFront offers pay-as-you-go pricing, allowing customers to only pay for what they use. CloudFront helps reduce customers' costs by caching content at the edge and reducing the need to scale origin servers. Customers who use AWS native origins such as S3, ALB, or EC2 can experience reduced data transfer costs. Customers willing to make a 12-month usage commitment could save up to 30% on monthly usage fees. Additionally, RIVA can help reduce costs and save up to 60% compared to the competition.

Conclusion

In conclusion, migrating to Amazon CloudFront offers federal agencies a robust, scalable, and secure content delivery network that addresses common challenges in delivering high-quality experiences to end users. By leveraging AWS CloudFront, agencies can achieve significant cost savings, improve operational efficiency, and enhance their security posture. The seamless integration with AWS services and the ability to optimize delivery for specific regions further amplify these benefits.
RIVA Solutions has demonstrated success in implementing CloudFront solutions, ensuring smooth transitions without service interruptions, and providing tailored configurations that meet agency-specific needs. Our approach focuses on thorough discovery, the use of Infrastructure as Code, and optimizing services to deliver maximum value to our clients.

To learn more about how RIVA Solutions can help your agency transition to a next-generation CDN and achieve unparalleled performance and security, please contact Vice President of Cloud and Infrastructure, Austin O'Donoghue.

Discover how our expertise and AWS CloudFront can transform your content delivery strategy.

Austin O'Donoghue
VP of Cloud and Infrastructure
aodonoghue@rivasolutionsinc.com