White Paper

Backup and Disaster Recovery as a Service: Driving New Data Protection Opportunities for Healthcare Organizations

Sponsored by: Commvault and Mercy Technology Services

Lynne Dunbrack Phil Goodwin

August 2018

IDC OPINION

The data protection market is highly dynamic, driven by new application workload deployments and cloud capabilities. Healthcare organizations are embracing cloud computing and are more willing to move certain workloads, such as IT operations, to the cloud. Healthcare IT executives acknowledge that managed service providers know more about datacenter security than their own organizations, especially when it comes to cybersecurity. Given the rise of ransomware attacks, a solid data protection plan that combines backup as a service (BaaS) and disaster recovery as a service (DRaaS) is an imperative. This paper examines the growing need for data protection services, including BaaS and DRaaS. It also looks at the role of Commvault and its customer Mercy Technology Services, which is using Commvault data protection solutions to offer BaaS and DRaaS to other healthcare organizations.

Healthcare Data Is Growing Exponentially and Must Be Protected

The volume of healthcare data has grown exponentially as a result of investments in healthcare IT and medical advances such as more sophisticated imaging machines and genomics. A typical patient will generate 1,200 terabytes of data over his or her lifetime. Increasingly, data will be generated and aggregated by consumers themselves. By the end of 2020, 25% of data used in medical care will be collected and shared with healthcare systems by the patients themselves — a concept referred to as "bring your own data." Thus, healthcare data will be increasingly complex, with more than 80% of the world's healthcare data unstructured, making it more difficult to analyze, manage, and protect.

Larger volumes of electronic health data create an irresistible target for cybercriminals who perceive healthcare organizations as a soft target compared with financial services companies and retailers. Historically, healthcare organizations have invested less in IT, including security technologies and services, than organizations in other industries, thus making themselves more vulnerable to successful cyberattacks. The value of health information, which can be used to commit medical fraud, is surpassing the value of social security and credit card numbers on the black market, increasing the attractiveness of stealing health information. Nearly every week, another healthcare organization reports a serious privacy and security breach that has compromised tens of thousands to millions of consumer health records.

In the past, these breaches occurred because of loss or theft of a laptop or mobile device. Today's breaches involve cybercriminals representing sophisticated organized crime rings and, in some extreme cases, nation-states engaging in cyberespionage. These types of attacks require a level of cybersecurity expertise that is often out of reach for healthcare organizations because security professionals are in such demand across all industries. The ability to attract and retain cybersecurity professionals is particularly problematic for smaller community and critical access hospitals that cannot afford the competitive salaries that larger healthcare organizations, companies in other industries, and even IT suppliers and service providers can afford to pay.

IT organizations are also under increasing pressure to focus on IT initiatives that meet the demands of value-based health and digital transformation, thus shifting attention away from important foundational tasks such as backup and recovery. New care delivery, reimbursement, and business models are rapidly evolving to address the healthcare industry's objectives to reduce costs and improve quality of care as well as patient and clinician satisfaction. Legacy infrastructure simply cannot keep up with the pace of change. Forward-thinking healthcare organizations are modernizing their infrastructure by accelerating their adoption of 3rd Platform technologies, including cloud, which will play a vital role in digital transformation.

Public cloud and hybrid IT infrastructure offers healthcare organizations a way to deploy, manage, and refresh IT with an eye to increasing operational efficiencies and reducing IT costs. However, as healthcare organizations modernize their infrastructure and embrace hybrid IT, their backup and data recovery strategies need to be updated as well. Another challenge facing healthcare organizations is that infrastructure advances are outpacing the investment cycles of healthcare organizations. Outsourcing datacenter operations, including BaaS and DRaaS, allows healthcare organizations to focus on digital transformation and their core competencies surrounding patient care.

Backup as a Service and Disaster Recovery as a Service Defined

BaaS and DRaaS are component building blocks of the larger data protection as a service (DPaaS) market. According to IDC, BaaS suppliers offer, maintain, and manage a cloud repository where backup data sets can be stored. On-demand cloud resources for recovery may be available from suppliers but are not required by our definition. Restores usually involve copying the data back to a recovery environment. Suppliers must provide a data mover as part of the solution. The repository is often deduplicated and should include encryption for protected health information in motion and at rest. The solution may or may not include a purpose-built backup appliance (PBBA) either on-premise or in the cloud.

DRaaS must include on-demand resources (compute, network, storage, security, and authentication) to facilitate a full workload recovery in the cloud environment. Suppliers may offer a range of associated professional services, from minimal "do it yourself" plans to "white glove" service, including threat assessments, runbook development, and recovery assistance in the event of a disaster. Data movers, as-a-service enablers, and DR test capabilities (even for "do it yourself" environments) must be included in DRaaS.

Key Benefits of BaaS and DRaaS

IDC's April 2018 *CloudView Survey* revealed that 72.4% of providers and 78.4% of payers agree or strongly agree that cloud services offer better business continuity and disaster recovery than traditional technology provides. Benefits of BaaS and DRaaS include:

- **Improved reliability of data backup and speed of data recovery that drive the achievement of recovery point objective (RPO) and recovery time objective (RTO) metrics.** RPO refers to the point in time in the past to which you will recover. RTO refers to the point in time in the future at which you will be up and running again. BaaS ensures that backups are automatically done on a regular schedule, minimizing lost data in the event of any type of disaster and thus helping the IT organization achieve RPO KPIs. DRaaS facilitates and expedites the activation of recovery services, thus improving data recovery and getting mission-critical systems back online.

- **Lower IT costs.** By leveraging BaaS and DRaaS, healthcare can reduce or eliminate the need to own and operate expensive backup and recovery infrastructure. These services also make better use of IT resources, including staff, and reduce the complexities associated with managing backups, thus reducing the total cost of IT ownership.
- **Reduced risk.** BaaS provides a more secure method of file transfer and eliminates tape-based storage, which can often fail and from which it takes a long time to recover large volumes of data. More efficient, automated backup services improve compliance with data storage requirements.
- **Smarter BaaS and DRaaS.** BaaS and DRaaS now include embedded artificial intelligence (AI) and machine learning (ML) algorithms to make these and other data operational processes smarter and more efficient. Solutions that include AI and ML may be able to proactively protect data against such threats as cyberattacks or extreme weather events.
- **Protection of valuable data in the event of a cyberattack and natural disaster.** Healthcare data is particularly vulnerable against cyberattacks because healthcare organizations historically have not made the requisite investment in security and data protection technologies. Natural disasters can strike a dual blow — devastating healthcare facilities and datacenters when the local community needs access to care and patients' health records the most. Housing backups and archives in different geographic locations provides access to critical data in the event of a local natural disaster such as a hurricane or tornado. Airgaps (i.e., a physical or manual break between primary and secondary data stores as well as a break in the business process of copying data between the two) between live systems and backup provide an additional layer of protection against system infiltration and data exfiltration in the event of a security breach.

The Emerging Opportunity for Managed Services and Niche Specialty Providers

Healthcare data volumes are growing exponentially with structured and unstructured data adding to the complexity of protecting sensitive health information. Advances in genomics, AI, and personalized medicine are accelerating, thus making data growth planning all the more difficult for healthcare IT organizations. As a result, healthcare organizations are beginning to turn to cloud storage options, which can scale up and down based on dynamic data storage requirements. In fact, according to IDC's April 2018 *CloudView Survey*, 28.9% of providers and 36% of payers expect to move storage capacity to a public cloud within 24 months.

Healthcare organizations are also moving other workloads, including those that involve protected health information, to the cloud. They want BaaS and DRaaS integrated with their major cloud providers. IDC sees parallel growth of data moving to private, public, and hybrid clouds along with XaaS offerings. In turn, this increased growth of cloud adoption by healthcare organizations and data volume in the cloud is creating the next evolution of cloud service offerings and the emergence of managed services and niche specialty vendors offering backup and recovery as a service to enhance their service offerings.

Healthcare organizations are also offering backup and recovery as a service to business units and/or divisions across the enterprise both internally and externally. These new providers of BaaS and DRaaS understand the nuances of the wide variety of healthcare data types, how complex healthcare data models are defined, and the importance of protecting healthcare data in compliance with local, state, and federal privacy and security regulations. For example, they are willing to sign business associate agreements with their customers as required by the U.S. Health Insurance Portability and Accountability Act (HIPAA).

Considering Commvault and Mercy Technology Services

Commvault (Nasdaq: CVLT) was founded in 1996. Over the past 22 years, the company has experienced significant growth, with 2,400 employees and offices in 6 continents. Commvault's core offering is an enterprise-class data management platform that provides data protection, recovery, and search capabilities to midlevel and enterprise-level organizations on-premise or in the cloud. Commvault's healthcare solutions leverage Commvault's data management platform to provide a single platform to manage clinical and business data assets across the enterprise. Core functionality of Commvault's health data management platform encompasses backup, recovery, and archiving; application and data management; mobile and endpoint data protection; search and ediscovery; and cloud services. Commvault provides a complete view of all stored data regardless of whether the data is stored on-premise or in the cloud. Commvault has more than 2,500 healthcare customers worldwide.

MTS Partners with Commvault to Provide Data Protection Services to Healthcare Organizations

Mercy (**www.mercy.net**) is a nonprofit Catholic healthcare system that includes 40-plus acute care and specialty hospitals in four states (Arkansas, Kansas, Missouri, and Oklahoma). The organization includes more than 700 physician practices and outpatient facilities; 40,000 employees; and 2,000 Mercy Clinic physicians. Mercy's mission is to provide the best care possible through the health system's hospitals, physician clinics, outpatient facilities, outreach ministries, and other health and human services. Mercy was named one of the top 5 large U.S. health systems in 2016, 2017, and 2018. To facilitate this clinical mission, Mercy centralized IT operations, and in 2010, the health system consolidated IT infrastructure in its $60 million datacenter, which was opened by Mercy Technology Services (MTS). The investment supported Mercy's early adoption and enterprisewide deployment of Epic's electronic health record (EHR) system. Since 2014, MTS has been sharing its healthcare expertise and IT solutions by offering Epic EHR as a service, data analytics, and consulting to small and midsize hospitals outside of Mercy.

In 2015, MTS evaluated Commvault data protection capabilities based on recommendations from its storage provider, which also used Commvault solutions. MTS not only needed backup and recovery capabilities for its 10,000 virtual machines but also needed to be able to back up individual servers. In addition to the centralized datacenter, MTS provided services to hospitals running on-premise systems. Therefore, a single solution to address the data protection needs of the datacenter and remote sites was attractive to MTS.

Scott Richert, vice president of infrastructure at MTS, described the Commvault solution as having a "solid mature architecture and easy-to-use set of configuration tools. It was exactly what we needed and less expensive than the alternatives."

Before MTS began using Commvault solutions, it sometimes took hours to stand up a virtual machine. Now that task takes only minutes using Commvault's solutions, thus creating a significant net gain in recovery capabilities and the opportunity to provide data protection services as part of MTS' service capabilities to external customers.

In addition to deploying Epic EHR as a service, MTS offers cloud and managed hosting services. Offering BaaS and DRaaS thus became a natural extension of the services MTS provides, especially to customers that were in technical debt and that needed help from a tier 4 datacenter. The combination of hosting services and backup services creates an opportunity for disaster recovery services and more recovery options. For example, MTS can stand up hot virtual machines very quickly in the MTS datacenter to expedite the disaster recovery process.

As MTS became more agile using Commvault's BaaS and DRaaS solutions, it contemplated offering these services to its own Epic-as-a-service customers. In 2017/2018, MTS approached Commvault about MTS becoming a BaaS and DRaaS provider. Commvault understood and respected MTS' growth path and worked very closely with MTS on its journey from Commvault customer to service provider.

Most of the Epic-as-a-service customers tend to be small to midsize hospitals, but for BaaS and DRaaS, any size healthcare organization can take advantage of these expanded data protection services by MTS. MTS offers three levels of service options — bronze, silver, and gold — to provide additional support (e.g., cold versus hot standby recovery).

BaaS and DRaaS combined with healthcare expertise differentiates MTS from other managed services and niche specialty vendors. MTS staff as healthcare IT professionals are very familiar with backing up healthcare databases, working with healthcare applications, the quirks of the applications, and what they will or won't tolerate. They also understand that while backup capabilities are important, the ability to activate recovery resources quickly to maximize recovery speed is essential for clinical operations and patient safety.

Challenges and Market Opportunities

The market challenges that customers of Commvault and MTS face can also present opportunities for the two organizations:

- Data volumes are growing exponentially, putting healthcare organizations at greater risk in the event of a natural disaster or cyberattack unless they have a solid data protection plan that includes backup and disaster recovery services.
- There is the increased threat of mission-critical healthcare applications and electronic health records being encrypted by a ransomware attack and healthcare organizations being extorted for ransom payments to gain access to their own data. In extreme situations, lack of access to patient health information could mean the difference between life and death. Uptime, computing performance, access to vital clinical and operational data, and reliability are critical considerations when evaluating technology to be deployed in a healthcare setting.
- Healthcare IT organizations are strapped, in terms of both staff and financial resources. Careful consideration of the total cost of ownership is essential. More efficient IT operations will enable healthcare organizations to reinvest IT cost savings in more innovative technologies, security, and data protection services.

Conclusion

Healthcare organizations should think about data protection in terms of not only the technical risk but also the business risk of a system failure. What happens to patient care and other services in the event of a system outage, whether it's the result of human error or a cyberattack? What happens if access to mission-critical applications, such as EHRs, is disrupted? What about the damage to the healthcare organization's reputation if patients are turned away because manual or semi-automated processes can't keep up with the volume of patients handled when data and healthcare IT systems are online?

Healthcare data is increasingly distributed across different locations and IT models. The ability to use a single software platform for the datacenter or a remote facility will help reduce the complexity of data protection across the enterprise and speed up recovery time and improve resiliency — critical aspects of data protection services. Also, point solutions typically cost more and require more resources and staffing than a single software platform. Healthcare organizations evaluating data protection service providers should consider the practical aspects of recoverability, such as what other technology services the service provider can offer. Examples include consulting, hosting, and healthcare expertise. Niche specialty vendors understand the critical nuances of managing and protecting personal health information, which is essential for complying with today's more stringent security and privacy regulations.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com