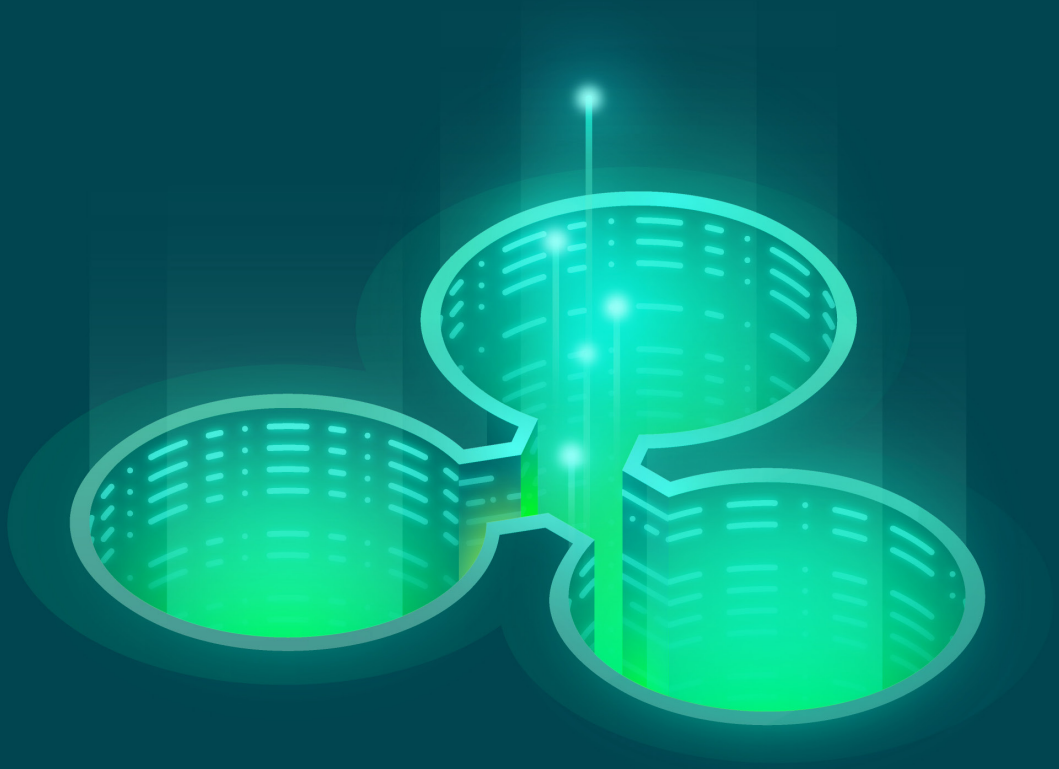
Why choose BaaS



Purvesh Dharamshi

Head – Cloud Service Provider Business SAARC

NET3 TECHNOLOGY

Data is **the essence of any organization,** or said another way, data is the new oil. That's why data protection is important, because without it, your business can suffer data loss due to user errors, ransomware attacks, hacking, sync issues, unverified updates or upgrades, malicious insiders, system issues, etc.

A sound data protection strategy is a must for organizations. Backup is like "Balle Killa" – the upper fort. In olden times, when forts were attacked by conquerors, soldiers would move to the upper fort region in response to invaders who broke through defenses so the king/commander could escape. The forward attack would continue from this upper fort. This is similar to how backup can be seen. **Backup is like this upper fort when all bastions fall — it becomes the last line of defense — and quick restores are like counterattacks.**

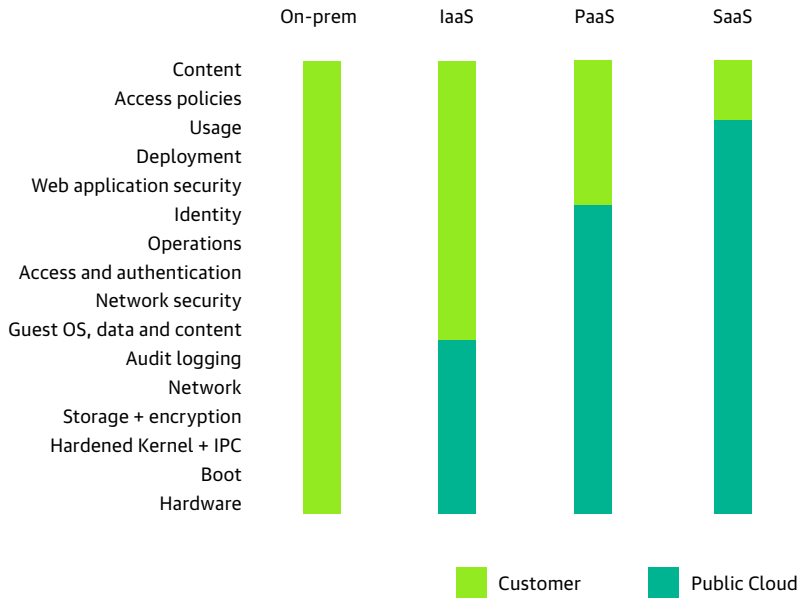
Managing data protection systems can be quite monotonous and laborious tasks for IT teams. Also, investing resources on daily mundane activities like backup would not be a good strategy for any organization. CIOs/CTOs/CISOs should consider an outsourcing strategy in their roadmaps as they build their robust systems. Many modern CXOs are adopting the cloud and outsourcing management to hyperscalers/cloud MSPs so their IT team to be more productive, focus on innovation and develop a competitive edge.

For small-to-medium-sized businesses, this becomes more relevant as maintaining multiple IT skill sets is very challenging. This outsourcing strategy works best for them as well.

Outsourcing backup jobs would help organizations:

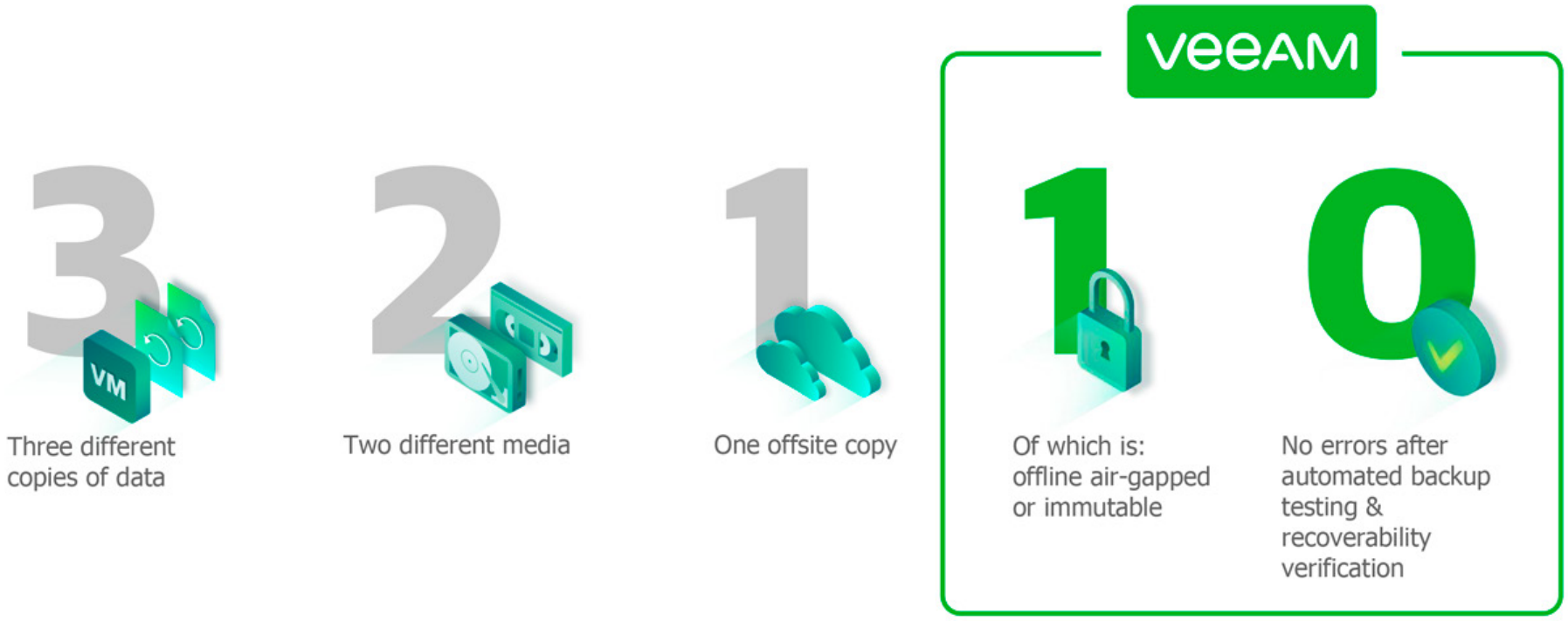
- Focus on core business functions
- Work toward innovation and rapid development
- Look at more sensitive and important issues like security
- Reduce overall TCO for backup
- Feel secure their data is protected
- Ensure compliances and reduce time to audit

Organizations should protect their data regardless of its source or where the data is generated/stored. Data can be on cloud hyperscalers, cloud storage, SaaS applications, on-prem DC servers, HCI Systems, endpoints (desktops and laptops), etc. Regardless of the data's location, organizations should have a sound data protection strategy to take backups of their data and maintain control. Also, organizations need to understand the shared responsibility model for cloud workloads and accordingly design a Modern Data Protection strategy.



What to look for in BaaS

Organization needs to decide on a data protection strategy. Outsourcing is still a good option for critical data and staying compliant. If an organization cannot put data in the cloud for compliance reasons, try BaaS. Depending on your situation, you can choose to have a service delivered within your DC or cloud. If you have data that can be in the cloud and other data that can't, you're free to choose a hybrid service. Kindly ensure your data protection strategy follows the 3-2-1-1-0 Rule: 3 copies of data, 2 on different media, 1 off site, 1 air gapped and 0 errors on backups.



Let's look at a few points to consider when choosing BaaS:

MSPs/CSPs: Choosing MSPs/CSPs can be daunting for an organization. CXOs need to evaluate the MSP/CSP org stability, services delivered, experience on BaaS, etc. If possible, try to have calls with MSP/CSP BaaS teams to build confidence. Also, check whether the MSP/CSP has offerings to cover all the data protection requirements and support you need (e.g. 9x5 or 24x7 etc.)

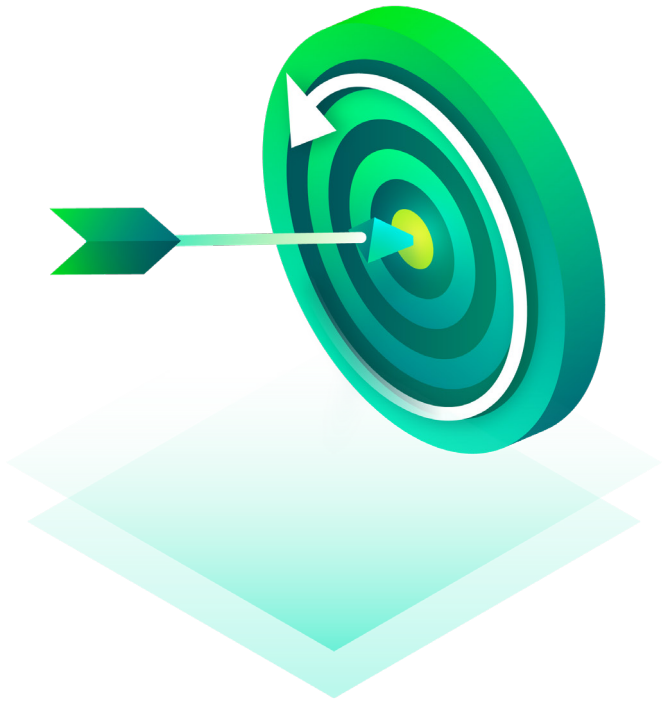
Modern Data Protection: MSPs/CSPs should provide protection for not only traditional workloads but also modern workloads. Ensure MSPs/CSPs provide data protection for traditional workloads like Windows, Linux, AIX, Solaris servers, NAS servers or virtual workloads like VMware, Hyper-V, RedHat KVM, Nutanix AHV, etc. The service should also provide a mechanism to protect data in AWS, Azure, GCP, SaaS applications or modern Kubernetes workloads. Customers should evaluate the breadth of services offered as based on business requirements. Customers can't or should not choose a service provider who doesn't offer breadth of services as it will lead to the creation of a siloed data protection strategy as they adopt various production infrastructure systems.

Encryption: While choosing a service, ensure the service/tool used for BaaS provides encryption for data at rest as well as on the fly. You should have an easy key management solution and follow industry standards like AES for encryption.

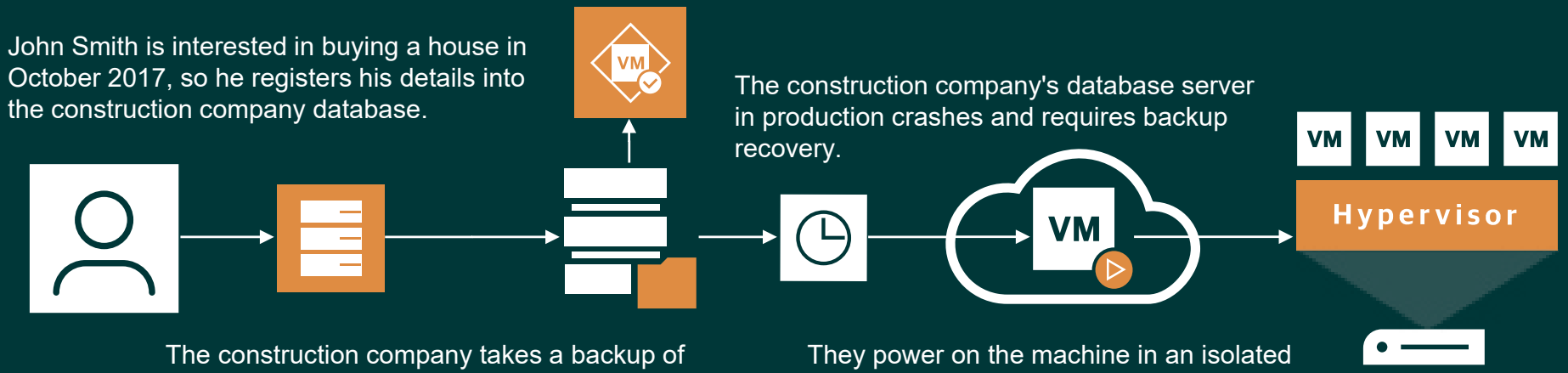
Backup verification: Customers should ensure the backups taken by a service provider are restorable and verified. Customers should get fortnightly/monthly reports and have review meetings for gaps if any. If the service provider has a tool to automate the verification, then that service provider should be preferred over a provider who does this manually.

Ransomware protection: Ransomware is a large threat that has evolved in recent times with the value of ransoms and number of attacks both going up significantly. Security companies have been helping customers with solutions, but the pandemic has opened a lot of gaps with risky behavior by users knowingly or unknowingly. One suggestion here is a data repository that's on immutable storage. But immutability alone is not enough.

Service providers also need to provide value services to customers to ensure recovery, for example, the ability to detect malicious data in repositories, and then scan and clean data with a security scanner before restoring from an immutable repository. Also, service providers should provide a choice to customers to store an air-gapped copy.



Compliance and reporting: Customers should set a desired frequency of reports from service providers on backup completion and verification. Customers should also ask for periodic review meetings to discuss the reports and open issues, if any. Service providers can also provide services for compliant restores as shown in example below.



Recovery: This is most important part when you select a service. Service providers should provide choices to customers for different recovery options, like single file, VM, DB, object, etc. The data should be easily recoverable. Customers should be able to choose which recovery style would be done by the service provider or have a self-service portal to do so.

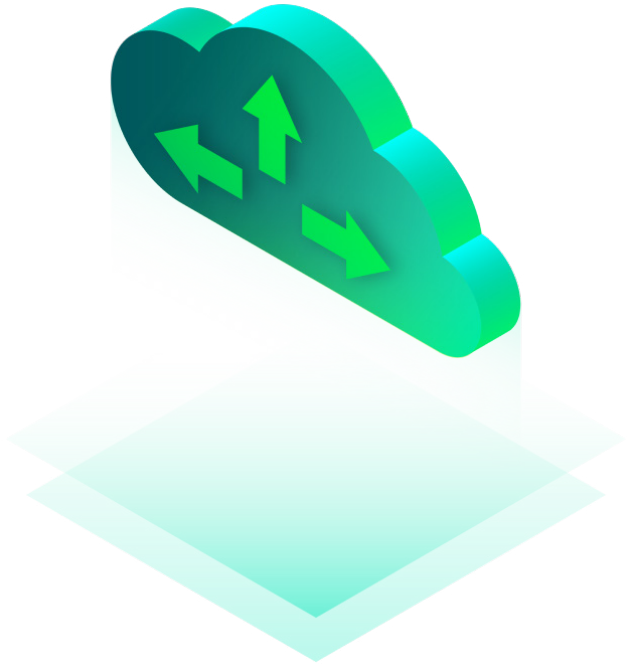
A service provider's recovery process should follow strict approval process to maintain data integrity and ensure data is not falling in the wrong hands. Customers can reduce their downtimes by choosing a service provider who provides **modern instant recovery solutions** or have **stand by infrastructure** to start the production services ASAP and reduce the overall downtime. For example: Let's say a top management executive's laptop crashed for some reason or stolen; then for immediate recovery, we boot the laptop as a virtual machine from backup on a cloud and give access to the top management executive to ensure minimal downtime. Meanwhile, the IT team works on recovering the data on a new laptop/machine.

Above is a normal, average example. Amplify that to an organization's critical data and imagine all the hard work and business disruptions you would have to avoid disaster. Modern day customers have DR solutions in place, but there's a few situations like ransomware attacks where DR sites are also compromised. As stated earlier, backup is a last line of defense.

Cloud mobility: Customers tend to get locked in specific platforms or clouds. Many a times, they would want to leverage a best-suited infrastructure/cloud for a specific business requirement, and that may be better available in another platform. When you choose a service provider, ensure the backup tool used by the provider is capable to restore across platforms, helping you get unlocked, if desired. This will avoid costly migrations and simplify moves between clouds.

Also, customers desire long-term archival of backup data. Service providers should have a capability to deliver the same by tiering to Object or Hyperscaler Cloud Storage and help bring customers' cost of storage down, ensuring the access to data in time of need. This ability to move data between different storage tiers is very important for compliance reasons and helps reduce cost.

Reduce management and TCO: Customers can reduce the management effort of backup infrastructures and also enjoy cloud-like consumption with monthly/quarterly/yearly contracts and billings. The overall TCO reduces drastically with reduction in resources required and management effort outsourced.



A few tips:

- Outsource the backup to a service provider
- Take backups to a local service provider and avoid egress charges
- Archive Backups to Public Cloud for Long Term Retention
- Follow the 3-2-1-1-0 Rule
- Don’t choose tools that lock you in
- Try to have Cross Platform Backups
- Make a Ransomware Recovery Plan

Conclusion

Data loss, and the worry that surrounds it, can be easily avoided by pairing your server, cloud, PaaS and SaaS applications with a complete BaaS backup and recovery solution. Veeam®, along with its **Veeam Cloud & Service Provider (VCSP) program**, provides solutions to customers of all sizes and needs. VCSP partners provide breadth of solutions in BaaS and DRaaS to protect modern workloads along with unmatched flexibility, choice and agility. The services can be tailor made for customers and customized to suit all customer needs and compliances.

About Net3 Technology

Net3 Technology is a leading Cloud Services Provider, headquartered in Greenville, SC. Net3 owns and operates PvDC Cloud, which is located on both the East and West coasts. Nationwide, Net3 provides clients with customized cloud solutions for Backup, Disaster Recovery, and Production. Net3's Cloud Services encompass discovering the right cloud platform for businesses, planning and migration, and day-to-day cloud management for peak performance.

For elite customer service, every client has a dedicated team of Net3 Cloud Engineers. From training to on-boarding, through the length of your contract, Net3 works with each client form a true business partnership to ensure cloud confidence.

Veeam-powered BaaS and DRaaS

Infrastructure Protection

Offsite backup and DR

Public cloud data protection