
WHITE PAPER

# Your Last Line of Defense Against Ransomware

Quantum®

## CONTENTS

## YOUR LAST LINE OF DEFENSE AGAINST RANSOMWARE IS NOT THE ONE YOU THINK.

Ransomware has been in the news a lot recently, scams like Cryptolocker, Locky, and ScareMeNot—you name it. For those who haven't heard of it, ransomware is a type of malware that prevents or limits users from accessing their computer system, either by locking the system's screen or by locking/encrypting the users' files unless a ransom is paid (typically in bitcoins) in exchange for the deciphering key.

The first known ransomware was created in 1986, with more sophisticated RSA encryption-based schemes appearing in 2006. But since 2015, attacks have grown globally at an alarming rate. Cybercriminals are not only targeting individuals, they're also beginning to target corporations with more advanced targeted attacks. This sort of crime against business networks is on the rise. Once this software gains a foothold in your system, due to its deceptive nature, it can infest your entire system before you can detect it.

Let's take Locky as an example. Locky, a 100KB malware developed in C++ and compiled with Microsoft Visual Studio, deploys itself on your system and deletes the files that usually allow Windows to alert you that suspicious items have been downloaded from the Internet. The ransomware then starts to interact with a central server to report the successful infection, and receive an RSA-2048 encryption key and an identifier relating to the corrupt system. From there, it starts encrypting your computer or server—that's when the attackers can demand a ransom to stop the attack. There are many variants or clones of Locky or Cryptolocker around today, and while not related to the original Trojan, they all basically do the same thing.

But ransomware is not only targeting Windows systems, it also attacks other operating systems such as Mac OS with Trojans like KeRanger or Mabouia, Linux with Linux.Encoder.1, FairWare, and others, and network-attached storage (NAS) systems with SynoLocker. Mobile devices and even cloud-based file synchronization services have been attacked. Recently, the ransomware variant ScareMeNot infected 30,000 mobile devices in just three weeks. And, you know those Windows volume shadow copies (VSS) or System Restore functions you might otherwise deploy? Ransomware can disable those as well. Attackers are now targeting administrator accounts, in particular backup ones, to start encrypting backups before the primary data.

## HOW DOES RANSOMWARE GET INTO YOUR ENVIRONMENT?

Emails with malicious links and attachments account for 59 percent of ransomware infections. According to a June 2016 Osterman Research survey, users are more than twice as likely to be infected by clicking a link in an email than visiting an infected website directly. Does it only happen to others? In the same survey, almost one out of every two participants indicated their organization had suffered at least one ransomware attack in the past 12 months. With the arrival of Locky, the average number of ransomware infections reached 56,000 in March 2016 according to Symantec.

With more and more criminals attracted by ransomware as a source of easy income, ransomware authors have scrambled to meet the demand. According to Trend Micro, 50 new ransomware families were discovered in the first five months of 2016. The FBI estimates ransomware will be a $1 billion dollar source of income for cybercriminals this year. But, the actual ransom payment totals may be even larger since many choose not to report the crime. One widely reported case involved the Hollywood Presbyterian Medical Center. The hospital publicly reported paying an anonymous hacker $17,000 to free itself from a cyberattack, according to the New York Post.

Last but not least, Invincea researchers discovered a new ransomware variant called Cerber. This Trojan, along with encrypting files, installs a botnet capable of conducting DDoS attacks (a Distributed Denial of Service). A DDoS attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. This is double jeopardy. If the ransom is not paid, not only do the files continue to be encrypted, but the targeted system is recruited as part of a botnet for DDoS attacks—another boon for criminals because DDoS is a source of income.

## HOW DO YOU PROTECT YOUR DATA FROM RANSOMWARE ATTACKS?

**Protect your protection**

Given the increase of ransomware attacks, you need a strategy for defending your files against one of these debilitating events. First, you need to start with a proper data protection strategy. If you don't have a proper backup plan, you'd better have a bitcoin account ready to pay the ransom. Of course, payment is not recommended, as criminals don't always follow through with their promises to decrypt the data, as experienced by the Kansas Heart Hospital in May 2016 (reported by Healthcare IT News).

As the ransomware quietly encrypts your files, your backup program will likely back up the newly encrypted versions of the files. So, you need a program that does versioning. That's not too much of a problem as the majority of IT professionals keep multiple backups to enable applications or individual files to be recovered to a previous point in time before data was encrypted. But, even those older versions will be useless if the ransomware succeeds in encrypting all the files on your backup target, or even on a replicated distant repository (remember, ransomware can spread to other machines via your network). As long as the user has no write access to the location of the backup files (NAS share, Veeam Backup & Replication repository), the Trojan running under a user security context would be unable to encrypt specific backup files. Only 42 percent of IT pros who had experienced a ransomware attack reported being able to successfully recover all their data from backups, according to a 2016 Barkly study. One of the reasons was the fact that the backups were also encrypted.

As a best practice, you should make sure that administrators aren't using their accounts with elevated privileges on a continued basis. You need to protect the protector and carefully manage backup administrator accounts. The most advanced—and motivated—attackers are now targeting backups first via social engineering or other methods to obtain administrator privileges.

An excellent approach is the tried-and-tested 3-2-1 backup rule. A 3-2-1 strategy means having at least 3 total copies of your data, 2 of which are local but on different mediums (devices), and at least 1 copy off-site. Let's go further and call it the 3-2-1-0 rule. You need 3 copies, 2 mediums, 1 off-site, and the last one needs to be off-line with 0 real-time connectivity. So, the unsexy backup is becoming more and more attractive as your first line of defense for remediation.

### Is cloud ransomware protection heaven?

Smaller shops and end users at home rely increasingly on cloud backups as their last line of defense. It's easy to claim that using target cloud storage services such as Dropbox, Google Drive, and others will save your data against ransomware attacks.

Cloud-based backup is always on, but the files upload slowly. While that pace can be annoying, it adds an additional level of protection. It could be days, or even weeks, before all of the encrypted files get into the cloud. But with deduplication, compression, or bandwidth optimization techniques, access to the cloud becomes faster. The problem is that most of your files will be synchronized the moment something changes. In the event that your files are being encrypted by a ransomware attack, they will be uploaded encrypted. And if your organization uses cloud-based collaboration tools like Office 365 OneDrive for Business or Google Drive, the impact from a ransomware attack is multiplied at compute speed.

Of course, some cloud backup solutions can manage versions of your data, but the devil is in the details. As stated in a major public cloud provider's terms and conditions, "You can only restore previous versions one file at a time." Time to restore—if only one file can be restored at a time—is a key metric to include in your backup strategy.

Another issue is that attackers can now specifically target cloud storage, such as Dropbox and many more. You won't be aware that you're downloading encrypted files to one of these locations. Hackers don't even need your password anymore to get access to your cloud data. They simply steal your credentials and delete or encrypt your cloud backups, using a man-in-the-middle-like attack (now called "man in the cloud" according to security firm Imperva).

### Is tape the last line of defense?

Keeping a disconnected off-line copy of your data is a pragmatic way to improve your backup strategy. Your last line of defense needs to be an off-line backup. From an off-line perspective, tape storage provides some of the best options in this regard. It's cheap, portable—and off-line.

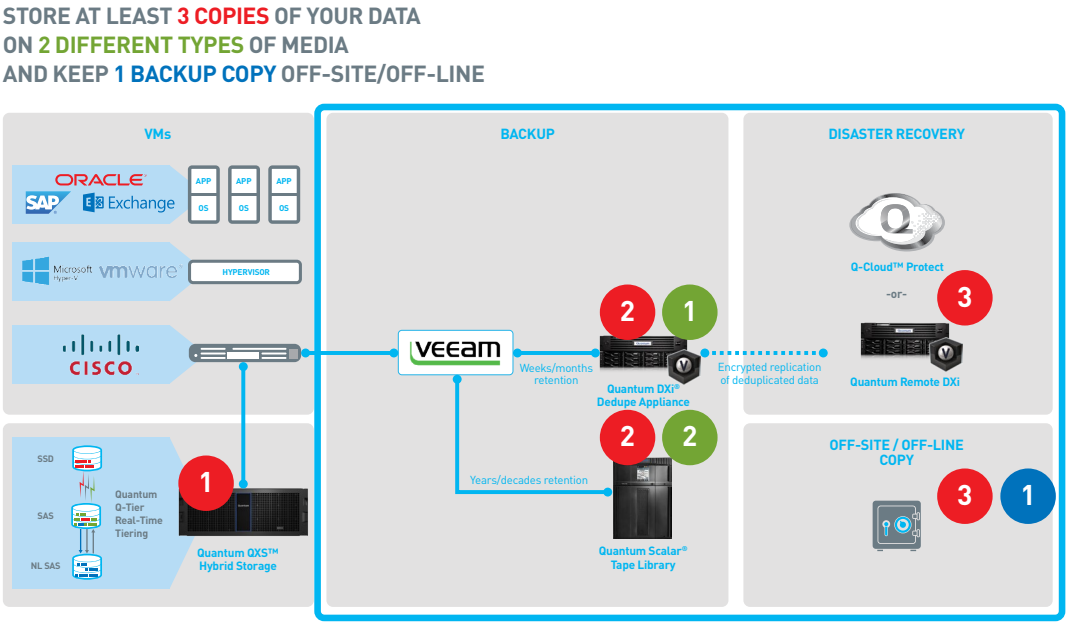
Other options include replication technologies and storage snapshots. But they're not entirely off-line, just, in a sense, "out of band" from real-time propagation.

Tape is your last line of defense—simply because criminals can't delete or encrypt what they can't access over the network.

To fully protect your data against ransomware, you need to prevent the infection in the first place, and then perform regular backups following the 3-2-1 backup rule, replicating data to off-site and off-line media, such as tape.

If you're a victim of a ransomware attack, visit www.nomoreransom.org to see if there is a decrypter tool available for the ransomware you were attacked with.

### About Quantum's 3-2-1 approach




*Example of 3-2-1 approach with Veeam and Quantum*

Quantum's unique tiered solutions maximize the production system availability and performance while cutting storage costs. At the core of our solution is the DXi® deduplication appliance. DXi can be physical or virtual and use patented variable-length deduplication to maximize data reduction and network bandwidth savings, without making a trade-off when it comes to backup and restore performance. DXi software enables fast backups and support for advanced features like Veeam instant recovery for fast recovery at near raw disk speed from deduplicated storage, or Concurrent Optimized Duplication for faster replication for Veritas Netbackup users. This means our customers can get the benefits of fast backups, fast replication, and fast restores while getting the full benefits of backup deduplication. DXi can replicate to other DXi appliances or to the cloud, and it can also tier data to tape.

Tape is the best solution for long-term retention and to protect your data from ransomware attacks. Tape cost per petabyte (over three years) is eight times cheaper than disk, and with a 30-year archive life—tape is the best media for long-term retention. But, it can also be used for archiving. One of the exciting features available with Quantum tape drives is our Linear Tape File System (LTFS), which allows you to use the tape almost as if it were a hard disk. You can drag and drop files from your server to the tape, see the list of saved files using a standard operating system directory (no backup software catalog needed), and use point and click to restore files. LTFS is an open standard, interchangeable with other LTO brands. It is also cross-platform, so you can use the tape as you would a USB flash drive. Simply load an LTFS-formatted tape into your LTO drive, mount it into the file system, and it becomes visible as if it were a disk. Currently, Quantum LTFS software supports Windows, Linux, and Mac OS X.

Tape as an off-line media is not only your last line of defense against ransomware, it can also help reduce your backup costs for long-term retention, and simplify your archiving strategy.

For more information, visit us at www.quantum.com or call 800-677-6268.

**ABOUT QUANTUM**

Quantum is a leading expert in scale-out storage, archive, and data protection, providing solutions for capturing, sharing, and preserving digital assets over the entire data lifecycle. From small businesses to major enterprises, more than 100,000 customers have trusted Quantum to address their most demanding data workflow challenges. Quantum's end-to-end, tiered storage foundation enables customers to maximize the value of their data by making it accessible whenever and wherever needed, retaining it indefinitely and reducing total cost and complexity. See how at **www.quantum.com/customerstories**.

www.quantum.com • 800-677-6268

Quantum



WP00221A-v01 Oct 2016