Wasabi Cloud Storage Security:

Tools, Controls, and Compliance Explained

Executive Summary

At Wasabi, security is foundational to everything we do. Our singular focus on cloud storage allows us to deliver a secure, high-performance platform built to help organizations of all sizes protect, access, and manage their data with confidence.

Robust security is inherently part of a great storage solution. Wasabi continually innovates and seeks to offer the most useful security tools and practices available on the market today.

Wasabi employs defense-in-depth security principles to prevent unauthorized access and reduce the risk of data loss or theft. This includes end-to-end encryption, IAM policies, credential reporting, versioning, bucket logging, integrations with leading security providers, and many other capabilities that help you build and maintain a cyber-resilient cloud storage solution. Wasabi's defense-in-depth capabilities and best practices equip organizations with the tools they need to protect their most important asset: their data.

This whitepaper outlines Wasabi's multi-faceted approach to security. It describes the policies we enact to defend your data and highlights the best practices we encourage security practitioners, service providers, and partners alike to consider when evaluating their own security framework.

Wasabi Hot Cloud Storage: Security at Every Layer of the Data Landscape

In an era of rapidly evolving cyber threats and increasing regulatory scrutiny, data storage security is no longer a feature requested—it is a fundamental requirement of all organizations that store data in the cloud. At Wasabi, we've built our cloud storage platform with a defense-in-depth strategy to ensure your data is secure at every layer: from account access and infrastructure to the data itself and the transactions that support it.

Account Security

Identity and access management (IAM) are the first lines of defense in any secure cloud environment. Wasabi provides a suite of controls designed to prevent unauthorized access while giving organizations the flexibility to scale securely. Multi-factor authentication (MFA) strengthens identity verification by requiring users to authenticate with a time-sensitive code generated on a trusted device, such as a smartphone. This ensures that access is granted only when both identity and possession factors are satisfied.

Taking things a step further, Wasabi offers Multi-User Authentication (MUA), a first-of-its-kind feature in the storage industry that prevents any single user from deleting a storage bucket or account without the unanimous approval of designated security contacts. By introducing an internal checks-and-balances system, MUA serves as a safeguard against rogue actions or insider threats.

Wasabi also provides robust IAM capabilities, enabling administrators to define granular policies for users and groups. These policies ensure that users only have access to the resources and actions they need, supporting least-privilege principles at scale. For enterprise environments leveraging existing identity providers, Single Sign-On (SSO) integration with solutions like Okta and Azure Active Directory allows for streamlined, secure user management without compromising usability.

Physical Security

Wasabi partners with globally recognized data center providers—including Iron Mountain, Flexential, Digital Realty, NTT, Retelit, and Equinix—to operate a distributed and fully redundant infrastructure. These Tier IV and Tier III data centers offer rigorous access controls, biometric security, video surveillance, and power redundancy, ensuring your data resides in environments designed to withstand both physical and cyber threats. Wasabi storage regions are deployed in fully secure and redundant data centers that are SOC-2 compliant and certified for ISO 27001 and PCI-DSS. Wasabi users have full control over where their data is stored by selecting the region-specific bucket. For example, if they only want to store data in the us-east-1 location, they will configure and select a us-east-1 bucket.

Security at these facilities is validated through independent third-party audits. Wasabi is certified under ISO 27001, offering assurance that our information security management

system meets the highest international standards. In addition, Wasabi complies with major data privacy regulations such as the GDPR & UK GDPR and FERPA, ensuring you can meet regional and industry-specific requirements with confidence.

Data Security

Data protection is built into Wasabi's core architecture. All data is encrypted at rest and in transit using AES-256 encryption and TLS 1.2 or higher, which prevents unauthorized access during storage or transfer. For organizations with strict internal governance or compliance mandates, Wasabi also supports Server-Side Encryption with Customer-provided keys (SSE-C) to give you complete control over encryption lifecycle management.

To increase data availability and support disaster recovery strategies, Wasabi provides built-in object replication between intercontinental regions. Data durability is ensured through object-level redundancy that offers eleven nines (99.999999999%) of object durability. Additionally, Wasabi's Object Lock feature enables immutability at the object level, which protects against ransomware and enables compliance with regulatory mandates such as SEC 17a-4, HIPAA, and CJIS.

IAM policies also play a critical role in securing data access. Administrators can create highly specific policies that govern read, write, and administrative privileges across buckets and users. This ensures data is only accessible to those with an explicit need.

Payment Security

Security extends beyond data and into financial transactions. Wasabi partners with Stripe, a globally trusted payments platform, to process all transactions with industry-leading security. Stripe's infrastructure ensures that credit card data is never exposed and that transactions are monitored for fraud and abuse in real time.

All payments processed through Wasabi's billing infrastructure are PCI DSS compliant, ensuring that your financial data is protected according to the industry's most rigorous standards.

Summary

Wasabi is engineered to meet the most stringent data security and privacy requirements within the local, federal, and global landscape. The Wasabi Hot Cloud Storage service is built and managed according to security best practices and standards and continuously provides new tools and innovative practices to provide customers with the most resilient data security possible. Wasabi employs a defense-in-depth approach to protect against a wide array of threats organizations may face, internally and externally, both physical and digital. 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 backup and cyber-resilience vendors, compute, storage, and networking platforms, and related services. IT 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.

Looking to better secure your storage at a price you can trust?

Contact Wasabi Today

Contact Wasabi

Get up to 1 TB for 30 days

Try Wasabi Free

wasabi

wasabi.com