wasabi | COMPANY INTRODUCTION

What is Wasabi?

A Brief Introduction to Wasabi Hot Cloud Storage

Who We Are

Wasabi is the hot cloud storage company. We're storage experts. We only do cloud storage. And we do it less expensively and faster than the competition.

Founded by David Friend and Jeff Flowers, the co-founders of Carbonite, our mission is to make cloud storage a simple, open-standard commodity and utility, just like electricity.

What is Hot Cloud Storage?

Hot cloud storage is insanely cost effective and fast cloud object storage for any purpose. It is fast to write, fast to read and instantly available. We believe in keeping storage simple with a universal storage product that satisfies nearly all cloud storage requirements.

Hot cloud stor•age
/hät kloud stôrij
noun

A universal, one size fits all cloud storage service that eliminates confusing storage service tiers and satisfies nearly all storage performance requirements. Hot cloud storage costs significantly less than traditional cold storage services and is significantly faster than traditional frequent-access storage services.

No More Tiers

Unlike legacy cloud storage services with confusing storage tiers and complex pricing schemes, Wasabi hot cloud storage is extremely easy to understand and implement, and incredibly economical to scale. One product, with predictable and straightforward pricing, supports virtually every cloud storage application.

Optimal Price, Performance & Protection

Wasabi is 80% cheaper and faster than the competition, with no fees for egress or API requests. And Wasabi hot cloud storage immutable buckets protect against the most common causes of data loss.



Amazon S3 Bit Compatible

Wasabi is fully compatible with Amazon S3 APIs. That means all your existing S3 storage management applications like backup and recovery tools work seamlessly with Wasabi.

Simple to Use

Wasabi is amazingly easy to use. You can set up an account in seconds. With our intuitive S3-like web console you can create storage buckets, set up users and configure access policies in no time. And with support for a wide range of S3-compatible storage clients for a variety of host platforms, you can move files in and out of the cloud the same way you would with a local drive, with drag-and-drop simplicity and convenience.

Remarkably Versatile

Inexpensive, fast and reliable, Wasabi is ideal for a wide range of applications. Some examples include:

- **Multi-cloud storage** - keep a secondary copy of your S3 storage for 20% of the cost of Amazon S3
- **Hybrid Storage** - protect and extend on-premises storage investments
- **Big Data and IoT** - move massive datasets in and out of storage at extremely high speeds
- **Regulatory compliance** - meet stringent government regulations with encryption at every step and immutable data buckets
- **Media & Entertainment** – store massive video libraries with breakthrough performance and economics
- **Video archiving** – store any type of archived video for future search and playback

Disruptive Pricing

Affordable, simple and predictable, Wasabi's pricing blows away the competition. With two ways to pay, choose the model that works best for your business.

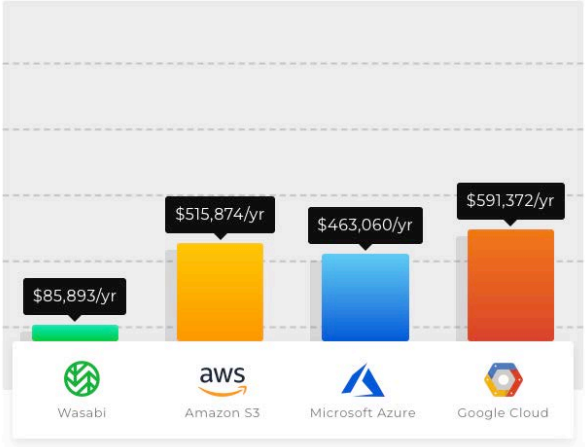
Wasabi's pay-as-you-go pricing model is billed monthly and is built to scale with your data needs.

Wasabi Reserved Capacity Storage makes buying cloud storage a natural addition to your on-premises storage. If you are thinking about buying more hardware storage, compare the price against 5 years of Reserved Capacity Storage.

You can purchase cloud storage in 1, 3, or 5 year increments and achieve greater discounts for term and capacity.

Unlike Amazon, Google and Azure we don't impose extra fees to retrieve data from storage (egress fees). And we don't charge extra fees for PUT, GET, DELETE or other API requests.

Annual Storage Fees for 1 PB of Data[1]



Groundbreaking Performance

Wasabi's pioneering highly parallelized system architecture delivers a read/write performance advantage over the competition.

> **The purpose-built file system design used by Wasabi offers meaningful performance advantages over Amazon S3. In recent performance testing, Wasabi displayed better performance than S3 in the majority of the write (PUT) use cases that were tested.**

Robust Protection

Wasabi hot cloud storage is engineered for extreme data durability, integrity and security. We provide eleven 9s object durability—same as Amazon S3 Standard.

Configurable immutability prevents accidental deletions and administrative mishaps; protects against malware, bugs and viruses; and ensures compliance with HIPAA, FINRA, CJIS and other government regulations.

And active integrity checking (we validate data every 90 days) keeps your data fresh forever.

Next Steps

- **CONTACT WASABI TODAY.** Learn more about our price, performance and protection benefits.
- **TRY WASABI FOR FREE.** Get up to 1 TB for 30 days.

[1]Assumes 20% of stored content downloaded monthly

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

©2023 Wasabi Technologies, Inc. All rights reserved. WASABI and the WASABI Logo are trademarks of Wasabi Technologies, Inc. and may not be used without permission of Wasabi Technologies, Inc. All other brand names mentioned herein are for identification purposes only and may be the trademarks of their respective holder(s).

Wasabi does not provide internal policy documentation to third parties because it exposes Wasabi and our clients to potential risk. A summary of our policy and procedures is provided.

Access Control and Access Review

Wasabi Technologies' (Wasabi) Information System Activity Review Policy is reviewed, updated, and approved by management annually. It includes restrictions on remote access, wireless network access and access to applications utilized internally by Wasabi, and to the user's issued workstation, etc.

Wasabi employee system access is reviewed quarterly to ensure appropriate access and reviewed anytime an employee's role changes within Wasabi. In the event of an employee termination, access is disabled within less than 24 hours.

Any remote access using VPN to the Wasabi Production Environment must be reviewed and approved by appropriate management. All employees by default will have account settings set to deny remote access. Only upon approval will the account settings be changed to allow remote access. Authentication is managed using Okta and 2-Factor Authentication. No remote access to the customer's network is required.

Application user access policy and procedure is controlled and managed by the customer's local administrator/root user in the Wasabi Console. Application user account management, including provisioning, roles, groups, policies, deleting/disabling user accounts, and other settings (i.e., MFA, MUA, Billing Access, etc.) is controlled solely by the customer's local administrator/root user. Wasabi is unable to access the customer's account, therefore cannot alter customer configurations.

Wasabi does not provide internal policy documentation to third parties because it exposes Wasabi and our clients to potential risk. A summary of our policy and procedures is provided.

Compliance And Regulatory Audit Procedure

Wasabi Technologies' (Wasabi) has implemented a standardized procedural approach to any compliance and/or regulatory audits. The primary contact for any audit is the Director, Compliance & Security, who can be reached at compliance@wasabi.com. If another other Wasabi personnel receive notification of an audit, the Director, Compliance & Security, is notified via slack message and/or email.

In General, third-party compliance & regulatory audits will follow the below noted steps:

- Evidence Request phase
    - The third-party organization conducting an audit will assign an Auditor/Assessor, who will provide an online questionnaire, IRL (evidence request), and/or link to an online portal.
    - The auditor/assessor will provide a completion due date.
    - The Director, Compliance & Security, will schedule a required meeting(s) with the auditor/assessor.
- Evidence gathering phase
    - Consider our most recent response to the specific audit, comparing to the current controls list. This assessment will be utilized to assess for changes in process that require first time documentation and/or previous audit controls no longer use (thus previous evidence no longer needed or requires updates)
        - Necessary edits due to changes – review with Wasabi SME(s) to ensure we consider any changes since the last revision.
        - New questions - involve Wasabi SME(s) as needed
        - Review the system for evidence request responses with the Auditor
        - Internal Policies are not to be shared unless required by statute or regulation, instead provide policy summaries
        - Upload evidence/validation

- Evidence validation phase
    - The auditor/assessor may request follow up evidence/validation/documentation
        - NOTE: There may be documentation or screenshots that Wasabi as a company prefers to show online due to Intellectual Property and/or Security-related concerns with sharing a copy; request review w/ our SME(s) & the auditor
- Report phase - Draft Report
    - Review the draft report & follow up with organization conducting the audit should any clarifications be needed
        - The Senior Product Manager, Security & Compliance will conduct the initial review, then forward to Executive Leadership and Wasabi SME(s) for review and comment
        - The Director, Compliance & Security, will return the draft report containing our review/comments/corrections to the organization conducting the audit
- Report phase - Final Report
    - The organization conducting the audit publishes the final report and any supplemental documentation, which is received by the Senior Product Manager, Security & Compliance
        - The Senior Product Manager, Security & Compliance compares the final report against the edited draft report:
            - If the updates provided by Wasabi are reflected in the final report: The Senior Product Manager, Security & Compliance forwards the Final Report to the Executive Leadership Team and SME(s) that participated in the audit.
            - If the Wasabi updates are included in the final report: the Senior Product Manager, Security & Compliance contacts the organization conducting the audit and request an explanation/corrected final report and/or a meeting.
    - The Director, Compliance & Security, uploads the final report to the appropriate SharePoint folder following approval of report by the Executive Leadership Team.

Wasabi does not provide internal policy documentation to third parties because it exposes Wasabi and our clients to potential risk. A summary of our policy and procedures is provided.

Cybersecurity Incident Response

Wasabi Technologies' (wasabi) Cybersecurity Incident Response Policy defines roles, what constitutes a security incident, outlines incident response phases, discusses how information is passed to appropriate personnel, assessment of the incident, minimization of damage, response strategy, documentation, and preservation of data. In addition, the incident response policy defines areas of responsibility, establishes procedures for the identification, response, reporting, assessment, and follow-up of suspected or various actual security incidents that meets the requirements of the HIPAA Security Rule, HITECH provisions of American Recovery and Reinvestment Act ("ARRA") FBI CJIS Security Policy, and process recommended by NIST and SANS.

If the person who discovers the incident is not a member of the wasabi IT department, they will contact the 24/7 emergency number to reach wasabi support. The support representative will notify wasabi network administrators via phone, text, and email, and log the call. If the person discovering the incident is a wasabi workforce member, they will report suspected and known events to the Information Services Help Desk as well as Management, the HIPAA Security Officer, and/or the Privacy Officer. If the event is a security incident the Cybersecurity Incident Response Team (CIRT) is activated.

The CIRT will meet to determine a response strategy. An incident ticket will be created, and team members will establish pre-defined procedure based on the incident assessment.

CIRT members will use forensic techniques including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized people should be performing interviews or examining evidence and the authorized personnel may vary by situation and the organization.

Thorough documentation is maintained, including, and not limited to, incident discovery, category, how the incident occurred, source of the incident, the response plan, and effectiveness of response.

CIRT members will recommend changes to prevent the occurrence from happening again or infecting other systems. Upon management approval, the changes will be implemented. CIRT members will restore the affected system(s) to the uninfected state.

Wasabi does not provide internal policy documentation to third parties because it exposes Wasabi and our clients to potential risk. A summary of our policy and procedures is provided.

Data Retention and Destruction

Wasabi Technologies' (wasabi) Record Retention and Destruction Policy ensures that necessary records and documents are adequately maintained, and to ensure that records no longer needed by Wasabi or of no value are appropriately discarded. Wasabi's customer agreement, addendums, and other contractual documents define retention of customer data.

In the event Wasabi is served with any subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning Wasabi Technologies or the commencement of any litigation against or concerning Wasabi, any further disposal of documents shall be suspended until shall time as the Administrator, with the advice of counsel, determines otherwise ("Litigation Hold"). The Litigation Hold requirement supersedes any other retention period or policy applicable to the affected records.

Customer uploaded data is retained so long as the account remains active and in good standing, unless otherwise directed by a lawful court order received by Wasabi prior to the cancellation or termination of an account. Customer data on a Wasabi Ball Appliance is retained until the customer verifies successful upload of data to their account. Data cannot be retrieved once the account has terminated or expired, nor can data be retrieved from a Wasabi Ball Appliance once it has been sanitized.

Any customer data that require destruction will be sanitized per methodologies defined within the most current version of NIST Special Publication 800-88. A valid encryption key is required to access customer data stored on Wasabi's servers and Wasabi Ball Appliance. Section 4.1 of the Wasabi Customer agreement notes that customer data is deleted upon termination of the customer account, including any customer encryption keys. Data on Wasabi Ball Appliances are sanitized after the customers verify upload of the data to their account. Per NIST 800-88, this constitutes a cryptographic erase, which is defined as leveraging "the encryption of target data by enabling sanitization of the target data's encryption key. This leaves only the ciphertext remaining on the media, effectively sanitizing the data by preventing read-access.". Customers who have terminated their account may request a Certificate of Sanitation by contacting compliance@wasabi.com.

The Wasabi employee conducting the sanitization shall complete and sign the certificate, and a second employee who has verified destruction will also sign the certificate. The completed certificate is then forwarded to the Wasabi Security Officer. The requesting party (former Wasabi Customer) shall also be provided with a copy of the signed certificate.

Unneeded or outdated Wasabi internal records are destroyed either (1) systematically, such as through periodic purging of email, or (2) by disposing of outdated documents and records as they are observed in files. Records containing highly sensitive information such as confidential or proprietary information of Wasabi Technologies or personal information must be destroyed in an appropriate manner so that the sensitive information contained in the record cannot practicably be read or reconstructed. All backup and archive copies of records are destroyed when the originals are destroyed.

Wasabi does not provide internal policy documentation to third parties because it exposes Wasabi and our clients to potential risk. A summary of our policy and procedures is provided.

Maintenance

Wasabi Technologies (wasabi) reserves the right to conduct maintenance of the production systems as needed. The goal is to have any maintenance transparent to the customer. Should an outage be needed or occur, customers will be notified via the email on file for their respective account. In addition, customers may also monitor Wasabi's status page at https://status.wasabi.com/ , and can choose to subscript to update using the "Subscribe To Updates" button on the status page.

Wasabi maintains a continuous version releases, which are completed without interruption to customers.

Wasabi does not provide internal policy documentation to third parties because it exposes Wasabi and our clients to potential risk. A summary of our policy and procedures is provided.

Risk Assessments

Wasabi Technologies (wasabi) performs internal Risk at least annually and assessed by third-party auditors on an annual basis. A Risk Assessment report is provided to the Wasabi Executive Staff and Board of Directors annually.

All risk assessment information is considered sensitive.

Wasabi scans for outside vulnerabilities weekly with tenable.io, and scans code with SonarQube.

Wasabi does not provide internal policy documentation to third parties because it exposes Wasabi and our clients to potential risk. A summary of our policy and procedures is provided.

Security

Network Security

Wasabi Technologies' (wasabi) Security policies are reviewed, updated, and approved by management annually. The review includes restrictions on remote access, Wasabi internal systems access., and 3rd Party applications in use by Wasabi. Wasabi does not provide internal policy documentation to external parties.

The Wasabi workforce receive general Security Awareness training upon hire, and complete Security Training annually thereafter. Wasabi employee system access is periodically reviewed to ensure appropriate access and reviewed anytime an employee's role changes within Wasabi. In the event of employee termination, access is disabled within less than 24 hours.

Any access using VPN access to the Wasabi servers (information resources) must be reviewed and approved by the appropriate Management. All employees by default will have account settings set to deny VPN access. Only upon approval will the account settings be changed to permit VPN access. Employees cannot connect to the system using mobile devices, and direct access with passing through the access control system is prohibited.

Wasabi Systems that allow public access to host computers, including servers, warrants additional security at the operating system and application levels. These systems have the ability to monitor activity level to ensure public usage does not degrade systems responsiveness.

Subcontractors are not permitted access to the information resources until a review based on the contract Statement of Work is completed and then is granted with the appropriate restrictions to preserve the principal of least access control model.

Data Security and Encryption

Security Standard

- Wasabi Technologies supports the HTTPS protocol for encryption.

Data at Rest

- All data at rest is encrypted using 256-bit AES. Wasabi Technologies also supports server-side encryption (SSE). The SSE options include SSE-S3 (using AES256 encryption - X-Amz-Server-Side-Encryption: AES256) and SSE-C (customer-based key - X-Amz-Server-Side-Encryption-Customer-Key). The customer is able to specify the SSE parameters using a S3 client application when writing objects to bucket(s).

Data in Transmission

- Wasabi Technologies supports the HTTPS protocol for encryption during transmission of data to and from Wasabi.

Intrusion Detection Systems

- An intrusion detection system is used for all IDS based incidents. Network defense and host intrusion prevention systems are monitored and updated daily by our Operations Teams. If tests or monitors fail, the Operations Team are automatically notified via slack notification, email and text message.

Antivirus

- An anti-virus software suite is used to protect all organizational resources against intrusion by viruses and other malware. Products operate in real time and the anti-virus library definitions are updated at least once per day. No one may stop anti-virus definition updates or scans except for domain administrators. Anti-virus scans are performed at least once per week on all workstations.

- The servers with a public IP address are protected with Access Control Lists (ACL's), and private subnet servers are protected by Network Address Translation (NAT). Wasabi Technologies owns the public IP Addresses and hosts the domain with Cloudflare. If any authenticated user uploads any content that alerts Cloudflare, Wasabi immediately takes action up to and including taking the bucket offline. Authenticated users uploading malicious code (viruses, malware, etc.) will not impact Wasabi's production system.

Firewalls

- A firewall with ingress and egress filtering is employed. Firewall protection is managed over SSH.
- Firewall policies are deny-all/allow-by-exception, by default.
- Internal network segmentation is used to further isolate sensitive production resources.

Physical Security – Facility Access

To safeguard the confidentiality, integrity, and availability of protected health information (PHI), business, and proprietary information within Wasabi Technologies (wasabi) information systems/applications, Wasabi controls access to the physical buildings/facilities that house these systems/applications in accordance with both the HIPAA Security Rule 164.310 and FBI CJIS Security Policy, Section 5.9, Policy Area 9: Physical Protection, and its implementation specifications.

Physical Access to all Wasabi facilities is limited to only those authorized. In an effort to safeguard PHI and CJI, the facility(s), and systems/applications from unauthorized access, tampering, and theft, access is allowed to designated areas only to those persons authorized to be in them and with escorts for unauthorized persons. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Wasabi Technologies' facility(s) to areas containing information systems/applications.

Wasabi Technologies' (wasabi) production environments are on Wasabi servers that are collocated in Data Center Provider partner facilities. The respective Data Center is responsible for the Physical Security, Surveillance, and Fire Suppression of their facility. Access to any Data Center must be requested by Wasabi Operations Team leadership. Wasabi Employee access rights to the Data Center facility and Wasabi's server cage(s) entail submitting access key card, biometric authorization, and a PIN. In addition, all racks are locked.

Visiting vendors register (sign in and out) and obtain Visitor identification badges. Vendors are instructed to return the Visitor identification badge and sign out prior to leaving the premises. Other Visitors (i.e., for regulatory purposes) must register (sign in and out) and obtain a Visitor identification badge, and then must be escorted by authorized personnel both in the Data Center and Wasabi's server cages. Visitors are instructed to return the Visitor identification badge and sign out prior to leaving the premises. It is not possible to access the data center(s) and server cage(s) unless authorized to do so.

Wasabi is in possession of the SOC 2 Report and ISO 27001 Certificate for each Data Center Provider location, and customers are able to request these documents. Additional information is available at https://wasabi-support.zendesk.com/hc/en-us/articles/115002145572-What-third-party-compliances-have-been-attained-by-Wasabi-

Wasabi undergoes the following Audits: Type 2 HIPAA/HITECH, CyberGRX, and SEC SEA Rule 17a-4(f).

For more information contact compliance@wasabi.com

Wasabi does not provide internal policy documentation to third parties because it exposes Wasabi and our clients to potential risk. A summary of our policy and procedures is provided.

Service Notifications

Wasabi Technologies' (Wasabi) customers will be notified of planned maintenance as per the Wasabi SLA, section 1. Wasabi Support will notify impacted customers of Severity 1 or 2 incidents as defined in the Support Plans Overview.

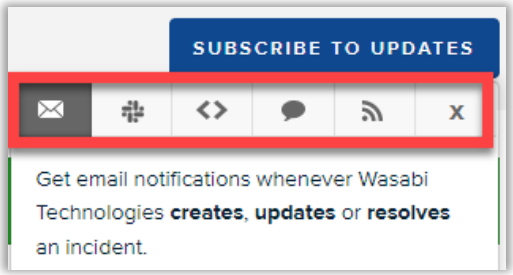
User are also able to manually monitor https://status.wasabi.com/ for planned and unplanned service interruptions. In addition, users can choose to subscribe to updates for one ore more of Wasabi's storage regions using the following steps:

1. Navigate to https://status.wasabi.com/

2. Click on the blue "Subscribe to Updates" Button.

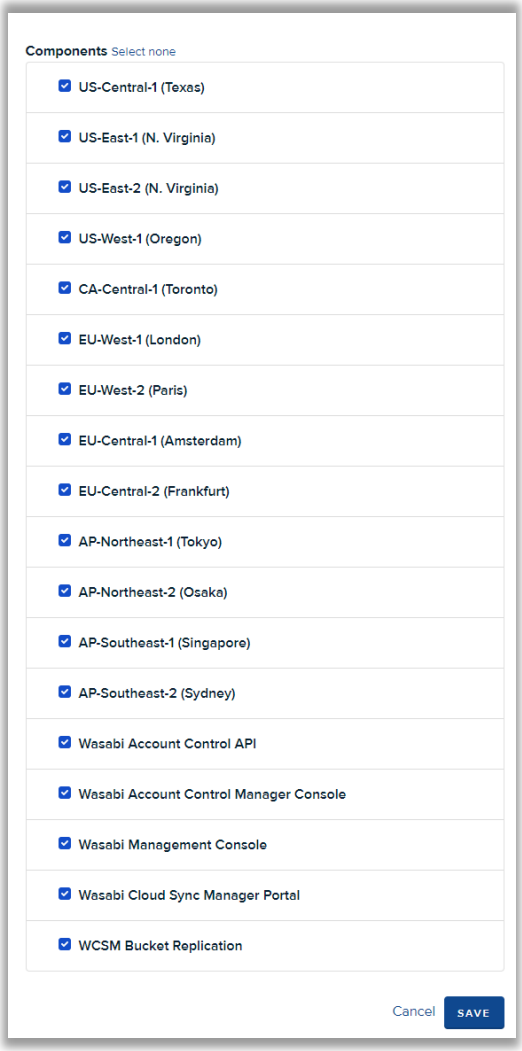


3. Select the method of notification (email, slack, webhook, Atom or RSS Feeds).



4. Users will be prompted to enter the contact information for the method selected.

5. On the next screen all the Wasabi Storage Regions will be selected, as indicated by a blue checkmark. Simply uncheck any region for which you do not want to receive a notification.



6. Click the blue “Save” Button.

7. Once saved, notifications will be received for all events, such as routine maintenance and/or unplanned service interruptions.

8. Users can update their subscription preferences by repeating steps 1-6.

9. At any time users may contact support as noted in the Support Plans Overview.

Wasabi does not provide internal policy documentation to third parties because it exposes Wasabi and our clients to potential risk. A summary of our policy and procedures is provided.

Software Development Lifecycle

Wasabi Technologies' (wasabi) Software Development Lifecycle (SDLC) policy includes the following phases of the SDLC: Discovery, Architecture, Planning, Development, Quality Assurance (QA), and Deployment.

Wasabi uses JIRA for change management with GitHub integration to manage the SDLC, and leverages internal workflow documentation for how Issues are created and managed through the planning phase, development phase, QA phase before being released into Production. The QA and Operations teams are included in technical discussions with the development and product management teams for all features, from inception to release.

Wasabi's Quality Assurance program is based on industry best practices. QA is integrated into every Agile sprint planning session. QA entry criteria is defined for builds delivered to QA from the development team. The QA process includes functional testing, regression testing, and manages the defect process throughout the release cycle. QA process includes functional testing, regression testing, and manages the defect process throughout the release cycle. Upon successful exit from the QA test cycle, QA publishes a MOP and the software is released for production deployment.

Wasabi maintains separate development, QA, and production server environments. Only specific personnel can promote software from one server environment to the next, and only Wasabi Development Operations (DevOps) are able to deploy software to Wasabi's production servers.