

YOUR DATA PROTECTION STRATEGY FOR SUCCESS: 3-2-1-1-0

As you prepare your organization to prevent cyberattacks, it's also critical to think through how to recover if the worst-case scenario happens.

Long-term data-backup guidance consistently offered a 3-2-1 strategy – that is, three copies of your data on two different media with one copy stored offsite – but that is evolving. The gold standard is now **3-2-1-1-0**, and here's why that strategy is so important.

Gartner predicts that at least **75%** of IT organizations will face one or more ransomware attacks by 2025.

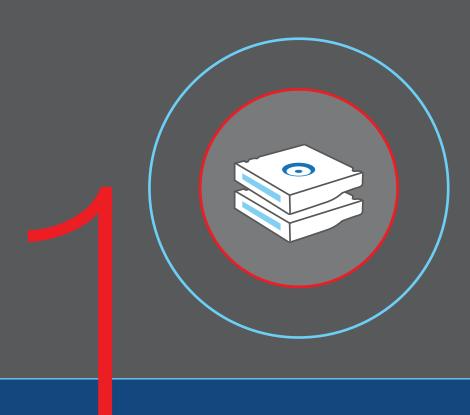
Source



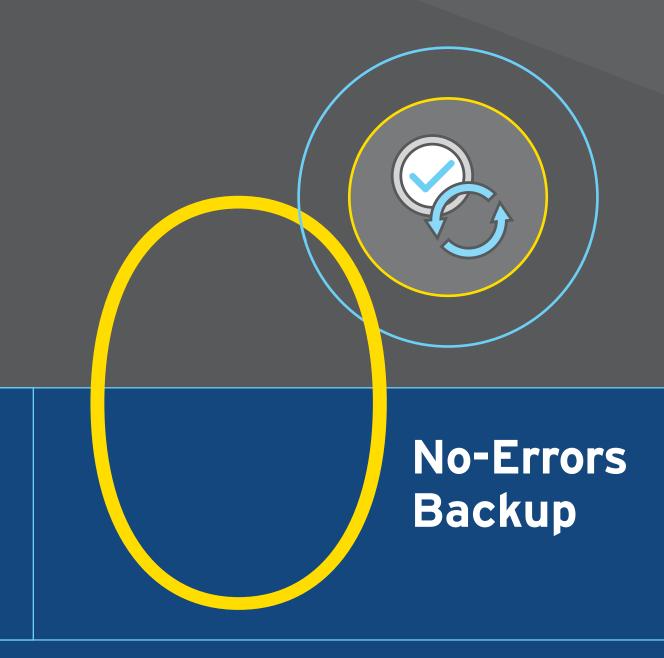




Copy That Is Kept Offsite



Copy That Is Kept Offline



WHY 3 COPIES?

The three copies of your data include your primary data plus two backup copies.

In addition to any rapidly restorable failover copy, there should also be true backups.

WHY VARIOUS MEDIA?

The three copies should be kept on at least two different types of storage media. With so many applications, data, and storage solutions moving to the cloud, it's important to diversify storage between cloud and on-premises storage solutions.

39% of SMB organizations don't have an incident response plan for responding to cyberattacks and data breaches.

WHY OFFSITE?

How your cloud backups are stored is often tied to your cloud provider's data protection strategy. It's best to ensure a copy of that data is virtually isolated from the production network. When preparing for natural disasters, you want to make sure at least one backup copy is physically removed from the main site and transferred to a different zone in case a hurricane, tornado, or other natural disaster strikes.

WHY OFFLINE?

When a backup is physically isolated, ransomware can't get to it. Your air-gapped backup copy is separated from the network where your primary copy is stored. If the primary copy or onsite backup is corrupted or compromised, the offline backup can be used for a restore. This is often a tape backup.

The software air gaps common in object storage go a long way, but nothing beats a physical air gap when you are trying to protect data.

WHY NO-ERRORS?

Copy O is a no-error backup, that is immutable and cannot be altered in any way. It is typically held offline, and can be used to recover from a ransomware attack.

To ensure zero errors are maintained, data monitoring should be done daily and errors corrected as soon as they're identified. A 3-2-1-1-0 backup strategy reduces the impact of a single point of failure. As ransomware attacks continue to rise, plan ahead to make sure your data protection strategy has you covered.

LEARN MORE ABOUT IRON MOUNTAIN SOLUTIONS

Iron Cloud® Data Protection

Iron Mountain has joined forces with leading cloud backup providers Carbonite and Veeam to offer expanded data protection for businesses of all sizes.

- Iron Cloud® Data Protection Powered by Carbonite
- Iron Cloud Backup and Replication
 Powered by Veeam
- Iron Cloud Secure Offline Storage (SOS) with Vault Lock

© 2022 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain USDM-INFO-021422 Incorporated in the U.S. and other countries. All other trademarks and registered trademarks are the property of their respective owners.