Backblaze

# Fully Protecting Critical Veeam Data From Ransomware Using Immutability

# Contents

# Overview

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands that the victim pay a ransom in order to have their unencumbered access restored. Ransomware attacks are one of the biggest threats to businesses today, and the risk continues to rise.

As ransomware becomes more sophisticated and hackers demand bigger payouts from organizations big and small, even small and medium-sized businesses (SMBs) are well served to view protection as essential.

In this white paper, we review the current state of ransomware and different vectors of attack. We then walk through what you can do to protect your business when using Veeam backup solutions, review specific protection strategies, and compare different backup methods. We explain why and how to set up cloud storage with immutability using Veeam Backup & Replication™. Finally, we compare different cloud storage options to achieve ransomware protection with Veeam.

## Introduction to Veeam

With more than 400,000 customers worldwide, Veeam is a market leader in virtual machine backup and data protection. Veeam users find themselves at an advantage when it comes to protecting themselves against ransomware because their data is securely backed up. Notably, 96% of Veeam customers attacked by ransomware kept their average ransomware recovery costs under $5,000, a fraction of the average recovery cost.

# Current State of Ransomware

Ransomware has come a long way since the days when bad actors handed out infected floppy disks to unsuspecting victims. In terms of prevalence, cost, and increasing threats to organizations, ransomware is pervasive and on the rise.

## Growth and Prevalence

The first ransomware attacks occurred in 1989 with floppy disks distributed across organizations, purporting to raise money to fund AIDS research. At the time, the users were asked to pay $189 to get their files back. Since then, ransomware has taken advantage of multiple developments in technology, similar to other high-growth industries.

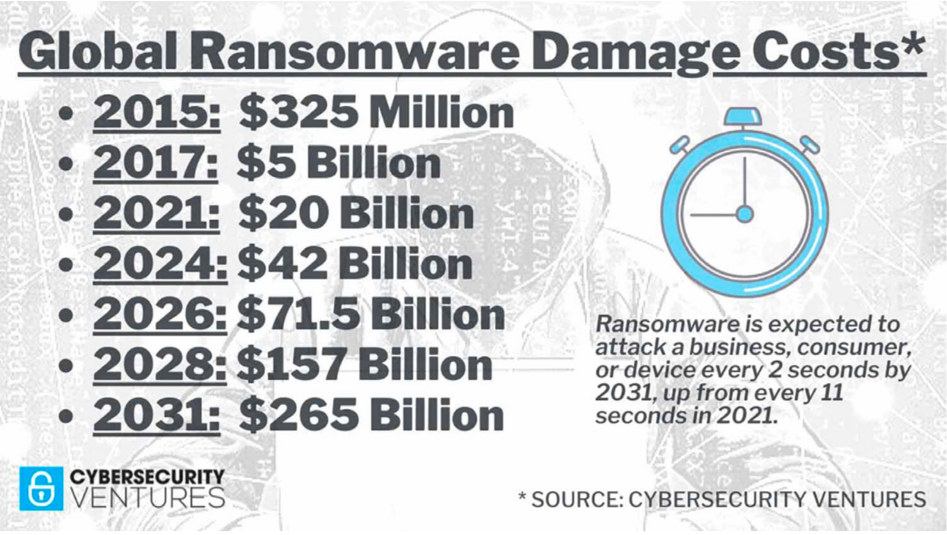
With the advent of multiple facilitators, ransomware has grown significantly since the mid-2000s. Sophisticated RSA encryption with increasing key sizes makes encrypted files more difficult to decrypt. Per TechRepublic, ransomware kits are now relatively easy to access on the dark web and only cost $70. With cryptocurrency now firmly in place as a financial pathway, payment is both virtually untraceable and irreversible. Sadly, as recovery becomes more difficult, the cost to business rises alongside it. The frequency of attacks has increased as ransomware has evolved to be more accessible, more virulent, and stealthier at evading detection.

# Cost

Today, cybercriminals demand higher and higher ransoms on the order of hundreds of thousands or even millions of dollars. In 2021, the REvil ransomware group demanded $70 million in an attack on Kaseya software. And in Q4 of 2021, Coveware found the average ransom paid was $322,168—up 130% from the previous quarter.

Recent predictions from Cybersecurity Ventures paint an even bleaker picture for the future, putting worldwide ransomware damages at $265 billion by 2031 and a new attack every two seconds, up from every 11 seconds in 2021. Cost

The number of days a company is down resulting from ransomware is on the decline, but the cost of downtime has increased. The average number of days a ransomware incident lasts is just around six days. The estimated downtime costs increased from $761,106 to $1.85 million. The increasing financial impact on businesses of all sizes has proven that the business of ransomware is booming, with no signs of slowing down.



**Global Ransomware Damage Costs***

- **2015: $325 Million**
- **2017: $5 Billion**
- **2021: $20 Billion**
- **2024: $42 Billion**
- **2026: $71.5 Billion**
- **2028: $157 Billion**
- **2031: $265 Billion**

*Ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up from every 11 seconds in 2021.*

CYBERSECURITY
VENTURES

* SOURCE: CYBERSECURITY VENTURES

*Ransomware Damages 2015-2031*

## Threats to SMBs

With total costs in the billions and threat actors demanding astronomical ransoms, SMBs risk being lulled into a false sense of security by thinking hackers set their sights on much larger businesses. That false sense of security actually makes SMBs prime, unsuspecting targets for ransomware attacks.

Why attackers target SMBs:

- **Constrained IT budgets.**
- **Lack of protections in place.**
- **More likely to pay a moderate ransom rather than risk downtime.**

In an article from Bitdefender, ransomware attacks have transitioned from one-off attacks to large-scale extortion operations aimed at vast server networks in a "spray and pray" approach. Ransomware slowly morphed into what model analysts call "ransomware as a service," or RaaS.

Cybercrime syndicates realized they could essentially license and sell their tech to affiliates who then carry out their own misdeeds empowered by another criminal's software.

### The Most Common Ransomware Variants in Q4 2021

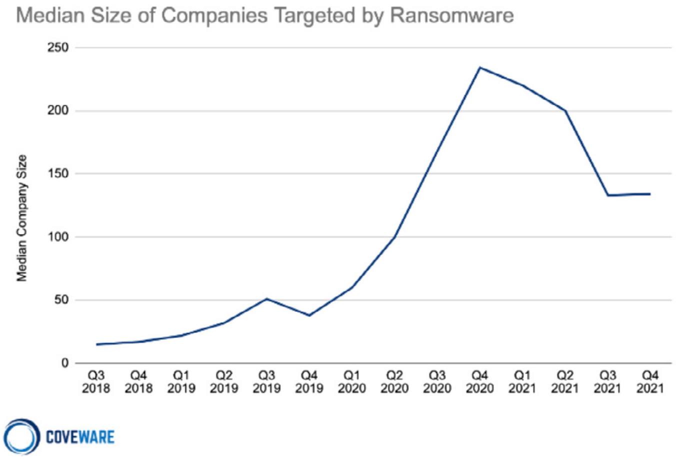
| Rank | Ransomware Type | Market Share% | Change in Ranking from Q3 2021 |
|---|---|---|---|
| 1 | Conti V2 | 19.40% | – |
| 2 | LockBit 2.0 | 16.30% | 2 |
| 3 | Hive | 9.20% | 5 |
| 4 | Mespinoza | 4.10% | -2 |
| 5 | Zeppelin | 3.60% | 1 |
| 5 | BlackMatter | 3.60% | 4 |
| 6 | Karakurt | 3.10% | New in Top Variants |
| 6 | Suncrypt | 3.10% | 2 |
| 6 | AvosLocker | 3.10% | New in Top Variants |

*Top 10: Market Share of the Ransomware Attacks*

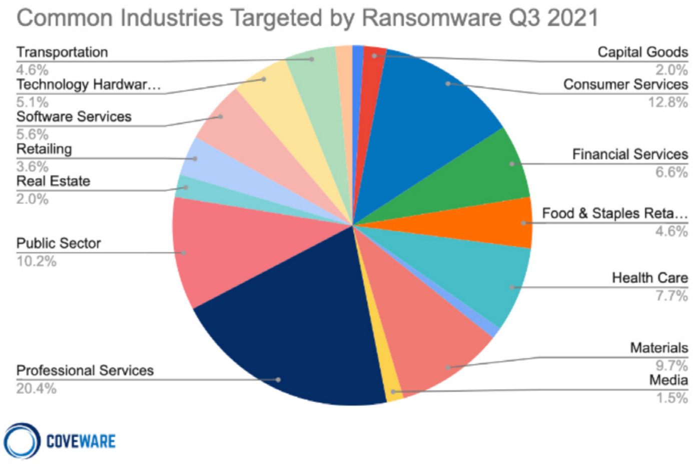
*Source:* February 2022 Coveware Quarterly Report

Though less sophisticated than some of the more notorious viruses, these "as a service" variants enable even amateur cybercriminals to carry out attacks on vulnerable SMBs that may not have the resources to defend themselves.

Coveware says they expect RaaS operations, likely spooked by the backlash to the Colonial Pipeline attack in 2021, to attempt to be more selective in their attacks so as to avoid disrupting some systemically important companies and thus drawing the ire and attention of law enforcement. However, they have not seen these groups demonstrate the actual ability to understand which companies are systemically important and which companies are not. Below is an image of the median victim size for Q4 2021. This shows that the median size has reduced over the past year and sits around 133 employees, still squarely in the SMB space with "82% of attacks impacting organizations with less than one thousand employees."



From health care to insurance to higher education, ransomware attacks happen in every sector. The Q4 2021 Coveware Report shows no industry is safe, and recent attacks prove it out.

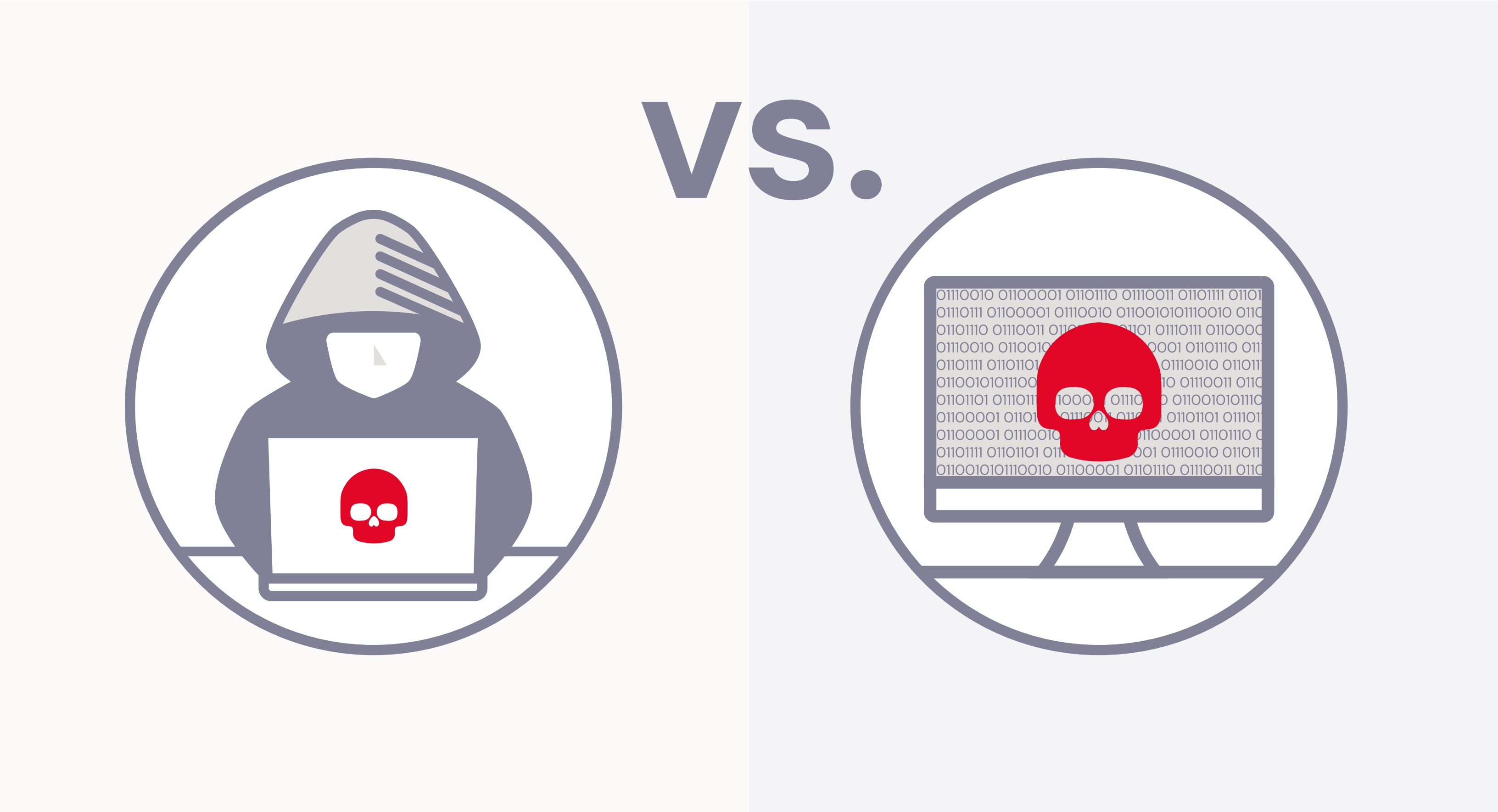


# How Ransomware Attacks

Similar to the world of infectious diseases, ransomware infects a host through a “vector” or point of entry. Much like biological viruses enter a body through the lungs or bloodstream, ransomware can infect a business through different means.

A report by security company KnowBe4 found that 91% of ransomware attacks start with a spear phishing email, but that’s far from the only method. Cybercriminals vary their tactics, and they continuously find new ways to infect victims, taking advantage of cultural, marketplace, and workforce distribution changes like the global COVID-19 pandemic.

There are two general types of ransomware attack vectors—human and machine.



# Human Attack Vectors

Cyber criminals like to exploit human factors—a tactic known as social engineering—to introduce viruses into a workplace through deception and manipulation. They prey on people's trust. Human attack vectors include:

- **Phishing:** Using fake emails to get people to click on a link or open a malware attachment.
- **Spear phishing:** Targeting employees with personal emails that appear to come from within an organization.
- **SMSishing:** Using fake text messages to get people to click on a link or provide personal information.
- **Vishing:** Leaving voicemails to trick people into installing malware on their devices to fix an imagined problem. (Yes, very convincing criminals will literally talk your staff into downloading ransomware.)
- **Social Media and Instant Messaging:** Manipulating people into opening files infected with ransomware through social media posts or by hacking into instant messaging apps.

## Machine Attack Vectors

This type of vector is automated and doesn't directly involve human input or action. An employee may unknowingly trigger a download by visiting a website, for example, but their active participation is not required. Machine attack vectors include:

- **Drive-by:** Embedding a website with malicious code that automatically downloads when users visit, or "drive by," the site.
- **Malvertising:** Placing infected ads on search engines or social media sites that download malware when a user clicks on them.
- **Remote Desktop Protocol (RDP) Vulnerabilities:** Using trial-and-error to guess user credentials or purchasing credentials on the black market to gain access to a system.
- **System Vulnerabilities:** Studying a system, particularly when a system has not been updated with the latest security releases, to find ways to break in.
- **Shared Services Vulnerabilities:** Using file sharing or file sync services to spread viruses throughout an organization, employing automated sync to copy the virus over many machines in seconds.
- **Network Vulnerabilities:** Exploiting poorly protected networks to spread viruses rapidly throughout an organization.

Once through a vector point, the ransomware locks every file it can using advanced encryption, effectively shutting a business down. It then demands payment, typically in Bitcoin, in exchange for decryption and restoration of normal operations. This type of approach, also known as cryptoware, may be the most common variety of ransomware, but it is far from the only one. Others include:

- **Non-encrypting Viruses:** These lock screens restrict file access without encrypting files.
- **Master Boot Record (MBR) Encryption:** This variant encrypts only the MBR or Microsoft's NTFS and prevents local devices from booting up in a live OS environment.
- **Extortionware or Leakware:** This ransomware threatens to expose sensitive or confidential data unless a ransom is paid.
- **Mobile Device Ransomware:** This type of virus targets cell phones using drive-by downloads or fake app downloads.

## A typical ransomware attack follows the following phases:

PHASE 01

### Infection

The ransomware enters through a vector, like a phishing email or attachment, and initiates an install on the endpoint and any available, networked devices.

PHASE 02

### Secure Key Exchange

The ransomware alerts the hacker's command and control server to create cryptographic keys for use on the local network.

PHASE 03

### Encryption

The ransomware encrypts files on the local devices and network.

PHASE 04

### Extortion

The ransomware displays instructions on local device screens demanding the organization make ransom payments or risk destruction of the data.

PHASE 05

### Payment or Recovery

The organization has two choices at this point.

(1) They can pay the ransom and rely on the hackers to restore encrypted files—far from a guarantee.

(2) They can delete infected files and restore data from a clean backup.

Unfortunately, paying the ransom doesn't always lead to decryption—a 2021 survey found that only 8% of organizations that paid ransoms were able to recover all their data, and the average amount of data that was recovered after paying was only 65%.

# What You Can Do

The old saying, “an ounce of prevention is worth a pound of cure,” could not be more applicable when it comes to ransomware. Rather than stockpiling cash in the event of an attack, spend that money on prevention—it is the most pragmatic protection to implement.

Invest in training for employees on how to recognize phishing scams. Human vectors are the most frequently used points of entry for ransomware, and training employees to identify and report suspicious emails, websites, ads, messages, and phone calls is still one of the most effective methods to avoid ransomware attacks.

After training, make sure to update your anti-virus and anti-malware software. Finally, a solid data backup approach is key. Make sure you frequently back up important files and keep them safe with the 3-2-1 strategy—the industry standard for data protection.

## Why 3-2-1 Works

A 3-2-1 backup strategy means you have three copies of your data: two local copies and one off-site. For many businesses of scale, you have a copy on your server, a copy on another on-premises repository like NAS, and a copy off-site. Keeping a backup copy of data on-site works best when you need to restore data quickly. It’s right there at your fingertips. But, for that very reason, it’s also susceptible to many of the same data loss risks as the copy on your main device or server. Unexpected events like floods, fires, or ransomware could potentially wipe out both copies, leaving you without any way to get your data back.

An off-site, disaster-recovery copy protects you from that fate. Your off-site copy—typically kept in the cloud or on tape—enables you to easily restore your virtual environment in the event of a disaster or attack where your two on-site copies are destroyed or infected.

# Not All Backups Are Bulletproof

Most Veeam administrators approach backups in one of two ways: Veeam to an on-premises repository or Veeam to tape, but these approaches are only moderately effective when it comes to protection against ransomware. Here, we outline the advantages and disadvantages of each approach.

## Veeam to On-premises

### Advantages

Storing Veeam backups on an on-premises appliance or private cloud offers some security as backups are stored on a different piece of infrastructure. Additionally, there are disk-based solutions that offer a Write Once, Read Many (WORM) model. With data on a different piece of infrastructure, you would be protected from minor disasters, for example a small fire that destroys a server, and some ransomware attacks. However, the main advantage of on-premises storage is speed—you don't need to rely on an internet connection to back up or restore data. If you need to restore quickly, the data is readily available.

### Disadvantages

This approach is only moderately effective because the same natural disasters or infrastructure failures that affect your primary storage can eliminate backups. The cost of spinning up a secondary storage with appropriately-sized infrastructure is both challenging and time consuming. Determining the exact size of disk space needed involves educated estimates at best. When deploying infrastructure with too little space, you risk errors or malfunctions due to lack of space or the need to deploy additional infrastructure as your business scales. When deploying infrastructure with excessive free disk space, you are paying for storage that will not be used. Managing a secondary set of infrastructure increases IT load exponentially. Moreover, without an off-site backup, this approach is not 3-2-1 compliant, and only moderately effective at best.

*Efficacy: Moderately Effective*

# Veeam to Tape

## Advantages

Unlike an on-premises repository, backing up Veeam to tapes allows for the data to be moved off-site, creating an "air-gapped" backup. Creating an "air gap" means physically isolating data away from any connection that hackers could use to access and encrypt it. The tapes are not connected to the internet or LAN, so they're quite well protected. Air-gapped tapes provide protection from ransomware as it cannot infect something that has no physical or virtual connection to your on-premises IT infrastructure.

## Disadvantages

Air-gapped tape backups provide excellent protection from ransomware and hackers. For this reason, the use of tapes has increased as ransomware proliferates, but it's not without drawbacks—namely, cost and maintenance.

### 1. Cost

There are plenty of cost calculators out there to help you understand the long-term cost of tape, and you might get a different estimate from each of them. First, tape backups require an up-front investment in infrastructure—the hardware and the tapes themselves. With a capital investment, you have to consider depreciation and tax implications. After that, the total lifetime cost of tape can be influenced by a wide variety of factors, including:

- **Backup Model:** The backup model you choose can impact how many tapes you'll need.
- **Data Compression:** The data compression ratio you use can increase the cost of tapes. For example, companies that store a lot of images and videos likely don't compress their data, driving the cost of tapes up.
- **Data Retention:** Your data retention policy can increase the cost of tapes. For example, healthcare companies subject to HIPAA requirements and local governments with legal information are frequently required to keep data for months or years, again, driving costs up.
- **Tape Systems:** Different tape systems may cost more up front and require more maintenance than others.
- **Tape Migration:** The hardware you buy is not the hardware you'll be using in 10 to 15 years as versions become unsupported. At some point, you'll face the prospect of migrating a decade or more of data.

- **Transport Costs:** Whether it's an employee or a vendor, someone has to take your tapes from place to place, and that comes at a cost.

- **Physical Storage:** Storage providers like Iron Mountain charge fees to keep your tapes off-site.

Costs associated with tape might take the form of relatively small monthly bills that nonetheless add up over time, or they can come as huge expenses like migrating decades of data to a new version of tape. Depending on your needs and specific use case, the costs can make something that seems affordable up front become a substantial expense in the long run.

## 2. Maintenance

You'll likely be paying at least one employee to spend most of their time managing, operating, and maintaining the tape system. Alex Acosta, Senior Security Engineer at Gladstone Institutes, a Veeam client who in 2020 switched from tapes to cloud storage using Backblaze B2 Cloud Storage as a storage tier, described dealing with tapes in no uncertain terms: "It's cumbersome. It's messy. The tape drives get dirty. We had issues with tapes going bad. Backup files would fail because the tape failed. We spent a lot of time just troubleshooting things that in 2020 we shouldn't be troubleshooting anymore." When the company invested in the tape infrastructure, he'd spent countless hours unpacking tapes, organizing them, labeling them, and filling them in a 900-tape library.

Tapes require complicated upkeep—keeping track of which content is on what tape, making sure you have the proper hardware to read old tapes, dealing with tape failures, cleaning tapes, pulling tapes whenever data is needed, the list goes on. All that takes time and resources away from other job duties and company priorities.

*Efficacy: Effective*

> **"It's cumbersome. It's messy. The tape drives get dirty. We had issues with tapes going bad. Backup files would fail because the tape failed. We spent a lot of time just troubleshooting things that in 2020 we shouldn't be troubleshooting anymore."**
>
> – Alex Acosta, Senior Security Engineer, Gladstone Institutes

# Veeam to Cloud Storage With Immutability

## Advantages

Cloud storage with immutability creates a virtual air gap, providing the protection of air-gapped backups without the expense and maintenance of tapes or other specialized storage appliances. Creating immutable backups means no one can modify, encrypt, tamper with, or delete your protected data for a specified period of time.

The public cloud—third-party computing and storage services accessed via the internet—is uniquely suited for this type of protection. Your data is always accessible (for you), it's off-site, making it compliant with a 3-2-1 philosophy, it's easily scalable, and you can manage costs with affordable and transparent pricing.

When comparing the options for ransomware protection, the cost varies greatly between on-premises storage, tape, and cloud storage. Unlike on-premises hardware, by default, cloud storage is sized to your backup set. With cloud storage, you only pay for storage in use and the storage scales automatically to meet your needs. Additionally, the cost of on-premises and tape backups don't often include the extraneous cost of IT load, which is automatically included in cloud storage pricing.

## Disadvantages

Backups and restores with cloud storage are only as fast as your internet connection. Bandwidth limitations can slow download times especially when you're dealing with large amounts of data. Cloud services providers increasingly offer integrations and solutions to manage this issue, but bandwidth remains a physical reality that should be considered as part of a business's migration to the cloud.

*Efficacy: Most Effective*

## How It Works

A virtual air gap works like a physical air gap, but without the need for separate physical infrastructure like tape. Veeam accomplishes this using Object Lock functionality. With Object Lock, you can store objects using a Write Once, Read Many (WORM) model, meaning after it's written, data cannot be modified. Object Lock must be enabled on a bucket at the time the bucket is created. For files going into a bucket with Object Lock enabled, there are two ways to lock them:

1. **Set a date when you upload the file as part of the call to the API.**
2. **Set a date on a file that is already uploaded.**

For both methods, you must set a date indicating how long the file should be locked. After that, any attempts to delete the file or make any changes to it before the set date will fail. While you can use the second method to extend the lock on a file, you cannot use it to shorten the lock.

## Why It Works

With Object Lock functionality, there is no longer a need for tapes or a Veeam virtual tape library. You can now create virtual air-gapped backups directly in the capacity tier of a Scale-out Backup Repository (SOBR). The benefits to this approach include:

- **Data is WORM protected and cannot be modified.**
- **Even during the locked period, data can be restored and used on demand. Only the backup is locked, and it is only locked to prevent deletion or modification.**
- **Once the lock expires, data can safely be modified or deleted as needed.**
- **If retention policies shift due to regulatory compliance, with Object Lock, data is retained for the necessary time frame per regulatory guidelines.**

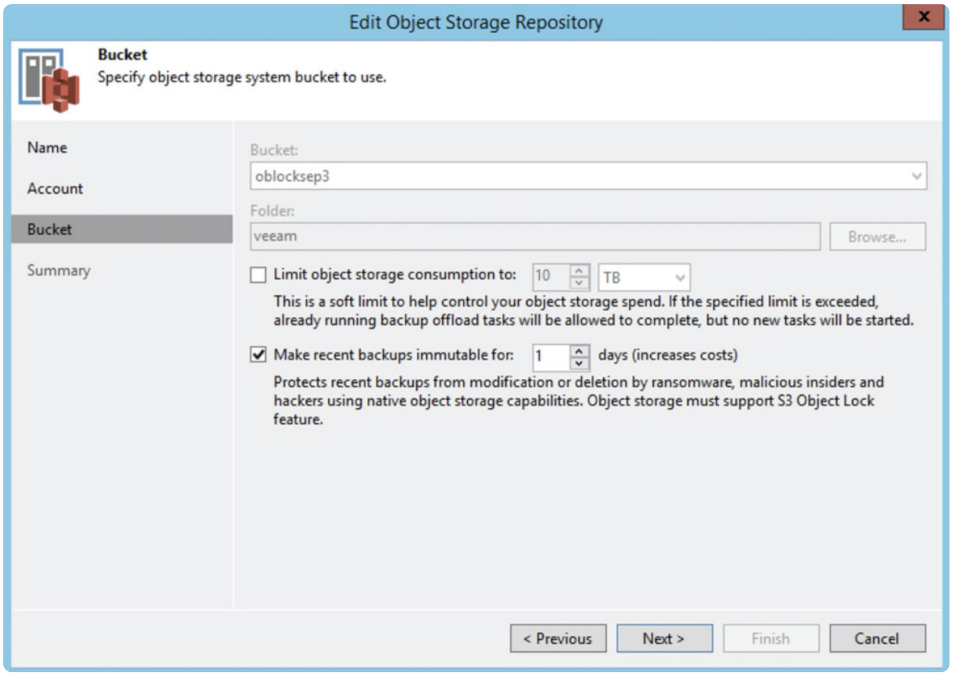
### A Case Study in Immutability

Alex Acosta of Gladstone Institutes, who sees his role as directly enabling scientific research to fight COVID-19, explained that immutability can help his organization maintain healthy operations. "Immutability reduces the chance of data loss," he noted, "so our researchers can focus on what they do best: transformative scientific research."

## How to Set It Up

Using Veeam Backup & Replication™, you can now just check a box and make recent backups immutable for a specified period. It's simple to get started and easy to maintain.

1. Create a bucket that has Object Lock enabled.
2. Within your SOBR, simply check the box to make recent backups immutable.
3. Specify your time frame.



Edit Object Storage Repository

**Bucket**

Specify object storage system bucket to use.

Bucket: oblocksep3

Folder: veeam

☐ Limit object storage consumption to: 10 TB

This is a soft limit to help control your object storage spend. If the specified limit is exceeded, already running backup offload tasks will be allowed to complete, but no new tasks will be started.

☑ Make recent backups immutable for: 1 days (increases costs)

Protects recent backups from modification or deletion by ransomware, malicious insiders and hackers using native object storage capabilities. Object storage must support S3 Object Lock feature.

# Finding a Cloud Storage Option

To achieve immutability, you will need to connect your backup data to a cloud storage option. Veeam offers a number of cloud-tiering options. Of those, both Amazon S3 and Backblaze B2 Cloud Storage supports immutability, and there are a number of differentiators to consider when weighing which offering to choose.

## Cost

Though it's not the only decision factor, cost is an important differentiator when it comes to comparing providers. Amazon S3, for example, offers a range of pricing tiers, but navigating them can be highly complicated. For those of you considering this step, the following information aims to simplify decision factors between different storage tiers to help you understand what kind of cloud storage will work best for your needs.

## Multiple Tiers: Amazon S3

Amazon S3 offers several classes for hot and cold storage. There are no standard industry definitions of what hot and cold mean when applied to data storage, so you'll find them used in different ways. Hot storage, in the case of S3 Standard, stores data that needs to be accessed right away. If your data backups are business-critical and you can't wait for them when you need them, you'll need hot storage. Amazon charges a premium for hot data storage because it is resource-intensive.

## Cold Storage: Amazon S3 Glacier and Deep Glacier

Cold storage, such as Amazon's S3 Glacier and Deep Glacier tiers, stores data that is accessed far less frequently and doesn't require the fast access of warmer or hot data. That includes data that is no longer in active use and may not be needed for months, years, or maybe ever. Data retrieval and response times for cold storage systems are typically much slower than services designed for active data stores. Storage prices for cold cloud storage systems are lower than warm or hot storage but often incur high warming fees and high data transfer costs for quick retrieval. Access to the data in cold storage typically requires patience and planning.

## The Additional Cost of Complex Billing

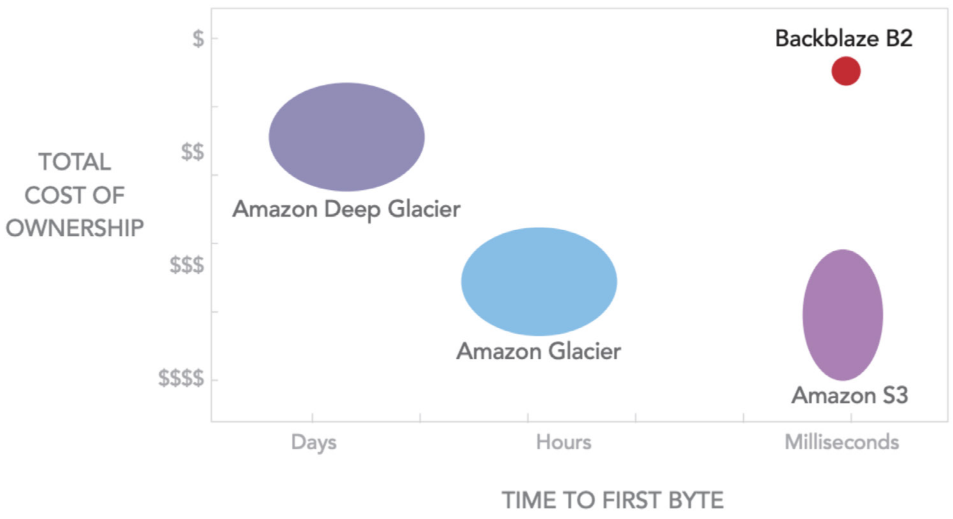
Many businesses who prefer S3 now employ third-party vendors that specialize in cloud optimization consulting to help them navigate this complexity. This translates to a higher price of deployment than what standard estimates might suggest. However, if your infrastructure needs are optimized to a tee, you may be able to avoid such services.

## Single Tier: Backblaze B2

While structuring cloud storage by temperature is commonly used by the first-generation cloud storage providers—Amazon, Microsoft, Google—to describe their tiered storage services and set pricing accordingly, Backblaze has a simple approach.

Backblaze's B2 Cloud Storage product offers a single storage tier with the performance and availability of hot cloud storage, at the cost of cold cloud storage. B2 Cloud Storage doesn't only compete on price with tape and other traditional cold storage services, but can also be used for applications that are usually reserved for hot storage, such as data retrieval in the case of ransomware attacks.

When comparing providers, running cost scenarios that compare total cost of ownership between providers can help clarify your decision-making process:



# Conclusion

From this paper, the conclusions should be twofold. First, ransomware attacks are here to stay, so preventing and responding to them will become an increasingly critical aspect of IT workloads. Second, and more important, there are simple steps you can take today to massively reduce *your* workload in this area. Ensure your backup strategy is 3-2-1 compliant, and consider air-gapped backups using cloud storage and immutability. Testing these solutions with any range of services is easy, and once you choose one, you'll rest easy, too, knowing that your data is safely tucked away from any malicious code or actors.

# About Backblaze

Backblaze makes it astonishingly easy to store, use, and protect data. The Backblaze Storage Cloud provides a foundation for businesses, developers, IT professionals, and individuals to build applications, host content, manage media, back up and archive data, and more. With over two billion gigabytes of data storage under management, the company currently works with close to 500,000 customers in over 175 countries. Founded in 2007, the company is based in San Mateo, CA.

For more information, please go to www.backblaze.com.