Abstract

The changing landscape of the data protection industry has evolved from backing up data in order to recover from hardware and network failures, software bugs and human errors, to fighting a mounting wave of cybercrime. Over the years, hardware and software have significantly improved their reliability and resiliency levels. However, cybercrime has now become a bigger threat to data protection and the stakes are getting higher as anonymous individuals seek to profit from other's valuable digital data. With a cease-fire in the cybercrime war unlikely, we are witnessing *the convergence of data protection and cybersecurity* to counter rapidly growing cybercrime threats, including ransomware.

Cybercrime and Ransomware on the Rise

Though digital extortion is not new, the growing use of ransomware is the latest crypto-viral digital extortion technique that locks the system's screens by encrypting selected users' files unless a ransom or extortion fee is paid (typically into an anonymous bitcoin account) in exchange for the deciphering key. A ransomware attack typically begins when an end user clicks on a website link or opens a file attachment in a malicious email that is part of a phishing (random) or spear-phishing (targeted) campaign. Emails deliver over 60% of all malware infections and initially land on HDDs or SSDs -- but not on tape.

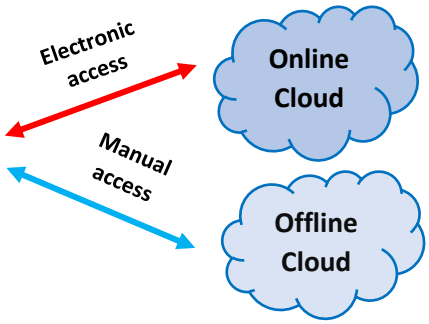
According to the findings in a report by Symantec Corp., hackers successfully stole or extorted an estimated $172 billion in 2017 with ransomware leading the way. Presently ransomware is growing unabated with over 4,000 attacks estimated daily. Nathan Thompson, CEO and founder of leading storage provider Spectra Logic, states in his recent book, Society's Genome, that "manufacturers of antivirus products have reservations about their ability to keep pace with this malware tidal wave". Thompson also states that "the aging power grid infrastructure in the United States is particularly vulnerable to cyber-

attacks as the unthinkable becomes the inevitable when one considers the possibility of extended outages across a large geographic area". Clearly the magnitude of the potential impact from cybercrime attacks cannot be underestimated.

The Tape Air Gap Provides the Optimal Backup Security

Many of the fundamental IT concepts of data backup are delivering additional values and are regaining momentum. One of those original backup concepts is the 3-2-1 rule. This rule states enterprises should have three copies of backups on two different media types, one copy of which is kept offsite. There are two ways to store an offsite data copy – either with an online (electronic access) or with an offline (manual access). Each of these approaches may use a data vault or a cloud service provider. Both options use the same SSDs, HDDs and tape storage devices for backup storage just like a typical data center.

The 3 – 2 – 1 Backup Rule		
3 **Copies of data**	**2** **Different types of media (HDD, Tape, SSD)**	**1** **Copy Offsite … (Cloud/remote storage) (HDD, Tape, SSD)**



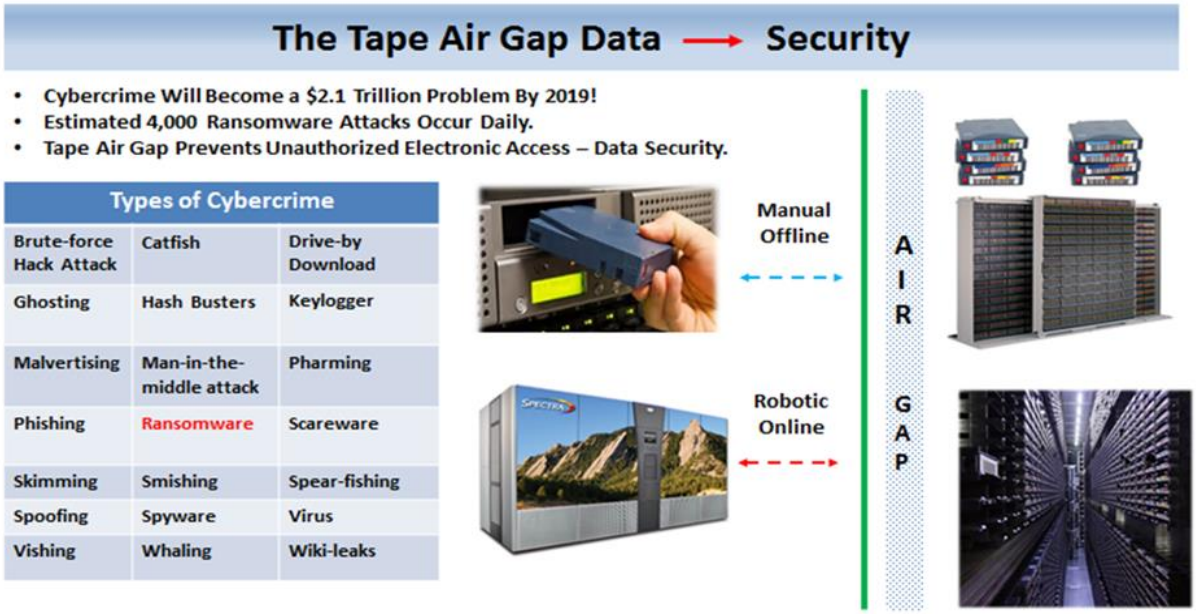
The rise of cybercrime makes the offline copy of data stored on tape more critical and describes what is referred to as the "tape air gap". An air gap is an electronically disconnected or isolated copy of data that prevents cybercrime from attacking a backup, archive or other data. Without an electronic connection to tape (or any other offline media), data stored on tape can't be hacked.

A tape air gap can be created between a backup server and backup storage by ensuring that the backup media is not accessible via any network or electronic connection. Tape is the most widely used data center air gap solution. Most tape cartridges typically reside in robotic tape library slots or in manually accessed media storage racks, meaning they are online only when the tape cartridge is mounted on the drive.

When tape media is not mounted on a drive and, therefore, protected by the tape air gap, it is not accessible to hackers, while HDDs SSDs are always online and accessible to hackers. For enterprises using multiple tape formats, Spectra's TFinity® Exascale Tape Libraries support LTO and the IBM and Oracle enterprise tape formats in the same robotic library creating an easy-to-manage and unique "tri-media tape air gap" supporting all three current types of tape media in a single storage system.

Cloud services can generate millions of dollars a day and represent a massive payday for a cyber-criminal organization. For cloud-based backup, critical data is backed-up over the internet and most likely stored in a shared storage infrastructure at an offsite data center maintained by a third-party cloud company providing backup, archiving and replication services. Attackers now specifically target cloud services as they no longer need a password to get access to cloud data. They simply steal the credentials and delete or encrypt an organization's cloud backups using a man-in-the-middle-attack. It's critical that cloud providers take advantage of the tape air gap to block cloud cyber-crime attacks.

Whether an organization has the best backup solution, the latest anti-virus protection tools, multiple versions of backup repositories, or use cloud services, the next generation of cybercrime is evolving so quickly that those concepts seldom matter for very long.



Attack Loops Make Ransomware More Challenging

Protecting against cybercrime presents a continual challenge to the IT industry. Some types of malware -- specifically ransomware -- are using Attack Loops to circumvent standard security measures. Attack Loops specifically target backup data to prevent successful recoveries and force a ransom payment from the affected parties in order to regain access to the encrypted data.

These more-sophisticated types of attacks embed time-delayed, undetected malware into online files. The malware stays dormant, sometimes taking several months to reactivate. In the meantime, the dormant malware will eventually and unknowingly be backed up to a backup device, normally tape or HDDs. After a time-delayed online malware detonation on a file(s), the pre-attack generation of the backup file(s) is restored only to realize that the recovery data re-inserts the ransomware back into the system, recreating the ransomware and re-encrypts the data all over again for a perpetual loop of attacks. This makes file restoration pointless because as data is recovered, the ransomware re-ignites.

Fortunately, Attack Loop prevention software is becoming available and uses signature-less technology which identifies and quarantines malicious code upon entry into the backup repository and again prior to recovery into the online environment to ensure safe, secure and reliable data recovery with the malicious code disabled. Effective Attack Loop software platforms use automated, self-learning (AI) strategies, and may include a zero-day Attack-Loop preventative technology. The general definition of zero-day attacks (or zero-day exploits) are attacks that target publicly known, but unpatched system vulnerabilities.

Software vulnerabilities may be discovered by hackers, security companies, government researchers, software vendors themselves, or users. If discovered by hackers, an exploitation of the weakness will be

kept secret for as long as possible and will circulate only through the ranks of hackers, until software or security companies become aware of the weakness, or of the attacks targeting the weakness.

Given the steady increase and growing impact of malware, especially ransomware attacks, organizations must develop strategies for defending files against these potentially crippling events. As we have witnessed in the past few years by many highly visible attacks on well-known corporations, the impact of ransomware can damage organizations operationally and financially, causing customers to lose trust and cease to do business with the company.

Tape Technology Keeps Advancing

Keep in mind that tape technology is not standing still. Data centers and cloud service providers are addressing many new applications leveraging tape for its security and significant economic advantages. Tape has proven to be a critical building block of a complete modern data protection plan at the industry's lowest cost per gigabyte. The TCO for HDD is typically 6 to 15 times higher than tape as tape delivers significant cost savings over HDD solutions. Tape has further expanded its position as a highly effective complement to SSDs and HDDs in a tiered storage environment for the foreseeable future. This is due to its higher reliability (over HDD by three orders of magnitude), higher capacities, much faster data rates, and significantly lower energy costs. Coupled with encryption, WORM, and the tape air gap, tape is armed to deliver the highest levels of data protection. This recognition is driving continued investment in new tape technologies defining robust roadmaps that face few technological limits for the foreseeable future.

Summary

Today's world is more interconnected than ever before. Yet, for all its advantages, increased connectivity brings much greater risk of theft, fraud, and abuse. To fight cybercrime, organizations must reevaluate their data protection strategies. If an organization does not have a robust backup plan, it had better have a bitcoin account ready to pay the ransom. The most important thing to do when dealing with ransomware is to make sure that a backup copy of critical data is stored offline behind an air gap, so the data can be restored, and operations can resume as quickly as possible. The tape air gap is the last line of defense for data simply because criminals can't delete or encrypt what they can't access over the network or any other electronic link. As a result, tape provides an inherent degree of cyber protection not available in other storage products. Remember backup is one thing – recovery is everything.

Bottom line: Given the rising wave of cybercrime, the role of tape-based storage and cloud solutions taking advantage of the "tape air gap" will expand to provide the last line of defense for cybercrime. With new challenges appearing daily, the convergence of data protection and cybersecurity to counter rapidly growing cybercrime threats, including Ransomware, is well underway.