WHITEPAPER

Retrospect
A StorCentric Company

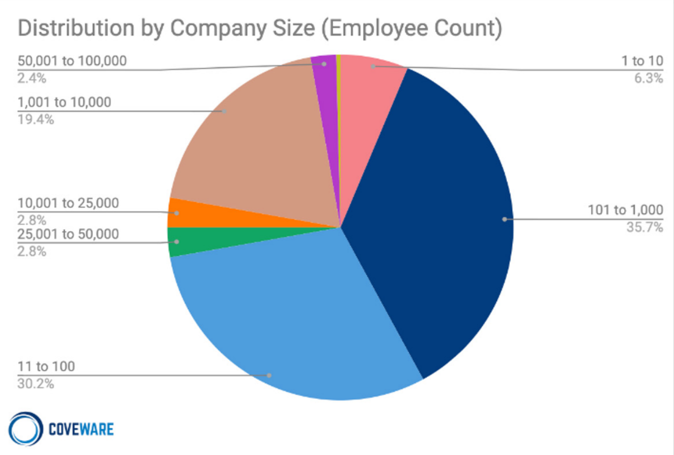
Data Protection for Businesses

Retrospect Backup

Ransomware Protection and Detection: Immutable Backups and Anomaly Detection

Backup Less. Manage Less. Worry Less.

Ransomware is a huge global threat to businesses around the world. The high-profile attacks are well-known: Colonial Pipeline, JBS, Garmin, Acer. But many people now know a colleague whose small business was attacked, because the majority of corporate targets are small and medium businesses. According to Coveware, 72% of targeted businesses have fewer than 1,000 employees, and 37% have fewer than 100. These aren't large corporations with the resources to plan for this vector of attack. These are small businesses that have one or two IT administrators on staff or even no in-house IT. Businesses are projected to pay out $20B in 2021, a 100% Y-o-Y increase for the last four years, and it's only going to get worse with new business models like RaaS: ransomware-as-a-service.



The problem for companies is that their storage is always connected with full access for admins. When ransomware gets the administrative credentials, it has full access too. There is no policy to say that no one, not even the administrator, can change this file for a set amount of time. Ransomware attacks are increasingly sophisticated, having the capability of watching for cloud account credentials, deleting backups and cloud storage, then encrypting everything and demanding a ransom. It's imperative to build defenses against these escalating attacks.

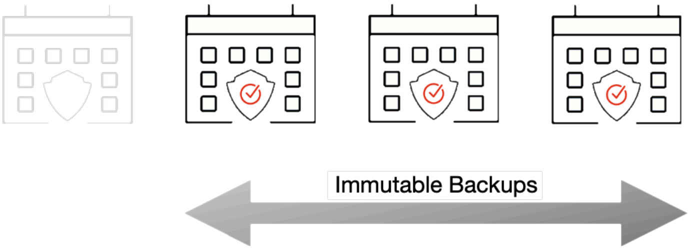
SMBs and large businesses need two layers of defense:

- **Protection**: A backup target that allows them to lock backups for a designated time period for immutable backups.
- **Detection**: An algorithm for detecting changes in the source volumes that is outside of expected variance.

Protection: Immutable Backups

Cloud Object Lock locks files for a period of time. Because cloud storage providers like Amazon S3 control the API, they can add features like Object Lock, also referred to as Write-Once-Read-Many (WORM) storage or immutable storage. This lock is a retention policy for a specific version of a file that is locked from changes from every user, including the administrator. You can think of this as a virtual air-gap in the cloud because there is no way, barring to close the account, to delete that file before the retention date is passed.

Retrospect Backup uses Object Lock to create Immutable Backups. These backups are locked for a specific amount of time. Users can set a retention period for backups stored on supporting cloud platforms. Within this immutable retention period, backups cannot be deleted by any user, even if ransomware or a malicious actor acquires the root credentials.



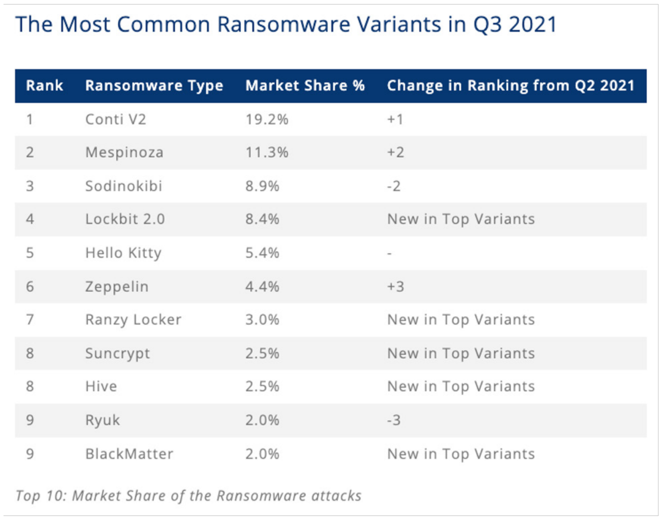
Using ProactiveAI for advanced scheduling logic, Retrospect provides a rolling window of immutable backups, combining forever-incremental backups with point-in-time restores even after the initial backup passes out of the immutable retention policy.

Retrospect Backup's ransomware protection is certified with Amazon S3, Microsoft Azure Blob Storage, Google Cloud Storage, Wasabi, Backblaze B2, and MinIO.

For more information about ransomware protection with Retrospect Backup, see Ransomware Protection.

Detection: Anomaly Detection

Organizations need to detect ransomware as early as possible to stop the threat and remediate those resources. Anomaly Detection in Retrospect Backup identifies changes in an environment that warrants the attention of IT. Administrators can tailor anomaly detection to their business's specific systems using customizable filtering and thresholds for each of their backup policies, and those anomalies are aggregated on Retrospect Management Console across the entire business's Retrospect Backup instances or a partner's client base with a notification area for responding to those anomalies.

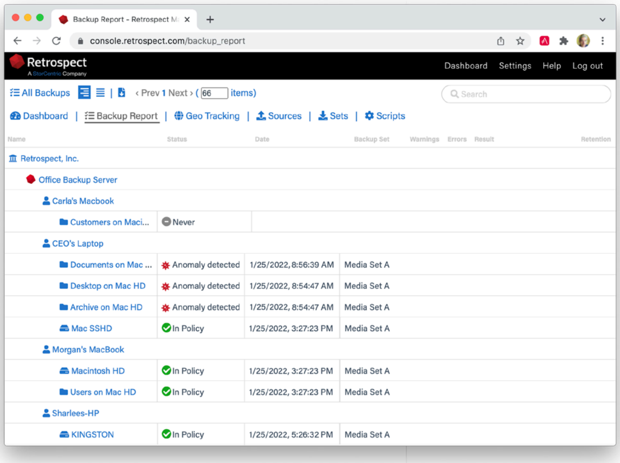


The Most Common Ransomware Variants in Q3 2021

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2021
1	Conti V2	19.2%	+1
2	Mespinoza	11.3%	+2
3	Sodinokibi	8.9%	-2
4	Lockbit 2.0	8.4%	New in Top Variants
5	Hello Kitty	5.4%	-
6	Zeppelin	4.4%	+3
7	Ranzy Locker	3.0%	New in Top Variants
8	Suncrypt	2.5%	New in Top Variants
8	Hive	2.5%	New in Top Variants
9	Ryuk	2.0%	-3
9	BlackMatter	2.0%	New in Top Variants

Top 10: Market Share of the Ransomware attacks

Retrospect Backup detects all of the major ransomware variants using an algorithm that focuses on file metadata anomalies. According to Coveware, the top variants are always changing, with over 50% changing every quarter. The key to detection is combining technologies such as signature detection in processes with file-based irregularities. Using a multi-pronged defense, with immutable backups, anomaly detection, and other security layers, businesses will know when they're being attacked and will have the tools to remediate it and move on.



Name	Status	Date	Backup Set	Warnings	Errors	Result	Retention
Retrospect, Inc.							
Office Backup Server							
Carla's Macbook							
Customers on Maci...	Never						
CEO's Laptop							
Documents on Mac ...	Anomaly detected	1/25/2022, 8:56:39 AM	Media Set A				
Desktop on Mac HD	Anomaly detected	1/25/2022, 8:54:47 AM	Media Set A				
Archive on Mac HD	Anomaly detected	1/25/2022, 8:54:47 AM	Media Set A				
Mac SSHD	In Policy	1/25/2022, 3:27:23 PM	Media Set A				
Morgan's MacBook							
Macintosh HD	In Policy	1/25/2022, 3:27:23 PM	Media Set A				
Users on Mac HD	In Policy	1/25/2022, 3:27:23 PM	Media Set A				
Sharlees-HP							
KINGSTON	In Policy	1/25/2022, 5:26:32 PM	Media Set A				

For more information about anomaly detection with Retrospect Backup, see Anomaly Detection.

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