HYCU

EBOOK

Safeguarding your critical data from ransomware threats.

Best practices for backup and recovery.

Ransomware happens be prepared... Be very prepared!

Cybercrime to Cost the World $10.5 Trillion Annually by 2025.

Source https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

Think a ransomware attack can only happen to someone else? ...THINK AGAIN!

No organization is immune to ransomware attacks, and attacks continue to wreak havoc across the globe, crippling companies at an alarming rate. Furthermore, threat actors are not biased to company size, personas or industry verticals and are discovering new and clever tactics to impose their destructive will on IT infrastructures.

In today's ever-changing digital environment, the value of data to business, plus the alarming rise in cyberattacks makes securing and protecting critical data assets one of (if not the) most important responsibilities in the enterprise.

We want to help you out. Our subject matter experts have identified and pulled together some best practices to help you lock down your data and reduce the risk posed by ransomware and other security breaches.

It's as easy as 3-2-1

Formulating a robust backup, copy, and archival strategy is a necessary first step for protecting your most critical data, applications, and systems.

Follow the 3-2-1 rule.

While this is still a good, but traditional approach, it is critical to carefully select the types of backup targets you use with this kind of approach.

03 3-copies of data.

02 On a minumum of 2-separate storage solutions.

01 With 1-medium being offsite, alternate location or in the cloud.

Keep reading for additional considerations.

The power of worm.

Worm.

One of the most useful ways to safeguard backup data is to implement a copy or archival strategy that incorporates WORM (Write Once, Read Many) capabilities. Nearly every cloud-based or on-prem object storage solution offers this capability.

Dare.

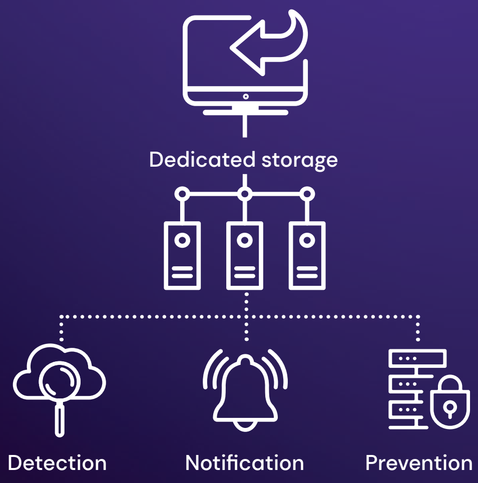
When considering cloud storage providers, look for one that offers security measures such as DARE (Data-At-Rest-Encryption), secured transport technologies (VPNs and HTTPS/TLS), and the AES 256 encryption for data destined for cloud targets.

Blob.

WORM is designed to provide data immutability, meaning it is unchangeable. The technology implements a retention policy that prevents data from being overwritten or deleted over a period of specified time. An Object Storage bucket or Azure BLOB (Binary Large Object) containers are great options for copy or archival backups.

Cover all your on-perm bases.

There are unique situations where on-premises NAS (block) storage options are used for initial backups, before copy and archival. These require distinct consideration.



A best practice is to ensure primary storage targets are dedicated for backups and are not used and mounted to other systems. In addition, look for a backup and recovery solution that offers detection, notification, and prevention features to help safeguard your initial NAS backups.

Create intelligent policy.

Another best practice is to employ a policy-driven approach to protecting critical VMs, data and applications.

This requires some careful thinking about setting the proper policy options around snapshots, backups/copies/archives, data retention, RPO (Recovery Point Objective), and RTO (Recovery Time Objective). Make sure your backup and recovery solutions offer the ability to easily establish and enforce policies to ensure your applications and data are protected with the right degree of consistency.

Backup and recovery policies are not a “one and done” proposition. Things change, so revisit policies periodically to ensure they continue to meet the needs of the organization – and the evolving cyber threats.

Establish secure network accessibility.

Focus on securing the pathways to and from your sources, hosts and targets.

Based on your selected target, you should consider the following:

01 Whitelist setting.

If using an NFS target for primary backups, be aware that the appliance may require a whitelist setting to permit traffic to the network storage from your backup solution.

02 SMB target sharing.

If you opt for an SMB target, you will need to configure an account with access to a share that you create. It is also important to disallow (or not improperly allow) any unauthorized network access to your backup data share – and do not attach it to other machines in your environment.

03 iSCSI consideration.

If you select an iSCSI (Internet Small Computer Systems Interface) target, consider enabling/configuring CHAP (Challenge-Handshake Authentication Protocol) on the target and on your backup solution.

04 Cloud target access.

For cloud object storage targets, you will need to configure accounts or secret access keys to grant access. Then decide if you need an encrypted high-speed isolation connection (configured with peered connection points and appropriate routes), a site-to-site VPN connection, or if you can simply go over the public internet with HTTPS/TLS.

05 Common-sense measures.

Other common-sense measures include not permitting internet access to servers, paying close attention to admin workstation hygiene, and selecting storage targets that provide anti-ransomware features. For added protection, look for a backup and recovery solution that allows the use of a customer or provider-generated PKI (Public Key Infrastructure) certificate.

Check your R-score.

The final step in the process of protecting your backups is to check your ransomware readiness regularly with R-Score.

What is R-Score?

R-Score is a first-of-its-kind assessment tool designed to rate your organization's recovery readiness in the event of a ransomware attack. Developed by HYCU and its partners, R-Score is built from 5-main categories that will assess how well prepared your organization is in dealing with cyber and ransomware threats. Similar in nature to a FICO score, R-Score is based on a scale from 0-to-1,000. The higher the score, the better prepared an organization will be. Additionally, it provides recommendations on how you can make it better.

UNPREPARED PREPARED

0 R-Score 1000

To learn more about R-Score, and how prepared your organization is against ransomware threats, visit getrscore.org

Don’t procrastinate… It could be to late.

Globally, the frequency for ransomware attacks has escalated to occur every 11-seconds with an average recovery timeline of 21-days. Chances are you and/or someone you know just became a victim in the time it took you to read this. That is a scary thought. Your best protection is making sure critical applications and data are safely backed up and isolated from potential intrusion.

Attacks occur every

11 seconds

Average recovery timeline

21 days

Following the best practices outlined in this eBook is a great start.

It is equally important to choose a backup and recovery solution that makes implementing strong data protection simple and flexible. That will make it easier to keep pace with the ever-changing needs of your organization and the evolving threat landscape.

Try HYCU

Do you still have questions about securing your critical data? Reach out to us at **info@hycu.com** or you can experience HYCU firsthand by signing up for a free, no-obligation trial at **TryHYCU**.

About HYCU

HYCU is the fastest-growing leader in the multi-cloud backup and recovery as a service industry. The company provides unparalleled data protection, migration, and disaster recovery to more than 3,100 companies in 78 countries worldwide.
hycu.com

HYCU

27-43 Wormwood Street Suite #650, Boston MA 02210, USA | Phone: +1 617 681 9100 | E-mail: Info@hycu.com |