



Tape Backup Encryption: Hardware versus Software

SOFTWARE

Q3 HARDWARE

Software solutions are usually only available for limited operating system.

The Q³ family of encryption products are designed to work across a full range of operating systems as they appear transparent to the OS.

With software you are usually restricted to those specific backup packages that may have encryption as an option. If you change packages or implement as a server not covered by the package your security policies are exposed.

The Q³ family works with all major backup packages as well as with standards such as TAR, CPIO etc.

Changes to software require changes to operational procedures and may require extra operator training.

Q³ has no impact on the way the backups, restores or archives take place so need no changes to the procedures.

Tape drives use compression to get high speed data transfer, but when data is encrypted it can no longer compress. The results are slower speeds and potentially additional data cartridges will be used.

The Q³ family has built in pre-compression before encryption thus keeping the data transfer speeds high.

Software has to rely on the system processor to do the encryption so will have an impact on other processes running at this time including the actual backup process.

The Q³ family have two dedicated encryption engines and therefore have no impact on the system processor when encryption/decryption is in use.

Software that does offer compression at the system requires power from the processor to perform this function so the throughput is not predictable and can be very slow so negating the advantage.

The Q³ family use dedicated compression chips rated at 80 Mb/sec so do not impact on the speed of throughput

With software solutions the encryption software must be installed and configured on the system before a restore can be performed.

The Q³ family need no changes to the system so the restore of a bare bones system is no more complex than with a system not using encryption.

The key for the encryption key is retained in the system when using a software solution and hence open to attack.

The Q³ family has the key held internally and this cannot be extracted. The only connection to the Q³ unit excepting the SCSI or Fibre Channel connections is via a serial connection that can be left disconnected once the key is installed.

Software normally only offers a single key that is kept in the system and provides only single-factor security.

The Q³ family has dual soft keys entered by the user along with the hard key unique to the specific customer offering two-factor authentication.

Software encryption usually needs to be upgraded (i.e. purchased again) when the OS or backup software is upgraded.

Hardware such as the Q³ is system independent does not need to be changed when the OS, backup software or even the host system is changed (i.e. no cost).

Software costs are often based on the capacity of the attached library, if the library is upgraded to add extra tape slots then you also need to pay an extra licence for the encryption software "upgrade".

Hardware costs are fixed, whatever the number of slots in the library or amount of data to be protected.

With software you are simply buying a licence to use it, you never actually own anything.

When you buy a Q³ unit you own it and as a capital cost it can be set against tax in many cases.

Software normally involves several updates during the life of the system.

Hardware does not change even if the complete system or OS is changed.

With software anyone who knows the user key could restore the tape if they have moved on to another company.

Q³ uses a mixture of the user key and a hardware key unique to the customer. Even with another Q³ unit and knowing the user key they cannot restore the tape.

If you change the system or OS in use you will need to copy all that data to the new system so that it can then be encrypted under the new software or keep the old system live in order to restore old archives and tapes.

As the Q³ family can move across systems it will still decrypt the data when connected to the new system. As long as the clear data format can be read on the new system then there is no need to copy tapes.

Q3 HARDWARE