TapeTrack Security

The purpose of this section is to outline the measures we take to ensure that your use of TapeTrack in no way compromises the integrity of your information management environment; in fact our objective is to ensure that TapeTrack is always available to provide the information that you require to recover your other systems, should the needs arise.

TapeTrack is used by enterprises all over the world, including jurisdictions with high levels of compliance and security constraints such as Israel and the United States. These enterprises range from government through to private and publicly listed companies.

GazillaByte Employees

All GazillaByte staff are subject to a criminal background check and understand that any criminal conviction will result in an immediate termination of their employment.

In addition to this, many of our employees have worked in military and law enforcement roles and have obtained the required clearances to perform these functions.

Design Methodology

Security and reliability are our primary considerations when developing and maintaining TapeTrack. Our changes are extensively beta tested by experts who use the product on a daily basis.

TapeTrack is built upon an Application Programming Interface (API) written in C. This API is available for Windows, Linux, AIX, Solaris, HPUX and z/OS. Through the use of this API, all inquiries and updates to TapeTrack must occur via our API.

In addition to this protection, it is also possible to lock and encrypt the TapeTrack database so that updates may only occur via our software.

To eliminate the chance of buffer overflow exploitation, all records that are managed internally, stored on disk and sent via TCP/IP have a fixed length.

To minimize the chances of third-party components creating exploit opportunities we do not use middle-ware and only use third-party components when they provide the source code.

License Agreement

The TapeTrack End User License Agreement (EULA) was written in consultation with our customers. The EULA clearly and fairly outlines your rights as a Licensee of our product.

SOURCE CODE ESCROW

The TapeTrack source code is regularly deposited for escrow with EscrowTech in Salt Lake City and The NCC Group in London. As a TapeTrack Licensee, our License Agreement ensures your right to register as an Escrow Beneficiary. This protects your rights as a Licensee should a dispute arise around your use of our intellectual property.

DIGITAL CODE SIGNING

All TapeTrack executable code for the Microsoft Windows platform is Digitally Signed with GazillaByte LLC's Code Signing Certificate. Where we provide third-party DLL's and executables, these will either be signed with the owner's Digital Certificate, or in the absence of a signature, signed with GazillaByte LLC's certificate.

THE TAPETRACK PROTOCOL

TapeTrack uses a proprietary TCP/IP protocol. This protocol uses only one port (usually 5000), but can also be tunneled through a HTTPS proxy server (TapeTrack clients use an outbound connection and the server accepts inbound connections).

ENCRYPTION

TapeTrack uses symmetric AES encryption to encrypt data and all passwords are hashed and stored using the MD5 algorithm.

ACCESS CONTROL

TapeTrack has its own native access control mechanism. This access control is independent of Active Directory1 to ensure that in the event of a disaster recovery there is no dependence between TapeTrack and systems which may need to be recovered. TapeTrack's native access control mechanism can limit access to TapeTrack and TapeTrack resources based upon: 1. The connecting interface. 2. The connecting IP Address or IP Sub-Net. 3. The User's access rights to individual resources and functions.

HIGH AVAILABILITY

TapeTrack's High Availability Option provides one or more read-only TapeTrack systems which replicate with the primary system in real-time. This replication requires no supporting middleware and uses very little bandwidth.

SIMPLE HOT BACKUP

In addition to High Availability Replication, the TapeTrack database can be simply backed up using a supplied command line utility even when the system is active.