COMMVAULT

SOLUTION BRIEF

Managing Rapid Data Growth: Lower Costs and Mitigate Risks

Drive storage efficiencies, manage data risks, and comply with policies and regulations

Today more than ever, organizations are relying on data to drive their business. More than 79 zettabytes of data was created or replicated in the world in 2021, and its only continuing to grow.[1] With all of this data growth, organizations are looking towards digital transformation to ensure their data can continue to deliver a competitive advantage but are met with new data challenges, such as identifying and managing data risks, complying with policies and regulations, and reducing data sprawl. If these challenges are ignored, organizations will run the risk of data breaches from cyber threats such as ransomware and could incur costly fines due to compliance breaches or operate at a higher cost.

ROT (redundant, obsolete and trivial) data is the 80 percent or so of unstructured — and unprotected — data that is beyond its recommended retention period and no longer useful to the business. Whatever the case, ROT data can contain sensitive information and may not be maintained appropriately[2]

The average cost of a data breach hits $4.24M globally[3]

In 2021, the SEC brought 697 enforcement actions for non-compliance, totaling approximately $2.4 billion in penalties[4]

Driving storage efficiencies

With the continued daily creation of data, organizations need to find a way to efficiently manage and store their data based on business value. Data that is critical to daily business operations and is frequently accessed, such as proprietary code, should be stored on high-performing tiered storage to optimize performance and data availability, whereas low-value data that is accessed infrequently should be stored on lower-tiered storage to reduce expensive storage costs. In addition, redundant, obsolete, or trivial (ROT) data accounts for around 80% of an organization’s unstructured data and yields no value to an organization. If ROT data is not managed correctly, organizations will experience data sprawl related issues, impacting daily operations such as extended backup windows or increased search times, as there is more data for knowledge workers to search through.

As industry best practices drive organizations to adopt a policy-based Information Lifecycle Management (ILM) approach, many organizations are taking on projects to deal with data sprawl. Without data insights to support ILM, organizations cannot effectively implement retention and disposition policies to align data to the correct tiers and remove unwanted ROT data. This extends projects such as cloud migrations, data consolidations, and infrastructure modernization, meaning increased costs to an organization.

[1] https://firstsiteguide.com/big-data-stats
[2] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-data-remediation-focus.pdf
[3] https://www.ibm.com/downloads/cas/OJDVQGRY
[4] https://www.sec.gov/news/press-release/2021-238

Finally, a rapid increase in data also impacts eDiscovery and compliance efforts. Without the correct means to identify and reduce ROT data, an organization cannot implement an efficient, defensible deletion strategy - retaining large amounts of ROT data. This directly sees larger data sets, meaning increased times for data collection, higher costs for IT, and additional costs spent on external legal teams searching for the right data.

With this rapid data growth, data must be carefully managed to keep storage costs under control and to implement a successful information life cycle management strategy. Without the correct means to reconcile the needs and value of the data to the correct storage tier or remove ROT data, organizations will experience uncontrolled data sprawl, encounter underperforming storage response times, and operate at a higher cost.

Lowering risk

The data landscape is becoming more and more complex to manage. Data itself has become more complex when considering explosive growth, structure, use, and habit of replicating uncontrolled across the organization. The adoption of cloud services, including SaaS offerings, has fragmented the storage across an ever-increasing set of providers, subcontractors, geographies, and jurisdictions. The compliance landscape has similarly accelerated with many national and international regulations, such as Data Privacy (GDPR, CCPA, etc.) being enacted and often conflicting with each other. This environment is understandably overwhelming to most knowledge workers.

There are two main types of data at risk in an organization — business-critical data and sensitive data. If either are compromised, this can lead to significant business disruptions, including downtime, data loss, revenue loss, and damaged business viability.

Business-critical data risks

Business-critical data can be defined as data that is critical to maintaining an organization's daily operations. If this data gets compromised, the entire function of the business is halted. Business-critical data could include proprietary code, trade secrets, or any type of data that an organization deems vital for continued daily operations. Cyber threats such as ransomware or malware look to exploit vulnerabilities in an organization to gain access to this business-critical data, locking access using encryption until a ransom is paid. But threats to business-critical data don't just come from the outside. Internal threats such as accidental or malicious deletions can also cause disruptions. Whether it be an employee having incorrect access and mistakenly deleting files, or a disgruntled employee intentionally deleting files, both can cause damage and threaten an organization's data availability.

Sensitive data risks

Sensitive data can be defined as any data that an organization would not want to be leaked. This most often relates to personal data, including personally identifiable information (PII) that must be managed within regulatory frameworks such as GDPR, CCPA, etc. However, sensitive data could include intellectual property, trade practices, restricted financial documents, medical records, or any other classified information. Unlike typical ransomware, which threatens an organization's data availability, a specialized form of ransomware known as leakware looks to exploit vulnerabilities in an organization to gain access to sensitive data and threatens to leak this information to the public unless a ransom is paid. Although this does not disrupt business continuity, leaking of sensitive data threatens business viability, damaging an organization's reputation, causing financial loss of any potential future revenue opportunities. The outfall of sensitive data leaks can also have further legal implications, with lawsuits and expensive legal costs if the sensitive data contained PII such as medical records or financial documents.

Compliance risk

All organizations are subject to regulations and policies. Public sector organizations are also open to public scrutiny with FOIA (Freedom of Information) or Public Records requirements. Most organizations perform audits and investigations of one form or another. These can all represent compliance, legal or financial risk to the organization.

To support these actions, an organization must prove that they responded to actions in a correct and defensible manner. This requires collecting ESI (electronically stored information) from data custodians and from other sources ensuring trust in the data.

If organizations don't have the ability to properly enforce a defensible deletion strategy (deleting old data to avoid exposure) and a means to follow a proactive preservation method (to guarantee trust in the data for legal purposes), this will only lead to increased risk and cost should compliance breaches be seen.

How Commvault can help

Commvault delivers solutions to proactively protect your business-critical and sensitive data, identify and remediate ROT data, and provide the means to support compliance, investigations, and legal audits - Commvault® File Storage Optimization, Commvault® Data Governance, and Commvault® eDiscovery & Compliance. These solutions can be used independently or combined, enabling organizations to drive actions based on data insights - lowering costs, lowering risks, and supporting compliance. Combining with Commvault Complete™ Data Protection allows for an organization to augment the management of risks such as ransomware and costs through policy-based decisions and actions such as backups and archiving.

Commvault® File Storage Optimization

Commvault® File Storage Optimization provides organizations with cost reduction through the means of valuable data insights and remediation actions, delivering improved storage efficiencies, streamlined cloud migrations and data consolidations, and reduced risks of ransomware. This is achieved with a highly efficient means to survey both live and backup data silos at a massive scale while providing easy management through a single user interface.

Providing insights into an organization's data allows for informed policy-based decisions when aligning data based on Information Lifecycle Management. These decisions allow for cost and risk reduction by enabling organizations to reconcile the costs of storage to the needs and value of the data, while efficiently managing ROT data and reducing data sprawl. Organizations can also use these data insights to identify data risks, such as incorrect file permissions that can result in data breaches of business-critical or sensitive information, and further drive the necessary remediation actions to refine access controls, ensuring only the correct personnel have access. This can extend to orphan data, which can, if not managed correctly, can leave an organization vulnerable to cyber threats such as ransomware.

Commvault® Data Governance

Commvault® Data Governance provides a streamlined framework for risk management to define, find, manage, secure, and remediate sensitive data. This is achieved by profiling and identifying sensitive data across live and backup data silos, providing data insights for review, and the means for collaborative decision making for immediate or workflow-driven remediation to lower data risks such as data leaks. Commvault® Data Governance further supports the management of critical compliance components to adhere to data privacy regulations, including GDPR and CCPA.

Sensitive data can be defined as any data that an organization would not want to be leaked. This most often relates to personal data (including PII) that must be managed within regulatory frameworks. However, sensitive data could include personal health data (PHI), intellectual property, trade practices, restricted financial documents, or any other classified information. The identification and management of this data ensures that any unnecessary sensitive data that exists within an organization's environment is disposed of (to eliminate the chances it is compromised) or ensures the appropriate controls are in place for sensitive data that must remain.

Commvault® eDiscovery & Compliance

Commvault® eDiscovery & Compliance provides a fast, efficient, and scalable data collection solution with means to quickly collect electronically stored information (ESI) - including emails and documents for investigations, legal and compliance matters, and Freedom of Information Act (FOIA) / Open Records requests from immutable backups, assuring a trusted chain-of-custody. This is achieved through the simplicity of a single user interface, providing streamlined data review via advanced keyword search capabilities and self-service eDiscovery & Compliance operations with joint IT and Legal collaboration.

The use of immutable backups provides a proactive preservation method that ensures data cannot be accidentally or intentionally deleted, assuring chain-of-custody of the ESI. It also allows ESI queries and data collection for any relevant custodians and storage locations over a large period of time, for specific terms, metadata, or other advanced search criteria.

As the collected ESI assets are added to Case folders, Commvault provides an additional layer of preservation (as legal hold) to ensure that any Case folder contents collected from backups are not deleted due to backup retention policies. Cases can be refined to add or remove assets depending on relevancy to the matter and can allow teams to classify, tag, and annotate to reflect their analysis of materials. The case can also be exported in a variety of formats used by 3rd parties or external systems.

For those organizations using external legal counsel who charge for the amount of data they review, significant savings can be realized by providing faster results with a more refined (smaller) data set to review and to charge for. This translates into direct savings.

The end result of this process is a discovery process that can be performed quickly, producing relevant results from huge amounts of content generated over long periods of time that can be trusted for their chain of custody in the context of a legal proceeding.

Commvault® Complete™ Data Protection

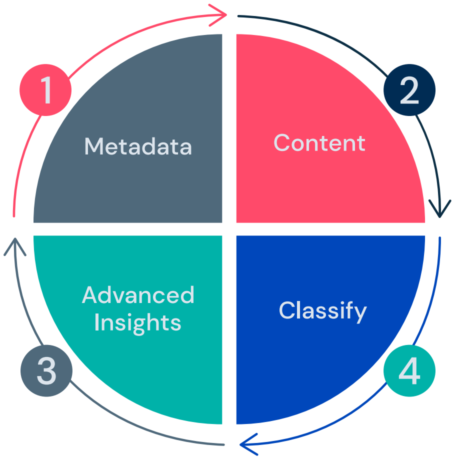
Organizations can also combine with Commvault CompleteTM Data Protection, enhancing backup and archiving strategies driven by information lifecycle management to implement policy-based decisions. The ability to combine backups allows for identified business-critical data to be prioritized and aligned with the highest SLAs to maximize recoverability. Furthermore, multiple copies of this business-critical data can be stored in multiple locations to maximize data availability and redundancy. Backups also enhance an organization's ransomware strategy, mitigating risks by proactively protecting and securing business-critical data prior to a ransomware attack.

Combining with archiving provides an efficient means to automate the retirement of old data, further enhancing information lifecycle management through policy-based decisions. Archiving also benefits ransomware risk reduction by providing a streamlined means to proactively remediate sensitive data from at-risk data silos, preventing potential data leaks while maintaining a trackable means for auditing. Compliance benefits are also seen with policy-based archiving, as defensible deletion can be enforced to safely dispose of redundant data without the impression of deleting evidence.

Insights with intelligence and flexibility

Commvault streamlines the need for data insights using the Commvault 4D Index, a shared component of the Commvault architecture used by all Commvault products. The 4D index catalogs information about data, Commvault operations, and access controls along four dimensions.

- First dimension is the foundational dimension – using email or file metadata to build basic awareness about the assets and how they are accessed
- The second dimension extracts the contents of emails and files to make them all visible through search functions. This includes built-in functions to use optical character recognition (OCR) for image-based documents
- The third dimension uses various advanced techniques for data profiling, including advanced AI/ML algorithms that provide a layer of understanding and context. This is critical to classify document types and sensitive entities such as SSN, credit card numbers, etc. Users can define their own profiles for document types and entities to enhance the index with what matters most to their business
- The fourth dimension allows the index to be enriched with manual content tagging, or with insights from external sources such as databases, applications, and web services. This might include Active Directory, AI services applied to content, Service Now, and other data sources that provide the context for customer-specific decision making and business processes



Of course, Commvault products support the creation, customization, and integration of dashboards, workflows, and integrations with a simple yet powerful, set of tools and APIs packaged with Commvault software.

COMMVAULT®

SOLUTION BRIEF

Highlights

- Identify opportunities to save operating / ownership costs of data
- Support investigations and evidence gathering
- Identify and manage business-critical and sensitive data risks
- Across both live and backup data
- Immediate or workflow driven remediation with joint decision making
- Single pane of glass user interface – Commvault Command Center™

For more information, visit **www.commvault.com/activate >**

COMMVAULT® Be ready™

commvault.com | 888.746.3849