WHITE PAPER

Defending Data Against Ransomware

Best Practices for the Worst-Case Scenario

Quantum

CONTENTS

INTRODUCTION

Ransomware has become big business, and every organization is a potential target. One estimate projects that global losses from ransomware will top $20 billion in 2021 alone. The number of attacks and size of the ransom demanded are on the rise too[1], with the FBI reporting that losses from ransomware in the US increased 225% in 2020. The impacts on businesses are real, with research indicating 66% of attacked organizations suffered significant revenue loss, 53% suffered reputational damage to their brand, and 29% were forced to eliminate jobs in the wake of an attack.

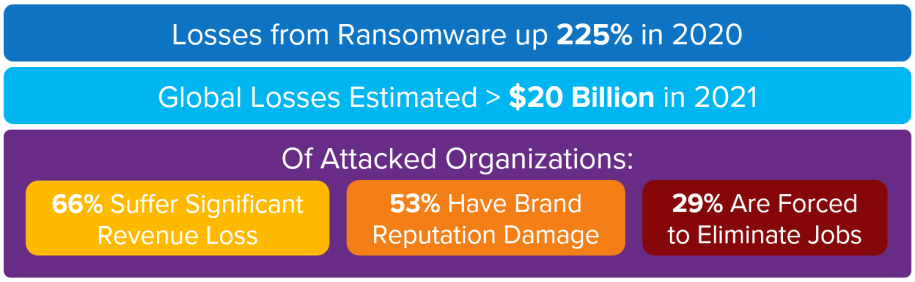

Figure 1 - Ransomware Statistics

There are many tools available to make it harder for ransomware to gain entry, but the biggest vulnerability in any data center is one that can never be patched: human nature. The primary attack vector for ransomware is social engineering, which takes advantage of human nature to get malicious code into the target network. Educating employees can reduce risk, but not eliminate it.

The unfortunate truth is that IT professionals must plan for the day when ransomware gets in. This means protecting vital data so that it can be recovered without paying the ransom. There are various ways to meet this objective, but this paper will highlight the use of LTO tape – including unique features found only in Quantum Scalar® libraries – to provide the necessary protection. Useful tips for preventing ransomware from gaining entry are published by the US government's Cybersecurity & Infrastructure Security Agency (CISA), here.

WORST-CASE SCENARIO PROTECTION

Ransomware works by encrypting data. Protecting files against ransomware, then, means making them inaccessible to ransomware, or if they are accessible, ensuring that they are immutable. Disconnecting all your storage and locking it in a safe is clearly not practical, so what this really means is making a copy of the data inaccessible or immutable. In case of ransomware attack, this copy is used to recover. The frequency with which copies are made and where and how they are stored is important and will be discussed later.

It's valuable to calibrate your assumptions about both potential attackers and your protection strategy. These attacks aren't perpetrated by an individual in a black hoodie. They are the business focus of extremely sophisticated and well-funded criminal organizations. They may spend months capturing keystrokes and recording administrator passwords before launching an attack. They have the skills to compromise your backups, and gain root access to the nodes of your object storage system. Not even your cloud accounts are safe. Unfortunately, the only thing you can reasonably count on is that the attackers will not have physical access to your data storage. Ransomware, and cybercrime in general, is almost always perpetrated remotely.

[1] *https://www.paloaltonetworks.com/resources/research/unit42-ransomware-threat-report-2021*

Offline Data is Safe Data

A conservative approach is to assume that anything and everything connected in any way to the network is potentially hackable. Even systems designed to store data immutably by design may be vulnerable if the underlying operating system is compromised.

The only way to keep a copy of data completely safe from ransomware is to provide a physical barrier to its access that a remote attacker cannot overcome. The classic physical barrier is often referred to as an "air gap." The term was originally used with respect to network security, where an air-gapped system is one not connected to any outside networks. It can also be applied to data storage, where it refers to storage that is not connected to a network or networked system. In other words, offline.

The key with an offline copy is that it can't be accessed without a person first doing something to put it online. Tapes or other removable media sitting on a shelf are classic examples.

The Role of Software-Based Locking

A range of technologies are available that promise to make HDD or SSD-resident data immutable, usually by putting software-enforced time-based "locks" on stored files or objects. This works if all access attempts are through expected channels, but if the storage system or locking software itself is hacked or exploited all bets are off. Even though it isn't perfect, time-based file and object locking technology is valuable for reducing the chances that an attack will be successful – but it's not enough. An offline copy is still required.

What About Hardware-Based WORM?

Hardware-based Write-Once, Read Many (WORM) technologies make it impossible to erase or overwrite data once written. This provides an additional layer of protection that can be useful. Hardware-based WORM technology is available in both optical storage media and tape, both using special media.

WORM optical relies on physical changes that happen to the media at the time of writing and cannot be reversed. With LTO WORM tape, the physical tape media in the cartridge is identical to that in non-WORM cartridges, but differences in the factory-recorded servo tracks and cartridge memory work with the tape drive firmware to enforce WORM. It might be theoretically possible to override all the inbuilt protections and erase or overwrite an LTO WORM cartridge, but it would require deep knowledge of the system and at minimum the ability to write custom tape drive microcode. Cyber-criminals will never take the time to do this, as softer targets are always available. LTO WORM is extremely secure.

WHY TAPE?

Because it has been around for so long, it's tempting to dismiss magnetic tape as obsolete. But the tape of today is as different from the tape of 1951 as a Tesla is from a Studebaker. There are other options with their own pros and cons, but tape has the best combination of characteristics for offline data storage. Let's examine the options.

	Portable HDD	Optical	Tape
Intuitive/Convenient			
Cost $/TB			
Stability over Time			
Scalable/Automatable			
Hardware WORM			
Hardware Encryption			
Performance			
Density			

Table 1 - Offline Media Characteristics

Portable HDD / SSD

In terms of "easy" offline storage, it's hard to beat the USB hard drive, at least at a conceptual level. Copy your data to it, unplug it and put it on the shelf, and sleep soundly. Your data is protected from ransomware. It's true, this is a great and simple solution, provided you're a typical individual. But it's an expensive solution in terms of $/TB and it doesn't scale. SSDs have the same challenges, and cost even more. For all but the smallest organizations, other options are needed.

Optical Storage

Recordable DVDs and Blu-Ray discs are another option that at first glance appears attractive, and like portable hard drives are a comfortingly familiar form factor. Optical media can offer much higher stability over time compared to HDD storage, depending on the media composition. Density can be reasonable, with capacities up to 128 GB for Blu-Ray, and the lower-capacity media is affordable. WORM media is available for making immutable copies. But optical recording is very slow, and not any less expensive than portable HDD. High-density media is commonly only rated for 4x, or 17 MB/s. If you have many TB to write or fast retrieval is a requirement, the slow speed is a deal-breaker. At best it might be suitable for creating an archival copy of unchanging data that must be kept for many decades.

Tape

Then there's good old magnetic tape. Modern LTO tape has unmatched streaming performance - up to 1000 MB/s for LTO-9 - and higher density, up to 45 TB in a single cartridge (also LTO-9, with 2.5:1 compression). Worst case, if the data isn't compressible at all, a cartridge holds 18 TB, in less space than a portable HDD. Reliability is unmatched, with an unrecoverable bit error rate of $1x10^{19}$, which is four orders of magnitude better than disk. Let that sink in. Ten-thousand times better than disk, which is already very reliable. Stability over time is very good also, with cartridges being readable for 15-30 years. Optional LTO features like WORM and hardware-based encryption provide additional levels of security. Finally, tape is the lowest-cost medium, with ESG calculating that the ten-year total cost of ownership for an LTO-8 solution is 86% lower than an all-disk solution, and 66% lower than an all-cloud solution.

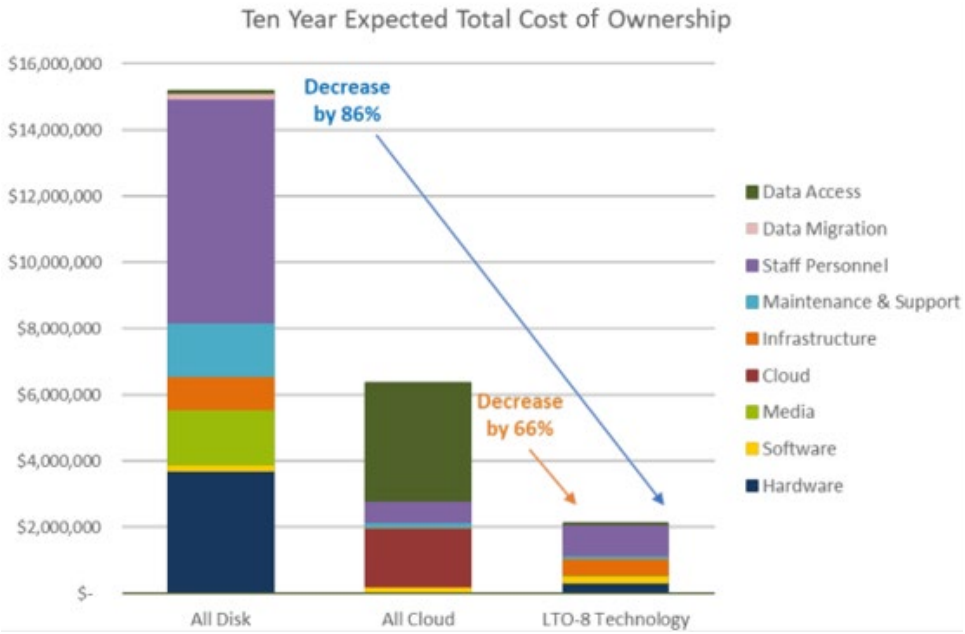

Figure 2 - Ten Year TCO Comparison

Like time-based file and object locking, WORM tape can play a part in a ransomware protection strategy, but it must be used judiciously. Commonly tape cartridges used for backups are rewritten multiple times, further lowering the cost of ownership. WORM cartridges by their nature may only be written once. Due to their lower sales volumes, LTO WORM cartridges are also more expensive than regular LTO, compounding the financial effects of their non-reusability. The best place to leverage LTO WORM is for archival data that will never change, or for an immutable "checkpoint" backup every now and then.

With all its benefits, tape isn't perfect. It's not suitable for heavy random access, the cartridges must be stored under controlled conditions, and like any removable media, handling tapes can be inconvenient and error prone. But unlike the downsides of the other media discussed above, these disadvantages are minor and easily managed. Keeping tapes inside a robotic tape library in a climate-controlled datacenter eliminates concerns about handling and storage conditions, and backup and archive are not random-access use cases. There is no question that tape possesses the best combination of characteristics for offline storage.

THE MEANING OF OFFLINE TAPE

"Offline" is usually thought of as a binary condition, with "online" being the opposite state. This was the case when a physical switch controlled the state of a peripheral, but software has made things more interesting. Applied to tape, a cartridge resident in a tape drive controlled by an application is clearly online. A cartridge on a shelf is clearly offline. A cartridge in a tape library, however, lies somewhere in-between fully online and fully offline.

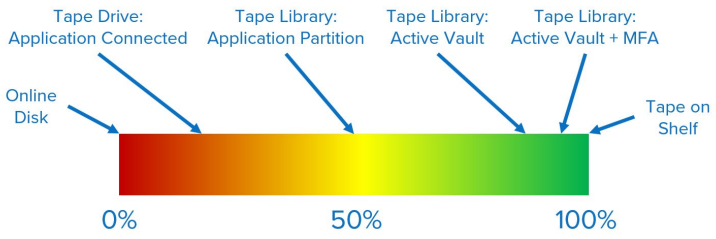

Figure 3 - Tape: Resistance to Remote Attack

The degree of "offline-ness" correlates directly with the resistance to remote attack. Even tapes in an application-connected tape drive are a bit safer than data on disk, as more knowledge is required to access them. Tapes on a shelf are completely protected from ransomware and other remote attacks. Tapes in a robotic tape library that reside in an application partition are moderately secure, but a sophisticated attacker with knowledge of backup systems could co-opt the backup or archive application to erase, overwrite, or encrypt the data on tape.

Quantum Scalar libraries have an industry-unique partition type known as Active Vault. Tapes that reside in an Active Vault partition are extremely safe, as the application can't see or access them, and the partition cannot be connected to the network. Before the tapes can be used, an administrator must move them back into the application partition using the library GUI. To compromise data on tapes stored in an Active Vault partition, a remote attacker needs knowledge of the environment and the ability to compromise a library administrator account. The use of two-factor authentication on admin accounts makes this extremely unlikely. For all the details on Active Vault, download the full Tech Brief.

BEST PRACTICES

Every organization is different. Different exposure to cyberattack, different risk tolerance for data loss, different consequences of a successful attack. It makes sense, therefore, that there is no one single approach that fits all. There are, however, some general best practices that can help anyone build a protection strategy that works for their organization.

Understand the Real Requirements

Before a ransomware protection strategy can be constructed, everyone needs to agree on what is at stake. This is the old recovery time objective / recovery point objective (RTO/RPO) conversation. Put bluntly, how long can you afford to take for recovery, and how much data can you afford to lose? This is a business discussion more than an IT discussion, and the answers will be different for different systems in the same organization. An e-commerce platform that records thousands of dollars of transactions per second will have different requirements than the marketing department shared folders. Data classification is critical to understand the business risks and protection needs of each system.

When talking about ransomware protection, the concepts are the same as with other types of disaster recovery (DR). It's all about probabilities and money. The idea is to mitigate the perceived risks to the maximum extent, without spending more than necessary.

Layer Your Defenses

The best defense isn't comprised of a single technique or technology, it's based on layering several different, complementary approaches together. The objective is to make it difficult for an attacker to get in and limit the potential damage if they succeed. Although not the topic of this paper, prevention is key, and ransomware prevention involves many layers. The most important is training and education to raise awareness, sensitizing the people in the organization to the threat and potential consequences of an attack.

Protecting your data against the worst case should also involve multiple layers. Not all attacks will have the same level of sophistication, and it's important to be able to recover as quickly as possible. If you are the victim of a very basic attack, you might be able to roll back a few snapshots and be in business. A slightly more complex attack might require you to recover data from backups stored on a deduplication appliance. If your backup systems are compromised, the copy stored with file lock or object lock technology might still be OK. If all else fails, your offline copy will get your organization back on its feet, but recovery could take longer than online methods and the most recent data might not be protected.

Use the Available Tools

Deploying new hardware and software takes time. Administrators and system architects are overloaded, and it's common to deploy new technology quickly in a "just get it running" way, while planning to come back later and tune it up or make it better. Due to the demands of the job that day often never comes. This is a missed opportunity, and when it comes to security, it's dangerous.

Understand the security tools available in the hardware, software, and cloud products you deploy, and make the most of them. This holds true for secondary storage systems too, like tape libraries. For example, is two-factor authentication an option? If so, use it. Is role-based authentication available for a product? Use it and the principle of least privilege to configure user and administrator accounts. Read user manuals and release notes to stay abreast of the security features available as products evolve and take advantage of the tools that make sense for your situation.

Once cybercrime actors are inside your network, they will try to move laterally and gain a more complete picture of your systems and data. Using all the security tools available will slow down lateral movement and buy more time to detect, react to, and repel threats.

Keep a Copy of Last Resort

It's a sobering thought, but you must prepare for the day ransomware is unleashed on your networks. If all your prevention efforts have failed, all your defenses have been outmaneuvered, and your backup systems and cloud accounts have been compromised, what will you do? Having a truly offline copy of each data set, as up to date as necessary (as defined during data classification and the RTO/RPO discussions), is your safety net. Having a copy of last resort can be the difference between staying in business or not, or between inconveniencing your customers and being sued by them.

Retention time of offline copies is also important. Sophisticated attackers will bide their time, sometimes for months, while exploring your networks. They will try to incrementally erode your defenses without your knowledge, or plant virtual time bombs. Restoring backups that contain malware only wastes time. Having a long retention – months to years - for at least some of your offline copies maximizes the chances that you will be able to recover unpolluted data when it counts.

Levels of Protection

As discussed throughout this document, various levels of protection are available using different storage technologies. Table 3 below summarizes the most common options. This view is necessarily simplified and does not account for differences between specific vendor implementations.

Technology	Protection	Cost	Recovery Speed
Replication	Low	$$$$	High
Snapshots	Medium	$$	High
Write-Protected Snapshots	Medium High	$$	High
Backup to Disk / Deduplication Appliance	Medium	$$$	Medium
Write-Protected b/u to Disk / Dedupe Appliance	Medium High	$$$	Medium
Backup to WORM Disk or Object Storage	High	$$ to $$$$	Medium High
Offline Tape in Active Vault Partition	Very High	$	Medium Low
Copy to WORM Tape	Ultimate	$ to $$$[2]	Medium Low
100% Offline - Tape on Shelf	Ultimate	$	Low

Table 2 - Levels of Protection Against Ransomware

Every organization should already have several of these protection methods in place for standard backup and DR purposes, even before any discussion of ransomware protection. That's good news, because it means that with potentially a single change or addition, ransomware protection may be added or enhanced.

[2] Since WORM tape media cannot be re-used, cost depends on frequency of use and rate of change of data

When adding additional layers of protection, calibrate the RPO to the risk and business requirements. Do this for each data set. Keep in mind that RPO in this case defines the amount of data you are willing to lose to a ransomware attack. This could mean writing a copy of data to tape as infrequently as once per month, or as frequently as once per day.

For example, if you have a critical application with an RPO of less than one day, it would be prudent to make a copy to tape daily and retain that copy for at least a few months. After a few months, keep one copy per week for 6 months to a year. This ensures that if you discover malware has been lying dormant in your backups, you can still recover with reasonable granularity.

With multiple layers of protection, laddering RPOs is an option. For example, write-protected snapshots on primary storage may occur once per hour and be kept for 3 months, with offline tape copies made once per week and kept for one year. Just be sure that your copy of last resort – your offline copy – is current enough so that the business consequences of a loss of that duration are manageable.

Example 1:

Current Situation: Using Snapshots, Replication, and deduplication appliances (such as Quantum DXi®) for backup and DR protection.

Ransomware Protection Enhancements: Add frequent write-protected snapshots on primary storage, or on backup storage using the secure snapshot capability of Quantum DXi backup appliances. Install a Quantum Scalar tape library with Active Vault. If Quantum DXi appliances are in use, the tape library may be integrated with the DXi to produce tape copies without putting additional load on the backup servers, with most applications. Choose the frequency of write-protected snapshots and Active Vault tape copies to meet the business RPO.

Result: Two additional layers of ransomware protection.

Example 2:

Current Situation: Primary backups to a deduplication appliance. Copying some data to time-locked object storage (such as ActiveScale™ Object Lock) for compliance.

Ransomware Protection Enhancements: Back up all data periodically to time-locked object storage, not just data sets subject to compliance requirements. Expand object storage system as needed. Add a small Scalar tape library. Regularly back up all data to LTO tape, export tapes from the library, store on a shelf in the data center.

Result: Expanded ransomware protection for all data, including a totally secure copy of last resort.

Example 3:

Current Situation: Snapshots on primary storage to protect against user error. Primary backups to a Quantum DXi deduplication appliance with monthly copies to a Scalar tape library. Long-term retention and compliance requirements for some data.

Ransomware Protection Enhancements: Enable DXi secure snapshots for all backups. Expand Scalar tape library. Write full backups weekly to LTO WORM cartridges, keeping one month's worth in the library, export the remainder and store in the vault.

Result: Multiple layers of ransomware protection, plus WORM storage that may be used to meet regulatory compliance needs.

THE MOST SECURE TAPE LIBRARIES

Tape libraries, like any data storage system, need to be secure. Considering that a tape library can easily hold multiple PB of data, and may hold irreplaceable data with long-term value, it's puzzling that most on the market offer only the most basic security features. Quantum understands the value of backup and archive data and is continually improving the security of the Scalar line of tape libraries to ensure they are the most secure in the industry. No other libraries have as complete a set of security features.

Security Feature	Description
IP Restrictions	Limit which IPv4/v6 addresses can access the library UI
Login with RBAC	Multiple roles and options to limit user access
Login Failure Lockout	15-min Lockout after 5 failed attempts
Inactivity Timer	Users logged out after a configurable period of inactivity
Service Login Security	Restrict service user access to local on-device UI only
Service Access Window	Set a time-limited window for service access
Service Access Disable	Completely disable service login access
Complex Passwords	Support for long (64 character) and complex passwords
LDAP / LDAPS	Support for user authentication using LDAP and secure LDAP
Reverse Tunnel Support	Configurable time-limited reverse tunnel for Support access
ICMP Disable	Prevents discovery of the tape library via 'ping'
Tape Encryption	Support for LTO tape encryption, including FIPS-validated
Encryption Key Management	Support for application-based or centralized SKM or KMIP Mgmt
Encryption Key Usage Policy	Choice of one key per tape, partition, or library
Media Security Notifications	Notify on expected and/or unexpected media removal events
Active Vault Partition	Secure, isolated partition not visible to applications or network
EDLM	Monitors tape health, alerts & takes action on suspect or bad media
Temp & Humidity Monitoring	Alerts if temperature or humidity fall outside safe range for media
Audit Reports	Log user activity, library configuration changes, and more
Vulnerability Scanning	Every FW release tested with multiple security scanners, Cloud-Based Analytics (CBA) portal scanned weekly
Firmware Signing	New library firmware is authenticated prior to being installed
Firmware Update Notification	Library alerts operator when updated firmware is available
Remote Logging	Support for sending log events to a remote syslog server
SNMP Support	Security and health information may be monitored via SNMP
WORM	Support for LTO WORM media

Table 3 - Quantum Scalar Tape Library Security-Related Features

IN CONCLUSION

Cybercrime attacks are becoming more sophisticated and more frequent. Human nature is exploited to launch attacks, making airtight prevention impossible. Ransomware is commonly used to extort attacked organizations, making it critical to maintain an offline copy of data that cannot be compromised. LTO tape is the best all-around technology for maintaining offline copies and is even safer when used within ultra-secure Quantum Scalar tape libraries.

Quantum

Quantum technology, software, and services provide the solutions that today's organizations need to make video and other unstructured data smarter – so their data works for them and not the other way around. With over 40 years of innovation, Quantum's end-to-end platform is uniquely equipped to orchestrate, protect, and enrich data across its lifecycle, providing enhanced intelligence and actionable insights. Leading organizations in cloud services, entertainment, government, research, education, transportation, and enterprise IT trust Quantum to bring their data to life, because data makes life better, safer, and smarter. Quantum is listed on Nasdaq (QMCO) and the Russell 2000® Index. For more information visit www.quantum.com.

www.quantum.com | 800-677-6268

WP00267A-v01 Sept 2021