WHITEPAPER

Retrospect
A StorCentric Company
Data Protection for Businesses

Retrospect Backup

5 Steps to Ransomware Protection

Backup Less. Manage Less. Worry Less.

Ransomware has become a global threat, affecting homes and businesses across the globe. According to Kaspersky, ransomware attacks, such as WannaCry, Petya, and NotPetya, have increased by 250% in 2017. WannaCry in particular has hit thousands of businesses, including high-profile organizations like the U.K.'s National Health Service, with estimated damages exceeding $1 billion dollars.

"Over the past four years, ransomware has evolved into one of the biggest cyber security threats in the wild, with instances of ransomware in exploit kits."
- Nathan Scott, Malwarebytes

Let's walk through the five essential steps to ensuring your business is protected against ransomware, so that if it hits your computer, your business will be restored quickly.

Step 1: System Protection

The first critical step to protecting your business from ransomware is system updates and anti-malware software. Keep your systems up-to-date with the latest patches provided by the manufacturers. Keep in mind that latest ransomware attacks exploit a Windows security bug that has been patched for months. Beyond system updates, it's a good IT practice to run anti-malware software to prevent as many variants as possible.

However, you need to prepare your business for an attack. That's why every business should prioritize backups of their infrastructure. It's the number one solution against an attack.

Step 2: Endpoint Protection

Malware can hit any computer in your environment. The WannaCry Ransomware was actually an internet worm, not simply a phishing attack, so the malware was able to spread automatically across networks using a security flaw in Windows. With threats like this, you need to protect every computer, not just your server or file share.

With features like smart incremental backup, file-level deduplication, proactive backup, block-level incremental backup, and script hooks, Retrospect makes it easy to protect every computer in your environment, be it Windows, Mac and Linux desktops, laptops, and servers. Retrospect backs up each computer quickly and automatically according to a dynamic schedule, so your computers will be fully protected against attacks.

Step 3: 3-2-1 Backup Strategy

IT administrators know the best strategy for data protection is the 3-2-1 backup strategy: 3 copies of your data, 2 different formats, 1 offsite location. If all of your backups are on a single disk that is connected to your computer, those backups can be encrypted at the same time as your source data, rendering them useless. With three copies of your data–on your computer, on local storage, and on offsite storage– you'll be able to recover from ransomware quickly and get your business back up and running.

Retrospect supports a long list of cloud storage providers, including Amazon S3, Google Cloud Storage, Backblaze B2, and Dropbox. Cloud storage is a great way to manage offsite protection because the storage isn't mounted as a volume on your computer like local hard drives or network-attached storage (NAS), so malware does not have access to it. Moreover, our offsite protection fully supports advanced encryption like AES-256 for complete security.

Immutable Backups allow you to protect your backups using Object Locking in certified cloud providers with Retrospect Backup. Learn more in Retrospect's Immutable Backup white papers.

Step 4: Detection

Ransomware encrypts the user files on a computer, so monitoring your backups routinely can help detect that you have been attacked. A sudden spike in data being backed up may be an indication that ransomware has encrypted your machine. Retrospect makes it easy to monitor backups with an intuitive dashboard view and extensive email reporting.

Step 5: Recovery

If your business is hit with ransomware. do not pay the ransom. There is no guarantee that you'll get your data back. There have been many incidents where ransomware software bugs have prevented file decryption, and NotPetya was specifically designed to only encrypt, regardless of whether a ransom was paid. You should consider that data lost.

"Paying a ransom doesn't guarantee an organization that it will get its data back—we've seen cases where organisations never got a decryption key after having paid the ransom."
- James Trainor, FBI

Instead, if you have a full system backup using Retrospect, erasing your hard drive and restoring from a known safe backup is your best guarantee. With Retrospect Disaster Recovery, you can restore your full system using a clean snapshot prior to the attack.

With Immutable Backups, you know you will be able to recover your backups from the cloud.

Before erasing and going through the full restore, do a small restore of a known infected file to make sure that backup is unaffected. Retrospect can run 16 simultaneous restores, so if you have multiple computers affected, you can restore them all at the same time.

About Retrospect, Inc.

Retrospect Backup has been protecting data for small and medium businesses for thirty years. We support businesses where they are, with local sales representation and thousands of partners across the world, on six continents and seven languages. Contact us at https://www.retrospect.com/contact_sales.

retrospect.com/try