Hewlett Packard
Enterprise

Business white paper

Five endpoint backup considerations for ransomware protection

How businesses can protect themselves from loss when ransomware strikes

Table of contents

Endpoint backup for ransomware protection
Data backup is critical for protecting your organization from ransomware attacks. Preparing the right strategy for endpoint data protection, and finding the right solution that meets your strategic requirements are even more crucial.

The key to protect your data from ransomware attacks is to plan and adopt the following strategy:

- Backing up data regularly
- Isolating backups from endpoints
- Securing the backup
- Verifying backup data for integrity and availability
- Enforcing efficient recovery practices

Executive summary

Ransomware attacks have been on the rise in the last few years causing damages worth millions of dollars to businesses and increasing burden on law enforcement. Most organizations have malware detection solutions installed on their endpoints to protect them from such threats. These solutions, while effective most of the time in neutralizing known ransomware, can’t promise to fully prevent against all the new variants of ransomware injected into the cyber world on almost a daily basis. Keeping this in mind, the United States Department of Homeland Security (DHS) issued a ransomware alert recommending businesses to back up critical data. However, not all endpoint backup solutions are capable of protecting your business from ransomware—especially crypto ransomware, a powerful malware that blocks access to a computer system by encrypting data stored on it. To ensure your organization is protected against ransomware risk, careful consideration is required in selecting an endpoint backup solution.

This paper explores the key capabilities an endpoint backup solution must have to successfully protect your business from ransomware attacks.

Ransomware menace

The threat of a ransomware attack is a major concern businesses are facing today. The United States Federal Bureau of Investigation (FBI) received 2,453 complaints related to ransomware attacks in the year 2015.[1] The year 2016 started with a headline story of a hospital in Hollywood that ended up paying $17,000 USD to the hackers in order to get their data back.[2] The FBI warns that there would be more attacks focused on organizations than on individuals in the coming days, as organizations are more likely to pay the ransom.

Ransomware has been one of the most successful moneymaking schemes devised by hackers in the last few years. It is a type of malware that infects computer systems, restricting end users from accessing the infected systems and its data until a ransom is paid to the hackers who spread the malware. If they fail to pay the ransom, the data is lost forever. The earlier versions of the ransomware—Locker ransomware—were annoying but weren't such a significant threat. They are able to lock the computer screens but the data on the computer remained untouched. Hence, it was fairly easy for end users and IT administrators to restore the computers to a clean state. The advent of crypto ransomware—the ransomware that not only locks the computers, but also encrypts the user data—increased the threat level. The newer variants of crypto ransomware use sophisticated asymmetric keys for encryption making it hard to get back the data. They also use privacy-enabling tools such as Tor and anonymous payment options such as Bitcoin making it hard for the law enforcement authorities to trace the source of ransomware.

Ransomware have no geographical boundaries. It has affected businesses within many market segments in major countries around the world. The United States DHS, in collaboration with Canadian Cyber Incident Response Centre (CCIRC) released an alert warning individuals and organizations to prepare themselves to face the threat of ransomware. The alert recommends individuals and organizations to back up all critical data wherever it resides, whether endpoints or data centers, and follow proper procedures for endpoint data protection.

[1] **pymnts.com/news/security-and-risk/2016/city-held-hostage-via-bitcoin-ransomware**

[2] **fortune.com/2016/04/01/u-s-hospitals-face-growing-ransomware-threat**

Preventive controls are necessary, but not sufficient

The DHS alert and the FBI warning suggest that organizations must implement proper cybersecurity procedures and solutions to prevent from ransomware attacks. Regular updates to operating systems and antivirus and antimalware tools are strongly suggested to detect new types of ransomware and prevent them from spreading across the network. Using modern security solutions that leverage advanced machine learning to monitor unusual activities, organizations can proactively detect ransomware attacks and swiftly act to prevent greater damage.[3]

The preventive controls, though necessary, are not sufficient to maintain business continuity. As ransomware evolves, such controls lag behind in identifying and neutralizing the new variants of ransomware. The preventive controls also assume that the organizations keep their patches up to date, which is not always the case. Solutions that depend on notifications and end-user interventions to stop unusual activities cannot fix the damage that's already done. Therefore, organizations must have a contingency plan in place to recover clean data when unable to prevent the ransomware attack.

Backup and recovery is the only true contingency plan

When the preventive controls cannot stop a ransomware from affecting a computer, the organizations have only two options to restore data:

1. Pay the ransom
2. Recover data from backup

Paying the ransom doesn't guarantee data recovery. The FBI is investigating cases where the affected party has paid in Bitcoin currency, but weren't able to get their data back. Some of the new variants of ransomware put a deadline for ransom payment (such as three days) and delete the private key after the deadline.[4] Once the private key is destroyed, data is lost forever and no amount can bring it back.

Having a proper endpoint backup and recovery strategy is important for organizations to recover their data. Selecting the right endpoint backup solution is critical for business continuity as ransomware targets endpoint computers to penetrate organizations and corporate networks. They get into endpoints either by user initiated actions such as visiting a malicious website, or clicking on a phishing link or an email attachment. In most cases, the primary target of ransomware attack is endpoint devices.

[3] sfchronicle.com/business/article/santa-clara-charity-has-a-narrow-escape-from-7384755.php

[4] theinquirer.net/inquirer/news/2350303/nca-warns-thousands-still-at-risk-from-gameover-zeus-and-cryptolocker-malware

What is the right endpoint backup solution?

When implementing a comprehensive endpoint backup and recovery strategy that can protect against ransomware, organizations must consider the following:

1. Backing up data regularly

With no regular backup policy, the organizations risk losing critical data and employee productivity. At times, the loss of productivity cost could be higher than the ransom itself, which may motivate organizations to pay for the ransom and get back the most recent copy of the data.

Regular backup is a challenge with increasingly mobile workforces, as it is hard to predict the schedule and location of the end users. Therefore, it is important that organizations maintain a short recovery-point objective (RPO) with backup solutions that support continuous data protection (CDP).

Verify consideration #1

- Is the data backed up with continuous data protection, or is it schedule based?
- Does the backup happen when the end user is mobile and not within the office network?
- Can your administrator learn from the reports whether all backups are up to date?

2. Isolating backups from endpoint devices

As the DHS alert warns, some variants of ransomware encrypt network-connected backups and mapped network drives. Some new ransomware variants such as Locky affect even the unmapped drives that are used for file sync and share.[5] The variants of CryptoWall also delete the Volume Shadow Copy Service (VSS) to stop the end users from getting the clean files back from snapshots.[6] Those who have been affected by ransomware have noticed that though the malware knows how to encrypt files in the network drives, it cannot decrypt those files back to the original state all the time even after paying the ransom.[7]

There is a growing awareness that the cloud drives and shared network drives do not replace endpoint data protection. Organizations must have a strategy to isolate the storage for endpoint backup, and choose the solution that does it effectively.

Verify consideration #2

- Does your backup solution isolate the storage from the endpoint?
- Is your backup store a mapped network drive or a cloud drive with write permission?

3. Securing the backup

Having proper security checkpoints in place ensures the authorized personnel and applications can access and use the backup data for specific purposes such as recovery. The cost of data breach has gone up by 23 percent in the last two years.[8] Malware-based data breaches have used endpoint devices as a pivot before targeting the corporate network. Running an unsecure endpoint backup solution may expose the endpoint backup data to a future malware or cyber criminals.

A secure endpoint backup solution would support higher quality encryption (e.g., AES 256 bit) for data in transmission and storage, customer-managed encryption keys (e.g., HPE Enterprise Secure Key Manager [ESKM]) and federated authentication (e.g., SAML v2) for data privacy, and Lightweight Directory Access Protocol (LDAP) integration for authentication and authorization.

Verify consideration #3

- Does your backup solution use strong encryption for data transmission and data storage?
- How does your solution ensure data privacy in a multitenant environment?
- Does your backup solution support disaster recovery?

[5] **securityweek.com/locky-ransomware-encrypts-unmapped-network-shares**

[6] **blogs.sophos.com/2015/12/17/the-current-state-of-ransomware-cryptowall**

[7] **pcworld.com/article/2901672/how-to-prevent-ransomware-what-one-company-learned-the-hard-way.html**

[8] **securityintelligence.com/cost-of-a-data-breach-2015/**

4. Verifying backup data for integrity and availability

As crypto ransomware encrypts the user data on an endpoint device, in all likelihood, an automatic backup solution would end up backing up the encrypted data making the backup copy useless. The backup strategy must ensure that the previous versions of the files are intact and available for recovery for the required period of time.

Some endpoint backup solutions allow the administrators to disable file versioning to cut the storage cost. While this strategy may help reduce the storage costs, it has dangerous consequences. Therefore, organizations must adopt a strategy to leave file versioning always on, or even better, select a backup solution that does not disable file versioning.

Data retention policies on most backup solutions define how long the file versions are stored. Such backup solutions keep the latest version and delete the older versions after the retention period ends. Typically, end users detect ransomware only after ransomware puts up the extortion notice, which it does after encrypting all the files attached to the computer. If the computer has a large data set, or if it is connected to a network drive, it may take a long time before the end user learns about the infection. With a short retention period, organizations run the risk of losing clean data. Therefore, they must have the flexibility to extend the retention period when they detect ransomware. It is even better to set an extended retention period, preferably a few months to factor in the delays that they may encounter in recovering the data.

Verify consideration #4

- Does your backup solution support file versioning?
- Does your solution give an option to the administrator or the end user to disable versioning?
- How long is the file retention period? Is the retention period long enough to restore original data?
- Does your solution support a flexible retention policy so that the administrators can extend the period?

5. Enforcing efficient recovery processes to facilitate business continuity

Backing up data solves only half of the problem. Data restore is as important as backup, if not more. While planning data recovery strategy during ransomware attacks, organizations must first formulate a procedure that affects the business continuity the least. An efficient data recovery procedure keeps the operational cost low.

The planners must address whether they should support restoring data on the same device with a reimaged operating system or a new device with the same or a different operating system, and whether the file metadata such as timestamps must be restored to the original state.

Point-in-time data restore is an important capability that allows the end users to restore previous versions of files at any given time. This removes the need for end users to restore each file individually to the correct state.

Organizations must plan to be in charge of the data restore process and not depend on vendor's technical support to restore the data. Ideally, the end users must have the ability to perform point-in-time data restore on a newly imaged endpoint without the need for administrators or technical support.

Verify consideration #5

- Does your endpoint backup solution allow restoring the data on a new or a reimaged endpoint?
- Does your solution restore file and folder metadata?
- Can you perform point-in-time restore?
- Can the end users and administrators restore the data on their own without the help of your vendor's customer support?

HPE Connected MX for protection against ransomware

HPE Connected MX is an enterprise-focused endpoint data protection solution offering a comprehensive suite of capabilities for organizations to protect their data from ransomware attacks. It is designed to meet the needs of an increasingly mobile workforce while providing business assurance and continuity. Supporting an organization's strategic and tactical needs to protect endpoint data from ransomware, HPE Connected MX offers the following key capabilities:

- Isolated endpoint backup with no mapped network drive
- Self-managed data restore on a new or reimaged endpoint
- File versioning turned on all the time
- Point-in-time data restore
- Flexible data retention policies that can extend up to 180 days
- Continuous data protection
- Enterprise grade security with AES 256-bit encryption, SAML v2 support, HPE ESKM integration for customer-managed keys

References

- **Ransomware and Recent Variants, US-CERT**
- **Ransomware brochure, FBI**
- **Incidents of Ransomware on the Rise, FBI**
- **All You Need To Know About Ransomware, University of North Carolina**
- **The evolution of ransomware, Symantec**

Learn more at
hpe.com/software/connectedmx

Sign up for updates

Hewlett Packard
Enterprise