WHITE PAPER

AMAZON CLOUDFRONT FOR FEDERAL CUSTOMERS

Cost Efficient Migration to a next-generation content delivery network (CDN)

Prepared By Manal Elhak
melhak@rivasolutionsinc.com
Partnerships Manager, RIVA Solutions Inc.

THE CHALLENGE

Many federal agencies spend a large portion of their IT budget protecting mission critical applications and websites that are integral to serving their agency mission. Those applications and websites benefit most when a service addresses both performance and security needs simultaneously to improve customer experience and Amazon CloudFront cost-effectively meets those needs.

Delivering robust content intended to reach a large portion of US and global over the internet at scale poses a unique set of challenges for architects and platform operators. End customers expect the highest-quality experience with reliable delivery, low startup latency, and the ability to choose from a wide range of content. Amazon CloudFront is a CDN platform that securely delivers video, data, applications, and API operations to customers globally with low latency, high transfer speeds, and with a developer-friendly environment.

CloudFront is integrated with AWS FedRAMP services and physical locations that are directly connected to the AWS Global Infrastructure. Several agency customers using CloudFront have seen significant cost and feature benefits when compared to other CDN providers. In addition, a security savings bundle is a simple way to save up to 30-60% on CloudFront charges on an AWS bill when you make an upfront commitment. The savings bundle provides credits for AWS WAF, a web application firewall that helps protect your CloudFront distribution against common web exploits and adds another layer of security onto the CDN.

CloudFront edge locations are connected to the AWS regions through the AWS network backbone. Amazon CloudFront runs on Amazon Web Services global network backbone, allowing for an efficient transmission of requests between the CloudFront Edge locations and other Amazon Web Service services.

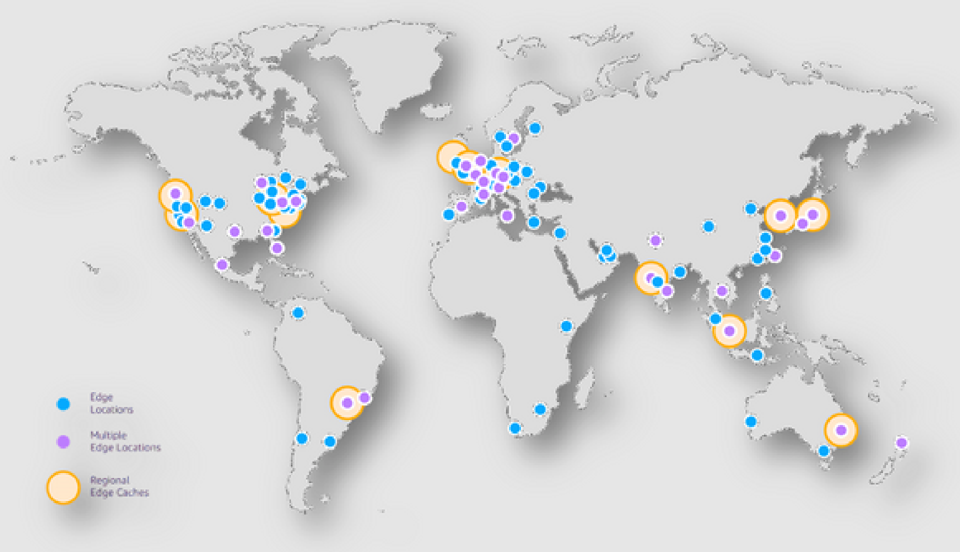

Figure 1. illustrates how Amazon CloudFront uses a global network of 410+ Points of Presence (PoPs) including CloudFront Edge locations in 13 regional mid-tier caches in 90+ cities across 48 countries to deliver content to end users with low latency. In a nutshell, this allows content to be delivered securely and cost efficiently regardless of where your customers reside.

Figure 1. AWS CloudFront Points of Presence & Edge Locations
(Source: https://aws.amazon.com/cloudfront/features/?whats-new-cloudfront)

Two critical security elements of a CDN deployment including using an Application Load Balancer and Web ACLs as outlined below:

- **Utilize an Application Load Balancer to Protect Content -** 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 a robust CDN.

- **Use AWS WAF Web ACLs -** You can use AWS WAF, a web application firewall service, to create a web access control list (web ACL) to restrict access to your content. Based on conditions that you specify (such as IP filters, or values of query strings), CloudFront responds to these requests either with the requested content or the appropriate status code.

A CASE STUDY

On a $36M Web Modernization contract, the RIVA team led AWS CloudFront strategy to migrate the current legacy CDN architecture to a service-oriented, containerized, cloud-ready architecture. This effort required planning for a complete migration of features in an existing legacy CDN and migrating that configuration into AWS CloudFront which would serve as the new Content Delivery Network (CDN) for the agency. With CloudFront we were able to replace the services that the agency currently received from the legacy provider as well as ensuring there would be no service interruptions or site downtime during the migration. The migration advantages ranged from cost savings, consolidation to one platform, and flexibility to scale based on usage to expanding into net 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
- Improving scalability and availability at a reduced cost
- Improving developer experience interacting with AWS Edge Services

Some of the common pitfalls that we have seen customers experience with their current CDN providers are outlined below:

A simple CDN misconfiguration can cause an extended outage. AWS CloudFront configuration is simple to deploy and maintain. Outages have a lasting negative effect on customer satisfaction. They also cause a large deal of stress on IT Teams as a result of addressing the outage and the resulting corrective actions where a significant amount of time is spent on documentation or lessons learned instead of focusing on customer needs.

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

Pricing that does not align with the level of service provided. Federal Agencies often are overpaying for CDN Services where they are utilizing only a small portion of the services available and paying for unnecessary add-ons. CloudFront pricing allows agencies to consolidate contracts by purchasing CDN with other AWS services, improving procurement processes and timeline.

BUT WHAT ABOUT SECURITY?

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

- **Using Signed URLs or Cookies -** You can restrict access to content that is 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.
- **Easily Restrict Access to Content -** If you restrict access to CloudFront signed URLs or signed cookies, you also won't want people to view files by using the direct URL for the file. Instead, you want them to access the files only by using the CloudFront URL, so that your protections work and use a “Deny by Default” policy for protected content.

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 is able to store (cache) content closer to the end user. For dynamic content or API's our global private network helps accelerate delivery. Over time, cache retention in CloudFront has emerged as a key contributor to performance. Techniques like tiered caching and de-duplication optimization of objects in cache help maximize cache retention.

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. CloudFront further ensures availability with 13 regional mid-tier caches in 90+ cities across 48 countries.

24/7
DDOS PROTECTION

Security: CloudFront provides several native security controls such as SSL/TLS Encryption, Geo-Restriction, Signed URL's and protection against network layer DDOS attacks. CloudFront also integrates seamlessly with AWS WAF and AWS Shield to provide advance protection against hackers, bots and volumetric cyber-attacks. RIVA helps improve security posture to ensure content is protected through robust DDOS protection.

30%
COST SAVINGS

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

CONCLUSION

This white paper has detailed key drivers, system considerations and benefits for content delivery with Amazon CloudFront for Federal Government customers. We described how CloudFront is part of the end-to-end CDN architecture. We learned about important features and optimizations for performance and security and how CloudFront provides a low friction and cost-effective path to displace existing CDN providers using a risk managed approach for implementation. In addition, you can always depend on DDOS protection with CloudFront just by using the AWS Shield service at no additional charge.

ABOUT RIVA

RIVA Solutions Inc. is an IT-service provider for the Federal government experiencing explosive growth since our inception in 2009. We specialize in Digital Transformation of the public sector providing best in class solutions and products in Digital Platforms, Data & Analytics, Cloud & Infrastructure, Human Centered Design, Application Services, and Cybersecurity.

CONTACT US

BD@RIVASolutionsInc.com
1676 International Dr Suite 520, McLean, VA 22102