Ensuring MPAA Content Security Compliance With Wasabi

Table of Contents

Executive Overview

Wasabi is an affordable and fast cloud storage service. Media and Entertainment companies can use Wasabi hot cloud storage for a variety of purposes including primary storage for video and other multimedia content and data; secondary storage for backup or disaster recovery; and archival storage for long-term retention.

The Motion Picture Association of America (MPAA) has established a series of voluntary content security best practices to protect intellectual property against theft, piracy or tampering. Media and Entertainment companies can use Wasabi to store and maintain electronic content in accordance with MPAA security recommendations.

Wasabi provides comprehensive identity management and access controls, and encrypts data at rest and in transit to protect digital rights and safeguard intellectual property. In addition, Wasabi supports configurable data immutability to protect content against accidental and malicious deletions, ransomware, viruses and administrative mishaps.

This white paper provides an overview of the Motion Picture Association of America content security program and explains how Wasabi helps organizations comply with MPAA recommendations for safeguarding intellectual property.

Introduction – MPAA Content Security Program Overview

The MPAA is committed to protecting intellectual property rights for its member companies and the larger community of entertainment content creators. To that end, the organization established a set of content security practices guided by four fundamental principles:

- Don't lose content.
- Don't let someone steal content.
- If content is lost or stolen, report it immediately.
- Don't let security measures disrupt production.

The MPAA guidelines are specifically intended to protect content during production, post-production, marketing and distribution. They provide third-party vendors engaged by MPAA members with an understanding of general content security expectations and current industry best practices. The guidelines are completely voluntary. MPAA members are not required to comply with them.

The MPAA has defined a Content Security Model that provides a common framework for assessing the ability of a third-party (such as Wasabi) to protect a client's content. The model is based on relevant ISO standards (27001/27002) and security standards from bodies such as the Open Web Application Security Project (OWASP), Cloud Security Alliance (CSA), Payment Card Industry (PCI) Security Standards Council, National Institute of Standards and Technology (NIST) and the SANS Institute. The framework covers five distinct security disciplines: management system security, physical security, digital security, application security and cloud security.

MPAA maintains and publishes two content security best practices guidelines:

- Common Guidelines cover management system security, physical security and digital security.
- Application and Cloud/Distributed Environment Security Guidelines cover application security and cloud security.

The MPAA does not offer a formal accreditation process. The onus is on an individual member to evaluate a potential business partner for conformance. Vendors and service providers can complete self-assessment questionnaires to help evaluate and demonstrate compliance with MPAA guidelines.

Wasabi has conducted a thorough self-assessment and completed both the Common Guidelines questionnaire and the Application and Cloud/Distributed Environment Security Guidelines questionnaire that are published in the MPAA Member Registry. Copies of both are available upon request. Customers can review the responses to evaluate Wasabi's ability to secure content and protect intellectual property.

Wasabi Hot Cloud Storage Overview

Wasabi hot cloud storage is affordable, fast and reliable cloud object storage for any purpose. Unlike legacy cloud storage services with confusing storage tiers and complex pricing schemes, Wasabi hot cloud storage is easy to understand and implement, and cost-effective to scale. One product, with predictable and straightforward pricing, supports virtually every cloud storage application.

Media and Entertainment companies can use Wasabi to maintain massive video libraries in the cloud with breakthrough economics and performance. Wasabi hot cloud storage is well suited for a wide variety of Media and Entertainment applications including:

- **Production/post-production –** use Wasabi as primary storage throughout the production workflow.
- **Backup –** use Wasabi to efficiently back up video content to the cloud for data protection and disaster recovery.
- **Active archive –** use Wasabi for long-term video preservation and active archival with rapid retrieval.
- **Origin storage -** use Wasabi as high-speed origin storage for video-on-demand applications.

Ensuring MPAA Content Security Compliance with Wasabi Hot Cloud Storage

MPAA members can use Wasabi to store and maintain content in accordance with MPAA security recommendations. The Wasabi cloud storage service is engineered to ensure the protection, privacy and integrity of customer data. The service is built and managed according to security best practices and standards, with MPAA content security guidelines in mind, and Wasabi has conducted a thorough compliance assessment as recommended by the MPAA.

Wasabi takes a "defense-in-depth" approach, employing multiple layers of security to address relevant MPAA Content Security Model elements. Wasabi ensures the physical security of its data centers; institutes strong authentication and authorization controls for all its cloud compute, storage and networking infrastructure; and encrypts data at rest and in transit to safeguard content.

Physical Security

The Wasabi service is hosted in premier Tier IV data center facilities that are highly secure, fully redundant, and certified for SOC-2 and ISO 27001 compliance. Each site is staffed 24/7/365 with on-site security personnel to protect against unauthorized entry. Security cameras continuously monitor the entire facility—both indoors and outdoors. Biometric readers and two-factor or greater authentication mechanisms secure access to the building. Each facility is unmarked so as not to draw attention from the outside.

Secure Network Architecture

Wasabi employs advanced network security elements, including firewalls and other boundary protection devices to monitor and control communications at internal and external network borders. These border security devices segregate customers and regulate the flow of communications between networks to prevent unauthorized access to Wasabi infrastructure and services.

Data Privacy and Security

Wasabi supports a comprehensive set of data privacy and security capabilities to prevent unauthorized disclosure of intellectual property. Strong user authentication features tightly control access to stored content. Access control lists (ACLs) and administratively defined policies selectively grant read/write and administrative permissions to users, groups of users, and roles.

Wasabi encrypts data at rest and data in transit to prevent leakage, protect against piracy and ensure privacy. All video content stored on Wasabi is encrypted by default to protect data at rest. And all communications with Wasabi are transmitted using HTTPS to protect data in transit.

Access Logging

Wasabi supports detailed storage access logs for audit purposes. Log records contain information about each access request such as the request type, accessed resources and the date and time the request was processed.

Data Durability and Protection

Wasabi hot cloud storage is engineered for extreme durability and integrity. Wasabi provides eleven 9s object durability, protecting data against hardware failures and media errors. In addition, Wasabi supports an optional data immutability capability that protects data against administrative mishaps or malicious attacks.

An immutable object cannot be deleted or modified by anyone—including Wasabi. Wasabi data immutability protects content integrity, mitigating the most common causes of data loss and tampering including accidental file deletions, viruses and ransomware.

Customer Responsibilities

Wasabi customers typically interface with the Wasabi service using third-party file management applications and backup tools. To ensure MPAA content security compliance, IT personnel must ensure the storage management tools and applications they use are configured to take advantage of Wasabi security features. For example, HTTPS must be enabled to encrypt data in transit.

Media and Entertainment companies must also ensure they have strong security systems and practices in place to safeguard other elements of their on-premises and cloud-based infrastructure. The Wasabi storage service is typically employed as part of a larger public or hybrid cloud IT implementation that includes multiple compute, storage and networking components.

Conclusion

The MPAA content protection guidelines introduce stringent data privacy and security requirements for Media and Entertainment companies. The MPAA does not provide formal certification mechanisms, so the onus is on every MPAA member to determine if its IT systems and practices comply.

Wasabi's cloud storage service ensures the protection, privacy, and integrity of electronic content, helping members comply with MPAA security best practice guidelines. Wasabi ensures the physical security of its data centers, employs strong authentication and authorization controls to safeguard infrastructure and services, and encrypts data at rest and in transit to prevent theft and piracy.

Wasabi is typically used in conjunction with other compute, storage and networking platforms and services. Media and Entertainment companies must implement strong security systems and practices across all on-premises and cloud-based infrastructure to fully protect content and comply with the MPAA content security guidelines.

Additional Information

For additional information about MPAA and Wasabi consult the following resources:

- MPAA Content Security Program
- MPAA Common Guidelines
- MPAA Application and Cloud/Distributed Environment Security Guidelines
- Wasabi Media and Entertainment Solutions

About Wasabi

Wasabi is the hot cloud storage company delivering disruptive storage technology that is 1/5th the price of Amazon S3 and faster than the competition with no fees for egress or API requests. Unlike first generation cloud vendors, Wasabi focuses solely on providing the world's best cloud storage platform. Created by Carbonite co-founders and cloud storage pioneers David Friend and Jeff Flowers, Wasabi is on a mission to commoditize the storage industry. Wasabi is a privately held company based in Boston, MA.

wasabi®

Tel 1-844-WASABI-1
Email info@wasabi.com

wasabi® hot cloud storage

www.wasabi.com