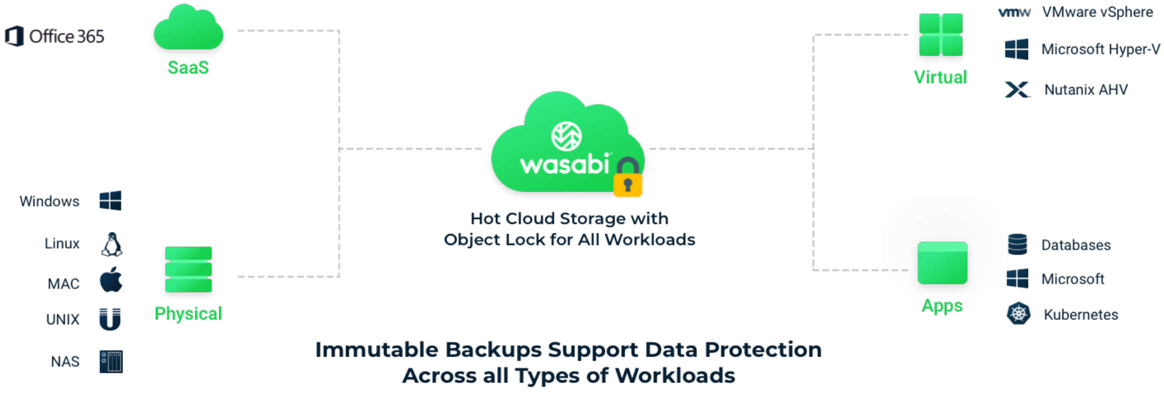
Mitigating Ransomware Attacks with Wasabi Hot Cloud Storage and Immutable Backups

There is no end in sight to the ongoing campaign of ransomware attacks. What started years ago as a stunt to prove coding superiority has evolved into a global ransomware industry, complete with a full portfolio of “As-a-Service” offerings and 24-hour help desk support. This lucrative pursuit has attracted professionals and amateurs alike to the criminal fold. There is no doubt that each and every internet-connected business today will be the target of an attack in the next 6 to 18 months. The questions for each and every potential target are simple “What are you doing to prepare for the inevitable attack? How will you protect your systems and data assets from theft and destruction?”

Enter hot cloud storage with immutability for data protection. Combined with a comprehensive backup and recovery application like Veeam, Rubrik, or Commvault, hot cloud storage provides a secure, high-performance, air-gapped, and immutable data protection option that is virtually impossible for cyber terrorists to compromise. The consistent and secure practice of backing up applications, configurations, and data is considered the cornerstone of a ransomware mitigation best practice. Without having a secure backup, stored offsite and away from the impact of a breach, there is very little anyone can do but pay the ransom and hope they get all their data back.

> *“It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.”*
>
> - Ransomware Guide,
> United States Cybersecurity & Infrastructure Security Agency



Immutable Backups Support Data Protection Across all Types of Workloads

In order for any data protection offering to be effective in mitigating ransomware attacks, it must provide at least these three things - cost-effectiveness, high performance, and data security.

PRICE

A cost-effective solution not only serves to mitigate the impact of a ransomware attack but also supports the broader goal of continuous data protection. Cloud-based storage, especially for backup datasets, is the most economically feasible solution for storing enterprise data in a secure off-site location. In most cases, the exceedingly low cost of Wasabi’s cloud storage offsets the licensing costs of the backup and recovery application, reducing the overall cost and significantly improving the expected ROI by years or months.

PERFORMANCE

A performant solution will ensure that your data backups are always available and accessible at the speeds necessary to bring applications and datasets online sooner than later. With proven ingest and egress speeds across a plethora of object sizes and thread counts [refer to forthcoming performance testing results], it is reasonable to depend upon cloud-based storage for rapid system recovery, as opposed to hoping the tape you shipped out last week will be on the first truck back to your facility… sometime soon. Other cloud storage services, especially those that tier data to lower/slower forms of data storage (aka - tape), will be delayed in their response for retrieval. Using hot cloud storage ensures that when rapid recovery is required, the files are immediately available and delivered at maximum speed.

SECURITY

A secure data protection solution will provide Nth-level safeguards from data loss or tampering. For cloud-based storage, that begins with the basics - account management, authentication, and authorization. A secure solution will also ensure that NOBODY can delete or alter your data. That part of the solution is provided by data-at-rest encryption and immutability.

While encryption is commonly employed end-to-end, starting with the backup application across the network to the storage, immutability is a relatively new technology for some. Immutability protects your data from EVERYONE, including yourself. That means when a backup is stored as an immutable object, or as a series of immutable objects, the immutability policy dictates when the object can be removed or altered. Most of the major backup and recovery applications support the S3 API for immutability/object locking today and manage the locking process as part of their backup policy definition.

KEY FEATURES

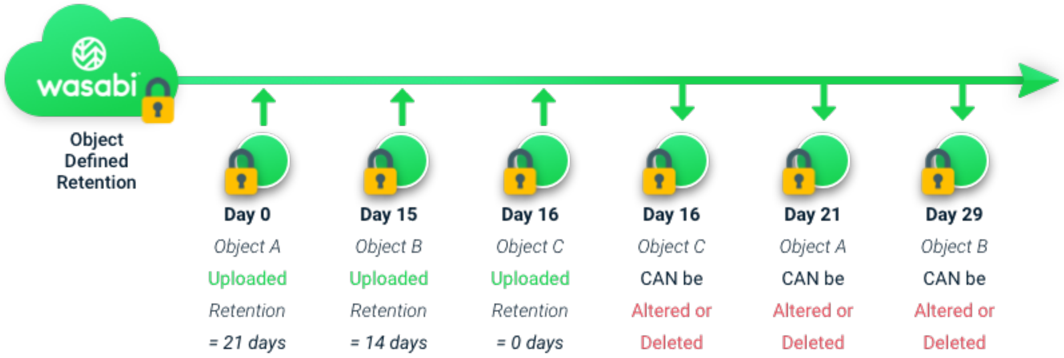
- Affordable pricing at a fraction of the cost of Amazon/Google/Azure storage
- Industry-leading performance for upload and egress
- Instant accessibility, no delays ever
- Immutable objects are unalterable and indestructible
- Satisfies regulatory compliance - HIPAA, CJIS, GDPR, FERPA, and MPA
- Integrated with leading data protection applications

BENEFITS

- Predictable cost, with options for pay-as-you-go and reserved capacity
- Fast ingest to meet tight backup windows
- Fast egress to meet demand RTOs
- Exceptional system resiliency and data integrity
- A key element in data protection best practices for ransomware defense

Wasabi S3 Object Lock with Compliance

Retention dates can **ONLY** be extended; **NOBODY** can shut off object lock



A WELL ROUNDED, DEFENSE-IN-DEPTH SOLUTION

Combating ransomware requires an arsenal of processes and technologies all focused on keeping your data secure and available. Organizations, such as NIST, CISA, and others have published and promoted a plethora of resources and guides for avoiding the impacts of a ransomware attack. Each and every resource references the critical importance of a robust backup process that utilizes secure storage physically separated from the primary systems - cloud storage utilizing encryption and immutability being the obvious choice for recovery performance. Regardless of the scale of your IT infrastructure, you will be attacked. Employing multiple levels of defensive processes, with an emphasis on secure, immutable backups, is your best defense today and in the future.