"I've taken my backup, so I'm protected." No, that isn't correct. With issues like ransomware attacks being so common, you should rethink your backup strategy to consider these risks.

While momentum gathers for digital transformation (DX), the importance of business data is increasing. Unfortunately, criminals know this, so they use ransomware to target business data. To protect your data and your company against ransomware attacks, natural disasters, and system failures, you should implement a comprehensive backup system for your business data that can ensure full-state recovery of data and operating systems in case of an emergency.

So, now we have to re-examine your backup system. But why?

(Photo/Getty Images)

Enhanced backup system is highlighted through the threat of ransomware

As the implementation of DX accelerates, tasks previously performed by relying on paper materials and manual labor go digital, and an increasing number of businesses are approaching the transformation of their business model by taking advantage of digital technology. As they do so, the company's data integrity becomes more critical.

As companies ask the question, "How do we protect our data?" They should consider all the potential risks facing their data. Many companies prepare for natural disasters and system failures but fail to account for criminal activity, like sabotage and ransomware.

Once ransomware infects your company, it crawls through your systems, encrypting all your files and data, making it impossible for you to access that information. Then, they demand payment from you for an encryption key you can use to unlock all your data. If you refuse to pay the ransom, your data is locked forever.
In these scenarios, having adequate security protocols in place to prevent ransomware attacks is essential, but it is hard to avoid an intrusion 100% of the time. However, an accurate, timely, and complete backup can save your company should a ransomware attack on your data prove successful.

Unfortunately, more than just having a backup is needed. Recently, criminals have become more sophisticated and have started targeting your files, data, and backups. You cannot simply say, "No problem. We have backups." You must consider these risks and create a backup plan that protects your data during an attack.

Let's re-evaluate The "secondary storage" saving backup data

Mr. Shogo Sato, Senior Vice President and CSO of Actiphy, Inc., stated, "Backups saved to a single storage location are no longer enough. Nowadays, companies must also deploy their backups to secondary storage locations." Actiphy, Inc. is a publisher of backup/disaster recovery software.

So, what do we need to consider when building our new, more robust backup strategy? First, the closer your backup files are to your ransomware-infested environment, the higher the risk of losing your backup files. For example, after infiltrating one of your PCs, a ransomware virus will spread itself across the network to infect whatever remote drives it can access. If your backup server is accessible, those files will also be encrypted, and you will not be able to access them without an encryption key.

An increasing number of companies today choose to use public cloud storage for their backups to avoid the risk of ransomware infections and reduce the burden of managing in-house IT infrastructure. However, cloud storage options still have issues you must consider. For example, data

transfer may become a problem, especially if your company possesses large amounts of data.

"Recently, we have more cloud storage options than ever; however, transferring large amounts of data to a cloud storage provider is still impractical. Moreover, since many small to medium-sized businesses own only one internet connection, transferring large amounts of backup data to the cloud may significantly impact other network needs," according to Mr. Sato.

In addition, frequently transferring large amounts of data to the cloud can significantly impact your monthly fees. Moreover, laws, regulations, and internal policies can prohibit companies from storing some types of confidential information in the cloud.

If you have such limitations at your company, you'll need to build an on-premise backup environment. Many companies are turning to on-site options to reduce bandwidth fees, comply with laws and regulations, and effectively store more significant amounts of data. If you choose this option, you can reduce the risk of ransomware infections by prohibiting your systems from overwriting backup files in tape storage, disallowing network access to backup files after the backup completes, etc.

"You cannot make sweeping statements on the best backup solutions to protect against the threat of malware attacks, such as ransomware. You must consider your industry, business size, laws, regulations, etc. You should carefully examine your company's needs before designing your backup strategy," says Mr. Sato.

"ActiveImage Protector" enables fast and reliable full-state data recovery

We have designed Actiphy's ActiveImage Protector software to meet your company's needs.

ActiveImage Protector includes the following features:

- It supports Windows physical and virtual servers.
- It backs up your entire machine, including the OS.
- It can back up entire volumes, disks, files, and folders.
- You can save your backups to any available storage location, Including NAS / USB HDD / LTO tape storage / Amazon S3 (including its compatible object storage) / SFTP servers / Local HDD.

Mr. Shogo Sato, Senior Vice President and CSO of Actiphy, Inc.,

When thinking about your backup strategy, you must also think about recovery. What good is a backup if you cannot use it to recover and restore your data quickly?

ActiveImage Protector offers a variety of reliable features designed to ensure you can restore your data quickly and safely".

1.User friendly GUI provides easy-to-use controls of backup operation, meeting users' needs

ActiveImage Protector has an intuitive and user-friendly interface to help you save and restore backups from both physical and virtual servers. The built-in wizards guide you through every step of the process. ActiveImage Protector makes it easy to back up and restore volumes, disks, directories, and files.

ActiveImage Protector includes an intuitive scheduler that allows you to automatically execute full and incremental backup tasks once or on a monthly, weekly, or daily schedule. You can even schedule backups on certain days or during specific months. The scheduler is flexible enough to fit your needs.

"Overseas companies produce most backup software, but we developed ActiveImage Protector in Japan. We have worked hard to ensure our products handle Japanese data and have added features based on customer feedback in Japan. Naturally, the more features software has, the more complicated it can become. For this reason, we have made great efforts to develop an easy-to-operate product that allows users to fully utilize all the features without dealing with the complexity," said Mr. Sato.

2. Agent-based and agentless backup of virtual machines

ActiveImage Protector supports agentless backups on virtual machines, meaning you can back up virtual machines without needing a backup agent running on the system. We also support agent-based backups of both virtual and physical machines using ActiveImage Protector agents. Agentless backups are helpful when backing up a legacy system (e.g., Windows Server 2003) for which we don't provide an agent.

If you back up virtual machines using VMware vSphere, running on HCI (Hyper-Converged Infrastructure) using vCenter, moving your virtual machines to another host will break your incremental backup chains.

With ActiveImage Protector, on the other hand, regardless of whether you use agentless or agent-based backups, your incremental backup chains will stay intact even if you move your virtual machines to another host. There is also no need for you to register the host with vCenter. You do not have to deploy your backup server separately; you only have to select a disk as the destination storage.

3.Save backups to any available storage at faster backup speed

As stated above, you can save your backups to an Amazon S3-compatible object storage. However, when saving backups to the public cloud, you must consider backup speed. For example, if you were backing up 15GB of data directly to cloud storage using another backup tool, it would take an average of 20 to 30 minutes. However, with ActiveImage Protector, the process completes within about five minutes," said Mr. Sato.

Another feature of ActiveImage Protector is its ability to save to LTO Tapes suited for backing up large volumes of data for long-term storage. You can protect backup data saved to LTO tape so others cannot overwrite it. In addition, you can disconnect your LTO tapes from in-house internet access and physically isolate your backups from ransomware attacks.

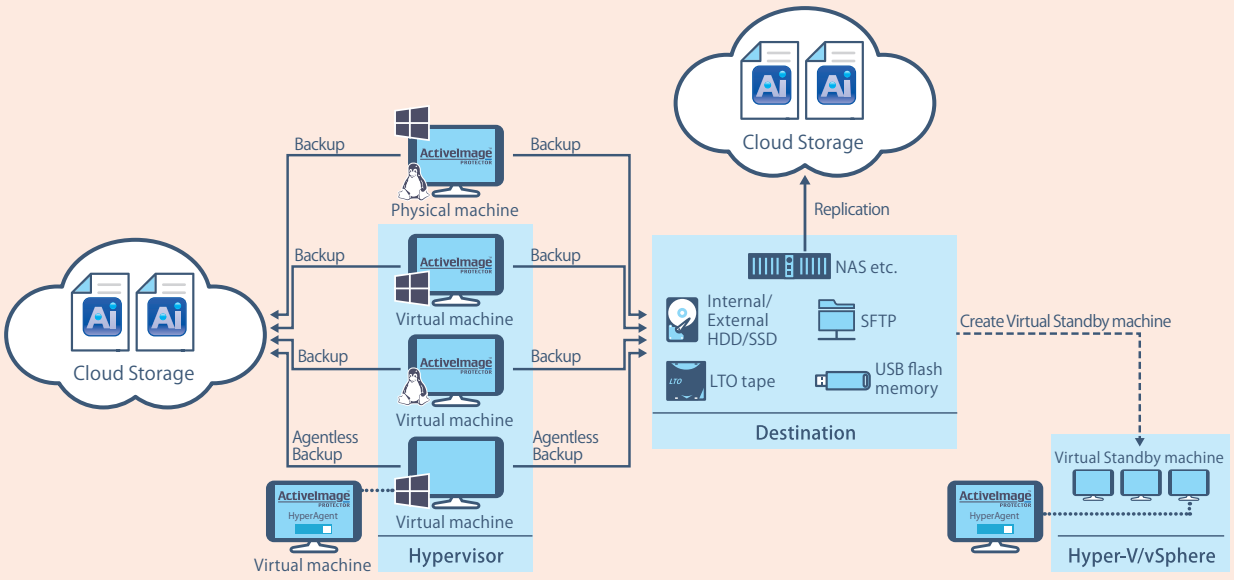
ActiveImage Protector is also cost-effective. For example, we license ActiveImage Protector Virtual to your virtual host instead of your virtual machines. In other words, you can run as many virtual machines as you'd like on your host with a single license. ActiveImage Protector also provides a free replication option to save backup data to a remote site.

Actiphy solves your problem based on our concept "Support Service is a part of our software product"

ActiveImage Protector eliminates the complexity of managing today's complex backup and disaster recovery strategies.

"We understand that service contracts are a part of the cost of the software. To help our customers, we include the first year of service for free with the purchase of a perpetual license. We have an organized telephone support team to support our customers. One of our strengths is the short amount of time between the initial support call and a proposed solution to our customers' issues," said Mr. Sato.

ActiveImage Protector quickly and reliably restores system and data in full-state even in complex system environment



Case Report - Quick recovery from ransomware infection

A wide variety of customers have deployed ActiveImage Protector in their environments. We want to share one of the cases where a customer successfully and quickly restored their data after a ransomware attack.

One system administrator in this company, headquartered in Tokyo, maintains ten physical servers running forty virtual machines. This administrator had scheduled their physical servers to be fully backed up once a month, with incremental backups scheduled daily using ActiveImage Protector.

One day, the company fell victim to a ransomware attack and realized its files were encrypted and inaccessible. So, the system administrator stopped all the servers to prevent the virus from spreading. But unfortunately, the ransomware encrypted their shared folders, email server, and other mission-critical systems. The system administrator tried to restore their data to the point when the server got infected with ransomware by using ActiveImage Protector; however, most of the backup data saved in the Tokyo office was encrypted and rendered useless.

Then, the administrator used ActiveImage Protector's Offsite Replication feature and restored nearly all their data from their servers in Osaka. Thanks to ActiveImage Protector, employees could return to work within the day.

In another case, one of our customers couldn't boot one of their machines after running Windows Update. They restored the machine from a backup within five minutes and were back to work using ActiveImage Protector.

Also, in one of our customer's factories, an inexperienced employee successfully used ActiveImage Protector to restore a failed system.

There are many cases where ActiveImage Protector's ease of use has helped our customers restore their data and get back to work as quickly as possible.

Actiphy's goal - Quick and uncomplicated data recovery in any system environment

Recovering your data from a backup should be quick and easy, and your downtime should be minimal. ActiveImage Protector allows even the untrained to restore their data and get back to work.

ActiveImage Protector is the solution meeting these users' needs.

"Actiphy has developed its flagship software to enable full-state recovery of your systems and data in any environment. We believe that the role of ActiphyImage Protector is to quickly and easily restore your data to enhance your business productivity," said Mr. Sato.

Furthermore, Actiphy, in collaboration with companies that provide network security and storage products, can work with you to propose security countermeasures and IT infrastructure that fits your company's needs.
If you have data that needs protecting, please get in touch with Actiphy and let us help you build the perfect data protection solution for your business.

Contact:

Actiphy

Actiphy, Inc. Global Sales Dept.
Phone:+81-3-5256-0877 https://www.actiphy.com global-sales@actiphy.com