Technical Brief Series

How to Evaluate the Data Security Capabilities of Cloud-Based Services

Executive Summary

One of the critical issues in evaluating cloud-based services is data security. Cloud-based services today can be compared to Internet banking. Consumers were initially afraid that online banking would make them more vulnerable to fraud or identity theft. Now that online security technologies have improved, online banking is actually safer than getting paper statements in the mail.

Likewise, using a cloud-based service supplier instead of operating your own internal system can be a major step toward becoming liberated from serious security issues. However, you must choose your provider wisely. Suppliers must demonstrate that they have the optimal technologies, infrastructures and processes in place to ensure data security. And each healthcare facility needs to require evidence that patient data is protected at all levels and stages of the workflow – from duplicate disaster recovery copies and physical protection of the data center to data transmission, storage, and user access.

It's important to understand the four key components of data security: availability, integrity, confidentiality, and traceability. Data availability ensures continuous access to data even in the event of a natural or man-made disaster or events such as fires or power outages. Data integrity ensures that the data is maintained in its original state and has not been intentionally or accidentally altered. Data confidentiality means information is available or disclosed only to authorized individuals, entities, or IT processes. And data traceability means that the data, transactions, communications, or documents are genuine and that both parties involved are who they claim to be.

All components of data security must be maintained at the following three levels:

1. The physical infrastructure of the data center;
2. The hosted application that manages data; and
3. The policies and procedures to maintain continuous security in the cloud.

1. Physical Security at the Data Center

The data center must supply a secure physical hosting environment. This typically includes:

- Redundant utilities, particularly power supply and air conditioning.
- Protection against fire with appropriate extinguishers in each computer room, as well as emergency power-off switches.
- Specially equipped ventilating and air conditioning systems. While temperature is an important factor, equipment must also be protected from external heavy pollution (such as smoke from a nearby fire).
- Windowless rooms for servers and storage equipments.
- Access control to enter the data center. This includes a security guard at the building entrance, no unscheduled visits, a single entrance to the most sensitive area of the data center, and surveillance cameras around the building and at each entrance. Employee access should be monitored through the use of badge-based entry, security guards, and cameras that monitor all building entrances and exits. Extra authentication should be required to access sensitive areas within the building where patient data is stored. Ask to see the supplier's security policy and find out how employees' online access to data is monitored.

Data center designs can be broken down into four tiers. Most hospital data centers are a Tier 1 or Tier 2. In Tier 3 and Tier 4, cloud service providers are best equipped to make the significant investment required to guarantee higher security.

Tier Level	Requirements
1	• Single non-redundant distribution path serving the IT equipment • Non-redundant capacity components • Basic site infrastructure that guarantees 99.671% availability
2	• Fulfills all Tier 1 requirements • Redundant site infrastructure capacity components that guarantee 99.741% availability
3	• Fulfills all Tier 1 and Tier 2 requirements • Multiple independent distribution paths serving the IT equipment • All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture • Concurrently maintainable site infrastructure that guarantees 99.982% availability
4	• Fulfills all Tier 1, Tier 2 and Tier 3 requirements • All cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems • Fault-tolerant site infrastructure with electrical power storage and distribution facilities that guarantee 99.995% availability

2. Application-Level Security Design

Application-Level Availability

Any application should start with a secure and reliable storage mechanism:

- The cloud service provider should maintain at least two copies of ingested data, thus reducing the risk of data loss. One of the two copies is made on removable media so it can be stored at another location—in case a disaster impacts the data center. The system should ensure that the two copies are permanently synchronized.
- Database is stored on RAID-10 (1+0) disk system. RAID-10 provides high availability and performance when there is a need to reconstruct data in the case of disk failure.
- Data is stored on RAID-6. While this type of RAID is slower to reconstruct in case of disk failure, it offers excellent reliability with a higher ratio of usable storage/physical storage.

One of the often overlooked areas of data security is authentication procedures. It is not enough to maintain two copies of patient data—the cloud service provider must also have a validation process that ensures that each copy of the data maintains its integrity. Damaged files must be able to be detected and reconstructed. Responsibility for maintaining data integrity should be clearly defined as part of any contract with a service provider.

Application-Level Integrity

Application-level signatures should be computed for every document and kept in the database. The encryption mechanism used to ensure confidentiality during the TCP/IP transmission includes an integrity check that prevents the risk of data corruption.

A typical integrity check is the use of hashes. Hashes can be included in a signature to ensure authenticity. In such a case, the signature contains the document hash encrypted with the sender private key and the public key to allow decryption. It also points to the certification authority. The key used to encrypt the data should be stored (encrypted) with the data itself. If data has been modified intentionally, or accidentally, data decryption would then fail. This protection also prevents the sending of corrupted data to clinicians and other users.

Multi-Level Data Confidentiality

Data protection is required at both the application and network level. Communication between healthcare sites and the data center is performed with SSL-based encryption at the application level to ensure end-to-end protection between the service access point and the data center. This encryption ensures that none of the employees of the network provider can access data. It also prevents data from being viewed while it is being carried over the Internet to an end user's viewing software. SSL can implement several encryption algorithms, the most common being AES, 128 bits key length encryption.

Access control also combines two levels of restriction:

- Site-level access control defines which originating sites can access data. A default configuration specifies that data ingested by an originating site may only be accessed by the same site. Any other access, such as queries from other sites or from the web portal, must be specifically set up. This restriction applies to most imaging IT clouds that require a local server as point of access.

- A user profile specifies access to both features and data. Access rights for a given user can also be defined for patients and types of studies.

Secure Connection to the Cloud

Secure access requires the data center to equip its Internet connection with the following:

- Firewalls to control network transmissions based on a set of rules that protect networks from unauthorized access.

- Demilitarized Zone (DMZ) - A physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, providing security from external attacks.

- Permanent updates to anti-virus software with the latest virus signature databases.

To guarantee secure data exchange, the connection between the data center and a customer site is usually made through an SSL-encrypted tunnel.

3. Policies and Procedures to Maintain Security

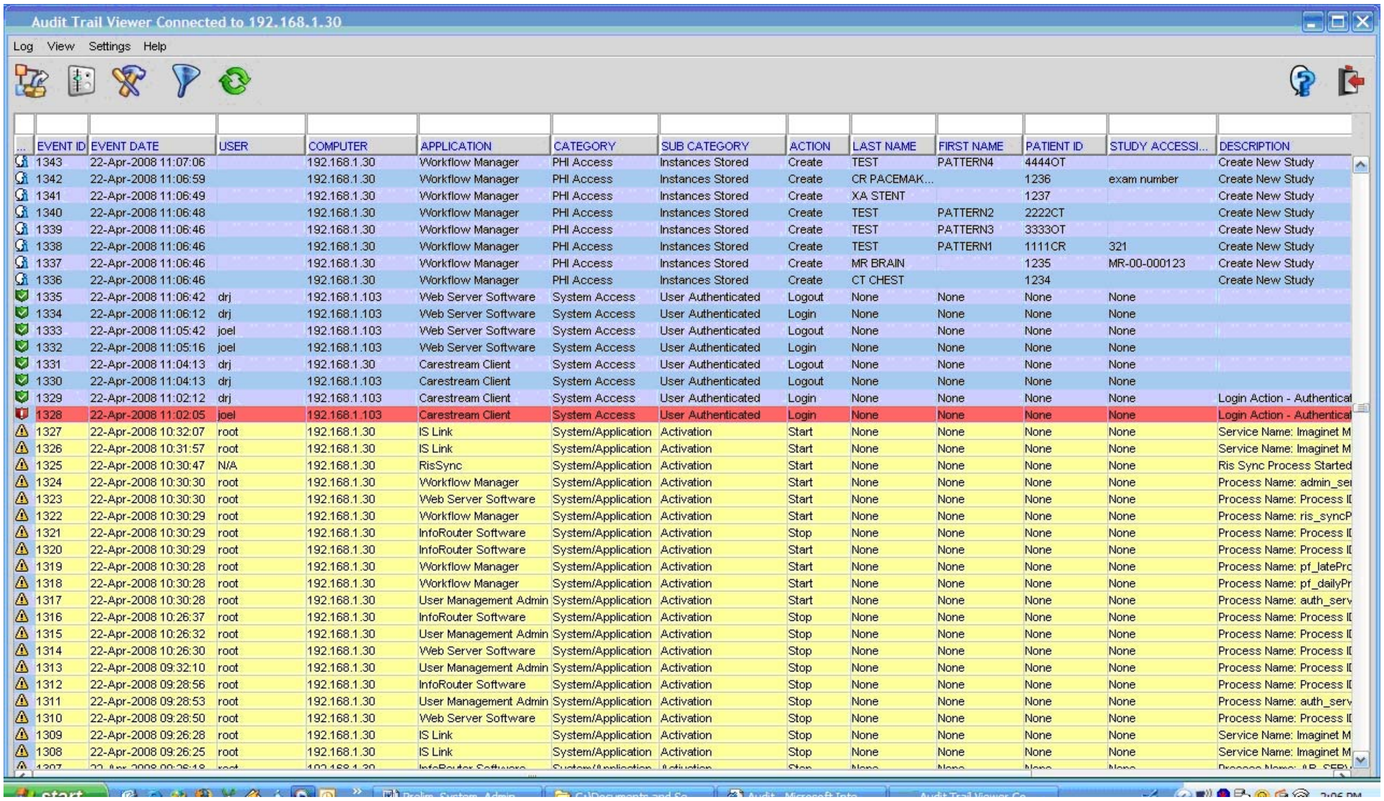
Beyond physical and application-level design, proper policies and procedures are required to maintain on-going security for cloud-based services, completing the traceability component of the security design.

Establishing an Audit Trail

While data privacy addresses who can access data and what a user can do, a comprehensive auditing function is needed to track all patient health information (PHI)-related activities, warnings, and failures that occur in the system.

Using the audit viewer tool, security administrators can exclude events from auditing and define filters to manage information collected by the system. This information can be used to trace the source of selected changes to information in the system, as well as to detect unusual system activity.

The following screenshot of an audit trail viewer shows warnings in yellow, red highlights to indicate critical events, and blue represents normal events. In the example, the red row indicates a connection attempt with the wrong password.



Audit Trail Viewer Connected to 192.168.1.30

...	EVENT ID	EVENT DATE	USER	COMPUTER	APPLICATION	CATEGORY	SUB CATEGORY	ACTION	LAST NAME	FIRST NAME	PATIENT ID	STUDY ACCESSI...	DESCRIPTION
ℹ	1343	22-Apr-2008 11:07:06		192.168.1.30	Workflow Manager	PHI Access	Instances Stored	Create	TEST	PATTERN4	4444OT		Create New Study
ℹ	1342	22-Apr-2008 11:06:59		192.168.1.30	Workflow Manager	PHI Access	Instances Stored	Create	CR PACEMAK...		1236	exam number	Create New Study
ℹ	1341	22-Apr-2008 11:06:49		192.168.1.30	Workflow Manager	PHI Access	Instances Stored	Create	XA STENT		1237		Create New Study
ℹ	1340	22-Apr-2008 11:06:48		192.168.1.30	Workflow Manager	PHI Access	Instances Stored	Create	TEST	PATTERN2	2222CT		Create New Study
ℹ	1339	22-Apr-2008 11:06:46		192.168.1.30	Workflow Manager	PHI Access	Instances Stored	Create	TEST	PATTERN3	3333OT		Create New Study
ℹ	1338	22-Apr-2008 11:06:46		192.168.1.30	Workflow Manager	PHI Access	Instances Stored	Create	TEST	PATTERN1	1111CR	321	Create New Study
ℹ	1337	22-Apr-2008 11:06:46		192.168.1.30	Workflow Manager	PHI Access	Instances Stored	Create	MR BRAIN		1235	MR-00-000123	Create New Study
ℹ	1336	22-Apr-2008 11:06:46		192.168.1.30	Workflow Manager	PHI Access	Instances Stored	Create	CT CHEST		1234		Create New Study
✓	1335	22-Apr-2008 11:06:42	drj	192.168.1.103	Web Server Software	System Access	User Authenticated	Logout	None	None	None	None	
✓	1334	22-Apr-2008 11:06:12	drj	192.168.1.103	Web Server Software	System Access	User Authenticated	Login	None	None	None	None	
✓	1333	22-Apr-2008 11:05:42	joel	192.168.1.103	Web Server Software	System Access	User Authenticated	Logout	None	None	None	None	
✓	1332	22-Apr-2008 11:05:16	joel	192.168.1.103	Web Server Software	System Access	User Authenticated	Login	None	None	None	None	
✓	1331	22-Apr-2008 11:04:13	drj	192.168.1.30	Carestream Client	System Access	User Authenticated	Logout	None	None	None	None	
✓	1330	22-Apr-2008 11:04:13	drj	192.168.1.103	Carestream Client	System Access	User Authenticated	Logout	None	None	None	None	
✓	1329	22-Apr-2008 11:02:12	drj	192.168.1.103	Carestream Client	System Access	User Authenticated	Login	None	None	None	None	Login Action - Authenticat
!	1328	22-Apr-2008 11:02:05	joel	192.168.1.103	Carestream Client	System Access	User Authenticated	Login	None	None	None	None	Login Action - Authenticat
⚠	1327	22-Apr-2008 10:32:07	root	192.168.1.30	IS Link	System/Application	Activation	Start	None	None	None	None	Service Name: Imaginet M
⚠	1326	22-Apr-2008 10:31:57	root	192.168.1.30	IS Link	System/Application	Activation	Start	None	None	None	None	Service Name: Imaginet M
⚠	1325	22-Apr-2008 10:30:47	N/A	192.168.1.30	RisSync	System/Application	Activation	Start	None	None	None	None	Ris Sync Process Started
⚠	1324	22-Apr-2008 10:30:30	root	192.168.1.30	Workflow Manager	System/Application	Activation	Start	None	None	None	None	Process Name: admin_ser
⚠	1323	22-Apr-2008 10:30:30	root	192.168.1.30	Web Server Software	System/Application	Activation	Start	None	None	None	None	Process Name: Process ID
⚠	1322	22-Apr-2008 10:30:29	root	192.168.1.30	Workflow Manager	System/Application	Activation	Start	None	None	None	None	Process Name: ris_syncP
⚠	1321	22-Apr-2008 10:30:29	root	192.168.1.30	InfoRouter Software	System/Application	Activation	Stop	None	None	None	None	Process Name: Process ID
⚠	1320	22-Apr-2008 10:30:29	root	192.168.1.30	InfoRouter Software	System/Application	Activation	Start	None	None	None	None	Process Name: Process ID
⚠	1319	22-Apr-2008 10:30:28	root	192.168.1.30	Workflow Manager	System/Application	Activation	Start	None	None	None	None	Process Name: pf_latePro
⚠	1318	22-Apr-2008 10:30:28	root	192.168.1.30	Workflow Manager	System/Application	Activation	Start	None	None	None	None	Process Name: pf_dailyPr
⚠	1317	22-Apr-2008 10:30:28	root	192.168.1.30	User Management Admin	System/Application	Activation	Start	None	None	None	None	Process Name: auth_serv
⚠	1316	22-Apr-2008 10:26:37	root	192.168.1.30	InfoRouter Software	System/Application	Activation	Stop	None	None	None	None	Process Name: Process ID
⚠	1315	22-Apr-2008 10:26:32	root	192.168.1.30	User Management Admin	System/Application	Activation	Stop	None	None	None	None	Process Name: Process ID
⚠	1314	22-Apr-2008 10:26:30	root	192.168.1.30	Web Server Software	System/Application	Activation	Stop	None	None	None	None	Process Name: Process ID
⚠	1313	22-Apr-2008 09:32:10	root	192.168.1.30	User Management Admin	System/Application	Activation	Stop	None	None	None	None	Process Name: Process ID
⚠	1312	22-Apr-2008 09:28:56	root	192.168.1.30	InfoRouter Software	System/Application	Activation	Stop	None	None	None	None	Process Name: Process ID
⚠	1311	22-Apr-2008 09:28:53	root	192.168.1.30	User Management Admin	System/Application	Activation	Stop	None	None	None	None	Process Name: auth_serv
⚠	1310	22-Apr-2008 09:28:50	root	192.168.1.30	Web Server Software	System/Application	Activation	Stop	None	None	None	None	Process Name: Process ID
⚠	1309	22-Apr-2008 09:26:28	root	192.168.1.30	IS Link	System/Application	Activation	Stop	None	None	None	None	Service Name: Imaginet M
⚠	1308	22-Apr-2008 09:26:25	root	192.168.1.30	IS Link	System/Application	Activation	Stop	None	None	None	None	Service Name: Imaginet M
⚠	1307	22-Apr-2008 09:26:18	root	192.168.1.30	InfoRouter Software	System/Application	Activation	Stop	None	None	None	None	Process Name: AR_SERV

Remote, Proactive Monitoring

Remote, proactive monitoring is an extremely important function offered by leading cloud-based services, requiring both technology and experienced personnel. Monitoring enables early detection of potential incidents, ideally before they impact users.

Monitoring is executed by a dedicated tool that permanently watches each node of the cloud infrastructure, along with access points at each customer's location and platforms at data centers. Monitoring controls key application processes, systems, and wide area network between the service access point and the data center. An appropriate proactive monitoring infrastructure collects metrics from each device and automatically triggers alerts when a faulty condition is detected. Conditions that trigger an alert can range from a failure to back up data, to unauthorized attempts to access data. Depending on the severity of the incident detected, the monitoring system will send an email to the support team or open a case file and display a visible alarm at the dashboard—allowing follow-up action to be performed by the incident-management team.

In addition to protecting data, monitoring activities also ensure that the systems achieve specified performance and uptime guarantees. Monitoring is conducted 24/7/365 and trained personnel investigate each incident.

Defining the Appropriate Security Policy

The final element in a comprehensive security system is the organization's security policy and its support team. The security policy tracks how security is achieved through the technical and human resources aspects of the product, operations, and organization. The security policy is maintained under the responsibility of a designated security officer. The security officer is involved every time a change is performed to the infrastructure or to the services that could impact data integrity or confidentiality. This includes upgrades, new functionality, or organizational changes.

The Security Policy addresses the following topics:

- Security organization: The security officer ensures that the security policy is updated. Internal audits are conducted and corrective actions are identified and implemented. The officer maintains the list of employees, including staff in human resources, legal, operations, research and development, and other departments.

- Human resources: The policy lists security procedures to be used when employees are hired, resign, or move within the organization. Forms must be signed by employees and security training must be conducted. When an employee leaves, specific network access must be disabled and equipment such as tokens must be returned.

- Assets management: Describes the procedures to ensure that patient information is identified and well managed. It describes how data must be destroyed when required. It explains how equipment is identified (serial number, internal identification number) and where this information is stored and maintained.

- Physical security: Data center security is the responsibility of the hosting company, but the list of employees allowed to enter in the data center is maintained internally and communicated to the hosting company. The data center should restrict physical access and require badges to enter specific areas. Security guards protect the removal of equipment and prevent any unauthorized physical access.

- Operations: Defines the boundaries of responsibility of the hosting company, operations and R&D. Upgrades and monitoring shall be performed by operations, while R&D is the only department that has access to source code. The policy also describes which technical solutions are put in place and enumerates the protocol and encryption mechanisms that are allowed to be used from customer site to the data center resources. Describes how data is secured (copies, media), how changes are tracked (logs), and methods for database back-up.

- Access control: Lists how and from where sensitive data can be accessed and restricts access to appropriate users using SRSA network, secure ID, authentication with login, and passwords. Also describes how servers are hardened and protected.

- Security incident management: Describes the tracking and logging of all security incidents. Depending on incident severity, the security officer may coordinate immediate corrective action, and communicate with R&D (to develop a workaround), operations (to deploy), human resources (should the incident involve an employee), and legal department (in case of a regulation or contract violation).

- Business continuity: Refers to the technical solutions implemented in the data center (RAID, cluster, network and fiber redundancy).

Every healthcare organization needs to ensure that the security policy is endorsed and implemented as part of each element in a cloud–based operation.

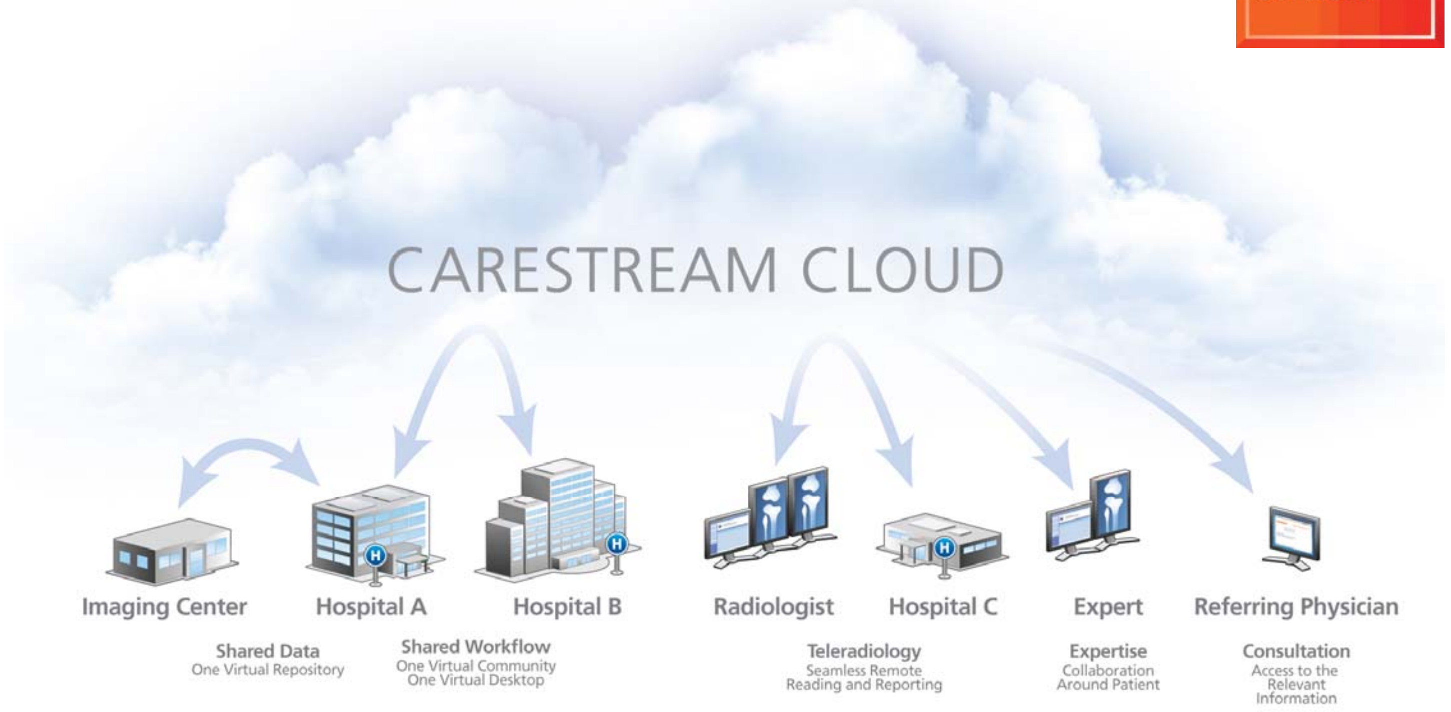
Conduct a Background Check on Suppliers

When a healthcare provider purchases a PACS or archiving system, they are purchasing features that the user must support and protect. Purchasers of cloud-based services are investing in a high-quality service that includes not only uptime guarantees but also data security levels.

Many cloud-based services vendors make the same claims, so how can a healthcare provider decide which supplier offers a better solution? In addition to evaluating data security techniques, conduct a background check on the cloud services provider. How long have they maintained cloud-based services? Ask for customer references.

Carestream Health is a well-respected, worldwide cloud-based services provider that manages 30 million studies (1 Petabyte of data) in ten different clouds. Carestream is a world leader in the technologies, infrastructures, and processes that deliver data security, data integrity, and data privacy. Patient data is protected at all levels of the workflow—including the physical infrastructure of the data center, the hosted application that manages data, and the policies and procedures to maintain continuous security in the cloud.

Vue for Cloud-Based Services



Conclusion: Cloud-Based Services Can Provide the Highest Level of Data Security

It is cost prohibitive for many individual healthcare systems to support the investment in the equipment, technology, personnel, and ongoing training required to deliver the highest level of data security. Converting to best-in-class cloud-based services allows healthcare providers to achieve industry-leading data security—including data availability, integrity confidentiality and traceability. This security is delivered through the physical infrastructure of the data center, the hosted application that manages data, and the policies and procedures that govern data access, audit trails, remote monitoring, incident management, and business continuity.

As the standards for data security rise, it's time to evaluate cloud-based services from a world-class provider. Selecting the best cloud-based services provider for your needs allows this technology to liberate you from security problems.

www.carestream.com

Carestream