TechTarget | Custom Media

Tape or Cloud Backup? Why Both Should be Part of Your Cybersecurity Plan

By David Strom

The old standby of data protection—tape backups—is still alive and well in many IT shops. Ironically, it is making a resurgence because of ransomware and other malware attacks. "In the modern era, there is a lot of comfort in having something offline, like a tape, and everyone has a story about how a tape backup saved their operations," said Rick Vanover, director of product strategy for Veeam Software. "We don't know what tomorrow's threats will look like, and there is a lot of risk to having something online that is connected to a network with these types of threats today."

Tape has a long history as a backup medium, to be sure, but the fact that it can easily move from online to offline status brings a lot of appeal in these days when a malware infection can spread like wildfire from server to server across an enterprise network. Sometimes, having too much connectivity can be a bad thing, especially when you don't know how many of your endpoints have been harmed with an attack or when you have made mistakes in your network configuration and access controls. That is why it is useful to balance both tape and cloud technologies to help fight attackers and create the best backup strategy out of advantages from both methods.

VEEAM

"With the cloud, you can deploy a completely different file system, a different API, have a different type of storage. All of that diversity is very attractive and helps with data protection"

Ironically, Veeam didn't support tape for a long time, until they kept hearing from their customers and put in support for tape backups in version 7. Now, they consider that there are benefits to having both tape and cloud-based backups to improve your cybersecurity posture. Both have low acquisition costs, although for different reasons: Tape because the technology is well known and inexpensive; the cloud because you aren't investing in a lot of capital equipment. Having both helps to reduce potential data loss, and the two technologies can be very complementary.

"With the cloud, you can deploy a completely different file system, a different API, have a different type of storage. All of that diversity is very attractive and helps with data protection," says Vanover.

In fact, diversity means having a lot of other elements, too. For example, there is appropriate account management when it comes to the usernames that backup processes employ. Many IT shops grant full access rights to the backup processes, meaning that if someone were to use this login credential, they could have universal permissions to production data and files. This is more than theoretical: A recent attack by Russian actors on various energy-sector targets had hackers run scripts that created local administrator accounts disguised as legitimate backup accounts to gain network access.

When Vanover first began working at Veeam, their engineers saw that their customers kept the usernames of older backup vendors' products when they migrated them over to Veeam. "They kept the usernames because **they had these universal permissions and didn't want to change them**."

That is a potential disaster on several levels. "This is a honeypot waiting to happen," he says. "It can attract all kinds of malware and propagate around your network and encrypt all of your production systems." Instead, you should consider limiting these access rights, and set up different authentication mechanisms for your backups, to make it more difficult for hackers and others to move about your network. You also shouldn't use a single username for all backup processes. Backup users shouldn't share the same domain or Active Directory tree that contains the regular users, too.

Another way to do this is by using **different file systems**: Backing up a Windows server on a Linux machine, and vice versa. And it helps to have the backups in two different physical places, again to increase diversity of your backup solutions.

This latter suggestion has been around seemingly since the dawn of time, and usually goes by the **3-2-1 rule: Keep three different total copies of your data, two of which are local but on different media, and at least one copy offsite**. "You would be surprised how often I find companies that don't implement this basic rule," says Vanover. "I had one IT manager who wanted to make backup copies of his virtual machines on the same network storage device that was running them. Nothing surprises me anymore."

Another part of data diversity is in doing **multiple and different types of restore points**. This makes it easier to find a particular set of files or a single application to restore. You want to consider making file-only backups, too, because you might need to skip the malware that was inadvertently saved on a backup job. "If a server gets infected with ransomware, it could be restored with the infection intact and then Windows will just re-encrypt the files. You want to make sure you don't re-introduce the sources of infections," says Vanover.

One of the attractions for having tapes is their essential "air gap" nature, segregating the online and offline worlds. Having an air gap can

Treat your backup repositories with the same care that you treat your production data.

remove a system from constant online contact. But **how an air gap is implemented is key**. You have to look at the applications and the data, and how they implement the backup. "For example, does a tape always sit in a tape drive? For it to be an effective air gap, it has to be a regular tape rotation schedule and you have to manage the movement of the tapes, because this is what dictates how well the air gap exists," he says.

One way to implement air gaps is to have the tape system operate mostly offline, and **only come online when it is time to perform a backup**. For further security, you can implement an offline means to initiate the backups. Again, the goal here is to help keep this medium safe from unauthorized access, and free of infection.

Finally, treat your backup repositories with the same care that you treat your production data. "Many CISOs don't have the same controls in place for their backups, and don't think about the security implications," Vanover says. "They think they are doing enough by encrypting their backups." He posits the following situation, where a backup administrator can restore the CEO's email box to a local machine, and have access to all of the messages. "You have to put controls in place, as well as track who is restoring what data to what location, so you can highlight potential issues like these," he says.

This points out the difference between replication and backups. The two have different use cases and procedures, and need to be kept distinct. But it also points out that you need a variety of backup methods, too. "Tape and cloud are both needed these days. You really should use both," says Vanover.