White Paper

December 2021

DCIG

Mitigating Ransomware through Active Archive Solutions

By DCIG Analyst, Todd Dorsey

DCIG

WHITE PAPER

Mitigating Ransomware through Active Archive Solutions

Executive Summary

Ransomware reigns as today's chief malware threat. Businesses may lose revenue, employee talent, customers, and even close from a ransomware attack. Coupled with the ransomware problem, exponential data growth challenges organizations with gathering, storing, and protecting their data cost-effectively with limited budgets. Strong data governance through active archive solutions helps organizations mitigate ransomware attacks and provides a framework for strategically managing their data growth.

Readers will learn:

- Distinctions between archives, backup and active archives
- Active archive attributes
- Benefits of active archive solutions
- How active archive solutions mitigate ransomware

Contents

DCIG

WHITE PAPER

Mitigating Ransomware through Active Archive Solutions

The Chief Malware Threat

There is little argument that ransomware reigns as the chief malware threat. Reports estimate that a ransomware attack occurs every 11 seconds.[1] And Statista, a global research firm, reported 304 million attacks worldwide in 2020.[2] But it is not just the volume of attacks that make ransomware the chief malware threat; it is the business impact when a successful attack occurs.

Beyond ransomware payment fees, successful ransomware attacks trigger many additional expenses and negative outcomes, including:

- Data loss
- Computer restoration costs
- Business interruption losses
- Brand and revenue losses
- Fines, legal fees, and higher insurance premiums

Ransomware Figures

600%	Increase in malicious emails since COVID-19[3]
54%	of phishing sites used HTTPS[4]
65%	of encrypted data recovered after ransom paid
35%	of encrypted data not recovered after ransom paid
$170,404	Average mid-sized corporation payout
$1.85M	Average organizational cost to recover[5]
$40M	Largest ransomware payout by an insurance company[6]

Added up, the average total expense for business recovery from a ransomware attack: $1.85 million.[4] And the leading expense, greater than the ransomware payout itself, is the median twenty-one-day business interruption costs.[7]

On top of all of this, it is not uncommon for a business to lose C-level talent, lay off employees, or close because of a successful ransomware attack. No wonder that nearly a quarter of C-level IT leaders rank protecting their company against ransomware as their top priority for data security.[8]

The Data Deluge Worsens Ransomware

Coupled with the ransomware problem is another well-known challenge: massive enterprise data growth. Research indicates that the world creates 1.134 million terabytes of data each day.[9] For many organizations, terabytes of data under management have become petabytes and even exabytes.

The largest segment of this data growth is unstructured data such as video, images, documents, emails, presentations, spreadsheets, and similar file types. It is estimated that 90% of the world's data is unstructured and growing at 55-65% each year.[10]

The unrelenting growth of unstructured data challenges the enterprise response to ransomware for two reasons:

"Strong data governance strengthens the enterprise response to ransomware attacks and brings a large number of collateral benefits."

- **Data exposure.** The deluge of data worsens the exposure to ransomware attacks. Each existing and newly created megabyte of data represents growing vulnerability and complexity to protect this data from criminals looking for a hole to exploit. And unstructured data is especially problematic. Problematic because, for ransomware attacks, unstructured file data is easier to locate and then encrypt.[11]
- **Ransomware's impact.** The influx of data increases the potential breadth of a successful attack. Each added file adds to the time required to restore data and return the organization to normal operations.

Unfortunately, while data is growing exponentially, IT budgets are not. This issue is a major disconnect. It forces IT organizations to store, manage, and protect existing data, and deal with the new data coming in with constrained resources. This challenge will only become greater in the time ahead from hi-resolution video, edge computing, 5G, IoT, and new regulatory demands.

Ransomware Attacks—Two Main Types

Locker ransomware: Locks the victim out of their computing device, leaving the underlying data files untouched.

Crypto ransomware: Prevents data access through file encryption. Attacks may steal (exfiltrate) data for double extortion.

Here is the good news: Strong data governance that helps organizations deal with its ever-growing data accumulation strengthens the enterprise response to ransomware attacks and brings many collateral benefits.

This is where active archive solutions can help.

Backup, Archives, and Active Archives

The archiving objective provides long-term storage of files that are not relevant for regular business processes but must be retained for regulatory compliance or other business reasons.

Archived data is not backup data. Backup and archive are different processes with different objectives.

Backups. The backup process makes copies of data, leaving the original data in place. The primary backup objective enables organizations to recover from a data loss incident within a specified data loss window and time frame.

Archives. The archiving process moves inactive files off of primary storage to economy storage such as disk, tape, optical, or the cloud where it typically remains unchanged. Archived data is not backed up. Instead, it is protected through erasure coding or replication.

Active archives. With active archives, the key word is 'active.' The archived data is moved off of expensive primary storage yet remains available to business workflows. This is an 'active' archive, not a 'store and forget' archive.

DCIG

WHITE PAPER

Mitigating Ransomware through Active Archive Solutions

Backup	Archive	Active Archive
A combination of software and backup storage	A combination of software and archival storage (tape, optical, HDD, cloud)	A combined solution of data management software, SSD, HDD, Archival Storage (tape, optical, HDD, cloud)
Copies data to backup storage	Moves inactive data to cost-effective long-term storage	Automates data movement to appropriate storage based on user-defined priorities
Enables organization to recover from a data loss event within a specified loss window and time frame objective	Removes files from the backup stream and frees space on primary storage systems	Leverages the unique attributes of SSDs, HDDs, tape, and the cloud to optimize data storage

Active archives are not limited to a single storage technology, like only tape, optical, or only cloud storage. Active archives can leverage the unique attributes of SSDs, HDDs, tape, and the cloud to optimize data storage for cost, performance, energy consumption, and monetization priorities.

Active Archive Attributes

Active archive implementations vary and are flexible to accommodate different use-cases. An active archive solution integrates intelligent data management software that manages the movement of files between storage systems and media. Transparent to end-users and based on user-defined policies, these solutions manage files across multiple storage tiers as it ages for long-term retention and user accessibility.

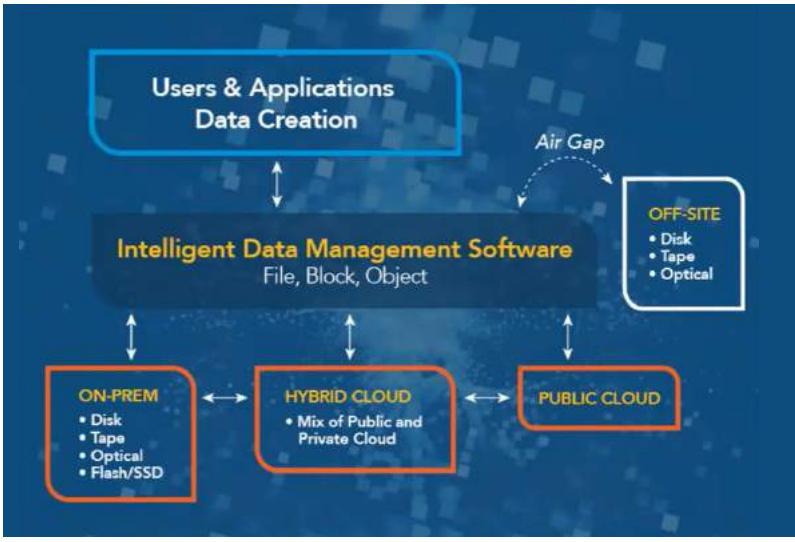
Intelligent data management software. Intelligent data management software serves as a key attribute of active archive solutions. The data management software views its source storage systems as a virtual data repository. The solution provides analytics, insights, and oversight across all tiers of storage. Through meta-data-driven data management and user-defined policies, active archives move data so that it is on the right platform for the right service.

Wide storage integration. Organizations use active archive solutions across storage platforms, technologies, and protocols. Architectures involve data center and remote locations. Solutions integrate multiple storage technologies such as flash, disk, or tape. And, of course, enterprises can leverage public cloud storage for economics or cloud-based services. Active archives are compatible with block, object, and file storage protocols. Active archives work with all of these technologies to manage and optimally place data as it changes from hot to cool, to cold, and back to hot again.

Data migration features. Active archive solutions automate tiering and migration of data between hot and cold stores through the data management software. Prioritizing the needs of the data first, solutions migrate data between tiers for cost, performance, and monetization priorities. The software performs data movement in the background without affecting performance.

Transparent end-user access. End-users experience transparent file access regardless of which pool the data resides in. Unlike traditional archive solutions, active archive users can search, find and access files without administrator intervention. Depending on organization requirements and budget, end-users can retrieve files in:

- Milliseconds – flash or disk
- Seconds – cloud
- Minutes – tape
- Hours or days – deep archive cloud or offline tape



The Active Archive Integrates Intelligent Software and Scalable Storage for the Optimum Archive Solution

Source: Active Archive Alliance 2021 Annual Report

Active Archive Benefits

The most significant advantage for organizations implementing active archive solutions is that they lay a foundation for strategically managing their data growth, now and in the future. This strategic management, even leadership, over their digital assets strengthens their response to cybersecurity threats such as ransomware.

And enterprises implementing active archive solutions enjoy these benefits:

Unlimited scalability. Active archive solutions bring virtually unlimited scalability for handling massive amounts of unstructured data. This scale may be through cost-effective disk, optical, or tape storage, or through archiving data with public cloud storage providers.

Strengthens data management. The data management software component of active archive solutions virtualizes and views data from its source systems as one central repository. These tools can extend to managing offsite replication and disaster recovery locations. The software application presents a snapshot of an organization's data landscape and who is using that data. Armed with patterns and trends of their data

DCIG

WHITE PAPER

Mitigating Ransomware through Active Archive Solutions

landscape, IT decision-makers can make knowledgeable business and storage decisions across multiple storage types and vendors.

Relieves primary storage demand. In an active archive model, a virtual file system includes storage tiers from primary flash or disk to archival, long-term storage. By policy, data management software identifies aged data and migrates it to appropriate storage tiers. The probability of data being accessed again after one month drops off rapidly. Many estimate active data represents a ten percent average of their storage. By only keeping active data on primary storage, organizations free valuable space on tier 1 storage. It creates a lean, organized, and higher performing primary storage infrastructure focused on critical business needs. This reduction in expensive primary storage leads to less maintenance and energy costs.

Reduces backup and disaster recovery storage needs. Many enterprises use backup for storing archive data. This practice costs organizations time and money. Consider that one terabyte in primary storage may add two terabytes to enterprise storage when added to backup and disaster recovery. As data management software reduces the demand on primary storage, backups and disaster recovery storage are also reduced. Backup software, which must scan for incremental changes, speeds up, only scanning active data.

Improves storage budgeting and costs. As organizations understand their data regarding the who, what, when, and why of its creation and use, they can better plan and budget for its growth. Enterprises increase flexibility in deferring storage upgrades and replacements. They also reduce their storage expenses through optimizing necessary storage for cost and performance. These savings free up the IT budget to address other business priorities.

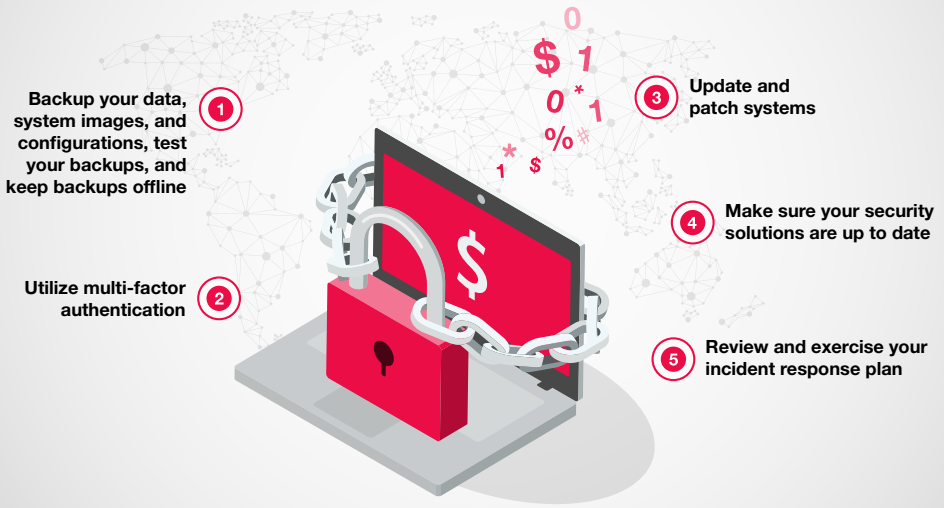
Data monetization. IT organizations are under pressure to not only store data efficiently, but monetize data through fresh business insights and revenue opportunities. Active archives enable organizations to make data available to new workflows and use-cases on-premises and in the cloud; use-cases that bring business intelligence, competitive advantages, and returns on investments.

These strong advantages enable organizations to holistically understand and orchestrate their data throughout the data lifecycle.

Ransomware Mitigation through Active Archiving

Ultimately, cybersecurity software serves as a first-line of defense against ransomware. IT leaders recognize that cybersecurity software alone does not stop all ransomware attacks. And, under an assumption an attack may succeed, these leaders recognize they must protect and recover their enterprise data.

FBI's Best Practices to Minimize Ransomware Risks[12]



Active archive solutions offer permanent and long-term protection for archived data, not only from ransomware, but other forms of accidental or malicious data loss or corruption.

Protects Archive Data. As archived content is typically unchanging, enterprises may use WORM (write once, read many) or Retention Management in "View-Only" mode. This method prevents accidental or malicious deletions or overwrites. Encryption should also be used to protect data from unauthorized use.

Secure offline storage. Active archive solutions may secure archived data through offline storage, providing true air gap protection. Air-gapped meaning there is a physical access gap, and thus the storage media is not online. Once removed from the network, the data cannot be attacked.

Replicates archived data. Archived data may be replicated for additional data protection. This may mean replication to a secure offsite location, or it may involve hybrid cloud or multi-cloud replication.

Leverages cloud storage. Active archive solutions can leverage cloud-based archive storage for protection and recovery from ransomware and other data loss incidents. Public cloud providers offer Secure Socket Layers (SSL) data encryption and multi-factor authentication to control who has access to archived data. In addition, on-premise archive solutions can complement cloud-based archive storage to protect organizations from cloud data breaches.

Supports 3-2-1 data archiving. IT administrators can mitigate ransomware incidents through 3-2-1 archiving. These same principles may be

applied to backup storage. Here best practices recommend three replicated copies are maintained. These replicas should be stored on two different technologies. And one replica should be offsite on air-gapped media. These practices ensure archived data may be recovered if ransomware should compromise active archive storage.

And for active data, archive solutions mitigate ransomware attacks and speed the recovery process.

Maintains data hygiene. Intelligent data management software help organizations understand their data landscape. As organizations identify unnecessary data such as duplicate files or files belonging to previous employees, they may use data hygiene practices to remove these files and mitigate the impact of ransomware attacks. Some data management solutions offer file system activity monitoring to report anomalies in file behavior. Such monitoring may alert IT administrators that a ransomware attack is occurring, enabling them to take counteraction.

Limits file access. Data hygiene and permissions monitoring can limit data for which an employee has authorized access. IT administrators must also utilize multi-factor authentication for protecting an organization's data assets. If a bad actor obtains valid login credentials, these practices limit the scope of the damage.

Reduces ransomware attack surface. Active archive solutions also limit the ransomware attack surface by identifying inactive data and moving this data to secure cloud or on-premise offline archive storage. If ransomware should penetrate an organization's cyber security defenses, a smaller active data set means a smaller attack surface.

Recovers data faster. Active archive solutions bring faster recovery from ransomware incidents. Data management software can identify files that have recently changed through encryption. Recovering these files from backup can be an arduous process taking days and even weeks. Because active archive solutions identify and move inactive data, backups are smaller. Smaller backups mean faster recovery, allowing businesses to return to normal operations much faster with minimal impact to operations.

"Next-generation machine learning and artificial intelligence will create value in archival data through new insights from combining old and current data, insights, bringing competitive advantages and profits."

Cybersecurity experts recommend layered approaches for protecting organizations from malware incidents. These approaches recognize no single defense is ever fully effective. Active archive's capabilities complement enterprise cyber security strategies throughout the data lifecycle, and they provide countermeasures to recover from a ransomware attack should one occur.

Healthcare Industry Benefits from Ransomware Protection through Archiving First

Industries such as healthcare can mitigate ransomware attacks through an archive first model. As an example, medical image files remain unchanged after creation. These images can be archived immediately. When there is a need to view the file, a user may pull a copy down to their local device. Here, the original source remains protected in archive storage. If ransomware should encrypt local, cached copies, they can be replaced with the original archived version.

Conclusion: Active Archives—A Strategic Solution to Ransomware

Data is the lifeblood of organizations and critical for growing revenue and remaining competitive. As stewards of their company's digital assets, IT leaders are tasked with gathering, storing, protecting, and monetizing their data with limited budgets. All the while, bad actors, through ransomware and other malware threats, daily seek to attain a breach in a company's cybersecurity defenses; if these criminals obtain a single success, that breach can ruin a company.

Challenges like ransomware pose must be dealt with tactically and strategically. While FBI best practices above offer tactical responses to daily malware attacks, strong data governance through active archive solutions provide a strategic approach to mitigating and recovering from a ransomware attack should one occur. Results from a recent business survey indicate that data security is the number one driver for investing in data governance initiatives.[13]

Beyond data security, active archive solutions provide a framework that helps organizations oversee and manage their data holistically across the organization wherever it may reside. It enables enterprises to optimize data storage and access throughout its life.

The golden opportunity for organizations implementing active archive solutions are the data monetization possibilities. Today though, research indicates two-thirds of IT and business managers report their organization's data remains untapped. A percentage that increased by ten percent from the previous year.[14] The deluge of data will only widen this gap.

Next-generation machine learning and artificial intelligence will create value in archival data through new insights from combining old and current data, insights bringing competitive advantages and profits.

And this is why enterprises well serve their stakeholders by implementing active archive solutions. Not only for the strategic response to ransomware, but for the many other benefits that strong data governance delivers.

DCIG

WHITE PAPER

Mitigating Ransomware through Active Archive Solutions

About the Active Archive Alliance

The Active Archive Alliance is a vendor-neutral, trusted source providing end users with technical expertise and guidance to design and implement active archive solutions for intelligent data management. The goal of the Alliance is to encourage a multi-vendor effort to promote and align the awareness and technologies needed to meet the rapidly increasing requirements for archival data. Please visit **www.activearchive.com**.

Active Archive Alliance Members and Sponsors

FUJIFILM
SPECTRA
MediQuant
IRON MOUNTAIN
harmony HEALTHCARE IT
ATEMPO
POINT software & systems
Western Digital.
IBM
QSTAR TECHNOLOGIES
Quantum.
STRONGBOX DATA SOLUTIONS
XenData
StorMagic
Legacy Data Access
ELLKAY Healthcare Data Plumbers
IMT SoDA
Sullivan | Strickler

Sources

1. https://www.cbsnews.com/news/ransomware-attack-hackers-70-million-demand-1500-businesses
2. https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/#statisticContainer
3. https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542
4. https://mypage.webroot.com/2021-threat-report.html
5. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
6. https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5
7. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
8. https://www.egnyte.com/governance-trends/2021
9. https://financesonline.com/how-much-data-is-created-every-day/
10. https://www.forbes.com/sites/bernardmarr/2019/10/16/what-is-unstructured-data-and-why-is-it-so-important-to-businesses-an-easy-explanation-for-anyone/
11. https://securityboulevard.com/2018/09/my-take-the-no-1-reason-ransomware-attacks-persist-companies-overlook-unstructured-data/
12. https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf
13. https://www.erwin.com/whitepaper/2021-state-of-data-governance-report8149147/
14. https://www.businesswire.com/news/home/20200901005035/en/New-Industry-Research-Shows-the-Volume-and-Value-of-Data-Increasing-Exponentially-in-the-Data-Age

All references accessed November 2021

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of TOP 5 Reports and Solution Profiles. Please visit **www.dcig.com.**