Cross Origin Resource Sharing

A major source of headache for engineers around the world, Cross-Origin Resource Sharing (or CORS for short) is a security feature in web browsers that controls how web pages can request resources from a different domain. It ensures safe interactions between web pages and resources across different origins, protecting against **cross-site scripting (XSS) attacks**.

As a general rule of thumb, enabling CORS is basically essential for public-facing services like Amazon S3 and API Gateway. For S3 in particular, it allows web applications to directly request and interact with S3 buckets from different domains, useful for functionalities like file uploads. While for API Gateway, CORS settings enable APIs to be accessed from web applications on different domains. This integration allows client-side applications to connect to serverless backend services securely and efficiently.

Also worth noting is that Amazon CloudFront also leverages CORS through its `Access-Control-Allow-Origin` header. This header specifies which origins are permitted to access resources on a CloudFront distribution. By configuring the `Access-Control-Allow-Origin` header, we can control which domains can make cross-origin requests to your CloudFront-distributed content, ensuring secure and efficient delivery of static and dynamic content across different domains.