



AWS Whitepaper

Secure Content Delivery with Amazon CloudFront



Secure Content Delivery with Amazon CloudFront: AWS Whitepaper

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Abstract	1
Abstract	1
Introduction	2
How AWS Provides Security of the Cloud for Amazon CloudFront	3
AWS security processes	3
Compliance validation for CloudFront	3
Securing HTTPS delivery	4
Resilience and availability	5
How CloudFront Can Help You Ensure Security in the Cloud	7
Using HTTPS with CloudFront	7
Viewer HTTPS configuration	7
Origin HTTPS configuration	9
Securing your contents with CloudFront	10
Geo-based content access	10
Authorize access at the edge with signed URLs and cookies	10
Using CloudFront to encrypt sensitive data at the edge	11
Protecting your origin by allowing access to CloudFront only	12
Amazon S3 origins with CloudFront	12
Custom origin with CloudFront	13
Improving security by enabling security specific headers	14
Protecting from external threats at the edge	15
Managing access permissions to your CloudFront resources	16
Logging and monitoring in CloudFront	18
Configuration management	19
Conclusion	21
Contributors	22
Further Reading	23
Document revisions	24
Notices	25