Backup as a Service

Harbour IT's Backup as a Service solution gives you peace of mind that your data is safe, secure and, most importantly, restorable. The continuous, automated system reduces your valuable time spent on manual and repetitive tasks, allowing your team to focus on core projects.

Minimise your vulnerability to data loss and remove the burden of disk and tape backup management with this secure solution. Your data is protected as it's created, mirrored in the cloud and available to be restored. Your data is encrypted at the source, using a 256-bit AES encryption with a unique key. For an additional layer of protection, the server backup and recovery solution uses the Secure Sockets Layer (SSL) protocol to establish a secure, resilient communication tunnel to the off-site Harbour IT data centres.

Even recovery is automated - simply select the data to recover from a catalogue of archived file versions. The data is then automatically restored to your location. The time you save on backup and recovery lets you focus on more mission-critical projects for your business.

Protect and Recover

Our solution delivers point-in-time recovery of server data through continuous backup, providing nearly 100 recovery points daily.

Continuous backup enables you to choose the exact version of the file to recover from numerous point-in-time versions each day, for vastly improved Recovery Point Objectives (RPO). It also provides built in protection of open files and databases, without complex plug-ins or costly third-party tools.

FULLY AUTOMATED OFFSITE DATA PROTECTION
Speed and reliability in both backup and recovery operations with little or no IT intervention.

CONTINUOUS BACKUP
Minimize data loss with continuos backup and mirrored data centres.

BUILT-IN DE-DUPE
Delta technologies de-duplicate at the source for native, embedded data de-duplication.

OPEN FILE AND DATABASE PROTECTION
No complex plug-ins or costly third-party tools needed.

RELIABLE RECOVERY
Restore is simple through web portal - gives IT personnel point-and-click access to data—at any time, from anywhere.

RAPID BACKUP AND RECOVERY
Speeds recovery by automatically recovering only the data that has changed since your last backup.

SCALABILITY
Protect large servers and environments.

Security in the Cloud

Is the cloud really secure? It is at Harbour IT. We've invested the time and resources into ensuring the physical and virtual security of our cloud service. Our devoted, specialist resources solve and prevent security issues. We offer a transparent solution that ticks all the boxes to lay your mind at rest.

Physical Security

Harbour IT's data centre has been built from the ground up, giving you access to the highest quality facilities with supreme physical security. Security features include security mesh around our cages, biometric readers on all doors, UPS and generator protected power, CCTV recorders and an around-the-clock security team monitoring all physical access. Visitors entering the state-of-the-art facility must pass through a security check point, mantraps and individual biometric fingerprint scanners.

These security features, combined with structural protection against fire, flood, earthquakes, and even terrorist attacks, create a rigidly controlled operating environment that protects valuable customer assets and operations.

Access industry-leading operational expertise, world-class physical security, and a high-performance network ecosystem within Harbour IT's Data Centre.

Network Security

Each client is securely segmented into their own VRF (Virtual Routing and Forwarding). This technology prevents each client from seeing or accessing each other's network. VRF technology also eliminates the problem of clients having the same IP address range as another client.

All clients will have their own dedicated public IP range which enhances public security for services such as VPN connections.

Utilising Cisco firewalling technologies, each client will have their own set of firewall rules which are not shared or impacted by other client configurations. This means firewall configuration and changes are completely independent of other customers. Each customer will be provisioned with one or more VLANs to cater for any internal requirements, these VLANs map back to the individual clients VRF. Private WAN networks and physical hardware can be patched into your VLAN at this level.

Virtual Server Security

VMware is recognised within the industry as the leader in virtual technology platforms. As such, Harbour IT makes use of VMware's vSphere version 4. This offering was specifically built for the cloud.

Each customer's virtual servers will be attached to the network via one or more customer-segmented port groups. Each port group ties the servers into the customer allocated VLANs created as part of the cloud network security per customer.

Data Security

Each customer's Virtual Servers have their own VMDK (Virtual Machine Disk) which is a file that represents the drives created as part of the virtual server. This virtual disk contains the server's operating system, and associated data drives. The virtual server operating system has no visibility of SAN storage or other VMDK's existing in the environment.

All of Harbour IT Cloud SAN storage connectivity is IP based, which helps to alleviate security implications associated with other methods of attachment.

Our Partners

HARBOUR IT

Infrastructure & Networking
Infrastructure Design
Virtualisation
Integration
Security Review
Procurement

Managed Services
Infrastructure Monitoring
Infrastructure Managment
Security Managment
24x7 Help Desk

Cloud Computing
Infrastructure as a Service
Software as a Service
Back Up as a Service
Disaster Recovery
Desktop As A Service

Resourcing
Project Management
IT Consultants
Contractors
Training

www.harbourit.com.au
enquiries@harbourit.com.au