FROST & SULLIVAN

VIDEO & VOICE ARCHIVING

A Frost & Sullivan Paper
Sponsored by EMC

Author: Jarad Carleton, Principal Consultant

TABLE OF CONTENTS

AUDIO AND VIDEO RECORDING – A GLOBAL PRACTICE ACROSS INDUSTRIES

Technological advancements and cost reductions for video and voice recording have had a direct impact on the proliferation and increased use of these technologies in a variety of industries and government agencies. The reasons for using video recording, voice recording, or both vary by industry or government agency, but the one common factor across all organizations using these technologies is an increasing need for storage capacity.

Voice Recording

Public Safety

Voice recording technology has been used in public safety control centers around the world for several years as an important part of criminal investigations, which are also submitted to the courts as evidence. These recordings have also been used by public safety officials and civilian oversight committees conducting internal investigations following a serious event where the efficacy or judgment of emergency responders is in doubt. Another less discussed use of voice recording technology in the public safety sector is training. The use of archived voice recordings from past emergencies where public safety officials have had to deal with a variety of issues differing in severity from minor traffic accidents to violent crime have proven invaluable for training new public safety officials.

Financial Services

As voice recording technology improved and costs decreased its use expanded beyond the public safety control centers into the financial services sector where it has been implemented in call centers and on trading floors. Although training is one reason for the use of voice recording in call centers and on trading floors, the driving force behind its use is regulatory compliance and liability risk reduction on a global scale. Thus, one shouldn't be led to believe that voice recording is only used in the U.S.; the truth of the matter is that regulatory oversight in Europe, the Asia/Pacific region, and Latin America are major factors behind the global implementation of voice recording technology today.

Video Recording

The success of UK law enforcement to leverage CCTV video footage to apprehend criminals in cases ranging from child abduction and murder to a serial nail bomber, and identify terrorists has led to an upsurge in CCTV use in the UK leading some to estimate that there are approximately 4.2 million CCTV cameras used in the UK. Successful use of CCTV by law enforcement in the UK has led other nations to implement video surveillance programs and has led to increased interest in the private sector among businesses that could be targeted by terrorists or other types of criminals.

As governments and businesses look towards the UK as a trend setter in what is possible with CCTV use and more systems are implemented, the issue of video archive storage and management has become one of the biggest challenges faced by business and government using the technology. In fact, it is easy to see why archive storage and management can quickly become a cumbersome issue when one considers the fact that these cameras run 24 hours a day and require as much as 30-40 gigabytes of storage per camera each day. In large installations, video archive demands can easily reach the multi-petabyte range depending on how long archives are retained. One of the most significant changes in post 9/11 policy is the retention period for storing video. Historically, video surveillance data was saved for brief periods of one to seven days. Policies have changed for many organizations around the world, with many saving video for months to years depending on the evidentiary situation.

TECHNOLOGY ISSUES

Although audio files are smaller in size than video and less demanding of storage infrastructure, the volume of recorded conversations has grown exponentially in the public and private sectors. The fact is that audio recording of telephone conversations by many organizations in addition to laws such as the European Data Retention Directive that require the retention of call detail records (CDRs) has created a massive content management and archiving challenge.

In addition, when the expanding use of video surveillance technology is taken into account, the content management and archiving challenges become acute due to the fact that modern IP video cameras record onto digital video recorders (DVRs) that are not integrated into an enterprise content management (ECM) system. Complicating matters further, organizations are phasing out video tape archives for operational improvement reasons, and in some jurisdictions they are being replaced due to regulations that directly or indirectly encourage the transition to digital archives.

As that transition continues to take place, the need for archive storage will grow, particularly in organizations that are expanding audio and video recording capabilities for facilities in high threat regions of the world or for those that are high profile targets for criminals.

Digital Video

Although the transition to digital video has enhanced the speed and productivity of personnel tasked with reviewing video surveillance archives, recording to DVR-type devices has created ECM and storage archive problems for the legal discovery process that weren't anticipated by many organizations. The leading problem for most organizations has been the fact that recording video surveillance to DVR systems created siloed storage archives that cannot be centrally managed by an ECM system. The problem has become severe for

As a result of the European Data Retention Directive, a telecom company with 10 million customers could generate over 100 GB a day in call detail records (CDRs).

…in some jurisdictions the elimination of video tape archives is due to regulations that directly or indirectly encourage the transition to digital archives.

Several changes are taking place globally that have translated into increasing storage requirements for video surveillance. The leading factors include:

1. New mega pixel cameras that require 30-40 gigabytes of storage per day.
2. Upgrades of legacy surveillance systems to record video digitally in place of tape.
3. Leveraging IP networks for video surveillance.
4. Expansion and installation of surveillance systems to protect government, business, and private citizens from criminal threats.

organizations with large scale camera deployments in places such as casinos, Embassies, government buildings, ports of entry, high profile financial services buildings, and retail establishments where centralized management, review, legal discovery, and end-of-life disposition are critical for the effective use of video surveillance technology. Another major challenge is how to provide high availability, information protection, and application recoverability in the event of an outage. As the management of large video archives moves into the data center there is an expectation that the same level of protection will be applied to physical security data as is applied to other mission critical applications.

DVR systems create siloed archives that can't be centrally managed by an enterprise content management system. The problem has become acute for organizations with large scale camera deployments.

Digital Audio

Complicating the storage archive silo problem even further, some organizations have also made a practice of digital voice surveillance at places such as ports of entry, places where financial transactions take place, and at the gaming tables of the most modern casinos in the world. This is in addition to digital recording of telephone voice conversations for financial services, law enforcement, healthcare providers, etc., which in some instances also need to be archived and reviewed in conjunction with video surveillance archives. The end result has been a storage archive management nightmare for organizations that have chosen on their own or as a result of regulations to utilize audio and video surveillance as part of daily operations.

Additional silos of information are also being created for audio surveillance that in some instances is created separately from the video surveillance.

The Need for Enterprise Content Management

As the number of storage silos for video and audio increase, it becomes increasingly difficult for a central security office or law enforcement organization to review surveillance files, connect them to related document and case files, and is even worse when the storage silos are in different physical locations and not remotely accessible. Not only do multiple storage silos reduce productivity, a factor that the new technology was supposed to improve, but they also create an operational environment where it becomes more difficult to maintain physical access control to audio and video archive infrastructure. This is critical in situations where audio and/or video are needed as part of a legal discovery process that requires audit trails documenting when files where accessed and by whom. It also creates a situation where archive files could potentially be altered or destroyed intentionally or by mistake.

Not only do multiple storage silos reduce productivity…they also create an operational environment where it becomes difficult to maintain physical access control to the audio and video archive infrastructure.

The Lack of Regulatory Oversight Will Not Continue

Outside of numerous regulations around the world pertaining to video surveillance in casinos and audio recording of telephone calls in the financial services industry, regulations on archive retention, audit trails, and end of life disposition are limited. In many regions of the world, how audio and video archives are stored, retention timelines, and end of life disposition tend to be guided by non-binding government and privacy advocate recommendations rather than actual regulations. The major exception to this state of affairs is the European Union, which has some of the most stringent privacy laws in the world as

a result of the EU Privacy Directive. Outside of Europe however, it is believed that regulations will catch up with use of video and audio surveillance and force the need for comprehensive ECM systems, strict physical access control, time/date stamping of video and audio archives, creation of secure audit trails for archive access, a consistent retention and end-of-life disposition policy, litigation hold capabilities, and dual archive systems that prevent anyone except attorneys and the courts to access original surveillance archives.

EMC TECHNOLOGY SOLUTIONS

Although EMC did not set out to create an end-to-end solution for video and voice content management and archiving, its strategic acquisition of complimentary technologies over the past several years have made it possible to offer organizations a range of technologies and storage solutions that manage the information lifecycle of audio and video files as well as documents that need to be linked with those files. Through the use of EMC® Documentum® for enterprise content management of audio, video, text, and other files, content can be brought under control enabling organizations to apply access controls, business intelligence, workflows, and information lifecycle management to all types of digital content. When combined with storage platforms such as EMC CLARiiON for active recording of audio and video, and EMC® Centera® for regulatory compliant archive storage, organizations are able to achieve levels of business continuity and compliance that were not possible with DVR's and multiple storage silos.

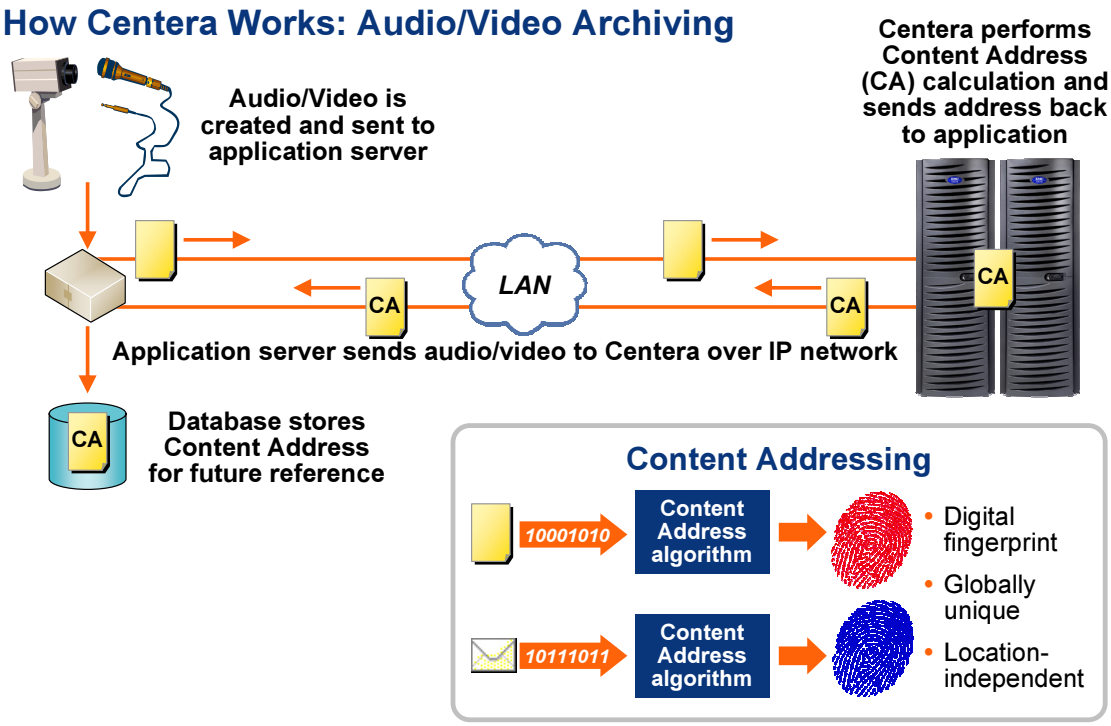
Other acquisitions that have played a role in EMC's offering are VMware for its ability to virtualize hardware and software providing a reduction is management cost, and the acquisition of RSA for information security. Among other features, RSA allows an administrator to access the physical security applications as a credentialed user. This prevents the wrong people from getting access to sensitive information.

EMC® CENTERA® ARCHIVING

Addressing the complex storage archive needs of organizations that rely on audio and video recording, EMC Centera provides end-users with an archive storage solution that enables the elimination of multiple storage silos for audio and video files. EMC Centera is a disk-based IP network storage archiving platform used globally by over 4,500 customers that require fast online access to fixed content archives and guaranteed data authenticity. EMC Centera also simplifies the task of managing, sharing, and protecting content repositories, regardless of size. Its self configuring, self healing, and self managing features help customers meet day-to-day business, governance and compliance requirements.

EMC Centera is an IP network storage archiving platform specifically designed to store and provide fast, easy access to fixed content.

… in the event that any content is altered and stored again, a different content address is created and the new file is then stored. Original fixed content is never overwritten, ensuring an intact audit trail.



EMC Centera keeps audio and video archive secure from unauthorized access, modification, and accidental deletion through the use of its content addressed storage (CAS) system. CAS works by storing and indexing data with a content address (CA) rather than using the physical or logical placement of content within the storage array. With a CA derived from the content itself, EMC Centera eliminates the storage of multiple copies of identical information and the possibility of accidentally overwriting content with similarly named files or directories.

For business continuity as well as for governance and compliance needs, EMC Centera safeguards data using advanced content protection technology[1] within the storage infrastructure. This allows EMC Centera to heal itself when it detects a failing disk drive and to generate new copies of audio / video or other content onto a healthy disk drive. As the self-healing process takes place, the failing disk drive is isolated from the system and can be hot-swapped without disruption to enterprise applications while continuing to allow access to redundant copies of all content stored in the system.

Non-disruptive upgrades are possible for audio and video recording and content management systems since applications no longer require knowledge of a file system location storing content. The result is a dramatic reduction in system/storage management and a solution architected to easily scale to a multi-petabyte solution ideal for audio and

1. EMC Centera offers both Content Protection Parity and Content Protection Mirroring, allowing customers to choose the protection scheme that best addresses their business needs.

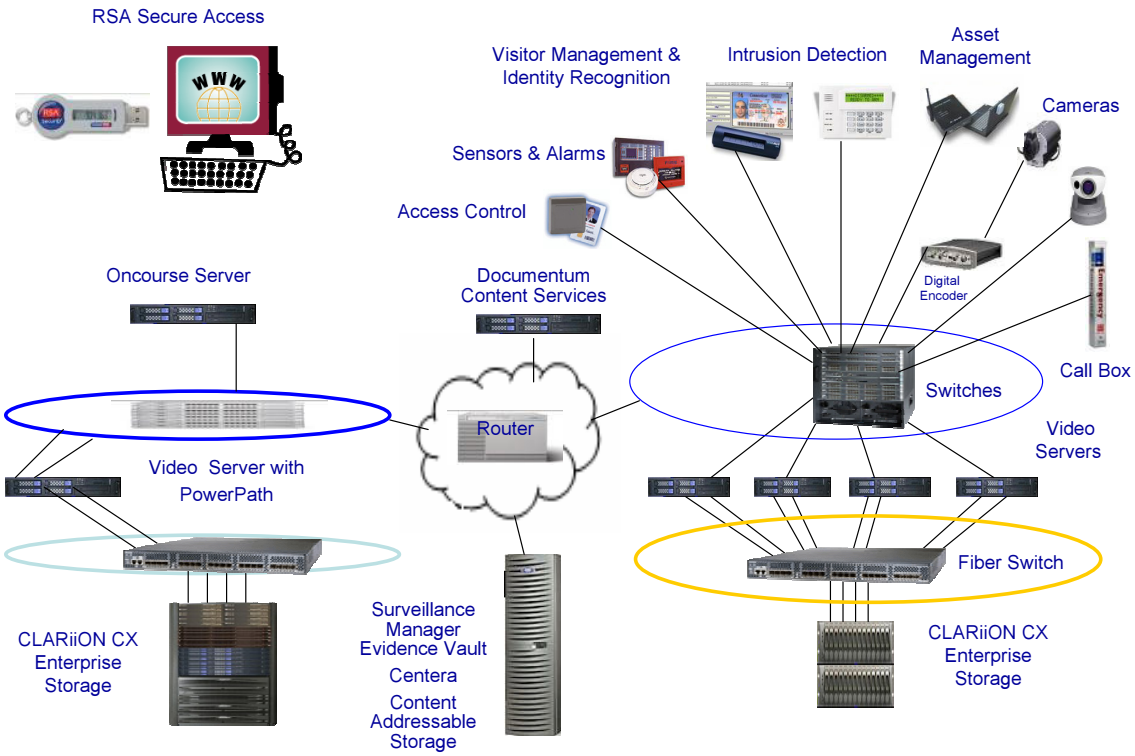
video surveillance archives. In the event that content is accessed and altered in any way, EMC Centera creates a different content address for the altered content before storing them. The unique CA of each piece of content ensures data authenticity and verifiable audit trails, all of which are critical from a regulatory and governance perspective[2].

This high level of data protection and storage management flexibility is crucial for public safety control centers, call centers, financial services, and other organizations that rely on audio and video archives for regulatory compliance and liability minimization. Neither tape nor optical storage can offer this level of availability, reliability, and flexibility as optical jukeboxes can be prone to mechanical breakdown and tape media is known to have high failure rates.

The Business Value of EMC Centera for Surveillance Archiving

Numerous applications including voice, video, and public safety applications from NICE and Verint, and call data record retention and search solutions to meet the EU Data Retention Directive from Sensage actively leverage EMC technology. Furthermore, these applications can target EMC Centera for archive storage by logically separating data into virtual pools. Virtual pools enable the partitioning of content within an EMC Centera cluster thereby restricting the ability of applications to query content outside of authorized pool(s).

Expanded Architecture Example



2. EMC Centera is WORM (write once, read many) storage and was designed to enforce application-based retention periods within its operating software.

Frost & Sullivan

Numerous applications including voice, video, and public safety applications from NICE and Verint, and call data record retention and search solutions to meet the EU Data Retention Directive from Sensage actively leverage EMC technology. Furthermore, these applications can target EMC Centera for archive storage.

Business continuity needs are met by the ability to place priority on restoring video and audio surveillance archives to ensure access to critical files that are important to a civil or criminal investigation.

EMC Centera can be configured to meet the most stringent regulatory requirements by enforcing application-based retention periods within its operating software that permit IT staff to lengthen retention periods, but never shorten them.

EMC Centera supports electronic shredding in accordance with U.S Department of Defense 5015.2 Standard 7 (data destructions standards). This feature enables permanent deletion of content at the end of its information lifecycle when it is no longer needed for legal or regulatory reasons.

This method of data segregation also allows an organization to prioritize which systems to replicate and restore first in situations where systems are taken offline due to natural or man-made disasters. Thus, business continuity needs can be met by enabling the organization to place priority on restoring video and audio archives and minimize any disruption in the ability to access critical files that are important to an investigation. EMC Centera can also be configured to meet the most stringent regulatory requirements by enforcing application-based retention periods within its operating software that permit IT staff to lengthen retention periods, but never shorten them.

Just as important as data retention however, is the importance of end-of-life archive disposition, which is a sensitive matter for organizations needing to comply with the more stringent privacy protection laws in the world. EMC Centera manages end-of-life disposition using U.S. Department of Defense 5015.2 data destruction standards to ensure that destroyed files are unrecoverable. Automating this process for content with expired retention periods frees IT personnel from performing a low-level maintenance task and while also ensuring a standardized data destruction policy to eliminate legal problems that arise with inconsistent data disposition in an organization. However, in the event that surveillance archives are about to expire and are needed as part of a legal discovery process, EMC Centera operating software can enable extension of data retention periods as needed for any eventuality.

CONCLUSION

Audio and video recording has been used around the world for several years by public safety officials, call centers, casinos, and financial services, but increasing crime as well as terrorist attacks in the United States, the United Kingdom, Spain, Turkey, Israel, Russia, Kenya, Tanzania, Yemen, Saudi Arabia, India, Sri Lanka, Indonesia, and other countries has accelerated the use of audio and video recording technology in both the public and private sectors. As usage increases the need for a centralized, scaleable, redundant and highly secure storage archive is critical to ensure audio and video content is available on demand with secure audit trails and guaranteed authenticity.

Since every organization has storage archive needs unique to its business or industry, the ability of a solution to archive content from any business application as well as audio and video content is a capability that maximizes finite IT personnel and budget. Just as important however, is the ability to satisfy the business needs of an organization as well as regulatory mandates governing the retention and end-of-life disposition of archived data. Although many countries don't regulate the retention and disposition of audio and video surveillance files, there is no doubt that regulations will be developed in more lax parts of the world to address privacy concerns, chain of custody issues, retention periods, and permanent destruction of audio and video at the end of the information lifecycle.

As (video) usage increases the need for a centralized, scaleable, redundant and highly secure storage archive is critical to ensure audio and video content is available on demand with secure audit trails and guaranteed authenticity.

… the ability of a solution to archive content from any business application as well as audio and video content is a valuable benefit that maximizes finite IT personnel and budget.

As national laws catch up with the explosion of audio and video recording, EMC Centera is positioned to ensure regulatory compliance for archived content.

EMC Centera offers organizations these capabilities today and is currently used by over 4,500 organizations in the public and private sector as an archive solution of choice in the most stringent and heavily regulated environments around the world. As national laws catch up with the explosion of audio and video recording, EMC Centera is positioned to ensure regulatory compliance for archived content. It is important to keep in mind that being prepared for near-term storage needs is just as important as planning for future regulations that will complicate archive management and create the need for a simplified and secure archive storage solution. EMC Centera has a proven track record helping organizations in regulatory environments to simplify archive storage management and is a solution that should be evaluated by organizations with audio and video archive needs now and in the future.

EMC², EMC, Centera, EMC Centera, CLARiiON, Documentum and where information lives are registered trademarks of EMC Corporation. All other registered and unregistered trademarks are the property of their respective owners.

CONTACT US

Silicon Valley
2400 Geng Road, Suite 201
Palo Alto, CA 94303
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
http://www.frost.com

Palo Alto

New York

San Antonio

Toronto

Buenos Aires

Sao Paulo

London

Oxford

Frankfurt

Paris

Israel

Beijing

Chennai

Kuala Lumpur

Mumbai

Shanghai

Singapore

Sydney

Tokyo

ABOUT FROST & SULLIVAN

Based in Palo Alto, California, Frost & Sullivan is a global leader in strategic growth consulting. This white paper is part of Frost & Sullivan's ongoing strategic research into the Information Technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.

The information presented in this publication is based on research and interviews conducted solely by Frost & Sullivan and therefore is subject to fluctuation. Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or end users.

This publication may not be downloaded, displayed, printed, or reproduced other than for non-commercial individual reference or private use within your organization, and thereafter it may not be recopied, reproduced or otherwise redistributed. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.

For information regarding permission, write:
Frost & Sullivan
2400 Geng Rd., Suite 201
Palo Alto, CA 94303-3331, USA