

## TeraCenter IT Guardian Services Overview

### **Introduction**

TeraCenter's data vaulting service is a highly scalable, off-site digital backup and archiving service designed for cost-effective, data backup and disaster recovery service. TeraCenter provides the IT Guardian server appliance, installed at the client's premise, where data is centrally stored. Dedicated backup processes from other servers and/or local users can save data directly to the IT Guardian. All data residing on the IT Guardian is then backed-up, off-site, to TeraCenter's secured facility on a scheduled basis in a highly efficient and secure manner.

TeraCenter's IT Guardian and the supporting network architecture is founded on a simple to use and managed best practices model. TeraCenter maintains confidence and security for their clients through technologies such as PKI infrastructure, AES encrypted connections, and chain-of-authority validation for accessing client's data. TeraCenter's services provide organizations with turnkey backup and disaster recovery solutions, along with first-class service and support. With TeraCenter's solutions, these organizations can avoid initial capital investment and costs associated with software, hardware, maintenance, training and administration. Additionally, TeraCenter's clients enjoy free upgrades, hardware replacement, and only pay for what they use.

TeraCenter's IT-Guardian can be used for dedicated "Disk to Disk to Offsite" backup and also for storage of production data. This allows clients to secure complete backups from existing servers and direct-stored data such as documents, spreadsheets and images.

All data stored locally on the IT Guardian's RAID-based storage array(s) are backed-up off-site to TeraCenter's secured datacenter facility using 'block-level' replication of local data and transferred using AES-based encryption. TeraCenter uses a multi-tiered architecture for archive rotation and maintains all data on active spinning-disks, versus tape.

### **TeraCenter's Backup Process**

#### Storing data on the IT Guardian

The IT Guardian appears a NAS device to the clients network. Data may be stored by connecting via CIFS or NFS protocols. TeraCenter recommends using proven backup or replication utilities designed to efficiently replicate data across existing LAN connections to the IT Guardian. Client specific needs should be evaluated when considering the replication schedule, application-agents, data/file types, data quantity and server resources.

## Securing the connection

In order to maintain the confidentiality of client data, TeraCenter takes multiple steps to ensure that data communications are secure between the IT Guardian (located at the client's facility) and TeraCenter's off-site facilities (DataCenter). The following are a series of requirements and/or transactions that must occur.

TeraCenter IT Guardian maintains an independent stateful firewall (in addition to client maintained network security), which is secured for both LAN and WAN interfaces utilizing network, protocol and port inspection. All management access to the IT Guardian MUST come from restricted addresses within TeraCenter's Datacenter Facility or direct serial-console.

At the scheduled time(s), a connection is initiated from the IT Guardian to one of TeraCenter's backup servers via a backup-gateway. At this point, host validation is performed utilizing 2048 bit key-pair, unique to each IT Guardian (as a host). Additionally, an account-based authentication is performed to access and connect to a change-rooted environment within a second tier backup server. This authentication uses an additional and unique 2048 bit key exchange to authenticate the access. Once host and account level access has been authenticated, a SSL connection is established using 128 bit AES encryption to secure the application level backup process.

## Performing backups

TeraCenter's backup process utilizes a highly efficient comparison methodology, which allows file systems between the IT Guardian, and its backup host/server to be synchronized with minimal data transfer during normal operation. File systems on both sides are compared using file attributes and binary checksums to compare and confirm any changes that have occurred on the IT Guardian. Once the comparison operation is completed, block-level differentials of the changed file system are replicated to the backup server to create a complete offsite mirror of the client's data.

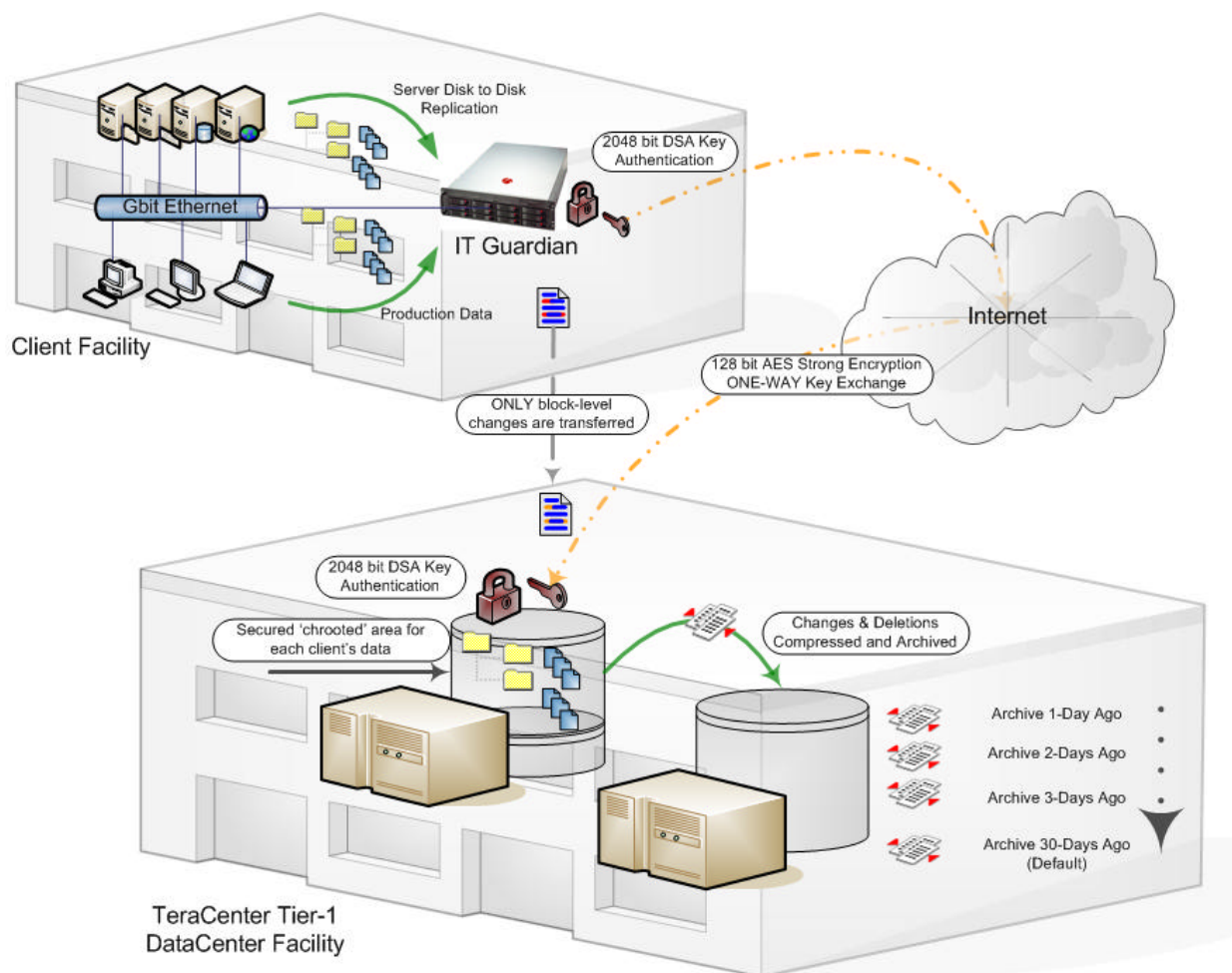
## Data updates, deletions and additions

During the backup process described above, files will have been added, changed and/or deleted. New files that have been added will simply reside on the off-site backup. However, changes and deletions to data need to be captured, and are stored/shifted to an alternate location which will create an archive and log of all data that was modified since the prior backup. These files are saved, compressed and transferred to TeraCenter's archive servers for longer-term retention. TeraCenter maintains a minimum of 30 days worth of changes by default. Longer retention of data is available based on client needs.

## Completion and reporting

Upon completion of the backup process, several auditable records exist for confirmation and/or discovery of any additions, changes or deletions of data. Each backup that occurs creates and maintains a log of all files transferred or deleted both on the IT Guardian and the off-site backup servers. Secondary logs are generated during the archive process, which record all files that were changed and/or deleted during the archive process and also as a record of all files stored within a particular archive.

## TeraCenter IT Guardian Data Replication Process



### Network and system monitoring

In addition to monitoring of backup and archiving processes, TeraCenter also monitors all key aspects of the IT Guardian on a daily basis. Statistics are gathered and graphed to provide analysis and trending data for: disk usage, system load, memory usage, raid-array/drive status, bandwidth utilization and other performance metrics. This enables TeraCenter to discover issues and anticipate requirements for future growth of data.

### Datacenter facilities

TeraCenter's primary datacenter is located in San Diego, California within a zone-4, structurally reinforced and secured CLEC facility. This facility is equipped with multi-tiered redundancy and security, including: BGP-routing, power and battery-backed power supplies, temperature and humidity controls, fire suppression systems, 24x7 onsite security guards, motion detectors, security cameras, individually locking cabinets and cages and area-specific card-key access.