DISASTER PROOF STORAGE FOR DISTRIBUTED IT ENVIRONMENTS

As the needs of businesses change, as do the needs of employees tasked with growing business in current fast-paced environments. Once confined to single locations due to technological constraints, modern businesses are increasingly spreading out by taking advantage of tools, which make it easy to work remotely or set up satellite offices that are just as efficient as corporate headquarters. While this flexibility enables new gains in productivity, it also leads to dangerous inconsistencies and compromises in terms of information security, data management, and backup. Distributed IT environments have unique challenges that must be addressed. The modern mobile, or remote office requires a multitude of storage features in order to be convenient and effective for remote employees conducting business.
For distributed IT environments ioSafe recommends a multilayered data redundancy approach, combining the proprietary fireproof and waterproof hardware with advanced software options for backup, replication and mobile access.

CHALLENGES OF DISTRIBUTED IT ENVIRONMENTS

For IT organizations, serving, storing, and backing up data at a single location can prove difficult; however with multiple locations in a distributed environment this task proves to be much more difficult. In order to understand how to overcome the issues plaguing data management in a distributed IT environment; we must better understand why the issues exist in the first place. To better comprehend how ioSafe network attached storage can help to address these data management issues in distributed IT environments, it is wise to first understand why these issues exist.

Business Continuity and Disaster Recovery
Data distributed outside of the primary corporate network may not receive all of the advan-

tages of the data housed inside of the corporate infrastructure. Due to lack of competent remote IT staff, or power and cooling options, it is less likely that data residing in small branch offices or home offices is protected with hardware redundancies such as RAID, clustering or advanced firewalls. It is also unlikely that remote data is protected with software features such as snapshots, redundant virtual machines or enterprise backup applications. These limitations represent difficult problems for centralized IT wishing to ensure business continuity and data redundancy for employees residing in distributed offices. By standardizing on common practices and utilizing the appropriate hardware and software, corporate organizations can minimize the impact of site disasters and data loss at all endpoints

Branch Offices or Home Offices

Branch offices may be in commercial office spaces far removed from corporate headquarters, providing remote employees with closer alternatives for easier commutes and face-to-face meetings with clients. The commercial business spaces typically include a more reliable class of Internet and phone service and provide employees with a professional environment to conduct business. Home offices, on the other hand provide users with residential grade Internet and phone services and may not include enough bandwidth to reliably run all applications. However, it is up to the corporate IT staff to come up with solutions, which fit all employees down to the lowest common denominator when it comes to access and reliability.

Mobile Employees

The modern workforce is becoming increasingly decentralized and mobile. These employees are not necessarily associated with centralized offices and must be free to access data from anywhere, in real-time. The necessity of this instant communication overrules the strict IT regulations of yesteryear. However the importance of security and data protection still remains paramount. IT organizations are now faced with coming up with mobility solutions or potentially fall prey serious data security and compliance issues from employees using unapproved file sharing software and public cloud services.

Cloud Services

Cloud based software or storage services have become a simple way to add enterprise applications and storage without the need for enterprise class hardware deployments at remote or branch offices. Cloud services are added using an on demand model with the ability to instantly provision storage or add software features on the fly. Cloud also provides enterprise class backup and disaster recovery services without the need for any additional hardware or service contracts.

Scalability

Storage scalability in a distributed IT environment is more about meeting the needs of the individual offices and employees than providing a monolithic storage resource remotely available for all. The needs of distributed businesses today require that storage be distributed to meet the needs of users at each site and maintain security across the entire network without sacrificing features such as provisioning and compatibility with all devices. In some environments where compliance is paramount, storage systems must be able to scale along with the rapid growth of data, and be available for retrieval for years, or potentially decades.

Data Archiving

Archiving systems of old, were meant for nothing but long-term, unchanging data, reserved for the most devastating circumstances. These systems are often composed of antiquated technologies such as tape or optical media hardware. They are also never meant for business continuity, but instead for emergency recovery. These older technologies have the result of creating small data silos, which are restricted to slow restore times in the exchange for long shelf life. This type of long-term data

retention requires many resources, as well as time, to maintain and recover data. Modern, distributed businesses require that archival data be readily accessible and rapidly recoverable, all while ensuring security throughout the process.

THE IOSAFE SOLUTION

ioSafe manufactures disaster tolerant storage products, which are easily integrated into the distributed office environment. From the USB 3 direct-attached Solo G3 to protect and backup workstations, to the SoloPRO which protects server data, and finally the Network Attached Storage (NAS) systems which are perfect for file sharing, data backup and disaster recovery at small or remote office locations. Local or remote administrators can build a robust, on-site disaster recovery solution by combining the ioSafe disaster-proof storage.

ioSafe 1019+

The ioSafe 1019+ is the most robust network aUached storage server available. With fireproof and waterproof data protection, the 1019+ can withstand devastating conditions, which would otherwise destroy other local storage arrays. Powered by the Synology® DSM operating system, ioSafe NAS includes RAID, replication, high availability, backup, and additional software features which improve security and provide mobile access for all users.

With a minimal footprint, ioSafe NAS is manageable both locally and remotely by corporate IT staff. This allows for nimble troubleshooting and configuration in the event a remote connection is down or remote staff is unavailable. The user interface is equivalent when viewing from a local workstation as well as remote devices. The NAS units support the needs of the local staff while being compliant with corporate security. Local disaster recovery is absolutely necessary for the remote office. In the event an Internet connection is compromised, the local IT team must be able to recover from backups without the aid of the cloud, or corporate servers to move data back onsite.

With the built-in Cloud Station software, ioSafe NAS can replicate and/or sync for both disaster recovery and remote access. Remote employees can access private cloud data away from the office. Remote users of Cloud Station have the ability to open, edit and save files remotely from iOS or Android mobile devices and laptops. Cloud station is an easy way to create a corporate private cloud and keep data secure, without being exposed to public cloud networks. Using Cloud Station for remote replication to another ioSafe NAS or Windows, Mac or Linux Server creates a fully redundant target at an off-site location for near-instant file recovery.

ioSafe 1019+ NAS systems are scalable by adding or replacing hard drives within the chassis, or by adding a 5-drive expansion chassis. The Synology Hybrid RAID feature makes expansion easy, with the ability to mix and match hard drives of different sizes to maximize both storage capacity and data protection.

When archiving data for long term access, administrators can combine ioSafe network attached storage with ioSafe USB attached options such as the SoloPRO hard drive. By scheduling regular, automatic backups, this creates another level of redundancy by copying data to an external, fireproof and waterproof portable enclosure. ioSafe also supports other external media such as RDX and USB attached ioSafe hard drives for simple, removable archiving for shipping data to an off-site, long-term archival sites.

For administrators who need the peace of mind that their data is backed up and highly available, the ioSafe 1019+ can be set up to run in an active-passive cluster with an adjacent unit, creating a system which will automatically failover in the event of a hardware or software catastrophe.

By combining all of the redundant software and hardware features, administrators can create the most robust and resilient shared storage array available. ioSafe storage combines the best in data protection with a feature-rich operating system protecting the most vulnerable environments from data loss, while allowing distributed offices to manage and access crucial data from anywhere.