wasabi
hot cloud storage

Tech Brief

Wasabi's Strong Security Systems and Practices for Video Surveillance

Defense-in-Depth Architecture Protects Against Wide Range of Threats

Executive Overview

Wasabi is fundamentally transforming cloud storage for the video surveillance industry with the most affordable and highest-performing storage solution. The proliferation of high-resolution cameras and regulation increasing retention periods are driving the need for large storage capacities, establishing Wasabi as the best option to store surveillance video. In the video surveillance space, we've seen that the hybrid-cloud approach works best, keeping Video Management Software "air-gapped" on-premises, moving infrequently accessed video to the cloud. Wasabi is engineered to meet stringent security and compliance requirements and to safeguard the integrity and privacy of customer data. This tech brief provides a short overview of Wasabi hot cloud storage and reviews the strong security systems and best practices Wasabi uses to protect surveillance video files against a wide variety of threats.

Strong Security Systems and Practices Safeguard Customer Data

Wasabi hot cloud storage is engineered for extreme data durability, integrity and security. The service is built and managed according to security best practices and standards, and is designed to comply with a range of industry and government regulations including HIPAA, HITECH, FINRA, CJIS and FERPA.

Wasabi takes a "defense-in-depth" approach to security to protect against the widest range of threats. We ensure the physical security of our data centers; employ strong authentication and authorization controls for all cloud compute, storage and networking infrastructure; and encrypt video at rest and in transit to safeguard confidential data.

Physical Security

The Wasabi service is hosted in top tier 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 access and disclosure. Strong user authentication features tightly control access to stored video files. Access control lists (ACLs) and administratively defined policies selectively grant read/ write and administrative permissions to users, groups of users, and roles. Wasabi encrypts video files at rest and in transit to prevent leakage and ensure privacy. All video stored on Wasabi is encrypted by default to protect data at rest. And all communications with Wasabi are transmitted using HTTPS to protect video in transit.

Data Durability and Protection

Wasabi hot cloud storage is engineered for extreme data durability and integrity. Wasabi provides eleven 9s object durability, protecting video against hardware failures and media errors.

Object/Bucket Immutability

Wasabi supports an optional immutability capability at the bucket or individual file level that protects video from administrative mishaps or malicious attacks. Object lock is a new feature to Wasabi storage wherein a user can designate certain files or "objects" to be immutable, meaning they cannot be deleted or modified by anyone - including Wasabi. Users set an allotted time for an object to be immutable, after which it can be deleted. Wasabi immutability protects against the most common causes of data loss and tampering including accidental file deletions, viruses and ransomware

Hybrid Cloud Solution for Video Surveillance

A hybrid cloud architecture is one that combines the use of on-site resources as well as cloud based services. Recent events have illustrated how some VMS platforms can be vulnerable to hacking and unauthorized access when based in the cloud. In most cases, VMS platforms are best suited to operate on-site and connect to cloud storage. This adds an extra layer of protection. All video files can be encrypted to and from cloud storage as well as being encrypted while at rest. While being stored in Wasabi, video files are completely protected from any disaster or attack that could happen on-premises. If the VMS or local servers are destroyed, the video footage that is stored in Wasabi remains intact.

Wasabi Direct Connect

Wasabi Direct Connect is a high-speed, private, secure connection from your on-premises data center or colocation site directly to Wasabi. Sending data to Wasabi through a private connection adds another level of assurance that your data is secure while in transit. The Direct Connect provides greater security than a shared network resource such as an Internet connection.

Customer Responsibilities

Customers storing video surveillance recordings typically interface with Wasabi using Video Management Software or third party file management applications such as cloud gateways or bridges. Customers 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. Customers must also ensure they have strong security systems and practices in place to safeguard other elements of their on-premises and cloud-based infrastructure.

Summary

With cyber attacks on the rise and the increasing sensitivity of surveillance video, it's incredibly important to implement effective security measures to prevent breaches. Wasabi is engineered to meet stringent data security and privacy requirements. The service is built and managed according to security best practices and standards, and employs a defense-in-depth approach to protect against a wide array of threats. We ensure the physical security of our data centers, implement strong authentication and access controls to safeguard infrastructure and services, and encrypt data at rest and in transit to protect privacy and prevent unauthorized disclosure.

Wasabi is typically used in conjunction with other compute, storage and networking platforms and services. Organizations must institute strong security systems and practices across all on-premises and cloud-based infrastructure to ensure data privacy and protection across all enterprise assets.

Wasabi provides simple, predictable and affordable hot cloud storage for businesses all over the world. It enables organizations to store and instantly access an infinite amount of data at 1/5th the price of the competition with no complex tiers or unpredictable egress fees. Trusted by tens of thousands of customers worldwide, Wasabi has been recognized as one of technology's fastest-growing and most visionary companies. Created by Carbonite co-founders and cloud storage pioneers David Friend and Jeff Flowers, Wasabi has secured $140 million in funding to date and is a privately held company based in Boston.