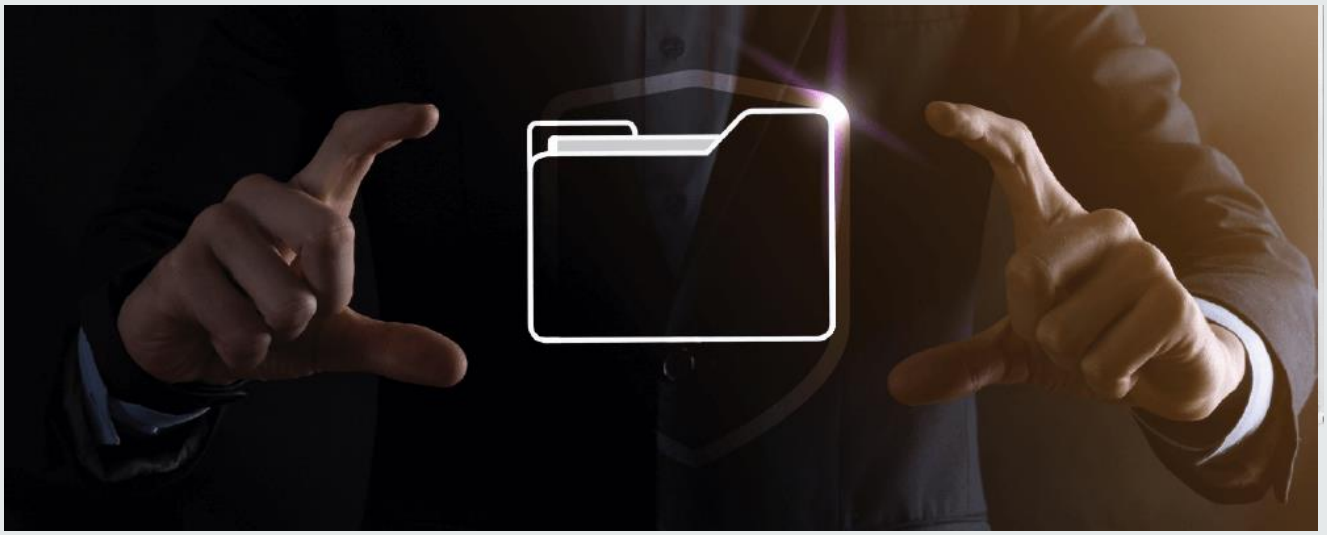
PARABLU

Why Data Immutability should be a critical element of your Backup Strategy



Most people think of backups of just being a secondary copy of data. Something you can go back to in case you lose your primary copy. Lost a file? Download it from the backup. Lost an email? Restore it back from the backup.

And this makes a lot of sense – and these are definitely obvious backup use cases. You may add to these, scenarios like "I lost/damaged my laptop".

Enterprise backup strategies with Immutable backups

However, it turns out businesses have many more uses for backup than simply being able to give employees their data back when they lose it.

Regulatory Compliance

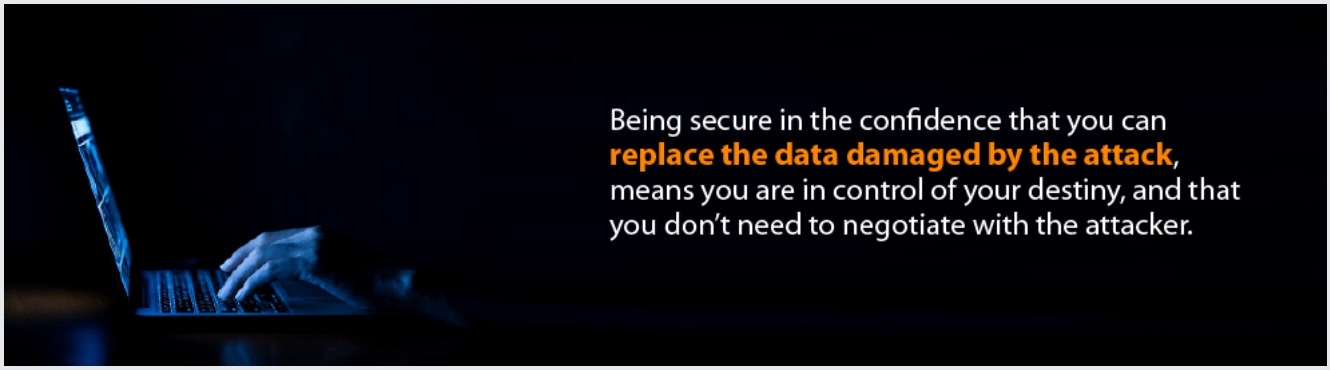
Many businesses function in regulated verticals like banking, financial services or healthcare. Even companies outside these verticals, if doing business internationally, need to stay compliant with regulations like Sorbanes-Oxley (SOX) or the General Data Protection Regulation (GDPR). Almost all regulations require a few basic compliances and one of them is that you don't lose data! Losing data can be viewed seriously, and penalties for non-compliance can be stiff.
The accountability that these regulations impose, drives businesses to put together processes in place to preserve and secure their data assets – in other words, "*a data backup*".

PARABLU

Ransomware

Ransomware is a form of malware that has existed for several decades but has really taken on a visibly destructive form only over the last few years. It operates by encrypting files on the infected computer and then demanding a bitcoin ransom in return for the decryption key. On an average, ransomware demands have gone up exponentially, with several demands in 2021 exceeding a $1M. It is estimated that ransomware costs companies up to $75 billion each year worldwide, and with the availability of DIY (Do It Yourself) ransomware kits available for sale on the dark net, the frequency of attacks is only increasing.

An important way to defend against, and recover from a ransomware attack is to have a reliable data backup. Being secure in the confidence that you can replace the data damaged by the attack, means you are in control of your destiny, and that you don't need to negotiate with the attacker. This is massive leverage which can be critical at the time of a crisis. Businesses who end up negotiating and paying ransom many times don't even get their data back – what's more – they've even been known to get attacked a second time in just a few weeks!



Ransomware has evolved to seek out and damage copies of backup data as well – all the more reason the backup strategy should be designed to be resistant to such attacks. Read on!

Insider Threats

Insider threats are data losses that are caused by employees. This can be caused by trusted actors within the organization. Perhaps some of them even operating with elevated privileges.

Not all insider threats are necessarily malicious. Some of them can be genuine errors like coffee spills or a dropped laptop – but Malicious Deletion – destruction of data by a disgruntled employee or an unhappy co-worker who has been terminated – is a common problem businesses face.

According to the Global Data Risk Report, an average employee has access to as much as 17% of an organization's files – which is quite a bit of exposure enterprises have to live with.

Once again, a reliable backup is a key weapon in the business arsenal. Having a way to restore back deleted data – reduces business risk massively in the case of such incidents.

Data Immutability

The types of use cases we touch on above, go well beyond the need for a single user to recover data. These use cases are designed to protect the business as a whole – and all of them demand Data Immutability.

In the case of regulatory compliance – it is important for the business to be able to prove to a regulator or an audit team that they have processes in place to protect data and ensure that it cannot be tampered with or modified.

In the case of ransomware, it is imperative that the backup data be out of reach of the ransomware attacker. Simple backup copies that are kept on the same system or synced to the cloud – are easy pickings for sophisticated attackers. Building immutability into the backup strategy is critical.

Last, but not least – a disgruntled insider who knows how the backups are made and where they can be accessed – can just as easily delete the backups along with the primary data copies. Ensuring that the backups are off-limits and protected – is a key part of a good enterprise backup strategy.

PARABLU

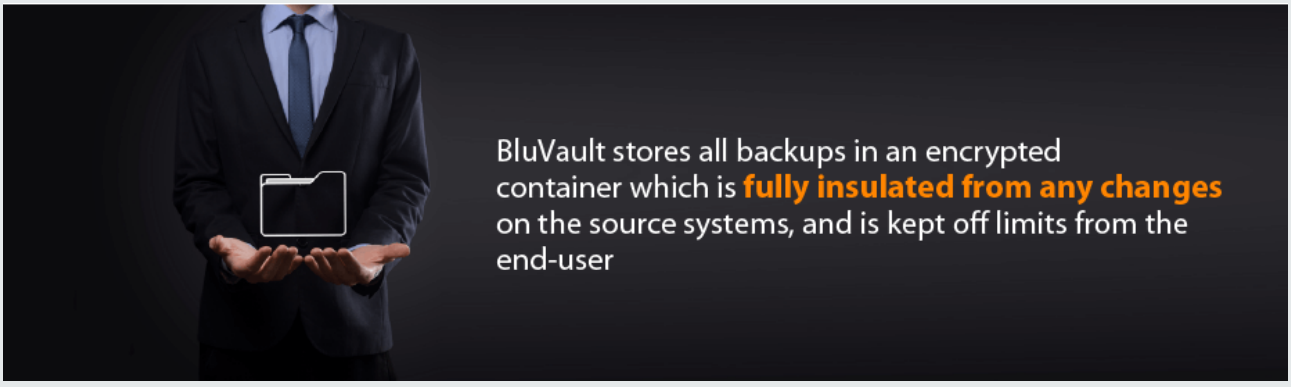
Data Immutability, simply put, means that the copy of data that is backed up belongs to the business, only to the business, and should not be available for deletion, tampering, or modification by anyone else.

Securing Backups

It is important to protect backup data from actors both external and internal. Most security barriers are placed with external threats in mind.

But once a threat has penetrated the security perimeter – it becomes an insider threat for all practical purposes. So, a threat from ransomware designed to delete backups, or a malicious insider – are both equally dangerous and have to be defended against just like from an outside attacker.

Many "sync" solutions which position themselves as backup solutions fail this test right away. A data copy which has been synced to the cloud – while it may qualify as a secondary copy – fails the immutability test. An insider (i.e. an employee) or ransomware which has unfettered access to the copy of secondary data can delete (or tamper with) it at will.



Enterprise class backup software, like Parablu's BluVault are designed and built to protect against such scenarios. BluVault stores all backups in an encrypted container which is fully insulated from any changes on the source systems, and is kept off limits from the end-user.

Even if an insider (e.g. an Administrator) has to delete something out of the backup – to satisfy a "right to be forgotten" request from a GDPR regulator, for instance – they will have their actions fully audit-logged by BluVault.

BluVault's secure container is equally protected from external threats as well. All data not only stays encrypted, but is protected by a strict enforcement of Separation of Duties. What this means is that while BluVault can encrypt or decrypt data – the encryption/decryption keys are always controlled by the enterprise, and they can be changed by the business at any time they wish.

PARABLU

Expensive storage investment?

Does data immutability mean you need an expensive storage investment? Not necessarily.

Parablu has patent pending technology that can take storage assigned to end-users (like Microsoft OneDrive for Business) and create a secure container using the unused storage allocation they already have.

The secure container not only keeps all backup data encrypted, but it is also made invisible and off-limits to the end-user. They will be able to see files and folders they've uploaded via the Office 365 web interface or using the OneDrive sync utility – but none of the data from the backup.

Self-service restores and recoveries are still possible. To restore or download any data from the backups, users simply use BluVault's web interface or Parablu's special native agent on Windows or Mac devices to recover files/folders they need.

So, when designing a backup strategy – don't ignore data immutability. And pick an enterprise class solution which can do this for you economically without having you make a heavy infrastructure investment.

For details or if you wish to explore some more, get in touch with our experts and ask for a callback.

Write to us at info@parablu.com to learn more.