Offsite Data Storage
Protecting Backup and Archival Data

David Harris
Senior Government Solutions Manager
Iron Mountain Records Management

IRON
MOUNTAIN®
GOVERNMENT SOLUTIONS

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.

3 — Different Copies of Your Data

2 — Different Media Types for Storage

1 — Copy That Is Kept Offsite

1 — Copy That Is Kept Offline

0 — No-Errors Backup

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.

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.

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

› *Source*

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.

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 0 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.

Risks Come in All Shapes and Sizes

Natural Disasters

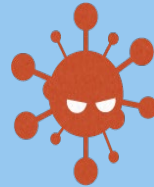Hurricanes, Flooding, Earthquakes, Tornados and Fire

Normal Accidents

Bad Patches, User Error and Hardware Failures

Security Breaches

Malware, Ransom Ware and Attacks by Bad Actors - Foreign and Domestic

Long-Term Storage Growth & Retention Times Increasing

DATA GROWTH

The Global Datasphere will grow from **33 ZBs in 2018** to **175 ZBs by 2025**[1]

ARCHIVAL GROWTH

The growth of **archive data outpaces** the growth of transactional data and high-performance apps

LONGER RETENTION

Archival data retention requirements of **100 years or more** are now common

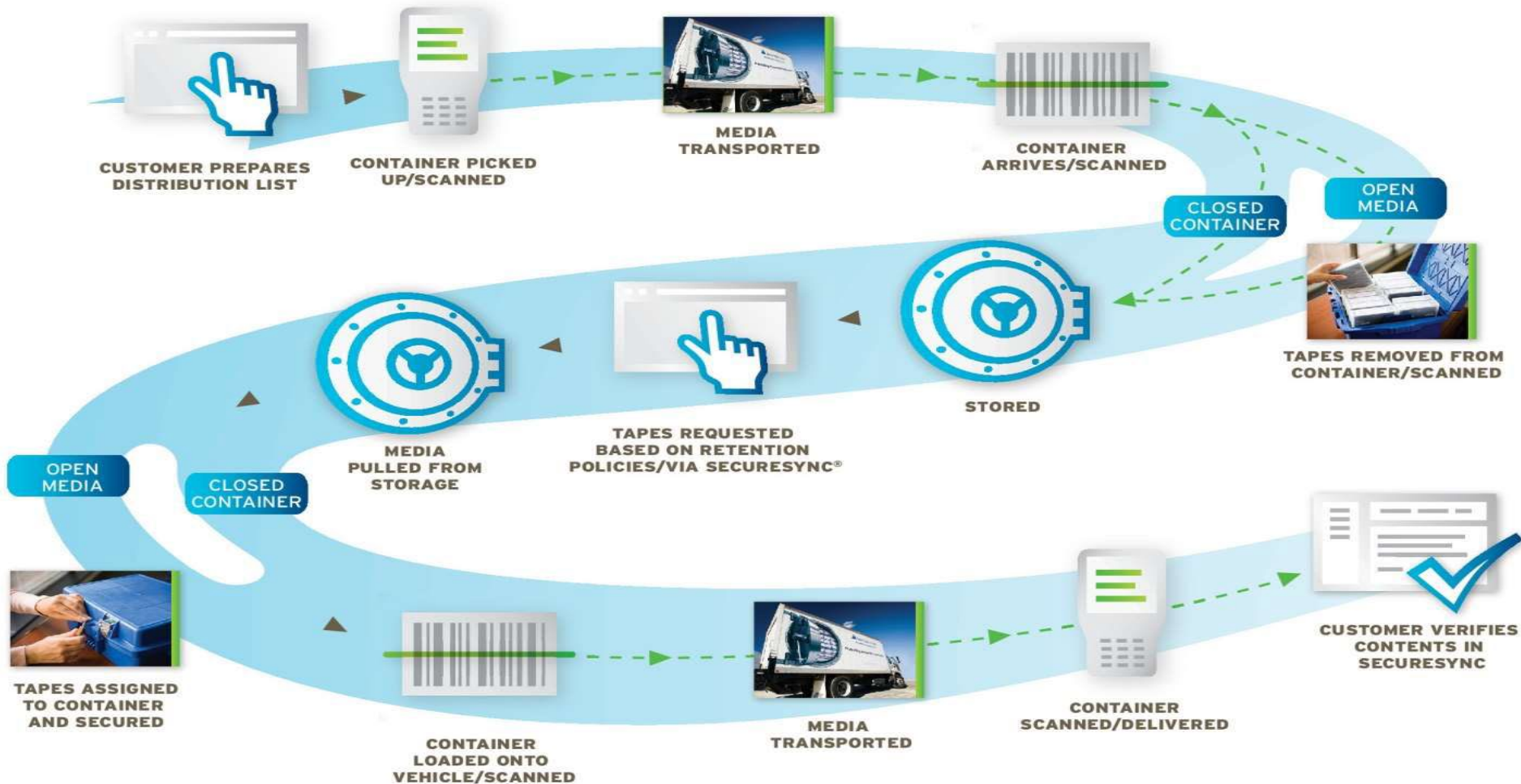Ideally A Multipronged Approach is Best

Offsite Tape Vaulting

Slotted

Closed Container

OFFSITE TAPE VAULTING WORKFLOW

CUSTOMER PREPARES DISTRIBUTION LIST

CONTAINER PICKED UP/SCANNED

MEDIA TRANSPORTED

CONTAINER ARRIVES/SCANNED

CLOSED CONTAINER

OPEN MEDIA

TAPES REMOVED FROM CONTAINER/SCANNED

STORED

MEDIA PULLED FROM STORAGE

TAPES REQUESTED BASED ON RETENTION POLICIES/VIA SECURESYNC®

OPEN MEDIA

CLOSED CONTAINER

TAPES ASSIGNED TO CONTAINER AND SECURED

CONTAINER LOADED ONTO VEHICLE/SCANNED

MEDIA TRANSPORTED

CONTAINER SCANNED/DELIVERED

CUSTOMER VERIFIES CONTENTS IN SECURESYNC

Tape Vaulting – What to Look for

- Secure vehicles and vault

- Employees accurately screened

- Facility maintains correct environmental controls

- Easy to use client interface to manage inventory

- Ability to provide rush and critical delivery of media

- Heritage of Trust and Operational Excellence

- Auditable

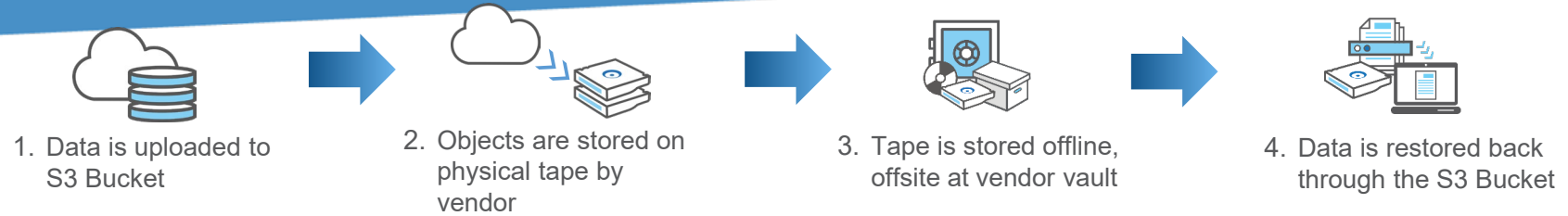- Multiple solution provider – future needs

Secure Offline Storage

- True air-gapped

- Cost-effectively meet compliance requirements

- Ultra-low cost, simplified pricing

- Native integration with existing backup services

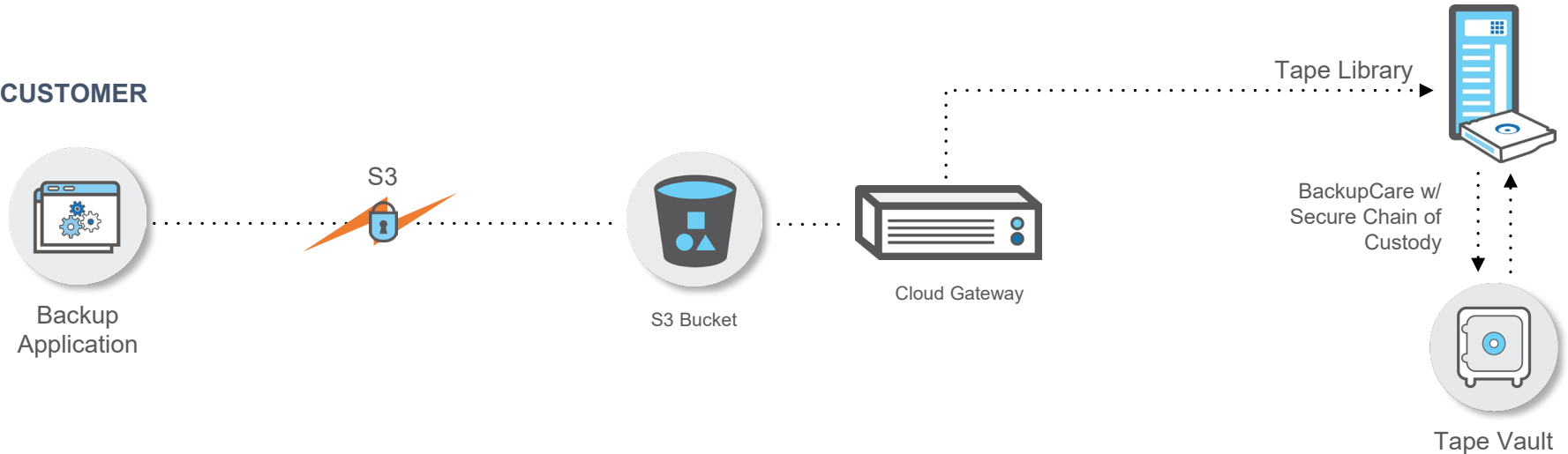- No tape gear or tapes, no technician and no upgrade requirements

SOS Cold Storage: How it Works

Data Journey

1. Data is uploaded to S3 Bucket

2. Objects are stored on physical tape by vendor

3. Tape is stored offline, offsite at vendor vault

4. Data is restored back through the S3 Bucket

CUSTOMER

Tape Library

Backup Application

S3

S3 Bucket

Cloud Gateway

BackupCare w/ Secure Chain of Custody

Tape Vault

Offline Cloud Storage – What to Look For

- Gold copy of valuable data for ransomware recovery
- True "air-gap" takes data offline
- Multi-factor authentication ensures safe recovery
- Easy pricing model; no extra costs to access data
- Virtual compute available to failover and recover
- Clean room data verification to recover from ransomware (add-on service)

Cloud Storage - Archival

Solutions to protect your entire organization

Rapid Recovery

- High availability or DRaaS for your physical, virtual, cloud servers
- Real-time replication across platforms
- Rapid failover to the destination of your choice
- Tier 1 protection to meet optimal RPO & RTO

Data Migration

- Migrate physical, virtual or cloud servers, "any to any"
- Real-time replication across platforms
- Minimal downtime… Minimal risk… Minimal cost…

Long-Term Backup

- Backup physical or virtual servers
- Backup to a local appliance, to the cloud … or both
- Retention policies to meet your needs

Endpoint Protection

- Protection of endpoint devices (Windows, Mac, iOS, Android)
- Centrally managed with features such as backup policies, legal hold, device tracking

Rapid recovery

Data migration

Long-term backup

Endpoint protection

The data protection platform for business
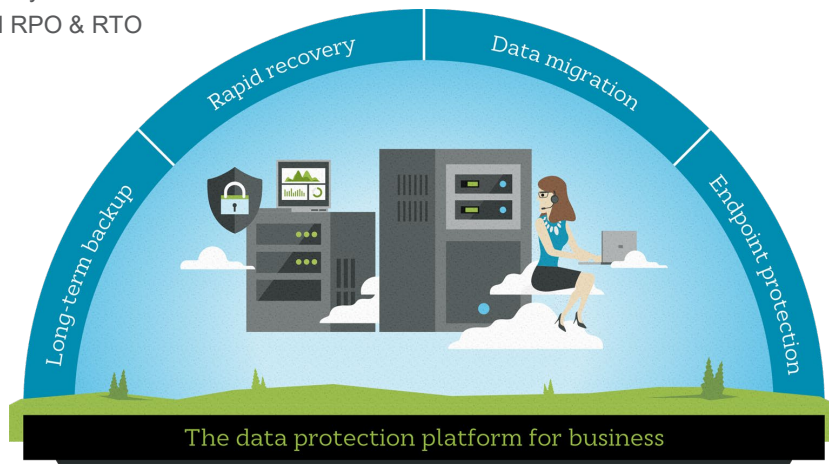
Cloud Storage – What to Look For

- Heritage of Trust & Operational Excellence
- Ultra-secure Data Centers
- Data is always encrypted and never exposed to public internet reducing your risk
- Network locked down so only you have access
- Geo-resilient across multiple data centers for built-in data protection
- Single global namespace with automatic failover
- Advanced network load balancing
- Enterprise-class SLAs for durability, availability and accessibility

SOC 2
Type II

PCI-DSS 3.1

ISO 27001

HIPAA

FISMA
(High)

Vendor Assessment

Work with a vendor who provides you with Today's solution but can provide you evolving solutions and options for Tomorrow.