ComputerWeekly.com

Why immutable buckets are a worthy risk management tool

Michael O'Dwyer

Immutable buckets offer businesses benefits in terms of data compliance, backup, archiving and security

Data loss, even if temporary (prior to restoration after a ransomware attack, for example) disrupts business activity and causes reputational damage, driving companies to find better ways to protect their data better to minimise the risks associated with a cyber-attack, hardware failure or any other external or internal threat such as malicious employees.

One way of achieving this goal is by using immutable data storage objects known as buckets, according to David Friend, co-founder of Carbonite and CEO of Wasabi, a Boston-based cloud data storage company.

Immutable, by definition, means set or inflexible i.e. cannot be changed. System administrators are familiar with the concept of immutable folders from their use of Windows Server, Unix, Linux and other operating systems.

Wasabi's primary offering is cloud storage, but immutability is an optional feature, one that is currently limited to a few other providers, says Friend, citing Microsoft's Government Cloud as an example.

"Immutable means that the user cannot delete files under any circumstance. There is no 'admin privilege'.

Even at Wasabi, no one person can delete the data. For instance, if a customer fails to pay their bill, it's a big process involving multiple people having to simultaneously 'turn their keys' to delete an abandoned immutable bucket", he says.

It could be argued, that when a service provider has to take extraordinary measures to delete an immutable bucket, it is an indication that enhanced security procedures are in play.

Backups and archives

System admins regularly work with backups and archives, as part of an overall risk management regime.

"Most often, companies backup their data to local hard disks using specialised software," says Dmitry Vyrostkov, chief software architect and security expert at DataArt, a global technology consultancy.

"Companies that use managed hosting providers or cloud solutions typically take advantage of included backup solutions. Archives are different from backups as they aim to create a searchable database of company files so that critical documents could be found by their attributes even if these documents were processed years ago.

"Archiving is not a replacement for backups but rather serves a different purpose. It is often used in forensics, for example. Archives could be used for restoring specific damaged files, although it would be hard to use them to restore the entire system," says Vyrostkov.

Ransomware has several attack vectors that exploit vulnerabilities (human error, software or hardware) but once launched data encryption is the aim before a ransom demand is made. In terms of backup, there are multiple solutions to prevent this encryption stage.

"Immutable folders are one solution to ransomware but most backup products have some good protection from ransomware," says Oscar Arean, technical operations manager at Databarracks, a London-based DRaaS provider.

“A lot is made of the ‘air gap’ that a truly offline backup has – for instance, tapes,” he says. “There is no possible way for the ransomware to get onto a tape backup that is physically separate from the systems it has a backup of. In fact, most backup systems are well protected from ransomware even without this gap. Well managed backup systems sit outside the domain of the business they are protecting. They may be onsite or offsite, but they aren’t using the same permissions as the rest of the network.”

Tangible benefits

Unfortunately, if speed of recovery is a factor, or read-only access to data in real time is needed, such as for data analytics purposes, then tape or other offline solutions are not feasible. The benefits of Wasabi’s immutable buckets include, but are not limited to:

Speed

“Nothing is faster than an array of disks all pumping out data simultaneously onto a very high-speed backbone,” says Friend. “With highly parallelised architecture, like Wasabi’s, data restoration speed is highly unlikely to be governed by the speed of the storage. It’s more likely to be limited by the speed of the machine that is being restored.”

The Wasabi service is promoted as being six times faster than Amazon S3 although the access speed will depend on the client’s broadband connection speed.

Durability and Permissions

Given the earlier comparisons between Amazon and Wasabi offerings, does durability and access control suffer?

“A lot of the storage experts I’ve talked to obsess about ‘durability’ or how many ‘nines’ does your storage have. Both Amazon S3 and Wasabi have 11 nines of durability,” says Friend.

“To put this in real-world context, if you gave me one million 1MB files to store, statistically I will lose one file every 659,000 years. There is so much redundancy built into these systems that suppliers just don’t ‘lose’ their customers’ files any more. But I can tell you from experience, that even the best-run shops lose data every day.

“The reasons are always the same: human error, bugs in application software, viruses, malware, and employee sabotage. If you want to protect your data, worry about these causes of data loss, not how many nines your storage vendor has,” he says.

Permission management

“On the permissions topic, Wasabi uses the same proven identity and access management (IAM) as Amazon Web Services (AWS). This approach ensures our service offers the same sort of user management and policy controls for permission management as S3 does,” according to Friend.

“Whether the user can overwrite existing data is also a factor of the permissions and policy settings of that user and the target bucket,” he says. “For example, if the bucket is configured as an immutable bucket, the existing data cannot be modified/deleted/overwritten etc. If the bucket is not set for immutable mode, an existing file can be overwritten or if versioning mode is configured, another copy of the file will be saved (with a different file name from the original file).”

Data protection

Immutable buckets can block encryption if ransomware evolves to the stage where it targets data outside the company network. Since data cannot be overwritten, even infected data that is added to the bucket cannot infect other existing files or folders.

“If you don’t store your backups in immutable buckets, they too could be vulnerable to attack and then you risk losing everything,” says Friend, adding that most backup software will allow you to restore backups without including malware or other infected files.

Security against insider threats

In an age of internal employee threats, whether deliberate or accidental, immutability offers an additional level of protection and is totally distinct from previous permission-based access levels set by an administrator.

It's not at all like read-only folders with admin privileges. Such folders are not immutable because an admin can accidentally or maliciously delete or alter files. At Carbonite, we saw many instances of internal sabotage by disgruntled employees deliberately destroying files to which they had admin privileges," says Friend.

Cost

Wasabi offers a flat-rate price of S$.0039 per gigabyte per month for storage (regardless of how much you store). This results in a price per terabyte per year of $47.92, which is about five times cheaper than Amazon S3.

Is immutability worth it for your business?

Experts indicate that immutable buckets are a good idea. DataArt's Vyrostkov says they are a good option for businesses of all sizes.

"It is easy to setup a background task that would regularly upload most critical files or databases to the online bucket and make it immutable," he says.

"However, for protecting against ransomware threat, immutability is not a key factor here, as ransomware is far from being sophisticated enough to damage online backups of files being encrypted," says Vyrostkov, adding that Immutability helps prevent accidental or deliberate deletion of backups by company employees.

This is certainly a more important function, considering that traditional methods rely on admin control of some sort, some might say this is an inherent security gap.

Regulatory and legal requirements worth considering

Immutability is a feature that is interesting for archiving and legal-hold, according to Databarracks' Arean.

"Backup and archive are two different things but there is a lot of cross-over. You might say that the only purpose of backups is to be able to recover, whether that is from a ransomware attack or something more mundane like an accidental file deletion. Or, you need to recover data to meet a compliance requirement. A backup is a copy of your data whereas the archive is the older data."

Given the low storage cost involved, immutable buckets are worth considering, but not for all data.

"When the value of the data greatly exceeds the cost of saving it, I would always use immutable buckets. As the cost of storage drops, the decision to store immutably becomes ever easier," says Friend. "If data are short-lived, for example temporary files associated with a word processor, or are of very low value, then there may not be any point in storing it in immutable buckets.

"If you won't really miss it if it gets destroyed, then it's not worth the trouble and expense of storing it immutably," he says. "Whatever you decide, it is important to test your solution according to a defined disaster recovery plan."

Regular testing of disaster recovery plans

Among the most important factors, says Vyrostkov, is that companies should invest in regular testing of their disaster recovery plans that they designed and implemented.

"Otherwise, in the event of data loss, it may happen that due to a human error, the restoration process is not possible or it will take significantly more time that was anticipated initially," he says. "For example, backing up complete systems hosted on-premises to the online store may be risky, because in the case of a successful attack, it may take quite a long time to download all required backups."

Arean agrees that restoration time is important but selecting the correct backup to restore is also an issue.

“One of the biggest factors in recovering from ransomware is that if you aren’t certain when the infection occurred, you may need to carry out recoveries from several backups to find the most recent, clean backup,” he says.

Businesses should ask if their storage provider offers immutable options. If not, then it will likely do so soon, as it seems to me that protecting data from accidental or deliberate deletion, even by an administrator, is a means of closing risks that were previously unavoidable.

Original article can be found here: http://www.computerweekly.com/feature/Why-immutable-buckets-are-a-worthy-risk-management-tool